Brought to you by

servicenow

Digital Transformation & Risk

for dummies®
A Wiley Brand

ServiceNow Special Edition

Understand the risks to your digital business

Chart your course to manage the risks

Accelerate your digital transformation

Vasant Balasubramanian
Barbara Kay
Teddy Guzek
Aaron Pritz

About ServiceNow

ServiceNow makes the world of work, work better for people. Born in the cloud and built for the front line, ServiceNow products seamlessly embed risk management, compliance activities, and intelligent automation into your digital business processes to continuously monitor and prioritize risk. ServiceNow Risk solutions help transform inefficient processes and data siloes across your extended enterprise into an automated, integrated, and actionable risk program. You can improve risk-based decision making and increase performance across your organization and with vendors to manage the risk to your business in real time.

Make risk-informed decisions in your daily work.

www.servicenow.com/risk

Digital Transformation & Risk

ServiceNow Special Edition

by Vasant Balasubramanian, Barbara Kay, Teddy Guzek, and Aaron Pritz

for dummies®
A Wiley Brand

Digital Transformation & Risk For Dummies®, ServiceNow Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-69248-5 (pbk); ISBN: 978-1-119-69246-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie Burchfield-Leighton

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Siddique Shaik

Special Help: Barbara Kay, Colleen Gobin

Table of Contents

Introduction

Digital transformation is a critical priority for many companies across most industries, and it's more than a catchphrase. Digital transformation is truly changing consumer and business experiences. With solutions like Uber and Venmo, we've gone from "there's an app for that" to "there's *only* an app for that."

No industry is immune to these competitive and global pressures, and the changes go beyond the actual products and services. Companies must conduct business where their customers are while marketing and selling their products through mobile, online, or social channels. Businesses must interact with their not-particularly-loyal customers in more simple, efficient, and satisfying ways through the customer life cycle.

It's not the "digital" part that's the biggest problem. "Transformation" means both reinvention and completely new invention. These rapid changes produce all sorts of new — and often unexpected — side effects, including new risks. The companies that rise successfully on the other side of the digital transformation must find ways to achieve speed and quality in the digital world while maintaining trust.

Risk management across everything digital (cybersecurity, privacy, compliance, and so on) is no longer an Information Technology (IT) department-only topic and objective. The more that can be understood and applied across all areas of the enterprise, the more successful companies and their leaders will be.

About This Book

This book is written so employees of transforming companies can read it, understand the content, and better see how they can contribute to the company's success by managing their risks. This book isn't intended to be a prescriptive implementation manual. It's for education and calls out some of the most common examples and elements of digital risk management. You can take many different approaches to risk management, so before embarking on an actual risk program, hire knowledgeable people or engage consultants.

This book equips you with basic knowledge and experience-based learnings to understand and apply risk management. Throughout the book, we include elements about the journey of digital risk management at Acme Corp, a fictitious but realistic example company. These skills matter, whether you're in a formal risk management role or just want to apply good risk-driven behaviors to any role at any level.

Icons Used in This Book

This book uses special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information that you may want to come back to for reference or use to discuss the topic in an elevator.

TIP

Tips are much more than a suggested amount you should wire to the authors for writing this book; they also include nuggets of information that you can apply in your company.

WARNING

Think of these icons as advice around avoiding mistakes or dodging hidden land mines based on the experiences the authors have had directly or learned from others while applying concepts from this book.

Beyond the Book

This book gives you an intro, refresher, or a different simplified point of view on how digital risk can be managed across a company. But if you want to take your knowledge, skills, and acumen to the next level, visit `www.servicenow.com/risk`.

IN THIS CHAPTER

- Following the digital transformation journey
- Understanding digital risk
- Deriving the sources of digital risk
- Looking at digital risk in different industries

Chapter 1
Digital Risk 101

Acme Corp is a global producer of a large variety of products. Acme Corp is beginning to pursue a digital transformation of both the products and the way the company runs. The company has historically thrived through self-contained products that weren't connected to the Internet. As the market advances, Acme Corp needs to make its product more digitally connected, "self-learning," and remotely serviceable.

Risk management hasn't been a real focus for Acme Corp in the past, and the organization has mostly been reactive to security, audit, and regulatory issues. Acme Corp leadership is aware that it has growing digital risk: The big, bold ideas being generated by the Acme Corp Digital Team have the potential to create many compliance, data, security, and privacy risks for Acme Corp. Acme Corp knows it must better understand how risk management could help bring a productive analysis and decision-making approach to the team.

This chapter helps you, like Acme Corp, learn about digital risk, how managing digital risk during a transformation can support productive analysis and decision-making, how risk applies to your company, and where you could help.

Exploring the Digital Transformation Journey

What's so important about digital transformation? Isn't business already digital? Yes, we live an amazingly digital lifestyle, and every year digital technology gets more invisible, sophisticated, and important. Successful businesses — whether they build products (medical devices), services (insurance), relationships (support), or increasingly a combination — have invested and are continuing to invest to stay ahead. *Digital transformation* is a convenient term to reflect the disruptive journey that companies undertake to make use of new, fast, and frequently changing digital technology and business models. It's not about taking old products and simply rebuilding them in the cloud; it's about solving problems better, with more creativity, to create experiences that excite and build fierce loyalty from customers, users, and employees. If your company isn't already talking this way, it should be, or it will inevitably fade away.

