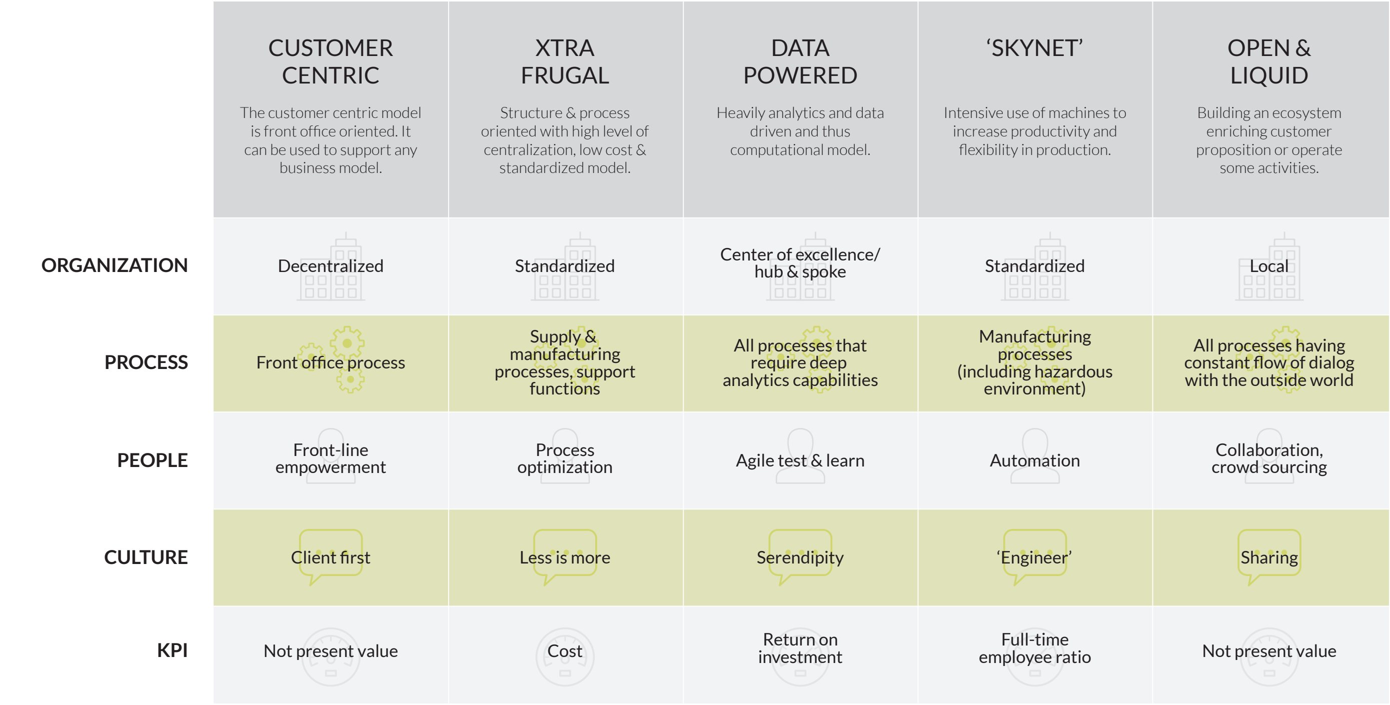
WHITE PAPER

FIVE RISK PROFILES OF DIGITAL OPERATING MODELS

Digital transformation affects all organizations in some form or fashion. It’s not unusual for all the different segments of an organization today to be facing transitions from traditional analog processes to a much more connected, digital approach. Even if these initiatives mainly involve existing processes, most organizations are looking for technology that can help unlock additional value across their business or mission.

The World Economic Forum (WEF), in Digital Transformation of Industries, identifies five digital operating models to portray the various forms digital initiatives take within organizations.



