Optimization of IT internal audit coverage within the financial services industry

The value of a seat at the table

EY

Building a better working world

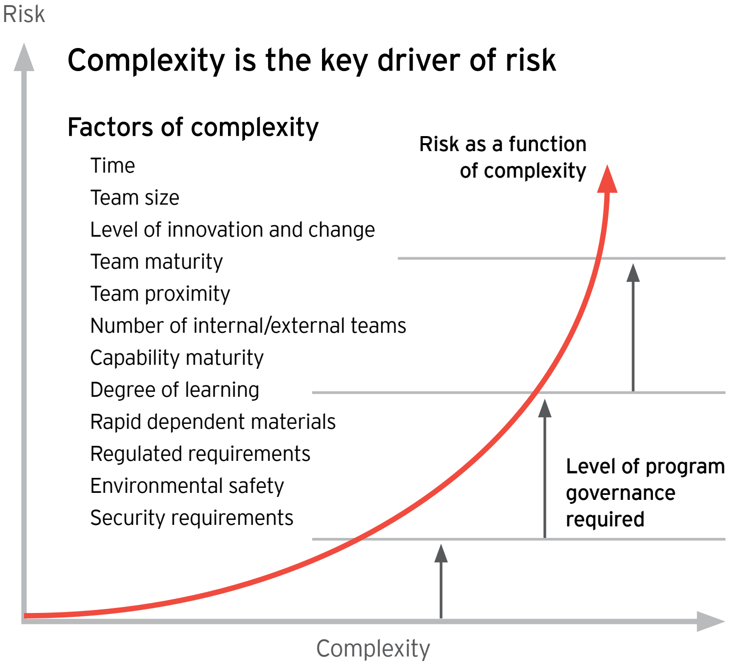
Optimization of IT internal audit coverage within the financial services industry

The value of a seat at the table

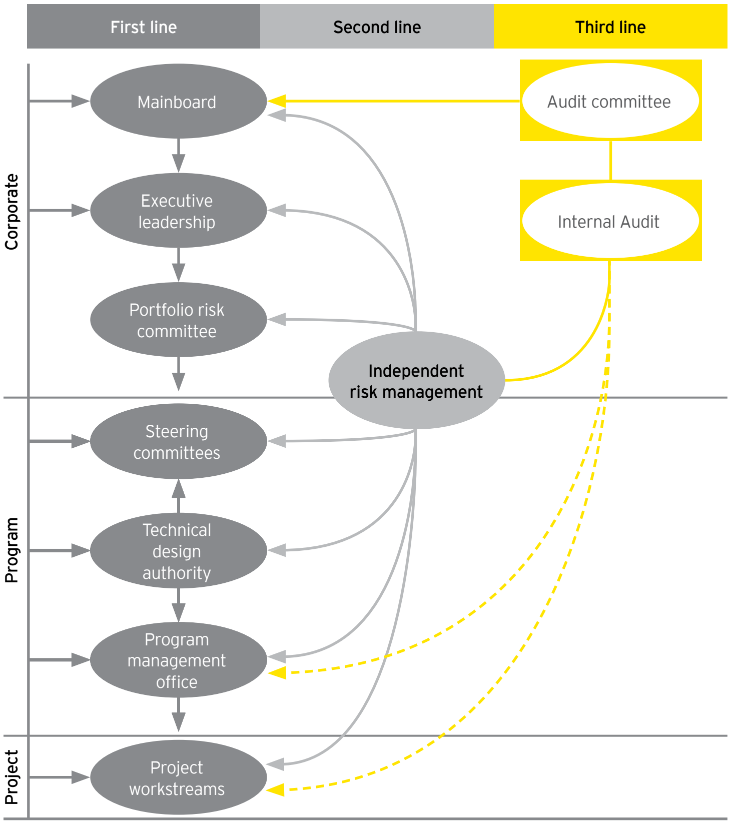
Overview

Within the financial services industry, strategic and transformational initiatives continue to present significant risk to organizations. The complex interconnectedness of today's systems, ever-changing business requirements among various stakeholders, and the constant time pressures for production releases are factors that elevate exposure to all key stakeholders within an organization. Although Audit Committee and Board of Director attention toward regulatory scrutiny (e.g., SEC, Fed, OCC, CFPB), business strategy and the operating model is influenced by the portfolio of system initiatives (specifically due to the potential reputational ripple effects of disjointed initiatives both internally and externally), the degree of Internal Audit's continuous monitoring coverage has inconsistently aligned with this shift in focus.

