Looking at Trends in ERM

5

Contents

Learning Objectives

When you have finished studying this chapter, you should be able to:

- identify the drivers of digitization and analyse the impact for ERM
- name key digital technologies and assess their opportunities and risks
- know possible data analytics methodologies and their application in ERM
- create an individual set of requirements for an ERM tool for your organisation
- recognise future skills and competences for risk management professionals

S. Hunziker, *Enterprise Risk Management*,
https://doi.org/10.1007/978-3-658-25357-8_5

5.1 Emerging Digital Risks

The current business environment is very exciting in many ways. Numerous organisations are increasingly affected by the opportunities and risks of digitization; responsible managers are more challenged than ever. An active approach to these challenges posed by the environment appears to be essential in order not to be confronted with serious consequences in the future. For neither from an economic, political-social, regulatory nor technological point of view, a decline in complexity and speed can be expected. The digital revolution is not stopping at the ERM function either.

Digitization offers great opportunities in various areas of business activity, and this is now beyond question in many respects. An adequate approach to the associated risks, however, appears to be crucial, as opportunities are always risky. In order to assume this responsibility, there must be awareness and knowledge of the risks of digitization. It is important to consider what impacts new disruptive technologies such as distributed ledger technology (blockchain) or Artificial Intelligence (AI) can have on one's own field of business. Managers must ask themselves whether there is a possibility that other market participants could use these technologies in such a way that their own company could be driven out of the market (Hunziker et al. 2018, pp. 55–58).

5.1.1 Impact of Disruptive Technologies

While risk managers are not expected to know every detail and all technical backgrounds about disruptive technologies such as AI, Blockchain and the Internet of Things (IoT), they need to understand the full scope of opportunities and challenges these innovations present for the companies and markets they serve. Risk professionals are advised to proactively educate themselves about disruptive technologies, including what is already in use at their organisations, what technologies may be on the horizon, and the respective risks and rewards of using such technologies.

In the following, some of the most important technologies that could be relevant for risk managers are introduced. Some opportunities, challenges and risks of these technologies are briefly described. However, the statements are not exhaustive, but they depict some very important aspects from a business perspective (adapted from Ernst & Young 2017).

Firstly, robotic process automation (RPA) is the application of software that mimics human action and connects multiple systems through automation. The existing IT landscape is normally not changed. RPA enables organisations to automate existing high-volume and complex process steps as if business users were doing the work. It collects and interprets data across systems, triggers reactions and communicates with other systems in- or outside the organisation (e.g. fully automated client profile updates or straight-through processing of customer orders) (see Table 5.1).

Table 5.1 Opportunities and risks of robotic process automation. (adapted from Ernst & Young 2017)

Benefits and opportunities	Key challenges and risks
• Non-invasive technology, helps to close the "gaps" between existing (information) systems • Reliability (e.g. no sick days) • Audit trail (fully maintained logs) • Productivity (release of personnel resources) • Accuracy (correct result, decision or calculation the first time)	• Lack of robotics governance can lead to ineffective and inefficient process automation • Access management for robotics is ineffectively managed • Automation requirements that are not adequately or accurately identified and documented • Implementation is not properly designed and tested

Secondly, internet of things (IoT) is a system of interconnected computer devices, mechanical and digital machines, objects, animals or persons that are provided with unique identifiers and are capable of transmitting data over a network without requiring human-to-human or human-to-computer interaction (e.g. detection of rubbish levels in containers to optimise the trash collection routes or monitoring of parking spaces availability in the city) (see Table 5.2).

Thirdly, cloud computing involves storing and delivering applications and data over the Internet, not on local servers and PCs. There are three different service models, some of which overlap: Infrastructure, platform and software are three superimposed layers. Infrastructure as a Service (IaaS): The cloud as a virtual data centre. As a rule, these are computers, networks and storage that can be used via IaaS. Platform as a Service (PaaS): The cloud as a development environment. With PaaS, users develop their own software applications or test them in an environment provided by the cloud provider. Software as a Service (SaaS): The cloud as a programme starter. The most common form of cloud service offers concrete applications at a fixed monthly price per user or license (see Table 5.3).

Fourthly, blockchain is a type of database known as a distributed ledger that works on a consensus basis. Whenever a user sends a new data block to the blockchain, the majority of other users must confirm that it is valid. The database does not have a central administrator. Each user keeps a copy of the distributed ledger on their own computer and the data is replicated and synchronised in real time across all copies of the ledger Table 5.4.

Table 5.2 Opportunities and risks of internet of things. (adapted from Ernst & Young 2017)

Benefits and opportunities	Key challenges and risks
• Comfort in everyday life, efficiency and an overall improved consumer experience • Real-time execution of transactions • Supply chain optimization, quality control, asset management, remote control and predictive maintenance	• Since the sensors begin to communicate with each other without human intervention, cyber security should be a major concern • Partly unclear business benefits and lack of expertise • Connectivity issues, including technologies, authorization, and authentication

Table 5.3 Opportunities and risks of cloud computing. (adapted from Ernst & Young 2017)

Benefits and opportunities	Key challenges and risks
• Increasing the effectiveness of IT initiatives • Reduce the cost of internal operations • Avoid high initial investments • Increase operational flexibility • Generate a competitive advantage	• Organisations systems and those of the provider can communicate with each other (security concern) • Reduced visibility and accountability for security controls and processes implemented by vendors • Cloud users rely on their vendors' business continuity programmes and disaster recovery capabilities • Vendors fail to meet performance requirements

Table 5.4 Opportunities and risks of blockchain. (adapted from Ernst & Young 2017)

Benefits and opportunities	Key challenges and risks
• Blockchain transactions can reduce transaction times from days to minutes • Blockchain data is complete, consistent, timely and accurate • Changes to public blockchains are publicly visible to all parties and create transparency, and all transactions are immutable • Helps reduce counterparty risk and eliminates the presence of third parties or intermediaries	• As a young, still developing technology, there are certain aspects of the technology that may require further development • Policy makers and regulators want to ensure that potential risks are adequately addressed • Most block chains have not taken advantage of production-level testing or the pressure of a live environment • New IT systems pose new cyber security risks, particularly a distributed IT architecture that spans multiple business functions or organisations

Fifthly, artificial intelligence (AI) is a field of computer science that deals with the simulation of intelligent behaviour in computers via cognitive abilities that enable a machine to mimic intelligent human behaviour. They are characterised by the fact that they interact in a way that seems "natural" to humans and learn from these interactions. Other terms and technologies used synonymously are smart machines and cognitive computing.

Even today, so-called "weak" AI applications can perform certain tasks such as recognizing texts. In the future, "strong" AI applications will even be able to control autonomous vehicles, make more accurate weather forecasts, diagnose illnesses, conduct financial transactions or operate and monitor industrial machines. AI often occurs in conjunction with other new technologies, such as IoT, data analytics or Blockchain (RiskNET 2018) (see Table 5.5).

Sixthly, big data refers to a set of technologies and architectures used to extract values from large amounts of diverse data generated at very high speeds. This value or insight is then used to drive business decisions that can impact a company's bottom line. The type of data used is not simply captured and managed by relational databases and is therefore not analysed by traditional analytics or business intelligence solutions (see Table 5.6).

