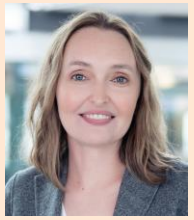
The Risk Agenda for Assurance Functions 2026

Financial Services
PwC
December 2025

In an era of constant motion, resilience, trust and assurance fuel confident reinvention.



Alexandra Burns

Partner
FS Risk, Compliance and Internal Audit Leader

M: +41 79 878 31 69
E: alexandra.burns@pwc.ch

Jürgen Supersaxo

Director
Internal Audit FS Leader

M: +41 79 507 15 32
E: juergen.supersaxo@pwc.ch

PwC
Birchstrasse 160
8050 Zurich
+41 58 792 44 00
www.pwc.ch

The pace and interconnectedness of today's risks are reshaping how organisations grow, compete and are governed. PwC's Value in Motion study highlights how artificial intelligence, climate risk and geopolitical shifts are reconfiguring value pools and creating new 'domains of growth,' underscoring the need for leaders to continually reinvent business, operating and energy models to stay ahead. The scale of change is significant: under a high-trust, high-adoption path, AI could increase global gross domestic product considerably by 2035, while unchecked climate impacts could pull growth in the opposite direction.

In Switzerland, the economic outlook remains mixed. Inflation has eased compared to global peers, while export exposure and sector-specific challenges – particularly in the energy and housing sectors – persist. The Swiss National Bank's monetary stance, alongside broader market conditions, continues to influence corporate risk profiles and assurance function priorities across financial services.

Against this backdrop of economic, regulatory and technological change, assurance functions in Switzerland play a pivotal role in transforming complexity into confidence – supporting boards and audit committees with forward-looking insights, agility and assurance.

This year, our document covers the following areas:

- **Macro risk landscape**: Latest perspectives on global and geopolitical uncertainty, highlighting the realignment of political and economic systems and their implications for risk and resilience in financial services
- **Regulatory landscape**: Key developments from FINMA, SNB and Swiss industry bodies shaping the national regulatory agenda, with selected international intersections in areas such as liquidity, governance, sustainability and financial resilience
- **Risk hot spots**: We have curated a list of risk hot spots that are shaping boardroom discussions and affecting the financial services sector. These are emerging and evolving areas of risk that assurance functions should be bear in mind when setting priorities for the year ahead.
- **Internal audit practices and capabilities**: This section includes what is front of mind for chief audit executives. We share our point of view on the early experience of the implementation of the Institute of Internal Auditors' (IIA) Global Internal Audit Standards, which came into effect in January 2025. Finally, we consider good practices in relation to adopting AI in internal audit.

We hope you find this a helpful document to guide planning for the year ahead and spark meaningful conversations on risk and reinvention. If you would like to discuss any aspect further, please do not hesitate to contact us or one of our colleagues, whose contact details you will find at the end of this paper.

PwC's Value in Motion study

Contents

1

Macro risk landscape

- Geopolitical uncertainty

Geopolitical uncertainty (1/3)

What organisations should be doing

Against the backdrop of this continued volatility, business leaders remain focused on adaptability and resilience.

Summary

We continue to live in an era of geopolitical uncertainty. The systems and structures that have helped govern the global system in recent decades are weakening and changing. Responding to this changing environment, world powers are competing for influence and looking to new diplomatic, economic and security relationships. The level and pace of geopolitical shifts and shocks looks unlikely to be checked in the months ahead.

For businesses, changes in the geopolitical environment will affect supply chains and production, regulatory and fiscal environments, global trade and tax norms, the movement of information, and the security of workforces, facilities and technology. In the coming year, organisations will face the challenges emerging from three strategic themes:

Political realignment

01

Globalism to regionalism

02

The decline of multilateralism

03

Adaptability

As uncertainty increases, predicting the trajectory of international events will become increasingly difficult. Businesses need effective monitoring and scenario analysis to provide early warning of emerging risks and opportunities. Agile responses are required to mitigate risks effectively.

Resilience

With the pace of change accelerating, businesses will not be able to plan for every scenario. Resilience means building the capacity to absorb shocks, maintain critical operations and adapt quickly to new realities, ensuring that organisations can withstand disruption while positioning themselves for recovery and growth.

Geopolitical uncertainty (2/3)

Strategic themes

Looking to the year ahead, there are several strategic trends shaping the operating environment for Swiss and international firms.

Political realignment

Many of the world's democracies are in transition following the 'year of elections.' Accompanying this is the growing popularity of far-right politics, increased political polarisation and a resulting rise in societal tensions.

Political realignments will be felt differently in different countries. This is most significant for businesses with an international footprint, where the political cultures of particularly Western democracies may be increasingly diverse. Organisations managing global workforces will need to navigate issues ranging from diversity, equity and inclusion to immigration and regulation.

Political transitions

2025 will be defined by political transitions as the anti-incumbent wave of 2024 elections reshapes governments worldwide. With opposition movements gaining influence and voter frustration fuelling polarisation, geopolitical uncertainty is set to rise.

The new normal

Western Europe, including Switzerland, faces challenges from US tariffs, slow economic growth and insecurity. Finding lasting solutions to these issues will prove extremely difficult.

From globalism to regionalism

Multilateralism – the cooperation of multiple countries through international institutions and agreements – has long underpinned global diplomacy and trade. As approaches to multilateralism evolve, we are seeing a shift away from Western-led structures towards alternative models of influence. This is placing greater emphasis on regional alliances, national security priorities, protectionist trade barriers and heightened competition over the control of emerging technologies.

An increased focus on regionalism could affect global trade practices and encourage more localised models. Securing resilient, cost-effective supply chains will be increasingly challenging as organisations navigate complex regulatory environments, rising trade barriers and the weaponisation of trade as a geopolitical tool.

Trade re-orientation: Politically motivated and national security-related trade barriers are continuing to reshape world trade. Divergence between the West and other regions could result in incompatible trading and market regulations across all sectors, which will affect data sharing, among other things.

Technology: Competition is at the forefront of technological innovation and will remain a key geopolitical driver. The focus on artificial intelligence, quantum computing and other advances, including blockchain and digital assets, will lead to continuing competition over all aspects of innovation, from critical minerals to data, intellectual property and financial infrastructure. Controlling tokenisation, central bank digital currencies (CBDCs) and digital payment systems is becoming increasingly linked to national security, digital sovereignty and future economic influence.

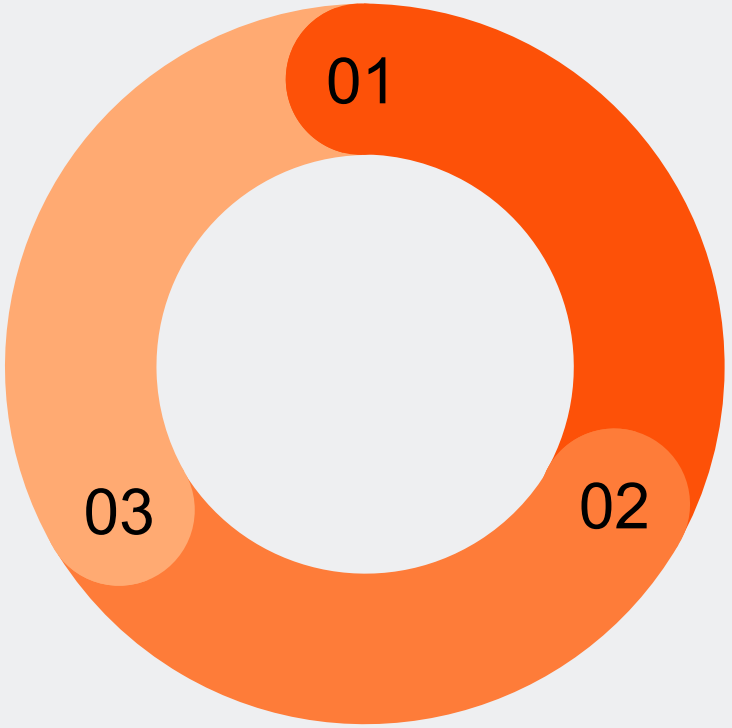
Changing international alignments: Emerging coalitions are gaining momentum and offering small and medium powers alternatives to a Western-led order. This could have implications for global security, as well as creating new norms and opportunities in global trade.

Geopolitical uncertainty (3/3)

The decline of multilateralism

International institutions and norms that have long governed states' behaviour are weakening, leading to some states taking bolder unilateral actions with fewer consequences. As a result, conflicts, cyber and physical sabotage attacks continue to proliferate, and increased uncertainty and insecurity are driving defence spending worldwide.

The decline of multilateralism could lead to shifting global alliances, greater insecurity and a disregard of international rules and conventions. Such changes can affect supply chains and production, regulatory and fiscal environments, global trade and tax norms, free movement of information, and the security of workforces, facilities and technology.



01 Europe-Russia relations

Russian influence campaigns and 'grey zone' attacks such as cyber, sabotage, assassination attempts on defence industry executives, and attacks on undersea infrastructure will probably continue. This could undermine EU and North Atlantic Trade Organisation (NATO) unity, complicate the operating environment and raise direct security threats.

02 Shifting approaches to defence

Rising geopolitical uncertainty, combined with US pressure on its allies to increase contributions, is likely to reshape approaches to defence spending. This could trigger action–reaction cycles, boosting opportunities for defence and security industries while reducing government funding available to other sectors.

03 Conflict proliferation

As international norms break down and international institutions weaken, there is a growing risk of interstate conflict. Even limited conflict can have an impact on security, operations, markets and supply, particularly if organisations are faced with several crises at once.

2

Regulatory landscape

- Key regulatory developments in the Swiss financial sector

Regulatory landscape

Key regulatory developments in the Swiss financial sector

Q1/Q2 2025

- FINMA information sheets: mandated enhancement of supervisory instruments
  - Early intervention
  - Crisis instruments
  - Fines
  - Public information
  - Accountability regime
- Information Security Act (ISA) and Cybersecurity Ordinance (CSO)
- FINMA Circular 2025/4 'Consolidated Supervision'
- FINMA Circular 2025/3 'Liquidity – insurers'

Q3/Q4 2025

- Consultation: FINMA Ordinance on liquidity for banks and securities firms (LiqO-FINMA) – daily liquidity reporting ability in times of stress
  - Planned entry into force: 1 January 2027
- Consultation: Capital Adequacy Ordinance (CAO) – Full common equity tier 1 (CET1) deduction for software and deferred tax assets, prudent valuation adjustments, stricter additional tier 1 (AT1) payout rules
  - Planned entry into force: 1 January 2027
- Revision of FINMA Ordinance on Accounting
- Swiss Bankers Association (SBA) recommendations for BCM

Dec 2025

Jan 2026

- Consultation: Banking Act and CAO – Full CET1 deduction for foreign participations
  - Planned entry into force: 1 January 2028
- Consultation: Transparency of legal entities and combating money laundering and terrorist financing
  - Planned entry into force: Q3/4 2026
- Extension of the international automatic exchange of tax matters (AEOI) to crypto assets

- 2026 -

- Entry into force:
  - FINMA Circular 2026/1 'Nature-related Financial Risks'
  - Asset Management Association Switzerland (AMAS)/SBA Greenwashing self-regulation
- Regulatory developments resulting from PUK report postulates, motions:
  - 'Too big to fail' regulation
  - The future of regulatory audit

Dec 2026

- First test deliveries for new individual credit survey (Einzelkrediterhebung, EKE):
  - First reporting: March 2027

2027+

- New programme (Extended Liquidity Facility, ELF): Expanded SNB emergency liquidity for all Swiss banks
- December 2027: Ending transition period preparatory measures for timely and proper payout of secured deposits in the event of insolvency
- FINMA Ordinance on risk diversification for banks and securities firms (RDO-FINMA) and LiqO-FINMA
- 'Too big to fail' instruments for withholding tax

3

Risk hot spots

Contents

Artificial intelligence (AI)

Governing agentic and generative AI: managing autonomy, ethics and accountability in intelligent systems

The challenge

Agentic and generative AI systems are transforming how financial services firms operate, innovate and engage with customers. These advanced systems autonomously make decisions, generate content and execute tasks in complex enterprise settings with minimum human intervention. As their capabilities grow, the boundary between human-led and AI-driven actions is becoming increasingly blurred.

Regulatory landscape driving change

The regulatory environment is evolving rapidly to address AI-specific risks:

- **EU AI Act (2024-2027):** Risk-based classification framework
  - Prohibited AI practices (social scoring, real-time biometric surveillance)
  - High-risk systems require conformity assessments, human oversight and transparency
  - **Fines up to EUR 35 m or 7% of global annual turnover**
- **UK AI Governance Principles**: Safety, transparency, fairness, accountability and contestability embedded in sector regulation
- **Financial Conduct Authority (FCA) expectations:** Consumer duty compliance for AI-driven customer outcomes; algorithmic accountability; clear governance and oversight
- **Prudential Regulation Authority (PRA) priorities**: Model risk management frameworks; operational resilience for AI-dependent processes; board-level AI literacy

Compliance timeline: EU AI Act provisions begin in August 2025 (prohibited practices), with full compliance required by August 2027.

Governance imperatives for financial services

Organisations must act now to build effective governance frameworks that enable innovation while managing risk:

Design AI-specific risk frameworks that account for autonomy, decision thresholds, safe failure modes and alignment with human intent.

Establish board-level AI oversight with clear accountability, risk appetite statements and regular reporting on AI portfolio risks.

Implement explainability and transparency practices to ensure that stakeholders understand how outputs are generated and decisions made.

Map decision boundaries defining where AI can operate independently and where human judgement must intervene, including escalation protocols.

Continuously monitor training data and model performance to detect bias, drift and harmful content, and to ensure responsible data sourcing.

Prepare for evolving AI regulations, including sector-specific expectations from FCA, PRA, Information Commissioner's Office (ICO), and alignment with EU AI Act requirements.

Embed AI governance within enterprise risk frameworks to ensure consistency across credit, operational, model and cyber risk domains.

Promote a culture of responsible AI use supported by values-based principles and cross-functional collaboration across data, risk, legal, compliance and assurance teams.

Understanding complexity, autonomy and governance requirements across the AI adoption spectrum

The evolution path

Stage 1
AI-embedded

Simple, rule-based automation
Examples:
E-mail filters, basic chatbots

Governance
Standard IT controls

Stage 2
AI-led enhancement

Intelligent process automation
Examples:
Document processing, KYC automation

Governance
Enhanced monitoring and human oversight

Stage 3
AI-driven reinvention

Strategic transformation
Examples:
Credit decisioning support, fraud detection

Governance
Model risk management and ethical frameworks

Stage 4
Agentic enterprise

Autonomous goal-seeking systems
Examples:
Portfolio optimisation, dynamic pricing

Governance
Continuous assurance and accountability boundaries

Use case risk matrix: complexity vs autonomy

Low risk (simple and low autonomy) → light-touch governance
- E-mail categorisation, meeting scheduling, smart notifications
- **Controls**: Standard IT oversight, basic logging

Medium risk – supervised (complex and low autonomy) → human in the loop
- Regulatory report generation, contract analysis, customer service chatbots
- **Controls:** Output validation, escalation protocols, audit trails

Medium risk – autonomous (simple and high autonomy) → exception management
- Transaction monitoring alerts, data quality checks, routine reconciliations
- **Controls:** Threshold monitoring, regular review, kill switches

High risk (complex and high autonomy) → board oversight required
- Algorithmic trading, credit approval automation, dynamic pricing engines
- **Controls:** Pre-deployment validation, continuous testing, independent assurance, regulatory reporting

FS AI risk taxonomy: a structured framework for identifying, assessing and managing AI-specific risks for financial services

Risk level	Risk category	Key risk indicators		Potential impact
CRITICAL	**Model risk**	• Training data bias and quality issues • Model drift and performance degradation	• Overfitting and poor generalisation • Hallucinations and incorrect outputs	Direct customer harm, wrong decisions, regulatory breach
CRITICAL	**Operational risk**	• Loss of human oversight (automation bias) • Third-party AI vendor dependency	• System failures and cascading effects • Integration complexity with legacy systems	Business disruption, service outages, customer complaints
CRITICAL	**Compliance and regulatory risk**	• Unexplainable AI decisions (consumer duty violations) • Breach of FCA/PRA expectations	• GDPR/DPA data protection violations • Inadequate model documentation	Fines up to EUR 35 m (EU AI Act), licence conditions, enforcement action
HIGH	**Security and resilience risk**	• Adversarial attacks and data poisoning • Model extraction and intellectual property theft	• Prompt injection and jailbreaking • AI supply chain vulnerabilities	Confidentiality breaches, system manipulation, reputational damage
HIGH	**Ethical and reputational risk**	• Discriminatory outcomes (protected characteristics) • Lack of transparency and explainability	• Erosion of customer trust • Media scrutiny and brand damage	Long-term franchise value erosion, customer attrition
MEDIUM	**Strategic risk**	• Misalignment with business objectives • Over-reliance on AI for competitive advantage	• Skills gap and talent retention challenges • Opportunity cost of wrong AI investments	Competitive disadvantage, missed innovation opportunities

AI governance operating model: embedding AI assurance throughout the organisation with clear accountability

Three lines of defence for AI

1st line: Business units and AI developers

Owns: AI use case design and deployment; define AI requirements and responsible use principles; conduct initial bias and fairness testing; maintain model documentation, logs and performance monitoring, and identify and escalate AI risks and incidents.

2nd line: Risk, compliance and AI ethics

Owns: AI risk frameworks, policies and oversight; develop AI risk appetite and tolerance metrics; validate model risk assessments and bias testing; review third-party AI vendor arrangements; monitor regulatory changes and operate AI Ethics Review Board.

3rd line: Internal audit

Owns: Independent assurance over AI governance; audit AI governance effectiveness and board oversight; test controls throughout AI lifecycle (design → deployment → monitoring); assess skills and capability adequacy across all three lines and provide forward-looking risk insights to Audit Committee.

Governance overlay: Board/Audit Committee (ultimate accountability) → AI Governance Committee (cross-functional oversight) → Senior Management (strategy and risk appetite)

Role	AI knowledge required	Training priority
Board/ Senior Management	AI strategy literacy, ethical implications, risk appetite	**High – Quarterly updates**
1st line Business	Responsible AI use, output validation, prompt engineering	**High – Role-based training**
2nd line Risk	Model risk frameworks, bias testing, vendor due diligence	**Critical – Specialist certification**
3rd line Internal audit	AI audit methodologies, data analytics, control testing	**Critical – Annual CPE requirement**
AI specialists	MLOps, explainability, adversarial testing	**Medium – Continuous learning**

Assurance functions' focus areas for AI assurance in 2026

Critical audit domains

01 | Governance and accountability

- Is there a board-approved AI strategy with clear risk appetite?
- Does the AI Governance Committee have the appropriate mandate and meeting cadence?
- Have escalation protocols for AI incidents been defined and tested?
- Is accountability clear for AI decisions?

Approach: Charter review, committee minutes, decision log analysis

02 | Model lifecycle and data management

- Are AI models validated before deployment?
- Is training data documented with lineage and bias testing?
- Are model performance metrics monitored with drift detection?

Do audit trails capture all AI decisions?

Approach: Technical testing, log review, validation reperformance

03 | Reg. compliance and consumer outcomes

- Are AI systems compliant with applicable laws and regulations?
- Is model explainability sufficient for regulatory authorities?
- Are customer-facing AI disclosures clear?
- Can customers challenge AI decisions?

Approach: Regulatory mapping, customer journey testing, complaints analysis

High-priority audit domains

04 | Third-party AI risk management

- Has due diligence been performed on AI vendors?
- Do contracts include liability and exit provisions?
- Is vendor performance monitored against SLAs?

Approach: Vendor file review, contract analysis, performance dashboards

05 | Ethical AI and bias management

- Are fairness metrics tested across protected characteristics?
- Is there an AI ethics review board with documented decisions?
- Are bias results acted upon?

Approach: Statistical testing, ethics committee minutes, culture surveys

06 | Skills, training and culture

- Have AI literacy programmes been rolled out?
- Are critical AI roles appropriately filled?
- Can employees escalate AI concerns safely?

Approach: Competency assessments, training records, speak-up metrics

Cybersecurity

Identity and access management (1/2)

Identity attackers are increasingly using compromised identities as an entry way into organisations to exfiltrate data. Robust identity management is key to defending organisations against modern identity threats such as phishing, credential stuffing and social engineering.

Attacks on identities are increasingly becoming the primary cause of significant cyber breaches. The conventional perimeter is disappearing and identity has emerged as the new perimeter. In increasingly hybrid and cloud-native environments, users are accessing systems from multiple locations, devices and networks. Infrastructure is thus becoming increasingly virtualised, with third parties and customers connecting via platforms and portals.

Identity is complex in sectors in which potentially thousands of internal users and extensive third parties have access and legacy systems do not integrate well with modern systems. Identity is not just a tech problem. It is also a governance problem, and many organisations struggle with orphaned accounts, overprivileged roles, lack of joiner-mover-leaver enforcement and minimum identity assurance for non-human accounts.

The challenges surrounding identity management are compounded by the growing prevalence of non-human identities, such as service accounts, application programming interfaces (APIs), bots, and Internet of Things (IoT) devices, which often lack the same level of oversight and governance as human users. These non-human identities are frequently overprivileged or poorly managed, creating significant vulnerabilities that attackers can exploit. Additionally, the rise of remote work and hybrid work models has further blurred the boundaries of traditional identity management, as employees and contractors access sensitive systems from personal devices and unsecured networks.

Key considerations for firms

In the financial sector alone, 93% of organisations have experienced at least two identity-based attacks in the last 12 months. As a result, increased investment in identity security is more pertinent than ever, especially if there has hitherto been a lack of investment. Organisations should look at leveraging modern identity controls from the outset to bolster identity security.

80% of data breaches stem from compromised identities with third-party access, which is considered an increasingly common identity governance challenge for organisations. Evolving threats require strategies to be adjusted, moving from compliance-led to more threat-led.