Internal Audit serves as the third line of defense and the backbone to promote control effectiveness and validate control adherence within organizations. Therefore, Internal Audit has a distinctive vantage point to maximize previously established relationships and synergies across various departments. Due to the responsibilities and positioning of Internal Audit within the organization, Internal Audit possesses a unique opportunity to obtain and provide visibility regarding prior, current and future system initiatives with limited resistance from key stakeholders. Internal Audit may implant itself within critical governance, steering committee and strategy meetings to remain abreast and aware of the portfolio of technology and business activities that may warrant Internal Audit's attention. Internal Audit may profile the inventory of initiatives to determine the optimal level of involvement at varying periods within the life cycle (e.g., prior to deployment, following deployment or via continuous monitoring) based upon the nature, risk and downstream implications of the system initiative.



Lines of defense



Although system initiatives may be categorized as "technology-related," the catalyst for system initiatives is frequently a result of business demands regarding enhanced functionalities and decommissioning of legacy infrastructure replaced by innovative, cost-effective operating models. Additionally, minimal key milestones within a system initiative are truly "technical" in nature beyond pure coding efforts and unit testing performed by developers. However, the current efforts that leverage technology enablement often lack the recommended resources, competencies and rigor to address the increased internal and external pressures to realize the benefits from proposed major programs.

- 73% of executives believe their businesses are increasingly challenged to assess risks and returns of major programs.
- Greater than 50% of executives believe that corporate effectiveness is constrained by a lack of delivery effectiveness in major programs.
- One in six projects experience an average schedule overage of almost 70% and cost overage of 200%.
- 31% of projects are canceled, 53% of projects underperform and 16% of projects are deemed a success.

Sources: MORI Captains of Industry, EY CBK, Dept. of Trade & Industry, Standish Group International and Harvard Business Review 2011

If managed proactively, Internal Audit can play an instrumental role to foster governance and address the needs and concerns of the two categories of constituents "interested" in the progress of system initiatives and the effectiveness of risk mitigation measures enforced — assessors and stakeholders. Recent trends have demonstrated an increased appreciation and involvement for Internal Audit to embed independent, objective perspectives at critical quality junctures, specifically system initiative milestones "analyze and design" and "test." Internal Audit's challenges related to analysis and design (e.g., process/control design, security integrity for applications/infrastructure/ data) and testing (e.g., data conversion, regression, report, system integration) in real time present opportunities for remediation of identified exposures prior to production deployments.

Program confidence elements during technology-enabled initiatives

Confidence element	Key questions
Program governance	Does the business case have integrity? Are the appropriate governance, change and decision-making processes in place, and are they performed effectively? Is sponsorship obtained prior to and throughout the investment?
Project management	Are the appropriate processes in place for the program to be planned, managed, and tracked effectively? Are the appropriate resources, quality, risk and communication processes in place?
Functionality integrity	Is the technology initiative and its supporting infrastructure/interfaces tested, validated and prepared for production deployment?
Data integrity	Is the financial and business data that drives business processes and management information reporting tested, validated and prepared for production deployment?
Business readiness	Are the new business operating models, processes and controls tested, approved and prepared for production deployment? Is the organization and its people trained and ready to use the new technology?
Regulatory readiness	Is the technology initiative in compliance with key financial services regulations (e.g., Dodd-Frank, Basel)?
Support readiness	Are the support organization, processes and tools ready to utilize the new technology?
Post-deployment	Are the activities to support post-deployment, sustainability and adoption of the technology established? Is the return on investment achieved, and are monitoring mechanisms established to determine value?