Table 5.5 Opportunities and risks of artificial intelligence. (adapted from Ernst & Young 2017)

Benefits and opportunities	Key challenges and risks
• Reduces human error and increases precision and accuracy in performing tasks • Improves risk management by identifying patterns in large data sets that indicate fraud or other concerns • Intelligent machines can be used to perform certain dangerous tasks • They can adjust their parameters, such as speed and time, and are encouraged to act quickly, regardless of factors that affect people	• Scenarios in which AI systems react unexpectedly to human instructions • Programming and coding errors in the AI software (algorithmic/programmatic bias) • Lack of training and inexperience in dealing with AI • Cyberattacks on AI systems or AI algorithms • Legal risks and liabilities (especially data governance)

Table 5.6 Opportunities and risks of big data. (adapted from Ernst & Young 2017)

Benefits and opportunities	Key challenges and risks
• Big Data enable organisations to build a robust data set that covers all aspects of the customer from all angles • Enables complex analysis and correlation between different types of data sets to provide a real-time view of operations, customer satisfaction, transactions, and behaviour • Large amounts of data have the ability to reduce risk, detect fraud and monitor cyber security in real time	• Analytics data is generated, but not aggregated in a way that is valuable to management • Business and Internal Audit management has difficulty identifying trends in data • Without a hypothesis, correlations are searched that do not have any causality • Organisations lack the resources (software, know-how) to use advanced analytics

No technology in the narrower sense but closely related to the above mentioned technologies are cyber risks. These have gained increased attention recently because more and more systems are connected, communicate with each other and can be operated independently of the location. This means that a potential intruder can cause great impact. Some important cyber risk aspects are explained in the following.

Background Information

On the risk horizon, cyber risks and associated risk assessment and mitigation methods that go far beyond traditional risk management are becoming increasingly important. Experts from the fields of information technology and cyber risk point out that organised crime in Darknet is much better connected than expected to orchestrate agile, sophisticated and complex cyberattacks. In comparison, organisations are very inefficient with their defensive measures. Due to hierarchical corporate structures and the limited cooperation mechanisms within the industry, the costs for highly automated cyberattacks are low and the criminal profits very high.

In this context, it is particularly important that cyber risks are analysed in a sophisticated manner. For example, many highly complex systems such as geolocation satellites, ground stations, vehicle electronics, data networks and software components will communicate with each other at a highly automated traffic control centre for the control of autonomous automobiles. A cyberattack

on only one of the system components can have a major impact on the resilience of the overall system and, consequently, on the lives of users of connected cars. This can be transferred already today to air traffic management systems or smart grids (Romeike 2018, pp. 221–222).

5.1.2 Digital Risk Framework

The digital risk framework depicted in Fig. 5.1 has been developed by the Lucerne University of Applied Sciences and Arts in cooperation with SwissERM. It is based on scientific and practice-oriented literature, in-house research and discussions with experts and many risk management professionals. The aim of the framework is to provide companies a tool for risk identification in the area of digital transformation. In the following, the digital risk framework is briefly explained.

Core Elements of the Digital Risk Framework

As we know, a risk may have negative or positive impacts on business objectives and can influence strategy development and execution. The digital risk framework is based on the well-accepted premise that digital transformation generally includes upside potentials (opportunities) when appropriately embedded in the company's strategies. Thus, accepting this premise, the focus of the digital framework lies on the specific risks associated with digital transformation. They are explicitly presented in column form according to different risk categories (see Fig. 5.1). The following two examples illustrate the basic idea behind the framework:

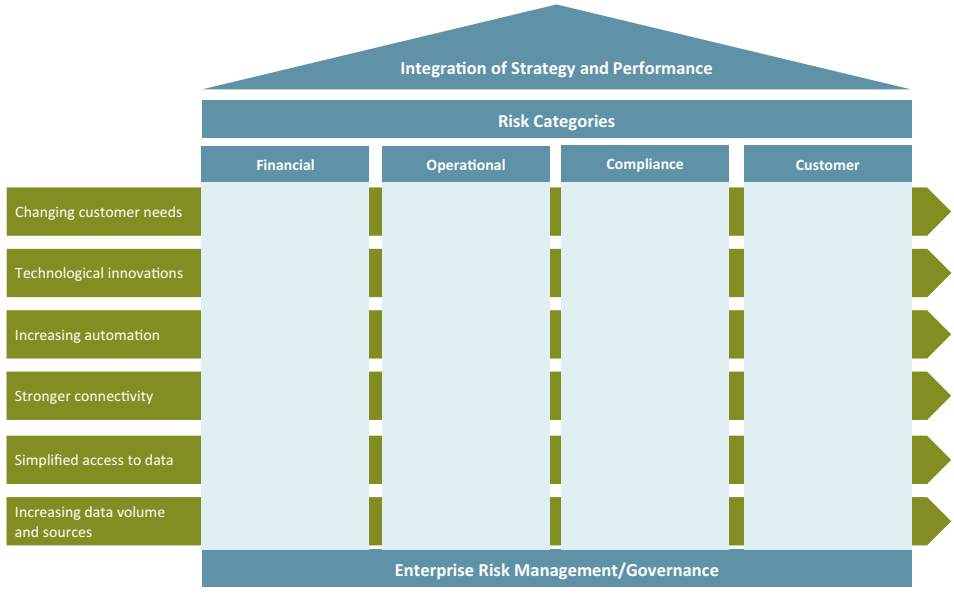

Fig. 5.1 Digital risk framework. (Hunziker et al. 2018, p. 5)

- The transfer of applications to the cloud enables organisations to use data that is always up-to-date, regardless of time or place. In this way, however, the company may also run the risk of being dependent on an external IT service provider.
- The use of data and knowledge about the customer and the services he or she uses opens up the potential of cross-selling for companies. Under certain circumstances, however, there is a risk that the data may fall into the wrong hands (risk source) and be used to the disadvantage of the customer. This can lead to a loss of reputation and possibly legal consequences for the company (impact).

In line with the suggestions of COSO (2017), the digital risk framework links the risks associated with digital transformation to the company's strategy. Moreover, the foundation of the framework comprises the ERM process and a well-established governance structure. ERM of course focuses on the identification, assessment and reporting of (digital) risks. Good governance covers topics such as risk culture, the establishment of a common understanding of values and organisational aspects.

Drivers of Digitization

Digitization is characterised by technological innovations, changing customer needs, increasing automation, stronger connectivity, simplified access to data, and increasing data volumes and sources. These drivers are causing changes in the business environment. As a result, organisations must adapt to new circumstances, digitally transform their business model and value chain to compete with existing and new competitors. As part of this realignment, new technologies can significantly support businesses. This change process can have a positive impact on a company in terms of new opportunities (rewards) as well as a negative impact in terms of (downside) risks.