Security programmes to defend organisations against the compromise of identities can be uplifted by implementing a zero-trust access principle to modernise identity and access controls. Identity controls also need to be hardened against evolving threats, with specific training on new social engineering threats and dedicated training for help desk staff provided.

Building threat focused identity capabilities can be done by focusing on:

- Continuous identity security posture and exposure management
- Identity threat detection and response
- Just in time and just enough access
- Risk based access controls.

Regulatory compliance adds another layer of complexity to identity management. Data protection regulations mandate robust identity verification and access controls. Failure to comply with these regulations can result in severe financial penalties and reputational damage, further underscoring the importance of a strong identity governance framework.

Threat management tooling should also be extended to cover identity by deploying identity-specific threat detection and response tooling and expanding red and purple teaming to cover identity-based attacks and social engineering.

Identity and access management (2/2)

Assurance functions: focus areas

01

Governance and strategy

- Assess whether identity and access management (IAM) governance structures, roles and accountabilities are clearly defined and aligned with the firm's overall security strategy and risk appetite.
- Review board and senior management oversight, including reporting mechanisms, KPIs/KRIs and escalation protocols.
- Evaluate whether IAM policies, standards and procedures are up to date, approved and consistently implemented across the organisation.

02

User access provisioning and lifecycle management

- Test the adequacy and timeliness of access provisioning, modification and de-provisioning processes (e.g. joiners, movers, leavers).
- Validate segregation of duties controls to ensure access conflicts are identified and appropriately mitigated.
- Confirm whether privileged access management (PAM) processes are in place and effective.
- Regularly execute recertification process to validate user access.

03

Authentication and access controls

- Evaluate the use and effectiveness of multi-factor authentication (MFA), password standards and session management.
- Review system-enforced access controls and role-based access models to confirm alignment with the principle of least privilege.
- Test access restrictions to critical systems, applications and sensitive data, including cloud and third-party-hosted environments.

04

Monitoring, logging and incident management

- Review the design and effectiveness of monitoring controls, including logging, alerting and anomaly detection for unusual access activity.
- Assess whether escalation and incident response processes for IAM-related breaches are defined, tested and aligned with broader operational resilience frameworks.
- Validate the adequacy of periodic user access reviews, certification processes and reconciliations across business-critical systems.

05

Regulatory and compliance alignment

- Evaluate alignment of IAM controls with regulatory requirements (e.g. DORA, ISO 27001, NIST).
- Confirm that IAM practices are adequate to support audit trails, accountability and regulatory reporting expectations.

Response and recovery (1/2)

Response and recovery are a crucial part of cyber security to ensure business continuity and minimise damage from security breaches. Only 2% of companies have implemented cyber resilience actions throughout their organisations in all the areas surveyed.

Response: Prompt, decisive action is crucial when a cyber breach occurs. Initially, it is imperative that the incident be quickly detected to ensure that anomalies are recognised and reported immediately. Following detection, compromised systems must be isolated swiftly to halt the attack's progression and prevent the threat from spreading further, enabling response teams to focus on mitigation strategies without incurring additional damage.

Recovery: Preserving evidence is vital during the recovery process. This involves capturing system logs, taking snapshots and rigorously documenting all actions taken throughout the incident response. Such measures not only support investigations but also enhance the organisation's ability to bolster future defences. Equally important is the safe and secure restoration of systems, data and services to their original state. Resilience in recovery processes is pivotal for maintaining operational integrity and rebuilding stakeholder confidence.

In the past 12 months, cyber incidents such as those targeting a prominent UK retailer and attributed to Scattered Spider have had considerable repercussions. These attacks led to significant operational disruptions, including an inability to process online orders and shortages on store shelves. Furthermore, they caused a sharp decline in share prices and eroded customer trust, highlighting the profound impact of cyber threats on businesses. The necessity for robust response and recovery strategies has never been more apparent, as organisations strive to protect their assets and uphold their reputations in the face of increasingly sophisticated threats.

Key considerations for firms

There are time-sensitive actions that should be taken in the first moments of a ransomware incident, including:

- Embarking on immediate action to limit the damage (e.g. disconnecting critical systems).
- Appointing/consulting with specialist third parties, including:
  - External legal counsel
  - Incident response (IR) provider(s)
- Invoking a command-and-control structure
- Deciding whether to operate under legal privilege
- Identifying safe channels for communications.

Organisations are often not prepared for the rapid, sophisticated response required. With complex IT environments and often unclear information about critical systems, restoration can present a significant challenge.

Organisations must engage constructively with regulators and ensure that they understand the obligations in managing the response potentially across multiple jurisdictions.

Sustaining business operations while IT systems are being recovered presents a challenge, often necessitating the continuation of business activities without IT support, potentially lasting several weeks or longer.

In the initial stages of a ransomware incident, timely actions are crucial. Organisations should ask questions like:

- Have we identified and mapped out essential business processes?
- Do we have immutable back-ups in place, and have we tested our ability to restore from them?
- Are there contingency plans for vital business operations?
- Can we restore our most privileged assets and accounts, including identity management systems like Entra and IAM services, if needed?

Further considerations include the following:

- Have we established clear communication channels for crisis management?
- Do we have an incident response team ready to engage immediately?
- Are the security patches and system updates current?
- Can we quantify the potential financial and reputational impact?

These questions help to assess readiness and resilience in facing IT risks and ensuring business continuity.

Response and recovery (2/2)

Assurance functions: focus areas

01

Governance and oversight

- Assess clarity of roles, responsibilities, escalation protocols, and board and senior management oversight during cyber events.
- Assess how cyber response and recovery arrangements incorporate third parties, suppliers and outsourced services.

02

Incident detection and response

- Review monitoring, detection and response processes, including timeliness and effectiveness of escalation.

03

Recovery and continuity

- Evaluate recovery strategies, playbooks and restoration plans for critical systems and data to confirm alignment with resilience requirements.

04

Testing and exercises

- Validate the adequacy and frequency of cyber incident simulations, crisis management exercises and integration of lessons learned.

05

Regulatory and reporting compliance

- Review alignment with regulatory requirements (e.g. DORA, NIS2) for incident reporting, notification timelines and recovery expectations.

Threats emerging from AI (1/2)

Advances in AI have led to exploitation shifts and a widening gap between development and detection capabilities.

In the world of cyber threat actors, automation is not a new concept. Whether it is automating the scanning of vulnerable internet-facing devices or scripting functions that easily propagate ransomware across a network, the modern threat has evolved to be an automated attack system. This notion raises the question of how will new AI technologies change the way attackers conduct their malicious activities, which in many cases, are already relying less on human input.

The degree to which AI, particularly GenAI, technologies have advanced over the past year is significant and indicative of an ongoing race among those seeking to develop, invest in, embrace, operationalise and exploit these solutions. This advance, however, has caused a widening gap between these technologies and the technologies developed to detect AI-generated content and media.

Threat actors have, and will, continue to capitalise on this widening gap, exploiting AI solutions and developments to enhance their operations and impact on victims. By leveraging AI, threat actors will be able to enhance their attacks, making them faster, more sophisticated and more targeted than ever before. This targeting at scale underpins the importance for continuous threat exposure management to proactively identify, assess and mitigate risk, and highlights the need for organisations to prioritise robust, timely vulnerability management.

Key considerations for firms

The potential use cases for a threat actor leveraging AI could theoretically be endless. However, there are several areas that stand out and can potentially improve the success of attacks:

- Enhanced personalisation of social engineering operations;
- Targeting at scale;
- Identification or processing of targets; and
- Accelerated reverse engineering of 0-day vulnerabilities.

As the threat landscape is constantly evolving and with the advances in AI contributing to the situation, organisations must:

- Have an accelerated process for protecting against new cyber threats and 0-day vulnerabilities, and increase dependence on AI-/ML- powered anomaly detection solutions (xDR) to identify new exploits quickly;
- Maintain robust supply chain and third-party management;
- Have clear accountability and responsibility of AI and machine-learning security within the organisation;
- Ensure that security is factored into any decisions on AI adoption;
- As AI provides increased capabilities in reconnaissance and social engineering, it is imperative that training and awareness programmes of organisations be adapted to address this accordingly; and
- AI should also be leveraged to improve the detection and triage of cyber attacks.

The following exploitation trends have also been identified:

Threat actors using AI tools to conduct reconnaissance activities against a target organisation, its operations and employees, as well as the broader industry, for use in follow-on activities, such as financially motivated attacks, exploitation of identified vulnerabilities, disinformation campaigns, and social engineering against key roles.

Threat actors targeting AI tools that may be adopted by an organisation, such as customer-facing chatbots or internal tools used by the organisation's employees, to steal sensitive information (e.g. user inputs involving proprietary information, biometrics, user behaviour analytics, etc.).

The use of deepfake video content and AI-generated voice-based technology pose detection challenges. Voice or audio is one of the most important channels of human communication, and GenAI developments in this space will therefore have potentially significant ramifications for security. There have already been numerous documented examples malicious threat actors seeking to exploit this type of content generation. Application to date has largely, although not exclusively, been financially motivated, but the potential application of this technology is much wider, including for espionage or disinformation purposes.

Threats emerging from AI (2/2)

Assurance functions: focus areas

01

Governance and risk assessment

Assess how AI-related cyber risks are identified, evaluated and integrated into the enterprise risk governance, taxonomy and cyber risk appetite.

02

AI system security

Evaluate safeguards protecting AI models, data and algorithms from manipulation, adversarial attacks, or unauthorised access. Ensure control of data input and output, as well as continuous testing where appropriate, to avoid model drift.

03

Threat detection and monitoring

Review controls for detecting and responding to AI-enabled attacks, including anomaly detection, behavioural analytics and incident escalation processes. Compare security activities (security patching timelines) against AI-powered acceleration of threats.

04

Third-party and supply chain risks

Verify oversight of AI-related risks introduced through vendors, cloud providers and third-party tools. Ensure that the role played by third parties versus the organisation in terms of the EU AI Act is clearly defined, particularly if a third party customises and AI model in any way.

05

Training and awareness

Test training and awareness programmes to ensure that employees can recognise AI-enabled threats (e.g. deepfake fraud, generative phishing) and respond appropriately.

06

Regulatory and ethical alignment

Validate alignment with emerging regulatory standards and ethical guidelines on AI use in cyber defence and resilience.

Quantum advances: new horizons in cyber threats (1/2)

Advances in quantum computing mean that world governments anticipate the availability of a cryptographically relevant quantum computer (CRQC) between 2029 and 2035. The threat to modern cryptography is substantial, with asymmetric encryption, typically used for internet communications and crypto currencies, most at risk. However, all forms of cryptography will probably need to be reviewed and enhanced. Digital signatures (code signing, identity, transaction authorisation) are equally critical. Harvest-now-decrypt-later risk means long-lived data (5–20+ years) is exposed today. Plan for post-quantum cryptography (PQC) first. Use quantum key distribution (QKD) selectively for niche high-assurance links – QKD is not a substitute for PQC.

Based on historic precedent, governments anticipate a transition period to newer PQC of 5–7 years, and some have begun to mandate clear milestones for 2025 and 2026 to launch the effort to identify and inventory cryptography used by organisations, with dates to complete the work varying from 2030 to 2033.

Whilst modern IT devices are generally capable of handling the new PQC algorithms, many older IT devices, and most OT/ICS devices will need to be upgraded. Plan phased refresh of HSMs, network gear, smartcards/tokens and firmware. Test performance impacts (larger certs/handshakes) and enable hybrid TLS/VPN as quick wins. A period in which replacing cryptographic algorithms is automated, so-called cryptographic agility, is also predicted.

Key considerations for firms

Identifying and inventorying the use of cryptography across the technology estate and mapping key elements that will drive risk scoring are the current priority task, resulting in the creation of a so-called crypto-inventory.

This should be automated, continuous and comprise scans of network traffic, corporate data and cryptographic libraries used in software (CBOM) in order to be complete. In 2026 the focus should shift to assessing the risk exposure of each use case identified, so that work can be prioritised.

Specific recommendations for organisations to consider include:

- Regulatory expectations vary by sector, and historic legislation has broadly addressed the topic calling for inventories of cryptography such that rapid replacement of vulnerable algorithms can be performed (GDPR, DORA, EIDAS, NIS2, etc.), though more specific expectations have not been defined.
- Data breach recording, particularly when classified down due to encryption, should begin to record the type of encryption in use for future reference.
- Supply chain considerations around vendors, cloud technology and hardware procurement should be shaped now to smooth the transition.
- A centre of cryptographic excellence should be established to assess veracity of rumours and threats, and deal with bespoke cases.

Additional points to consider

Most technologists understand that Moore's Law has meant humans tend to underestimate the exponential acceleration of computing power. Quantum has accelerated faster than standard exponential, meaning Q-Day (the date a CRQC is known to exist) and the speed with which further challenges will develop is also usually underestimated.

Even leading government bodies recognise the complexity of such activity to identify and ultimately replace modern cryptography. Governments have established a programme office for civil services, with a mandate to replan annually as Q-Day draws closer and understanding of the nature of complexity of crypto usage grows. Western governments have a multi-year plan and budget set aside, but recognise that this will need to be reviewed and revised annually.

Organisations should prepare for a more turbulent future with cycles of cryptographic vulnerabilities, and rather than assume that PQC algorithms will remain indefinitely secure should prepare for a period during which much more frequent cycling of algorithms is required.

So-called 'crypto-agility' is an approach to (semi-)automatically replace cryptographic algorithms in a much faster and automated way.

It is recommended that organisations architect for crypto-agility as they work through PQC deployment work.

Quantum advances: new horizons in cyber threats (2/2)

Assurance functions: focus areas

01

Cryptography inventory and governance

A robust transition strategy is essential for migrating to PQC. This involves risk assessment, prioritising critical systems and planning phased migrations.

02

Crypto-agility and readiness

The ability to switch cryptographic algorithms rapidly is a cornerstone of quantum resilience. Technical readiness means upgrading infrastructure and piloting PQC solutions.

03

Third party and cloud

Organisations must assess vendor and cloud service compliance, update contracts and coordinate migration plans.

04

Regulatory and compliance readiness

Align with evolving global regulations (e.g. DORA, Basel 3.1) that emphasise operational resilience and are expected to incorporate PQC-readiness in the near future.

05

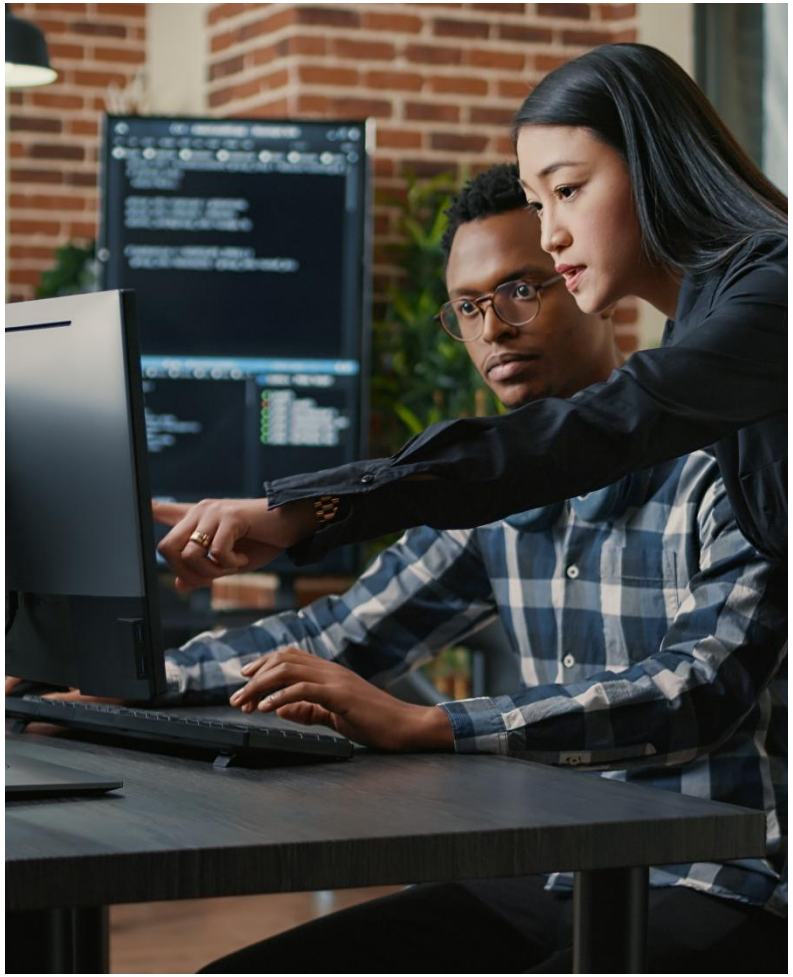
Continuous audit

Internal audit teams should update methodologies to include quantum risks, review the effectiveness of quantum-safe controls and report findings to Senior Management and the Board.

06

Awareness and strategic risk monitoring

Ongoing awareness and strategic risk monitoring are vital for quantum readiness. Regular training, board updates and risk dashboards.



New IIA Topical Requirement: Cybersecurity

Overview

Topical Requirements are a new mandatory component of the International Professional Practices Framework issued by the Institute of Internal Auditors (IIA). Internal auditors must follow Topical Requirements in line with the Global Internal Audit Standards when providing assurance services on the respective topic.
The first Topical Requirement issued is related to cybersecurity and was released in February 2025, taking effect in February 2026. The cybersecurity Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management and control processes.

Governance

Internal auditors must assess whether:

- A formal cybersecurity strategy and objectives are established, updated and reviewed by the Board.
- Policies and procedures are established and periodically updated to strengthen the control environment.
- Roles and responsibilities are established, competences are periodically assessed, and a process exists to periodically assess knowledge, skills and abilities.
- Relevant stakeholders are engaged to address vulnerabilities and emerging threats.

Risk management

Internal auditors must assess whether:

- Risk assessment and management processes exist to identify, analyse, mitigate and monitor cybersecurity threats.
- Cybersecurity risk management is conducted throughout the organisation.
- Accountability and responsibility are established, with monitoring and reporting on risks and emerging threats.
- A process is established to escalate any cybersecurity risk quickly.
- A process is established to communicate cybersecurity risk awareness to management and employees.
- Incident response and recovery processes are established and tested.

Controls

Internal auditors must assess whether:

- A process is established to ensure internal and vendor-based controls are in place to protect the confidentiality, integrity and availability of systems and data.
- A talent management process is established and maintains technical competences.
- Processes are in place to monitor and report emerging threats and improve operations.
- Cybersecurity is embedded in the IT asset lifecycle.
- Processes are established to strengthen cybersecurity, including configuration, end-user device administration, encryption, patching, user-access management, etc.
- Network-related controls are established, such as network-access controls and segmentation, firewalls virtual private network (VPN)/zero trust network access (ZTNA), etc.
- Endpoint-communication security controls are established for services such as e-mail, internet browsers, videoconferencing, messaging, social media, cloud and filesharing protocols.

Key implications for Internal Audit

The cybersecurity Topical Requirement provides a minimum baseline for assessing cybersecurity in an organisation and:

- Establishes a mandatory global framework for cyber-related assurance engagements.
- Requires documentation and justification for any excluded requirements.
- Promotes cross-functional collaboration (Risk, Compliance, Legal, IT, vendors).
- Supports integration of cyber risks into the audit universe and annual plan.
- Aligns with other cybersecurity standards and frameworks (the application guide of the Topical Requirements includes mapping to the following frameworks: NIST Cybersecurity Framework 2.0, COBIT 2019 and NIST 800-53).

Operational risk

Operational resilience (1/3)

Operational resilience is a key focus for financial institutions, given the growing sophistication of risks they encounter. Swiss regulatory requirements emphasise that institutions must continuously develop their resilience capabilities to effectively prevent, respond to, recover and learn from operational disruptions. This involves identifying critical functions, defining acceptable disruption thresholds and implementing robust frameworks covering risk management, business continuity, ICT and cyber risks, and crisis management.

By July 2025, 70% of the top 20 largest countries (by GDP) had released/ subscribed to a set of resilience rules/guidelines.

For financial services, it is important to recognise that operational resilience is an ongoing commitment. The implementation phase is just the beginning of a continuous process to maintain, manage and further enhance resilience capabilities. As processes, firm strategies and market conditions evolve in response to the external threat landscape and changing financial market structures, institutions must continue to mature their resilience frameworks.

FINMA has defined a transitional period, but full compliance with the operational resilience requirements stipulated in FINMA Circular 2023/1 'Operational risks and resilience – banks' is expected by the end of 2025.

Internal and external audit teams will need to adjust their assurance approaches to align with the dynamic and evolving nature of operational resilience.

Key considerations for firms

Ongoing regulatory developments

Regulatory expectations continue to advance, encompassing areas such as operational risk management, information and communication technology, cyber risk management, critical data risk management, business continuity management and third-party risk management. Financial institutions need to understand the impact of these developments on their resilience capabilities and ensure that effective assurance processes are in place to demonstrate compliance with these evolving requirements.

Integrating resilience into existing risk frameworks

As institutions strengthen their resilience programmes, it is increasingly important to align these efforts within the overall risk management framework to achieve a comprehensive and cohesive approach to risk and resilience. This integration is gaining greater emphasis.

Ensuring adequate workforce capacity and skills

Institutions must ensure that they have sufficient resources with the necessary skills to respond effectively and dynamically to evolving internal and external risks. Maintaining adequate headcount and continuously addressing skills gaps are essential to sustaining operational resilience.

Comprehensive mapping of critical functions

Firms often develop inventories of critical functions but lack end-to-end mapping to key resources (people, systems, third parties, data, business continuity plans, disaster recovery plans). An end-to-end view is essential for effective resilience.

Continuously enhance testing to assess the impact of internal and external changes on the resilience of critical functions

Institutions are expected to test and evaluate their resilience capabilities for critical functions regularly in line with FINMA Circular 2023/1. This includes conducting integrated testing programmes and scenario-based exercises to address evolving risks and operational challenges. Institutions should also validate the effectiveness of remedial actions identified in previous tests during subsequent assessments to ensure continuous improvement of operational resilience.

