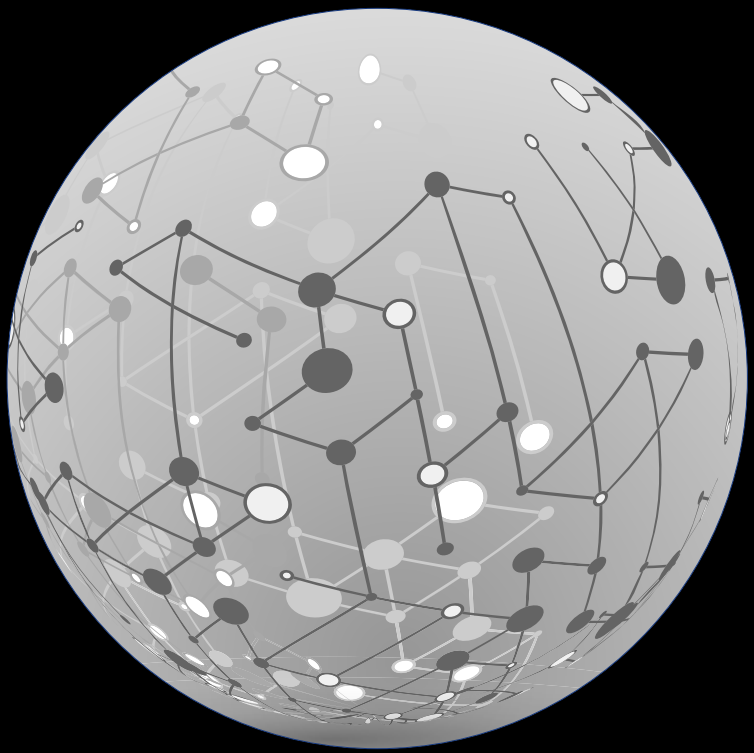
Deloitte.



Managing Risk in Digital Transformation

January 2018

Risk Advisory

Introduction

Digital. Is it a buzzword in the corporate world or way beyond that?

In the current times, every industry/enterprise has its own definition of 'Digital' and what it means to them. Boards, CIOs, and Executives are extensively talking about going digital.

Organizations can no longer evade the truth that Digital has become the need of the hour and the most effective enabler for creating a differential and unique competitive advantage.

A "digital mindset" and the requisite investment of capital, are critical enablers for a successful transformation exercise.

Key trends

Several factors have been playing a crucial role in the exercise of digital transformation. A few among them have been listed below:

- Exponentially increasing penetration of smart devices.
- Evolving customer expectations and changing demographics.
- Increase in internet speed and its penetration.
- Technological innovations and inclination towards advanced technologies.

Digital Technology is slowly being recognized as an important enabler for innovations. Digital Transformation brings forth unmatched opportunities and capabilities for growth and value creation.

None of the opportunities, however, can be realized without dealing with the associated risks. Managing risks in the changing era is, thus, critical to an organization's sustainability.

Digitalization means different things for different stakeholders

For an effective digital environment to meet the desired objective, it is critical to consider risk areas beyond traditional risk.

Enterprise View

Strategy and Vision

- Define a digital vision and strategy
- Conduct a feasibility assessment of the initiatives which can undergo digital transformation

Implementation

- Transforming the tools and capabilities used to deliver services
- Identify the key stakeholders in the ecosystem aiding the digital transformation

Program Management

- Focus on timely and cost-effective implementation of the digital initiative, for the respective business teams

Risk View

Contextual Risk

- Adequacy of selection of digital enablers of the digital program, in the context of business objectives
- Setting the tone of risk management at the design stage of digital program
- Prioritization of initiatives ensuring minimal impact or disruption of service.

