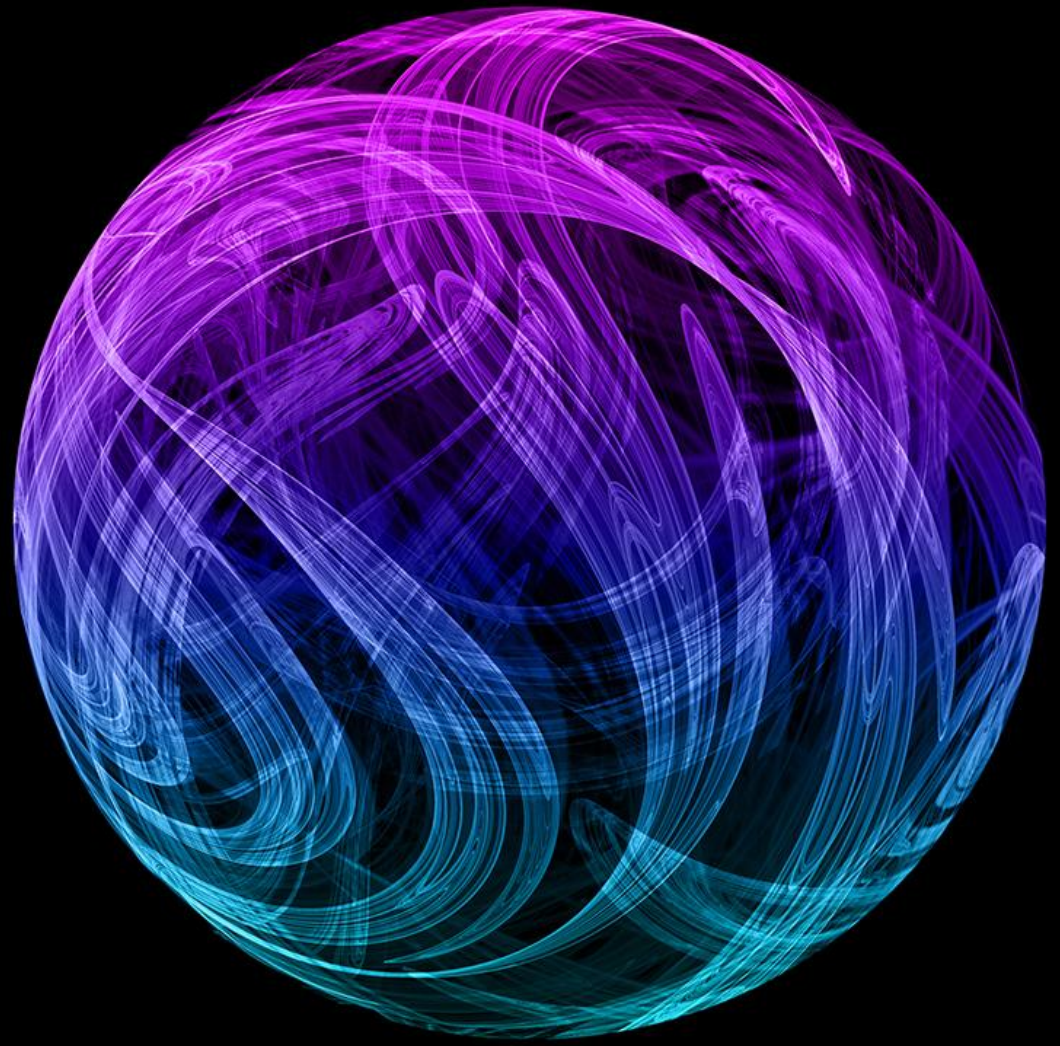
Deloitte.



Financial services

Internal audit planning priorities 2026

Navigate uncertainty: future-proofing financial services

Executive summary

The financial services landscape has been set amid a backdrop of ongoing uncertainty and global disruptions. For financial services organisations, staying resilient in this environment is more important than ever. Two emerging areas are to be considered as firms prepare for the future, both near- and far-term. These include geopolitical risk and GenAI adoption.

The nature of geopolitical risk is complex and intertwined with all other risk areas affecting financial services. For internal audit to effectively leverage its unique position, a broad understanding of how potential geopolitical events will impact individual risk profiles with their organisation is key. This holistic view enables internal audit to provide more insightful and strategic guidance in navigating the evolving geopolitical risk landscape.

The growing adoption and normalisation of emerging technologies at all levels of business and society demonstrate how technology is transforming into an environment we inhabit, not just a tool to access. As GenAI becomes further deployed, while the rapidly evolving area of agentic AI materialises, responsible use of technology is paramount to achieve productive growth for the future. What's more, the speed of regulation building around GenAI may drive risk functions to seek more support for technology-related assurance. The increased efficiency gained from integrating Generative AI into internal audit will necessitate an evolving role for the internal audit profession, requiring enhanced strategic evaluation skills. For instance, if real-time reporting is rolled out in the future, the role of the internal audit personnel, department and skillset will need to be prepared for a transformed operation.

Meanwhile, the changing regulatory landscape is driving an overhaul in both organisations and populations globally. Differences in regulatory progress across geographies have created divergent environments for growth and global competitiveness. For internal audit professionals, emerging regulation could suggest new specialisms in the internal audit discipline as workflows and reporting mechanisms could be affected by regulation and/or deregulation.

Alexandre Buga
Partner
E: abuga@deloitte.ch

Nadejda Groubnik
Partner
E: ngroubnik@deloitte.ch

Corina Ruchti
Director
E: cruchti@deloitte.ch

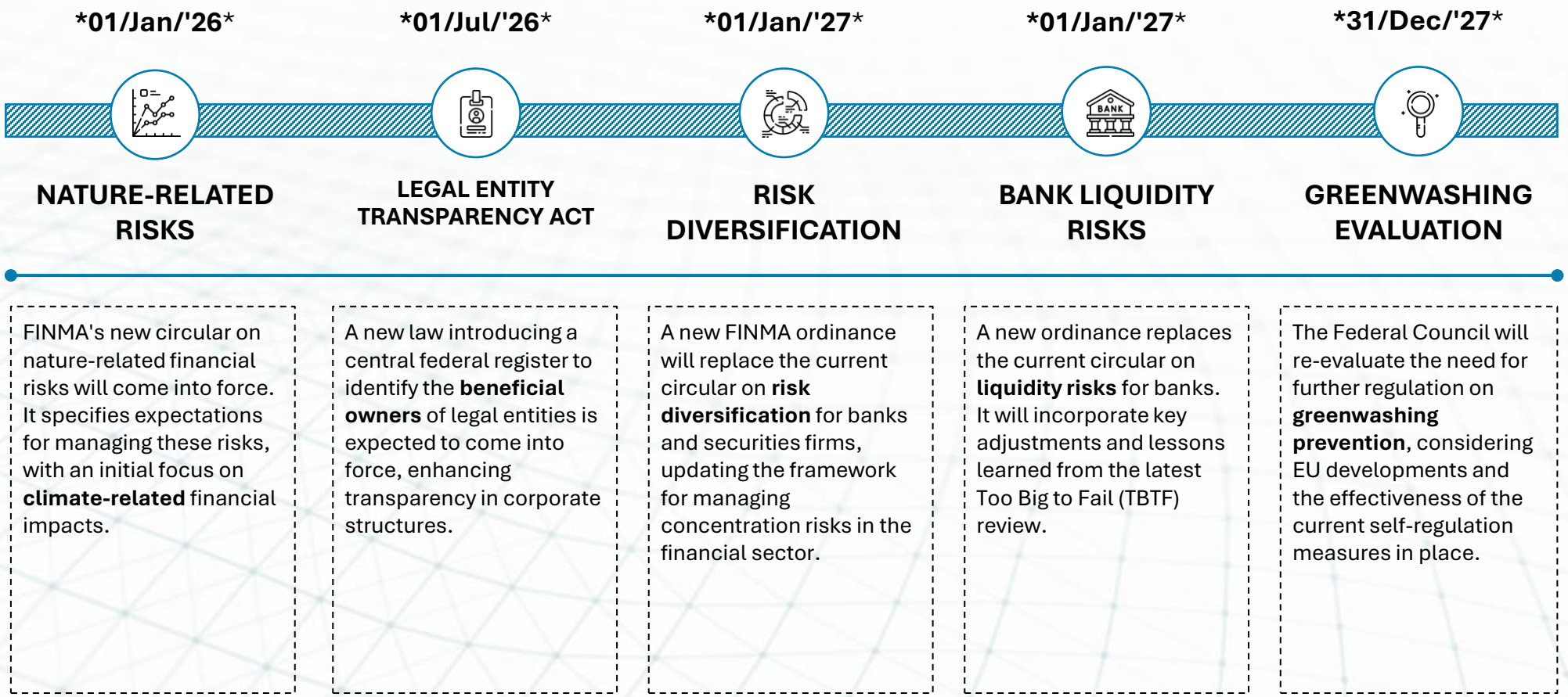
Sandro Schönenberger
Partner
E: sschoenenberger@deloitte.ch

Denise Wipf
Partner
E: dwipf@deloitte.ch

Christian Jung
Director
E: cjung@deloitte.ch

Regulatory overview 2026 and 2027

This timeline provides a strategic overview of key regulatory changes impacting the Swiss financial sector in 2026 and 2027. It highlights significant upcoming projects, offering a crucial at-a-glance reference for compliance planning and strategic adaptation. The upcoming regulations will introduce new requirements for risk management, transparency, and reporting, shaping the operational landscape for financial institutions.



Financial services planning priorities topics overview

Emerging risks	Payments and financial crime	Prudential and credit risk	Technology and operations	Governance	Environmental, social and governance	Insurance specifics	Internal audit innovation and transformation
Geopolitical risk	Swiss payments modernization initiatives	Model risk management	Change and transformation	Governance regime	Nature-related financial risks	ISO and ISA changes	GenAI across IA lifecycle
Responsible adoption of GenAI	Financial crime	Credit risk	Operational resilience	Risk culture		Liquidity insurers	Data analytics
	Digital assets		Third party risk management				High performing internal audit function
			Cyber				Standards and QA hotspots
			Data governance				
			Cloud				

- Cross sector
- Banking and capital markets
- Insurance

Sections

Click on each section to navigate through the report and use the home button on the right to return to this page.

01

Cross sector and emerging risks

02

Banking and capital markets

03

Insurance

Key contacts

Cross sector and emerging risks

Emerging risks

Geopolitical risk

Geopolitical risk is paramount in today's volatile global environment. 2025 has delivered many material and unpredictable developments in the world's political and economic landscape. Financial services firms must proactively respond to disruption and external shocks, building resilience by identifying and assessing these risks as part of broader risk management and resilience frameworks. This includes considering the interconnected nature of geopolitical risks and their potential systemic impact.

Internal audit can play a vital role by providing a valuable independent assessment of firms' geopolitical risk management, both at the firmwide level and by evaluating sensitivity to and mitigation of firm-specific risks.

Unlocking internal audit's potential: A strategic lens on geopolitical resilience

- Internal audit is increasingly expected to contribute to the development of a firm's strategy and resilience. With its independence, broad reach and unrestricted access, internal audit is uniquely positioned to provide the Board, senior management, and regulators with critical assessments of a firm's geopolitical resilience.