Severe but plausible scenario management

While severe but plausible scenarios are discussed periodically, there is often a lack of formal documentation and evaluation processes. Some aspects (e.g. critical data and data governance) are frequently not included, and no simulated stress tests or live scenario exercises are typically defined. Developing comprehensive scenario coverage is essential.

Operational resilience (2/3)

Assurance functions: focus areas

01

Governance and oversight

- Evaluate whether the oversight structures, escalation procedures, and reporting channels provide the Senior Management and the Board of Directors with clear, accurate and timely information regarding operational resilience capabilities.
- Review the design and proportionality of the reported metrics to ensure that they are appropriate for the institution's size, business model and risk profile, enabling responsible bodies to make well-informed decisions on resilience management.

02

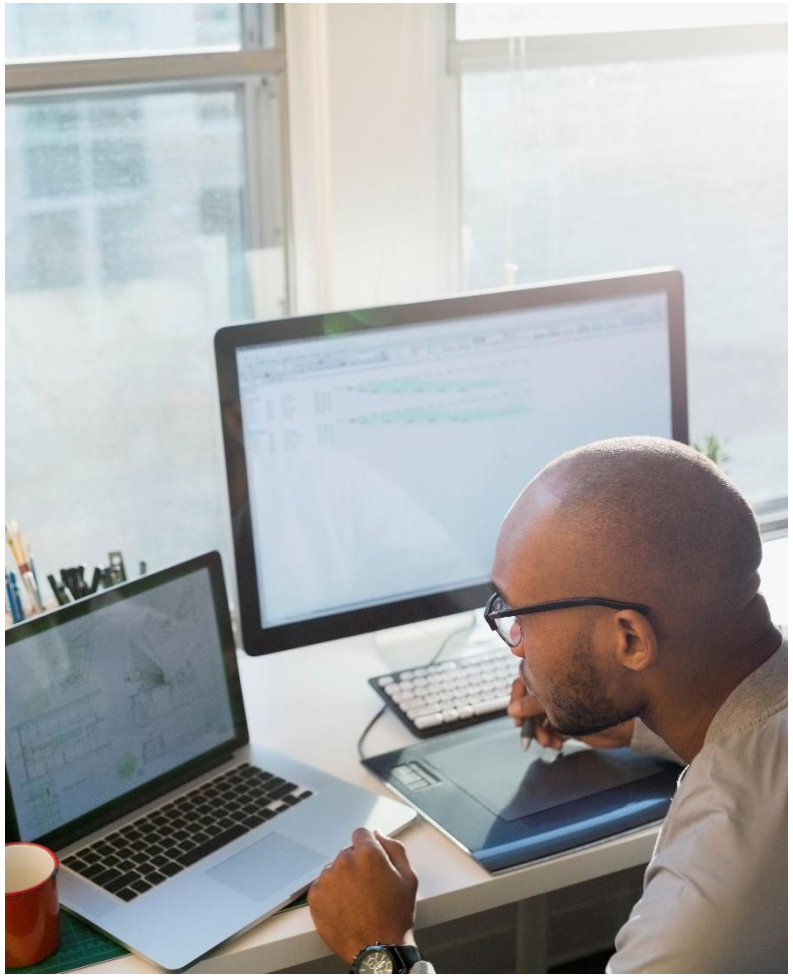
Continuous assurance

- Provide assurance regarding the effectiveness of remediation measures implemented by business units and resilience managers.
- Verify that identified vulnerabilities and temporary solutions have been properly addressed and that corrective actions are incorporated into subsequent testing cycles to ensure their ongoing effectiveness.

03

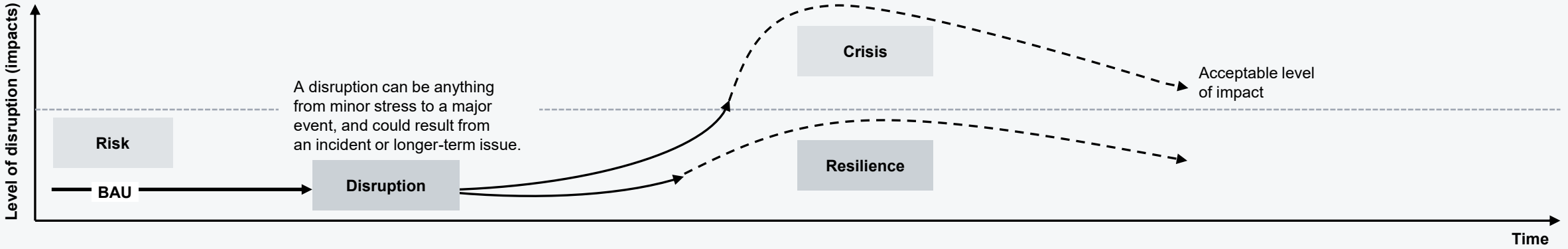
Embedding resilience

- Evaluate how resilience considerations are integrated into key institution processes such as comprehensive mapping of relevant resources, new initiatives, change management, outsourcing arrangements and product approval procedures.
- Assess alignment with applicable frameworks including enterprise risk management, third-party risk management, critical data risk management, business continuity, crisis management and cyber resilience.
- Review whether investments in resilience tools and mapping capabilities are enhancing the speed and accuracy of insights, minimising disruptions during incidents and supporting a sustainable, long-term resilience strategy.



Operational resilience (3/3)

Crisis response in the context of operational resilience



Assurance functions: focus areas

01

Risk

- Provide assurance that governance structures, reporting channels and reported metrices enable key stakeholders to make informed decisions on the firm's resilience capability, and that they are proportional to the firm's size and risk profile. A resilience programme should have assigned ownership alongside executive sponsorship to provide accountability and drive cultural change.

02

Resilience

- Assess the extent to which a firm has moved beyond a traditional business continuity focus to a more holistic operational resilience approach. This should enable firms not only to recover from disruptions but also adapt, evolve and thrive amid ongoing uncertainty. Resilience should be aligned with what matters most to a firm by identifying and mapping critical functions.
- Understand how firms have/can embed resilience considerations into new initiatives, change management, outsourcing and new product approval processes. Firms can further support their resilience capabilities by investing in the right technology tools to support speed to insight through understanding underlying mapping better, resulting in a reduction of noise in disruption and delivering a sustainable approach to resilience.

03

Crisis response

- Examine the extent to which firms have put in place structures that will enable them to respond effectively to crises. This should include the availability of plans and scenario-specific playbooks that set out team structures, roles and responsibilities, and mobilisation procedures. Firms should have stress-tested these structures and rehearsed the capabilities of their response teams (at each level) against plausible, challenging scenarios.

Digital Operational Resilience Act (DORA) (1/3)

"DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats." – Council of EU

The Digital Operational Resilience Act (DORA) is a European regulation that defines detailed and comprehensive requirements for the digital operational resilience of financial services firms at EU level.

Its objectives are to:

- Harmonise local regulations in the financial sector across the EU member states.
- Ensure that financial entities and third-party providers respond to and recover from all types of ICT-related disruptions in a timely and appropriate manner.
- Improve ICT risk management.
- Empower financial supervisory authorities to monitor and audit financial entities and their third-party ICT providers more closely.
- Standardise incident reporting mechanisms and knowledge sharing.

Whilst this is an **EU regulation**, extraterritorial implications exist:

- Non-EU branches or subsidiaries of EU financial services firms must comply if their ICT operations affect the EU parent company or EU-based customers.
- Outsourcing to non-EU providers (e.g. payment processors or cloud vendors) must meet EU supervisory expectations, including full access, audit rights and compliance assurance.

Key considerations for firms

DORA repositions operational resilience as a strategic priority, with regulatory consequences and clear expectations around ownership, oversight and demonstrable capability. It requires a mindset shift: resilience is no longer a supporting function; it is a core business responsibility with direct accountability at the regulated entity level.

- **Entity-level ownership**: In-scope entities must retain direct accountability, even where services are delivered at group level or by third parties.
- **Leadership accountability**: Senior Management must lead resilience efforts and be able to evidence control to regulators.
- **Third-party and intragroup oversight**: All ICT dependencies must be governed with formal controls (e.g. SLAs, audit rights, exit plans).
- **Strategic planning impact**: Expansion, outsourcing and new services must take resilience capacity and DORA compliance into account.
- **Ongoing obligations**: Compliance is continuous, requiring regular testing, reporting, assessments and improvement cycles.
- **Increased regulatory scrutiny**: Authorities expect clear, auditable evidence of compliance and readiness.

Ultimately, DORA is not just about preventing outages, it redefines operational resilience as a regulated, measurable and enforceable capability that must be embedded throughout the business lifecycle.

DORA is applicable as of 17 January 2025 in the EU and as of 1 February 2025 in Liechtenstein. In-scope firms must be able to transition effectively from a project-style approach of readiness for DORA to **operating against the requirements as part of BAU**. This can be a considerable challenge for firms, and it is necessary to resource appropriately to meet the expectations now in place.

Digital Operational Resilience Act (DORA) (2/3)

The DORA directive covers five key areas/pillars that are relevant for reporting entities.

ICT risk management

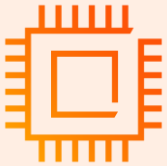
- The **ICT risk management framework** must be detailed and aligned with the corporate strategy and objectives.
- A **strategy for digital resilience** must be defined.
- **Enhance first line of defence capabilities**, from threat detection to response, recovery and communications, with an emphasis on – but not limited to:
  - ✓ Threat scenario modelling
  - ✓ Cyber protection and prevention
  - ✓ Business continuity and disaster recovery communication (e.g. with customers).

ICT-related incidents

- **Report** ICT-related incidents (and significant cyber threats)
- Submit **initial, interim and final reports** on serious ICT-related incidents (and significant cyber threats).
- Conduct a **root cause analysis** after ICT-related incidents.
- Identify and **report required improvements**.

Digital operational resilience testing

- **Annual testing** of all critical ICT systems
- Advanced **threat-led penetration testing** every three years
- **Involvement of ICT third-party** providers



Management of ICT third-party risks

- Integration into ICT risk management framework
- Multi-vendor strategy (optional)
- Essential contractual requirements
- Keeping an **information register** on all services provided by ICT third parties
- Reporting on changes in the use of critical ICT services
- Assessment of ICT concentration risk and sub-outsourcing
- Restricted use of third-party ICT providers in third countries

Information sharing

- **Share cyber threat intelligence** and insight to improve digital operational resilience.
- Agreements on the **exchange of information** (including conditions for participation)
- Implement mechanisms to review and act on the information shared by the authorities.

Digital Operational Resilience Act (DORA) (3/3)

Assurance functions: focus areas

01

Validate that remediation actions for gaps identified through the DORA-required ICT risk management framework are timely, effective and sustainable, with clear evidence of implementation and oversight to strengthen resilience.

02

Ensure that required DORA compliance artefacts and outcomes, such as risk assessments, self-assessments and digital operational resilience strategies, are complete, accurate and embedded, providing clear evidence of adherence to regulatory expectations.

03

Assess ICT response and recovery plans as mandated by DORA Article 11, ensuring that they are comprehensive, tested and effective in supporting timely incident response and recovery to maintain operational resilience.

04

Ensure audits of key business processes, even where not DORA-specific, incorporate DORA's prescriptive requirements. For example, reviews of incident management, third-party risk or resilience testing should consider DORA expectations alongside existing objectives.

05

Assess how DORA compliance shifts from project mode to sustainable BAU operations, evaluating readiness, resourcing and integration challenges that may affect firms' ability to maintain compliance and resilience.

06

Verify that there is clear ownership and accountability for DORA compliance, ensuring that responsibilities are defined and upheld, particularly where regulated entities rely on services delivered within a wider group structure.

07

Ensure that the resilience approach is sufficiently robust to deliver resilient outcomes, with scenario testing and related activities that meaningfully challenge critical functions and validate the organisation's ability to withstand disruptions.

08

Provide assurance of the ICT risk management framework as required by DORA Article 6, including rules for the timely verification and remediation of critical ICT audit findings.

Third-party risk management (1/2)

Accelerated by rapid digitisation, increasingly complex third-party dependencies are causing institutions to sharpen their focus on operational resilience.

Institutions rely extensively on third-party service providers, both external and intra-group, for a wide range of services to support their business, including those that are critical to their operations. These dependencies continue to grow in scale and complexity, accelerated by the increasing use of cloud, AI and other new technologies.

Although continuing to offer firms considerable benefits, including sizeable operational and commercial efficiencies, the risks associated with the use of third parties are pervasive. If not properly managed, they have the potential to significantly impact firms, customers and markets.

Regulation continues to evolve in parallel to these developments, with an extension of the historic focus on outsourcing to a more holistic, outcomes-based focus on broader third-party risk management, with operational resilience at its centre. In Switzerland, the FINMA Circular 2018/3 'Outsourcing' sets out the requirements for the outsourcing of material functions, including obligations in terms of governance, risk assessment, contractual standards, inventories and the oversight of sub-outsourcing. Recent FINMA communications – particularly in the context of operational risk (i.e. FINMA Circular 2023/1 'Operational risks and resilience – banks') – highlight increasing supervisory attention on concentration risks, cloud and ICT dependencies, and the need for firms to ensure adequate resilience and effective monitoring of critical third-party service providers.

Despite initiatives towards increased interoperability, regulations continue to vary by jurisdiction. Nevertheless, universally, firms remain fully responsible and accountable for the third-party services on which they rely. They are expected to have robust, proportionate processes and controls in place to identify, assess, monitor and manage all risks resulting from arrangements to which they are or might be exposed, aligned to strategy and risk appetite.

Key considerations for firms

Group versus legal entity

Ensure that TPRM frameworks are clear on jurisdictional scope and that key governance processes and controls are set up to support demonstrable senior management control, aligned to Group and regulated entity accountabilities.

Re-wiring TPRM

Greater integration of complementary processes across TPRM, procurement, legal and operational resilience to promote cross-functional synergies, eliminate gaps or duplication, better manage key dependencies, drive efficiency and enhance resilience

Integrating new and evolving risk types

Update TPRM frameworks to integrate processes and controls for identifying, assessing, managing and reporting important new and evolving risk types, including AI and ESG.

Embracing technology

Overhaul legacy systems and technology to support more integrated and proactive risk management, including leveraging enhanced data models to drive increased risk intelligence and promote more proactive risk monitoring.

Data quality and reporting

Clarity on which data attributes are needed to support which internal and external reporting obligations, and how and where these are collected, with transparency on golden source and ownership, and robust quality controls

Enhanced assurance and oversight

Ensure that contractual terms support access, audit and information requirements, leveraging emerging third-party service provider reporting where possible, while ensuring that the use of any pooled audits or third-party certifications is appropriate to the scope of services received.

Third-party risk management (2/2)

Assurance functions: focus areas

01

Third-party risk management framework

Confirm that the firm's framework for managing third-party arrangements, including the TPRM policy(/ies), complies with applicable laws and regulations, is effectively implemented and aligns with board-approved strategy and risk appetite.

02

Risk assessments and due diligence

Assess the adequacy, quality and effectiveness of criticality/materiality assessments and broader third-party risk assessments, including initial and ongoing due diligence.

03

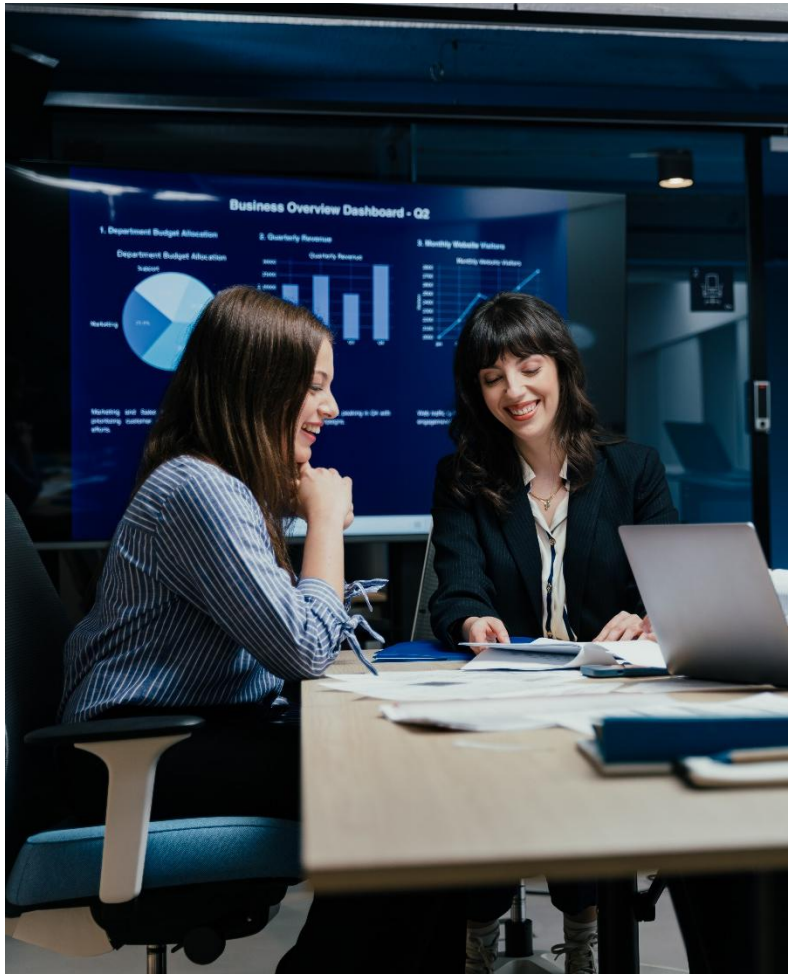
Governance and oversight

Evaluate the involvement and oversight of relevant governance bodies in the approval, monitoring and management of third-party arrangements.

04

Monitoring and ongoing management

Review the monitoring mechanisms and management practices in place for third-party arrangements to ensure that they remain effective and proportionate.



Internal audit reviews for this area should align with reviews of operational resilience and applicable risk areas, assessing the design and operating effectiveness of processes and controls to enable the firm to protect itself from threats and potential disruption, including response and recovery capabilities. Follow-up processes for findings should also be formalised, including the timely verification and remediation of material audit findings.

New IIA Topical Requirement: Third party

Overview

Topical Requirements are a new mandatory component of the International Professional Practices Framework issued by the Institute of Internal Auditors (IIA). Internal auditors must follow Topical Requirements in line with the Global Internal Audit Standards when providing assurance services on the respective topic.
The third-party Topical Requirement was released in September 2025, taking effect in September 2026. It sets out mandatory expectations for internal audit when assessing the governance, risk management and control frameworks that govern outsourced and third-party relationships.

Governance

Internal auditors must assess whether:
- A formal approach for third-party contracting is established and periodically reviewed.
- Policies and procedures are established to define, assess and manage third-party relationships and risks throughout the lifecycle.
- Roles and responsibilities are defined, with competent individuals assigned.
- Protocols for communicating with relevant stakeholders are defined and include timely reporting on the status of the performance, risks and compliance of prioritised third parties.

Risk management

Internal auditors must assess whether:
- Risk management processes for third parties are standardised and monitored.
- Risks related to third parties are identified, assessed, ranked and updated regularly.
- Risk responses are adequate, implemented and adjusted as needed.
- Escalation processes are in place to manage and escalate third-party issues and remediation actions.

Controls

Internal auditors must assess whether:
- A robust due diligence process for sourcing and selecting third parties is in place including appropriate documentation and approvals.
- Contracting and approval processes follow the internal policies and procedures.
- Final contracts are reviewed, approved, signed, stored and assigned.
- An accurate, complete and current listing of all third-party relationships is maintained.
- Onboarding processes are established and followed.
- Ongoing monitoring exists to verify that the third party's performance meets the terms of the contract.
- Protocols are established to initiate corrective actions.
- Expiration and renewal dates are appropriately tracked.
- A formalised offboarding plan exists to ensure adequate termination, data return/destruction and access revocation.

Key implications for Internal Audit

The third-party Topical Requirement provides minimum criteria for evaluating how organisations identify, monitor and manage third-party risks, including subcontractors and critical service providers. In addition, it:
- Establishes a mandatory global framework for third-party risk assurance.
- Requires documentation and justification for any excluded requirements.
- Promotes cross-functional collaboration across Risk, Legal, Procurement and IT.
- Supports integration of third-party risk into the audit universe and annual planning.

Technology and operations: digital transformation – cloud risk (1/2)

Financial services firms and other regulated industries face unique challenges when embarking on the journey to unlock the potential of cloud technology, given the regulatory scrutiny of cloud adoption and the need to demonstrate that they are embedding resilience at the heart of their architecture. Successfully navigating these challenges requires a holistic approach addressing the regulatory, security, technical, operational and organisational aspects of cloud adoption.

Key considerations for firms

Regulatory compliance (e.g. EU data act, EU AI act) – Secure both regulatory and internal policy approval for migrating critical services or workloads to the cloud.

Security and risk management – Manage cloud adoption risks by enhancing risk frameworks and embedding security and operational controls upfront.

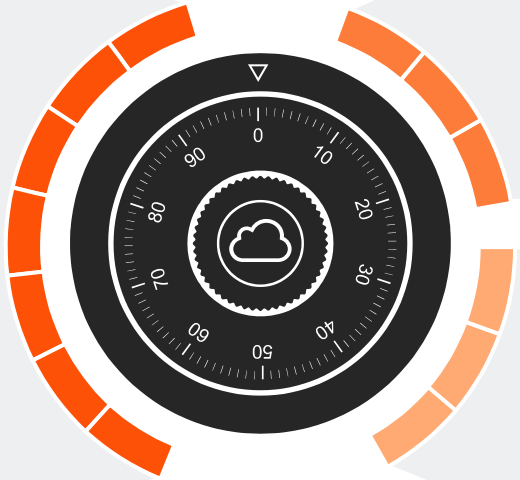
Lawful access (e.g. CLOUD Act) – Use contractual and technical safeguards to prevent unauthorised lawful access to cloud data and ensure compliance with Swiss/EU regulations.

Operating model design – Design and implement shared responsibility models and establish oversight and governance arrangements.

