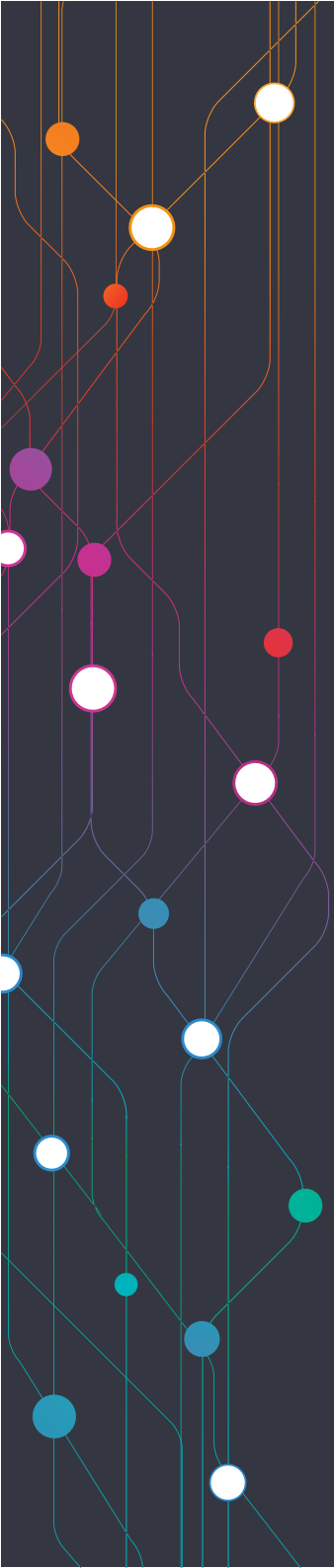
Deloitte.

Managing Risk in Digital Transformation

October 2018

Risk Advisory



Introduction

Consumers and businesses are adopting digital technology at a rapid pace, and while this is generating new opportunities, it is also creating new risks.

The digital transformation journey of many organisations is well underway. With Industry 4.0 we are already seeing the application of new technologies, including robots, the internet of things (IoT), artificial intelligence (AI), cloud computing, predictive analytics and blockchain rapidly changing the way many companies design and curate experiences, manufacture, distribute and service products.

An increased burden is being placed not only on the IT department but also on the internal risk function. Business leaders are making strategic choices on the investment, technology, resourcing levels and the skills needed to operate a digital business, all of which will have an impact on the short-term profitably and long-term viability of their businesses. These strategic choices inevitably involve an element of risk. At the same time businesses have to cope with external threats. For example, as businesses undergo digital transformation and more of their assets become digital, the threat of cybercrime and risks around data privacy are growing.

While digital transformation is creating major opportunities for organisations, it is also introducing a new dimension to the traditional view of risk.

Currently risk management teams remain on a reactive footing with a predominant focus on traditional IT general controls and risk assessment techniques, and are limited by the processes, systems and wider business insight with which they have been equipped. As technology transformations shift the risk landscape, organisations will need to develop an entirely new approach to digital risk. Our Deloitte Digital Risk Framework will assist our clients in this Journey.