	CUSTOMER CENTRIC The customer centric model is front office oriented. It can be used to support any business model.	XTRA FRUGAL Structure & process oriented with high level of centralization, low cost & standardized model.	DATA POWERED Heavily analytics and data driven and thus computational model.	‘SKYNET’ Intensive use of machines to increase productivity and flexibility in production.	OPEN & LIQUID Building an ecosystem enriching customer proposition or operate some activities.
ORGANIZATION	Decentralized	Standardized	Center of excellence/ hub & spoke	Standardized	Local
PROCESS	Front office process	Supply & manufacturing processes, support functions	All processes that require deep analytics capabilities	Manufacturing processes (including hazardous environment)	All processes having constant flow of dialog with the outside world
PEOPLE	Front-line empowerment	Process optimization	Agile test & learn	Automation	Collaboration, crowd sourcing
CULTURE	Client first	Less is more	Serendipity	‘Engineer’	Sharing
KPI	Not present value	Cost	Return on investment	Full-time employee ratio	Not present value

Source: World Economic Forum

Figure 1: World Economic Forum Digital Operating Models

As organizations increasingly utilize digital technologies such as cloud computing, robotics and automation, data analytics, IoT, mobile products and services, and social media to drive growth and optimization, these operating models can be in various stages of deployment within the enterprise. In addition, they may overlap—a customer-centric project could result in more data on customer interactions and drive a data-powered project to glean new insights. These models are not always mutually exclusive but provide an interesting perspective for understanding potential risks created by digital initiatives.

RSA defines digital risk as “unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies.” In other words, following common definitions of risk as the effect of uncertainty on objectives, digital risk focuses on the effect of uncertainty on objectives that stem from digital transformation. As these emerging digital operating models take precedence within the organization, the mixture of risks—and the connected nature of the risks—pose the biggest obstacles to achieving the strategic gains that come with pursuing digital initiatives. The volatile, hyperconnected nature of digital business requires an integrated strategy that enables innovation while managing risk within new and evolving business operations.

RISK PROFILES OF DIGITAL OPERATING MODELS

While risk is a very broad topic, the digital risk domains RSA has defined capture the major dimensions of risk associated with digital initiatives:

- **Cybersecurity—**risk of cyber attacks
- **Process automation—**risks related to changes in processes from automation
- **Resiliency—**risk to availability of business operations
- **Third-party risk—**inherited risk related to external parties
- **Cloud—**risks due to the change in architecture, implementation, deployment and/or management of new digital business operations
- **Workforce/talent—**risks related to the dynamic nature of today’s workforce
- **Data privacy—**risks related to personal information
- **Compliance—**risks related to compliance requirements driven by new technology

To understand risk exposure and determine how much to invest to protect an organization from these risks, while still capturing the benefits of digital initiatives, risk and security leaders must implement a sustainable, evolving risk management strategy aligned with the business. Each of the five digital operating models has certain nuances that signal priorities that should shape the digital risk management strategy.

Customer-Centric

As organizations undergo digital transformation, customer-centric projects are likely to attract the most attention. Depending on the scope, these projects may be key to many growth strategies, thus creating significant pressure toward meeting strategic objectives. In addition, the customer-facing aspect generates a large amount of reputational risk. Failures in these types of initiatives will produce a wide range of short- and long-term impacts.

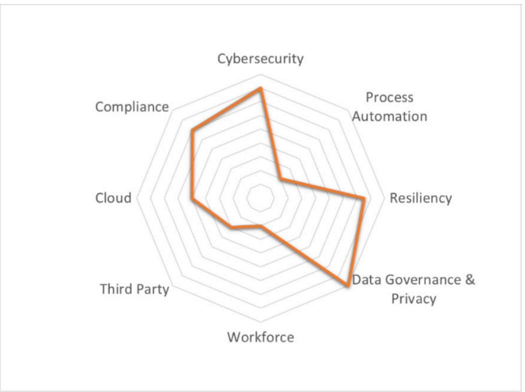


Figure 2: Customer-Centric Model Risk Profile

Customer-facing initiatives often result in the collection and processing of personal data. Therefore, cybersecurity, compliance and data privacy risks are elevated. Personal data not only carries the burden of compliance requirements, such as GDPR, HIPAA, GLBA and others, but also entails a significant level of reputational risk. Data breaches are extremely common—especially given the constant cybersecurity threats—and typically end up in public disclosures or, worst case, the national news. Additionally, given the expectations of customers for highly available systems, and the financial repercussions of business disruptions related to customer-facing systems, resiliency is an area of risk management that must be prioritized as well.

Xtra Frugal

Many organizations start their digital transformation journey focused on projects that optimize existing processes. These optimization processes, referred in the WEF model as “Xtra Frugal,” target cost control and can vary widely depending on scope. Examples include outsourcing of services or use of specialist skills and deployment of virtualization technologies to reduce IT costs.