Contracting – Negotiate optimum pricing agreements with cloud service providers (CSPs) to maximise value from contracts and ensure that commitments align with projected spending.

Data management – Migrate data from legacy systems into the cloud environment and establish capabilities to govern and protect data post-migration.

AI governance – Manage risks in cloud-enabled GenAI applications, enhance transparency, trust and security to accelerate GenAI adoption.



Cyber security – Deploy effective security measures throughout the cloud environment (including access controls and detection and response mechanisms) to mitigate potential risks such as data loss.

Third-party risk – Assess and control risks for outsourced cloud services, providing assurance through vendor audits and ongoing reviews.

Resilience – Guidance and contingency arrangements to manage disruption and build resilience, ensuring compliance with operational resilience regulations

Optimisation of cloud expenditure – Assess cloud expenditure and deliver cost savings by optimising infrastructure and services.

Sustainability – Understand the sustainability implications of cloud usage and assist with the journey towards Net Zero.

Process and control optimisation – Reduce the operational complexity associated with hybrid and/or multi-cloud environments.

Moving to the cloud ▶ **Operating in the cloud** ▶ **Optimising benefits and managing costs**

Technology and operations: digital transformation – cloud risk (2/2)

Assurance functions: focus areas

01

Governance and oversight

Establish clear roles, responsibilities and escalation pathways to ensure that risk management is embedded at all organisational levels and regularly reviewed by senior leadership.

02

Data protection and lawful access

Implement contractual and technical safeguards to mitigate lawful access risks, ensuring compliance with local and international data protection regulations.

03

Operational resilience

Develop and test robust business continuity and disaster recovery plans to maintain critical operations during disruptions, including cyber incidents and third-party failures.

04

Third-party and supply chain risk

Continuously assess and monitor third-party providers for compliance, security and resilience, with clear contractual terms and regular performance reviews.

05

Continuous improvement and training

Promote a culture of ongoing risk awareness and upskilling, ensuring that staff are trained on emerging risks, regulatory changes and best practices for digital operations.

Insider fraud risks (1/2)

Rising cost and complexity of insider risk

- Insider threats, while not new, have grown more impactful due to advances in technology and global changes.
- Insider risks have become one of the most significant and costly organisational threats, with incidents costing three times more than standard cyber breaches.
- The Cost of Insider Risk 2025 Global Report shows that companies have doubled investments in insider-risk management (from 8.2 % to 16.5 % of IT-security budgets).
- Despite higher spending, annual losses reached USD 17.4 million, with human error remaining the main cause.
- Containment times improved slightly (from 86 to 81 days), showing progress in detection and response.
- Organisations recognise insider threats as a governance and culture challenge, not merely an IT issue.

High-value targets in finance and innovation

- Financial institutions are particularly exposed due to their custodianship of sensitive client data and trading algorithms.
- Pharmaceutical and technology firms are high-value targets because of intellectual property and research data.
- In Switzerland, the combination of financial secrecy, innovation leadership and geopolitical neutrality increases attractiveness for insiders and foreign actors seeking to exploit trusted environments.
- Both employees and external contractors can be involved in insider incidents.
- The rise of remote work and digital transformation has expanded opportunities for insider fraud by increasing access points to sensitive systems and data.

Incidents evolve quietly – prevention is key

- Real cases illustrate that insider incidents often develop over months or years before detection – from gradual data theft and printing confidential lists to sabotage through hidden 'logic bombs.'
- Effective countermeasures include least-privilege access controls, joiner–mover–leaver processes, data loss prevention systems and behavioural analytics (UEBA).
- Negligence-related incidents cause the highest average costs. Awareness, ethics and accountability are therefore as critical as technology.
- Life events of employees such as health issues, injuries, financial struggles or relationship problems can affect behaviour and work performance. Companies should provide support systems to help employees address these challenges effectively.

PwC's view

"Culture eats technology for breakfast."

- Managing insider risk requires a holistic and culture-driven approach, integrating governance, preventive controls, monitoring and continuous learning.
- Building trust, transparency and accountability across the three lines of defence transforms employees from potential risks into active contributors to resilience.
- Conducting regular scenario-based table-top exercises is key to testing response plans and reporting outcomes to oversight bodies to ensure accountability and continuous improvement.

Insider fraud risks (2/2)

Assurance functions: focus areas

01

Governance and culture

- Assess whether ownership and accountability for insider risk are clearly defined at Board and C-suite level.
- Provide regular training and awareness programmes to educate employees on recognising and reporting potential insider threats.
- Promote a culture of trust and ethical behaviour rather than surveillance.

02

Preventive controls throughout the employee lifecycle

- Test the effectiveness of joiner–mover–leaver and least-privilege access processes.
- Review screening and awareness measures throughout the employee lifecycle.
- Monitor non-digital behaviours such as workplace conduct and stressors, alongside technical controls to identify potential risks.

03

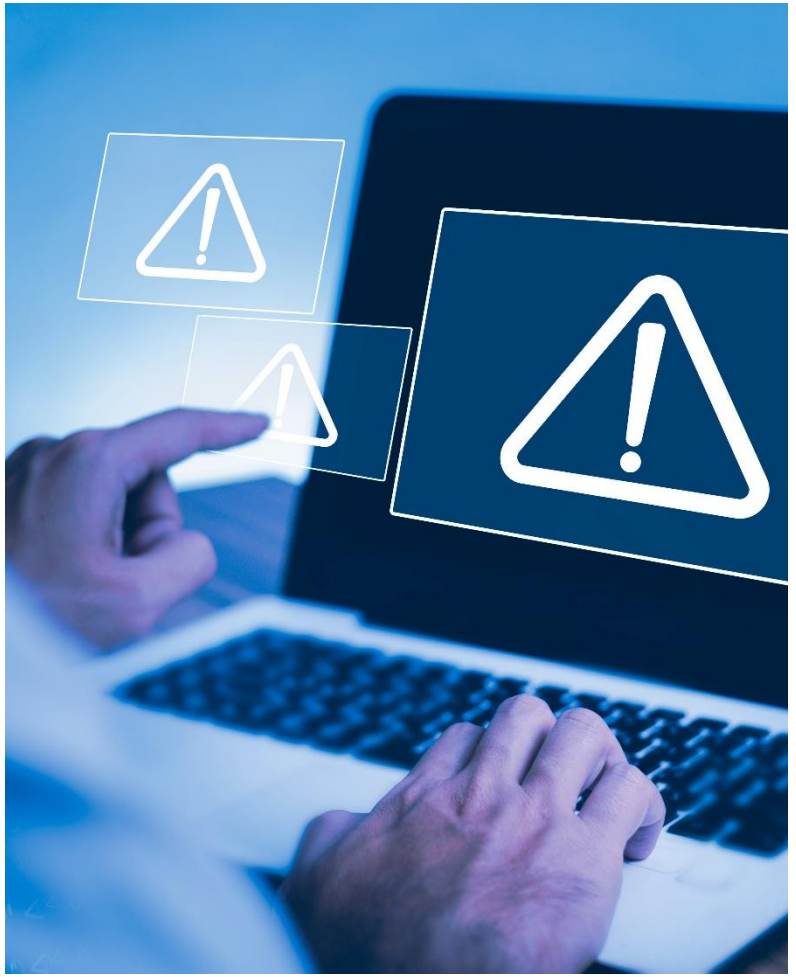
Detection and response

- Evaluate behavioural and analytics-based monitoring (e.g. UEBA) and data integration across HR, IT and security.
- Integrate physical security and HR signals, such as access logs, unusual behaviour or employee grievances, into monitoring systems.
- Ensure clear escalation paths, playbooks and coordination between Legal, HR and Risk.

04

Investigation, response and continuous learning

- Review forensic investigation processes and root-cause analysis.
- Verify that lessons learned and scenario testing strengthen future assurance coverage.
- Know whom to turn to 24/7. Consider losing access to digital infrastructure. Have printouts of playbooks, team member‘s names and phone numbers distributed to the crisis team.



Data

Data strategy reset (1/2)

Organisations are reassessing their enterprise data strategies to stay competitive in a landscape dominated by AI and advanced analytics.

A robust data strategy sets the blueprint for how an organisation collects, governs, manages and leverages data to drive its strategic objectives. Far beyond a technology or compliance document, a data strategy enables businesses to unlock tangible value, from alignment in investment to risk reduction. In today's landscape of proliferating data, increasing regulatory scrutiny and rising AI adoption, the absence of a coherent, adaptive data strategy often results in siloed ownership, inconsistent standards and suboptimal outcomes.

At its core, a data strategy typically defines the organisation's data vision, governance structure, key use cases and roadmap for capabilities across architecture, platforms, people and processes. It sets out how data supports enterprise priorities.

Static strategies quickly fall behind. The market is rapidly evolving, driven by generative AI, cloud-native architectures, digital operational resilience regulation and shifts in customer and shareholder expectations. Data strategies that were relevant even 18 months ago may now be lagging behind regulatory, architectural or business model changes. Organisations must treat their data strategy as a living document, revisiting and refining it regularly to reflect emerging technologies, new value drivers and shifting risk landscapes.

Key considerations for firms

Strategic alignment and value prioritisation

Data strategies should be explicitly linked to the organisation's business objectives and plans, whether focused on growth, transformation or risk mitigation. Initiatives should be sequenced based on value, with defined key performance indicators (KPIs) that are tied directly to measurable commercial, operational or risk outcomes.

Balancing central and federated delivery models

Many organisations are now combining data fabric technologies focused on unified access, metadata and governance with data mesh principles that place accountability for data with business domains. A strong data strategy should clearly define which elements remain centrally governed (e.g. data policies, architecture standards, compliance, etc.) and where domain teams are empowered to own and manage data as products.

Embedding data literacy and cultural change

Technical success is insufficient without human adoption. Organisations must embed data literacy at all levels: from executive understanding of AI and data ethics to the frontline use of dashboards and insights. Leadership sponsorship, incentivisation and education are key levers.

Performance management and accountability

Firms should establish clear governance structures (e.g. data councils, stewardship forums) and track progress using enterprise-wide metrics such as data issue closure rates, data usage trends or business case delivery. Strategy reviews should be built into planning cycles.

Data strategy reset (2/2)

Assurance functions: focus areas

01

Strategic alignment and oversight

- Evaluate the adequacy of data strategy, ensure that it is formally approved and regularly reviewed at executive level, with clear links to business objectives and value delivery.

02

Governance and accountability

- Assess whether roles, controls and ownership structures are clearly defined and operating effectively.

03

Culture and change management

- Evaluate how well data literacy, performance metrics and change initiatives are embedded across the organisation to support sustained adoption and impact.
- Review whether cultural factors and change management practices are enabling the adoption of new ways of working and supporting sustainable transformation.

Data – AI-ready foundations (1/2)

With the explosion of generative AI and advanced analytics, the quality and governance of the data feeding these models have become critical.

Organisations across sectors are investing in AI to streamline decisions, personalise customer experiences and unlock operational efficiencies. AI's impact potential is vast – but its success is fundamentally dependent on the adequacy of the data it consumes. Models are only as effective and fair as the data that feeds them. As regulators and boards increase scrutiny over explainability and outcomes, the need for robust data foundations has never been more pressing.

Many firms have been overestimating their AI readiness. Initial proof of concepts or attempts to scale solutions have often exposed weaknesses: fragmented data, inconsistent standards and legacy infrastructure. These gaps reflect overconfidence in perceived data maturity, a lack of formal data governance and insufficient investment in the roles and platforms needed to sustain enterprise-scale AI.

Organisations must strengthen core data management capabilities. That includes improving data quality and completeness, embedding clear metadata standards to support transparency and discovery, and maintaining lineage from raw inputs through to model outputs. Data must be continuously monitored, supported by governance frameworks that define ownership, oversight and issue management processes. Without this foundation, AI solutions may not be trusted, hence responsible data is needed for responsible AI.

Key considerations for firms

Assess and remediate foundational data capabilities

Organisations should conduct data management maturity assessments, examining whether standards and practices are fit for purpose. These assessments often reveal 'unknown unknowns' such as applications failing to meet standards and poor transparency of data flows (e.g. undocumented transformations and calculation logic). Addressing these issues early and in line with the capabilities you need set out by your data strategy will reduce rework and build trust in AI outcomes.

Reinforce traceability, explainability and trust

As regulatory scrutiny increases, organisations must demonstrate how AI models reach decisions and how underlying data is governed. This requires enterprise-wide standards for lineage, metadata and versioning, plus well-defined ownership and oversight. Data quality, security and privacy need to be built into the data foundation by design. Without this, organisations risk reputational damage, regulatory non-compliance and poor customer outcomes.

Ensure data readiness before scaling AI use cases

Before scaling AI solutions, organisations must ensure they have strong data foundations in place. This means verifying that data pipelines are stable, well-governed and continuously monitored, with clear accountability for detecting and resolving quality or integrity issues.

Embedding controls 'by design' from the outset enables sustainable AI adoption**:** this will ensure that AI initiatives deliver measurable value aligned to business objectives while keeping associated risks within acceptable boundaries.

Data – AI-ready foundations (2/2)

Assurance functions: focus areas

01

Test data management maturity

Review whether management's self-assessment of AI readiness is supported by evidence of the organisation's data-readiness, e.g. data lineage maps, data quality metrics, data catalogue usage. Alternatively, evaluate the organisation's data management policy framework and current-state data landscape against industry benchmarks (e.g. DAMA-DMBOK), and assess whether the capabilities in place are sufficient to support the prioritised use cases outlined in the data strategy.

02

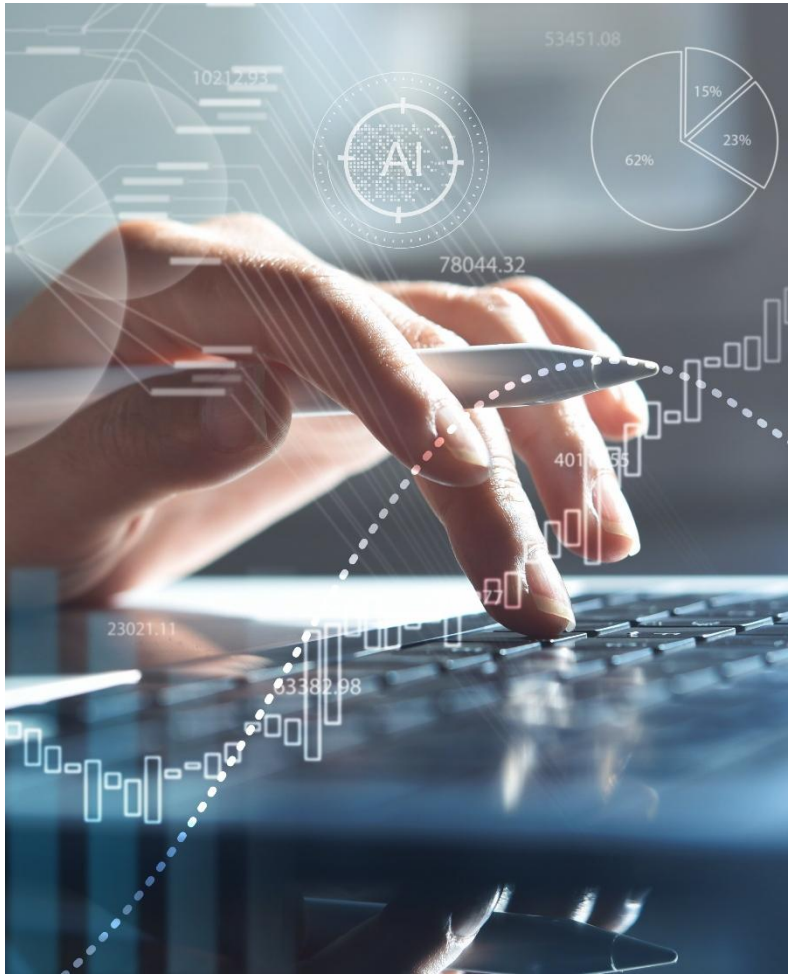
Evaluate controls across data pipelines for AI

Assess whether data sourcing, transformation and integration processes supporting reporting and AI are documented, tested and governed. Verify if continuous monitoring for data drift, missing values or outliers is in place and leads to actionable remediation.

03

Review governance forums and issue escalation

Confirm that data and AI governance structures are active, cross-functional and empowered to challenge data use in reports and AI models. Audit trails should demonstrate accountability for approvals, exceptions and issue resolution.



‘Dark’ data and unstructured information (1/2)

Organisations typically amass extensive information assets that remain poorly managed and under-utilised.

Unstructured data such as e-mails, chat logs and collaboration platform content continues to accumulate rapidly across most organisations. Much of it is unclassified, unmonitored and non-compliant with enterprise policies. This “dark data” often exists outside systems of record. As a result, many organisations face mounting challenges around discoverability, over-retention, and inconsistent archival and deletion practices.

These ungoverned assets increase exposure to data breaches, regulatory non-compliance and costly eDiscovery or legal hold processes. In the context of tightening privacy regulation, organisations must be able to demonstrate effective controls over where personal and sensitive data resides, including outside core systems.

Leading organisations are shifting to a proactive, risk-based approach to managing dark data. This includes defining targeted remediation objectives, such as identifying and securely deleting redundant, obsolete or sensitive data and deploying automated discovery tools to improve visibility. Accountability is embedded through appointed Data Owners and Data Stewards who coordinate structured reviews and champion enforcement of policy-aligned retention and disposal practices.

Key considerations for firms

Understand the profile and scale of dark data

Organisations should conduct structured discovery and risk assessment exercises to establish where unstructured data resides, whether sensitive or regulated data is present, and how current practices compare to internal standards on retention, archival and deletion. Discovery tooling and sample audits can help identify key policy gaps and high-risk repositories (e.g. shared drives, personal inboxes, legacy archives).

Adopt a risk-based approach to remediation

Not all dark data presents equal risk. Firms should define prioritised objectives, such as removing unneeded personal data, isolating records subject to litigation hold, or cleaning up legacy project files, and target interventions where the potential for regulatory exposure, cost or operational inefficiency is greatest.

Automate and embed lifecycle controls

Leading firms are deploying automated tools to enforce retention and disposal policies for unstructured content across collaboration platforms, cloud storage and on-premises systems. Policy configuration should reflect legal, regulatory and business needs, with capabilities for exception handling and audit logging.

Strengthen governance and ownership

Clear accountability is essential. Appointing Data Owners and Data Stewards for business domains ensures local oversight, while enterprise policies set consistent standards. Governance forums should review progress against dark data reduction targets and report on policy compliance, breach risks and remediation outcomes.

‘Dark’ data and unstructured information (2/2)

Assurance functions: focus areas

01

Evaluate unstructured data governance

Review whether the organisation’s data policies cover unstructured data and that roles, responsibilities and interactions are clearly defined for policy enforcement, remediation and ongoing monitoring.

02

Test discovery and classification capabilities

Assess whether the organisation has conducted recent scans or classification exercises on unstructured data stores (e.g. file shares, SharePoint, e-mail, etc.) to identify sensitive or high-risk content and whether discovery tools or manual reviews are consistently applied across business areas.

03

Review retention and disposal enforcement

Validate whether manual or automated controls are in place to apply retention schedules, execute secure deletions and provide evidence of ongoing compliance. Consider testing specific repositories for unused content or records beyond documented retention limits.

Data risk (1/2)

Organisations are increasingly recognising data as a stand-alone enterprise risk category with links to privacy, operational resilience and AI governance.

Enterprise risk management (ERM) frameworks provide organisations with a structured approach to identifying, assessing and managing the range of risks that could affect their ability to meet strategic objectives. These frameworks typically group risk into categories, such as operational, compliance and financial, and define processes for risk ownership, escalation, appetite-setting and control monitoring.

Data risk refers to the potential for adverse outcomes arising from poor-quality, unavailable, misused or uncontrolled data. As data becomes more tightly linked to customer trust, AI oversight and external reporting, firms face heightened scrutiny from boards, regulators and the public on how data is used, protected and governed.

FINMA's Circular 2023/1 'Operational risks and resilience – banks' has refined the supervisory practice regarding the handling of critical data (see FINMA circular 2023/1, Chapter IV, letter D) and broadened its previous focus on the confidentiality of client identification data (CID) to include the dimensions of integrity and availability of critical data, which is defined as data considered to be significant for the successful and sustainable provision of services or data required for regulatory purposes.

Since 1 January 2024, banks and other financial intermediaries have had to comply with the new requirements of the FINMA Circular 2023/1 related to critical data risk management.

Key considerations for firms

Define what data risk means for your organisation

Data risk is multi-dimensional, spanning quality, availability, integrity, misuse, privacy and security. Organisations should ensure that their definition of data risk is tailored to their risk taxonomy and unique operational characteristics, and that it is clearly understood by risk owners throughout the business.

Assess how data risk is captured in the ERM framework

Assess whether critical data risks (such as lack of data governance, poor data quality, unavailability, unauthorised data manipulation, data loss, data theft, data corruption) are integrated into the overarching operational risk management as a separate taxonomy and are thus comprehensively addressed in the identification, assessment, mitigation, monitoring and reporting of operational risks.

Develop meaningful metrics and escalation criteria

Identify and monitor leading indicators of data risk, such as material data quality issues in critical reports, control failures in AI models or high volumes of data privacy incidents. Ensure that these metrics feed into ERM dashboards, influence risk appetite discussions and trigger appropriate remediation where tolerances are breached.

Establish governance and reporting mechanisms

Data risk should be routinely discussed at senior governance forums and linked to strategic and operational priorities. This includes ensuring adequate reporting to risk committees, ownership by accountable executives and integration with broader initiatives such as AI oversight and resilience.

