

IT Risk Office

Improving Risk Management Efficiency and Effectiveness

TEAM

Advisor: Bill Kobel (Partner, Security Services, Deloitte & Touche LLP)
Vikram Bhat (Sr. Manager, Security Services, Deloitte & Touche LLP)
Phillip McMurray (Manager, Controls Assurance, Deloitte & Touche LLP)
Pooja Daswani (Sr. Consultant, Security Services, Deloitte & Touche
LLP)

Daria Lapshinova (Consultant, Internal Audit, Deloitte & Touche LLP)
Ashwini Doshi (Consultant, Controls Assurance, Deloitte & Touche LLP)

IT Risk Office Improving Risk Management Efficiency and Effectiveness

Executive Summary

The current risk and regulatory environment, rapid pace of technology advances and constrained investments are challenging traditional IT risk management processes. A centralized IT Risk Office (ITRO) and new approaches such as a Risk Catalog, Risk/Cost prioritization models and operations oriented risk processes provide effective solutions to improve the efficiency and reduce the costs of risk management.

Why this, Why Now?

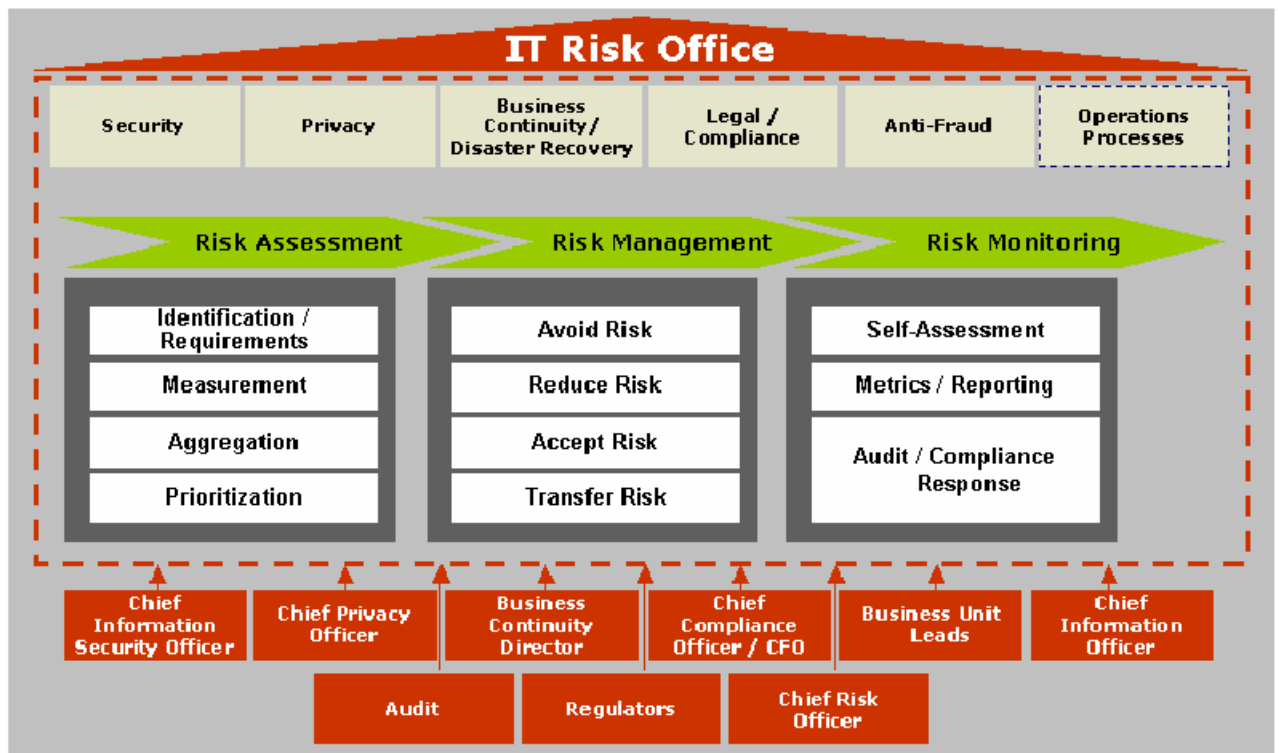
The events of the last decade such as 9/11 and regulatory changes such as Basel II and Sarbanes-Oxley have significantly altered the risk tolerance view of the Board and Senior Management. At the same time, technology innovations and new business models are exposing organizations to increasing risks (e.g. Phishing, data leakage, off shoring, etc.). Cost pressures have further complicated the landscape. Companies are being forced to “do more with less”. The combined effects of increased risks, lower risk tolerance and constrained investments are challenging traditional risk management approaches. The net result is that although organizations are diverting prized

dollars and resources into IT Risk Management, they are having minimal success in dealing with risk and compliance matters. Typical indicators of the current state include: the lack of an aggregated, prioritized view of enterprise risks; the lack of clear responsibility and process to define organizational risk tolerance; misinterpretation of risk requirements; inability to respond to risk requirements; excessive spend on audit; periodic confrontations with auditors and regulators, etc.

