Deloitte.

Driving excellence: The strategic role of internal audit in Global Business Services transformation

JUNE 2026

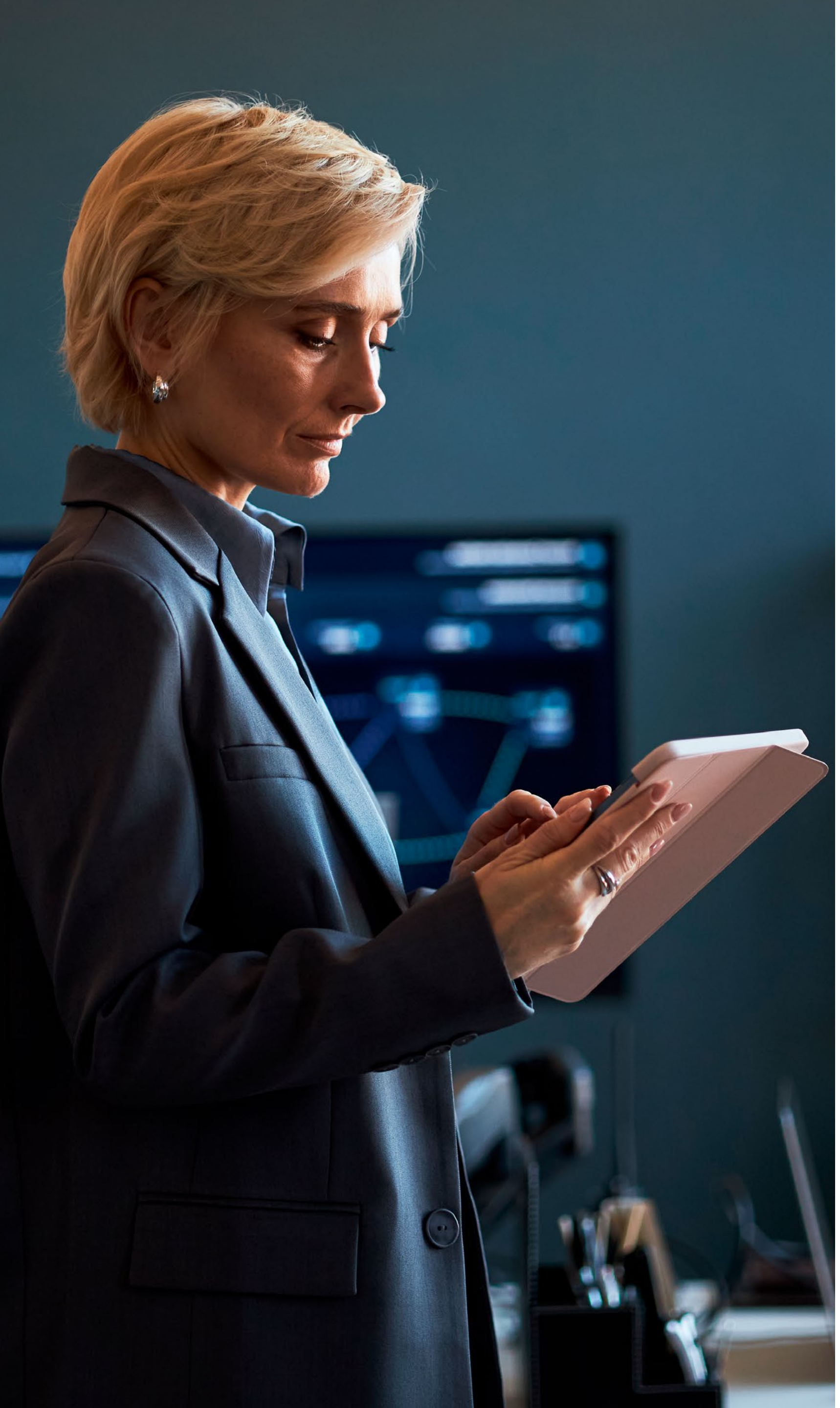


Table of contents

Executive summary

Global Business Services (GBS) has evolved from a cost-efficiency operation into a strategic enterprise hub. As GBS organizations expand in scope, scale, and digital enablement, they face greater complexity across governance, regulatory compliance, cybersecurity, talent, and operational resilience. This presents an opportunity for Chief Audit Executives (CAEs) and internal audit (IA) functions to contribute both independent assurance and practical advisory input throughout the GBS transformation life cycle. This article outlines the risks in GBS transformation and the ways IA can help management strengthen governance, embed scalable controls, and support sustainable execution.