Visibility and risk matrix

		Degree of visibility desired								Primary concerns
Key assessors	Regulators	Moderate-low	Moderate-low	High	Moderate-low	High	Low	High-moderate	High-moderate	Integrity, consumer protection, availability
	External audit	Moderate-low	Moderate-low	High	Moderate-low	High	Low	High-moderate	High-moderate	Governance, controls, financial statement impacts
	Audit Committee/ Board of Directors	Moderate-low	Moderate-low	High	Moderate-low	High	Low	High-moderate	High-moderate	Governance, communication, return on investment, availability
	Internal Audit (third line of defense)	Moderate-low	Moderate-low	High	Moderate-low	High	Low	High-moderate	High-moderate	Governance, controls, methodology
System initiative milestones		**Strategize**	**Plan**	**Analyze and design**	**Develop**	**Test**	**Train**	**Deploy**	**Post-go-live**	–
Key stakeholders	Enterprise risk management (second line of defense)	High-moderate	High	High	Low	High-moderate	Moderate-low	Moderate-low	Moderate-low	Governance, controls, methodology
	Business (first line of defense)	High-moderate	High	High	Moderate-low	High	High-moderate	High-moderate	Moderate-low	Functionalities, budget, return on investment, availability
	Technology (first line of defense)	High	High	High	High	High	Moderate-low	High	High-moderate	System requirements, data migrations, change management, resourcing, availability
	Business and technology compliance	Moderate-low	High-moderate	High	Low	High-moderate	Low	Moderate-low	High-moderate	Regulatory compliance
	Project management office	High-moderate	High	High-moderate	High-moderate	High	Moderate-low	High	High-moderate	Governance, timeliness, resourcing, interdependencies

Differentiators

System initiative milestones – key questions

- **Strategize** – Have key executives undergone a robust analysis to rationalize the driver(s) for the system initiative, software package selection (if applicable), competencies required and the timeline definition?
- **Plan** – Has the project team developed a project plan, risk register, competency matrix, budget, timeline and detailed business/functional/technical specifications?
- **Analyze and design** – Has the project team evaluated gaps in the current business process and functionalities, established solutions for those gaps, and determined/documented configurations and customizations that consider future-state controls that address security, architectural, regulatory and operational concerns?
- **Develop** – Has the project team created the required configurations, customizations and development to align with the business/technical/functional specifications?
- **Test** – Has the project team and user community performed detailed testing (e.g., stress, regression, performance) to validate that the functionalities are operating as intended and align with the business/functional specifications?
- **Train** – Has the project team documented procedures for usage of the new functionalities for the user community and future maintenance efforts? Has the previous business process documentation been updated accordingly to address new functionalities?
- **Deploy** – Has the project team conducted the cutover from the legacy system to the new system initiative following approval from key stakeholders?
- **Post-go-live** – Has the project team defined a strategy for issue management, support and maintenance following the new system initiative? Has an evaluation been performed to assess the satisfaction of key stakeholders?

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE No. CK0831
CSG No. 1405-1248184 NE
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

Key messages

- Identify key recurring meetings where IT Internal Audit should participate to understand strategic, transformational initiatives and promote a risk culture
- Challenge the current IT Internal Audit competencies and bandwidth (refer to Exhibit A)
- Establish a risk-based approach and methodology to consistently determine level of effort dedicated to proactively monitor system initiatives and enhance real time reporting
- Improve coverage over emerging risks rather than historical risks
- Align Internal Audit with ERM to reconcile risk taxonomies and maximize synergies created by the lines of defense model

Exhibit A

Traditional focus (competencies fully internal)
Identity access management
Change management
IT operations/job scheduling/backup and recovery
IT governance
System development life cycle
Service level management
IT asset management
Problem management
Program and project management
Segregation of duties
Emerging focus (competencies partially internal)
Business continuity/disaster recovery/crisis management
Vendor risk management
End-user computing
Surveillance (AML/BSA)
Mobile security/bring your own device
Cloud computing
Cybersecurity/attack and penetration
Data privacy and classification
Model risk management/stress testing/scenario analysis
Enterprise risk management
Anticipated focus (competencies primarily outsourced)
IT strategic management
Electronic trading
Big data/data quality
E-banking/mobile banking and applications
Enterprise architecture
Virtualization (Citrix/VMware)
Security event management/intrusion detection
Software licensing and contracting
Threat and vulnerability management/cyber crime operations
Data loss prevention