Look at previous disruptions: the web browser, the Public Cloud, and XaaS models (consumption-based). Where are the companies that haven't adopted these approaches? They were likely acquired or went out of business — certainly not the kind of company any digital natives would work for, buy from, or — truly — even notice. If digital natives aren't your target customers, consider the competitors entering every market from around the world. Status quo just doesn't cut it. That's why digital transformation is more than a buzzword.

Some of the technologies typically seen in digital transformation include

- Cloud technology
- Software/Platform/Database/Infrastructure-as-a-Service
- Internet of Things (IoT), including mobile devices and sensors
- Big data and advanced analytics

Explaining the Types of Digital Risk

Risks that are considered "digital" have been around since before the age of digital transformation. However, accelerated digitization introduces new risks and amplifies existing risks that many fast-moving companies overlook. Additionally, old ways of managing risks don't always account for these new types of risks, or are too cumbersome to scale.

Does your company address and have plans for managing these new types of risks? Check out this section to see the different types of risks your company may face as you go through digital transformation.

Privacy risk

Privacy risk is the potential theft, loss, or unauthorized disclosure of personal information (customer, workforce, consumer, and so on). With technology innovating ahead of most security efforts, companies have many soft spots for bad guys to go after in their search for this data. Country and regional privacy regulations keep expanding and may affect your business, too. All those cookies you have to accept are part of the General Data Protection Regulation (GDPR), but now there's the California Consumer Privacy Act (CCPA). Both are regulations about how to properly collect, handle, transfer, and store personal information. Because they affect most companies that sell to residents of these two economic powerhouses, they certainly impact most enterprises in some way. In addition, Brazil, India, New Zealand, and many other regions are rolling out regulations in a similar spirit. Factoring in flexibility to support expanding privacy requirements is really just self-defense for a digital business.

WARNING

Some companies may choose to ignore regulatory obligations, thinking that the fines will be less than the effort and expense required to comply. However, data privacy regulations are getting stricter and more complex, going far beyond basic personal identification and credit card numbers. Also, any customer, not just a regulator, can turn you in.

With so many regulations rolling out, the odds of avoiding a problem are much lower, and the costs to recover are much higher than with previous regulations.

Cyber risk

Cyber risk commonly refers to the potential for financial loss, business disruption, or harm to an organization and its reputation caused by the failure of its information technology. A simple example of cyber risk is database breaches. These can be caused by external forces like hackers or internal forces like employees who make mistakes or become disgruntled.

Cyber risk can include any compromise of confidentiality, integrity, or availability of a computer network, database, system, product, facility (including industrial control system), connected device, or application. In this digital age, your digital footprint (things that technology interacts with) is growing faster than you can possibly secure it.

Technology risk

Technology risk includes cyber risk (see the preceding section) but expands the definition to the potential that failures in computer, application, database, infrastructure, and connected devices can cause disruption of your business. Technology risks could come from accidents, acts of nature, or other catastrophes, and this risk isn't limited to within the walls of your company. Many companies leverage third parties, cloud-hosted software, tools, and infrastructure, and the same risks apply to those systems as well.

Data risk

Data officially surpassed oil as the most valuable resource on earth only a couple years ago, and it's not slowing down any time soon. You must be able to protect not only your client data but also your employees' and company's data. You have an ethical responsibility to protect data from both attackers and corporations. Not only do you have to worry about the confidentiality of your data, but also you need to ensure its integrity and availability.

REMEMBER

What's new with digital transformation is the range of ways people can capture and abuse data (with or without meaning to cause harm) and more detailed requirements about data handling. An example would be an insurance company that's branching out into a new business line of travel insurance, requiring collection of new types of personal information that could invoke new regulations. The company must capture, share, use, store, and destroy (when the time comes) this data according to regulations that

vary by geography. The risks and regulatory-required controls around selling or transferring data to other companies make the data landscape more challenging.

Third-party risk

Third-party risk comes from third parties that include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, agents, contractors, and guests to facilities. Third-party risk is the potential risk that comes with businesses being connected or involved with other businesses and entities. These entities could be "upstream" (suppliers and vendors) or "downstream" (distributors and resellers). Many times, large enterprises with many third parties or vendors don't understand the risks of their companies being extended outside their own walls. It is often difficult to measure the risk that outside organizations bring to your company.

REMEMBER

The use of third parties is nothing new — companies have worked with third parties for years. What has changed, however, is the frequency and scale of third-party use and the regulatory focus on how organizations are managing third parties to address the inherent risks.

Talent and culture risk

When you think of digital risk, you may not think of people. The truth is, people might be one of the biggest risks to organizations. You need to make sure you're creating an environment that's ready for the change.

TIP

Create digital-friendly workplaces by training your employees properly. Also, stay open-minded to change and don't be quick to discount early and late adopters.