To address these issues, organizations should consider establishing an IT Risk Office and implement new approaches to streamline traditional processes and reduce the costs of risk and compliance activities.

IT Risk Office – What do I do, How do I get there?

An example of an IT Risk Office framework that organizations can implement is depicted below. This example builds upon industry models such as the COSO Enterprise Risk Management, ITIL, ISO 17799/27002, etc. It is flexible to be adapted to the size and complexity of the organization.



There are two main components:

1. The IT Risk Office, i.e. the Governance structure and,
2. IT Risk Processes – Risk Assessment, Risk Management and Risk Monitoring

IT Risk Office – Governance

The IT Risk office is the governance structure that implements IT risk management across the organization. This office can either be a virtual organization or a new organization created through the merger of existing Information Security, Privacy, Business Continuity, and Legal/Regulatory Compliance organizations. The IT Risk Office is also a critical component of the overall Enterprise Risk management (ERM) framework of the organization. The latter, is broader, and includes other risk categories such as Strategic Risk, Financial Risk, etc. The IT Risk Office coordinates with the various business units, executive management, the Board of Directors and the Auditors to define the organizational risk culture and establish the management oversight from a technology perspective. In most cases, the IT Risk Office serves as a partner/advisor to business executives on technology risks but in some cases may need to act as the enforcer of organizational views on risk mitigation. This typically happens when franchise risk objectives are at crossroads with particular business unit objectives, especially their appetite for risk management investments.

To lead the IT Risk Office, some organizations are creating a new role called Chief Information Technology Risk Officer (CITRO). He/She is a Senior Executive and reports to the CIO (Chief Information Officer) or

the technology CAO (Chief Administrative Officer). This individual has overall responsibility for making management decisions on risk tolerance, working with other organizational stakeholders. The CITRO complements an organizations' Chief Risk Officer who is predominantly focused on Financial Risk Management.

IT Risk Processes – Implementing New Approaches to Traditional Processes

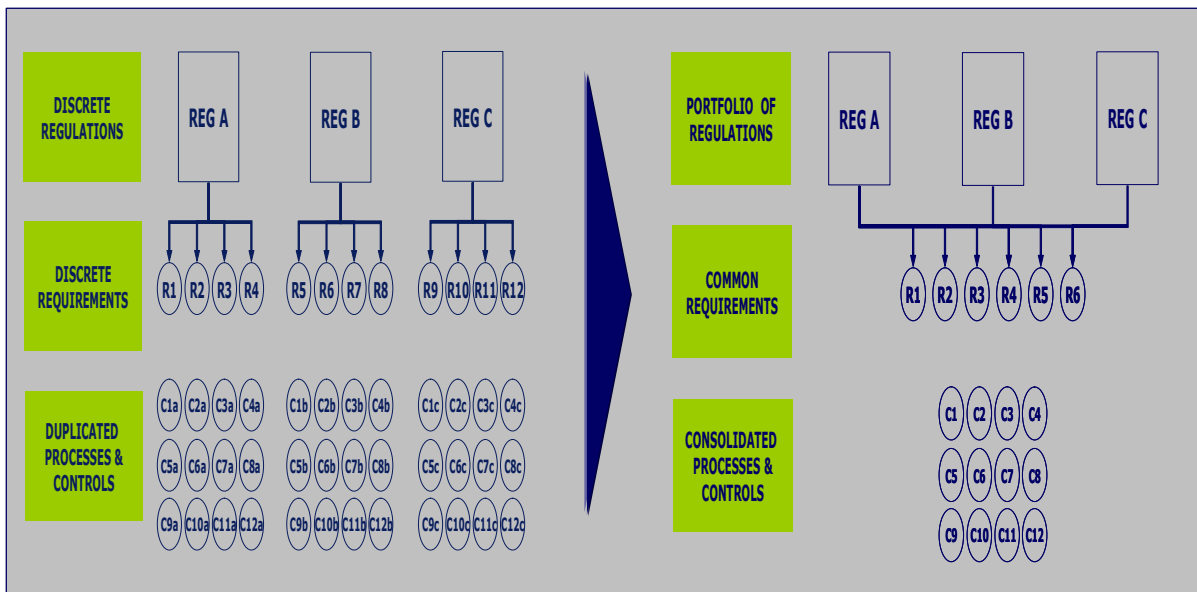
Risk Assessment

The IT Risk Office should consider implementing a Risk Catalog to improve the efficiency and effectiveness of the Risk Assessment process. A Risk Catalog is a common set of risk requirements (derived from multiple authoritative sources) and applied against a standard reference architecture (like an ITIL Configuration Management database). Examples of the sources of risk requirements include:

- Threat Scenarios – Phishing, Data leakage, outsourcing, off shoring, data confidentiality, tape loss, loss of confidential data, privacy violations, etc.
- Regulations (Basel II, OCC Bulletins, FCRA, FDIC Rules, FFIEC, etc.)
- Common Practices (AICPA/CICA Privacy Framework, CobiT, ISO/IEC 17799, etc.)
- Standards (American Express, Discover, Visa PCI, etc.)

