# RISK MANAGEMENT
# - Insights in the digital context

INNOVATION™
VALUE
INSTITUTE

## Introduction

This position paper presents an overview of key insights on the management of IT-related risks in the digital business context, as derived from pertinent academic and practitioner literature. These, along with insights from subject matter experts, have informed development of IVI's IT-CMF Risk Management (RM) Critical Capability.

## Changing Nature of Risk in the Digital Context

The digital landscape is characterized by significant risks and uncertainties, where risk relates to the potential loss traceable to IT/digital assets and digitally-enabled managerial and operational processes [1]. Risks are complex concepts that are dependent on time and the logical relationships and interrelationships with other objects [2]. Factors such as the pervasiveness of and reliance on technology, the rapid pace of technology advances, greater organizational connectivity, customer power, and information velocity and density increase the complexity of the digital environment and result in the need for the organization to evolve its traditional business operations and business models. These factors result in the organization being exposed to a landscape of unprecedented risk, and greater ranges, scales, and frequencies of digital attacks [3]–[7].

Numerous IT-related risks have been discussed in the literature (for example [1], [8–12]). Digital risks encompass traditional IT risk categories and an expanded set that are more specific to the transformational changes brought about by new and emerging technologies. They include, for example, strategic, operational, financial, technical, programme/project delivery, data/information, reputation and brand, political, legal and regulatory, supply chain/business ecosystem, new business models and business processes, conduct, and disruptive technology implications. A further risk for an organization is that of failing to actively pursue digital change – such organizations, sometimes referred to as 'digital laggards', may become irrelevant or may even be displaced in their industries by fast-moving digitally-enabled players [13].

## Relevance of Risk Management in the Digital Context

The existence of organizational structures, incentives, or culture that discourage adaptability or risk taking are a significant liability in effectively exploiting digital assets [1], [14]. In some studies, risk aversion is regarded as a significant cultural barrier to an organization's digital transformation journey [14]. Traditionally, organizations tended to be more risk averse with a predominant focus on risk and cost minimization, internal performance, metrics, and standard waterfall processes [15], and this mind-set still prevails in the 'digital laggards'. In the rapidly changing digital landscape however, digital leaders typically have a higher tolerance and appetite for risk. CEOs/CIOs with a more 'risk-on' attitude to technology [16] engage in risk-taking actions, experimentation, and digital business innovation using exploratory, fail fast approaches to identify the key opportunities for the future [13]. An organizational culture that embraces and supports more entrepreneurial and active risk-taking in digital programmes is characteristic of higher organizational performance. In a 2015 McKinsey survey, for example, 65% of digital leader organizations had a high tolerance for risk or bold initiatives and over half had changed the risk profiles of their corporate business portfolios in response to digital trends. In contrast, among average digital performers 70% of respondents did not see support for risk taking [17]. While this cultural shift may come more naturally to 'born digital' organizations, for others the path to digital transformation is more challenging.

With both greater ranges, scales, and frequencies of digital attacks, and greater appetite for risk-taking actions among digital leaders, the importance of an effective risk management capability for the organization is paramount. Risk-taking behaviour must be balanced with the use of proactive risk management approaches that minimize the potential downside of risk exposure. In a recent survey however, 43% of organizations did not recognise the risks of digital transformation or had not effectively addressed them. Approximately one third of respondents had not considered how their risk management approaches may need to evolve to account for the complexities of the digital environment; rather they adopted a 'wait and see' approach with the aim of emulating the risk management approaches of successful competitors. Only 25% of business leader respondents adopted proactive approaches to managing the risks of digital disruption [13]. Failure to effectively manage IT-related risks can result in regulatory, legislative, financial, and reputational implications that can impact business continuity [4], [18]–[20]. Hence, establishing a risk management approach that is responsive to the changing nature of risk and that enables the organization to manage risks to within its risk tolerance threshold must be a key priority in the digital context.

## Managing Risk in the Digital Context

Effective risk management in the digital context serves two objectives: 1) establishing awareness and a common understanding across organizational stakeholders regarding the nature of digital risks, and 2) establishing programmes to ensure risks are effectively addressed by relevant individuals [1]. Given the changes brought about by digital transformation [5], it is suggested that organizations need to ***re-conceptualize the management of risk*** as opposed to continuing with traditional risk management approaches. Hence, organizations should focus on developing a risk management capability [1], [21] that provides the organization with the ability to rapidly and dynamically respond to digital disruptions. The agility to sense and respond to unknown and unexpected risks is increasing in importance, relative to practices for prioritizing and mitigating known and expected risks [12].

