White Paper

Rationalizing Risk in the IT Domain

WP0209 | October 2015

Michael Lane

Mike is a respected technology professional with nearly 20 years experience, having held senior manager positions in Information Technology, Communications and Consulting.

Over his career he has managed a vast number of Telecoms, IT, Business and Consulting projects and programmes, and the associated global cross functional teams, with a strong track record of results. Mike is a specialist in many aspects of information technology, including infrastructure, architecture, systems development, business processes, service management, policies and standards, leadership, governance and management.

From the days of being seemingly perpetually tied to the 'support service' tag, IT has engineered itself into the 'must have' for any business. Through the last few decades the dependency of the enterprise on IT has grown unabated, fueled by exponential advances in technology and its pervasive entrenchment into everything the business does. This of course has provided extensive opportunity for return on investment, but unfortunately also brings with it considerable risk to the enterprise.

Enterprise risk management (ERM) for any organization is an essential cog in the business engine room, forming a critical component of the Governance of the enterprise. ERM comprises all of the risks of the organization including Financial, Operational, Human Resources, and IT. When it comes to IT specifically, what is particularly important for organizations to remember is that the use of information and technology is enterprise wide, not limited to one or more functions. IT doesn't simply perform at the tactical or operational levels, but also shapes and delivers strategic direction and execution. IT enables organizations to take on more than ever before – more products, more markets, more customers, more challenges and more opportunities…and inevitably, more risk.

Rationalizing Risk

I often get asked by organizations, what risk management approach should I take? How can I position risk in the organization to add the most value? Isn't risk management key to my enterprise's survival? How do I incorporate IT Risk into my overall Risk Management for the organization? Leaving risk management in the IT domain to chance has gone from not being an option to being a must have for the enterprise that wants to

survive and thrive in the long term. But in the world of Risk Management, what's out there and what's relevant today?

When it comes to standards, and Risk Management is no exception, one can always turn to the International Organization for Standardization (ISO) for information on specific subject matters. Within ISO, in the risk space, there are a number of well-versed standards, including the universally known:

IS0 30001, defined by Wikipedia as:

> *" A family of standards relating to risk management codified by the ISO. The purpose of ISO 31000:2009 is to provide principles and generic guidelines on risk management."*
>
> (https://en.wikipedia.org/wiki/ISO_31000)

ISO 27005, defined by Wikipedia as:

> *" The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series)."*
>
> (https://en.wikipedia.org/wiki/ISO/IEC_27000-series)

There are other standards in various guises such as the Institute of Risk Management (IRM)'s "A Risk Management Standard" developed in 2002 by the 3 leading risk management organizations in the United Kingdom (UK), or the "Red Book" from the OCEG, who are "a global nonprofit think tank and community… helping organizations achieve Principled Performance by integrating governance, assurance and management of performance, risk, compliance and ethics (GRC)"

But those and ISO aside, when it comes to ERM, perhaps it is COSO's frameworks and guidance's over the last decade which are some of the most widely known and practiced. From Risk Oversight, to Risk Indicators to Risk Appetites and Risk Assessments, and in keeping up with modern times, ERM for Cloud Computing, their works make for informative and interesting reading. Their original principles based guidance, the Enterprise Risk Management - Integrated Framework launched in 2004, was to "help entities design and implement effective enterprise-wide approaches to risk management." At the time of the aforementioned publication COSO were early leaders in recognizing the need for:

- A direction for organizations to use in determining how to enhance their risk management
- Criteria to enable them to evaluate whether their risk management is effective

Information and Technology Risk is a critical component of every contemporary organization's ERM, and failure to not only include but focus on IT risk can be of serious consequence to the enterprise, as highlighted by ICASA.

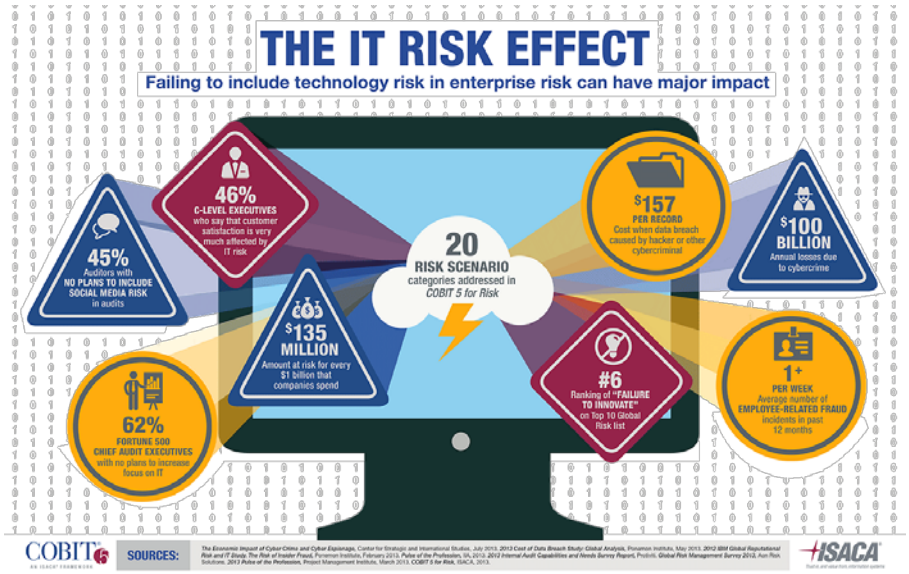

Figure 1 (COBIT® 5© 2012 ISACA® All rights reserved)