The geopolitical jigsaw: Connecting the dots for enhanced risk management

- Geopolitical risk is not new, but its impact is intensifying. The interconnected nature of geopolitical risk demands a more focused and proactive approach from internal audit.
- The European Banking Authority (EBA) and FINMA identify geopolitical risk as a significant concern for the financial markets and highlight the need for banks to incorporate geopolitical risk into their business strategies and risk management practices.
- Geopolitical risks are increasingly acting as drivers of traditional and emerging risks (it has been featured in over 50% of topics in this publication). Both global and domestic firms face direct and indirect impacts, including:
  - **Financial risks:** Increased credit risk due to deteriorating asset quality, heightened market volatility impacting liquidity and funding, and tariffs disrupting supply chains and tax strategies. Insurers offering political risk, cyber or business interruption insurance face the risk of increasing claims against those policies.
  - **Non-financial risks:** Strategic shifts requiring rapid market exits, operational disruptions from supply chain vulnerabilities and cyberattacks, reputational damage from operating in volatile regions and changing landscape around trade restrictions and sanction compliance regime.

Emerging risks

Geopolitical risk

This interconnectedness raises critical questions for internal audit functions. How can internal audit functions effectively assess and mitigate these interconnected risks?

1. **How can internal audit stay ahead of the curve?**
   - **Maintaining awareness** of geopolitical events impacting the business requires a multi-faceted approach. There's no single definitive source; instead, a combination of news sources, thought leadership, expert networks, and collaboration with economics, compliance, and risk functions is essential for staying informed about evolving market dynamics.

2. **Dynamic risk assessment: adapting internal audit to the pace of change:**
   - Developing a robust strategy to tackle geopolitical risk requires a **shift in mindset**, moving from static planning to dynamic risk assessment. This agility is crucial, as geopolitical risks can emerge and escalate far faster than traditional audit cycles allow.
   - Internal audit's role is not to predict the future, but to assess how well governance, risk management and controls are designed and operating to mitigate the potential impact of geopolitical risks - **a forward-looking lens**, anticipating the potential impact of geopolitical events on various risks, is essential in today's volatile environment.
   - While existing audit plans may adequately cover high-risk areas, the impact of geopolitical events on lower-risk and less frequently audited areas demands increased attention. Internal audit must also consider how **these events can reshape the risk landscape**, for example, rapidly rising inflation driven by geopolitical tensions can exacerbate interest rate risk.
   - **Integrating geopolitical risk assessment** into relevant audit planning discussions with stakeholders is paramount. Breaking down silos and fostering collaboration within the internal audit function (e.g. to address business, regulatory and technology risk) is no longer a best practice—**it is a necessity**. This collaborative approach enables a more comprehensive understanding of the evolving geopolitical risk landscape.

3. **Collaboration across the three lines of defence:**
   - Clear communication channels and defined ownership are essential for **sharing critical information** about geopolitical risks and coordinating responses across the first, second, and third lines of defence. Regulators may demand swift responses to emerging geopolitical events, requiring firms to have a **dedicated, cross-functional response team** ready to act.
   - A successful integrated assurance approach, uniting the perspectives and expertise of all three lines, is essential for navigating the complexities of geopolitical risk.

4. **Focus on existing coverage of horizon scanning, stress testing and resilience:**
   - Internal audit should assess the firm's current **horizon scanning process**, ensuring timely insights from risk owners across the organisation. As part of audit coverage, it is important to ensure current stress testing and scenario analysis are effective and that underlying models are challenged and refined, using lessons learned from the past events.
   - **Geopolitical risk and business resilience** should be viewed with the same end goal in mind. Operational resilience and broader technology resilience requires firms to understand their key resources and critical third parties required to deliver services to their customers.

5. **Data Driven insights**
   - Timely and accurate risk data is crucial yet often difficult to obtain. Internal audit should understand how existing data challenges might impact relevant risk reporting, and assess data reliability, system adequacy, and reporting processes. These aspects provide the basis of effective MI for informed decision-making in a dynamic geopolitical landscape.

6. **Internal audit's commentary of geopolitical risk:**
   - As part of internal audit's annual conclusion on risk management framework and periodic audit committee reporting, internal audit should highlight the geopolitical factors that affect key areas of the risk management framework.

Emerging risks

Responsible adoption of GenAI

Generative artificial intelligence (GenAI) continues to prove a strong driver for transformation within the financial services industry, unlocking significant value across the front, middle and back-office value chains.

First-to-market, innovation mindsets are now tempered with concern for risk; 30% of respondents to Deloitte's latest State of GenAI in the Enterprise survey indicated difficulty in managing AI risk as a barrier to its adoption, as a reminder of the importance of responsible governance and risk management to supporting safe and scalable adoption.

The evolving global regulatory landscape increasingly places an importance on and expectation for practices and structures that promote the responsible development and deployment of AI. The EU's AI Act to AI regulation emphasises risk management, transparency, and data protection, particularly concerning AI's potential for harm. FINMA's Guidance 08/2024 on Governance and Risk Management for AI further reinforces these expectations for Swiss financial institutions.

Five things you should know about the topic :

- **Expanded Audit Scope and AI Governance:** GenAI significantly broadens the audit universe. Internal audit must assess not only AI outputs but also the underlying algorithms, data sources, and training processes for bias, accuracy, and security vulnerabilities. FINMA expects institutions to maintain a centralised AI inventory with risk classification, clear assignment of responsibilities, and robust governance covering development, implementation, and monitoring of AI applications.
- **Data privacy, security and quality controls:** GenAI's reliance on large datasets raises critical data privacy and security concerns. Internal audit must ensure compliance with regulations such as FADP and GDPR, verifying that data handling meets stringent standards. FINMA further requires institutions to define and enforce data quality controls ensuring data completeness, accuracy, integrity, and bias mitigation, recognising that data quality is often more impactful than model choice.
- **Explainability and transparency challenges:** Many GenAI models operate as "black boxes," complicating audit assessment of reliability and fairness. FINMA highlights the importance of explainability, expecting institutions to understand and document AI decision drivers, enabling justification of outcomes to clients, regulators, and auditors.
- **Emerging regulatory landscape:** Regulatory frameworks globally vary in scope and scrutiny, requiring agile governance and compliance. FINMA's principle-based, technology-neutral guidance expects institutions to actively consider AI's impact on their risk profile and align governance and risk management, accordingly, including managing operational, model, IT, cyber, legal, and reputational risks.
- **Impact on internal controls:** While GenAI can automate control processes, it also introduces new risks related to data integrity, access control, and potential misuse. FINMA requires institutions to implement rigorous testing and ongoing monitoring of AI models for accuracy, robustness, stability, and bias, including detection of data drift and analysis of manual overrides as indicators of model weaknesses.

Five things internal audit should do:

1. **Develop AI audit expertise**

   Internal audit teams need to acquire the necessary skills and knowledge to effectively audit GenAI systems. This includes training on data science techniques, AI model validation methods, and the regulatory landscape surrounding AI.

2. **Assess data privacy and security controls**

   Audit the effectiveness of data governance policies ensuring data completeness, accuracy, integrity, and bias mitigation. Confirm compliance with data privacy regulations such as FADP and GDPR, and assess controls over data sourcing, handling, and protection within AI systems.

3. **Verify explainability and documentation practices**

   Ensure AI models and their decision-making processes are sufficiently explainable and documented. Review whether documentation covers AI purpose, data inputs, assumptions, limitations, and fallback mechanisms, enabling transparency for stakeholders including regulators and auditors.

4. **Monitor regulatory developments**

   Evaluate how the organisation identifies and manages AI-related risks—including operational, model, IT, cyber, legal, and reputational risks—ensuring alignment with FINMA's principle-based, technology-neutral guidance and evolving regulatory landscape.

5. **Test and monitor AI model performance and controls**

   Confirm that AI applications undergo regular, rigorous testing for accuracy, robustness, stability, and bias. Assess ongoing monitoring processes for data drift, model degradation, and manual overrides, ensuring timely detection and remediation of risks introduced by AI systems.

Payments and financial crime

Financial crime

The continuing evolution of financial crime typologies, coupled with a rapidly changing geopolitical environment, presents significant compliance challenges for organisations to remain resilient. These include responding to the evolving sanctions landscape, responsible integration of generative AI (GenAI) into operations, and leveraging industry lessons in risk assessment frameworks. Internal audit functions should proactively assess these areas to support their organisations in enhancing their effectiveness in combating financial crime, safeguarding organisational integrity, and fostering stakeholder trust. In 2026 and beyond, these priorities will be paramount in maintaining a strong defence against increasingly sophisticated criminal activity.

Given the significant financial crime fines issued recently, strengthening anti-financial crime controls and compliance programmes should be a high priority on the Board's agenda.

Six things you should know about the topic:

- **Robust financial crime enterprise-wide risk assessments (EWRA):** Strong EWRAs are vital for identifying and mitigating evolving threats. Regularly assessing risk identification, measurement, and mitigation strategies is essential, considering emerging risks, guidance, and industry insights.
- **Sanctions compliance:** Agile compliance systems are essential for navigating the evolving sanctions landscape. Effective and adaptable sanctions screening is crucial for mitigating breach risks amidst new designations and regulatory updates.
- **Financial crime target operating model:** A robust operating model is the backbone of effective risk management. Integration of new technologies and data sources into operating models ensure they remain adaptable to the changing regulatory landscape and industry good practice.
- **Responsible GenAI and Machine Learning (ML) integration:** GenAI and ML offer potential but require careful governance. Model validation, bias detection, and explainability are crucial for responsible compliance integration, ensuring human oversight and thoughtful assurance of outputs.
- **Enhanced financial crime monitoring:** Addressing data inconsistencies and fragmentation within internal audit's independent assessments is critical. Data analytics can be utilised to identify patterns and anomalies across disparate sources, improving detection and reporting.
- **Legal Entity Transparency Act (LETA):** Expected to enter into force in 2026, the aim is to reinforce the integrity and competitiveness of Switzerland as a financial and business location by means of a federal register of beneficial owners and due diligence for particularly risky activities in legal professions, as well as other provisions. Failure to comply can lead to significant fines. LETA complements FINMA's broader expectations on beneficial ownership verification under AMLO-FINMA and supports Switzerland's implementation of FATF recommendations.

Five things internal audit should do:

1. **Robust risk assessments**

   Critically evaluate the robustness and accuracy of EWRAs, ensuring alignment with regulatory guidance and emerging risks. Focus on the effectiveness of risk mitigation strategies and the integration of risk assessments into decision-making and governance processes.

2. **Deep dive into sanctions compliance**

   Whilst it is important to continue to assess the "basics" in the context of sanctions compliance, internal audit functions should also consider implementing data analytics and scenario-based testing to evaluate the effectiveness of sanctions controls against evolving typologies and evasion techniques.

3. **Holistic assessment of the financial crime target operating model**

   Assess the alignment of the financial crime target operating model with relevant regulatory expectations, industry good practice, the organisation's risk appetite and Consumer Duty principles, recommending opportunities for efficiency such as streamlining processes and leveraging technology where appropriate. This should include evaluating whether the firm's financial crime controls adequately protect vulnerable consumers.

4. **GenAI and ML governance**

   As businesses continue to adopt GenAI and ML, internal audit should consider the robustness of the governance frameworks around such models, with a focus on ethics, data privacy, model validation, and ongoing monitoring.