As a key aspect in developing an effective risk management capability, digital risk needs to be solidified as a ***key focus area of the corporate board's agenda*** as corporate board level involvement can set the mandate for the organization's risk-taking propensity. Such board-level involvement, as well as provision of adequate funding and visible and vocal engagement across the organization, communicates the message that risk management is a critical issue with business consequences and promotes development of a risk-aware culture.

***Heightened levels of awareness*** are necessary to keep pace with changes in the risk landscape. Hence, communication from senior management should direct each individual employee in being cognizant of IT-related risks, as in the event of a breach of the organization's preventive and detective barriers, the actions of employees become the last line of defense. Consequently, organizations need to develop ***comprehensive employee-directed risk management education*** as part of their IT risk management programmes [1], in order to facilitate employee decision-taking on risk [22]. Such training should cover general awareness training and training specific to emerging tools and holistic risk management approaches.

At an individual employee level, CIOs need to reflect risk management as a key improvement area in their individual and team's performance plans. The ***link to employee performance appraisals*** is important, as employee noncompliance with IT-related risk issues is regarded as a growing concern [1]. Success should be measured in how well the team responds to risk i.e. its resilience, as opposed to how well its prevent issues from occurring.

Corporate governance needs to be redefined to meet the requirements and demands of the digital business. The organization needs to ***evolve the focus on governance*** – from an IT governance and a tactical information security focus to enterprise digital governance and enterprise accountability i.e. establishing cross-functional responsibility for effectively and efficiently leveraging digital technology in support of the organization's goals [1], [23]. Organizational structures need to reflect a ***separation of the operational aspects of risk management from governance-related aspects***, with a distinction being made between those who own risk decisions, those who provide risk assessments, and those who audit risks, yet these should simultaneously work together [24]. Clear ownership and shared accountability should be assigned for risk management. It is the responsibility of those risk owners to establish specific policies and standards for the various risk areas, and to regularly assess and manage the risks faced [1].

Risk management policies, procedures, and programmes need to be linked to the organization's strategy, objectives, and culture [1]. A sole focus on minimizing technical risk is inadequate for engaging in digital transformation [1]. Organizations need to broaden the IT conversation beyond the IT function and ***a more strategic, enterprise-wide risk management approach, with a focus on business exposures*** is required. Due consideration must be given to encouraging partnerships between technical and business managers, and digital risk management practices must further consider the wider business ecosystem and the management of risks pertaining to the entire supply chain. Greater communication, collaboration, and an enriched risk dialog across departments are required to address digital risks, as well as partnerships between suppliers, partners, and external agencies [1], [3].

***A clear understanding of the organization's risk tolerance and the evolving risk landscape*** is required. Approaches to risk management need to be driven by the organization's appetite for risk, as this understanding enables an organization to balance the need to protect the organization and the need to effectively run and grow the business [5]. Typically, organizations need to shift from a mind-set that regards all risk as bad to an attitude to taking appropriate risks in order to realize increased profits. In instances where digital leaders strive to embrace experimentation, ambiguity, and uncertainty, and quickly and flexibly react to change [25], the organization needs to find the right balance in managing risks without impeding effective business operations. According to Sambamurthy and Zmud [1], '*the real challenge is to balance the necessity to secure an organization's computer systems, communication systems, and information systems against the necessity for the organization to apply IT productively and creatively in executing and evolving the organization's business models in the face of an ever-changing competitive environment*'.

Digital risks, by their nature, are dynamic - characterized by continuous changes in the external environment. Hence, ***the management of digital risks, that is assessing, prioritizing, treating, and monitoring risks, needs to be proactive and dynamic*** [12], [26]. Informed by discussions on risks with the organization's most senior executives and an up-to-date understanding of the evolving risk landscape, IT leaders need to conduct regular risk assessments and map out threat models for the business in order to help determine the rigidity of controls required [4], [23]. This process can be enhanced by incorporating external threat intelligence [23], [27] and participating in relevant industry sharing communities to share and glean valuable insights [28]. The level of risks faced must be continually monitored and re-evaluated as risks, technologies, and legal and regulatory requirements evolve [5]. In order to address the prioritized risks, comprehensive risk treatment strategies are required, with risk responses being matched to the magnitude of the risk posed to the organization and the particular needs of individual operating units [1]. In summary, the approaches for managing risk typically need to continually adapt to minimize the potential negative consequences of risk exposure [29]. They should agilely focus on business outcomes, reflect a phased containment approach to control risk in short sprints [12], [15], and balance the potential severity of the risks with the need for the organization to innovate and seize IT-related/digital opportunities [5].

