Three Lines of Defense to Enhance Technology Risk Management Maturity

Abstract

Increasing reliance on technology has added to high complexity of the risk landscape, making risk management and governance a huge challenge for senior management and boards. Enterprises therefore need to adopt a holistic risk management approach to enhance the maturity of their technology risk management capabilities. The Three Lines of Defense (LoD) model is often used to streamline the risk management process, which results in effective risk governance, management, and assurance.

The Need for Enhanced Technology Risk Management Maturity

The Technology Risk Management (TRM) capability of an enterprise indicates its ability to effectively execute core risk management processes, including communication and consultation, context establishment, risk identification, risk analysis, risk evaluation, risk treatment, and monitoring and review.

Enterprises today operate in a regulated and complex business environment and face several challenges related to risk management:

- No enterprise-wide risk management framework or standard is in place.
- Boards and senior management need to be involved in technology risk governance in terms of establishing security and privacy related roles and responsibilities.
- Risk management communication with business units is generally limited to compliance issues.
- Third-party risks may not be adequately assessed or tracked.
- Gaps in policies, processes, and controls may not be identified.
- There is often no overarching Governance, Risk, and Compliance program, resulting in duplication of effort, limited visibility of policy requirements exceptions, and lack of transparency on critical dependencies.

According to research conducted by the Enterprise Risk Management (ERM) Initiative at North Carolina State University, only 25% of the organizations surveyed claimed to have complete formal ERM process in place[1]. This implies a significant opportunity for improvement of ERM processes in most enterprises.

A Holistic Approach Based on Systems Thinking Perspective

A risk management system consists of the risk management framework and processes that are developed based on regulatory requirements and standards as well as inputs from the external environment. The Systems Thinking approach is recommended to look at the interdependence between the components involved in each risk management process and learn how they can work together to enhance risk management maturity.

Enablers of Enterprise Risk Management

The Three Lines of Defense model can be used as a primary means to structure the roles and responsibilities for risk-related decision making and control to achieve effective risk governance, management, and assurance. A close working relationship and proper communication between the three lines is crucial for effective functioning of the model.

First Line of Defense: Lines of Business

Each line of business needs to be vigilant about risk management through these activities:

- **Ensure Situational Awareness:** This entails knowledge of events, as well as being able to model the implications and project current events to predict what might happen. Input should be gathered from all the functions in the business unit, and all relevant channels need to be monitored.
- **Perform Horizon Scanning:** This involves going beyond mere situational awareness to perform a systematic examination of the internal and external environment for weaknesses and gaps, as well as of new and emerging risks that have the potential to affect the organization's performance.
- **Eliminate Single Points of Failure:** The products and services of an enterprise are delivered through a coordinated system consisting of six types of organizational resources: people, technology, information, facilities, supplies, and stakeholders. Vulnerabilities in any of these might make the resource a Single Point of Failure (SPoF) within the system.

The PAS 200:2011 standard has suggested the 'PESTEELO' tool methodology for the purpose.[2] Each letter of the acronym stands for a factor:

P- Political factors
E- Economic or financial factors
S- Social factors
T- Technical factors and issues
E- Environmental factors
E- Ethical factors
L- Legal or regulatory factors
O- Organizational factors

- **Embed Risk Management into Organizational Culture:** Senior management should ensure that risk management processes are integrated into day-to-day business activities and organizational culture, and not seen as a separate activity. The three key means of building a risk-aware culture are senior management support and involvement, creation of risk management check points, and development of risk management competence through training and awareness programs.

Second Line of Defense: Independent Risk Function

An independent corporate risk function needs to promote risk awareness and ensure risk mitigation across the enterprise.

- **Establish Risk Management Accountability:** Risk management roles should be defined, right from the board to the functional level, and accountabilities assigned at strategic, tactical, and operational levels.
- **Integrate Security, Business Continuity, and Compliance Programs with Risk Management:** Most enterprises have specialized business units for security, IT service management, business continuity, compliance, and risk management. Each of these units have their own policies, standards, operating procedures, and supporting tools, which results in duplication of effort and compliance conflicts.
- **Design and Implement Leading Risk Indicators:** Key Risk Indicators (KRIs) are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.[3] A key consideration in defining a leading risk indicator is to think through the chain of events leading to the loss and uncover the root cause.
- **Engage Stakeholders Effectively:** Stakeholders' risk perceptions are driven by their needs and concerns. These factors should be taken into consideration through the continuous process of communication and consultation, both before and after risk decisions are made.
- **Ensure Continual Improvement:** Management should drive continual process improvements through the risk management policy, risk management performance review, internal audits, independent review of risk management processes, as well as frequent communication and management review.

- **Automate Risk Management Processes:** Automation allows enterprises to identify control issues in real time with automatic alerts and remediation, aggregate risks, provide a single view of organizational risks to senior management, and enhance audit efficiencies.

Third Line of Defense: Internal Audit

Two measures help the Internal Audit function provide an effective risk assurance:

- **Adopt a Risk-Based Approach to Auditing:** Often, audits are undertaken for compliance purposes, and do not include analysis of the underlying root causes of the audit findings, as well as their implications. Audits, whether internal or external, should adopt a risk-based approach to uncover the root causes of audit findings and facilitate planning of corrective and preventive actions.
- **Link Audit Planning with Risk Management Initiatives:** The organization's annual audit calendar should align with other planned initiatives within the organization. For instance, a risk management initiative can be followed by an audit, so that the enterprise can obtain independent assurance of the effectiveness of the risk management initiative.

Robust risk management framework and cost-effective risk mitigation measures helped a government organization in Europe achieve a higher risk management maturity level with reduced residual cyber and data privacy risk. It also ensured smooth and continuous operations even in the event of business interruptions. The company also achieved ISO 27001 accreditation well within the mandated time.

Conclusion

With increasing pressure from governments and regulatory bodies on enhancing risk management oversight, enterprises need to invest in advancing the maturity of their technology risk management capabilities. High risk management maturity not only helps reduce the frequency of risk events, but also facilitates smooth business operations with increasing returns. Close collaboration among the Three Lines of Defense helps enterprises improve their risk management capability maturity, create a risk aware culture, and make the enterprise risk-enabled.

References

[1] NC State University, 2016 Report on The State of Risk Oversight: An Overview of Enterprise Risk Management Practices, April 2016, accessed November 2016,

https://erm.ncsu.edu/az/erm/i/chan/library/AICPA_ERM_Research_Study_2016.pdf

[2] The British Standards Institute, PAS 200:2011, Crisis management—Guidance and good practice, September 2011

[3] Committee of Sponsoring Organizations of the Treadway Commission, Developing Key Risk Indicators to Strengthen Enterprise Risk Management, December

2010, accessed May 2016, http://www.coso.org/documents/cosokripaperfull-finalforwebpostingdec110_000.pdf

About The Authors

Rama Lingeswara Satyanarayana Tammineedi

Satya TR heads the Center of Excellence for Fraud Management and Digital Forensics within the Enterprise Security and Risk Management business unit of TCS. He has 30 years of overall IT experience, including 14 years in GRC consulting.

Contact

Visit TCS' Enterprise Security and Risk Management services unit page for more information

Email: Global.esrm@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty. IT Services
Business Solutions
Consulting

All content / information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content / information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted or distributed in any form without prior written permission from TCS. Unauthorized use of the content / information appearing here may violate copyright, trademark and other applicable laws, and could result in criminal or civil penalties. **Copyright © 2016 Tata Consultancy Services Limited**

TCS Design Services | M | 12 | 16