Reputational risk

Reputational risk is the risk of a negative view of your company to the world. Reputational risk has been around for as long as business has been around, but digital transformation is shrinking our world. A lawsuit, a disgruntled customer, product failure, and a negative review are all examples of threats to a company's reputation and brand. Social media and the Internet create much more visibility and risk to your companies' reputations than in the past. The damage can be expensive to reverse.

Artificial intelligence risk

You've likely interacted with artificial intelligence (AI) already. It's enhancing your online shopping, customer service, and smart devices. The fear of robots taking over the world isn't the biggest concern for companies using AI (although it may become one down the road). What's more likely is that a host of other risks we discuss in this chapter surface in new ways: privacy, cyber, and technology especially.

In addition, the computer models used to build AI systems are susceptible to many issues: Incorrect training data can make a model think a blueberry muffin is a Chihuahua and can make suggestions for pet stores when you're looking for bakeries. Or an edge case situation may gradually move into the "too risky" bucket, with auto-response causing physical harm (think trains, planes, and automobiles). All the devices (including your car, phone, and smart devices) collect information that can drive helpful new suggestions — and violate privacy rules. The knowledge of data scientists, engineers, compliance leaders, designers, and marketing must come together to even think through the possible side effects of AI risk, and then there's the challenge of quantifying and managing the risk. This journey has just begun.

Defining Other Types of Risk

In one way or another, digital transformation has tied most risks to digital risks. There are, however, many other risks that aren't necessarily the result of digital transformation. This section identifies other types of risk, that aren't digital, to avoid confusion.

Regulatory/compliance risk

Regulatory/compliance risk is the risk that non-compliance with a company's regulatory obligations will negatively impact the business. Regulations being created by government bodies are outside a company's control and often difficult to predict. Regulations and the pace of change vary by industry, but some common examples exist in power and utilities, financial services, insurance, medical devices, and pharmaceuticals. The Sarbanes Oxley Act and Gramm-Leach-Bliley Act are examples of regulations that aren't limited to digital risks.

Financial risk

Financial risk is the possibility that your company will incur financial losses. Part of financial risk includes credit risk or the risk behind borrowing money. Financial risk can also tie back to cybersecurity and digital risk related to fraud, digital theft, identity theft, and government fines and fees.

Economic risk

Economic risk is the risk of markets (local, national, world) constantly changing. The markets have been going up and down for a hundred years. As various markets fluctuate based on economic factors, changes to customer demand — both expected and unexpected — can occur. Root causes could stem from failures of national governments, fiscal crises, unemployment, and so on. While many of these factors are difficult to predict, a mitigation plan may include how a company could pivot under certain economic conditions.

Competition risk

Competition risk is the risk that your competitors will outperform you, decrease your revenues, shrink your profits, or put you out of business. There is a connection between cyber and digital risk and competition if unethical competitors or governments use cyber techniques to steal digital or non-digital intellectual property (IP).

Digital Risk in Different Industries

Digital risk isn't the same across every industry. Different industries must address different risks, regulations, and drivers. In this section, we describe various industries and some of the risks they face.

Financial services/banking

The financial services industry is typically ahead of the curve when it comes to ensuring that its systems and sensitive information are secure. They face global, national, and regional regulations that often don't align. It's not all just Wall Street either. Insurance firms fall into this sector and have their own specific laws.

An example of a risk in the financial services industry is digitized financial products. No longer are we in the day of paper checks and cash. Most of your transactions are done online and with digital payments via credit cards. In addition to fraud, banks face scams, money laundering schemes, hacking, physical compromise of devices like ATMs, and more.

Manufacturing

Manufacturing companies are no stranger to risks in their operational technology. These companies live and die by the uptime of their equipment, the timeliness and predictability of their processes, and the quality of their products. Many systems that used to be stand-alone are now connected to the digital world. The end product itself also frequently includes some ongoing digital interaction for support and updates.

While this connectivity provides these companies with incredible efficiencies and insight into their plants and end products, it also increases their attack surface to hackers. In particular, systems often include multiple components, including computers or robots that are often found to be outdated and impossible to update. This increases the risk of a hacker compromising their systems and shutting down their production line. Digitally transformed products usually rely on newer technologies and vendor relationships (like the cloud) that are outside the core competence of typical manufacturers.

Energy and utilities

The energy and utilities industries are ones where the risks could be catastrophic for their communities and their industries as a whole. The technological risks involved may be difficult to wrap your mind around. Take a nuclear power plant, for example. These are incredibly efficient but can be dangerous if the risks aren't properly monitored. In nuclear power plants, sensors continuously monitor and report critical information about the status of nuclear reactors and other essential aspects of the process of generating energy from enriched uranium. These devices are great for monitoring areas that are unsafe for humans to be around. It is imperative that the proper risk management processes are put in place to prevent catastrophic accidents.

Other risks come from the way power is distributed across interconnected grids. These systems are also vulnerable to attack, including physical attack, which could lead to failures.