Evolution of GBS organizations

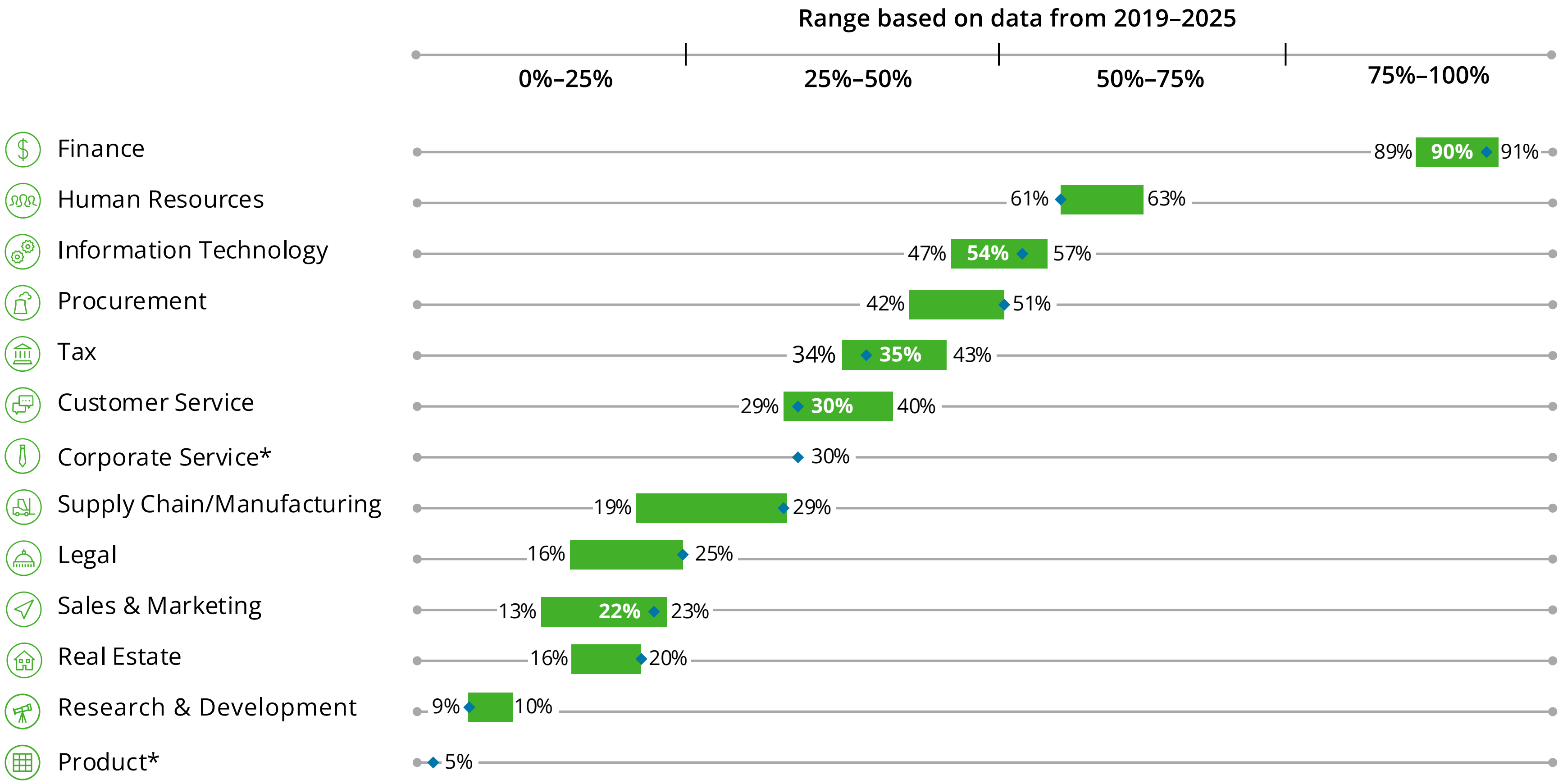
01
02
03
04
05
06
07

GBS organizations—sometimes referred to as Global Capability Centers (GCCs) or Global In-house Centers (GICs)—centralize business services and enterprise capabilities in offshore or nearshore locations. Unlike traditional outsourcing models, they remain owned and governed by the parent organization, allowing for tighter strategic alignment, operational control, and protection of intellectual property. Over time, GBS models have expanded beyond labor arbitrage and transaction processing. Many now are Centers of Excellence (CoE) that support higher-value work across technology, analytics, product development, and enterprise operations, making them increasingly important to business performance and transformation agendas.

Figure 1 reflects the results of a 2025 Deloitte survey on the evolution of GBS organizations, highlighting the percentage of work carried out by GBS organizations across different functions.

Evolution of GBS organizations (cont.)

Figure 1: GBS organizations enhance scope, expanding from traditional to specialized functionst



*Note: Option not available in previous surveys.
Corporate Service includes internal business support services such as communications, employee safety, etc.

- The **three traditional GBS functions**—Finance, HR, and IT—demonstrate continuous momentum to deliver in GBS
- GBS organizations have started to deliver **complex functions that require heavy interactions like legal, corporate services, supply chain/ manufacturing support, indicating a continued elevation of GBS organizations' roles as strategic partners** to the business.
- While other functions remained steady, procurement, supply chain/manufacturing and real estate functions are increasingly integrated in GBS scope.

Transitional risks and challenges in GBS establishment and transformation