Implementation Risk

- Risk-based architecture for the digital enablers, w.r.t. technology, operations, vendors, compliance, security and resiliency
- Right digital technologies for different business processes
- Culture of 'digital mindset' and a secure usage of the digital components

Governance Risk

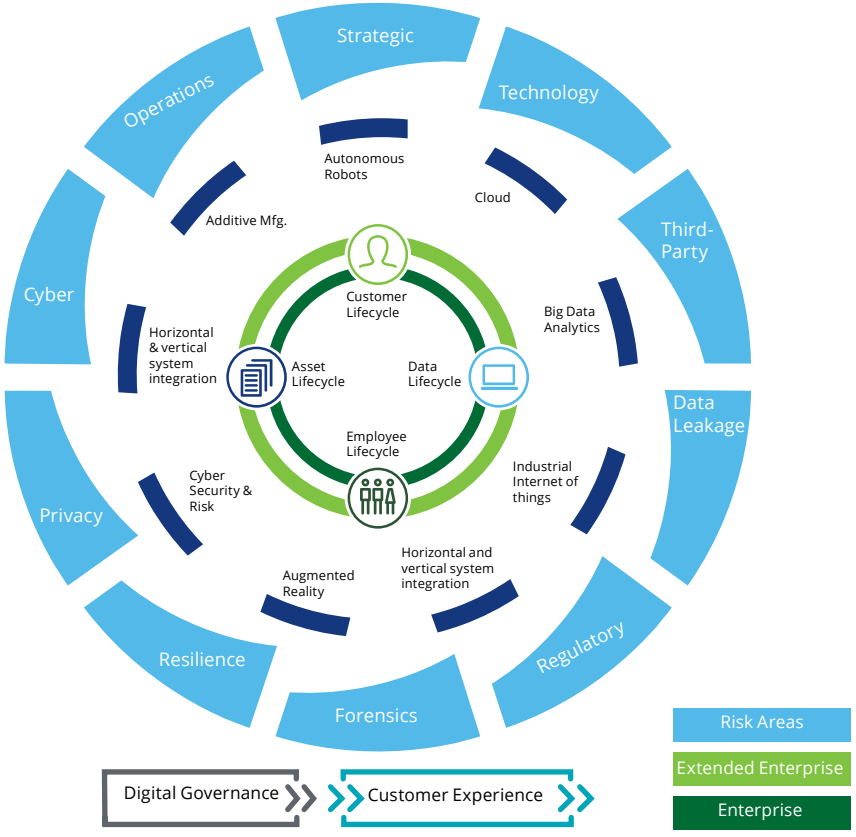
- Effective governance around the Digital transformations to ensure cross functional synergies and eliminate risks arising due to inter dependent processes
- Risk management framework that can be used by the organization for managing risks that may arise in any future digital initiatives.

Beyond Traditional Risk and Security

Laying out the building blocks of the digital risk strategy is crucial to its success. An immediate step by organizations is to have robust measures around cybersecurity and the easiest approach is to perform typical information security and/or cyber security assessments of systems. The questions which need to be addressed are, 'Is this enough? Is cybersecurity the only risk to a digitally enabled organization?'

For an effective digital environment to meet the desired objective, it is critical to consider risk areas beyond traditional risk. For example, social media is becoming an integral part of marketing, thereby, creating risks to brand value and reputation. Similarly, customer profiling is prominent for better customer experience, but then profiling process should be aligned to protect privacy of customer data. Another important aspect to be considered is digital resiliency–due to large dependency on the technology, the availability of the systems is non-negotiable. There are several other scenarios across different industries and operations that cover other risk domains that could be considered.

Deloitte's Digital Risk Framework



We have considered 10 risk areas– Strategic, Technology, Operations, Third Party, Regulatory, Forensics, Cyber, Resilience, Data Leakage, and Privacy–as the risk landscape in any digital ecosystem. Based on the applicable risk areas for the digital initiatives, different control measures need to be designed as per leading standards and industry practices. The critical aspect in defining the controls is to take into consideration the nature and level of digitization in the operations, as most of these areas are at a nascent stage and tightly coupled with systems or manual processes, so there might be constraints to implement the controls.

Understanding the risk areas is critical to identifying and dealing with all the risks that an organization may be exposed to in a digital environment. This section explains in brief all the risk areas considered in the framework.

Technology
Potential for losses due to technology failures or obsolete technologies. Technology related risks have an impact on systems, people, and processes. Key risk areas may include scalability, compatibility, and accuracy of the functionality of the implemented technology.

Cyber
Protection of digital environment from unauthorized access/usage and ensuring confidentiality and integrity of the technology systems. Key controls may include platform hardening, network architecture, application security, vulnerability management, and security monitoring.