When it comes to IT Risk Management, it's not surprising that ISACA step into the picture. ISACA's COBIT 5 – "the business framework for the Governance and Management of Enterprise IT" promises more effective and efficient IT risk management and risk reduction as its no.2 business benefit, and in addition, ISACA has also produced dedicated COBIT 5 for Risk guidance to provide organizations with:

- Guidance on how to use the COBIT 5 framework to establish the risk governance and management function(s) for the enterprise
- Guidance and a structured approach on how to use the COBIT 5 principles to govern and manage IT risk
- A clear understanding of the alignment of COBIT 5 for Risk with other relevant standards (including ISO 31000, IS0 27005 and COSO ERM)

Within COBIT 5 there are two key Risk Management processes, one in each of the Governance and Management areas:

Governance

- *Process:* Ensure Risk Optimization
  - *Process Description:* Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.

- *Process Purpose Statement:* Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

Management

o *Process:* Manage Risk

- *Process Description:* Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.
- *Process Purpose Statement:* Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

What is probably most important to note is that Risk Management in COBIT 5 spans Governance and Management. The primary governance objective of any organization is sustainable value creation, and to achieve this they need to optimize resource utilization and risk management. This doesn't simply mean risk scenarios associated with negative risk, but should encompass positive risk scenarios too and what to do when positive risks (opportunities) present themselves to the organization. Enterprises that get ahead today and stay ahead, don't do so by avoiding risk at all costs, they manage risks in their organizations in line with their enterprise risk appetite. They ensure that risk responses to risks faced by the business are continuously adequate and appropriate, thus allowing these organizations to not only prevent threats and issues from materializing, but to take on risk when the time and expected return are right.

Risk Management is indispensable. As is having a globally accepted and in use framework like COBIT 5 which includes both Risk Management and Risk Optimization processes supported by corresponding Management and Governance practices. Done correctly, Enterprise Risk Management can assure an organization's longevity, and assert a competitive advantage in the marketplace. The pressure to do the right things, be prepared for threats and liabilities, and satisfy burgeoning legal and regulatory demands is growing exponentially, and organizations who do not embrace the need and opportunity, will be left behind.

Conclusions

With the multitude of IT challenges to hand, organizations sometimes don't know where to turn when it comes to Risk Management. Enterprises are well aware they face ever increasing known risks from data breaches to employee fraud and the generalized cyber-sphere, not to mention exploding new entrants like social media. Organizations can ill afford to not only consider IT Risk Management, for IT Risk alone, but as a crucial cog in the ERM for the enterprise, and a platform for leveraging competitive

advantage. And as organizations continuously look to IT to help deliver more effective and efficient business processes, and reduce waste, so too are smart organizations looking for the optimal way to manage the enterprise's Governance, Risk and Compliance incorporating IT Risk consideration as a key ingredient in its strategy.

The real challenge organizations are faced with is choosing a Risk Management approach for the IT domain which manages and optimizes IT risk to meet organizational demands, that can seamlessly interface into the Enterprise's Risk Management framework, and that aligns to and supports the adoption of IT GRC by the organization. ISACA's COBIT 5 framework offers the ideal solution to this.

Additional Reading

www.orbussoftware.com/governance-risk-and-compliance/

References

The IIA The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework [PDF] Available from: https://na.theiia.org/standards-guidance/Public%20Documents/7-2-%20Article_on_ISO_for_Auditors_rev7-20.pdf

[Accessed July 2015]

http://www.oxforddictionaries.com/definition/english/rationalize

http://advisera.com/27001academy/knowledgebase/write-iso-27001-risk-assessment-methodology/

http://www.isaca.org/COBIT/Pages/Risk-product-page.aspx

https://cobitonline.isaca.org/

http://www.intechopen.com/books/risk-management-for-the-future-theory-and-cases/understanding-components-of-it-risks-and-enterprise-risk-management-a-literature-review

http://www.coso.org/guidance.htm

http://www.oceg.org/

Orbus Software UK
London

Orbus Software US
New York

Orbus Software AUS
Sydney

Orbus Software RSA
Johannesburg

enquiries@orbussoftware.com | **www.orbussoftware.com**

Seattle Software Ltd. Victoria House, 50-58 Victoria Road, Farnborough, Hampshire, GU14 7PG. T/A Orbus Software. Registered in England and Wales 5196435