It is a challenge to look at individual drivers of digitization in isolation because they influence each other. For example, technological innovation creates the prerequisites for increasing automation, stronger connectivity of people, systems and objects, or increasing data volumes and sources. On the other hand, changing customer needs, for example, are driving the need for more computing speed and larger memory capacities, i.e. technological innovation. In addition, stronger connectivity allows the increasing automation of business processes. The following listing illustrates examples to introduce some important drivers which accelerate digital transformation (Hüther 2016, pp. 4–8; OECD 2015).

- Technological innovation. This is the progress that enables the establishment of digital offers and processes. The internet, broadband networks, mobile applications, IT services and hardware form the basis of the digital economy and are considered as a growth and innovation engine. As already mentioned above, technological innovation in turn has a strong impact on other influencing factors.
- Changing customer needs. The customer need is the basic requirement for a (potential) relationship between the company and the customer. Accordingly, companies align their services and products with customer needs by providing corresponding

services and products. These customer needs are influenced by a variety of factors such as availability or individualization and the resulting need for innovative offerings. For example, orders are increasingly to be placed and delivered quickly via online channels, independent of time and place. Wherever possible, offers should be specifically tailored to personal needs. In addition, there is an increasing need for transparent information.

- Increasing automation. Automation refers to the use of machines or technologies to carry out a process increasingly without human intervention (robotics). The learning ability of the systems (AI) plays an increasingly important role here, as they learn from the past and carry out processes independently. Examples can be found in the automatic exchange of data or the control, regulation and monitoring of processes.
- Stronger connectivity. Technological developments simplify the connection and communication between systems. The combination of the resulting links can be called connectivity. In the production process, for example, infrastructure, plants and machines can be connected with each other and exchange data in real time. Similarly, digital networks between manufacturer and customer enable the control and optimization of services and products.
- Simplified access to data. The ability to access information has become much easier via internet and related technologies. Today, a large amount of data is available electronically in various forms. Databases, statistics, books, journals, newspapers, learning content, etc. can be accessed online. This also includes more and more company information that can be collected via various channels.
- Increasing data volume and sources. The simple recording of data (text, photo, film, etc.) promotes the input of data from different sources and thus the amount of data available. For example, trips can be recorded via apps/board computers and the corresponding states (traffic, road condition, route selection, time expenditure) can be assessed based on these data. Many other examples can be found in the social media (Instagram, Twitter, Facebook, LinkedIn, Foursquare, etc.).

Risk Categories

The four risk categories financial risk, operational risk, compliance risk and customer risk form the supporting pillars of the digital risk framework—and thus the link between the foundation (ERM process and governance) and the "strategic roof" of the framework. In this context, however, it is important that the risk categories are not assessed independently from strategic objectives and that risk interdependencies are taken into account as part of the holistic risk assessment. The four risk categories financial, operational, compliance and customer risk are drawn from the COSO ERM framework (2017, p. 85).

- Financial risks include, for example, unexpected changes in financial markets, prices and tariffs, liquidity supply/demand or currency fluctuations.
- Operational risks are unexpected changes in connection with ongoing operations such as personnel, technology, processes or catastrophes.

- Compliance risks comprise unexpected changes that arise, for example, from legal sanctions and reputational damage or from the violation of legal requirements.
- Customer risk include unexpected changes in customer needs, e.g. as a result of new technologies or social trends.

The analysis of digitization drivers and their influence on the digital transformation of companies and thus the risk landscape is complex and multi-layered, as the following risk catalogue illustrates.

Risk Catalogue

The risks of digital transformation are defined along the four risk categories introduced in the digital risk framework. In addition to extant literature, empirical studies and diverse subject matter experts have been used to derive the following risk list presented in Table 5.7.

Table 5.7 Risk catalogue of digital transformation risks. (Hunziker et al. 2018, p. 5)

Financial Risk	Operational Risk
• Loss of value of (crypto) currencies through automated trading • Errors in automated payments • Data loss/manipulation in the financial sector • Incorrect creditworthiness analyses of new business models • Low liquidity due to high IT investments • Slow monetization of digital strategies/offers • Outdated financial indicators for managing the business model • Low profitability of the digitised business model	• Dependence on external (IT) service providers • Misinvestments in technologies and applications • Loss of control due to automated business transactions • Failure of the (IT) operational infrastructure • Authorization and access problems due to new authentication methods • Lack of digital competence among employees • Internal resistance to digital innovation • Insufficient data management and generally incomplete information
Compliance Risk	**Customer Risk**
• Theft of intellectual property/sensitive data • Violation of privacy laws and policies • Disregard of special cases through automated processes • Non-conformity with new regulations and requirements • Increased risk of fraud through digital networking • Theft/extortion of funds through cybercrime • Unclear liability claims due to shared ownership • Data manipulation by internal and external causes	• Loss or unintentional disclosure of customer information • Low willingness to pay due to high price transparency • Competition from innovative organisations • Reputation loss on social media channels • Lack of digital interfaces to (potential) customers • Loss of customers due to discontinuation of business segments • Low customer loyalty due to increasing comparability of offers • Unfulfillability of fast process and order processing

It should be noted that this list does not replace every company's own risk assessment, but may be used complementary.

5.2 Digitization of ERM

ERM methods and techniques relevant to most companies today were developed before the turn of the century. In fact, ERM is often not yet ready to deal adequately with risks in today's digital world. More importantly, if ERM is implemented a stand-alone process (regulatory risk management approach), it cannot support companies to face the dynamic realities of the 21st century (see similar DeLoach 2017). Digital risk management is a term that encompasses all digital approaches to increase effectiveness and efficiency in order to take full advantage of the advances in digital, cloud, mobile and visualization technologies—specifically process automation, decision automation and digitalised monitoring and early warning (Ganguly et al. 2017).

The digital ERM approach leverages workflow automation, optical character recognition, advanced analysis (including machine learning and AI) and new data sources, as well as the use of robotics and interfaces. Digital risk management essentially means a concerted adaptation of processes, data, analysis and IT, as well as the entire corporate structure including talent and culture (Ganguly et al. 2017). Deeper and more insightful risk information helps organisations with strategy development, performance management and decision-making processes (DeLoach 2017).

Providing a new technology platform is certainly not enough to address the digital ERM challenges. It requires that such platforms are equipped with configurations and data so that companies can use it immediately with adequate effort. Basically, three dimensions of change can be identified: processes, data, and organisation (McKinsey 2017):

- To realise full advantage of process and decision automation, companies must ensure that systems, processes and behaviours are adapted to their purpose. In many companies, silos still exist, which is why an isolated risk assessment is often carried out. As a result, current processes have evolved organically, without a clearly defined final state, so that process flows are not always rational and efficient. Operational structures must be redesigned before automation and decision support can be activated. Figure 5.2 shows which sub-processes of ERM are to what extent affected by digitization.
- Data, analytics and IT architecture are the most important prerequisites for digital ERM. Highly fragmented IT and data architectures cannot provide an efficient or effective framework for digital risk management. Therefore, a clear institutional commitment is needed to define a data vision, update risk data, establish robust data management, improve data quality and metadata, and build the right data architecture.