Strategic
Usually derives from an organization's goals and objectives. It can be external to the organization and, on occurrence, forces a change in the strategic direction of the organization. Typically would have an impact on customer experience, brand value, reputation, and competitive advantage in the market place.

Operations
An event, internal or external, that impacts an organization's ability to achieve the business objectives through its defined operations. Includes risks arising due to inadequate controls in the operating procedures.

Data Leakage
Ensuring protection of data across the digital ecosystem at various stages of data life-cycle–data in use, data in transit and data at rest. Key focus control areas would be around data classification, data retention, data processing, data encryption, etc.

Third-party
Comprises of risks arising due to inappropriate controls at vendors/third party operating environment.
Key controls would be around data sharing, technology integration, operations dependency, vendor resiliency, etc.

Privacy
Risk arising due to inappropriate handling of personal and sensitive personal data of customer/employee, which may impact privacy of the individual. Key controls includes notice, choice, consent, accuracy, and other privacy principles.

Forensics
Digital environment's capability to enable investigation in the event of a fraud or security breach, including capturing of data evidences which is presentable in the court of law.

Regulatory
Adherence to statutory requirements including technology laws, sectoral laws, and regulations.

Resilience
Risk of disruption in operations or unavailability of services, due to high dependency on tightly coupled technology. Key areas of consideration would include business continuity, IT/Network disaster recovery, cyber resiliency, and crisis management.

Digital Risk Portfolio

Our portfolio of services to mitigate risks around digital enablers

Digital Risk Strategy

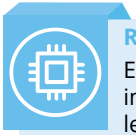
Establishing a governance framework to address the risks in implementation of Digital Programs

Digital Identity

Having an effective authentication & authorization mechanism across all digital enablers

Blockchain

Leveraging Blockchain architecture to secure against internal and external threats



RPA

Enabling a secure RPA implementation and leveraging of RPA for Cybersecurity & Risk management

IoT

Designing a risk-based IoT architecture for data collection and management of remote systems

OT (SCADA)

Protecting the OT infrastructure through secure integration with enterprise technology eco-system

Digital Payments

Secure digital payment offerings using a structured risk based approach

Cyber Analytics

Analytics based risk and compliance monitoring supported by Advanced Technologies.

Digitalization of RM

Enabling the risk management leveraging digital technologies

Navigating Digital Risks

Approach to establish an effective risk management in digital environment

Discover
Aligned to the organization's Digital vision, study the selection of digital enablers, and analyze the context so as to assess the digital footprint and its impact.

Develop
Based on Deloitte's Digital Risk Framework, develop a risk based digital architecture customized to the organization's digital needs and operating environment.

Implement
In the context of business, implement the risk based digital architecture for the selected digital enablers supported by an overall risk governance.

Monitor
Embed a continuous review process that evolves in response to disruption and new developments across the digital estate, legal and regulatory requirements.

Sustainability

"An approach to digital risk management should begin with an understanding of the organization's digital foot print and creating a register of digital risks"

01

Support Risk Management by conducting risk **awareness workshops and trainings.** Take it up as a as a **proactive exercise** embedding it into the organization's strategy instead of merely keeping it a reactive one

02

Periodically **monitor, review and update** the digital risk framework.

03

Enabling risk management **through a tool** will be appropriate for a **systematic identification** and management of the evolving digital risk

Conclusion

Digital Transformation across industries has led to a rapidly changing business environment which offers exponentially augmenting opportunities for new capabilities and initiatives.

One of the most critical success factors to win in this digital era is organizational agility. Businesses can create a scalable and adaptable digital journey encompassing a well-defined digital strategy, an appropriate business case, and a customized and flexible approach. Along with Digital transformation, it is imperative for organizations to also manage the risks that are introduced into the environment and its impact to the existing eco-system to drive optimum value from their digital initiatives.

Despite all the challenges and risks that the evolving environment presents, organizations cannot overlook the opportunities that 'moving to digital' brings forth along with the profound impact that it shall have on them.

Contacts

Rohit Mahajan
President - Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader,
Cyber, Risk Advisory
shuklagaurav@deloitte.com

Vishal Jain
Partner, Risk Advisory
jainvishal@deloitte.com

For further queries and feedback please email on indigitalrisk@deloitte.com

Deloitte.