5. **Data integrity and consistency**

   Focused testing on data quality, data lineage, consistency, and completeness, including assessing whether the organisation is making the most of potential data sharing opportunities across functions.

6. **Prepare for LETA implementation**

   Verify that the institution's readiness and remediation plans align with upcoming LETA provisions, including beneficial-ownership transparency and integration into KYC processes.

Payments and financial crime

Digital assets

The accelerating growth of digital assets as an asset class presents both significant opportunities and heightened risks. The increased regulatory scrutiny and inherent complexities associated with digital assets demand robust internal audit oversight. We encourage a proactive and risk-based approach to planning and ensuring alignment with the organisation's overall strategic objectives and risk appetite.

Five things you should know about the topic:

- **Evolving digital asset landscape**: The digital asset landscape is evolving, with notable growth being seen in stablecoins, tokenisation of real-world assets (RWA) and decentralised finance (DeFi), alongside the continuous growth of cryptocurrencies.
- **Global regulatory developments**: From a global perspective, the US's approval of Bitcoin and Ethereum ETFs, alongside a more collaborative stance between regulatory agencies and the introduction of targeted legislation (GENIUS Act for stablecoins), signals a move towards an increasingly defined regulatory framework. This shift marks a departure from the previous emphasis on enforcement actions and offers greater clarity for businesses. Across the Asia-Pacific region, jurisdictions like Singapore and Hong Kong are establishing themselves as digital asset hubs by implementing licensing regimes for Virtual Asset Service Providers (VASP) and strengthening consumer protections, including restrictions on retail access and enhanced disclosures.
- **The Swiss's crypto-asset regulatory framework**: Switzerland has established itself as a leader in digital asset regulation, with a comprehensive framework that supports innovation while ensuring consumer protection. The Swiss Financial Market Supervisory Authority (FINMA) has implemented clear guidelines for Initial Coin Offerings (ICOs) and digital asset trading platforms, emphasizing transparency and compliance. Switzerland's regulatory approach fosters a balanced environment that encourages growth in the digital asset sector while maintaining robust oversight.
- **New license ahead:** In October 2025, the Federal Council opened a consultation on an amendment to the Financial Institutions Act. Against this background two new licensing categories are being proposed. Payment instrument institutions (replacing the existing fintech license; will be allowed to issue a special type of stablecoin) and Crypto-institutions (designed to provide various services with cryptocurrencies; with licensing and operating criteria based on those for securities firms but less comprehensive; they will have to meet certain requirements to prevent conflicts of interest).
- **Data integrity challenges**: Immature frameworks could raise significant data independence concerns, increasing the risk of misreporting, fraud, and regulatory breaches. This can lead to vulnerabilities in areas such as data governance, access control, and transaction processing.
- **Managing conflicts of interest in the digital asset sector**: Failures to manage conflicts of interest in the digital asset sector have led to significant customer losses and market instability. Previous high-profile collapses, such as that of Futures Exchange (FTX), in the sector have underscored the tangible consequences of inadequate conflict management, highlighting the importance of clear governance, segregation of duties, and independent oversight.

Five things internal audit should do:

1. **Regulatory compliance internal audit review**

   Conduct a thorough review of the firm's compliance with the evolving regulatory framework for digital assets. Assess the adequacy of controls designed to mitigate the risk of non-compliance where the firm is already offering products and services to clients.

2. **Data reconciliation and integrity**

   Evaluate the effectiveness of data reconciliation processes, focusing on the independence and integrity of data sources. This evaluation should specifically address reconciliation of key data types, including transaction data wallet balances, custody records, and client account information. Identify and remediate any gaps or weaknesses in existing controls to mitigate the risks of misreporting, fraud, and regulatory breaches, including recommendations for strengthening data governance and control frameworks.

3. **Conflicts of interest assessment**

   Consider performing a comprehensive assessment of the firm's conflicts of interest framework and controls, paying particular attention to the interaction between trading, custody, and other business lines. The goal is to identify and mitigate potential conflicts proactively, ensuring robust and effective mitigation strategies are in place.

4. **Global best practice benchmarking**

   Benchmark the firm's digital asset risk management practices against market standards and regulatory expectations, including horizon scanning to identify emerging best practices and regulatory trends.

5. **Technology and operational resilience**

   Internal audit should conduct a thorough assessment of the firm's technology infrastructure and its ability to support digital asset operations. Identify vulnerabilities and recommend appropriate mitigation strategies to enhance operational resilience against potential disruptions, including an evaluation of the team's technical expertise and a plan to address any gaps.

Prudential and credit risk

Model risk management

Boards and regulators are maintaining their focus on model risk management (MRM) in the face of increasing adoption of models across all business functions. Firms are needing to adapt and expand their risk management framework and capability in order to meet this evolving challenge.

Five things you should know about the topic:

- **Broadening definition of model**: Model risk remains a key area of focus for regulators, who increasingly expect it to be managed as a risk discipline in its own right. The definition of "model" has broadened, encompassing a wider range of tools and techniques, including AI/ML models.
- **Model development:** Model risk is about more than just the model being 'wrong'; it also encompasses risks (and controls) around its development lifecycle, how models are implemented into live systems and their use across the business for decision making.
- **Global regulatory focus:** In Switzerland, MRM is gaining increasing regulatory attention as part of FINMA's broader supervisory expectations on risk governance, data quality, and model validation under circular 23/1. FINMA expects banks and insurers to ensure that models used for credit, market, liquidity, and operational risk — including AI- and ML-based models — are independently validated, documented, and regularly back-tested. This aligns with evolving international standards set by the ECB, PRA, and US regulators, which increasingly view MRM as a core component of operational resilience and prudential soundness. Swiss institutions operating cross-border are expected to harmonise their MRM practices with international developments while maintaining compliance with Swiss supervisory principles on governance, accountability, and data integrity.
- **Vendor vs. in-house:** Vendor-provided models are emerging as an area of weakness for many firms, where governance and attention have historically been light, but transparency in these models is low and the risks are just as significant as in-house developed models.
- **GenAI acceleration:** Finally, the widespread introduction of Generative AI (GenAI) models is driving a major change in how model risk is perceived and managed. These models have unique features and risk profiles compared to conventional models, which necessitate a joined-up approach across risk and technology functions.

Five things internal audit should do:

1. **MRM for financial and regulatory reporting**

   Internal audit should assess whether model risk management (MRM) controls for models used in financial, regulatory, and risk reporting comply with FINMA expectations on data integrity and governance. This includes verifying that models feeding into IFRS, capital adequacy (Basel III/IV), and liquidity metrics are validated, traceable, and appropriately approved by management committees.

2. **MRM framework design and governance**

   Audit the overall design of the MRM framework, including model inventory completeness, classification, and roles and responsibilities. Internal audit should confirm that governance aligns with FINMA circular 23/1 and that ownership, documentation, and escalation processes are clearly defined and periodically reviewed.

3. **Emerging model risks incl. AI and vendor models**

   Evaluate how the institution identifies and manages risks from AI-based, machine-learning, and third-party (vendor) models. Internal audit should review whether independent validation and explainability requirements are proportionate to the model's complexity and criticality, and whether related controls (data quality, bias testing, change management) are embedded.

4. **Review independence and capability of model validation**

   Assess whether the model validation function operates independently from model owners, has adequate skills, and applies a proportional risk-based validation framework. Internal audit should also challenge the adequacy of model performance monitoring and back-testing across all risk categories.

5. **Strengthen links between MRM and operational resilience**

   Internal audit should verify that MRM processes support operational resilience by ensuring model continuity, documentation, and data recoverability for critical models. Reviews should confirm that model dependencies on data, ICT, or outsourced providers are identified and governed under FINMA's operational-risk and outsourcing expectations (RS 23/1 / RS 18/3).

Technology and operations

Change and transformation

The global financial services sector is experiencing a market evolution, driven by the rapid adoption of GenAI solutions and a surge in market consolidations and reorganisation particularly within the insurance and banking sectors. Furthermore, ongoing geopolitical uncertainties have introduced considerable volatility into global markets, increasing risk profile, impacting investor confidence and forcing Boards to refocus investment on short term and defensive capabilities.

Internal audit functions should continue to challenge the change strategy, focusing on the effectiveness of return on investment and cost reduction for major changes, strategic alignment of change objectives during transition to BAU and the integration of GenAI technologies.

Five things you should know about the topic:

- **Ensuring success – a cost-effective approach to change management:** Uncertainty in the markets (and related revenue-generating opportunities) leads a business to focus on more controllable elements of business performance, such as the prudent management of costs. This involves integrating diverse resource models (including offshore), lean delivery, and technology. Risk managers and change assurance teams should identify and track the critical success factors, such as achieving clear outcomes for customers, employees, and regulators.
- **Navigating the challenges of 'as-a-service' transition:** The rapid adoption of 'as-a-service' solutions can leave customers and support unprepared, leading to change programmes not meeting their objectives during the transition to live operations. The internal audit function faces the challenge of not only providing oversight, but to advocate for customer experience, challenging the practicality of new solutions.
- **Balancing agile delivery with talent retention:** While agile and value stream change delivery methods drive innovation, retaining in-house expertise remains a challenge. Over-reliance on third parties, coupled with inconsistent agile application, can lead to wasted resources and drawn-out implementation timescales.
- **Navigating the regulatory shift:** The push for streamlined financial regulations in pursuit of economic growth and enhancing competition in the market presents a risk to end customers. The response of the change portfolio and product owners should be to create an environment conducive to progress without compromising the safety of customers.
- **Change programme pitfalls: Why transitions to BAU often fail:** Many change programmes struggle to fully realise their objectives during the transition to business-as-usual (BAU). Old problems resurface, hindering the intended benefits and highlighting the need for improved handover processes and more robust change management strategies.

Five things internal audit should do:

1. **Strategic approach**

   Internal audit should strategically assess change by considering key milestones and applying proportionate controls based on its nature and scale. Crucially, they must evaluate whether their assurance coverage remains fit for purpose.

   Internal audit activities should align on key corporate events (e.g., business process changes, new products/services, M&A activity).

2. **Governance**

   Internal audit should expand its role beyond assessing the change execution. It must actively examine business strategy, challenge existing practices, and proactively assess the risks of inaction, with a stronger emphasis on governance oversight.

3. **Skills versus skilled**

   Digitisation has increased reliance on external expertise for business transformation. Future-proof skills include using tools and GenAI technologies to automate development and other processes. Internal audit should review talent management and challenge future workforce strategies.

4. **Quality of reporting and data**

   Cost-cutting on change initiatives drives the need for internal audit to evaluate the appropriateness of objectives and key results (OKRs), quality of management information, stakeholder awareness, and risk management.

5. **Never a failure, always a lesson**

   Post-implementation reviews often prioritise large transformations, but continuous improvement, like DevOps, is key for long-term sustainability. Internal audit should ensure the organisation benefits from a centralised lessons-learned repository, especially learning from programmes that involve group level and local stakeholders.

Technology and operations

Operational resilience

While the FINMA circular 23/1 on operational risk and resilience for banks's regulatory deadlines will pass on 1 January 2026, operational resilience remains a key area of focus for firms, and internal audit functions alike. It is imperative that any momentum built up to the regulatory deadline is not lost. In an uncertain and constantly evolving landscape, firms need to remain alert to new vulnerabilities and ensure that important business services remain resilient. Recent large-scale disruptive events highlight the continued importance in building a resilient business that can respond and recover from a range of expected disruptions. How will geopolitical instability sanctions, trade wars, or unforeseen global events impact an organisation's ability to operate? This requires a more sophisticated approach to scenario planning than previous years.