## Conclusions

Rapid advances with respect to new and emerging digital technologies increase the potential risk of digital transformation, requiring organizations to rethink their approach to risk management. A critical mind-set shift is that of evolving the practice of IT-related risk management from an IT function-centric activity to an enterprise-wide activity, with shared ownership, responsibility, and accountability across IT and business function leaders, as well as greater engagement and collaboration with broader business ecosystem partners. Organizations now need far more proactive risk management approaches in order to minimize the potential downside of risk exposure – these approaches need to be sufficiently agile to sense and respond to continually evolving and unknown or unexpected risks, whilst balancing the trade-off between potential loss and potential benefit.

## References

[1] V. Sambamurthy, and R. Zmud, *Guiding the digital transformation of organizations*. Legerity Digital Press, 2012.

[2] A. Sienou, E. Lamine, H. Pingaud, and A. Karduck, ‘Risk driven process engineering in digital ecosystems: modelling risk’, in *Proceedings of the 4th IEEE International Conference on Digital Ecosystems and Technologies,* 2010.

[3] Accenture, ‘The state of cybersecurity and digital trust 2016 - identifying cybersecurity gaps to rethink state of the art’, 2016. [Online] Available: <https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf>.

[4] CapGemini, ‘Address c-level cybersecurity issues to enable and secure digital transformation’, 2016. [Online] Available: <https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2017/07/1602_cybersecurity_strategic_consulting_brochure_cc_web_en_1.pdf>.

[5] D.W. Cearley, M.J. Walker, and M. Blosch, ‘The top 10 strategic technology trends for 2015’, *Gartner*, 2015. [Online] Available: <https://www.gartner.com/doc/2964518/top--strategic-technology-trends>.

[6] Frost & Sullivan, ‘The 2017 $(ISC)^2$ global information security workforce study – benchmarking workforce capacity and response to cyber risk’, 2017. [Online] Available: <https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf>.

[7] M. Raskino, and J. Lopez, ‘CEO and senior executive survey 2013: As uncertainty recedes, the digital future emerges’. *Gartner*, 2013.

[8] J. Geraldi, L. Lee-Kelley, and E. Kutsch, ‘The titanic sunk, so what? Project manager response to unexpected events’, *International Journal of Project Management*, vol.28, no.6, pp547–558, 2010.

[9] Q. Hussain, E. Chang, F. Hussain, and T. Dillon, ‘Ascertaining risk in financial terms in digital business ecosystem environments’, in *Proceedings of the 2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies*, 2007.

[10] Q. Hussain, E. Chang, F. Hussain, and T. Dillon, ‘Quantifying failure for risk-based decision-making in digital business ecosystem interactions’, in *Proceedings of the 2nd International Conference on Internet and Web Applications and Services,* 2007.

[11] J. Luftman, and R. Kempaiah, ‘Key issues for IT executives’, *MIS Quarterly Executive*, vol.7, no.2, pp99–112, 2008.

[12] O. Lee, and D. Baby, ‘Managing dynamic risk in global IT projects: agile risk management using the principles of service-oriented architecture’, *International Journal of Information Technology and Decision Making*, vol. 12, no.6, pp1121-1150, 2013.

[13] J. Bradley, J. Loucks, J. McCaulay, A. Noronha, and M. Wade, ‘Digital vortex - how digital disruption is redefining industries’, *Global Centre for Digital Business Transformation*, 2015. [Online] Available: <http://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-vortex-report.pdf>.

[14] M. Fitzgerald, N. Kruschwitz, D. Bonnet, and M. Welch, ‘Embracing digital technology - a new strategic imperative’. *MIT Sloan and CapGemini Consulting*, 2013.

[15] H. Colella, T. Nunno, A. Rowsell-Jones, and M. Mesaglio, ‘Three steps to successfully implementing bimodal-aware IT governance’. *Gartner*, 2014.

[16] M. Raskino, ‘CEO resolutions for 2014. Time to act on digital business’. *Gartner*, 2014.

[17] T. Rickards, K. Smaje, and V. Sohori, ‘‘Transformer in chief’: The new chief digital officer’. *McKinsey*, 2015.

[18] ISACA, ‘COBIT 5 for information security’, 2012. [Online] Available: <http://www.isaca.org/cobit/pages/info-sec.aspx>.

[19] ISACA, ‘COBIT 5 for risk’, 2013. [Online] Available: <http://www.isaca.org/cobit/pages/risk-product-page.aspx>.