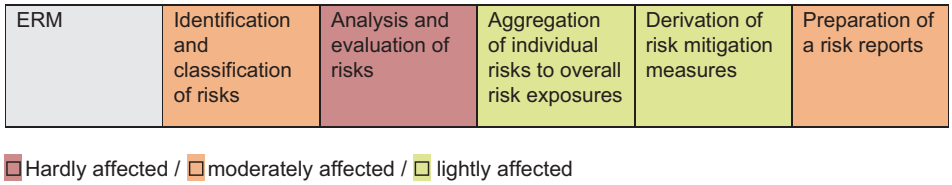

Fig. 5.2 Impact of digitization on ERM process steps. (Kirchberg and Müller 2016, p. 91)

Fortunately, today's processes and analytical techniques can support these goals with advanced technology in several key areas, including large data platforms, the cloud, machine learning, AI, and natural language processing.

- The business and operating model require new capabilities to drive rapid digitization. Although risk innovation takes place in a very specific, highly sensitive area, risk practitioners need to create a solid culture of innovation. This means deploying the right talent and fostering an innovative "test and learn" mentality. Governance processes must enable rapid responses to a rapidly changing technological and regulatory environment. The risk-adequate management of this innovation culture represents a central challenge for the digitised ERM function.

AI in the Risk Management Process

While the AI is still under development, it can already be used to reduce risk in some key areas. For example, machine learning can support more informed predictions about the probability of a person or company defaulting on a loan or payment, and it can be used to build variable income forecasting models.

For many years, machine learning has successfully detected credit card fraud. Banks use systems trained on historical payment data to monitor payments for possible fraudulent activity and block suspicious transactions. Financial institutions also use automated systems to monitor their merchants by linking trade information with other behavioural information such as email traffic, calendar entries, office check-in and check-out times, and even phone calls.

AI-based analysis platforms can manage supplier risk by integrating a wide variety of information about suppliers, from their geographic and geopolitical environment to their financial risks, sustainability and corporate social responsibility scores. Finally, AI systems can be trained to detect, monitor, and defend against cyberattacks. They identify software with certain distinguishing features—for example, the tendency to consume a lot of computing power or to transfer a lot of data—and then close the attack (Boillet 2018).

Most companies are planning to digitise their ERM relatively slowly and follow modular approaches for specific areas. A few have already undergone major change and made significant and sustained progress in terms of efficiency and effectiveness. A clear strategy needs to be developed that does not neglect corporate structures and corporate culture.

5.3 Using Multiple Sources of Data

For organisations and their risk managers, the modern definitions of the digital and interconnected world are big data, data analysis, predictive analytics and prescriptive analytics (Romeike 2017, p. 60). Companies such as Google and Amazon, which have large amounts of data at their disposal, measure the world, create personality profiles and search huge amounts of data for patterns and contexts at lightning speed to enable real-time predictions. The new methods of data analysis promise more targeted analyses and evaluations. Companies are also hoping for accurate forecasts of future developments, e.g. to minimise risks and better assess the opportunities for future action.

More and more people are using the internet and they are constantly producing data via their mobile phones, fitness bands, intelligent watches, networked navigation devices and cars. Companies with extensive data analysis allegedly know many secret desires better than people do. Data and algorithms can be used to anticipate potential events before they are even planned (e.g. next purchase). Behind all technologies are analytical methods from the world of quantitative ERM. For organisations and authorities, answers to questions about "where and why" are becoming increasingly important (Romeike 2018, p. 4).

An interconnected world with more data can lead to growth potential, but also entails more systemic risks. Because systems are interdependent, any event in this chain can spread rapidly. Automatisms and synergies reinforce the effects. Big data is a term that describes a large collection of different information sources, most of which are unstructured and sometimes generated as a by-product of other activities. The relevance to the use of big data is increasing not only in business but also in risk management, which benefits from the advantages of such analyses. For example, the data associated with card payment history, or the news and rumours in the press or even in social media, can all be used to gain knowledge about ERM. More useable data enables ERM professionals to better understand risk, continuously monitor and more effectively reduce business risks. For internal risks (e.g. bad debt losses or contractual penalties due to delivery delays), key figures (e.g. payment delays or safety stock fluctuations) are suitable, which can be aggregated with appropriate applications, continuously updated and displayed on risk dashboards. Deviations from defined target values trigger automated notifications and indicate acute need for action (see similar Brooke 2018).

In the following, selected application possibilities of big data in risk and compliance management are shown.

- Fraud detection: big data is used to feed machine learning algorithms that specialise in pattern detection. In case of possible fraud, this will be useful as changing the business as usual could signal malicious activity. The data included in the analysis can be changed at will, such as the geolocation, the type of device used to connect to the account, or the amount transferred. The identity of the parts involved in the

transactions is also a possible warning sign. The main advantage is that this type of fraud detection can trigger a warning through real-time processing and stop the operation until further authorization, thus minimizing the risks (Brooke 2018).

- Enhanced scenario analysis: before the emergence of big or smart data, scenario analysis and simulations were difficult to create and had inaccurate results. The ability to use large amounts of information increases the accuracy of the analyses and speeds up the decision-making process. The challenge at the moment is to find the perfect balance between the number and volume of simulations and speed limits. A well-known aid for this task is the already in this textbook introduced Monte Carlo simulation, which is supported by parallel computing over distributed systems. The result indicates the value-at-risk for a portfolio or the expected value, e.g. of sales, within a given time period (Brooke 2018).
- Develop new business models: the risk of new business models has so far been calculated both through audits and due diligence or through the evaluation of financial ratios. But these proxies do not tell the whole story, especially for new entrants. Thus, hardly any start-up company with an idea worth millions of dollars would qualify for financing. Here, too, Big or Smart Data is faced with the task of redefining risk measures and creating new valuation approaches. Some organisations today use more than thousand data points per application to measure creditworthiness, and they take much more than just credit history or income into account (Brooke 2018).
- Use the blockchain to validate applicants in advance: ERM is not carried out according to decades-old standards, but can be adapted to the situation. The introduction of blockchain technology, based on big data, can provide a way to track a person's history to their point of entry into the network. This new way of capturing business can eliminate the need for current risk mitigation measures. A risk score could be automatically calculated for each event and assigned to each account. This could mean that an applicant for a loan or smart contract would not even have to reveal his identity, but could be pre-validated by the network (Brooke 2018).

The risks associated with these applications known so far are only a handful of the dangers that will arise as technology advances. Big data's analysis should be able to identify cyberattacks in a similar way as it detects fraud, and have real-time mechanisms in place to prevent it. Since machine learning is usually a black box, correcting a biased model or its assumptions is more difficult than correcting a deterministic model, so proper testing and calibration should be an integral part of the model definition.

The maturity of data and technology in ERM provides an indication of how advanced the company is in this area. The following three maturity levels in Table 5.8 illustrate this (Deloitte 2016).