Data risk (2/2)

Assurance functions: focus areas

01

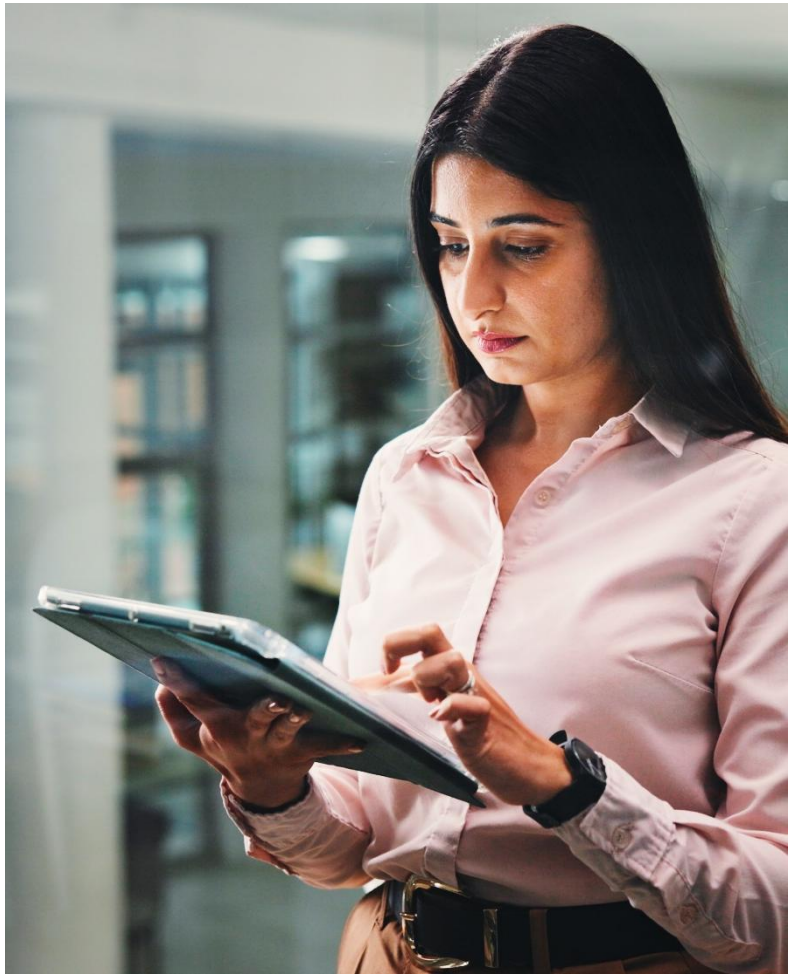
Review how data risk is defined and captured in the ERM framework

- Assess whether the organisation has clearly articulated its data risk profile and whether data risks are appropriately embedded into the overarching operational risk management, with defined ownership and board visibility.

02

Evaluate the design and use of data risk metrics and reporting

- Test whether key risk indicators (e.g. data quality exceptions, reporting errors, privacy incidents, etc.) are tracked, linked to appetite and trigger escalation.
- Confirm whether governance forums receive timely, insightful reporting to support effective oversight and remediation.



Environment, social and governance (ESG)

ESG overview (1/2)

The regulatory environment across ESG is constantly maturing, with new initiatives emerging. Firms need to have a clear strategy for managing risks and opportunities that arise from these market and regulatory pressures. Second and third lines are proactively engaging with ESG topics – particularly in larger organisations, which are already subject to a range of regulatory requirements and may have made public sustainability commitments.

ESG concerns are shaping organisations by influencing their strategy, governance and culture, and impacting all their functions.

Firms need to consider ESG risks across their functions, make new disclosures and play a more active role in driving sustainable outcomes for investors, society and other key stakeholders. Regulators are also focusing on financial risks arising from climate change and sustainability. Firms therefore need to ramp up capabilities and embed climate and ESG risks in their business strategy, decision-making processes and financial reporting.

At the same time, ESG provides commercial and transformative opportunities (e.g. gaining competitive advantage, benefitting from the green transition, attracting investors, efficiency in operations, etc.) for firms to seize in order to drive change.

Please also refer to our ESG website for further information.

Key ESG themes

Environmental concerns

The impact of a firm on the environment (e.g. climate change, nature) and the impact of the environment on the firm.

Social concerns

The impact of a firm on individual and societal well-being and the impact of social pressures on the firm.

Governance concerns

The processes a firm has for decision-making, reporting and ethical behaviour.

ESG overview (2/2)

On the following pages, we will delve into these key themes in more detail, providing further guidance on the role that assurance functions can play.

Greenwashing

The self-regulatory landscape updated by three Swiss industry associations – the Asset Management Association (AMAS), the Swiss Banking Association (SBA) and the Swiss Insurance Association (SIA) – aims to reflect the Federal Council's position on greenwashing prevention in the financial sector.

The self-regulation is currently considered an appropriate tool for preventing greenwashing in Switzerland in the light of dynamic developments in the international regulation of sustainable finance, especially in the EU.

More broadly, a new provision in the Unfair Competition Act explicitly prohibits climate-related claims that cannot be objectively verified.

The 'E' in ESG: Nature-related financial risks

Nature-related risks have gained traction and have become a priority area both in Switzerland and abroad. Financial institutions are increasingly recognised as having a responsibility to address the substantial financial risks posed by climate change and environmental degradation effectively.

FINMA published its circular on the management of nature-related financial risks in line with the recommendations of international standard-setters in December 2024. The circular takes a principal-based approach and is applicable to Swiss banks and insurers, with some transitional periods. More details can be found on pages 56-57.

Sustainability reporting

The requirements of Swiss sustainability reporting (CO 964b) remain in place.

The Swiss Federal Council has proposed aligning Switzerland's sustainability reporting standards, including climate disclosures, with international frameworks such as the Corporate Sustainability Reporting Directive (CSRD), International Sustainability Standards Board (ISSB) and Global Reporting Initiative (GRI). First proposals have already been put forward.

In view of the uncertainties regarding the reporting regulatory landscape in the EU, especially due to Omnibus, the Federal Council has decided to postpone changing the requirements at this stage. This will enable it to obtain greater clarity on the updated EU approach.

The postponement is currently in place until no later than 1 January 2027.

Enhanced self-regulation landscape to prevent greenwashing (1/2)

Following the Federal Council's position on preventing greenwashing in the financial sector, the Swiss financial sector has enhanced and tightened the self-regulatory provisions regarding sustainable financial products and services.

The sustainable finance regulatory framework in Switzerland has recently undergone significant changes.

The Asset Management Association (AMAS), the Swiss Bankers Association (SBA) and the Swiss Insurance Association (SIA) have developed and enhanced the self-regulatory provisions regarding sustainable financial products and services. The aim is to strengthen Switzerland as a base for this type of business and implement various elements of the Federal Council's stance on preventing greenwashing.

There is a new, uniform minimum standard for labelling financial products or services as sustainable. In addition to their financial objectives, sustainable investment solutions in Switzerland will have to align with or contribute to specific sustainability goals. Financial institutions offering such solutions will have to meet clearly defined requirements in terms of sustainable investment policy, asset allocation, reporting, external audit, providing information, rendering account and providing enhanced training to their staff. These self-regulations took effect on 1 September 2024, with transitional periods for implementation extending until 1 January 2027.

The Federal Council has recognised the financial sector's progress in adopting self-regulatory provisions to prevent greenwashing and will refrain from introducing state regulation at this time. It has directed the Federal Department of Finance to reassess the need for regulatory action by the end of 2027, or earlier, depending on the outcome of the EU's review of the Sustainable Finance Disclosure Regulation (SFDR).

More broadly, the Unfair Competition Act now includes a new provision (Article 3(1)(x)) that explicitly prohibits climate-related claims that cannot be objectively verified. This regulation applies to qualitative statements (e.g. 'sustainable'), quantitative data and procedural claims, underscoring the importance of transparency and accountability alongside self-regulatory efforts.

Key considerations for firms

Analyse the applicability and key implications of the enhanced and newly developed self-regulations for your organisation.

Consider strategic implications.

Understand your readiness and gaps for complying with the applicable self-regulations by screening sustainability-related product offerings, documentation, reporting, training, governance structures and processes.

Strengthen your internal anti-greenwashing framework and guidelines.

Monitor regulatory developments.

Prepare for the upcoming assurance.

Enhanced self-regulation landscape to prevent greenwashing (2/2)

Assurance functions: focus areas

01

Review the firm's sustainability-related policies, products, concepts, processes and training to ensure that they adequately consider the principles of self-regulation.

02

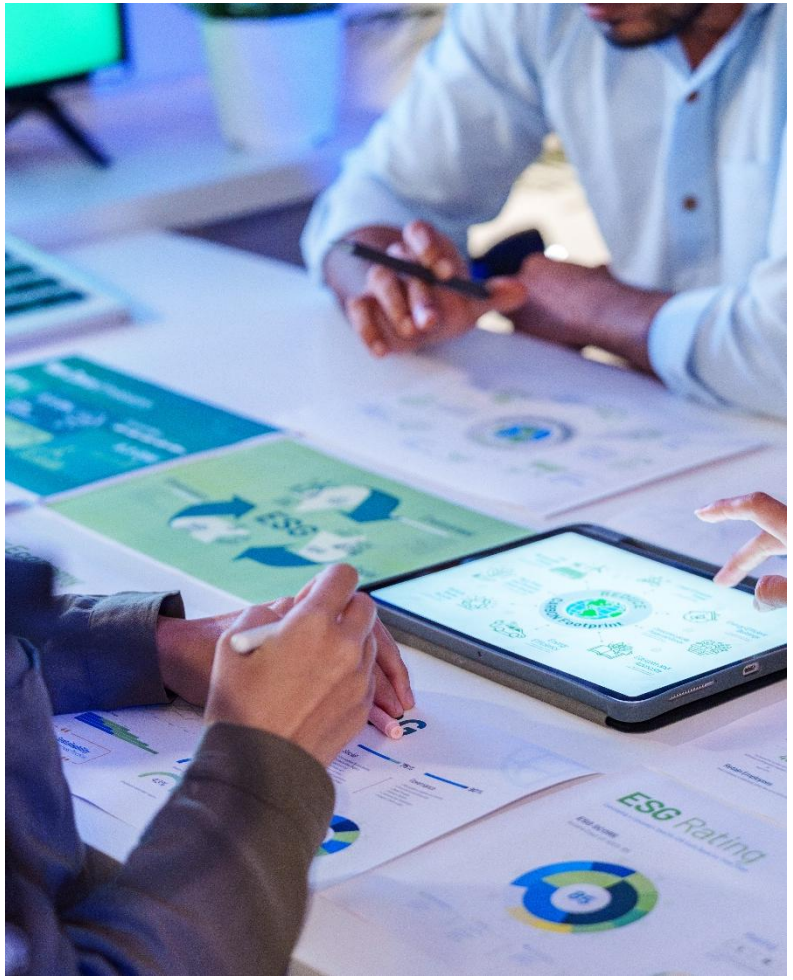
Check the risk and control frameworks and review product documentation, reporting, outsourcing agreements and other relevant documents.

03

Collaborate effectively with external assurance providers, if engaged, to streamline processes and align methodologies.

04

Review the firm's processes for monitoring and keeping up to date with the evolving regulatory agenda and expectations.



FINMA Circular on 'Nature-related financial risks' (1/2)

In line with the recommendations of international standard-setters, FINMA has issued a circular on nature-related risks for banks and insurers.

In December 2024, FINMA published its Circular 2026/1 'Nature-related financial risks', which significantly expands the scope of climate-related financial risk obligations for banks and insurance companies to encompass a broader, nature-related perspective. This regulatory development reflects FINMA's alignment with international standard-setters, including the Basel Committee on Banking Supervision (BCBS), the International Association of Insurance Supervisors (IAIS) and selected recommendations from the Network for Greening the Financial System (NGFS).

Nature-related financial risks are defined as the short-, medium- and long-term risks of direct or indirect financial losses or other adverse effects on institutions arising from their exposure to natural phenomena. These risks act as drivers across existing risk categories – such as credit (including counterparty credit), market, liquidity, operational (including legal and compliance), insurance, business and reputational risks – via multiple transmission channels.

The circular mandates institutions to embed nature-related risk governance within their organisational structures. Responsibilities must be clearly defined and documented across the Board of Directors and its committees, executive management, independent control bodies, Internal Audit and other relevant units in accordance with FINMA's supervisory expectations. Institutions are required to conduct materiality assessments of nature-related risks using scenario-based analysis across different time horizons. Larger institutions (Categories 1 and 2) are expected to incorporate these risks into (capital) stress testing frameworks, while smaller institutions must apply quantitative assessments for portfolios with elevated exposure.

There is a phased implementation timeline: requirements for category 1 and 2 institutions relating to climate will be effective from 1 January 2026. For category 3 to 5 institutions these requirements will be effective from 1 January 2027. Full nature-related financial risks (including biodiversity, water stress, etc.) will be applicable to all categories (1–5) from 1 January 2028. This staggered approach reflects the differing maturity levels of climate versus broader nature-related risk topics, as well as the varying degrees of preparedness across institutions. FINMA applies the principle of proportionality, setting more stringent expectations for larger and more complex institutions.

Key considerations for firms

Start early: Given FINMA's ambitious timeline, assessing the implications early is essential.

Prepare for materiality assessment and identification of all nature-related risks.

Analyse the expansion to nature-related risks. Understand how the shift from climate-only to a broader nature-related perspective (including biodiversity, water stress and ecosystem degradation) affects your risk management, governance and disclosure frameworks.

Evaluate your current climate-related financial risk set-up to identify gaps and opportunities for integration. Many governance and scenario analysis elements can be extended to cover nature-related risks.

Enhance scenario analysis and stress testing. Expand your climate scenarios to include nature-related dimensions. For larger institutions, this includes integrating nature-related risks into capital stress testing frameworks.

FINMA Circular on 'Nature-related financial risks' (2/2)

Assurance functions: focus areas

01

- Review the company's nature-related strategy and governance structures for decision-making.

02

- Review the internal risk management processes, including materiality assessments for nature-related financial risks.

03

- Review the internal framework for collecting nature-related data.
- Review the capital stress tests and scenario analyses for nature-related risks.

04

- Support the governance framework in identifying, assessing and managing nature-related risks.
- Monitor the integration of nature-related risks into risk management and reporting processes.

Governance – Risk culture (1/2)

In an era of increased regulatory scrutiny, fostering a robust risk culture at every level of the organisation is crucial for effective and responsible risk management.

Risk culture is the set of values, behaviours and subsequent actions that shape our collective approach to managing risk and making decisions. Risk culture works alongside risk management to help us all manage risk effectively and in line with our defined risk appetite.

Many organisations in a variety of sectors and industries are realising the benefits of investing in risk culture and how effective a strong risk culture can be as a key strategic enabler.

A strong risk culture goes beyond mere compliance, encompassing shared values, clear responsibilities and behaviours that guide risk identification, management and communication. Practical frameworks, transparent processes and effective monitoring empower employees to engage in prudent risk management and align risk appetite with business goals.

Neglecting risk increases the likelihood of operational failures, reputational harm and regulatory penalties. Conversely, nurturing a proactive risk culture enhances operational resilience, supports sustainable growth and promotes long-term success.

In this context, boards play a vital role by setting the tone from the top, embedding risk awareness into organisations' strategies and values, overseeing risk policies, encouraging accountability and fostering open communication. Continuous dialogue with management ensures that the risk culture aligns with the established risk appetite, underpinning long-term stability.

Key considerations for firms

From mindset to action: building the frontline of risk culture

Employees serve as the first line of defence in managing risk and ensuring compliance. Building an effective risk culture requires fostering daily awareness and safe behaviours across all levels, from frontline staff to senior management. Beyond rules and controls, a fundamental cultural shift is required to embed a robust risk mindset throughout the organisation. This shift hinges on the relationship between mindset, behaviours and actions.

Overcoming challenges and obstacles

To build a strong risk culture, organisations must address common challenges such as siloed risk ownership, overreliance on models, regulatory fatigue, inconsistent risk appetite and a weak speak-up culture. Overcoming these barriers is vital to promote open communication, alignment and effective risk management for lasting resilience.

Anchoring and measuring a strong risk culture

Aligning corporate strategy and values with risk objectives is essential. Leadership must demonstrate positive risk behaviours and set a strong tone from the top. Effective risk management relies on robust systems, policies and controls, alongside continuous investment in risk capabilities through targeted training and infrastructure. Clear roles and accountability foster responsible risk practices, while recognising successes and addressing failures drives continuous cultural improvement. Open communication and collaborative knowledge sharing empower employees to raise concerns and work cross-functionally, promoting a comprehensive approach to risk.

Regularly monitoring risk culture and engaging key stakeholders such as executives and board members provides valuable insights into the effectiveness of strategies and shifting risk behaviours. This process helps to identify areas needing course correction and, through risk culture metrics, enables organisations to anticipate emerging threats to a strong risk culture.

Governance – Risk culture (2/2)

Assurance functions: focus areas

01

Risk culture evaluation

Risk culture evaluation involves assessing the current state of the organisation's risk mindset and behaviours through tools such as surveys, focus groups and interviews. These methods help identify existing challenges, gaps and perceptions around risk management across different levels. In addition to understanding the present culture, the evaluation process defines the desired target state, establishing clear cultural goals that align with the organisation's risk appetite and strategic objectives. This foundation guides the development of effective initiatives to strengthen and embed a robust risk culture.

02

Risk culture monitoring

Risk culture monitoring focuses on the continuous measurement and observation of risk-related behaviours and attitudes across the organisation. It employs a combination of quantitative metrics and qualitative feedback to track changes in risk mindset, compliance with risk policies and openness in communication channels. Continuous monitoring enables early detection of cultural shifts or emerging risks, allowing organisations to take timely corrective actions and maintain a resilient, proactive risk environment.

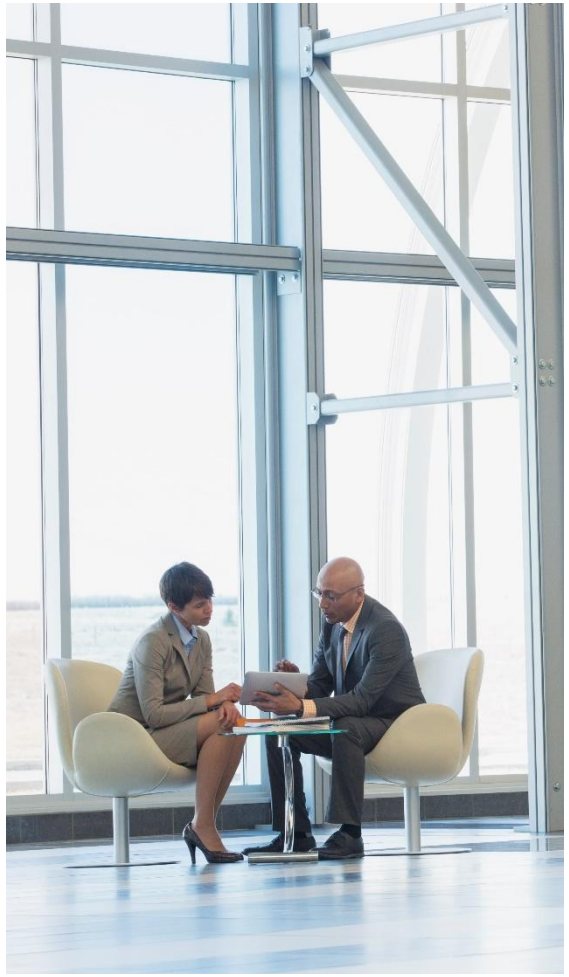
03

Auditing risk culture

Approaches to culture audits vary widely across organisations: some internal audit functions incorporate management awareness ratings in their reports; others break culture into specific themes such as leadership behaviours, decision-making, or accountability, while some embed cultural assessments into broader audits such as health and safety, conduct and HR.

Leading functions are developing structured methodologies for cultural assurance that combine targeted deep dives with broader organisation-wide assessments. In some cases, culture or behavioural specialists are engaged to design and deliver these reviews, adding expertise in assessing values and behaviours. Increasingly, functions are also leveraging data analytics and sentiment analysis tools to identify patterns and detect emerging cultural risks.

Crucially, culture audits should not be treated as one-off exercises but embedded in the audit universe as recurring themes. This provides boards and audit committees with clearer visibility of cultural strengths and weaknesses, as well as early warning indicators of behavioural misalignment before issues grow into regulatory, reputational, or operational challenges.



Banking

Prudential – Basel 3.1. overview (1/2)

Key considerations for firms

Overview of Basel III Final reform

- Basel III Final marks the completion of post-crisis regulatory reforms to strengthen bank resilience.
- It enhances risk sensitivity, transparency and comparability of capital requirements.
- The framework introduces stricter constraints on internal risk models and incorporates output floors to limit model-based capital reductions.
- The full scope of Basel III Final came into effect in Switzerland on 1 January 2025.

Implications for the cost of capital

- Based on within-year data reports, there are strong indications that the Basel III Final reform in Switzerland had a largely capital-neutral impact at aggregate level, consistent with the Swiss authorities' quantitative impact studies.
- However, minimum capital requirements vary significantly across banks depending on business models, credit portfolio compositions and historical loss experiences.
- The introduction of the output floor limits capital reductions from internal models, strengthening systemic stability but possibly affecting bank profitability and lending capacity.
- Notably, smaller banks have experienced marked increases in market risk capital requirements due to stricter parameters in the simplified standardised approach.
- Credit risk, the most significant risk category by far, shows mixed effects at individual level as risk weights were recalibrated to align better with underlying risk, contributing to heterogeneity across institutions.
- Meanwhile, operational risk capital requirements have generally decreased for many banks.