Evolving GBS organizations involves risks and challenges that are constantly changing, especially as these centers operate across borders and include strategic roles. As they evolve, they face a wide range of financial, regulatory, technological, and people-related risks, all of which grow more significant in times of change.

- **Operating model:** Operating model risk arises when GBS organizations are hindered by misaligned global and local priorities, complex governance across geographies, regulatory and vendor dependencies, and difficulties standardizing processes and technology—often leading to inconsistent execution, operational bottlenecks, compliance exposure, inefficiencies, and higher costs.
- **Governance and regulatory compliance:** These risks arise when GBS organizations must navigate diverse and rapidly evolving cross-border requirements, including data privacy, tax, transfer pricing, labor, permanent establishment (PE), and financial governance standards. This highlights the importance of monitoring regulatory change closely, embedding local compliance early, and establishing strong governance structures to meet rising reporting expectations and avoid fines, business disruption, and reputational harm.
- **Operational resilience:** As GBS organizations take on more critical processes and infrastructure, operational resilience has become a strategic necessity. Disruptions such as geopolitical instability, natural disasters, supply chain shocks, pandemics, and energy shortages have exposed the vulnerabilities of centralized or single-region delivery models, making diversified locations, strong business continuity capabilities, and regularly tested disaster recovery plans essential. Resilience is not just a compliance safeguard; it is fundamental to protecting enterprise value, sustaining operations, and enabling long-term growth and innovation.

Transitional risks and challenges in GBS establishment and transformation (cont.)