Four things you should know about the topic:

- **A holistic approach to operational resilience**: The focus up to the FINMA regulatory deadline is understandably on achieving regulatory compliance. However, there is a need for firms to understand and draw upon wider resilience capabilities such as business continuity and disaster recovery and third-party risk management, for which firms have often run separately to operational resilience programmes.
- **Effective communication to navigate disruptions**: High-profile disruptions in early 2025 alone highlight the importance of robust and effective communication strategies to manage both internal and external stakeholders, to reduce any potential negative impacts as much as possible. Strategies to support communication internally to staff and external stakeholders such as the media (including social media), suppliers, customers, and the regulator should be designed and regularly tested to provide management with assurance over its useability and continued effectiveness.
- **Enhancing MI to support resilience efforts**: Management information (MI), although not a new area of focus, is still a weak area for many organisations and requires continued development and maturity to enable Boards to apply appropriate governance over operational resilience activities. Effective and timely MI and reporting will support resilience investment decisions, so it is imperative that appropriate MI is in place.
- **Building a proactive culture of resilience**: One of the key aims of the regulation was to drive a cultural shift in how firms view operational resilience, by embedding resilience considerations in the day-to-day running of the business and operational processes. In the past, resilience has been as a by-product of investment into systems, processes and controls. However, management now needs to put resilience first – as the desired outcome – and systems, processes and controls should be developed to maximise the resilience of a firm's most important business services.

Five things internal audit should do:

1. **Assessment of wider resilience capabilities**

   Internal audit functions should assess their organisation's approaches to resilience beyond the regulatory requirements. Traditional areas such as business continuity, IT disaster recovery, and third-party risk management should be subject to review through the resilience lens to ascertain the end-to-end resilience capability. Technology resilience by design should be a key area of focus, given the advent of AI and automation, cloud security and quantum computing threats.

2. **Communications strategies**

   The robustness and useability of both internal and external communications strategies should be subject to scrutiny by internal audit, particularly in the context of understanding how they can be leveraged in the event of a disruption to minimise fallout and help to facilitate a stronger recovery.

3. **Embedding a culture of resilience**

   Internal audit activity should focus on resilience across the broader audit plan, considering whether resilience controls and associated risks are adequately embedded across a range of audits that impact important business services, both directly and indirectly

4. **Management information**

   Internal audit functions should continue to apply challenge to the quality and effectiveness of MI to ensure it is – and continues to be, in light of business change - appropriate for business needs. For example, they should challenge management on the use of data-driven insights to identify emerging risks and trends, using key risk indicators (KRIs) and key performance indicators (KPIs) to monitor operational resilience, and encourage the move beyond reactive reporting to proactive insights on emerging risks and opportunities.

5. **Embedding of operational resilience activities into BAU environment.**

   Focus needs to continue to be put on supporting areas of activity within businesses. In particular, existing technology resilience processes may need to be re-engineered, so they effectively support wider operational resilience outcomes. Change methodologies and controls should adequately dovetail into the operational resilience landscape, ensuring firms' resilience frameworks and practices are systematically refreshed and updated.

Technology and operations

Third Party Risk Management (TPRM)

The escalating complexity of global supply chains, coupled with unpredictable macroeconomic and geopolitical shifts, has amplified the vulnerability of organisations reliant on third-party services. Cyber-attacks, data breaches, and compliance failures are no longer hypothetical threats; they are frequent occurrences crippling businesses. The lack of reliable, accurate information from third and fourth parties further exacerbates the problem, leaving many TPRM programmes struggling to keep pace.

Six things you should know about the topic:

- **Intensified financial services sector regulatory requirements:** The FINMA circular 23/1 on operational risk and resilience for banks and the EU's DORA, significantly increase the complexity of financial services regulation, requiring firms to navigate distinct but overlapping requirements for managing critical third-party relationships, focusing on business continuity, and information and communication technology (ICT), cyber risk and critical data management. Stringent regulations and increased third-party disruptions are driving large-scale remediation efforts. Common compliance challenges include responding to large-scale remediation efforts across multiple divisions and geographies, as well as understanding the baseline for regulatory compliance across various regulations.
- **Emerging artificial intelligence (AI) risks in third-party relationships:** The increasing use of GenAI tools, both internally and by third parties, requires a sophisticated TPRM framework to address emerging risks. This includes data quality, algorithm reliability, cybersecurity, data privacy, and ethical considerations to mitigate potential operational disruption and reputational damage.
- **Operational resilience and TPRM:** Organisations must continue to integrate operational resilience with third-party risk management capabilities to meet the growing regulatory requirement. This ensures that third-party disruptions do not exceed acceptable impact thresholds.
- **Third party governance:** A robust governance structure for third-party risk management is essential for accountability, consistent policy application, effective monitoring, proactive risk mitigation, regulatory compliance, and transparent communication. It ensures that roles are clearly defined, risks are consistently identified and addressed, and the organisation demonstrates a commitment to managing third-party risks effectively.
- **Use of risk intelligence over traditional attestation-based assurance:** The traditional attestation-based and point-in-time approach to third-party risk assessment relies heavily on self-reported data, limiting its effectiveness. Increasingly, organisations are adopting risk intelligence, leveraging external data sources and advanced analytics to gain a more comprehensive and objective view of third-party risks. This shift allows for proactive identification of emerging threats and vulnerabilities, moving beyond reactive compliance checks to a more predictive and resilient risk management strategy.
- **IIA topical requirements:** The Institute of Internal Auditors (IIA) is expected to finalise their topical requirements on Third-Party risk, later this year, which will be mandatory for internal audit functions.

Five things internal audit should do:

1. **Intensified financial services sector regulatory requirements**

   Effective collaboration across all three lines of defence and consistent internal audit involvement is crucial to ensure the business and risk areas have considered the changes in the regulatory environment and uplifted policies and processes accordingly.

2. **Emerging AI risks in third-party relationships**

   Internal audit may provide independent assurance on the effectiveness of controls mitigating AI-related risks within third-party relationships, encompassing data governance, cybersecurity, and compliance; this includes evaluating due diligence processes, monitoring performance, and reporting on emerging threats to management and the Board.

3. **Operational resilience and TPRM**

   Internal audit may evaluate the impact of third parties on the organisation's ability to remain within its impact tolerance limits by assessing the consideration of third-party failures in stress testing scenarios and reviewing the robustness of business continuity plans (BCPs) and exit strategies for critical third parties, ensuring alignment with the organisation's overall BCP.

4. **Third party governance**

   Senior oversight is essential for all successful TPRM programmes and internal audit has a key role to play as the third line in the governance structure for TPRM in any financial services organisation, through proactive audit planning and identification of key roles and responsibilities within the TPRM governance structure.

5. **Use of risk intelligence over traditional attestation-based assurance**

   Internal audit should test the effectiveness of risk intelligence outputs, including feeding into the effectiveness of large-scale technology implementations in third-party risk management, by reviewing data sources and methodology, comparing results with traditional attestation methods, testing predictive capabilities, assessing alerting mechanisms, reviewing governance and controls, and interviewing key personnel. This multifaceted approach helps determine the reliability and value of the organisation's risk intelligence programme.

Technology and operations

Cyber risk

In an era defined by digital acceleration and systemic unpredictability, cyber security has transcended its traditional boundaries to become a cornerstone of enterprise resilience. The cyber security landscape is in constant flux, with new threats and vulnerabilities emerging daily.

For internal audit functions, staying ahead of the curve is critical to ensuring the effectiveness of their risk management and assurance activities. Proactive review and challenge of internal security controls, and continuous monitoring are essential for navigating the complex and ever-changing cyber security landscape.

Five things you should know about the topic:

- **Artificial intelligence (AI) is rapidly transforming the cyber threat landscape:** Attackers are leveraging AI for automated phishing campaigns, sophisticated malware development, and the rapid identification of vulnerabilities. This necessitates a shift towards AI-driven security solutions for detection and response.
- **Human error remains a significant cyber security vulnerability, despite technological advancements:** The 2025 attacks on major retailers highlight this, showcasing sophisticated techniques using advanced social engineering, custom malware. and modified leaked ransomware code. Robust security measures, including multi-factor authentication, endpoint detection and response (EDR), data loss prevention, and comprehensive security awareness training, are vital for mitigating these threats. Recent attacks such as that on insurers in the US, where hackers stole personal information from customers, highlight that this is global risk. Robust security measures, including multi-factor authentication, endpoint detection and response (EDR), data loss prevention, and comprehensive security awareness training, are vital for mitigating these threats.
- **Cyber-attacks targeting the supply chain are becoming increasingly prevalent:** Organisations need to assess and manage the cyber security risks associated with their third-party vendors and suppliers. This requires robust due diligence processes and ongoing monitoring of vendor security practices.
- **Cyber and the Internet of Things (IoT):** The expanding attack surface of IoT and Operational Technology (OT) devices presents significant cyber security risks. The sheer number and diversity of these devices, often lacking robust security features, creates numerous entry points for attackers. Legacy systems, outdated protocols, and insufficient network segmentation exacerbate vulnerabilities. The potential for cascading effects from a single compromised device necessitates a comprehensive and proactive approach to security.
- **IIA topical requirements:** The Institute of Internal Auditors (IIA) has released a cyber security topical requirement in Q1 of 2025, providing a baseline approach for assessing cyber security governance, risk management, and control processes. Internal audit functions must understand and comply with these requirements when conducting cyber security audits or when cyber security is identified as a risk within other audits.

Five things internal audit should do:

1. **Assess the maturity of cyber security programmes**

   Internal audit should evaluate the maturity of the organisation's cyber security programme against recognised frameworks such as NIST cyber security framework. This assessment should focus on the effectiveness of people, process and technology in mitigating identified risks.

2. **AI attacks**

   Internal audit must assess the organisation's readiness for AI-powered attacks. This involves evaluating AI-powered threat detection systems, deepfake detection technologies, and employee awareness. A crucial aspect is reviewing the security implications of AI deployment across all systems and processes, ensuring robust AI-related security practices are in place to mitigate risks.

3. **The evolving threat of ransomware**

   Internal audit should verify the effectiveness of security awareness training (including phishing simulations), assess the security culture, and confirm robust access controls. A comprehensive vulnerability management programme (patching, scanning, penetration testing) and strong data security measures (classification, encryption, DLP) are crucial. Finally, the incident response plan needs regular testing and updates to ensure effective communication and recovery.

4. **Supply chain security**

   Third-party vendor reliance expands cyber security risk. Internal audit should review supplier risk assessments, enforcing robust cyber security clauses in contracts, and monitoring the entire supply chain's security posture. This proactive approach strengthens overall security and resilience.

5. **IIA cyber security topical requirement compliance**

   The IIA's cyber security topical requirement (released in Q1 of 2025) will become mandatory for audit engagements. Internal audit should prioritise achieving and maintaining compliance with this requirement. This involves collaborating with information/cyber security teams to improve cyber security risk assessments, enhance the controls environment, and develop a robust technology strategy. The focus should be on aligning audit processes with the new standards and ensuring ongoing conformance.