Summary of major changes in the Basel III Final reform

- **Credit risk**: The Basel III Final reforms introduced significant changes to the Standardized Approach (SA) for credit risk to improve the comparability of Risk-Weighted Assets (RWA) measurement across banks. A few of the most impactful changes included refining and expanding the granularity of exposure classes, particularly for real estate, and adjusting risk weights to better align sensitivities across these categories. Additionally, the reforms mandated banks to perform due diligence when relying on external credit ratings, reducing dependence on credit rating agencies. There was also a new requirement to maintain the original loan value for a minimum of five years, along with an expansion of the eligible collateral instruments to enhance flexibility in securing loans.
- **Market risk**: The Basel III Final reforms for market risk centred on the revised boundary between the regulatory banking book and trading book exposures, as outlined by the Fundamental Review of the Trading Book (FRTB). The framework introduced stricter rules for the classification and potential reclassification of positions between these books, reducing opportunities for capital optimisation by shifting assets. Furthermore, Basel III Final recalibrated the existing standardised approach (under Basel III Final known as the 'simplified standard approach') and introduced a new "Standard approach". This new approach moves towards a standardised model in which add-on capital charges are foreseen for default risk and residual risk (e.g. for certain exotic instruments) that complement the sensitivities-based (delta, vega, curvature) capital charges.
- **Operational risk**: The revised approach in Basel III Final maintained the Business Indicator (BI) as a financial-statement-based proxy. However, a new non-linear logic has been introduced to accommodate the increased complexity of larger banks. This comes into effect for banks with a BI exceeding CHF 1.25 billion by incorporating a dynamic risk-sensitivity loss parameter called the Internal Loss Multiplier (ILM), which is determined by the bank's average historical operational losses over the past 10 years, reflecting its loss track record. Smaller banks, with a BI below CHF 1.25 billion, may, with FINMA's approval, either use the dynamic ILM or opt out of the historical component by setting the ILM to 1.

Prudential – Basel 3.1. overview (2/2)

Assurance functions: focus areas

01

Input data

- Ensure that the bank has sufficiently high data quality as transactional data is required for computing selected risk weights.
- Ensure availability of input data given that a wider range of data is required to allocate the correct risk weights.

02

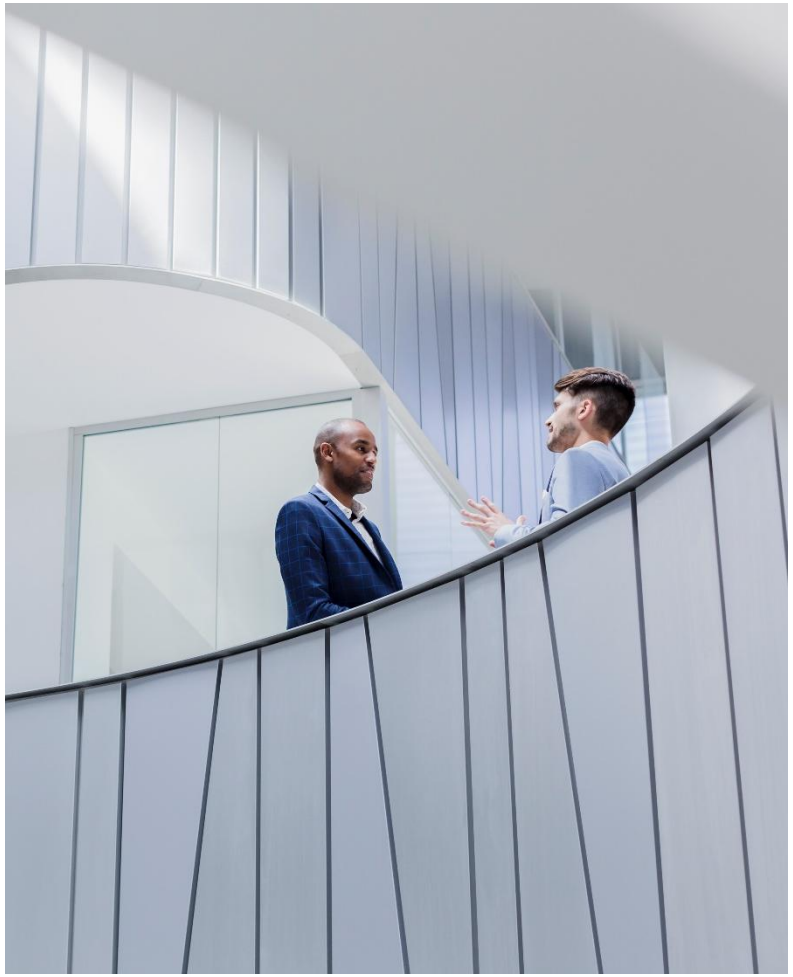
Governance and processes

- Ensure that the bank has adjusted the processes with regard to the updated controls and that governance of external ratings is established.
- Ensure that the bank has adjusted its internal documentation to reflect adherence to the new regulation, as several FINMA circulars will be replaced by new ordinances (e.g. FINMA Circular 2016/1 will be replaced by a new ordinance on disclosure: 'OffV-FINMA' (DE)/DisO-'FINMA' (EN)).

03

Regulatory text and public disclosures

- Validate whether manual or automated controls are in place to apply retention schedules, execute secure deletions and provide evidence of ongoing compliance. Consider testing specific repositories for unused content or records beyond documented retention limits.



Financial market stability: 'Too big to fail' reform package (1/2)

Key (proposed) components of the reform

Crisis management
- Introduction of expanded resolution options, including "orderly resolution", to improve flexibility in managing crisis involving Systemically Important Banks (SIBs).
- Enhanced stabilisation (recovery) and resolution planning requirements specifically (but not limited to) targeting SIBs to strengthen resilience and preparedness.

Emergency liquidity enhancement
- Strengthening of the lender of last resort (LoLR) framework as the second line of defence in liquidity crises.
- Implementation of regulatory requirements obliging banks to prepare adequate amounts of collateral for central bank emergency liquidity.
- Implementation of public liquidity backstop (PLB).

Supervisory powers
- Substantial expansion of FINMA's enforcement toolkit, including legally anchored measures to enable stronger early intervention and more decisive supervisory actions.
- Granting unrestricted authority to FINMA to conduct on-site examinations and inspections at all banks, ensuring comprehensive supervisory oversight.
- Introduction of pecuniary sanctions targeting supervised entities to impose financial penalties for serious regulatory breaches without resorting to license revocation.

Timeline
- The reform package is currently in the consultation process; the scope may be adjusted before final adoption.

What is planned to change
- More comprehensive crisis resolution coverage for SIBs
- Enhanced liquidity support mechanisms
- Stricter capital and supervisory requirements
- Greater legal certainty and coordination in crisis situations

Which institutions are affected
- The rules of the reform package concern SIBs.
- Although legally specific to SIBs, recent regulatory developments suggest broader regulatory expectations for recovery and resolution planning across all banks in Switzerland to strengthen operational resilience of the industry.

Challenges
- Complexity and costs of compliance for impacted banks, particularly in cross-border contexts
- Continuous dialogue between regulators and institutions will be critical for smooth and risk-oriented implementation.

Financial market stability: ‘Too big to fail’ reform package (2/2)

Assurance functions: focus areas

01

Enhanced regulatory expectations

Assurance functions will need to adapt to more stringent supervisory requirements, including enhanced stabilisation and resolution planning, which increase the complexity and scope of risk assessment and control activities.

02

Liquidity preparedness

Auditors and internal assurance teams should place greater focus on banks’ preparedness for collateralising access to central bank emergency liquidity and evaluate adherence to new liquidity frameworks such as LoLR enhancements.

03

Risk of operational complexity

The expanded regulatory landscape and new tools increase operational complexity, creating a need for assurance functions to focus on integrated risk management and continuous monitoring capabilities.

04

Increased transparency demands

Assurance providers should expect higher expectations for transparency in reporting enforcement and supervisory findings, requiring clear communication protocols and thorough documentation.

Anti-money laundering (AML) (1/2)

Regulatory focus

- Oversight continues to tighten in 2025. FINMA's new strategic goals emphasis uncompromising AML compliance, stronger governance and risk culture with clearly defined risk-tolerance thresholds and resilient risk management.
- Recent regulatory publications highlight persistent weaknesses with high-risk clients, delayed risk alert handling and focus on exposure to goods-related sanctions, which require attention.

Regulatory expectations

- High-level of KYC data quality and completeness.
- Holistic and institution-specific risk management measures.
- Technology-enabled connected surveillance for complex structures and domiciliary companies.
- Dynamic and tailored monitoring business rules and risk scenarios for higher-risk relationships and transactions.
- Maintain a well documented, business-specific AML risk assessment including clear risk appetite statements.
- Implementation and screening against new sanctions within 24 hours of announcement (or latest with the date sanctions enter into force). This particularly puts pressure on third-party providers which offer sanctions screening solutions).

Financial Intelligence Unit (Money Laundering Reporting Office Switzerland, MROS) developments in 2025

- The 2024–2027 strategy focuses on efficient SAR triage, targeted analysis, technology and training, and stronger national and international coordination.
- Activity continues to rise: SARs +27.5% to 15,141; referrals to law enforcement +20.4% to 1,043.
- The published Typology report gives financial intermediaries practical case studies on suspicious circumstances in money laundering and terrorist financing, highlighting indicators, risks and mitigation. Aimed at compliance, customer-facing staff and Senior Management, it is formatted in two volumes: Vol. I covers typologies (e.g. mismanagement, fraud, commodity trading, art, real estate, virtual assets); Vol. II focuses on enablers with actionable, practitioner-oriented insights.
- The published Negative Typology seeks to discourage "defensive" SARs. Reports must show a qualified, well-documented suspicion after required enquiries. Non-threshold submissions include: aborted online onboardings with no relationship or funds flow; "unusual" customers without links to criminal assets; unanalysed third-party information (production orders, listed persons, negative news); mere use of crypto; victim-only matters; assumptions of "black funds" without a predicate offence; and market-abuse cases lacking Swiss-listed instruments or statutory triggers.

Forthcoming regulatory changes

Transparency register: a separate federal law is expected to introduce a central beneficial-owner register for legal entities (administered by the Federal Office of Justice) with controlled authority access.

AMLA reform: expected to introduce i) AML due diligence duties for lawyers and advisors, ii) reduce cash thresholds, iii strengthen sanctions-risk controls, and iv) standardise reporting to MROS.

CDB (Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence) revision: Expected to be introduced in 2027 to leverage from the transparency register reforms.

Anti-money laundering (AML) (2/2)

Assurance functions: focus areas

01

AML risk analysis

Prioritisation of a clear and articulated risk tolerance, strong tone from the top, analysis of inherent, control and residual risk, executive involvement for high-risk clients, comprehensive risk identification and assessment, plausible key risk indicators, and demonstrable effectiveness of mitigating controls.

02

Control framework and documentation

Expectation of current, complete policies and guidance, up-to-date control plans and inventories, defined reporting processes including documented non-reporting rationales, clear first line accountability, enhanced training and proper record-keeping.

03

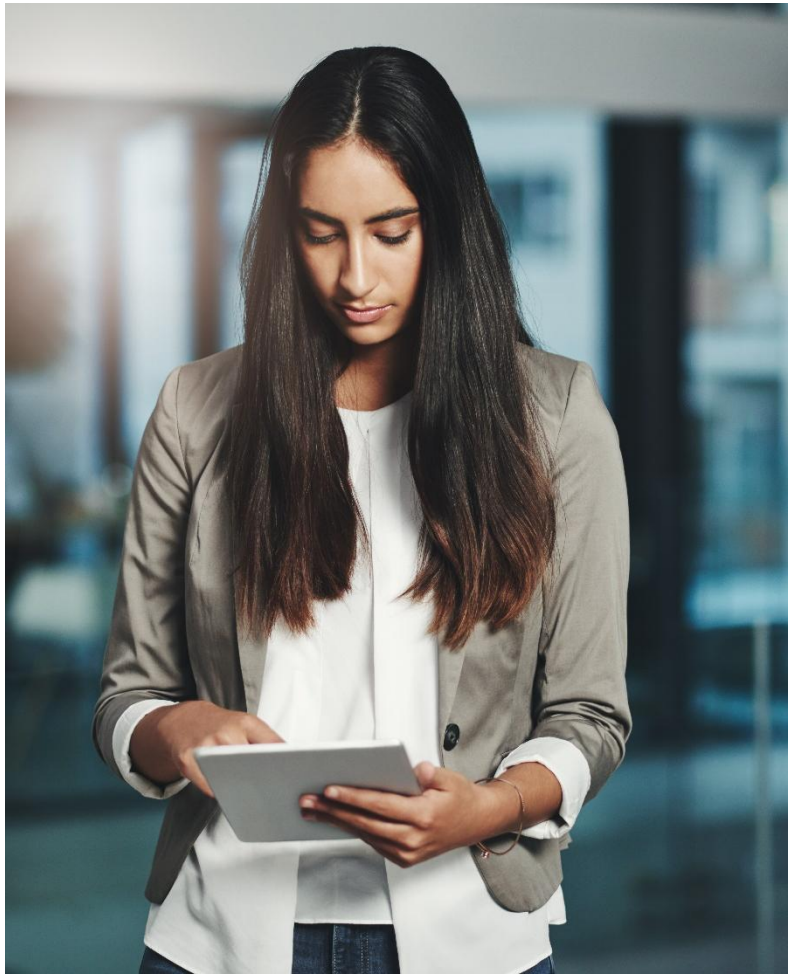
Institute-specific metrics

Scrutiny of institution-specific parametrisation for HRT/HRC, regular and event-driven validation of models, high-quality and available data, tailored cash and terrorism-financing scenarios (including static and dynamic factors), timely backlog remediation and fully traceable investigation documentation.

04

Complex structures

Heightened attention to complete, current KYC for complex structures and domiciliary companies (also for those which are part of the structure but not necessarily an own client): explicit rationale for the single entities and the whole structure, roles and cross-references across the structure, expected transaction behaviour and economic sense, harmonised risk classification, periodic reviews and holistic, IT-enabled monitoring.



FINMA Circular on 'Liquidity Risks'/Liquidity – Banking Act (BankA) public liquidity backstop (1/2)

Consultation LiqO and LiqO-FINMA

Background

- The new 'LiqO-FINMA' elevates the existing qualitative and quantitative liquidity risk management requirements from a circular to ordinance level for legal clarity. The revision transfers all key elements of FINMA Circular 2015/2 'Liquidity risks – banks' to the new ordinance. It adds detailed rules on liquidity and financing planning as well as information disclosure during liquidity stress, complementing changes in the LiqO.
- **Regulatory goal:** Improve timely and reliable liquidity information for authorities to monitor banks effectively and enable early intervention from authorities in crises.

Key changes

- Banks must enhance capabilities in a proportional manner to provide more frequent updates and transmit both existing and new liquidity indicators to FINMA, including:
  - The ability for daily reporting of regulatory liquidity measures in times of liquidity stress (e.g. liquidity coverage ratio, liquidity monitoring tools) as well as detailed data on current deposit outflows and internal scenario analysis.
  - Adaptable reporting infrastructure to ensure continuous and complete reporting post reorganisations in banking groups.
- **Proportionality:** Possible relief in reporting scope for category 4 and 5 banks.

Timeline

- **Planned entry into force**: 1 January 2027
- **Transition period**: Until 1 January 2028 to implement daily liquidity reporting capability in stressed periods

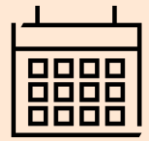
Public liquidity backstop (PLB)

Background

- The PLB is proposed as part of measures to strengthen the liquidity framework for systemically important banks (SIBs).
- it serves as a supplementary and last-resort liquidity support instrument provided by the Swiss Confederation, intended to cover situations when other liquidity provisioning is insufficient.

Timeline

- The legal basis and detailed implementation of the PLB is currently suspended until the Federal Council submits its message to Parliament on the modifications of the 'too big to fail' regulations. See also pages 63–64.



FINMA Circular on 'Liquidity Risks'/Liquidity – Banking Act (BankA) public liquidity backstop (2/2)

Assurance functions: focus areas

01

Data quality

- Auditors need to consider the regulators authority on submission timing, data scope, quality standards, format and frequency.

02

Process quality

- Verification that banks have implemented processes to deliver accurate, timely and comprehensive liquidity data to comply to the new requirements.
- Assessment whether reporting systems can meet increased frequency and quality standards.

03

Proportionality

- Awareness of regulators differentiated requirements and possible relief options for certain bank categories.
- Banking with a group structure: Assessment of adaptable reporting infrastructure to ensure continuous and complete reporting even after reorganisations.

Insurance

FINMA Circular 2025/3 ‘Liquidity – Insurers’ (1/2)

Background

In 2023, the Federal Council amended the Insurance Supervision Ordinance (ISO), introducing a requirement for insurers to submit annual reports on their liquidity planning to FINMA. These changes became effective on 1 January 2024. At the same time, the topic of liquidity has attracted increased international attention within insurance supervision. In response, FINMA has undertaken a comprehensive revision of Circular 2013/5 ‘Liquidity – Insurers’.

Content and scope

The new FINMA Circular 2025/3 ‘Liquidity – Insurers’ is divided into six key areas:

1. **Governance**: Establishment of a clear organisational and operational structure, with defined allocation of tasks, authorities and responsibilities.
2. **Liquidity management and planning**: Planning future liquidity inflows and outflows across different time horizons, including the management of available liquid assets.
3. **Liquidity reserve**: Provision of high-quality liquid assets to bridge short-term liquidity needs.
4. **Liquidity risk management**: Ensuring liquidity even under stress scenarios and integrating liquidity risks into the insurer’s overall risk management framework.
5. **Liquidity controlling and monitoring**: Implementation of effective processes for measuring, monitoring and managing liquidity; integration into the internal control system.
6. **Contingency planning**: Definition of processes and measures according to the severity of a liquidity shortfall.

This circular applies to insurance companies based in Switzerland as well as to insurance groups and insurance conglomerates. For insurance branches of insurance companies only certain referred marginal notes apply.

Timeline

- The revised circular has been in force since 1 January 2025.
- Insurers and branches must prepare an annual liquidity planning report for FINMA as of 31 December. The report for the previous financial year must be submitted to FINMA no later than 30 April of the following year. FINMA publishes the survey by 30 June of the financial year.
- The first ordinary reporting to FINMA for the 2025 financial year is scheduled for 30 April 2026.

PwC’s view

Although FINMA’s new requirements set a high bar for insurers, they also provide an opportunity to identify risks at an early stage and manage them sustainably.

FINMA Circular 2025/3 ‘Liquidity – Insurers’ (2/2)

Assurance functions: focus areas

01

Clear roles and governance structure

- Assess whether clear roles, responsibilities and governance structures are established for liquidity planning and management.
- Confirm that the allocation of tasks and authorities is documented and aligns with regulatory expectations.

02

Assessment of liquidity reserve

- Review the adequacy and quality of liquidity reserves, ensuring that high-quality liquid assets are available to meet short-term needs.
- Evaluate how reserves are planned and maintained across different time horizons.

03

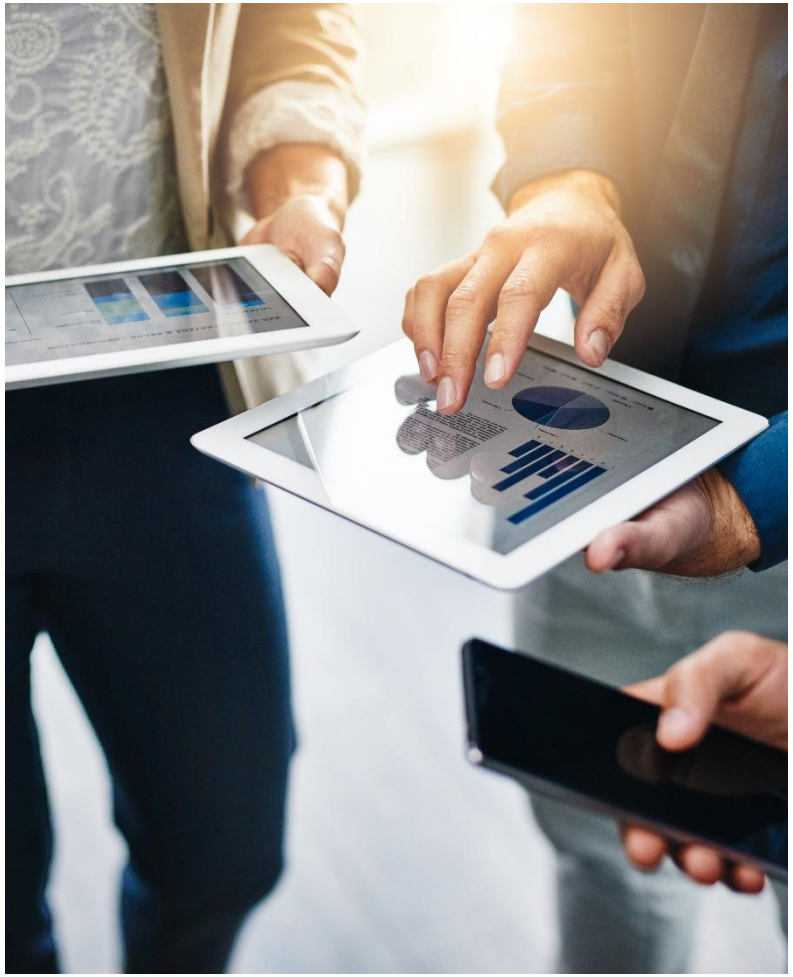
Contingency funding plan

- Review the existence and effectiveness of contingency plans for liquidity shortfalls.
- Ensure that processes and measures are defined for various levels of liquidity stress.

04

Completeness of reporting

- Verify that annual liquidity planning reports are prepared and submitted to FINMA in accordance with regulatory deadlines.
- Confirm that reporting is standardised and complete.



FINMA Circular 2024/1 'SST' (1/2)

Background

FINMA Circular 17/3 has been replaced by a new, significantly shorter circular on the SST. This new Circular 2024/1 'SST' includes elements from the previous version that have not already been incorporated into the Insurance Supervision Ordinance (ISO) or the FINMA Insurance Supervision Ordinance (ISO-FINMA). The previous guidance on scenarios is omitted. In terms of content, the new circular covers, in addition to SST governance requirements, FINMA's practices regarding disclosures related to standard models, requirements for SST calculation and reporting, and the review of SST reports and models by FINMA.

Relevant changes

- **SST governance:** Explicit requirements for governance related to the SST, based on Art. 14a ISO.
- **FINMA publications and announcements**: Consolidation and updates of previous guidance and current practice.
- **Review of SST models**: Clarification in FINMA's approach to reviewing models, distinguishing between summary and in-depth reviews. Summary reviews are for approval requests, while in-depth reviews examine models and SST calculations in greater detail, sometimes comparing models across insurers or delegating reviews to external parties.
- The revised FINMA Circular applies to all insurance companies, groups and conglomerates in Switzerland.