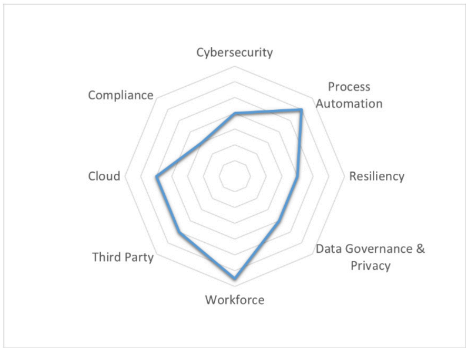


Figure 3: Xtra Frugal Model Risk Profile

Given the wide variety of these projects, the risk profile will fluctuate based on the nature of the initiatives. Looking at how organizations commonly approach these projects, certain aspects of risk are more dominant. Process automation risk is a key element since many of these projects look to transition existing processes to more digitally enabled operations. For example, complications resulting from implementing robotics process automation (RPA) to eliminate manual tasks in a service center must be managed to ensure proper models and procedures are utilized. Additionally, since many of these projects impact the employee base, workforce-related risks range from managing role changes of employees to maintaining skill sets and dealing with attrition. Finally, most optimization projects include elements of both cloud technology and third parties, highlighting both those areas of digital risk.

Data-Powered

It is difficult to imagine any digital initiative that does not have data at its core. Data-powered initiatives, though, are completely focused on utilization of data in new and innovative ways to unlock value. Much of this effort may be in the organization’s “back office”—utilizing existing or new stores of data and layering on complex analytics to find ways to optimize business processes.

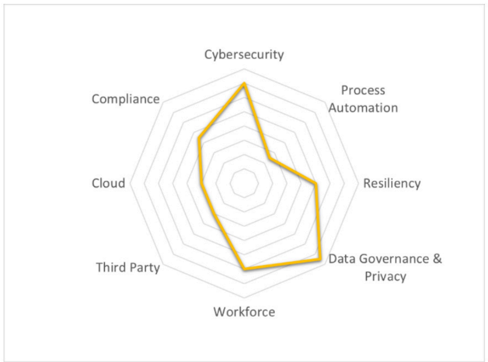


Figure 4: Data-Powered Model Risk Profile

The resulting risk profile is predictably skewed toward data-related risks. Data governance and privacy risks will depend on the nature of the data, e.g., personally identifiable information (PII) vs. intellectual property (IP). PII results in increased privacy and compliance risk, but data governance (understanding what data is processed, how it is processed, who is responsible for data, etc.) is necessary for any data-powered initiative. Cybersecurity is also a key part of managing risk around data-powered initiatives. Confidentiality and integrity of the data must be safeguarded. This includes assurance that access to data is appropriate, which elevates workforce-related risks.

Skynet

The WEF uses the term Skynet, affectionately named after the artificial intelligence (AI)-driven technology in the Terminator movies, to describe the "rise of the machines" and digital initiatives targeting heavy automation. Most commonly, this type of project is found in manufacturing and logistics companies. While robotics is already used extensively in manufacturing, these projects areas such as autonomous vehicles, augmented reality and more use of data to optimize production facilities.

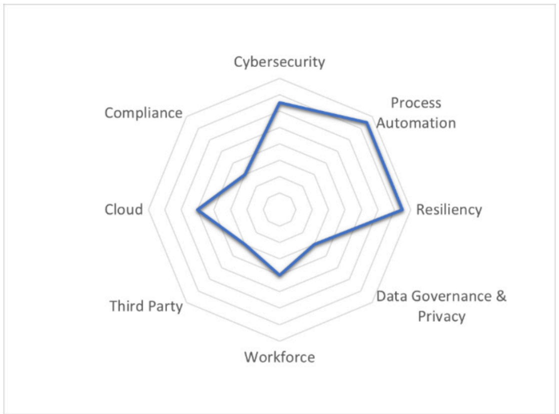


Figure 5: Skynet Model Risk Profile

The risk profile of these initiatives slants toward process automation, resiliency and cybersecurity. As automation takes a more integral part of the production lifecycle, any disruption will have a significant financial and reputational impact. These initiatives also depend on increased connectivity of systems, especially traditionally segmented infrastructures such as operational technology (OT) and IT systems. This connectivity brings the potential impact of security compromises down to the production floor, making cybersecurity an increasingly critical element.

In addition, In addition, because the application of AI is so transformative, governments and regulatory bodies are only beginning to understand how new AI-enabled technologies may need to be regulated. Organizations pursuing Skynet strategies should be vigilant in anticipating and monitoring applicable new laws and regulations.