Healthcare

One industry that must heavily invest in privacy protection is healthcare. Privacy risk is so great for the healthcare industry because it has massive amounts of data, and the attack landscape is large, dynamic, and diverse: people (medical staff, patients, guests); medical and IT devices; information and high-tech medical systems; and tele-medicine and distributed locations. This information is critical and should be properly sanitized, stored, transmitted, and destroyed when it's no longer needed. Multiple business entities participate in every patient transaction, increasing the chance of mistakes and opportunistic crimes. In fact, insider threat is high in this industry as staff can abuse their access to data out of simple curiosity. The loss or improper distribution of patient data could have serious consequences. Therefore, data risk is one of the healthcare industry's top risks.

A good example of how data risk becomes prominent in healthcare is where healthcare practitioners use mobile phones/tablets at the bedside to enter and update patient details, scan drug records, and order services and supplies. Tele-diagnosis and tele-prescriptions are offered at unconventional sites such as schools, retirement homes, and drugstores. With all the potential touchpoints and exposures of these capabilities, having the right risk management plan and associated controls is important.

WARNING

Healthcare tends to have a compliance focus driven from specific laws covering personal health information and mandating electronic patient data systems. Even if the regulations weren't complex, the business climate creates challenges for implementing, monitoring, enforcing, and reporting on compliance. Think about how much change you have seen around you: Consolidation in healthcare providers means multiple systems need to be integrated and maintained, often without the involvement of the people who built them. Intense competition has pushed for cost management through multiple tiers of operations (hospitals, urgent care, wellness centers, drop-in sites, doctors' clinics) and more adoption of cloud-based services. All this complexity is a recipe for a headache.

Recently, ransomware has directly started to impact patient safety as IoT-connected medical devices and equipment become completely locked by encryption. Faced with many different issues at once, the healthcare industry must prioritize actions based on which risks are most likely to impact their businesses, what assets are most necessary to protect, and the cost of mitigating or avoiding the problem.

Retail

Retail companies are in the business of high daily consumer interaction, sales transactions, and targeted marketing. Risks within daily operations include handling credit card data subject to Payment Card Industry Data Security Standard (PCI DSS), identity theft, operational impairment, and other consumer privacy focused regulations and concerns.

In the age of credit card fraud, PCI DSS was created to more effectively govern how companies are storing and transmitting credit card data to help minimize the chances of credit card fraud through cyberattacks. If a company is found to not be PCI DSS compliant, it faces strict consequences such as large fines, legal action, and even revocation of the capability to accept digital payment methods. When you go into stores that say "cash only," it could mean they either have had their privileges of accepting digital payments revoked, or they don't want to deal with the risk of trying to stay PCI DSS compliant.

Hi-tech (technology)

Since the turn of the century, the technology industry has quietly become one of the largest industries. It is also arguably under the brightest spotlight right now as reports continue to come out about the ethics and methods of how these enterprises are using the data they're capturing. For companies that make trillions of dollars off user data, regulation around privacy is sure to be one of the top risks for these companies.

Regulations like GDPR and CCPA have been put into place to help protect consumer data from being monetized and/or being used in unscrupulous ways. These regulations require companies collecting data to allow consumers to, among other things, opt out of the

sale of their data. For example, if a large Internet tech company takes what a consumer searches for on the Internet and sells it to a marketing company to help market products to the consumer without her permission, it will face strict consequences, such as large fines.

REMEMBER

Regardless of what the regulations require, consumer trust is becoming more of a key focus for the tech sector because of publicized breaches, fines, and congressional hearings. Beyond confidentiality risks and data trust, availability and integrity of critical systems and data in the tech sector are critical as more and more companies rely on shared cloud hosting of systems and data.

IN THIS CHAPTER

- Handling digital risks
- Spotting key digital risks
- Knowing your key stakeholders
- Choosing a platform

Chapter 2
Preparing to Tackle Digital Risk

After Acme Corp better understands risk management concepts, examples, and context in light of its desired digital transformation efforts (like you can do in Chapter 1 of this book), it needs to prepare for how it's going to move forward in implementing risk management practices and processes.

The company first evaluates its risk management maturity (in a broader context) to determine where its starting point is and then develops plans to surface, assess, and prioritize digital risks. Acme Corp realizes that risk management won't be successful without the right stakeholder buy-in and involvement. It also realizes that trying to do all this informally or via home-grown spreadsheets could overly complicate and paralyze the process.

This chapter describes the answers and recommendations to those challenges.

Handling Digital Risks Today

In Chapter 1, we describe various types of risks that can come up in the digital transformation journey. However, the diversity, scale, and pace of the digital technology being used requires different methods of surfacing and aggregating these risks.

REMEMBER

Everyone needs to start with an internalization that digital risk is real, and managing it is a journey. The best first step is an honest self-assessment to understand where you are on the road. This section helps you self-assess and address what that means and why it's important.

Level 0: Huh?

What is a digital risk?

Good news: If you're reading this book, you're probably past this step. Awareness and understanding are the first steps toward progress. Also, don't worry; plenty of leaders haven't dug into understanding and acting on their digital risks.

TIP

How to improve: If you need to brush up on digital risk, see Chapter 1 of this book.

Level 1: Meh, doesn't impact us.

I've heard the buzzword, but that doesn't apply here. No one wants to steal or disrupt what we do here.