Technology and operations

Data governance

Data remains a strategic asset, but inadequate governance creates a significant competitive disadvantage, hindering innovation and efficiency while raising costs and reputational risks. The rapid growth of data and accelerating technological change (e.g., changes in the AI landscape) exacerbate this challenge, further amplified by the increasing reliance on data-driven decision-making across all business functions. This is reflected in data's rise as one of the critical topics for internal audit functions.

Five things you should know about the topic:

- **Sustained and accelerated technological change:** The rapid pace of technological innovation creates a significant challenge for organisations to keep pace with evolving data security threats and best practices. This widening gap necessitates a more urgent focus on embedding data management practices and data governance frameworks. The migration of data to the cloud introduces new risks related to data security, privacy, and compliance.
- **Data management, privacy, and security regulations:** Switzerland's evolving regulatory framework places increasing emphasis on robust data governance, privacy and operational resilience. The revised Federal Act on Data Protection (FADP) and FINMA circular 23/1 on operational risk and resilience require firms to implement strong controls around data ownership, quality, integrity, and recoverability. These expectations align with international standards such as the EU GDPR, particularly for institutions managing cross-border data flows or using cloud-based infrastructures. Swiss firms are expected to maintain a dynamic compliance posture, ensuring that data management practices remain proportionate to their risk exposure while supporting transparency, security and regulatory resilience.
- **Data governance maturity:** Achieving robust data governance is a journey, not a destination. Organisations are starting to focus on sustainable maturity, building capabilities incrementally and fostering a culture of continuous improvement. "Walking before running" is key.
- **Digital savviness and leadership:** A strong commitment to data governance must be driven from the top. Successful organisations set the tone at the top to champion digital literacy and foster a culture of data responsibility throughout the organisation.
- **Data resilience and business continuity:** Organisations need to build data resilience into their operations to ensure business continuity in the face of disruptions, whether caused by cyberattacks, natural disasters, or other unforeseen events.

Five things internal audit should do:

1. **Prioritise and guide data governance initiatives**

   Internal audit should collaborate with the business to identify and prioritise key initiatives, offering practical guidance and risk assessments to bridge capability gaps and achieve sustainable maturity. Focus should be on incremental, achievable improvements.

2. **Champion a culture of continuous improvement**

   Internal audit should promote the implementation of a continuous monitoring programme for data governance, including regular data quality assessments and process reviews. Based on the findings, specific improvement recommendations should be developed and implemented iteratively. A feedback loop should be established to track progress and ensure ongoing improvement.

3. **Promote data literacy and digital savviness**

   Internal audit should champion data literacy training programmes, starting with senior leadership, to foster a culture of data responsibility and informed decision-making at all levels.

4. **Proactively assess emerging data risks**

   The use of emerging technologies, automation, data analytics, and AI for decision making requires strong data quality and data management processes. Internal audit needs to assess the risks associated with automated systems and ensure data quality throughout the automation lifecycle.

5. **Strengthen data resilience and business continuity**

   Internal audit should assess the organisation's data resilience by evaluating its data protection and recovery mechanisms. This includes reviewing data backup and recovery procedure, disaster recovery plans, and incident response strategies for data-related incidents. This should include consideration of adherence to recovery time objectives (RTOs) and recovery point objectives (RPOs).

Technology and operations

Cloud

Cloud adoption in Switzerland continues to accelerate, reshaping how financial institutions manage data, technology, and operational resilience. As organisations transition from on-premises infrastructures to multi-cloud and hybrid environments, regulatory scrutiny is increasing. FINMA's expectations under circular 23/1 on operational risks and resilience, together with the revised Federal Act on Data Protection (FADP), require firms to ensure transparency, data sovereignty, and secure outsourcing arrangements. These developments align with broader European initiatives such as NIS2 and GDPR, reinforcing the need for strong governance and continuous monitoring across the cloud ecosystem.

Four things you should know about the topic:

- **Geopolitics and cloud sovereignty:** Heightened geopolitical tensions and evolving data-sovereignty rules are prompting Swiss institutions to reassess cross-border cloud strategies. FINMA expects firms to understand and manage third-country risks, including data-access rights and operational dependencies on non-Swiss providers. Robust mitigation strategies should include defined data-location governance, contractual safeguards, and clear exit procedures.
- **ESG is a business driver:** Environmental and social considerations are increasingly integrated into cloud-strategy decisions. Organisations are expected to evaluate the environmental footprint of their IT infrastructure, including cloud-provider sustainability metrics and energy-efficiency goals, aligning ESG criteria with procurement and governance frameworks.
- **Cloud and data responsibility:** Under FINMA circular 23/1 and the revised FADP, financial institutions must maintain strong controls over data confidentiality, integrity, and recoverability within outsourced environments. This includes ensuring contractual clarity, audit rights, and effective monitoring of cloud service providers. Institutions operating cross-border should harmonise practices with international frameworks such as EU NIS2 and GDPR.
- **Resilience of cloud supply systems:** The increasing reliance on hyperscalers introduces concentration and continuity risks. FINMA and the SNB emphasise multi-provider strategies, robust exit planning, and ongoing testing of recovery objectives (RTO/RPO) for critical workloads to maintain operational resilience.

Five things internal audit should do:

1. **Assess geopolitical risk and data sovereignty exposure**

   Internal audit should evaluate whether the organisation's cloud strategy addresses FINMA expectations on data residency, third-country dependencies, and outsourcing risks under circular 23/1 and 18/3.

2. **Integrate ESG into cloud audits**

   Review how ESG objectives—such as carbon footprint, energy efficiency, and provider sustainability—are incorporated into the institution's cloud-governance and vendor-management processes.

3. **Enhance data security and privacy reviews**

   Test compliance with the revised FADP, FINMA circular 23/1, and EU NIS2 by assessing data classification, encryption, and access controls across hybrid environments. Confirm that incident-response and breach-notification procedures meet regulatory requirements.

4. **Review supply chain resilience**

   Verify that business-continuity and exit strategies are up to date, tested, and aligned with the organisation's recovery objectives. Ensure that dependencies on specific cloud providers are documented and that alternate-provider scenarios are feasible.

5. **Monitor cloud costs**

   Internal audit should regularly monitor cloud costs, identifying areas for optimisation and recommending cost-saving measures. This includes reviewing resource utilisation, identifying inefficiencies, and leveraging cloud cost management tools.

Governance

Risk culture

Increasingly, financial services regulators across the globe are focusing on the effectiveness of organisations' risk cultures, particularly in the UK, Europe (ECB and CBI) Australia (APRA), the Netherlands (DNB), and Canada (OSFI). This includes stronger enforcement of existing regulations and the introduction of new ones, designed to hold senior management accountable for fostering a strong risk culture. The institute of internal auditors (IIA) is looking to finalise topical requirement around organisational behaviour to assess if behaviour is aligned to strategy. Furthermore, FINMA sent out surveys to various banks on governance, risk culture and remuneration in 2025. Beyond regulatory expectations, organisations that consider how their risk culture can be a source of sustainable competitive advantage are well placed for success and may outperform those with undesirable cultures.

Five things you should know about the topic:

- **Internal audit's increasing role**: Internal audit's role in assessing risk culture is important for ensuring an organisation's long-term health and sustainability. A strong risk culture is not a one-time fix but an ongoing process requiring continuous monitoring and improvement.
- **Digital transformation and the evolving risk landscape**: As our world becomes increasingly digital and technologically advanced, including greater use of AI, this brings many benefits but also increased risk. Organisations need to ensure they have a risk culture that supports more AI adoption (i.e. risk management awareness at all grades, a culture of constructive challenge and clear accountability).
- **Global regulatory perspectives on risk culture**: There is increased regulatory interest in risk culture. The Canadian regulator, OSFI, has raised expectations regarding culture risk management (in November 2024) highlighting that culture can support (or undermine) sound decision-making, prudent risk-taking and effective risk management. The European Central Bank (ECB) recently issued its guide on governance and risk culture, which clarifies their expectations that a healthy risk culture that supports innovation and compliance. The FINMA risk monitor 2025 also mentions a special focus of FINMA on governance, risk culture and risk management and that an adequate risk culture can help mitigate the current risk exposition of organisations.
- **Effective risk culture framework**: A risk culture framework is essential for anchoring a risk culture review or assessment, as well as designing metrics. One example, the Deloitte risk culture assessment framework, considers both human capital and risk management perspectives to give greater depth of coverage.
- **Cybersecurity and technological advancements:** Organisations are investing heavily in cybersecurity infrastructure and training but are also focusing on fostering a culture of security awareness among employees. This involves promoting reporting mechanisms for security incidents and encouraging a proactive approach to identifying and mitigating potential threats.

Four things internal audit should do:

1. **Expanding your current assessment from risk culture to organisational culture and behaviour**

   Given the IIA's increased emphasis on consistency and the growing regulatory focus on behaviour, internal audit functions must develop a comprehensive audit strategy addressing culture and behaviour. This strategy should ensure behaviours align with strategic objectives, delivering positive outcomes for customers, employees, and society. It should cover audit coverage approach to include various toolkits, such as stand-alone review, thematic review and integrated coverage.

   While some mature internal audit functions benefit from dedicated behavioural risk specialists, all functions should strategically align skills to meet this evolving focus.

2. **Consider diversity, equity and inclusion**

   Growing research suggests a strong correlation between diversity and inclusion and effective risk management. This not only encompasses physical diversity characteristics, but also diversity of thought.

   Psychological safety/challenge

3. Regulators continue to focus on the extent to which environments are psychologically safe – that is, where individuals feel free to challenge without fear of retaliation at all levels. Internal audit should consider how this is incorporated into their regular risk culture assessments.

   Getting ahead using technology for better culture insights

4. Increasing availability of relevant data (including leveraging data analytics and GenAI) can provide quicker and greater insights into culture which can be used to the internal audit teams to ensure right outcomes are reached.

   Consider a risk culture assessment for AI readiness. A risk culture dashboard can support continuous improvement, which collates relevant metrics and data points, including a qualitative overlay on context (e.g., lessons learned) and historical movements to support the metrics.

Environmental, social and governance

Nature-related financial risks

The Swiss Financial Market Supervisory Authority (FINMA) along with European regulators has recognised the increasing relevance of nature-related risks for the financial sector. In response FINMA has developed its circular 26/1 on nature-related financial risks with the aim of raising awareness of the topic and providing greater clarity and guidance to banks and insurers. The circular, issued on 12 December 2024 and effective from 1 January 2026, covers both climate- and environmental-related risks and aims to equip these institutions with the tools needed to effectively identify, assess, manage, and control all the material risks they may encounter, ensuring robust risk management and sustainable operations. Implementation of the new circular is being carried out in phases from 1 January 2026 until 1 January 2028.