- State Laws (New York Inf. Security Breach and Notification Act, SB 60453, SB 1386, etc.)

The resulting common requirements are prioritized based on a risk/cost based prioritization model. The benefits of the Risk Catalog and prioritization model are that they significantly eliminate the duplication of effort and reduce the workload on IT staff. (See Figure below). More importantly, they allow management to develop an understanding of enterprise risks, decide on the acceptable level of risks and provide required investments for risk mitigation.



Risk Management

Risk Management involves the implementation of controls against the prioritized risks. The key to improving the risk management efficiency and effectiveness is to move from a compliance-based approach to an

operations oriented, standards based ongoing management process. In the latter approach, the operations organization (via the IT Risk Office) proactively assumes the responsibility for risk management and incorporates risk and control activities into the business-as-usual processes such as Change Management, Configuration Management, Service Availability, Systems Development Lifecycle (SDLC), etc. They rely on standards such as ITIL, ISO 27002, etc. to drive standardization and simplification and thus tackle many of the risk issues at the root cause level. (An example of such an implementation is that SDLC standards should include business continuity, security controls and all applications should be checked for the strength of these controls during pre-deployment testing.)

Architectural standards are also important mechanism through which an IT Risk Office drives efficiency and effectiveness. Typically, an IT Risk Office creates and maintains architectural standards for its core areas of responsibilities, namely Information Security, Privacy, Business Continuity, Legal/Regulatory, and Anti-Fraud. The use of such architectural standards allows new risk requirements to be addressed in a manner consistent with the existing technical operating environment and processes. It promotes consistency of tools, interfaces and processes which allows various elements within the organization to interact smoothly. An example of such an architectural

standard implementation is the Enterprise Security Reference Architecture (ESRA). An ESRA defines the manner in which the organization plans to address its information security requirements – perimeter defense, identity management, data protection, etc. Therefore, any new requirement (security or otherwise) gets addressed in the context of the ESRA, thus reducing the time to market for solution design and delivery.

However, the most important role that an IT Risk Office can play to drive efficiency and effectiveness is to develop a forward looking roadmap that integrates risk management with operational plans and enterprise cost reduction strategies. In our experience, synchronizing these activities creates a very powerful business case. Examples of such implementations include the resolution of proximity risks through data center consolidations, deployment of thin client technology to eliminate desktop related risks, hardware level tape encryption to mitigate tape loss, etc. This integration of risk and operations addresses the issue of inadequate funding, since risk management becomes a small incremental component of the overall business requirements and funding requests. In addition, the roadmap provides a powerful communication tool with senior management, auditors, regulators and other stakeholders regarding organizational plans to address risks in a proactive manner.

Risk Monitoring

Risk Monitoring is the last step in the closed-loop IT Risk Office process. At a minimum, the monitoring processes should include self-assessments, metrics, and audit/compliance related reporting. Automation tools for assessments and reporting are coming to the forefront. Many IT Risk Offices are also using risk management dashboards to create accountability and drive performance improvements. Example of metrics being tracked include “number of high risks”, “number of risks resulting in outages”, “outage time due to security incidents”, etc.

Lessons from the Trenches

Our experience in implementing an IT Risk office and related risk management processes has resulted in some key lessons.

1. IT Risk Management is a serious business. There are numerous examples of CIO’s and other senior executives being fired for not having an effective IT Risk Office and/or IT Risk Management processes.
2. Although global institutions have suffered some financial loss, the major drivers for establishing an IT Risk Office are franchise

protection, reducing risk management costs and streamlining risk processes.

3. Risks need to be evaluated and prioritized at a management level - with a financial business case and risk ranking. Otherwise, costs get rapidly out of control when junior staff applies a broad interpretation of risks.
4. While there are many legal and regulatory directives, there is limited specific guidance from regulators worldwide. Organizations, through their IT Risk Office, must decide whether to address the “spirit” or “just the letter” of the directives.
5. Ensuring the integrity of the technology environment is no longer an option; it is a core business requirement.

Conclusion

The rapid adoption of technology and the current corporate risk tolerance climate require organizations to proactively manage technology risks. Global organizations should consider implementing an IT Risk Office to improve the efficiency and effectiveness of their risk management processes. A well-run IT Risk office will lower risk management costs and improve the organizations ability to manage risks.