Open and Liquid

The last operating model emphasizes an ecosystem of partners and relationships to further digital strategies. These relationships vary: a full joint venture with an external party,

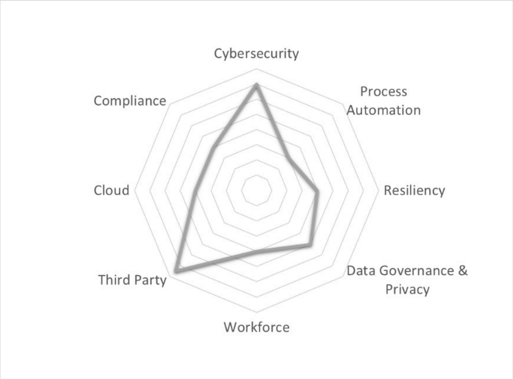


Figure 6: Open and Liquid Model Risk Profile

use of cloud service providers, deeper technical integration into the supply chain or selective use of specialist skills, to list just a few examples. One element called out by the WEF is the shared-customer concept in which different entities enrich the customer experience by working together. Whether customer-facing or part of a supply-chain integration, these initiatives typically include a flow of data and connected systems to benefit both sides.

Managing third-party risk and cybersecurity are obviously key objectives to mitigate negative outcomes of these relationships, given the connectivity between an organization and multiple outside parties. Ensuring governance processes establish ownership and accountability for third-party relationships, assessing and tracking known risks and issues, and ensuring proper access and monitoring of the data and activities will be critical elements. Depending on the nature of the ecosystem, resiliency may be a factor especially in terms of supply chain automation. Data governance and privacy are also concerns in data-oriented relationships.

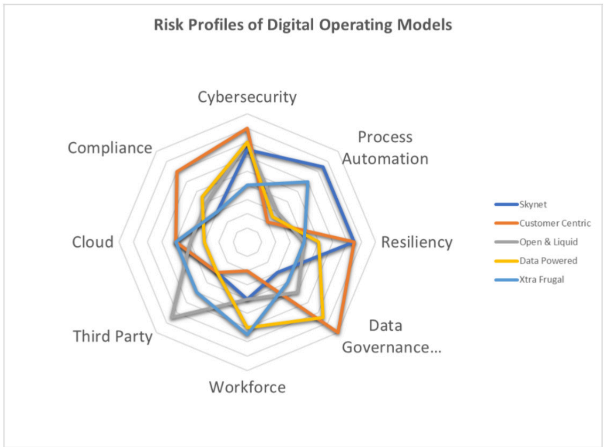
ACCOUNTING FOR THE NUANCES OF YOUR DIGITAL OPERATING MODEL

These risk profiles are based on general characteristics of the digital operating models. However, each digital initiative will have its own factors that will influence the overall digital risk profile. Use of cloud technology in any capacity will alter that element of digital risk. The same goes for factors such as third parties, compliance implications of extensive industry and regulatory requirements, or dynamic employee bases that include, for example, transient or seasonal workforces.

The critical action is to methodically identify, assess and treat the risks pertaining to changes in operations. As digital initiatives unfold, the unique attributes of the project will dictate priorities. Applying these general profiles can help spotlight areas for more in-depth analysis. The key is to approach this process as a continuous risk management lifecycle. Digital initiatives will continuously alter business operations, and the cycle of identifying, assessing and treating risks will be an ongoing effort. Since digital operations are generally tightly coupled, a failure in one area can quickly lead to issues in another. For example, a cybersecurity attack could originate via a third party (third-party risk) and result in a business disruption (resiliency risk) and a data breach (privacy or compliance violation). Therefore, an integrated strategy that addresses these domains proportionally is necessary.

CONCLUSION

Digital initiatives can take many forms. The alteration to business operations can vary from marginal to massive. Regardless, the shift toward digitally powered internal processes and external products and services is an irresistible force transforming organizations today. Each



digital initiative will have its own effect on business operations, and in turn, the risk posed to the organization. While the positive outcomes of technology adoption can fuel growth and spur innovation, the negative side of risk must always be managed.

Understanding the different risk profiles of digital operating models can highlight domains that must be priorities to identify, assess and treat risks effectively and efficiently. Getting out in front of these risk domains helps uncover the potential obstacles, so that risk management practices can evolve with the business. Successful digital transformation efforts will address risk management up front, allowing the organization to recognize the potential of a digital operating model supported by a highly optimized, transformed risk management function.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com