This state of maturity and behavior is a bit like sticking your head in the sand. If business leaders don't acknowledge that digital transformation results in new risks that impact them, the right action and funding won't be present. Perhaps there are some exceptions such as a manual typewriter-driven word processing company that only communicates via phone and the postal service — does this even exist anymore?

TIP

How to improve: This situation requires sharing real examples of where risks may reside in the organization's digital transformation journey. Benchmark against other companies like yours that may be ahead of you, or have had to learn from public-facing incidents. While you don't want to solely rely on scare tactics (sometimes called fear, uncertainty, and doubt, or "FUD"), real

examples and peer company references can go a long way to educating executive stakeholders on why they should care. Education won't be enough, either. Tying the chance of an issue to the related cost of it happening will be the best way to motivate business leaders to prioritize this process. This is the essence of risk-based decision-making.

Level 2: Sure, call IT.

I understand the importance. IT probably has that under control.

Just as a company's digital transformation can't be isolated within IT, the management of the related risks also can't be managed in an IT silo. If you are in IT and feel 100 percent ownership of digital risk, you're missing the executive sponsorship and business engagement. While it's great that someone in IT is attempting to move things forward, this rarely has the potential to holistically manage digital risk and get the right sponsorship/budget to mitigate things in the right way.


TIP

How to improve: This one can be trickier to solve because organizational structure and culture largely set the starting point for many companies. Developing a cross-organizational risk management strategy can help identify the "people" and "process" elements required to be successful. In many cases, this requires involvement of key stakeholders across the company, including legal, line of business owners, and finance, and getting to the true owner of digital assets. Influencing change through surfacing ownership, gaps, and needs is your best bet to improving sponsorship and success of a program.

Level 3: Progress.

We have some risk management efforts in place in pockets but haven't gotten to scale across the organization.

After you have pockets of risk management activities underway, you want to maintain momentum and enhance processes while looking ahead to create efficiencies. Many organizations implement separate tools and processes for each area of risk management, which is okay until you need to scale and start to connect data and reporting for executives and auditors. Email and spreadsheets won't cut it for long. You will likely find that varying tools and processes across departments can be difficult to integrate.

Companies that get stuck in this phase are doing some good things but never really seem to get to a solid enterprise scale. With digital transformation, pressure will likely increase until something breaks — at which point you start looking for a fix.


TIP

How to improve: Companies that want enterprise scale and integrated insights must consider a platform for efficiency and accuracy. Look for tools that use modern approaches (also known as the cloud and a unified data model) and offer lightweight configuration (versus expensive customizations and heavy support staff needs). It is also important to find solutions that can automate routine tasks to achieve desired efficiencies.

Level 4: Optimizing!

We have a fully integrated platform, processes, and sponsorship. We're continuously making improvements to our risk-enabled decision-making.

Congratulations! Few companies have attained this level of maturity.

At this point, business stakeholders are making risk-informed decisions. A risk-aware culture generally permeates across the organizations. Companies that have achieved enterprise scale on a common platform are in the best position to optimize both the risk-based decisions that are made and the risk management processes and staffing.


TIP

How to improve: At this point, continue small improvements to staffing and processes. Look at where people — your users, vendors, customers, and auditors — spend the most time, and consider how to make those processes simpler and faster, perhaps through mobile apps, a self-service portal, or chatbots that act like human agents but use artificial intelligence to answer questions and initiate processes. Look outside what you are already doing for areas around the company that are starting to transform, and engage with those stakeholders. Discuss the types of risk they might face, and how to minimize them. Risk is everywhere: in marketing, in product development, in accounting. It's at the heart of every business opportunity. The more you proactively integrate risk controls and processes into emerging business programs and projects, the easier and less expensive it will be to manage risk overall.

Knowing What Good Looks Like

Building a solid foundation of risk management is a critical first step to any program. After you build this foundation, it will support the organization's strategy, people, processes, and technology.

This solid foundation is made up of four things:


REMEMBER

- A shared understanding of risk across your organization
- A sound risk and compliance culture

  Strictly speaking, this isn't a foundation but rather a goal, but it's an important element that can be established at the beginning and iteratively improved over time.
- Executive sponsorship
- A single source of truth (a reliable and consistent place to go to understand risk)

With these foundational elements in place, businesses can take the right steps to evolve from managing compliance and risk with ad hoc manual processes to making risk-informed business decisions and providing holistic risk visibility to the Board.

Beyond these foundational elements, your risk management program needs to have strategic elements:

- **A vision:** Your program needs a vision. What do you want to achieve and why? How does risk management contribute to your company's digital transformation and enable longer-term success? Be sure to tie what you are doing to the bigger picture, so risk is understood as central to the business.
- **Objectives and goals:** What are your objectives/goals for the year and/or over a multi-year horizon? What milestones can you celebrate along the way? This journey won't be simple, so set both strategic and practical goals.
- **An operating model:** What operating model will you need to get started, and how will it evolve as your processes and technology around risk management get better? An operating model includes core people, process, and technology elements and really is the glue that makes everything work together. Things may be more manual upfront.

- **A measure for success:** Finally, but possibly one of the most important points, how will you measure success through a set of key performance indicators (KPIs) and key risk indicators (KRIs)? Make sure you include ones that matter to executives so you can communicate your program in a way they can understand and value.