Five things you should know about the topic:

- **Governance:** Financial institutions are expected to have in place an effective and sound governance structure to enable strategic oversight of these risks by ensuring that nature-related financial risks are embedded into the institution's long-term planning and risk appetite. In order to do so, institutions should ensure that roles and responsibilities are appropriately allocated within the controls functions and business units, and that trainings on the topic are provided in a timely manner.
- **Risk identification and materiality assessment:** Proper identification and materiality assessment of nature-related financial risks is fundamental element of the process. The circular requires financial institutions to periodically identify potential exposures to nature-related financial risks – such as climate change, biodiversity loss, deforestation, water scarcity, and pollution – and assess their materiality across different risk types (in particular, credit, market, liquidity, and operational risk).
- **Risk management:** Where an institution identifies nature-related risks as material, it must actively integrate these risks into its current risk management framework – for example, integration in their financial reporting, credit loss projections, internal capital and liquidity assessments.
- **Stress testing:** Category 1 and 2 Institutions with material nature-related financial risks are required to gradually integrate these risks into their stress tests and capital adequacy assessments (ICAAP for banks and ORSA for insurers).
- **Global focus on sustainability risk management:** Effective 1 January 2026, the circular represents a critical step towards the alignment of Swiss regulations for the financial sector with EU and other global regulatory practices. The circular sets a clear guidance for financial institutions for identifying, measuring and monitoring nature-related financial risks aligning with global regulatory and oversight efforts such as the ones shown in the EU, in the UK and in some Asia-Pacific geographies where climate stress tests and scenario analyses to assess climate change's impact on financial institutions have been conducted.

Four things internal audit should do:

1. **Appropriate governance and oversight**

   Ensure that policies that explicitly cover nature-related risks are developed, implemented, and aligned with internal risk appetite and sustainability goals. Regularly review adherence to these policies.

   BoD and top management should be upskilled on nature-related risks and actively oversee their integration into the risk management framework. Ensure roles and responsibility are appropriately integrated in the current governance framework and that proper oversight of these risks is in place.

2. **Robust methodologies to identify and assess materiality of risks**

   Verify proper formalization of approach and methodologies for the identification nature-related risks and assessment of their materiality on traditional financial risks. Evaluate adherence of the process to the defined approach and methodologies.

   Review scope and coverage of the identification and materiality assessment to ensure comprehensive coverage of all relevant portfolios and risk drivers.

   Ensure materiality of risks is regularly re-evaluated with a similar periodicity as traditional financial risks.

3. **Integration into existing risk management framework**

   Monitor the integration of nature-related risks into current risk management and reporting process. Verify appropriate KRIs and early warning indicators have been assigned also in relation to these risks.

   For bigger institutions, review stress testing methodology and assumptions to ensure all relevant considerations for material nature-related risks have been accounted for.

4. **Data availability**

   The scarcity of granular, reliable data, coupled with the cost and risk associated with third-party reliance, remains a challenge for effective risk management frameworks. Validation of third-party data and the optimal balance between outsourced and in-house data capabilities should continue to be reviewed and challenged.

Internal audit innovation and transformation

GenAI usage across internal audit lifecycle

In 2024, we explored the transformative potential of Generative AI (GenAI) for internal audit. Fast forward one year, and we're witnessing a remarkable surge in GenAI adoption across the industry. Our clients have highlighted tangible improvements in efficiency and quality, and impact is being realised throughout the audit lifecycle. Our latest research indicates that approximately 79% of internal audit functions are now utilising tools like Co-pilot, with a further 38% exploring custom-built GenAI solutions.

While many functions are still in the early stages – primarily leveraging chatbots and in-house wrappers around Large Language Models (LLMs) – a clear shift is underway towards more tailored GenAI applications and seamless integration with existing systems. Applications are expanding beyond initial risk assessment and audit planning to encompass automated testing, working paper drafting, report generation, issue tracking, resource scheduling, and even tailored learning paths for audit teams. The market is seeing a rise in several types of GenAI tooling, including enterprise tools (like ChatGPT and Co-pilot), agentic ecosystems, specialised GenAI (such as Deloitte's Internal audit and controls hub and Co-pilot integrations), and AMS GenAI (e.g., AuditBoard). These tools range in design from end-user driven to workflow-based and platform-embedded solutions.

Five things you should know about the topic:

- **Maturing adoption and practical deployment:** GenAI is moving beyond the hype cycle towards pragmatic, integrated deployment. The focus is shifting to secure, tailored solutions and effective integration with existing systems.
- **Elevating the auditor's role:** GenAI augments, not replaces, auditors. By automating routine tasks, it frees up time for higher-value activities like critical thinking, strategic insights and partnering with the business to identify the right response to audit findings. Robust human oversight - "human in the loop" remains crucial to mitigate risks such as "hallucinations" and bias.
- **Data strategy as a foundation:** The success of GenAI in audit depends on high-quality, accessible data. A comprehensive organisational data strategy is essential, encompassing proactive data curation, accuracy, security, and the potential use of synthetic data.
- **Navigating regulatory and ethical landscapes:** Internal audit in financial services must stay abreast of evolving AI regulations (e.g., EU AI Act, FINMA guidance 08/24) and ethical considerations. Assurance over fair, transparent, and explainable GenAI deployments is paramount.
- **Upskilling and mindset shift:** Harnessing GenAI requires significant upskilling in AI concepts and prompt engineering. A cultural shift is also needed to embrace AI as a collaborative tool, fostering a new approach to teamwork and leveraging intelligent tools effectively.

Five things internal audit should do:

1. **Develop a tailored GenAI strategy**

   Create a GenAI strategy identifying high impact use cases and set clear objectives for phased integration into audit processes. Consider the available technology i.e. enterprise (e.g., ChatGPT, Co-pilot), specialised (e.g., Deloitte's IA&C Hub), and AMS GenAI (e.g., AuditBoard), and select a design (end-user driven, agentic, workflow-based, or platform-embedded) that aligns with your organisation's capabilities and strategic goals. Prioritise secure, scalable implementation and define how success will be measured i.e. improved efficiency, quality and impact.

2. **Establish robust AI governance**

   Implement comprehensive governance for GenAI, encompassing policies for data privacy, model validation, output accuracy, and ethics. Ensure clear "human-in-the-loop" protocols for accountability. This governance framework should address the specific risks associated with the chosen GenAI tools and their integration into existing systems.

3. **Build a strategic data foundation**

   Collaborate with data teams to identify, curate, and prepare high-quality datasets for GenAI. Address data integrity and quality issues proactively to maximise effectiveness and minimise risks.

4. **Invest in upskilling and culture**

   Prioritise continuous learning for auditors on GenAI fundamentals and risks in addition to the skills needed to critically evaluate and challenge GenAI outputs, ensuring that the 'human in the loop' remains an effective and integral part of the process.

5. **Pilot and scale responsibly**

   Focus initial GenAI efforts on specific, high-value use cases in controlled environments. Successful piloting builds confidence and demonstrates ROI, paving the way for broader deployment.

Internal audit innovation and transformation

Data analytics

The past year has seen a dramatic shift in the urgency surrounding data analytics for internal audit. While the importance of data-driven insights has been discussed for years, 2026 marks a turning point: the sheer volume and velocity of data, coupled with increasing regulatory demands and stakeholder expectations, have made data analytics a non-negotiable for maintaining relevance and effectiveness. To succeed, internal audit functions must adopt a multi-faceted approach encompassing a well-defined strategy, comprehensive data literacy training, proactive data quality assessments, compelling communication of insights, and a robust plan for implementing Continuous Controls Monitoring (CCM). This proactive approach will enable internal audit to deliver greater value and enhance its contribution to the organisation.

Five things you should know about the topic:

- **A strategic approach is paramount:** Aligning analytics plans with the overall strategy of the function is crucial for success. Our 2025 internal audit data and analytics survey revealed that 90% of functions with aligned strategies reported successful analytics implementation, highlighting a strong correlation between strategic alignment and positive outcomes.
- **Data literacy is a core skill:** Strong data literacy empowers audit teams to derive accurate insights, make informed decisions, and build greater stakeholder trust. However, our survey revealed a significant gap: while 62% of functions provided basic analytics training, with the intention of increasing data literacy across the team, only 3% offered advanced training to a comparable number of staff. Bridging this gap is critical for maximizing the value of data analytics.
- **Data quality requires proactivity:** While 79% of functions evaluate data quality before analysis, a significant 52% still cite poor data quality as a major barrier. This highlights the need for proactive data quality management strategies, not just reactive evaluation, to ensure the reliability and accuracy of audit findings. Internal audit should continue to articulate the risk to the business and provide recommendations to support improvement in this space.
- **Effective storytelling is essential:** Communicating data-driven insights effectively is crucial for stakeholder engagement and decision-making. Visualisations, compelling narratives, and regular progress reporting are essential for translating complex data into actionable information. We have noted that functions who have better uptake when implementing new tooling, particularly GenAI, have been good at sharing success stories within team.
- **Continuous Controls Monitoring (CCM) requires clarity:** While the value of CCM is widely recognised, its optimal placement within the three lines of defence remains a subject of debate. The key to successful CCM implementation is clear definition of objectives and a well-defined process for translating insights into actionable steps.

Five things internal audit should do:

1. **Assess maturity, set realistic goals**

   Clearly define your ambitions and current capabilities. Conduct a self-assessment to identify your current maturity level and set measurable goals aligned with your resources and capacity for growth.

2. **Develop a robust analytics toolkit**

   Continuously evaluate and enhance your analytical toolkit to incorporate the latest technologies and techniques, such as generative AI, advanced processing, and effective visualisation tools.

3. **Integrate with existing systems**

   Streamline data access and reduce lead times by integrating analytics tools with existing audit management systems and data warehouses. This improves efficiency and reduces the risk of errors.

4. **Build a high-performing analytics team**

   Proactive communication between analytics and audit teams is key to effective data analytics. Invest in a skilled team that translates requirements into tests and insights into actionable recommendations, fostering collaboration and providing targeted training for clear communication and effective data storytelling.

5. **Foster a culture of continuous improvement**

   Embrace experimentation, feedback, and iterative refinement to ensure your data analytics initiatives remain effective and adaptable in a constantly evolving landscape. Stay current with industry trends and best practices to maintain a competitive edge.

Internal audit innovation and transformation

A high performing internal audit function

Impactful audit functions need to not just adapt but thrive in the face of ongoing change and disruption. Regulatory changes, digital transformation, organisational restructuring, shifts in target operating models, offshoring and the complexities of mergers and acquisitions — these aren't challenges; they're opportunities to forge a High-Performing Culture (HPC) that helps maximise the value which internal audit provides to its stakeholders.

Five things you should know about the topic:

- **Purpose-driven performance**: Our vision of the value-adding audit function of the future is one which is purpose-driven and digitally powered. The importance of a clear and shared purpose cannot be overstated in helping functions navigate change and disruption whilst maximising the value they add to their organisations.
- **Future-proofing IA culture**: To remain effective, internal Audit (IA) must build resilience to adapt to significant change events such as a change in leadership, shifts in strategic direction, or mergers and acquisitions. Thriving in today's environment requires recognising that change is not an exception but a constant. This means building the capacity within leaders and teams to navigate it effectively by fostering behaviours that enable confidence and fluidity. While this shift takes time and sustained effort, embedding these practices ensures internal audit continues to deliver value amidst disruption.
- **Connecting teams in hybrid environments**: A high-performing hybrid workforce requires strategic talent management: upskilling, reskilling, addressing skill gaps, and offering compelling career paths. As teams continue to explore onshore, near shore and offshore location plans, maintaining consistent quality control and training across geographically dispersed teams demands a carefully considered approach.
- **Championing innovation**: Internal audit must champion continuous improvement and innovation, establishing structures for idea generation, experimentation, and execution across integrated teams. This involves experimenting with new technologies, sharing best practices, and ensuring technology enhances, not replaces, human skills.
- **The human touch in technology**: We expect to see a shift of auditors' responsibilities - previously focused on defining risk and controls (e.g., RACMs), auditors now play a more critical role in challenging the output and managing stakeholder relationships to maximise value. Experimentation where teams explore new tools, share successes, and remember technology should augment, not replace, human skills and judgment.