- **Cybersecurity:** As GBS organizations handle more sensitive data and critical digital operations, they become increasingly exposed to cyber risk. A breach can disrupt essential functions, create regulatory issues, and damage customer trust—especially in highly regulated sectors. As artificial intelligence (AI), internet of things (IoT), cloud, and automation expand the attack surface, organizations need stronger security controls, effective incident response, and ongoing resilience testing. Recent cyber incidents—and regulations such as the European Union's (EU) Digital Operational Resilience Act (DORA) and updated US breach reporting laws—further reinforce the need for zero-trust models and advanced threat monitoring.
- **Talent management:** Talent management is a growing challenge for GBS leaders as competition rises for skills in AI, machine learning (ML), cybersecurity, product management, and data science. Technology and market shifts are driving wage inflation, attrition, and constant upskilling across both established and emerging hubs. Organizations must hire and integrate talent at scale while supporting retention, development, and cross-cultural collaboration. Remote and hybrid work, rising demand for digital skills, and the need for tech-savvy generalists have made talent strategies more complex and increased the need for continuous learning and culturally aware integration.
- **Cultural integration and change management:** Strategic and cultural misalignment can create meaningful risks for GBS centers, since success depends on integration with the parent organization's strategy, processes, and values—not just technical capability. These risks increase when leadership sponsorship is not visible through senior engagement, strong GBS roles, and culture-building mechanisms. Without that support, teams can drift from enterprise priorities, leading to "us versus them" dynamics, slower decisions, inconsistent execution, and retention challenges. The impact is often greater during rapid growth, technology transformation, or leadership transitions.

In summary, the risk landscape for GBS organizations is shaped by strategy and reimagined operating model alignment, regulatory scrutiny, cyberthreats, talent pressures, operational demands, and cultural factors. Addressing these requires resilient control governance, agile risk management, and coordinated oversight supported by analytics, scenario planning, talent development, and inclusive governance.

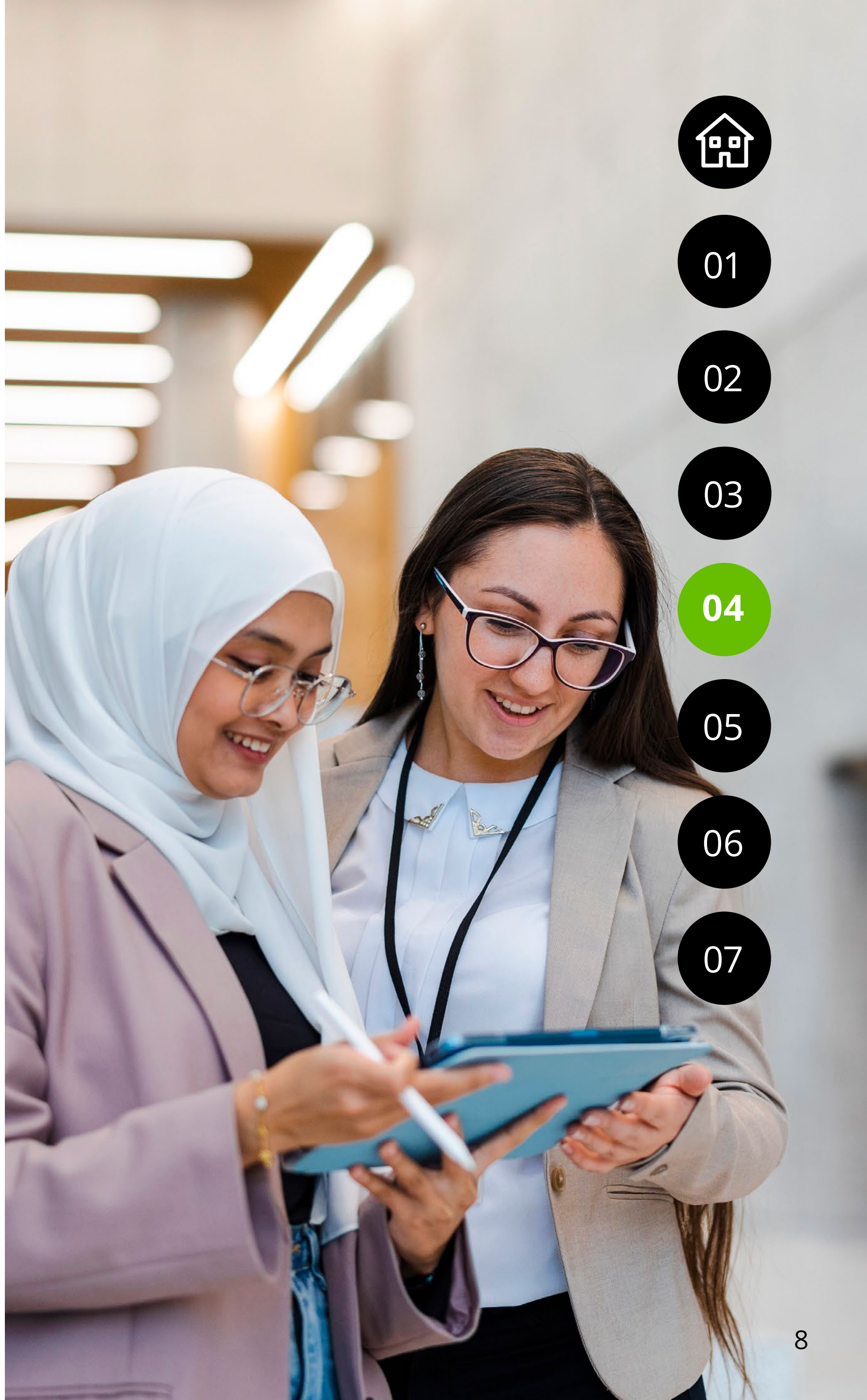
Redefined operating model for IA function