Table 5.8 Maturity of data and technology in ERM

Basic	Mature	Advanced
Data is nonstandard with varying levels of quality, and key risk tools exist in silos across the organisation	Automated technology solutions are used to store and analyse risk data. Risk data standards and data quality policy established	Automated and integrated technology is used to store, manage, and report real-time risk data. Risk flags are programmed, and data integrity checks are embedded in business processes

It can be summarised that data generation is unprecedented—over 90 percent of the data currently available has been generated in the last five years. As the ability to manage and access this data has become better and cheaper, companies are exploring the use of multiple and novel data sources to gain greater insight (Oliver Wyman 2018, p. 6). ERM professionals are also faced with the task of recording these developments and translating them into concrete applications. Otherwise, there is a danger that other functions in the company will procure the data themselves or that risk analyses will not correspond to the facts.

5.4 Increasing Demand for Analytic Skill Sets

Data flood, complex regulatory structures, new technologies, new risks and the ever-increasing pressure for greater efficiency and lower costs pose a challenge to ERM professionals. Innovative technologies such as AI, RPA, big data and analytics, machine learning and blockchain are increasingly becoming part of the solution to both reduce costs and manage much larger and more diverse amounts of data. Using these technologies can reduce costs, but it also provides companies with more accuracy and control, more agility, and improved risk analysis and insight into these investments (Culp 2017).

The lack of the skills needed to adopt new technologies, which has always been an issue in ERM, remains a challenge, but with a different twist. There are experienced people with ERM skills and people with technical understanding in areas ranging from data science to AI. However, it is extremely difficult to find and/or develop people who combine these skills into one package. Companies are trying to strike the right balance between risk experience and disciplines on the one hand and a deep understanding of current digital, data and technology tools on the other (Culp 2017).

This makes it clear that risk managers must also develop their methodological skills. The focus should be on issues involving techniques and methods for identifying, extracting and processing data for processing with analytical software and data visualization. An ERM professional should have the necessary skills to effectively organise and combine different data sources for analytical applications to address real business risks and challenges.

Among others, basic knowledge of data analytics must be acquired. The following list shows the four maturity levels in data analysis (Romeike 2017, pp. 60–61).

- Descriptive analytics deals with the question "what happened?", i.e. an analysis of data from the past to understand potential effects on the present (see business intelligence).
- Diagnostic analytics deals with the question "why did something happen?", i.e. an analysis of cause-effect relationships, interactions or consequences of events (see business analytics).

  Using techniques such as drill-down, data discovery, data mining and correlations.
- Predictive analytics deals with the question "what will happen?", i.e. an analysis of potential future scenarios and the generation of early warning information. Based on data mining technologies, statistical methods and operational research, the probabilities of future events are calculated.

  Using techniques such as regression analysis, forecasting, multivariate statistics, pattern matching, predictive modelling, and forecasting.
- Prescriptive analytics deals with the question "How do we have to act in order for a future event (not) to occur?", i.e. measures are simulated based on the results of predictive analytics, such as stochastic scenario analyses and sensitivity analyses. Using techniques such as graph analysis, simulation complex event processing, neural networks, heuristics, and machine learning.

The higher the maturity level of the data analysis, the more value is basically created for companies. Accordingly, the lower levels are more focused on information, while the higher levels are focused on optimization. The following example illustrates a company at a high maturity level of data analysis.

Swisscom: Comprehensive customer reporting

For organisations, customers are sometimes a black box whose characteristics and needs are largely unknown. In many organisations, different departments are busy collecting data and manually creating reports to learn more about their customers. At Swisscom, those responsible try to replace complex reports, which can only be carried out selectively, with an automatic real-time analysis. Predictive analytics is used to learn more about general customer behaviour. Instead of just accumulating individual properties, an overall picture should be created. The more information about customer needs is available, the better the specialist department can respond to customers and act accordingly. Swisscom always handles this data with care, as data protection always remains the top priority when dealing with customer data.

Swisscom uses predictive analytics at various levels: Carrier billing enables customers to pay for apps, digital services or products by mobile phone bill. In order to be able to make forecasts, it is necessary to find previously hidden relationships in the data records: Which customers use which services? Are 25-year-old Android users

more reliable payers than 40-year-old iPhone users? Is there a correlation between the type of mobile phone subscription and the type of products purchased? The calculation model tries to give answers to many such questions. Depending on the result, more suitable products can be offered, discounts can be given on preferred services or customers can be imposed a spending limit.

In order to provide answers to all questions, the data analysts used several dozen variables and searched for correlations between all these variables. These variables contain a variety of information, such as demographics, user behaviour, or previous transactions. Any employee can easily relate two variables to each other using an Excel spreadsheet. But it becomes more difficult with dozens or even hundreds of variables. This is precisely where the potential of automated models lies, which can uncover hidden relationships and undreamt-of correlations.

In order to understand the processes and find the complex correlations of all influencing factors, the data experts first searched explanatively together with experts from the business for possible variables with which the calculations could be carried out. They also had to find out which data sources were suitable and how the data could be used.

Accounts receivable defaults are also analysed. They are among the big unknowns at many organisations. Payments for products that have already been delivered are not paid for, as all mail-order organisations that offer payment by invoice find out. In order to keep the losses as low as possible, individual customers can be provided with an individual expenditure limit. But which customers should be subject to such a limit? Who pays late? Who doesn't? After all, no loyal customers should be frightened away simply because of a single omission. For example, there are customers who regularly do not pay their bills until a few days after the payment deadline has expired. Although these customers do not adhere exactly to the rules, they are still reliable and do not have to be disgruntled with unnecessary reminders. This not only saves administrative effort and thus costs, but also improves the customer relationship in the long term. With the predictive analytics method, such cases can not only be evaluated more precisely, but also much faster and with less effort (Swisscom 2017).

Parallel to data tsunami, there are increasing demands to understand and correctly interpret the underlying logics, laws and cause-effect relationships. Bits and bytes must be accompanied by the ability not only to evaluate but also to interpret the resulting data. And this is exactly where many experts fail in practice. The fact that a pattern exists presupposes that it was created in the past. This in turn does not necessarily mean that a conclusion based on this pattern is valid for the future.

ERM professionals and also big data analysts often fall into the trap if they do not have the difference between correlations and causalities on the radar and consequently misinterpret information and draw the wrong conclusions. A mathematically calculated correlation between two variables—which can only measure linear dependencies—does not mean that the two variables are causally related. This is also referred to as "spurious relationship" (Romeike 2017, p. 61).

5.5 Increasingly Sophisticated Software Tools

In the long term, only those companies will be successful that manage their risks efficiently and weigh up earnings and risks when making decisions. ERM software can support strategic corporate management in this if it meets the necessary requirements (Gleißner and Romeike 2005, p. 155). In principle, the software must provide applications for the entire ERM process. This includes, for example, the identification of risks for the company for which information must be collected and stored. An ERM solution should act as a central data repository. Furthermore, a risk taxonomy (e.g. definitions, classifications, categories and data links or relationships) can be developed and embedded in the solution to enable uniform risk assessments and analyses throughout the company. Finally, effective ERM requires a comprehensive view of different risk types and their impact on each other and in their entirety (RIMS 2009, p. 3).

