Internal Audit Focus Areas for 2026

Organisations continue to face heightened regulatory oversight, rapid technological change, and growing expectations around governance, risk management, and operational resilience. Internal Audit plays a critical role in providing assurance that risk and control frameworks are effective and aligned to strategic objectives. The IIA Global Internal Audit Standards (GIAS) raise the bar on risk-based planning, technology assurance, culture and conduct, and evidence-led auditing. Internal Audit functions should embed these requirements while staying sharply focused on their organisation's key risk drivers.

The Australian landscape is shifting with Privacy Act reforms, CPS 230 implementation for APRA-regulated entities, SOCI obligations, and emerging AI governance requirements. As a result, Internal Audit plans must be strategic, forward-looking, and anchored in the organisation's risk profile. The themes below highlight key focus areas for 2026, with practical considerations to help Internal Audit deliver high-impact, valued assurance.

Technology & Cyber Risk

Cyber Security

Cyber threats are becoming more sophisticated, with greater reliance on digital platforms, cloud environments and integrated systems, increasing exposure. Expectations for cyber governance, assurance and resilience have strengthened, requiring improved consistency in how organisations demonstrate their security posture.

Internal Audit should focus assurance on cyber security governance, controls and resilience to confirm that risk management practices remain effective. This includes assessing the maturity of cyber uplift initiatives, the reliability of cyber reporting to senior leaders, and whether identity, cloud and legacy platforms are appropriately and adequately configured and monitored, to mitigate vulnerabilities.

Potential audit objectives

- Assess cyber governance, including strategy, roles, responsibilities, escalation and reporting.
- Test operating effectiveness of key controls such as privileged access, vulnerability management, network segmentation and incident response.
- Review cloud and system configurations to identify misconfigurations or inherited vulnerabilities, including API connections and legacy interfaces.
- Evaluate completeness, accuracy and clarity of cyber metrics and reporting to senior management.
- Assess lessons learned and remediation activities following incidents or simulations.

AI, Data Governance & Privacy

Growing use of AI, analytics and automated decision making increases exposure to data quality, privacy and model governance risks. Organisations must strengthen data management and privacy controls while ensuring AI models are well governed and monitored.

Internal Audit plays a key role in evaluating data governance, privacy controls and AI risk management to confirm information is accurate, safeguarded and used appropriately. This includes reviewing data stewardship practices, the completeness of AI model inventories, the robustness of validation and monitoring activities, and the adequacy of controls applied by internal and third-party data processors.

Potential audit objectives

- Assess data governance structures, stewardship responsibilities and the effectiveness of data quality controls.
- Evaluate management of personal and sensitive information across the data lifecycle, including third-party processing.
- Review AI governance, including model inventories, risk classification, validation and monitoring.
- Test privacy controls such as consent management, data retention, access restrictions and breach response processes.
- Assess accuracy, completeness and transparency of data used for internal and external reporting.

Regulatory & Conduct Expectations

Regulatory Compliance & Change

Regulators are sharpening expectations across privacy, critical infrastructure, operational resilience and conduct, increasing scrutiny on how obligations are identified, interpreted and embedded across the organisation. Many organisations still face challenges coordinating regulatory responses across functions, maintaining clear ownership and ensuring reforms are implemented.

Internal Audit should direct assurance toward regulatory change management to confirm that obligations are understood, implemented and operating as intended. This includes reviewing monitoring mechanisms, governance oversight and the effectiveness of implementation across business areas.

Potential audit objectives

- Assess process for horizon scanning, regulatory interpretation and structured impact assessment.
- Evaluate impact assessments, including scope, required changes and key dependencies.
- Review implementation and embedment of regulatory changes across business areas.
- Assess governance and reporting frameworks for regulatory change programs.
- Evaluate sustainability of compliance through monitoring, periodic reviews and issue remediation.

Culture, Conduct & People

Culture and behavioural factors are increasingly recognised as drivers of organisational performance, compliance outcomes and risk exposure. Regulatory focus is intensifying, especially around psychosocial safety, accountability and leadership behaviour. SafeWork Australia's psychosocial-risk requirements and ASIC's attention to non-financial-risk governance reinforce the need for structured assessments.

Internal Audit plays a key role in evaluating cultural and behavioural drivers that influence decision making, accountability and staff wellbeing. This includes assessing behavioural risks, alignment between stated values and employee experience, and whether governance supports a safe working environment.

Potential audit objectives

- Assess effectiveness of risk culture frameworks, behavioural indicators and insight driven decision making.
- Review accountability frameworks, governance structures and decision making processes, including how consequences are managed.
- Assess speak up processes, reporting channels and protections against retaliation.
- Evaluate psychosocial risk management practices, including workload, leadership behaviours and escalation pathways.

Operational Risk & Resilience

Business Resilience & Continuity

Disruptions driven by technology outages, supply chain issues and evolving threat environments highlight the need for robust resilience and continuity arrangements. Organisations must identify critical services, define realistic impact tolerances and ensure coordinated continuity planning under a range of disruption scenarios. This includes alignment across business continuity, IT disaster recovery and crisis management practices.

Internal Audit plays a key role in assessing whether resilience capabilities are well deigned, integrated and validated through credible testing. This includes reviewing dependencies, recovery strategies and the effectiveness of testing programs. For APRA-regulated entities, alignment to CPS 230 expectations regarding credible BCPs, impact tolerances and resilience planning is essential.