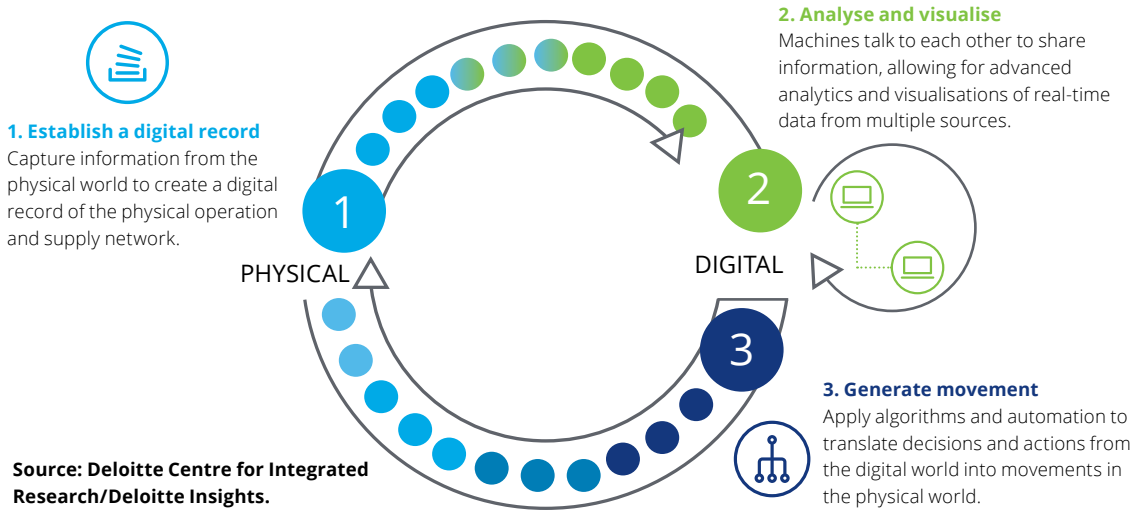
Beyond Traditional Risk

Industry 4.0 – A New Era bringing New Risks

Through Industry 4.0, smart, connected technologies are transforming organisations, operations, and the workforce by increasing information flow, creating new insights, and revolutionising business models. Although Industry 4.0 has its roots in manufacturing and supply chain, it extends to many other sectors. The power and value of Industry 4.0 lies in flows of information, and the ability to integrate digital information from many different sources and locations to drive the physical act of doing business. In this way, information flows in an ongoing cycle, where data from one process informs the next. This ongoing loop incorporates the use of many physical and digital technologies, including analytics, additive manufacturing, robotics, high-performance computing, natural language processing, artificial intelligence and cognitive technologies, advanced materials, and augmented reality. The illustration below depicts how information flow occurs through an iterative series of three steps, referred to as the physical-to-digital-to-physical (PDP) loop.

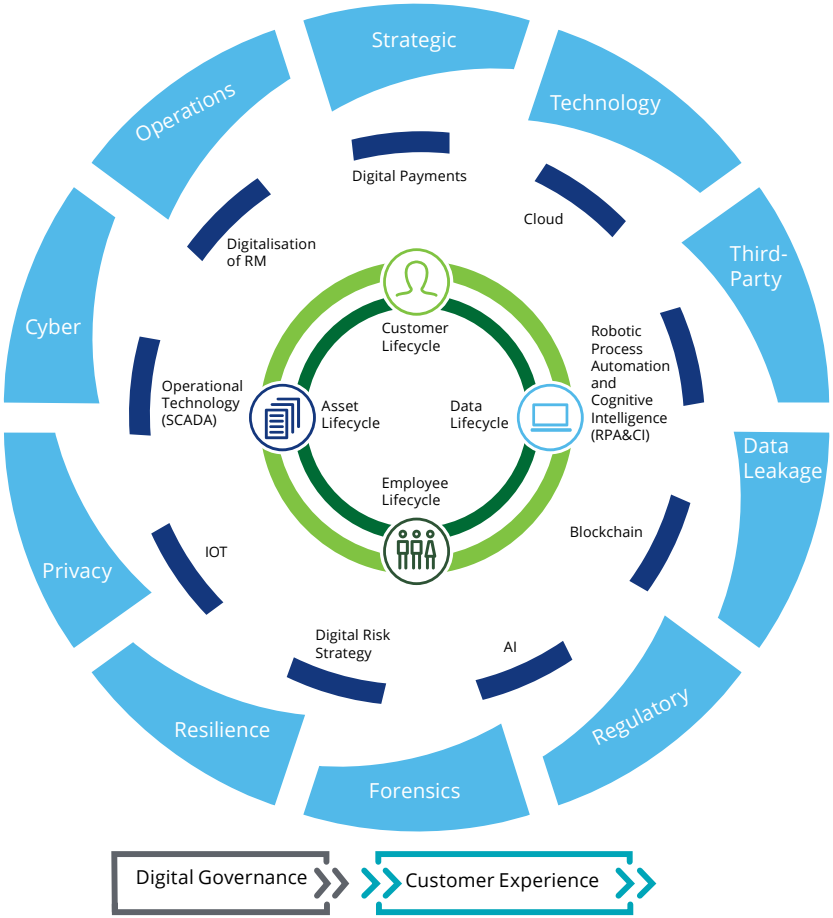
This introduces new risks as an example the digital environment's capability to enable investigation in the event of a fraud or security breach, including capturing of data evidences which is presentable in a court of law. Ensuring protection of data across the digital ecosystem at various stages of data life-cycle-data in use, data in transit and data at rest.

Physical-to-digital-to-phsycial loop and related technologies



Source: Deloitte Centre for Integrated Research/Deloitte Insights.

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 digitisation 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 organisation may be exposed to in a digital environment. This section explains in brief all the risk areas considered in the framework.