As organizations scale GBS, the IA operating model should be restructured. IA is moving beyond a centralized construct toward a hybrid model: a strong base-location team complemented by audit professionals embedded in, or tightly connected to, GBS centers. The intent is not incremental coverage; it's a structural shift that enables IA to operate with greater speed, consistency, and reach as enterprise processes globalize and digitize.

In this model, proximity to GBS operations changes IA engagement. With aligned time zones and connectivity to GBS leaders, IA can provide real-time advisory input; keep pace with in-flight process changes; and reduce latency between risk signals, decisions, and action, supporting transformation without slowing it down.

The hybrid approach broadly reframes how IA delivers outcomes in complex operating environments. It expands access to specialized capabilities (e.g., cybersecurity, AI-enabled analytics, and continuous auditing) and creates the foundation to scale automation, AI-enabled audit platforms, and risk analytics across the function. It also strengthens global execution through integrated workflows, standardized methods, and clearer handoffs, reinforcing consistent quality.

Finally, the hybrid construct provides practical capacity elasticity. It supports flexible staffing models, targeted upskilling and cross-training, and on-demand surge resourcing during elevated-risk periods (e.g., mergers and acquisitions, regulatory change, and major system implementations). By embedding IA closer to operational workflows and enabling follow-the-sun coverage, the function can surface emerging exposures earlier, accelerate remediation cycles, and validate control improvements more quickly, strengthening both risk responsiveness and the staying power of corrective actions.



CAE and IA departments: Strategic role in GBS transformation

01

02

03

04

05

06

07

Early-stage strategic advisory and transition planning

IA functions can help to maximize their impact by engaging early in the GBS transition life cycle. Early involvement allows IA to contribute to scenario planning, risk assessment, and the design of governance frameworks that align with organizational objectives. By participating in transition steering committees and cross-functional working groups, IA can insert risk, compliance, and control considerations from the outset, reducing the likelihood of costly remediation and operational disruptions post-implementation.

This proactive engagement positions IA as a thought partner for leadership, enabling real-time recalibration of risks and controls as strategies evolve. IA's early participation in the design and fit-gap analysis phases allows for the identification of legacy process risks, system cutover strategies, and the establishment of reporting and escalation pathways. Engaging the CAE in transition planning moves IA from a watchdog to a co-architect of the future operating model, shaping the control environment and operational blueprint through scenario modeling and facilitated workshops. Crucially, IA maintains its objectivity through this process by serving as a strategic adviser rather than a decision-maker, ensuring that while it provides the blueprint for a resilient control environment, management retains full ownership of its execution.

CAE and IA departments: Strategic role in GBS transformation (cont.)