REMEMBER

Your strategy should tell a clear and compelling story as to why risk management will yield positive outcomes to enable your company's digital transformation. Being able to tell this story helps your risk program get the resources necessary to be successful. After you get the proper resources, delivering and measuring value against your strategy are paramount to keep your momentum in managing digital risk.

Recognizing Your Key Digital Risks

Chapter 1 describes digital transformation and types of digital risk in general. In this section of this chapter, you explore *where* you can find digital risk across the company. Check out these locations:

- **Business operations:** Look in business operations that are increasingly digital and investing in new capabilities. Prioritize where you start, and focus based on the potential risk of compromise of those business operations or the systems within them. Look in business functions, such as IT, Finance, HR, Legal, Manufacturing, R&D, Marketing, Operations, and so on, as well as in different business units.
- **Technology:** Look in all the technology that you're building or leveraging across the enterprise. Look at technology investments that have been made internally and externally (for example, cloud and Software-as-a-Service [SaaS], and AI models). Additionally, as technology becomes consumer focused, it's widely available for almost any workforce member in your company to buy with a small monthly credit card charge (or sometimes it may be free). This process creates a hidden risk that many IT departments don't even know about or own.

- **Data:** Look at all the different types of data you're accumulating and evaluate them for business risk. Data can live almost anywhere. It's important to prioritize the data that's most critical to your organization because it may feel like you're trying to "boil the ocean" if you don't look for risks in a prioritized way.
- **Regulatory obligations:** Check if your expanding digital footprint changes your regulatory obligations: for example, the General Data Protection Regulation (GDPR), China Cyber Security Law (CCSL), California Consumer Protection Act (CCPA), Sarbanes Oxley (SOX), and so on. Consider what they are today and what they will be as your business expands into new services, locations, data types, and user communities.
- **Third parties:** Look at your third-party relationships based on the sensitive information or operations the third party (vendor, distributor, partner, and so on) is handling. Third-party risk can be contractual or legal, with specific business processes being performed on your company's behalf, or in digital assets (IT systems) that are operated or accessed by the third party. Third-party risk is a growing space of focus as many large companies realize how many third-party suppliers they interact with (often thousands). We cover third parties more in Chapter 1.
- **Business continuity:** Look at what resilience looks like and what happens (the impact) when systems or processes fail. Does your company have a process defined to determine how the business will operate if key systems or facilities aren't available? Consider the complete end-to-end system and its users, applications, and geographical risks to consider how it may fail or degrade, and what fallback or failover options you have.

REMEMBER

There are numerous ways to assess and discover risks in your company. There is no single perfect way to do this. Often, it is best to have a diverse mix of risk assessment capabilities. Here are two suggestions:

- Establish a multi-tiered library of your key risks. This library can be as simple as a spreadsheet, but it helps you document, communicate, and prioritize your risks.

- That said, companies need to start small and consider outside assistance as they are learning and building their own processes:
  - Program maturity assessments
  - Enterprise risk assessments
  - Control assessment
  - Self-assessments
  - Architecture assessments or reviews
  - Vulnerability risk management
  - Penetration testing
  - Third-party risk assessments

Who Are Your Key Stakeholders?

The management of risks related to digital transformation lies in the hands of accountable business owners who are responsible for various outcomes from the digital transformation. There are at least two types of key stakeholders:

- **Program-level stakeholders** must be executive level, influential, and emotionally committed to enabling the identification and management of risks. Individuals such as General Counsel, General Manager (of business unit), Chief Financial Officer (CFO), Chief Privacy Officer (CPO), or Chief Operating Officer (COO) are potential options. Some companies won't have access to the "chief" level roles, but the important part is finding the right support structure and functional knowledge. The Chief Information Security Officer (CISO), head of risk management, or Chief Risk Officer (CRO) often can own or oversee the process but should not own risk and business decisions around managing risks for the company. Think of them as the facilitator or process owner.
- **Risk/asset-level stakeholders** start at the top at each functional area and get more granular as specific business risks and critical digital asset vulnerabilities are discovered. For example, a General Manager of a business unit may own an overarching risk, but a director, layers beneath that, may own a process or IT system that has a specific flaw,

vulnerability, or risk. Individuals who own the digital assets that have the risks should own the mitigations. Tricks to managing risk/asset level stakeholders include publishing dashboards or reports to ensure that decisions are followed through on.

TIP

Another way to think about different groups of stakeholders is based on a three-lines-of-defense model:

- **Front line:** These are the users of systems who interact with systems and may notice, cause, or be a part of a risk process. These are also function and business executives. By making risk processes part of your typical processes and providing mobile and web tools for reporting issues, you make risk and compliance part of the company's culture and help employees make better risk-informed decisions.
- **Second line:** This group is in charge of overseeing and managing the risk program. Tools and automation can improve this group work and help it spend its time on program enhancement, strategic planning, and non-routine tasks.
- **Third line:** Auditors and assessors check on how well the controls and policies are being adhered to. It could be an internal group or outsourced to a firm specializing in providing independent audits. You can provide all the information an auditor needs in one interactive portal, with easy navigation to the data supporting the reports. This reduces the questions, data fetches, and audit findings that you have to respond to.