Timeline

The revised circular has been in force since 1 January 2025.

PwC's view

As part of the revision of the FINMA Circular on the SST in connection with the revision of the ISO-FINMA, there were no significant substantive changes. The content of the previous Circular SST was largely incorporated into the ISO-FINMA.

FINMA Circular 2024/1 'SST' (2/2)

Assurance functions: focus areas

01

Model governance

- Assess that models used for the SST calculation are validated, documented and regularly reviewed.
- Verify that there is an effective allocation of roles, ensuring that subject matter experts with sufficient expertise are involved.

02

Completeness and effectiveness of internal control system/data quality

- Verify that there is an effective and complete internal control system in place ensuring correctness of the SST results and accuracy, completeness and traceability of the data used for the SST calculations.

03

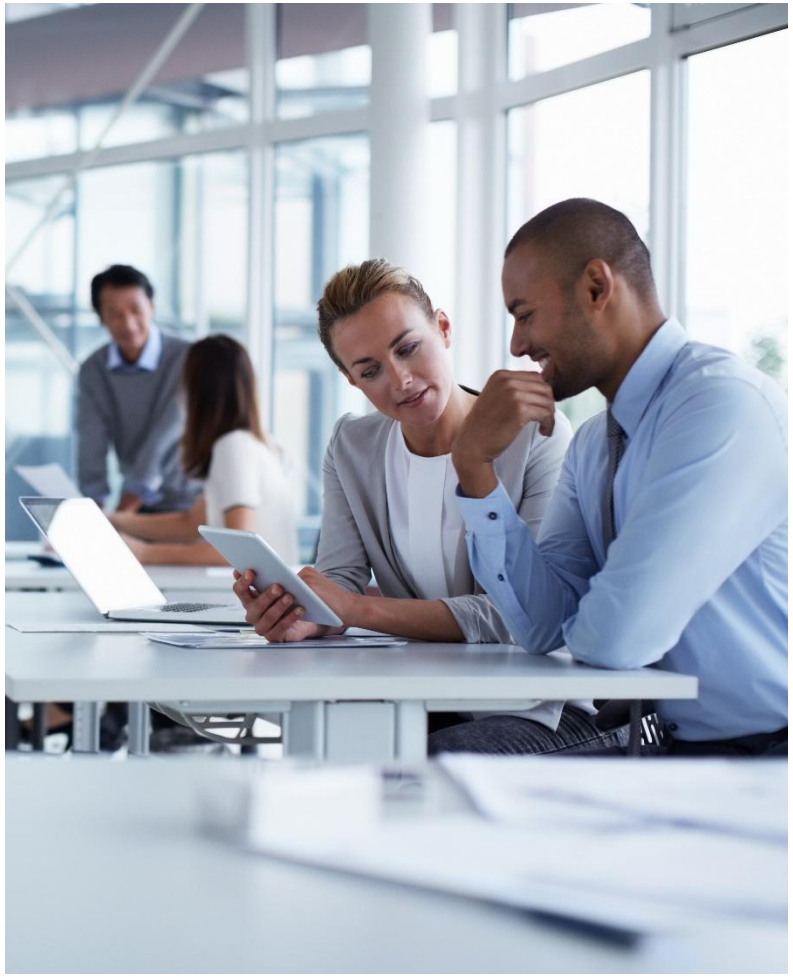
Completeness of risks and scenarios

- Assess whether all relevant risks are included in the SST calculation. For any risks that cannot be directly captured by the SST risk assessment, scenario analyses should be performed to ensure that plausible adverse events are adequately considered.

04

Regulatory compliance and reporting

- Assess whether the SST framework complies with the latest FINMA requirements and guidance.
- Verify that SST reports are prepared and submitted to FINMA in accordance with regulatory deadlines, including clear documentation of methodologies, assumptions and changes.



Insurance Intermediaries – FINMA Guidance 05/2024 (1/2)

General

On 1 January 2024, the revised Insurance Supervision Act and Insurance Supervision Ordinance entered into force. The new regulation introduces significant changes for the Swiss insurance industry, particularly regarding the cooperation with tied and untied insurance intermediaries.

Tied insurance intermediaries

Tied insurance intermediaries are natural or legal persons who distribute insurance policies exclusively for one insurance company and act on their behalf in a dependent relationship. Since 2024, they are no longer listed in FINMA's public register and are attributed to the insurance company they are tied to. This can include sub-insurance intermediaries, so insurance companies must understand their entire value chain. Insurance companies must perform checks before onboarding and conduct ongoing monitoring once the collaboration begins.

Checks before starting the collaboration

Before the collaboration begins, detailed checks must be carried out by the insurance company to ensure that all legal requirements are met. The initial review for natural persons covers (inter alia) the agreement, personal documents (such as CV, criminal records), no entry in FINMA's public register, financial security. Checks on legal entities, partnerships, and sole proprietorships include (inter alia) reviewing shareholdings and corporate governance, assessing the fitness and propriety of members of the Board of Directors and executive management, no entry in FINMA's public register, confirming the absence of negative entries on FINMA warning lists, check of the financial security and a check of the employees.

Ongoing checks

After the collaboration begins, insurance companies must continuously monitor compliance by the tied insurance intermediaries. This includes, among other things, the following obligations:

- **Conflicts of interest**: Organisational and contractual measures (e.g. directives and an appropriate control framework) must ensure that misaligned incentives and conflicts of interest are avoided.
- **Training requirements**: Compliance with initial and continuing training requirements is mandatory for all insurance intermediaries and is monitored by the insurance companies.
- **Reporting obligations for cyber-attacks**: Specific reporting obligations for cyber-attacks on tied insurance intermediaries must be strictly observed.
- **Complaint management**: Professional operation of a complaints management system at the insurance company that records complaints received in connection with intermediary activities.
- **Risk management and controls**: Insurance companies must establish a risk management framework that identifies, monitors and limits all operational risks associated with intermediary activity.

Untied insurance intermediaries

Untied insurance intermediaries are legally and economically independent natural or legal persons who may offer products from multiple insurance companies. Insurance companies may only work with untied intermediaries who are listed in the FINMA register. They must regularly verify the insurance intermediary's status and ensure registration is maintained throughout the collaboration. This duty also covers the natural persons acting for the legal entity, partnership, or sole proprietorship, as well as untied sub-insurance intermediaries. To comply with the rules, suitable controls must be implemented, and the insurance company must have adequate risk management and a complaints management system, as with tied insurance intermediaries.

Insurance intermediaries – FINMA Guidance 05/2024 (2/2)

Assurance functions: focus areas

01

Governance and oversight

- Adequacy of governance structures, roles and accountability for intermediary oversight.
- Effectiveness of onboarding, due diligence and ongoing monitoring processes.

02

Risk and compliance management

- Coverage of intermediary-related risks (operational, conduct, reputational) within the risk framework.
- Compliance with FINMA registration, training and conflict of interest requirements.

03

Incident and complaint handling

- Robustness of complaints management and escalation mechanisms.
- Compliance with reporting obligations for cyber incidents involving intermediaries.

04

Assurance integration

- Coordination on intermediary oversight between Internal Audit, Risk and Compliance.
- Integration of intermediary topics into annual assurance plans and thematic reviews.

4

Internal audit practices and capabilities

- Top of mind for CAEs
- Common challenges and first experiences of the new standards
- Preparing for EQAs under the new standards
- AI in internal audit

Top of mind for CAEs

Internal audit has always adapted to change, but today's pace feels different.

With the IIA's Global Internal Audit Standards taking effect in January 2025, attention is turning to how requirements should be interpreted, demonstrated in practice and assessed through external quality assessments (EQAs) or readiness reviews.

At the same time, Boards and Audit Committees are raising expectations: they want sharper insights, broader coverage and faster assurance – all against a backdrop of shifting risks from geopolitical uncertainty and cyber threats to climate change and organisational resilience.

For internal audit leaders, the question is no longer whether to broaden the remit, but how to do so without compromising independence or credibility. Drawing on recent EQAs, client experience and market insights, we explore how functions are adapting: how technology, particularly AI, is enabling smarter assurance and sharper analytics; and how Internal Audit can evolve to meet higher expectations.

Ultimately, Internal Audit has a unique opportunity to redefine its relevance. By balancing conformance with value creation, driving functional evolution and embedding responsible AI, it can position itself as a trusted partner that protects value while enabling resilience, innovation and growth.

We categorise our insights as three themes that are top of mind for chief audit executives (CAEs) today:

Common challenges and first experiences with the new standards: We share what we are seeing in practice as Internal Audit functions interpret the new requirements and work to demonstrate conformance. We also share our insights into leading practices, highlighting how functions that are ahead of the curve are embedding the standards.

Preparing for EQAs under the new standards: we comment on the new four-point quality rating scale, what we have learned so far from our EQA experience and some helpful tips to prepare for your next EQA.

Adoption of AI in Internal Audit: We share insights on how emerging technologies can support smarter assurance, sharper analytics and more compelling insights, while maintaining independence and responsible governance.

Common challenges and first experiences of the new standards (1/4)

The Global Internal Audit Standards (GIAS or the standards) came into effect in January 2025. Together with the updated Quality Assessment Manual and the first Topical Requirements (starting with cybersecurity (see page 27) and third-party (see page 37), they reinforce the profession's aim to elevate Internal Audit's strategic positioning in organisations. While the intent is to drive consistency, maturity and value creation; many Internal Audit functions are still working through how to interpret and evidence these requirements in practice.

01

Board and senior management responsibilities (GIAS Standards Domain III) – focuses on governance and sets clear expectations for the Board and Senior Management.

Over the past year, many Internal Audit functions have struggled with how best to conform with and evidence the essential conditions relating to board and senior management responsibilities.

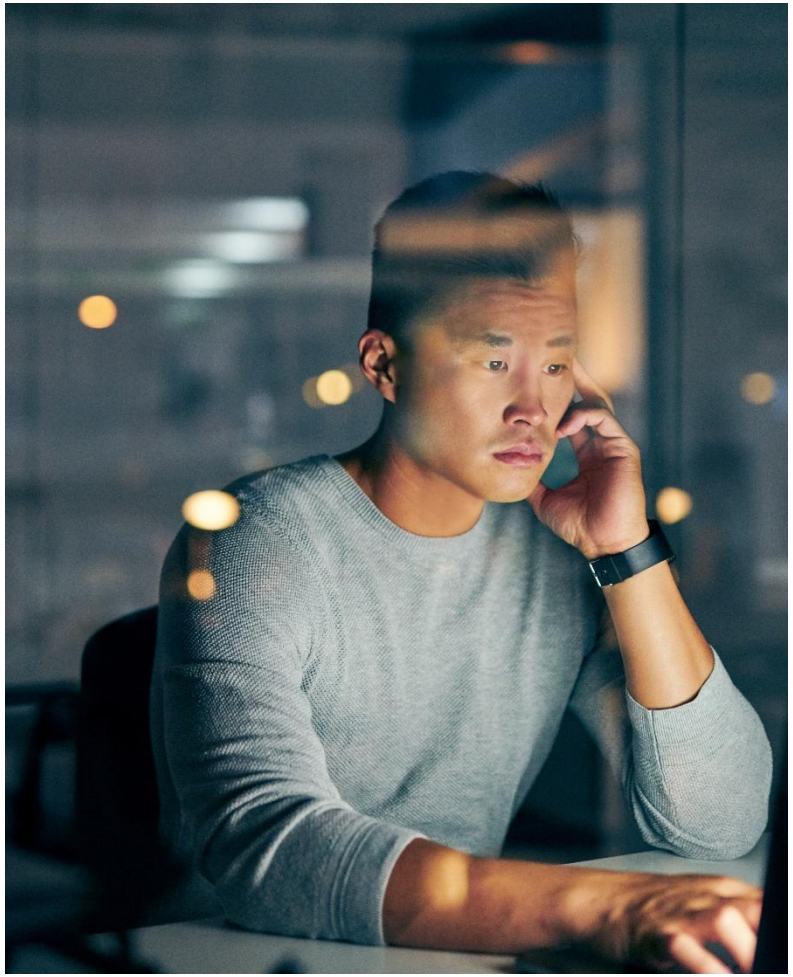
Those that undertook readiness assessments early are now ahead: they have mapped each condition to their governance structures, built frameworks aligned to their business and embedded these into day-to-day activity. In many cases, they have also actively engaged stakeholders through structured discussions and presentations to not only communicate their responsibilities but also to demonstrate how Internal Audit will help them deliver on those responsibilities.

02

Internal audit strategy (GIAS Principle 9) – emphasises the importance of developing and implementing an internal audit strategy that supports the organisation's strategic goals and meets stakeholder expectations.

We observe differences in how strategies are reviewed and approved. According to the standards, strategies should undergo regular review and be discussed with the Board and Senior Management.

Leading functions demonstrate strong 'golden thread' linking the internal audit strategy to organisational goals, convert this into KPIs and action plans, and review the strategy with the Board at least once a year to maintain its relevance. This approach ensures that the strategy does not remain as static 'on a page' document, disconnected from the organisation's priorities.



Common challenges and first experiences of the new standards (2/4)

03

Topical Requirements (GIAS) – specific requirements set out by the IIA to be used when providing assurance on a specified risk area.

The introduction of Topical Requirements under GIAS is a major step to driving improvements in consistency and quality across the profession. The first Topical Requirements on cybersecurity and third-party have already been released, with others including organisational resilience and organisational behaviour expected to be published shortly.

Although the first Topical Requirement (cybersecurity, see also page 27) does not take effect until February 2026, many functions are already reviewing and some adopting the guidance. The newly issued IIA's Topical Requirements Application Guidance is important, as it makes clear that not every requirement will apply in every engagement, but Internal Audit must document its rationale for inclusion or exclusion.

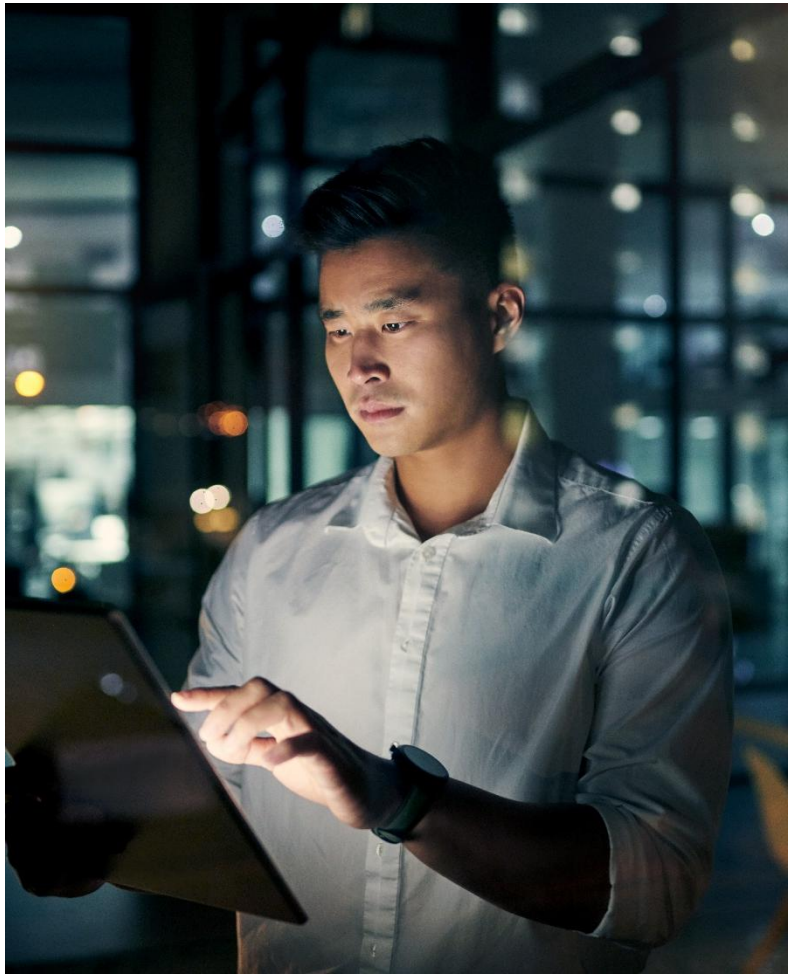
Some CAEs remain cautious, concerned the requirements may be too prescriptive.
The real opportunity is to apply proportionality while meeting a global baseline. Those who adopt early, document decisions and engage stakeholders will be best placed to demonstrate maturity when the requirements become effective.

04

Insights from Internal Audit, reporting and conclusion statements (GIAS Domain I, Standards 11.3, 14.5 and 15.1) – focuses on providing overall conclusion on the effectiveness of the governance, risk management and control processes.

While reporting formats continue to evolve, for many Internal Audit functions the requirement to provide an annual overall conclusion is challenging. Beyond compliance, there is also a growing expectation for Internal Audit to provide insights and foresights. The standards (Domain I: Purpose of Internal Auditing) emphasis the need for Internal Audit to enhance organisational value by helping stakeholders anticipate emerging risks.

We have seen leading functions excel by performing read-across analysis, for example, drawing out patterns by product lines, revenue streams, or regional performance to highlight systemic issues and forward-looking implications. This ability to connect the dots and provide an enterprise-level perspective is increasingly what distinguishes Internal Audit functions that are simply compliant from those regarded as truly value-adding.



Common challenges and first experiences of the new standards (3/4)

05

Quality assurance and improvement programme (QAIP) (Standards 17.1–17.3) – not a new requirement however this remains one of the most common areas of weakness. We continue to see undocumented QAIPs, internal quality assessments not performed annually, results not shared with the Board or Senior Management and action plans that are not tracked. The standards are clear: a QAIP must include an annual internal quality assessment, with results communicated to the Board and Senior Management and improvement actions incorporated and progress monitored. Yet in practice, QAIPs often remain underdeveloped, inconsistently applied, or entirely absent.

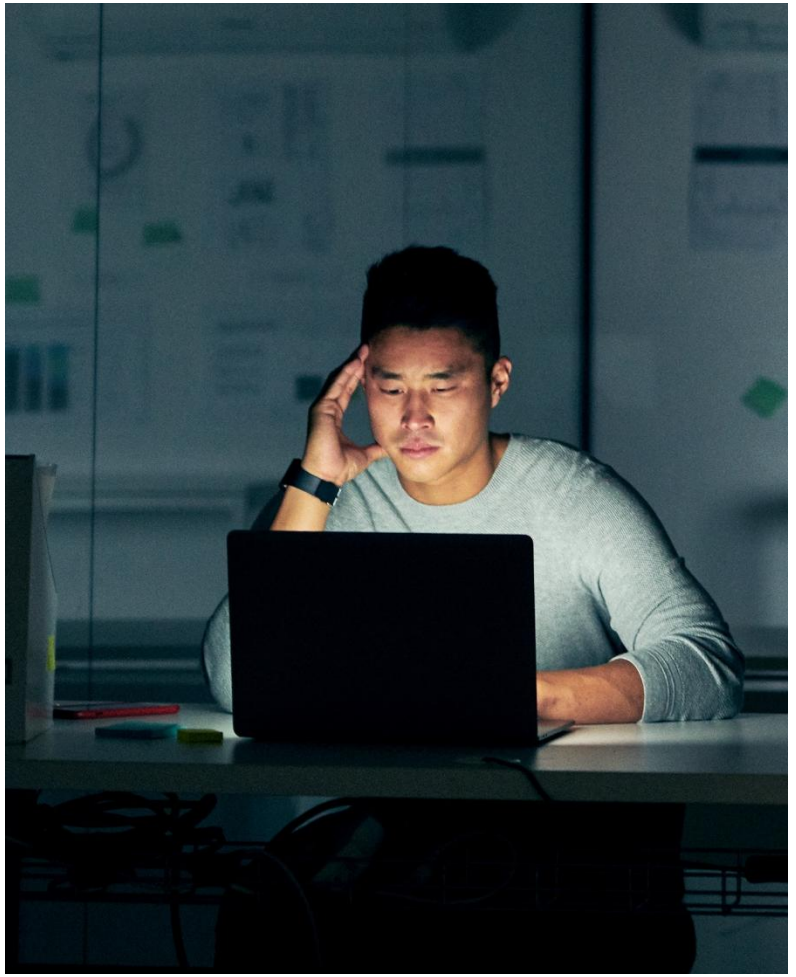
High-performing functions treat QAIP as a catalyst for continuous improvement rather than a compliance exercise. Leading teams escalate findings to the Board, track actions openly and link quality assurance outputs directly to capability development. It is important that quality assurance coverage extends beyond audit delivery into a wider universe, encompassing annual planning and risk assessment, stakeholder engagement, reporting and strategic initiatives. This broader approach ensures quality assurance insights drive continuous improvement rather than being confined to post-audit reviews. By contrast, common pitfalls include quality assessments that focuses too narrowly on audit execution, or varied maturity levels where no internal assessments are performed and no overall view of conformance is presented to the Board.

06

Performance objectives and effectiveness (Standards 9.2 and 16.1) – require the CAE to operate a performance measurement programme, with the Board approving Internal Audit's objectives annually.

The requirement for Internal Audit to set objectives is not new, but it is now made more explicit under the standards. CAEs are required to establish a performance measurement programme for the function, with the Board being responsible for approving Internal Audit's objectives annually and for assessing the function's effectiveness at least once a year.

We have seen leading functions align KPIs with the internal audit strategy, the internal audit mandate and the organisation's wider strategy, securing endorsement from both Senior Management and the Board. They are also adopting digital tools and data analytics to track KPI data dynamically through dashboards, providing real-time insights that support improvement programmes and enhance stakeholder reporting. This approach transforms performance management from a compliance exercise into a strategic enabler of functional growth and maturity.