[20] S. Pental, ‘Five ways information security can help IT improve stakeholder engagement’, *CEB IT Quarterly – Spotlight on business engagement*. Q2, pp30-33, 2015. [Online] Available: <http://ceb.uberflip.com/i/502110-cio152185syn-rp-q2-it-quarterly-web/33?m4=>.

[21] M. Carcary, ‘IT risk management: A capability maturity model perspective’, *Electronic Journal of Information Systems Evaluation,* vol.16, no.1, pp3-13, 2013.

[22] CEB, ‘IT quarterly - spotlight on business engagement’. *Corporate Executive Board*, 2015.

[23] Accenture, ‘Accenture technology vision 2014. Every business is a digital business - from digitally disrupted to digital disrupter’, 2014. [Online] Available:
<http://investor.accenture.com/~/media/Files/A/Accenture-IR/events-and-presentations/Accenture-Technology-Vision-2014.pdf>.

[24] CEB, ‘IT quarterly - spotlight on IT clock speed’. *Corporate Executive Board*, 2015.

[25] J. Peppard, ‘Digital dynamics in the C-suite: accelerating digitization with the right conversations’, *Sungard*, 2014. [Online] Available:
<https://www.sungardas.com/globalassets/_multimedia/document-file/digital-dynamics-in-the-c-suite.pdf>.

[26] S. Prentice, and K. McGee, ‘Master the six essential elements of a digital strategy’. *Gartner*, 2013.

[27] Ernst & Young, ‘Creating trust in the digital world - EY’s global information security survey 2015’, 2015. [Online] Available: <http://www.ey.com/publication/vwluassets/ey-global-information-security-survey-2015/$file/ey-global-information-security-survey-2015.pdf>.

[28] Accenture, ‘Accenture technology vision 2013. Every business is a digital business’, 2013. [Online] Available:

<https://www.accenture.com/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents8/Accenture-Technology-Vision-2013.pdf>.

[29] J. Fraser, B. Simkins, and K. Narvaez, *Implementing enterprise risk management: case studies and best practices.* Hoboken, NJ: Wiley, 2014.

## Recommended Reading

S. Elky, 'An introduction to information systems risk management', *SANS Institute*, 2006. [Online] Available: <http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204>.

J. Fraser, B. Simkins, and K. Narvaez, *Implementing enterprise risk management: case studies and best practices.* Hoboken, NJ: Wiley, 2014.

International Organization for Standardization (ISO), 'ISO 31000 – Risk management', 2009. [Online] Available: <http://www.iso.org/iso/home/standards/iso31000.htm>.

ISACA, 'Risk IT framework', 2009. [Online] Available: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx>.

ISACA, 'COBIT 5 for risk', 2013. [Online] Available: <http://www.isaca.org/cobit/pages/risk-product-page.aspx>.

Lloyds, 'Managing digital risk: trends, issues and implications for business', *Lloyd's 360 degree risk insight,* 2010. [Online] Available: <https://www.lloyds.com/~/media/lloyds/reports/360/360%20digital/lloyds_360_digital_risk_report%20(2).pdf>.

Office of Cybersecurity and Communications National Cyber Security Division, 'Information technology (IT) security essential body of knowledge (EBK): a competency and functional framework for IT security workforce development', Washington, DC: United States Department of Homeland Security, 2008.

Office of Government Commerce, *Management of risk – guidance for practitioners*. 3rd ed. London: The Stationery Office, 2011.

G. Williams, 'Everything you wanted to know about Management of Risk (M_o_R) in less than 1000 words', 2011. [Online] Available: <https://www.vanharen.net/Player/eKnowledge/everything_you_wanted_to_know_about_management_of_risk_guidance_for_practioners_mor_in_less_than_one_thousand_words.pdf>.

## Contributing Author

Dr Marian Carcary, Senior Lead Researcher, Innovation Value Institute.

## About IVI

The Innovation Value Institute (IVI) is a multi-disciplinary research and education establishment co-founded by Maynooth University and Intel Corporation. IVI researches and develops management frameworks to assist business and IT executives to deliver digitally enabled business innovation. IVI is supported by a global consortium of likeminded peers drawn from a community of public and private sector organizations, academia, analysts, professional associations, independent software vendors, and professional services organizations. Together, this consortium promotes an open ecosystem of research, education, advisory support, international networking, and communities-of-practice. IVI is supported through Enterprise Ireland's and IDA's Technology Centre programme.

## Contact IVI

For more information on this capability, IT-CMF and other IT management topics, or on becoming a member of IVI's international research consortium, please visit www.ivi.ie or contact us at: ivi@nuim.ie or +353 (0)1 708 6931.