Five things internal audit should do:

1. **Craft a compelling shared purpose statement**

   Collaboratively, as a function, crafting a purpose statement reflecting the function's mission fosters belonging and shared ownership. Designing innovative performance measures will highlight individual contributions.

2. **Implement a proactive cultural integration plan**

   When considering offshoring or operating during an M&A, implement a proactive cultural integration strategy that anticipates and addresses complexities of change.

   A thoughtful approach, addressing communication styles and technology platforms, creates a united, high-performing team, enhancing audit quality and stakeholder confidence.

3. **Develop a strategic talent management plan for a thriving hybrid and global workforce**

   To ensure consistent service delivery, establish clear communication protocols, utilise visual workflow tools, hold purposeful virtual meetings, and invest in cross-cultural communication training. Well-defined work agreements and a focus on joint accountability and team rewards, rather than individual achievements, foster collaboration and shared success.

4. **Cultivate disciplines for continuous improvement and innovation**

   Innovation should be promoted by all teams. This inclusive approach is key because it leverages the diverse perspectives and experiences of the entire workforce.

   Establishing structures that support this collaborative innovation process, and crucially, leadership giving explicit permission and actively fostering a culture of experimentation, will position internal audit to lead the business through transformation.

5. **Prioritise user experience in your technology strategy**

   When designing and rolling out technological change do not forget the user experience. An approach centred around the people using the technology which fosters experimentation and ensures technology enhances human skills. A well-defined technology strategy focused on innovation and efficiency will enhance collaboration, boost transparency, and deliver faster, higher-quality insights.

Internal audit innovation and transformation

Standards and quality assurance hotspots

The revised Institute of Internal Auditors (IIA) Global Internal Audit Standards ('Standards') continue to evolve with new mandatory topical requirements being consulted on and launched across the course of 2025. Although many functions conducted readiness assessments for the new Standards during 2024, audit methodologies and QA practices must continue to evolve as teams look to increase their impact on their broader organisations.

Five things you should know about the topic:

- **Topical requirements: Are you ready?** Topical requirements are a new mandatory component of the Internal Professional Practices Framework which, depending on a function's risk assessment results, must be applied when providing assurance services. Topical requirements on cyber security, third parties and organisational behaviour have been released/consulted on during 2025.
- **Setting your quality target:** The IIA's quality assessment manual now offers two 'pass' grades for the Standards: "General" and the new "Full" conformance, signifying complete adherence to all principles, standards, and requirements. With a significant increase in requirements under the new Standards, functions should determine their desired level of conformance with their audit committee.
- **Measure what matters:** The requirement under Domain IV for an internal audit strategy has driven a focus on a longer-term functional vision with clearly defined, purpose-driven outcomes. Defining meaningful performance measures that monitor both progress and the impact of the strategy remains a key focus for improvement.
- **Beyond compliance - unlocking QAIP's potential:** The higher conformance bar necessitates more efficient and impactful practices. Rapid technological advancements, including Generative AI (GenAI), offer opportunities to unlock efficiencies and expand the scope of Quality Assurance and Improvement Programme (QAIP) activities beyond basic compliance.

Five things internal audit should do:

1. **Evolve methodologies in response to new topical requirements**

   Topical requirements become effective 12 months after they have been issued. The cyber requirements will become effective from February 2026. Internal audit teams will need to integrate these into methodologies and develop awareness to ensure conformance. In areas such as organisational behaviour, this is likely to be an uplift for many functions.

2. **Set appetite for Standards conformance**

   Internal audit functions should have a view on any gaps to achieving "Full" conformance and understand the effort and benefits of achieving this. Discussion should be held with the audit committee on the appetite for "Full" versus "General conformance".

3. **Define performance measures which measure outcomes as well as inputs**

   Measuring performance against strategic goals with regular touchpoints with key stakeholders will help drive functions to achieve their longer-term visions. Balanced scorecards should be developed which go beyond traditional operational measures to monitor the outcomes and impact of strategic initiatives.

4. **Extend QAIP scope**

   Assess whether QAIP scope is in line with the new Standards. Consideration should be given to areas such as governance reporting, action closure validation, and annual risk assessment and audit planning processes.

   To ensure QAIP adds value, expand your definition of audit quality beyond conformance with methodologies and checklists to include the quality of insight and impact aligned to the internal audit strategy.

5. **Stretch and digitise QAIP approach**

   Is your QAIP approach aligned with your internal audit strategy digital ambitions? Does it contribute to team learning and continuous improvement in this area?

   Identify opportunities to use digital technologies in the QAIP process including GenAI in file reviews and leveraging functionality in audit management systems for continuous QA monitoring.

Banking and capital markets

Payments and financial crime

Swiss payments modernization initiatives

The evolving regulatory landscape in Switzerland, influenced by global standards, will drive the transformation of payments and digital assets. Swiss financial authorities, including FINMA, are emphasizing the importance of competition, innovation, and financial system integrity. This is reflected in their ongoing reviews and updates to risk frameworks and wind-down planning arrangements for Payment and E-Money firms.

Five things you should know about the topic:

- **Swiss regulatory structures and alignment with EU standards:** Switzerland is closely monitoring developments in the EU, such as PSD3 and PSR1, to ensure alignment where necessary. While Switzerland maintains its own regulatory framework, it is influenced by EU directives, particularly in areas like payment institutions (PIs) and e-money institutions (EMIs). Swiss firms operating across borders must adapt their compliance processes to manage regulatory divergence effectively.
- **Implementation timelines and impact on Swiss firms:** As the EU progresses towards implementing PSD3/PSR1, Swiss firms must prepare for potential impacts on their operations, especially those with cross-border activities. The transition period and go-live dates will require Swiss entities to consider readiness for changes in open banking services, strong customer authentication (SCA), and open banking requirements to ensure continued interoperability with EU frameworks. In parallel, Switzerland is pursuing its own payments modernization agenda, encompassing ISO 20022 message enhancements, the rollout of instant payments via SIC5 and the introduction of new structured addressing standards.
- **Swiss payments modernization initiatives:** Switzerland is actively modernizing its payments infrastructure, driven by public-private collaboration. Key initiatives include enhancing open banking, developing digital identity frameworks, exploring Central Bank Digital Currency (CBDC) and stablecoins, and strengthening security and fraud measures. These efforts align with global trends and aim to position Switzerland as a leader in financial innovation.
- **FINMA's focus on risk management:** FINMA emphasizes robust risk management frameworks, including liquidity risk management and wind-down planning arrangements. Swiss firms are expected to meet comprehensive expectations, prioritizing enterprise-wide risk management and considering group risk. FINMA's guidance ensures that firms maintain financial stability and resilience.
- **Internal audit and governance for new entrants:** In Switzerland, new regulated firms are required to implement a robust three lines of defence model, including an effective internal audit function. FINMA expects strong internal controls, operational resilience, financial crime controls, oversight of outsourced functions, and business continuity plans. Boards and regulators will scrutinize internal audit's coverage and target operating model to ensure compliance and integrity.

Four things internal audit should do

1. **Assess strategic opportunity and business readiness (PSD3/PSR1)**

   Internal audit should assess the strategic and long-term business impact and related risks of proposed developments, including any additional regulatory or compliance requirements. For example, non-bank payment firms gaining direct access to payment systems represents a major change that increases compliance needs.

   Given the broad impact of new EU regulations, internal audit functions should determine whether robust readiness planning is in place to ensure compliance. Re-licensing under the new regime will require effective risk management, governance, and controls.

2. **Understanding upcoming impacts of Swiss payments modernization initiatives**

   Internal audit should understand how the business is monitoring and responding to key developments in Swiss payments modernization, including infrastructure upgrades and the payments forward plan. With a focus on regulating stablecoins and other crypto-assets, internal audit should assess planned enhancements to the risk management and control framework, ensuring alignment with Swiss regulatory expectations.

3. **Evaluate changes to strong customer authentication**

   As Switzerland aligns with international standards, internal audit should keep abreast of changes in SCA regulations and understand whether the impact of these changes can be addressed across their organisation. This includes assessing the flexibility and outcomes-based approach to SCA rules designed to strengthen fraud prevention without imposing undue burdens on users.

4. **Assess internal audit coverage of risk management framework and wind down planning**

   Internal audit should consider reviewing risk management frameworks and wind-down plans to challenge and assess how management have incorporated the thematic review's findings.

   For internal audit functions in firms subject to regulatory reviews, internal audit should review and challenge the design and effectiveness of management's remediation of regulatory findings, ensuring compliance with Swiss regulatory standards and maintaining operational resilience.

Prudential and credit risk

Credit risk

FINMA's latest guidance (02/2025) highlights ongoing risks in the Swiss real estate and mortgage markets, focusing on credit and market risks. Banks are urged to apply sustainable affordability criteria, prudent collateral valuation, and robust risk management practices—especially around exceptions to policy (ETP) and commercial mortgages. Deloitte's perspective reinforces these expectations and outlines practical steps for internal audit to support compliance and risk mitigation.

Five things you should know about the topic:

- **Sustainable affordability criteria:** FINMA's guidance emphasizes the importance of applying strict affordability limits to ensure borrowers can sustainably manage their mortgage obligations. For owner-occupied residential properties, banks are expected to adhere to a maximum of 33% of gross income or 38% of net income for exceptions to policy (ETP) limits. For income-producing real estate, the limit is set at 100% of net rental income. This approach aims to prevent overestimation of borrower creditworthiness, a key supervisory concern, and to mitigate the risk of defaults in the Swiss real estate market.
- **Collateral valuation and model validation:** Accurate property valuations are crucial for risk management. FINMA requires that valuations be model-based, validated annually, and thoroughly documented. This ensures that valuations reflect current market conditions and are not subject to procyclicality. The use of valuation ranges must be prudently justified to maintain transparency and avoid inflating asset values. Deloitte's perspective highlights the need for robust model validation processes to support compliance and enhance risk mitigation.
- **Loan-to-Value and amortisation limits:** To limit risk build-up, FINMA recommends loan-to-value ceilings of 75% for income-producing real estate. Strong amortisation requirements are essential to ensure that borrowers gradually reduce their debt levels, thereby enhancing financial stability. Deloitte advises internal audit functions to closely monitor these limits and assess the effectiveness of amortisation practices in mitigating risks associated with high leverage.
- **Exceptions to Policy (ETP) management**: ETP transactions, which deviate from standard lending criteria, must be clearly flagged, justified, and monitored. FINMA stresses that risk-mitigating measures do not eliminate the need for ETP classification and reporting. Deloitte suggests that internal audit should evaluate the processes for identifying and managing ETPs, ensuring that they are consistently applied and that any deviations are well-documented and justified.
- **Commercial mortgage oversight:** Given the higher risks associated with commercial mortgages, FINMA requires frequent reviews, clear risk tolerance definitions, and systematic portfolio-level monitoring. This involves assessing the financial health of commercial borrowers and the economic viability of their projects. Deloitte recommends that internal audit functions focus on the robustness of risk management frameworks for commercial mortgages, ensuring that risk tolerance levels are clearly defined and adhered to, and that portfolio monitoring is comprehensive and proactive.