Common challenges and first experiences of the new standards (4/4)

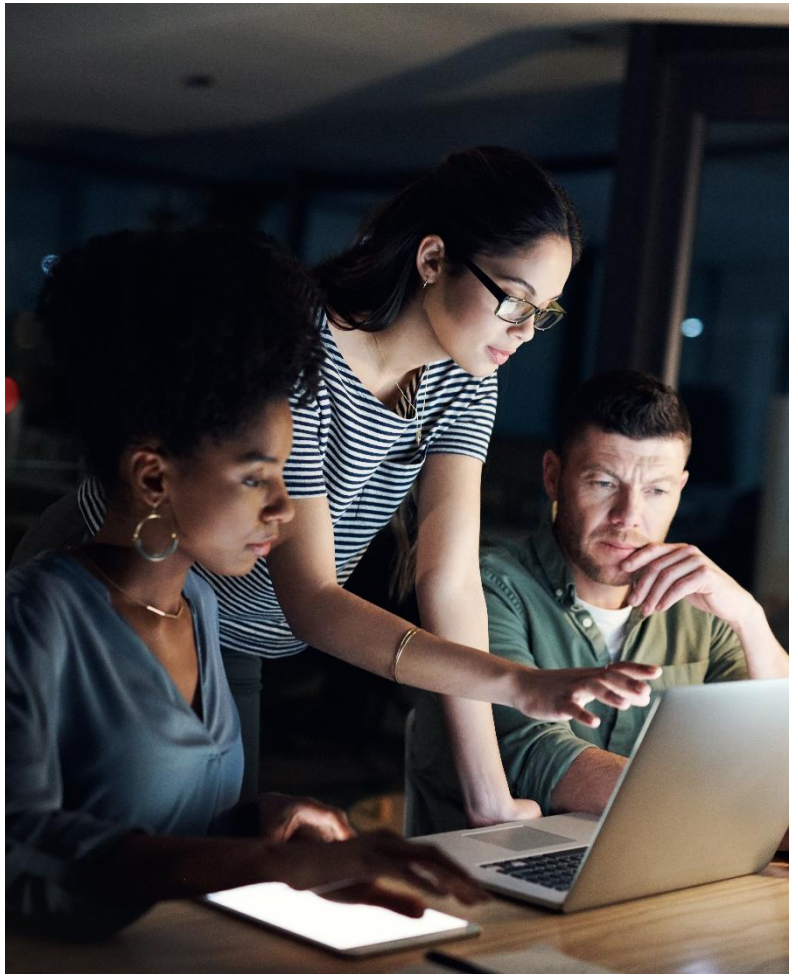
07

Coordinated assurance and reliance (Standards 10.2) – place emphasis on Internal Audit coordinating with other assurance providers to avoid duplication, identify gaps and present a holistic view of risks.

In practice, we continue to see challenges where many organisations lack a structured framework for coordinated assurance. This is often the result of varied levels of maturity across the three lines of defence, with risk and issue taxonomies that are misaligned, inconsistent documentation standards and fragmented reporting to the Board. The outcome is predictable: inefficiencies, duplication of effort and blind spots in assurance coverage.

By contrast, a number of mature and leading functions are embracing a more integrated approach. They are developing coordinated assurance maps and establishing governance forums with second-line functions to promote alignment. Common risk and control taxonomies are agreed, supported by integrated GRC systems. Roles and responsibilities are clear, and the extent to which reliance can be placed on other assurance providers is formally defined.

Proactive collaboration across the lines of defence enables a coordinated assurance framework and plan for the Audit Committee, giving clearer oversight of coverage and highlighting assurance gaps. By reducing duplication and coordinating requirements across an increasingly demanding regulatory landscape, organisations can ensure that assurance activity remains proportionate, efficient and focused on the risks that matter most.



Preparing for EQAs under the new standards (1/2)

Overview

Under the Global Internal Audit Standards, expectations of external quality assessments (EQAs) have been strengthened. While the minimum of five-year assessment cycle still applies, the new standards bring greater rigour, clearer accountability and stronger Board oversight.

The requirement for the Chief Audit Executive (CAE) to actively engage the Board in planning the EQA, including the method, timing and scope takes assessments beyond a box-ticking exercise and instead requires structured, strategic discussion with relevant stakeholders, including Senior Management.

The standards now also specify that the results of a full EQA must go directly to the Board, reinforcing accountability at the highest level. Another important change is the expectation around assessor qualifications: at least one member of the assessment team must hold an active Certified Internal Auditor (CIA) designation. This should be explicitly addressed when confirming the scope and appointment of the external assessor.

The IIA's Quality Assessment Manual and the four-point quality rating scale

The *Quality Assessment Manual*, updated in late 2024, sets out the IIA's expectations for evaluating Internal Audit functions. The most visible change is the introduction of a new four-point quality rating scale, replacing the former binary approach. The highest rating of **Fully Conforms** is now reserved for functions that not only meet the standards but also demonstrate maturity, impact and consistent performance.

Our point of view

This new model has sparked active debate. For example, what really differentiates "Fully Conforms" from "Generally Conforms"? Our view is that to achieve "Fully Conforms," a function must provide sufficient and appropriate evidence that each principle and Standard is fully met, in both design and intent, and that practices are consistently in place and working as expected. "Generally Conforms" recognises some differences against the standards, so long as the intent is still achieved. In practice, most functions will find "Fully Conforms" difficult to achieve in the early years, and group functions may face additional complexity when balancing local assessments against the group-level outcome.

It is important to emphasise that **not achieving "Fully Conforms" does not mean a function is ineffective**. Effectiveness should be measured by the extent of consistency, reliability and maturity demonstrated over time. Many Boards recognise the need to weigh the investment required to achieve full conformance against other priorities. For most Internal Audit functions, "Generally Conforms" will remain a credible and respected outcome, provided there is clear evidence that the intent of the standards is achieved and that the function demonstrates a commitment to continuous improvement.

Preparing for EQAs under the new standards (2/2)

What have we learned so far, and what should we expect next?

With only one year of implementation, adoption of the new standards is still in its early stages and the bar for conformance will continue to evolve as the profession gains experience. So far, we have observed three key takeaways:

- **Full conformance is possible but demanding**, requiring robust evidence and consistency across all standards.
- **Professional judgement is critical** and needs to be documented clearly and transparently. Decision logic should always be recorded and teams should be ready to explain and evidence, where applicable.
- **Maturity matters**, even if it is not rated, as it shapes the narrative of an EQA and demonstrates Internal Audit's impact beyond compliance. Functions can demonstrate maturity through evidence of continuous improvement under their QAIP, stakeholder engagement, innovation, adoption of technology and adaptability to business change.

Looking ahead, we expect greater clarity to emerge from the first wave of EQAs under the new standards, particularly on how assessors distinguish between "Fully Conforms" and "Generally Conforms," and how maturity narratives are received by Boards. For CAEs, the lesson is clear: treat EQAs not just as a compliance milestone, but as a strategic opportunity to demonstrate maturity, reinforce credibility, and demonstrate how Internal Audit is delivering value to the organisation.

Preparing for your next EQA

Based on our experience, Internal Audit functions preparing for an EQA should focus on the following:

- **Maintain governance oversight**: Engage the Board and Senior Management throughout to ensure alignment, visible oversight and conformance with the standards.
- **Define scope and requirements early**: Work with the Audit Committee Chair and stakeholders to agree the purpose, scope and timing of the EQA, including regional/ jurisdictional coverage, treatment of in-progress transformation or new tools and consideration of the IIA's Topical Requirements.
- **Complete a self-assessment**: Use the IIA's Quality Assessment Manual to benchmark against the standards, feed improvement actions into your QAIP, and communicate progress transparently to the Board.
- **Collate key documentation**: Ensure strategy, QAIP, audit plans, resourcing plans and budget, methodologies, and other core materials are ready for review.
- **Plan engagement activities**: Prepare for interviews with stakeholders (both Internal Audit and the business), document self-identified issues, and provide evidence of how they are being addressed.
- **Consider a maturity assessment**: While optional, maturity and peer benchmarking can add valuable insight and help shape the EQA narrative.

AI in internal audit (1/4)

Overview

Internal Audit functions are under increasing pressure to deliver broader assurance, sharper insights, and greater responsiveness to change. Traditional approaches built around cyclical reviews and sample testing are often too slow and narrow to match the pace at which risks now emerge. To remain relevant and impactful, Internal Audit must evolve its methodologies and toolset, expanding use of technology to enhance both efficiency and coverage.

AI in particular offers a step-change. Unlike earlier generations of automation, AI can read, reason, and generate outputs across vast datasets, enabling Internal Audit to expand its reach, accelerate reviews, and provide more tailored insights. This opens the door to more continuous, risk-weighted assurance, moving beyond retrospective testing to reflect how organisations operate today.

If used responsibly and strategically, AI can also strengthen Internal Audit's advisory role. By surfacing emerging risks such as cyber resilience and the governance of AI itself, functions can provide the Boards and Audit Committees with forward-looking insight while maintaining independence and rigour. This section explores how AI can be applied across the internal audit lifecycle and the practical steps needed to successfully embed AI into internal audit working practices.

Assurance in the loop: how AI is reshaping internal audit

AI reshapes assurance in two ways:

- First, Internal Audit must ***assure with AI***, applying AI capabilities across planning, fieldwork and reporting to widen coverage and shorten audit cycles.
- Second, Internal Audit must ***assure AI itself***, treating AI systems as a source of enterprise risk, applying proportionate, repeatable checks to validate how they behave and where accountability lies.

The result is a shift from periodic, sample-based testing to what we call **"assurance-in-the-loop"** routine: a risk-weighted evaluation that uses information the business already holds, including policies, activity logs, outcomes and incidents to provide earlier, clearer insight into how AI-enabled processes behave over time.

If done well, this expands Internal Audit's reach and the insights it can provide, raising the bar on coverage and timeliness, and moving from a conventional approach to an AI-driven one. At the same time, it reinforces Internal Audit's commitment to its core principles: evidence, independence, and professional judgement. The diagram on the right illustrates how an AI-driven approach could transform a conventional internal audit approach.

Conventional approach	AI-driven approach
Fixed rules	**Dynamic criteria**
Traditional automation followed fixed rules; AI adapts outputs based on context.	
Point-in-time snapshots	**Continuous evaluation**
Sample-based, point-in-time testing shifts to ongoing, risk-weighted insight-driven monitoring.	
Document extraction	**Rapid data synthesis**
Manual review of large volumes replaced by AI-assisted summarisation and gap-spotting.	

Tangible benefits to Internal Audit:

Increased coverage: Full populations tested, more scenarios examined, with stronger analysis, and linkage across control design and testing outcome.

Faster cycles: Shorter time from scoping to findings in document-heavy audits (e.g. compliance, governance).

Improved quality with consistency: First drafts that are consistent, well-sourced and tailored to each audience, minimising rework.

Earlier detection of anomalies: Detects shifts in behaviour or risks sooner, helping redirect audit effort to priority areas.

The next page features a case study showing how AI is transforming Internal Audit and delivering these benefits.

AI in internal audit (2/4)

Case study: From weeks to minutes – How AI reinvented reporting and follow-up

A global group piloted generative AI in its Internal Audit function to cut reporting time without compromising quality. Within the first cycle, drafting moved from weeks to days and follow-up shifted from reactive to predictive, while maintaining full traceability and human sign-off. The pilot established a repeatable approach that now supports assurance-in-the-loop across reporting and follow-up.

The challenge

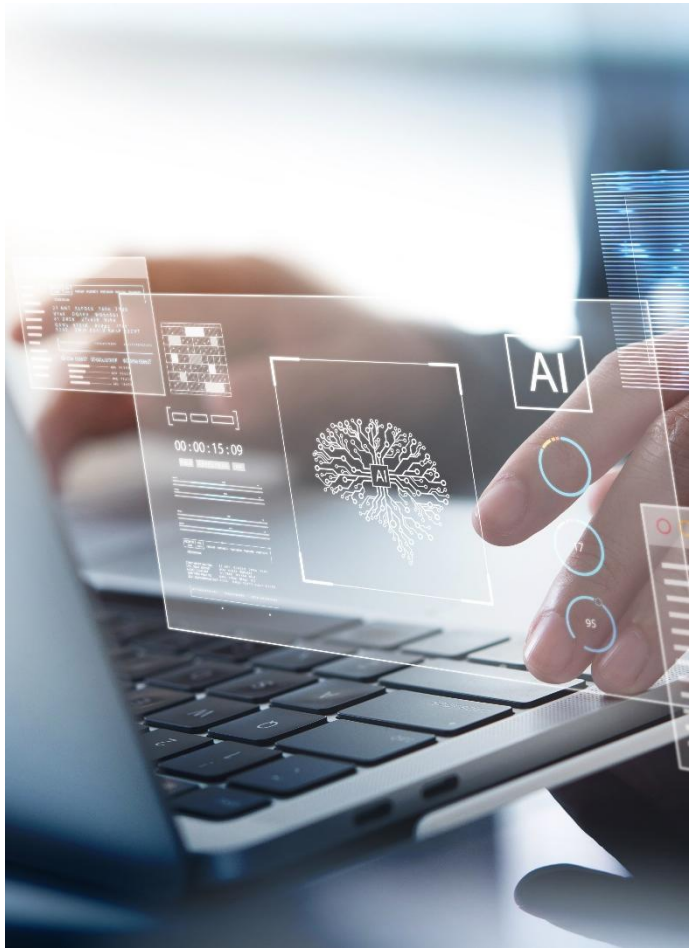
Audit teams were spending up to three weeks drafting reports after fieldwork. Walkthrough notes, meeting transcripts and evidence logs accumulated, and turning them into a clear narrative was slow and error-prone. Follow-up was largely reactive: overdue actions surfaced at quarter-end, leaving little time for remediation before Audit Committee meetings.

The AI-powered approach

- **Theme extraction at scale**. A secure, generative-AI workbench integrated with the audit platform processed more than 50 interview and walkthrough transcripts, clustering recurring issues such as 'access hygiene' and 'supplier Service Level Agreement (SLA) gaps'. These themes informed the executive summary and the Audit Committee narrative.
- **Two-minute drafts**. After fieldwork, auditors uploaded structured evidence and key observations. The tool produced a first draft in about two minutes, with well-articulated context, risk statements and suggested proportionate recommendations: each linked to the underlying evidence. A human reviewer validated the draft prior to issuance.
- **Predictive follow-up**. A machine-learning model analysed existing metadata (issue owner, complexity, IT dependencies) to flag actions likely to miss deadlines. At-risk items appeared on a dashboard, enabling earlier escalation and re-planning.

The impact

- Report cycle time reduced from 15 days to 3 days.
- Audit Committee packs added a concise 'risk of slippage' heatmap, improving oversight.
- Auditors reported higher engagement, spending more time on root-cause analysis and stakeholder discussion, and less on formatting.



AI in internal audit (3/4)

Given the breadth of the internal audit lifecycle, AI can be introduced to enhance consistency, speed, and coverage, while ensuring outputs remain fully traceable and reviewable. To achieve this responsibly, we group AI applications into an 'AI capability stack': a phased approach that enables auditors to adopt AI progressively and effectively. The stack has three capability layers: assistants, analysts, and agents. The following section explains each layer and provides use cases to illustrate how AI can reinvent conventional internal audit approaches.

I. **Assistants:** help auditors work faster by securely searching approved information and drafting materials with clear references.

Use cases

- **Policy recall:** Retrieve exact passages from approved regulatory/policy libraries in response to queries (e.g. "What are GDPR's requirements on data retention?").
- **Automated drafting:** Generate first drafts of scoping documents or audit reports from historic templates.
- **Meeting prep**: Compile summaries of prior findings, management actions, and relevant standards before walkthroughs.
- **Evidence collation**: Convert interview notes into structured first drafts of control descriptions or process narratives.

II. **Analysts:** support structured analysis by guiding auditors through scoping, testing, and reporting in line with methodology, making work more consistent and reliable.

Use cases

- **Scoping and risk assessment**: Prompt auditors with plain-language questions (e.g. "What decisions does this tool influence? What happens if it fails?") and structure responses into a risk framework.
- **Testing workflows**: Provide structured test scripts for areas like payroll processing, supplier onboarding, or IT change management.
- **Issue trend analysis**: Identify recurring issues or weak themes by analysing historic audit findings (e.g. procurement delays, repeated HR compliance gaps).
- **Consistency checks:** Benchmark sampled files (e.g. employee expenses, supplier contracts) against thresholds or industry practice for proportionality

III. **Agents:** carry out standard tasks or tests on approved data automatically, recording every step so results can be repeated and reviewed with confidence..

Use cases

- **Data accuracy testing:** Run reconciliations of HR, finance or inventory records against source systems, flagging missing fields or inconsistencies.
- **Transaction monitoring:** Replay test scenarios for procurement approvals or health & safety incident logging, checking whether thresholds, escalations and audit trails match policy.
- **Access control checks:** Continuously test joiner–mover–leaver data against HR records to detect access exceptions.
- **Model validation:** Run scripts against AI/ML tools in use (e.g. credit scoring, demand forecasting), capturing inputs/outputs to create a repeatable evidence pack.
- **Third-party assurance:** Automate periodic checks on outsourced service provider data (e.g. payroll, logistics, IT support), flag whether reconciliations were complete and within SLA.

AI in internal audit (4/4)

Bringing it all together

Having considered how AI can support auditors responsibly and where capabilities can be embedded, it is equally important to recognise that people, processes, technology, and culture must evolve together. To manage this effectively, Internal Audit should assess maturity on two dimensions: (i) the organisation's maturity in deploying and governing AI, and (ii) Internal Audit's maturity in assuring it. These will not always progress in parallel.

An organisation may be advanced in AI adoption while Internal Audit is still building baseline literacy, or Internal Audit may mature its assurance methods ahead of enterprise deployment. Balancing both dimensions is critical to setting the right pace, skills, and safeguards. The following brings this to life through the four areas of consideration: people, process, technology, and culture, together with an illustrative roadmap for AI adoption, which outline how Internal Audit can build capability progressively while maintaining trust and independence.

People: Building skills and defining roles

- All auditors should build baseline literacy in AI: what it can and cannot do, and how to interpret AI-related evidence.
- Selected staff need deeper expertise in evaluation design, data fluency and model risk.
- New roles may emerge, such as assurance engineers (designing test packs), internal audit AI product owners (governing audit tools) and AI evaluation leads (defining thresholds and quality checks).

Technology: Phased and responsible adoption

- Start with Assistants (secure search and drafting over approved sources).
- Progress to Analysts (guided workflows for scoping, testing and reporting).
- Mature into Agents (controlled automations that run standard test packs with repeatable results).
- The above phased path allows Internal Audit to learn quickly, prove value, then automate safely.

Process: Methods that safeguard quality

- Standardise scoping prompts when AI is in scope: purpose, data used, decisions influenced, expected controls, monitoring.
- Update methodology and workpapers to include an 'AI Evidence' page for any AI-assisted step.
- Build proportionate retention rules and link AI expectations into supplier management.

Culture: Putting independence and judgement first

- Human sign-off remains essential: AI supports coverage and speed, not final decision-making.
- Apply a learning loop: use review notes and rework to refine prompts, sources and test packs.
- Safeguard confidentiality by keeping sensitive data within approved environments.

Illustrative roadmap for adopting AI in Internal Audit:

0–3 months: Prepare and prove value

Pilot 3 or 4 AI use cases in Internal Audit; adopt an evidence approach; set core metrics.

3–12 months: Standardise and scale

Publish an Internal Audit AI playbook; train teams; standardise workflows; include AI in supplier reviews.

12–24 months: Embed assurance in the loop

Establish routine, risk-weighted evaluation; adopt controlled automations; refresh the audit universe to reflect AI-driven change.

5

Glossary

- Glossary of acronyms and abbreviations

Glossary of acronyms and abbreviations (1/2)

AI	Artificial intelligence
AML	Anti-money laundering
BAU	Business as usual
BCM	Business continuity management
CAE	Chief Audit Executive
CAO	Capital Adequacy Ordinance
CET1	Common equity Tier 1
CPE	Continuing professional education
CRQC	Cryptographically relevant quantum computer
DORA	Digital Operational Resilience Act
EQA	External quality assessment
ERM	Enterprise risk management
ESG	Environment, social and governance
EU	European Union
FCA	Financial Conduct Authority (UK)
FS	Financial services
GDP	Gross domestic product
GDPR	General Data Protection Regulation
GIAS	Global Internal Audit Standards
GRC	Governance, risk management and compliance
IAM	Identity and access management
ICT	Information and communication technology
IIA	The Institute of Internal Auditors
ISO	Insurance Supervision Ordinance
KPIs	Key performance indicators
KRIs	Key risk indicators

Glossary of acronyms and abbreviations (2/2)

KYC	Know your customer
LoLR	Lender of last resort
ML	Machine learning
MROS	Money Laundering Reporting Office, Switzerland
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology, United States
PLB	Public liquidity backstop
PQC	Post quantum cryptography
PRA	Prudential Regulation Authority (UK)
QAIP	Quality assurance and improvement programme
QKD	Quantum key distribution
SBA	Swiss Bankers Association
SIBs	Systemically important banks
SLA	Service level agreement
TLS	Transport layer security
TPRM	Third-party risk management
UK	United Kingdom
US	United States
VPN	Virtual private network

Contact us

If you have any questions on any of the topics in this document or would like a planning session, please reach out to your relationship contact or one of the following:

Alexandra Burns

FS Risk, Compliance & Internal Audit
Partner

+41 79 878 31 69
alexandra.burns@pwc.ch

Fabienne Wikler

Risk Consulting
Director

+41 78 666 97 79
fabienne.wikler@pwc.ch

Jürgen Supersaxo

Internal Audit FS Leader
Director

+41 79 507 15 32
juergen.supersaxo@pwc.ch

Beate Fessler

Risk Consulting
Director

+41 79 783 59 10
beate.fessler@pwc.ch

Selma Della Santina

Financial Crime Compliance
Director

+41 79 109 22 49
selma.della.santina@pwc.ch

Luca Bonato

Compliance & Regulation
Director

+41 79 334 68 31
luca.bonato@pwc.ch

Thank you

pwc.ch