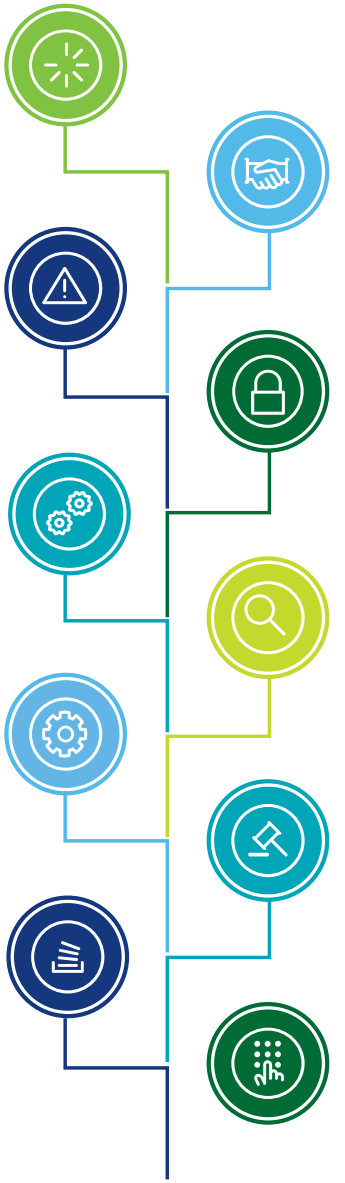
Technology
Potential for losses due to technology failures or obsolete technologies. Technology related risks have an impact on systems, people, and processes. Key risk areas may include scalability, compatibility, and accuracy of the functionality of the implemented technology.

Cyber
Protection of digital environment from unauthorised 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 organisation's goals and objectives. It can be external to the organisation and, on occurrence, forces a change in the strategic direction of the organisation. 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 organisation'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 the 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. These will include the electronic communications and transactions regulatory universe which is of general application and industry specific regulation including financial services, insurance and medical schemes to the extent applicable.

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.

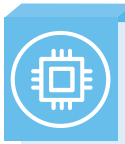
Digital Risk Portfolio

Example of 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

Cloud
Understanding and managing the risks of adopting a public/private/ hybrid cloud technologies for Infrastructure, Platform and Software

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

AI Risk Strategy
Enabling the adoption and implementation of AI with confidence

Digitalisation of RM
Enabling the risk management leveraging digital technologies

Navigating Digital Risks

Approach to establish effective risk management in a digital environment

Discover
Aligned to the organisation's Digital vision, study the selection of digital enablers, and analyse 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 customised to the organisation'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 organisation's digital footprint and creating a register of digital risks using our Deloitte digital risk framework as a base."

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

Periodically **monitor, review and update** the digital risk framework to ensure a complete and accurate digital risk landscape

Enabling risk management **through tools,** 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 organisational agility. Businesses can create a scalable and adaptable digital journey encompassing a well-defined digital strategy, an appropriate business case, and a customised and flexible approach.

Along with Digital transformation, it is imperative for organisations to also manage the risks that are introduced into the environment and its impact to the existing ecosystem to drive optimum value from their digital initiatives. Despite all the challenges and risks that the evolving environment presents, organisations cannot overlook the opportunities that 'moving to digital' brings forth along with the profound impact that it shall have on them.

Contacts

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navisingd@deloitte.co.za

Shahil Kanjee
Risk Advisory Africa Leader: Cyber Technology Risk
Mobile: +27 83 634 4445
Email: skanjee@deloitte.co.za

Wesley Govender
Risk Advisory Africa Leader: Data Analytics
Mobile: +27 83 611 2929
Email: wgovender@deloitte.co.za

Gregory Rammego
Risk Advisory Africa Leader: Forensic
Mobile: +27 82 417 5889
Email: grammego@deloitte.co.za

Rushdi Solomons
Risk Advisory Africa Leader: Internal Audit
Mobile: +27 741 414 444
Email: rsolomons@deloitte.co.za

Candice Holland
Risk Advisory Africa Leader: Regulatory Risk
Mobile: +27 82 330 5091
Email: canholland@deloitte.co.za

Michele Townsend
Risk Advisory Africa: Director
Mobile: +27 82 441 7164
Email: mtownsend@deloitte.co.za

Keshnee Naidoo
Risk Advisory Africa: De-risking Digital Transformation Leader
Mobile: +27 82 960 0982
Email: kesnaidoo@deloitte.co.za

Anthony Olukoju
Risk Advisory Regional Leader: West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Risk Advisory West Africa: Director
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Julie Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 20 423 0000
Email: woelofse@deloitte.com

Rodney Dean
Risk Advisory Central Africa: Director
Mobile: +263 867 700 0261
Email: rdean@deloitte.com.ng

Deloitte.