By using adequate ERM software, several weaknesses that occur during the implementation of ERM in practice can be avoided. These include, for example (adapted from Gleißner and Romeike 2005, p. 155):

- a missing or incomplete risk database
- no risk-relevant information for the different hierarchy levels
- redundant and inconsistent data acquisition
- lack of an overview of aggregated risk exposures related to business objectives
- unclear information and communication processes
- delayed or unfounded decision-making

As ERM is an important information function within the company, a great deal of relevant data is already available in various specialist areas. This means that re-entering data into systems would be inefficient if the data were already available in related systems. Therefore, ERM solutions should be used for integrated data storage so that information can be moved or pulled across the company (RIMS 2009, p. 3).

ERM software available on the market today differs widely in the scope of the functionality it offers, as well as in its analytical capabilities and reporting capabilities. In addition to comparatively simple Excel add-ons, there are complex simulation tools that can be purchased as extensions to the ERP system. Methodologically mature solutions offer methods such as what-if analyses, simulations, risk aggregation, forecasting procedures, mapping cause-effect relationships, data mining tools or advanced analytics, e.g. in the form of neural networks. Some products have integrated management cockpits with drill-down functions that are specifically tailored to the needs of decision-makers (Gleißner and Romeike 2005, p. 159).

The selection of the ERM solution must always be based on the needs of the company. In order to support modern ERM, the requirements listed in the following box should also be considered from a business, methodological and technical point of view (adapted from Gleißner and Romeike 2005, p. 161).

Business and Methodological Requirements for ERM software solutions

- Availability of checklists to complement key risks list
- Preparation of a "risk database" to store all risks, not only key risks.
- Prioritization of risks using clever filters (e.g. according to impact)
- Assignment of a risk owner responsible for assessing and monitoring risks
- Assignment of the most important policies—especially for risk reporting and risk monitoring
- Recording of all significant risk mitigation measures (e.g. also all insurance policies)
- Assignment of risk management measures to each risk, describing the possibilities for reducing or transferring that risk.
- Possibility to link ERM with business planning or controlling
- Allowing quantitative risk scenario development
- Allowing to correct for correlations of risks (correlation adjustment factors)
- Simulation of several risks affecting business objectives simultaneously (MC simulation).
- Linking risk exposures to performance measures (e.g. company value, cash flow, EBIT)
- Assignment of early warning indicators to each risk, which indicate a critical development at an early stage.
- If relevant: calculation of equity requirements, necessary liquidity reserves and a risk-adjusted cost of capital rates.
- Offer linking the tool to a variety of other data sources
- Offer integration with strategic planning
- Possibilities for the analysis of large data sets for the identification of risks and anomalies
- Extension or integrated functionalities for advanced analytics, data visualizations and trend analysis
- Functionalities to support (risk-oriented) corporate planning and company valuation
- Possibilities for creating risk dashboards, linked to business objectives.
- Possibility to present risk and opportunities related to business objectives in a meaningful way (no risk maps, rather tornado diagrams, bar charts and risk distribution charts)

Buying software is not as easy as buying a bar of chocolate. It requires that companies have a thorough understanding of the features and benefits of the software. In short, companies need to know if the functionality offered meets the needs of their business.

Participants in an RIMS survey were asked to list the specific capabilities or characteristics of ERM technology that would help improve the maturity of ERM programmes.

Responses varied, but the most commonly cited skills were dashboards, analytical tools, and automated risk monitoring. Other notable responses included risk maps (unfortunately!), risk registers, and survey and tuning tools. These actions reinforce the need for immediate and accurate information for risk practitioners. These results show that the technology solutions that would be most widely used if available: Risk prioritization tools, analysis software, predictive models and simulation. So, based on the survey data, the ideal ERM technology solution would include the following features (RIMS 2011, p. 9):

- Web-enabled "single source of truth"
- View of risks at multiple levels
- Automated risk input
- Auto reporting and calculations across the collected data
- Ability to set and calculate risk tolerance levels or triggers
- Project management capabilities
- Import/export capabilities in order to expedite the sharing of risk information and actions
- End-to-end tracking of risks as they are identified through their eventual resolution
- Common and consistent approach, traceability of account-ability, ownership and actions

Potential buyers and users of ERM technology should develop a clear understanding of what they are trying to achieve before they start looking at the available technologies. They should understand their current and intended ERM maturity levels (see Sect. 3.6.2) before looking for tools to support their business objectives. There seems to be considerable scope for the use of multiple technology tools in the ERM process, and it is unlikely that a single set of tools will meet all requirements. The decision to purchase a technology tool should include a cost-benefit analysis of the tool. Direct and indirect costs for the tool can be very far-reaching, but without a clear return on investment (ROI) it can be unwise to continue with the purchase of tools (RIMS 2011, p. 9).

5.6 Networked Economy and Collective ERM

Today more than ever, companies and people are connected with each other and operating as networked ecosystems. The modern enterprise produces and captures more data and business results, with people communicating more of this information more frequently through a variety of new communication platforms. Put simply, we all produce and share more knowledge at the workplace than at any other time. It is this culture of constant communication that risk managers should use to develop ERM solutions and strategies. A greater proportion of people in the workplace are now able to share experiences and results that can contribute to the development of ERM controls, contingency plans and mitigation plans (see similar Cammsrisk 2017).

Table 5.9 Opportunities and challenges of collective ERM. (Deloitte 2016)

What are the opportunities?	*What are potential challenges?*
• Use collaborative practices such as gamified crowdsourcing to reduce ERM costs and improve its effectiveness • Form alliances with risk experts, researchers and scientists to keep abreast of the latest threats and mitigation approaches • Take an ecosystem-based approach to ERM by forming industry-wide partnerships and consortia	• Possible follow-up costs, regulatory measures and damage to reputation if sensitive information is passed on via partners or data exchange portals • The results can be manipulated if bad actors deliberately enter inaccurate data to distort the models

As a result, they also share more risks. Increasingly, they are managing risk in a manner that reflects this new reality—transforming their risk processes through more open, collaborative approaches that rise to the challenges of a networked economy and working to identify, manage, and reduce risk together. But this new reality will also bring new challenges. Thus, companies should be prepared to take advantage of an increasingly networked business environment to identify, manage and report risks (Cammsrisk 2017). Table 5.9 illustrates some basic challenges and opportunities associated with collective ERM.

Companies might also form alliances with risk experts, researchers and scientists to keep abreast of the latest threats and mitigation approaches, and consider forming industry-wide partnerships and consortia (Deloitte 2016).

5.7 Improving ERM Skills

ERM, as we still know it today, will change in the future. The composition of the risk function will be less characterised by quantification techniques than by innovative and strategically thinking business partners. Because many risk reports (as learned previously), which are mainly based on historical data and usually arrive too late at the desk of decision-makers, will (hopefully) disappear more and more. There will be an increased relevance and impact of non-financial risks, whilst risk profiles will change.

Accordingly, ERM skills will enlarge. Future risk companies must be visionary and able to create added value (i.e. a positive ROI). This can only be achieved by building an effective risk culture across the organisation and by establishing a new mindset. The future CRO will probably still report directly to the board (Simon 2016), but he or she will also need skills that we have not attached too much importance to so far. The composition of ERM jobs and required skills will definitely shift.

