Technological Roles in Enterprise Risk Management; A Summary

The Enterprise Risk Management (ERM) framework is advantageous by design because it provides a strategy for managing all kinds of risk inherent in business applications, and performance objectives. It's use is to make the best of managing all types of risk for the user. Innovative technologies inherently pose a risk to business strategy and these are a key enabler of decision making when creating a business plan. Technology risk management is one of the most prominent examples of enterprise risk management painting the picture of the ERM framework. ERM has a global influence alongside integrated frameworks. It is important to take advantage of due diligence that COBIT5 offers when it comes to innovation that disrupts an enterprises' industry or new technology that may need quality control and oversight.

Governance elements, performance quantification, and internal control are emphasized within the COBIT ERM framework. Any foreseeable events must be reviewed using standards with principles, and any plans to support the undertaking and foresight of the business' strategy should be synergized with structures that operate as closed loop systems. The ERM is currently a closed loop system, sharing objective setting, risk prioritization, information system leverage, monitoring and reporting with other frameworks. In the application of the components, there's not a specific order in which the goals should be met. When risk strategy is monitored under NIST and COBIT5, the approach to it will be comprehensive and all-encompassing to the strategy being undertaken. The COBIT5 Goals Cascade has components that flow downward starting with what the stakeholders need. Stakeholders care about fruition of benefits, resourceful management of risk, and resourceful management of resources. Enterprise, IT-related, and Enabler goals are all used to assess what types of decisions should be made in support of ERM. The chances of successful implementation of technology is higher when using the cascade because it is more likely to be supported from the top down with proven risk management assets.

The ERM is meant to be understood by the board of directors so they can effectively implement the technological processes necessary without adding unnecessary risk alongside the chance that the technology is ineffective or not useful to their enterprises' strategies. Although this board may be effective, ERM professionals are certifiable in cyber security and have a duty to be as accurate and verifiable as possible in their implementation of risk management. The COSO ERM framework used by the professionals utilizes 5 principles that are mapped to COBIT5. Within COBIT5, they are establishing a holistic approach, applying a single integrated framework, covering the enterprise end to end, separating governance from management, and meeting stakeholder expectations and requirements. The COSO ERM principles that these lower level principles map to are recognizing culture, developing capabilities, applying practices, integrating with strategy setting and performance, managing risk to strategy and business objectives, and linking the business strategy to value for the stakeholders. COBIT5 principles are the enablers while the COSO ERM framework derives from COBIT5 implementation.

Risk analysis is one of the technological professions that spans across multiple domains of risk. Quality control objectives and information life cyle processes should support ERM principles that bring different risks together but maintain the level of differentiation across the domains. Both enterprise risk and those who operate and maintain the enterprises' technology should take both COSO ERM and COBIT5 in collaboration and recognize how they can be used beneficially in coordination.

References

Bayuk, J. *Technology's Role in Enterprise Risk Management* ISACA Journal Vol. 2 - Feature www.isaca.org/currentissue