Getting from Here to Good

Implementing an enterprise-wide risk program isn't something that can happen overnight. It should be done in iterations planned over a maturity improvement process. The road map must be closely aligned to your organization's digital transformation priorities. As you move up the maturity ladder, your road map should include a plan to break down and consolidate the different risk and compliance silos to the greatest extent possible. Where not possible, you should at least have a plan to connect the different risk and compliance silos (even if manually at a high level).

The road map should lay out the various projects and milestones, evaluating the business and transformation aspects independent of the technology choices. It should align to the broader digital transformation program elements of the organization.

Some key themes to keep in mind in this journey include

- **Strategy:** Ensure you have the right projects and focus to establish and activate a risk-aware culture, sponsorship, plans, and road maps. This includes development and implementation of an industry standard risk management framework (such as NIST or ISO) and performance improvement through effective governance and risk ownership.
- **People:** Empower everyone from leaders to individual contributors and give them the resources to perform their tasks. Look for ways to have frontline users identify and manage risks within their daily efforts. This can be through awareness programs, as well as technical approaches that add risk controls and questions into forms, approvals, and workflows.

  Change management processes will be important as you coach your people through new ways of recognizing and managing risk. This includes things like training, certification, clarity of roles and responsibilities, and so on. Communication and reporting are vital, and provisions must be made to implement the best and most appropriate means to track and inform stakeholders of an enterprise's risk response.

REMEMBER

- **Processes:** Create processes that are clear and easy to follow across the various teams, groups, and stakeholders that need to be involved. Identify and implement processes that track elements such as governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives, and the effectiveness of risk mitigation and controls.
- **Technology:** Take advantage of technologies that accelerate strategy, establish processes, enable collaboration, drive engagement, support risk management strategies, and keep people informed and involved. Look at the tools you already have in place and consider whether they will carry you where

you need to go. Work to avoid building or reinforcing silos by requiring data and process integration (many point tools work well as long as they don't have to share). One platform serving as a single source of truth mitigates risk through continuous, consistent processes for monitoring and enforcing policies. Part of your program plan should outline enabling the technology to drive efficiency and automation.

Picking the Right Platform

As you translate strategy into action, you want to activate your people and process with technology. These areas are highly interrelated. Risk management technologies are geared toward helping people be more effective in following processes.

In order to pick the right technology foundation, you want to review the basic requirements in this section. Most of the list will apply to you eventually. With change as the only constant, be sure you plan for flexibility. This is one reason to start with a platform rather than tools.

Take a look at the following considerations:

- **Configuration Management Database (CMDB) and IT alignment:** The information about your assets and business services stored in your CMDB is incredibly helpful in managing digital transformation risk. Why? Because so many of these risks come from or are influenced by technology. The CMDB provides a single source of truth you can use to understand the configuration of computers and other devices on your network, software contracts and licenses, and business services. As you work with IT and their processes, you discover that a common and accurate database helps you speak the same language, avoid mistakes and duplication, and gain easy access to critical information to help you make risk-based decisions. You can see what systems look like currently, what may be affected if something changes, and what things are out of compliance. When something goes wrong, you're in the best position to understand the issues and take the right action.

- **Policies and controls:** You need a place to manage your company's controls tied to applicable laws and regulations and/or defined risks your company will need to manage.
- **Risk assessment:** Determine how the potential platforms handle various methods of risk assessment. Nearly all platforms available facilitate manual assessments, but some of the more progressive platforms incorporate more automation and risk indicators to enable a better view of holistic risk.
- **Incident management:** Dedicated modules allow teams to manage various types of incidents and the surrounding requests or actions involving other teams. Consider a platform that integrates with other workflow tools (such as IT problem/exception/change management), because many actions need to be coordinated and implemented across organizational lines.
- **Risk mitigation action planning and tracking:** Make sure you have a consistent and reliable way to develop, assign, and track action plans and mitigations to identified risks. It's one of the most critical components to ensuring your risk management program is effective and doesn't cause unintended legal risk. Look for a platform that simplifies and coordinates things. This is where risk management teams have wasted a ton of time manually in the past.
- **Risk monitoring and communication:** The ability to understand, visualize, and communicate risk in an integrated view is the ultimate outcome that drives companies to pursue risk management platforms. Find one that maximizes your ability to do this with the least manual effort.
- **Risk quantification and analytics:** Quantitative depictions of how risks can affect an organization are an emerging capability in information security and IT risk management. Consider if a dedicated tool or a platform that integrates with risk quantification tools would be best if you want to pursue this capability.
- **Audit:** Audit modules are a form of risk management designed for internal audit processes (which typically require a different level of workflow, such as special documentation, approaches to testing, and audit reporting). Because of this

specialized need, find a platform that has alignment with your internal audit group. Many companies have struggled to get their audit teams on board with their broader GRC/IRM platforms. If this is the case, ensure the platform you choose integrates with the platform they have to use.