One of the key challenges for risk managers is to be engaged as a trustworthy business partner. For the transition towards the new digital and agile world, ERM should reinvent itself by deepening existing skills whilst acquiring new skills for a highly

digitised, innovative and agile company (McKinsey 2017). Some of these skills can be learned, others are intrinsic. Companies have different options to build or acquire the skills they need for the future, e.g. learning, recruitment, reallocation or partnerships (Dowdalls 2018).

Learning/Recruitment: More focus on non-financial risks and a holistic ERM approach is required

The training of ERM professionals often focuses on financial risks. Accordingly, many certifications are offered in this area (e.g. financial risk manager, quantitative modelling, etc.). However, the previous explanations have shown that non-financial risks from the strategic and operational areas have a high relevance. Accordingly, there is often a know-how and experience gap in dealing with these risks (Segal 2011, p. 31).

In general it can be observed that in most courses in the field of financial management, corporate finance, and valuation etc. either no or only financial risk management is taught. This is illustrated by the analysis of the accompanying textbooks, which describe a strongly quantitative risk management approach. Similarly, in the courses of strategic management and analysis, only the analysis instruments such as Porter's 5-Forces, SWOT or PESTEL are frequently taught. A holistic ERM approach in the sense of opportunity and risk management is thus often neglected.

If ERM is part of the curriculum, a basis is laid, but integration into other relevant subjects is often neglected. ERM is characterised by the fact that it is an interdisciplinary subject and the relevant links to accounting, strategic management, financial management etc. must be pointed out. Aspects of psychology (cognitive and motivational biases) and change management should also be linked to ERM.

The future role of the ERM professional can be determined by dividing the role into a number of dimensions. The focus will continue to be on fundamental ERM activities such as governance, risk analysis and risk reporting. Important developments can be identified around this. Each of these developments, in turn, requires a shift in the required skills of the ERM professional (see Table 5.10).

The role of the future ERM professional must be translated into the necessary skills (Dowdalls 2018). Surprisingly, many of these skills can be observed in people playing online games. Gamers are used to large, complex, social systems that are constantly changing. Games must therefore be able to attract and win the attention of their players because they are always new. It is very similar to the change we are seeing in many companies today. The pace and intensity of change in all companies are constantly increasing and so is the risk exposure (Simon 2016).

Many of the character traits needed for success in the future of risk management are in the gamers and these traits will help them to thrive as ERM professionals. Research done by Thomas and Brown (2011) highlights these five key character traits of gamers.

1. Focus on the bottom line: In the games that these online players are playing, each player is constantly being measured and assessed. Each player is ranked and compared to other players using systems of rankings, points, and titles (Simon 2016). This trend makes it clear that risk management will have to concentrate more on strategic

Table 5.10 Role of the risk manager of the future and the associated business value. (Dowdalls 2018)

Dimension	Role of risk managers of the future (examples)	Business value (examples)
ERM foundation	The risk managers of the future have a good understanding of business and a high organisational sensitivity. They proactively question the company, ensure that it operates within its risk tolerance and are the gatekeepers of the principles and standards of risk management	An effective balance between value creation and value objectives, while protecting reputation and maintaining the organisation's risk appetite by avoiding unnecessary risks and surprises
Strategic direction of the company	The risk managers of the future anticipate the effects of the strategic orientation, translate them into improvements in guidelines, procedures and techniques and anchor them in daily practice. They are driven by curiosity to understand the most important developments in the business world	Enable the company to develop and manage its systems, products and regulatory functions effectively and efficiently within risk appetite, while avoiding unnecessary cost growth as the company grows further
New ways of working	The risk managers of the future will work seamlessly with the company and feel comfortable in the rapidly changing business environment. They advise the company on the design and implementation of effective control environments using the principles of control-by-design and compliance-by-design	Increasing the pace of sustainable innovation through timely and effective identification and mitigation of potential risks and issues that allow faster decision making
Digitization and automation	The risk managers of the future are familiar with systems, data and disruptive technologies and keep abreast of trends in information technology and data sciences to ensure that they can challenge and advise the company on pitfalls, risks and problems	Leverage data exploration and modelling insights that enable management to make better and faster decisions based on reliable data
Increasing regulatory pressure and need for trust	The risk managers of the future are strong representatives of the 2nd line of defence who work closely with business, law and compliance to understand the impact of legal and regulatory requirements on business and protect the bank from unacceptable risks	Compliance with regulatory and industry standards for risk management, reducing the likelihood of fines and regulatory intervention

opportunities and risks. After all, these opportunities and risks ultimately determine the success or failure of a company (IRM 2017, p. 5).

2. Diversity is good. Gamers realise that they cannot do everything themselves. To be successful in a game, players often have to form strong teams. The teams that are most successful are those that consist of a strong mix of skills and talents (Simon 2016). This principle can be illustrated, for example, by risk identification. As a rule,

people with different experiences and skills will identify the opportunities and risks of a company more comprehensively. The same applies to further steps. A balanced risk assessment, for example, can only be achieved by discussing different views.

3. Change is good. Gamers thrive on constant change. The worlds in which they play is changing unexpectedly and nothing is constant. Even their own actions transform the world in which they play. Gamers are used to these massive changes and even demand them (Simon 2016). Organisations, too, are facing ever faster change. Accordingly, risk managers have to familiarise themselves with new circumstances. They have to get used to the fact that assumptions and decisions are constantly questioned and a high degree of flexibility is required (IRM 2017, p. 4).
4. Learning is seen as fun in games. The games in which the players participate consist of complex challenges that have to be mastered as quickly as possible. These challenges make the game so enjoyable. The discovery of the tools needed and the creation of the knowledge required to overcome challenges is what makes problem solving an entertaining activity (Simon 2016). Risk managers have to adjust to the fact that routine tasks are becoming less and less. Rather, the future will be about meeting challenges with creative approaches. For example, new approaches to risk sharing may become more important in the context of ERM.
5. Innovation is a lifestyle. Gamers are ready to develop new ideas and solutions to take a step forward. Even if the solution to a problem is known, gamers are willing to look for new solutions that solve the problem faster or with even fewer resources (Simon 2016). Innovative ideas will also be in high demand in risk management. New business models will create opportunities and risks that were previously unknown (McKinsey 2017). It is also becoming increasingly important to use resources in risk management as efficiently as possible. By taking a proactive role in promoting business change and opportunity, risk managers will benefit the company and improve their profile within the company (IRM 2017, p. 5).

In addition to this list, which is based on the abilities of gamers, there are many other categorizations (see e.g. Segal 2011). In this context, it is important that companies define the future function of their ERM department. Based on this, it can be determined which skills are required.

Key Aspects to Remember

Identify the drivers of digitization and analyse the impact for ERM

Drivers such as technological innovations, changing customer needs, increasing automation, stronger networking, simplified access to data, and increasing data volumes and sources characterise digitization. These factors in turn cause changes

in the business environment to which companies must adapt. They may need to digitally change their business model and value chain to compete with existing and new competitors.