Assurance by design

One of IA's highest-value contributions is helping management embed scalable controls during process, technology, and operating model design. Because GBS environments centralize standardized, high-volume activities, they provide a strong opportunity to build preventive, automation-enabled controls into the future-state model rather than retrofit them after go-live. IA can provide independent challenge and practical input on process flows, approvals, monitoring logic, and control ownership so that governance and control expectations are addressed early. Participation in process-mapping workshops and system blueprint reviews allows IA to advise management—while maintaining independence—on whether proposed controls, governance choices, and escalation paths align to the organization's risk appetite and regulatory obligations. This is particularly important during enterprise resource planning (ERP), automation, and broader digital transformation, where poor control design can scale inefficiency as quickly as it scales performance.

CAE and IA departments: Strategic role in GBS transformation (cont.)

Change management, knowledge transfer, institutional learning, and performance monitoring

GBS transitions often involve major workforce shifts, process redesign, and new control structures, making effective change management and knowledge retention critical to long-term success. IA can support these efforts by advising on change frameworks, readiness assessments, training, communication, and the alignment of governance, incentives, and performance metrics to reinforce adoption of new processes and controls. IA can also provide input on establishing scalable compliance and QC capabilities, including governance, roles and responsibilities, escalation paths, testing methodologies, performance metrics, and reporting, while helping embed quality and compliance checkpoints into end-to-end processes to strengthen first-line ownership and reduce rework. As transitions progress, IA can promote stronger knowledge transfer through documentation, cross-training, mentorship, shadowing, and knowledge management practices so that critical process knowledge, control ownership, and lessons learned are retained despite turnover, mobility, or outsourcing. Post-transition, IA can monitor the effectiveness of processes, controls, and governance through periodic reviews, data analytics, KPI tracking, dashboards, and automated alerts, helping identify deficiencies and improvement opportunities early. Ongoing CAE engagement in governance forums further supports continuous improvement, timely reporting, and recalibration as business, regulatory, and operational needs evolve.

Cybersecurity and data protection

IA should rigorously evaluate the organization's cybersecurity frameworks, data privacy policies, and incident response plans with a focus on offshore data controls and adoption of organization policies. IA should confirm these measures are thorough, are aligned with global standards, and are subject to regular testing and updates.

CAE and IA departments: Strategic role in GBS transformation (cont.)

Risk-based internal audits

IA should play the role of an assurance and advisory partner throughout the GBS transformation—first by providing independent assurance that risks are identified, controlled, and governance is working, and later by validating that the established GBS operates with effective controls, compliance, resilience, and performance.

- **GBS setup/expansion phase (figure 2):** In the setup or expansion phase, IA typically focuses on governance, risk management, control design, third-party and technology risks, regulatory readiness, and "control-by-design"—confirming that GBS operating model, process design, and enabling technologies embed the parent organization's policy and standards.
- **Steady state (figure 3):** Once the GBS's are established, IA shifts to operating effectiveness, continuous risk coverage, optimization, and thematic audits across business processes, IT, compliance, strategic alignment, and financial integrity—specifically assessing policy implementation and ongoing compliance through testing, data analytics, and ongoing monitoring to keep pace with scale and change.

CAE and IA departments: Strategic role in GBS transformation (cont.)

Figure 2: GBS setup and expansion phase

Process audits

- Process design assurance (control by design)
- Transition audits
- Policy/standard operating procedures (SOP) review
- Third-party operating model
- HR onboarding and workforce process readiness audits

IT audits

- Technology architecture design
- Identity and Access Management (IAM) design
- Software development life cycle (SDLC)/change management design
- Data migration and integration controls
- Cybersecurity baseline and secure configuration standards
- IT service management design
- Business continuity/disaster recovery design and test plan review
- Vendor/managed service controls design

Regulatory compliance

- Regulatory applicability and compliance readiness assessment
- Data privacy readiness
- Information security policy alignment and control mapping
- Records management and legal hold readiness
- Export control / sanctions screening process design
- Licensing and statutory compliance setup
- Ethics and whistleblower/ incident reporting mechanism readiness

Strategic audits

- Business case and benefits realization framework review
- GCC location strategy and site risk assessment
- Governance model design
- Culture, change management, and communications readiness review
- Key performance indicators (KPIs)/service level agreement (SLA) framework design and performance reporting integrity

Financial audits

- Budgeting and capitalization approach review
- Intercompany/transfer pricing design readiness
- Chargeback/showback model design and billing controls
- Procurement and contracting controls
- Payroll/expense design controls
- Controls over financial reporting

Note: The audits listed above represent recommended internal audits based on leading practices and not an exhaustive list. Additional audits may be required to be included based on organizations' specific risk, priorities, and operating environment.