Five things internal audit should do

1. **Embed FINMA affordability and valuation standards**

   Evaluate whether credit policies and underwriting guidelines incorporate FINMA's sustainable affordability criteria and ensure valuation models are subject to annual independent validation with clear documentation.

2. **Champion continuous model validation**

   Promote ongoing independent validation of valuation models, including controls around the use of valuation ranges, to ensure transparency and mitigate procyclical valuation risks.

3. **Monitor and report ETP transactions**

   Verify that all ETP loans are accurately flagged at origination and throughout the loan lifecycle, with comprehensive documentation and inclusion in risk reporting frameworks to support timely risk mitigation.

4. **Evaluate Loan-to-Value and amortisation compliance**

   Review adherence to loan-to-value limits and amortisation schedules, ensuring policies are aligned with the institution's risk appetite and regulatory expectations, and that exceptions are properly authorised and monitored.

5. **Strengthen commercial mortgage risk controls**

   Audit the frequency and quality of commercial mortgage reviews, verify that risk tolerance levels are clearly defined and approved by the Board, and ensure systematic portfolio-level monitoring and reporting of concentration and credit risks.

Governance

Governance regime

Governance and clear individual accountability remain key priorities for Swiss regulators. FINMA's guidance under Circular 2017/1 Corporate governance – banks and the Federal Council's draft amendments to the Banking Act (2025) emphasise effective oversight, risk culture, and clearly defined responsibilities at senior-management level.
Swiss institutions are expected to maintain transparent governance structures, document decision-making authority, and ensure accountability for cross-border operations. In parallel, Boards are steering major transformation programmes requiring effective change governance and remediation oversight.

Four things you should know about the topic:

- **What's new with governance under Capital Requirements Directive (CRD) VI?** The EU's sixth CRD VI includes a revised 'fitness and propriety' framework, as well as the requirement to maintain individual statements for key individuals that sets out their roles and a separate document mapping the duties, reporting lines and lines of responsibility of the persons that are part of the governance arrangements.
- **The Swiss accountability regime:** The federal council has presented parameters for the preparation of the draft consultation on amendments to the Banking Act mid 2025. One part is the introduction of an accountability regime. The regime requires banks to define in a legally binding manner who is responsible for which decisions. This enables a clear allocation of responsibility and thus targeted new sanctions. At the same time, it makes it easier to enforce existing measures such as withdrawing an individual's fit and proper designation or imposing an industry ban.
- **Execution risk is a major boardroom concern:** The volume of change that firms are currently experiencing is significant, the drivers vary, but be it business changes, technology advances, regulatory scrutiny or material transactions, the outcome is the same: there is a meaningful amount of execution risk that is a cause for concern in many boardrooms.
- **Refining delegated authorities, finding the right balance:** There is an increasing interest from firms and the regulators in ensuring that there are robust but practical executive governance arrangements in place. One important way in which this is manifesting is a revision of delegated authorities, where companies are seeking to strike the right balance of authority between group executives, business heads subsidiaries and functional roles.

Four things internal audit should do:

1. **Governance under CRD VI**

   Internal audit's focus should be on design effectiveness focusing on challenging areas such as technology, operational resilience and data.

2. **Parameters paper on the Swiss accountability act**

   Internal audit should assess the proposed changes to the Banking Act and incorporate into the internal audit plan as required.

3. **Governance change programmes**

   Ensure that the internal audit plan is adequately covering the current suite of change programmes and that the Board and Audit Committee are comfortable with the scope.

   When assessing the effectiveness of project oversight, internal audit should consider whether there is evidence of senior individuals or forums challenging outcomes as well as monitoring progress; assessing portfolio risk and not just the risk of individual projects; and taking action when there is management stretch, rather than passively accepting the consequences of management stretch.

4. **Executive governance and delegated authorities**

   Internal audit should review the operational effectiveness of existing delegated authorities, to provide assurance that authorities are documented clearly, followed throughout the organisation and escalations or exceptions follow an appropriate process and are supported by adequate MI and documentation.

Insurance

Prudential and credit risk

Revision of the ISA and the ISO

The revised Swiss Insurance Supervision Act (ISA) and Ordinance (ISO), effective January 1, 2024, modernize the regulatory framework to align with international standards like Solvency II. This update introduces a more risk-based, proportionate, and customer-focused approach. Key changes include refined rules for governance, capital management, and customer protection, along with a modernized framework for tied assets. As a result, insurers must better integrate their risk, capital, and governance processes, creating new priorities for internal audit functions.

Six things you should know about the topic:

- **Solvency and Capital Adequacy:** The Swiss Solvency Test (SST) is now more deeply integrated into insurers' internal risk and capital management. Under the new ISO-FINMA, companies must align their capital planning with SST results, facing stricter requirements for valuation, stress testing, and model validation. The revised framework also mandates a stronger link between solvency, recovery, and resolution planning, requiring insurers to embed these considerations into their strategic risk and capital management.
- **Regulation of Insurance Intermediaries:** The revision introduces a clear distinction between tied and untied intermediaries. Both categories must be registered with FINMA, meet qualification and continuing education requirements, and disclose remuneration structures transparently. Insurers are responsible for supervising tied and united intermediaries and ensuring their conduct complies with regulatory and ethical standards.
- **Customer Protection and Market Segmentation:** Insurance policyholders are now classified as professional or non-professional clients. This allows for differentiated levels of information, advice, and contractual protection. Professional clients benefit from certain supervisory simplifications, while retail clients receive enhanced protection. Insurers must document and regularly review their customer classification and advisory processes to ensure regulatory compliance.
- **Organisation and Governance:** The Board of Directors now has greater responsibility for overseeing risk, capital, and overall resilience. Internal control functions like Risk Management, Compliance, and Internal Audit must operate more independently under clear mandates. FINMA requires documented governance frameworks with defined escalation paths and coordinated interaction between these functions. These structures must also support effective recovery and resolution planning, including defined roles for crisis management and communication with FINMA to ensure stability during financial distress.
- **Life Insurance and Transparency Obligations:** Expanded information, advisory, and documentation duties now apply to life insurance products. Customers must receive clear and comprehensive information on costs, risks, surrender values, and the economic suitability of the product. For complex or long-term products, suitability and appropriateness assessments are mandatory. This calls for standardised processes, regular staff training, and thorough documentation of advisory interactions.
- **Tied Assets (Gebundenes Vermögen):** The updated rules for tied assets provide greater investment flexibility while still protecting policyholders. Insurers must ensure that these assets continuously cover all policyholder obligations through strengthened valuation, control, and reporting processes. Additionally, there will be increased supervisory focus on the coordination between Finance, Risk Controlling, and Asset Management.

Five things internal audit should do

1. **Review of Solvency Management**

   Ensure that the SST process is fully integrated into strategic capital planning and that internal models are validated in line with ISO-FINMA requirements. The audit should assess stress tests, scenario analyses, and internal reporting to executive management and the Board, as well as evaluate how risk assessments influence strategic decisions.

2. **Assessment of Governance Structures**

   Verify that governance frameworks meet the new regulatory expectations. This includes assessing the independence and effectiveness of key control functions (Risk, Compliance, Internal Audit, Actuarial) and ensuring roles, responsibilities, and escalation procedures are documented and effectively implemented.

3. **Intermediary Supervision Oversight**

   Review intermediary registration, qualification, remuneration, and monitoring, with emphasis on tied intermediaries and compliance with conduct and disclosure rules, including FINMA reporting accuracy.

4. **Sales Processes and Customer Protection Review**

   Verify that information and suitability assessments in life insurance distribution are properly performed and documented. Focus areas include advisory quality, training of sales staff, control mechanisms in distribution, and the completeness of customer files. Targeted sample testing of contracts can help identify regulatory weaknesses early.

5. **Audit of Tied Assets**

   Assess whether valuation and control processes related to tied assets are robust and ensure continuous coverage of policyholder liabilities. This includes verifying alignment between Accounting, Asset Management, and Risk Controlling, as well as the transparency and accuracy of reporting to FINMA. Special attention should be given to valuation policies, evidence of coverage, and the effectiveness of internal controls.

Prudential and credit risk

FINMA Circular “Liquidity – Insurers” (RS 25/3)

The FINMA Circular “Liquidity – Insurers” (RS 25/3), effective 1 January 2025, refines the requirements for liquidity and liquidity risk management within Swiss insurance companies. It replaces the previous circular of the same name and aligns with international standards such as the IAIS Insurance Core Principles and EIOPA Guidelines.

Its objective is to ensure that insurers can meet their financial obligations at all times – including under stress conditions. The circular defines six key areas: governance, planning, liquidity reserves, risk management, controlling and monitoring, and contingency planning.

Insurers must establish formal liquidity planning, conduct regular stress tests, and provide structured reporting to FINMA — differentiating between strategic liquidity management (governance-level planning and oversight) and operational liquidity management (day-to-day execution and monitoring).

Reporting to FINMA must be prepared annually by a cut-off date of 31 December and submitted at the latest by 30 April of the following year. Extraordinary changes in the liquidity situation must be reported immediately. Reporting is standardised via FINMA's EHP platform.

Six things you should know about the topic:

- **Governance:** Clear responsibilities and reporting duties for liquidity and liquidity risk management must be defined and documented. The Board of Directors retains overall accountability.
- **Liquidity Planning and Scenarios:** Insurers must implement structured liquidity planning that covers short-, medium-, and long-term cash flows, stress scenarios, and sources of refinancing.
- **Liquidity Reserve:** The liquidity reserve must be of high quality, appropriately sized, and readily available in times of stress. Composition and adequacy must be reviewed regularly.
- **Liquidity Risk Management:** Risks arising from cash shortfalls, mass surrenders, market disruptions, or refinancing issues must be identified, measured, and managed within the company’s broader risk framework.
- **Liquidity Controlling and Monitoring:** Insurers must establish early-warning indicators, key metrics, and monitoring systems to detect liquidity pressures promptly. Reporting must clearly distinguish between strategic reporting (long-term planning and governance oversight) and operational reporting (day-to-day liquidity management).
- **Liquidity Contingency Planning:** A crisis or contingency plan for liquidity stress situations is mandatory, including escalation procedures, communication lines, and predefined response actions.

Five things internal audit should do

1. **Governance and Responsibilities**

   Assess whether governance structures and accountabilities for liquidity management comply with regulatory expectations. It should verify that roles and reporting lines are documented, effectively implemented, and subject to oversight by the Board of Directors.

2. **Liquidity Planning and Scenario Analysis**

   Ensure that structured liquidity planning processes exist, incorporating realistic stress scenarios and refinancing options. It should also assess whether contingency measures and FINMA reporting are properly designed and executed.

3. **Liquidity Reserve and Risk Control**

   Evaluate whether the liquidity reserve meets quantitative and qualitative requirements and is reviewed periodically. It should also verify that liquidity risks are systematically captured and integrated into the firm’s overall risk management framework.

4. **Controlling, Reporting, and Monitoring Processes**

   Assess whether key indicators, early warning systems, and reporting mechanisms are in place and functioning effectively. Internal Audit should ensure that reports are complete, timely, and submitted to all relevant governing bodies.

5. **Contingency and Crisis Management**

   Confirm that an up-to-date contingency plan exists, is regularly tested, and includes clear escalation and communication procedures. It should also assess whether training and lessons-learned processes are in place to strengthen organisational readiness for liquidity stress events.

Deloitte.