Name key digital technologies and assess their opportunities and risks

Risk managers do not need to know every detail and every technical aspect of a new technology. However, they need to understand the full range of opportunities and challenges these innovations present to businesses and markets. The opportunities and risks of the following technologies are in focus: Robotic process automation, internet of things, cloud computing, blockchain, artificial intelligence and big data.

Know possible data analytics methodologies and their application in ERM

A risk management professional should have the skills necessary to effectively organise and combine multiple data sources for analytical applications to address real business risks and challenges. Among other things, knowledge in data analysis must be acquired. This includes basic knowledge of descriptive analytics, diagnostic analytics, predictive analytics and prescriptive analytics.

Create an individual set of requirements for an ERM tool for your organisation

The selection of the ERM solution must always be geared to the needs of the company. In order to support modern ERM, the requirements should be considered from a business, methodological and technical point of view. In particular, dependencies to source systems and interfaces, e.g. to the ERM system, must be specifically analysed.

Recognise future skills and competences for ERM professionals

The future role of ERM professionals can be determined by dividing the role into several dimensions. The focus continues to be on basic ERM activities such as governance, risk analysis and risk reporting. Important developments can be derived from this. These include, for example, the focus on the bottom line, a constantly changing environment, lifelong learning or constant innovation in methods and processes.

Critical Thinking Questions

1. Which external data, which has hardly been used up to now, can become important for ERM in the future?
2. Which ERM processes are suitable for using robotic process automation (RPA) to increase efficiency?
3. How should cooperation with stakeholders and other technical reports be organised in the sense of collective ERM?
4. How will the role and job profile of ERM professionals change in the future?
5. To what extent do ERM professionals need to acquire new digital competencies or develop existing ones?

References

Boillet, J. (2018). AI: a risk and a way to manage risk. https://www.ey.com/Publication/vwLUAssets/ey-reporting-ai-a-risk-and-a-way-to-manage-risk/$FILE/ey-reporting-ai-a-risk-and-a-way-to-manage-risk.pdf. Accessed 28 November 2018.

Brooke, S. (2018). How Can Big Data's Potential Be Unleashed for Risk Management? https://towardsdatascience.com/how-can-big-datas-potential-be-unleashed-for-risk-management-e7c62bcd02b7. Accessed 26 November 2018.

Cammsrisk (2017). Top 5 Trends in Risk Management. https://cammsrisk.com/blog/top-5-trends-in-risk-management/. Accessed 26 November 2018.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017). *Enterprise Risk Management—Integrating with Strategy and Performance.* Jersey City, NJ: AICPA.

Culp, S. (2017). Extending The Skills Of The Risk Professional Is The Next Big Challenge In Risk Management. https://www.forbes.com/sites/steveculp/2017/09/20/extending-the-skills-of-the-risk-professional-is-the-next-big-challenge-in-risk-management/#766ebe8f6e40. Accessed 26 November 2018.

DeLoach, J. (2017). Transitioning Risk Management to the Digital Age. https://blog.protiviti.com/2017/10/03/transitioning-risk-management-digital-age/. Accessed 22 November 2018.

Deloitte (2016). The networked economy demands collective risk management. https://www2.deloitte.com/us/en/pages/risk/articles/networked-economy-demands-collective-risk-management-future-of-risk-trend-eight.html. Accessed 26 November 2018.

Dowdalls, A. (2018). Building risk management skills for the future—where to start? https://axveco.com/building-risk-management-skills-for-the-future-where-to-start/. Accessed 22 November 2018.

Ernst & Young (2017). What are the new risks associated with digitization, IoT, analytics and robotics? Presentation Enterprise Risk Summit 9. November 2017. Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern, Zug.

Ganguly, S., Harreis, H., Margolis, B., & Rowshankish, K. (2017). Digital risk: Transforming risk management for the 2020 s. https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s. Accessed 22 November 2018.

Gleißner, W., & Romeike, F. (2005). Anforderungen an die Softwareunterstützung für das Risikomanagement. *Controlling & Management, 49* (2), 154–164.

Hunziker, S., Fallegger, M., & Balmer, P. (2018). *Risiken der digitalen Transformation in Schweizer Unternehmen* (ERM Report 2018). Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern, Zug.

Hüther, M. (2016). *Digitalisierung: Systematisierung der Trends im Strukturwandel—Gestaltungsaufgabe für die Wirtschaftspolitik.* Institut der deutschen Wirtschaft, Policy Paper 15, Köln.

Institute of Risk Management (IRM) (2017). Perspectives on the future of risk. Risk Agenda 2025. https://www.theirm.org/media/3105903/IRM_Risk_Agenda_2025_v8.pdf. Accessed 22 November 2018.

Kirchberg, A., & Müller, D. (2016). Digitalisierung im Controlling: Einflussfaktoren, Standortbestimmung und Konsequenzen für die Controllerarbeit. In R. Gleich, K. Grönke, M. Kirchmann & J. Leyk (Eds.), *Konzerncontrolling 2020* (pp. 79–96). Freiburg: Haufe.

McKinsey (Ed.). (2017). The future of risk management in the digital era. https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era. Accessed 19 November 2018.

OECD (2015). *OECD Digital Economy Outlook 2015.* Paris: OECD Publishing. doi:http://dx.doi.org/10.1787/9789264232440-en

Oliver Wyman (Ed.). (2018). *Next Generation Risk Management. Targeting a Technology Dividend.* Asia Pacific Risk Center, Oliver Wyman.

RIMS (Ed.). (2011). ERM Technology Tools: A Contemporary Look. A Report of the RIMS Technology Advisory Council and RIMS ERM Committee. https://www.rims.org/Sales/Documents/RIMS%20Executive%20Report%20on%20ERM%20Technology%20Tools%20September%202011.pdf. Accessed 22 November 2018.

RIMS (Ed.). (2009). *Enterprise Risk Management Technology Solutions.* New York: Risk and Insurance Management Society, Inc.

RiskNET (Ed.). (2018). Artificial Intelligence. Maximierung des Nutzens von KI durch Risikomanagement. https://www.risknet.de/themen/risknews/artificial-intelligence/cbd8995195a65d462243cf9a17eb2aaf/. Accessed 27 November 2018.

Romeike, F. (2018). *Risikomanagement.* Wiesbaden: Springer Gabler.

Romeike, F. (2017). Predictive Analytics im Risikomanagement—Daten als Rohstoff für den Erkenntnisprozess. *CFO aktuell, 11* (2), 60–63.

Segal, S. (2011). *Corporate value of enterprise risk management. The next step in business management.* Hoboken, NJ: Wiley.

Simon, H. (2016). The Future of Risk Management: Gamer boys and girls as Chief Risk Officers. https://www.linkedin.com/pulse/future-risk-management-gamer-boys-girls-chief-horst-simon. Accessed 22 November 2018.

Swisscom (2017). Predictive Analytics. Daten sagen die Zukunft voraus. https://www.swisscom.ch/de/business/enterprise/themen/digital-business/predictive-analytics.html. Accessed 30 January 2019.

Thomas, D., & Brown, J. S. (2011). *A New Culture of Learning: Cultivating the Imagination for a World of Constant Change.* CreateSpace Independent Publishing Platform.