Potential audit objectives

- Assess identification of critical services, dependencies and impact tolerances.
- Evaluate the design practicality of Business Continuity Plans, including activation triggers and escalation.
- Review alignment between business continuity, IT disaster recovery and crisis management arrangements.
- Assess continuity testing programs and follow up of remediation actions.
- For APRA-regulated entities, evaluate alignment with CPS 230 expectations for credible continuity planning and oversight.

Third Party & Supply Chain Risk

Reliance on third-party providers and complex supply chains continues to increase exposure to operational, technology and compliance risks. Stakeholders expect improved visibility of service provider performance, fourth-party dependencies and the resilience of outsourced arrangements.

Internal Audit should place emphasis on assurance over third-party governance, contracting and monitoring to support reliable service delivery and resilience. This includes evaluating due diligence, contractual obligations and oversight of performance, incidents and continuity. For APRA-regulated entities, this is further strengthened by CPS 230 expectations relating to material service providers supporting Critical Operations.

Potential audit objectives

- Assess third-party risk management policies, roles and responsibilities, including alignment with procurement and contract management processes.
- Evaluate risk tiering, due diligence and contracting arrangements.
- Review monitoring practices, including performance reporting and issue escalation.
- Assess visibility of fourth-party dependencies and the adequacy of contingency arrangements for critical providers.
- For APRA-regulated entities, assess compliance with CPS 230 requirements for identifying, managing and overseeing material service providers.

Strategic Change & ESG

Strategic Change & Transformation

Large transformation programs continue to reshape operating models, technology platforms and services. These initiatives carry significant delivery, governance, change management and benefits realisation risks. Organisations are expected to demonstrate that transformational change is well planned, appropriately governed and supported by effective risk management

Internal Audit plays a key role in providing assurance on transformation governance and execution to confirm alignment to strategic objectives and effective risk management. This includes assessing delivery risks, readiness for go-live and the extent to which business areas are prepared to adopt new processes, systems or controls.

Potential audit objectives

- Assess program governance, decision rights and oversight mechanisms.
- Conduct stage gate, pre-go-live and post-implementation reviews.
- Evaluate business readiness, including training, communication and change management.
- Review the design and implementation of controls within new systems or operating models, including management of technical debt and integration risks.

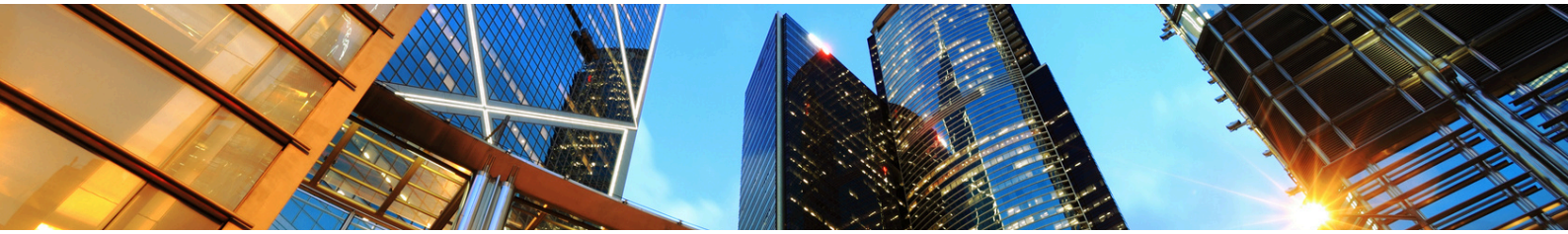
Sustainability, Climate & ESG

Sustainability and climate reporting expectations are increasing as organisations prepare for mandatory disclosure requirements under the Australian Sustainability Reporting Standards (ASRS 1 and 2). This necessitates accurate ESG data, well designed reporting processes, robust scenario analysis and the integration of climate-related risks into broader risk management frameworks.

Internal Audit plays a key role in assessing the governance, data quality and reporting processes that support credible ESG disclosures. This includes reviewing ESG governance structures, data controls and reliance on external data sources.

Potential audit objectives

- Assess governance, process maturity and data quality supporting ESG and climate reporting.
- Evaluate climate scenario analysis methodologies, assumptions and integration into risk management and strategic planning.
- Review controls over sustainability and climate data sourced from external providers, including transparency and validation processes.
- Assess how ESG risks and opportunities are incorporated into organisational decision making and risk frameworks.



Our Authors

Katherina Sau CA CIA
Director

Katherina is a risk and assurance professional with over 9 years of experience supporting internal audit and risk management functions to execute assurance plans and enhance risk maturity across organisations. She has also supported the development of multi-year internal audit plans for her clients, with her portfolio spanning public and private sectors, including Financial Services, Infrastructure, Education, and Health.

Jayashri Sood
Manager

Jay is a risk and assurance professional with over 5 years of experience delivering end-to-end internal and external audits across technology, operational and project environments in both the public and private sectors. She has supported major organisations in executing annual assurance plans, including reviews subject to APRA oversight, and brings experience across technology and data controls, operational process reviews, project assurance and governance uplift initiatives. Jay is also a certified ISO/IEC 27001 Auditor.

Meet Vyas
Consultant

Meet is a risk consultant with experience supporting internal audit, technology risk and process improvement activities across financial services. He applies analytical and technical skills to strengthen controls, improve system-enabled processes and uplift risk frameworks. His work includes controls testing, data integrity reviews and technology risk assessments across cybersecurity, general IT controls and data management.

View all services and case studies

Amstelveen

Email info@amstelveen.com

Website www.amstelveen.com

LinkedIn www.linkedin.com/company/amstelveen-pty-ltd