CAE and IA departments: Strategic role in GBS transformation (cont.)

Figure 3: GBS steady state

Process audits

- End-to-end process audits (e.g., record-to-report, procure-to-pay, order-to-cash)
- SLA performance management and service quality audits
- Operational controls testing
- Master data management and data quality governance audits
- Quality management/ continuous improvement governance
- Workforce operations audits
- Third-party performance and contract compliance audits

IT audits

- Cybersecurity operations audit
- IAM operating effectiveness
- Change management and release management operating effectiveness
- ITSM operations audits (incident/problem/ change; SLA adherence)
- Data governance and analytics controls
- Cloud governance and security posture audits
- Resilience audits (BCP/DR tests executed, RTO/RPO achievement, crisis management)
- Application controls/ interface controls audits for key systems

Regulatory compliance

- Ongoing data privacy compliance
- Compliance monitoring program effectiveness
- Regulatory reporting process assurance
- Ethics and conduct program effectiveness
- Anti-bribery/ anti-corruption (ABAC) and third-party due diligence effectiveness
- Industry-specific compliance audits (e.g., financial services, health care etc.)
- Physical security and facilities compliance audits
- Compliance to local laws and regulations

Strategic audits

- Benefits realization audit (actuals vs. plan; leakage; corrective actions)
- Governance effectiveness audit
- Strategic alignment audit
- Operating model maturity assessment
- Major transformation/ expansion assurance
- Talent strategy and succession/critical role risk review

Financial audits

- Intercompany transactions and transfer pricing compliance
- Chargeback accuracy and dispute management controls
- ICFR operating effectiveness
- Cost management and unit economics reporting integrity
- Treasury/cash controls
- Procurement savings realization and contract leakage audits
- Fraud risk assessment and fraud analytics

Analytics-driven continuous control monitoring across each of the audit categories

Note: The audits listed above represent recommended internal audits based on leading practices and not an exhaustive list. Additional audits may be required to be included based on organizations' specific risk, priorities, and operating environment.

Conclusion

The journey to establish and transform a GBS is fraught with risk, but it also presents immense strategic opportunity. CAEs and their IA departments should be positioned not only as an independent assurance function, but as a value-creating partner to broader GBS leadership, helping embed “control-by-design,” strengthen governance and decision rights, and accelerate confident execution across process, technology, third-party, and regulatory change. By staying close to transformation priorities while maintaining independence and objectivity, IA can provide timely, credible assurance to the audit committee and the board that emerging risks are proactively identified and addressed; controls are evolving in step with growth; and operating performance and resilience remain strong through periods of disruption.

Organizations that tightly align their audit, risk and transformation capabilities will not only sidestep pitfalls, but also unleash the full potential of the GBS as a catalyst for sustainable enterprise value.

01
02
03
04
05
06
07

Get in touch

Contact Deloitte today to learn how our tailored internal audit services can help you achieve your goals and build a more resilient, efficient GBS organization.

Michael Schor
Internal Audit Offering Leader
Audit & Assurance Partner | Deloitte & Touche LLP
+1 212 436 6208
mschor@deloitte.com

Nafees Ahmed
Managing Director
Audit & Assurance | Deloitte & Touche LLP
Assurance and Enterprise Risk Services India Private Limited | Offshore IA Offering Leader
+1 470 434 8740
cahmed@deloitte.com

Amit Nakra
Senior Manager
Audit & Assurance | Deloitte & Touche LLP
Assurance and Enterprise Risk Services India Private Limited
+1 678 249 2214
amnakra@deloitte.com