- **Vendor risk management:** Vendor risk management is another specialized form of managing risks for a company. The unique element is that your platform and tools used for this purpose need to enable all your in-scope third-party vendors to log in and participate in workflows. Traditional GRC tools have been too complicated to make this work well, so numerous software programs have cropped up in this space. Evaluate platforms against your vendor risk management needs and consider if an integration is possible to an existing tool/service you have.

Beyond capability-specific requirements, think about additional decision factors:

- Selecting a platform that's already in broad use by business users, IT, and other stakeholders so risk and compliance can be seamlessly embedded into day-to-day activities and decisions
- Having a platform that can support and integrate all the functional areas, including policy, operational management, technology, risk, audit, vendor risk, business continuity, and compliance
- Using significant automation to minimize manual work and keep pace with the explosion of digital risk sources
- Picking a technology platform that can support the scale of your digital transformation

  Digital transformation and automation will inevitably lead to a significant expansion of your digital footprint. Therefore, it is critical to pick a technology platform that can match that scale.
- Maintaining a simple user experience (UX) for first-line engagement (mobility, chatbots, web user interface, and so on)
- Using a cloud platform for quick ramp-up and scaling to global enterprise needs
- Making sure your technology platform is configurable and maintainable for low total cost of ownership

- Supporting integrations with other operational tools and data sources such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), CMDB, security operations, and so on
- Accessing a strong community of customers and other third parties with tools and expertise in helping you on your journey

REMEMBER

Technology isn't a panacea that will fully eliminate the people and process elements required in managing risk. However, the right risk platform can greatly reduce manual overhead and help drive successful business decisions based on risk.

IN THIS CHAPTER

- Setting up policies and control objectives
- Establishing controls
- Monitoring risks
- Developing targeted programs
- Developing interconnected risks
- Designing for resiliency
- Explaining digital risk for your stakeholders

Chapter 3
Managing Digital Risk

After Acme Corp successfully articulates its risk management strategy and selects a platform (see Chapter 2), it can move on to leveraging the platform for its risk management processes. Acme Corp wants to ensure these processes are simple, clear, and well-coordinated across the organization. This is especially true to get the value out of the integrated analytics and reporting across risk functions that Acme Corp desires.

This chapter outlines some of the key processes involved in managing digital risk.

REMEMBER

There are many, *many* approaches to managing different types of digital risks. Several risk management frameworks and companies make a living out of guiding customers based on different risk methodologies. This chapter describes common aspects that are found in most risk and compliance programs. We encourage you to do your homework and engage knowledgeable risk professionals (hire or consult) in setting up your appropriate program.

Setting Up Policies and Control Objectives

After you've prepared yourself to tackle digital risk (see Chapter 2), next you want to establish the high-level policies to address principles, guidelines, and actions around various risks and regulatory obligations. Within each policy, you should identify control objectives that address specific enterprise and business risks or regulatory obligations. The following list further explains policies and control objectives:

- **Policy:** A *policy* is a high-level document created by management to point you in a strategic direction or guide a decision. Policies also express the intention of the organization. For example, an acceptable technology use policy may outline how employees may use company-provided laptops.
- **Control objectives:** These are a series of statements that address how risk is going to properly be mitigated and provide a target for identifying the effectiveness of controls. For example, a control objective may be that your organization protects the use of unauthorized access to your employee and customer data. Your controls around this could be utilizing strong passwords, encrypting data, or proper access management.

These elements should be aligned to your organization's high-level strategy and operational risks.

Figure 3-1 shows you the relationship among regulations, risks, policies, control objectives, and controls.

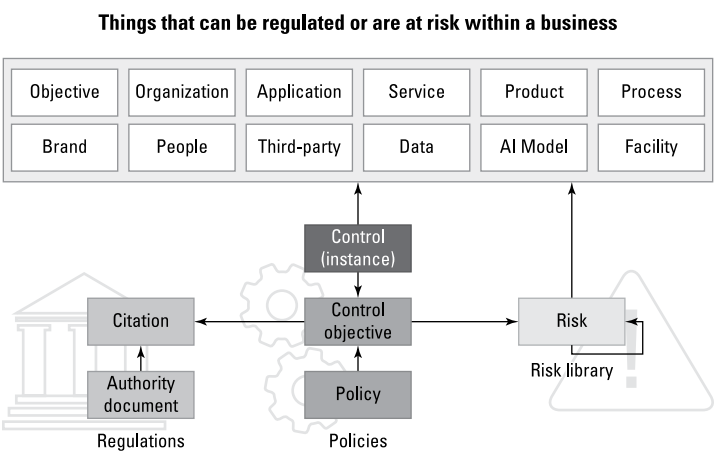

FIGURE 3-1: The relationship between risks, policies, and the business.

Establishing Controls

Establishing controls is when the process begins to move away from the high-level strategic aspects of risks. This step is about looking at your policies and control objectives (see the preceding section) and mapping them to where they apply across the enterprise. In other words, look at all the places across the enterprise where the various risks and regulatory obligations apply. Now create individual controls that address them and map the control objectives to these risks.

For example, setting a control objective about customer data being encrypted is the high-level strategic position of the company. However, the type of "control" you establish to achieve that control objective may vary or change depending on whether you're encrypting customer data maintained in spreadsheets by one department (for example, Finance) *or* those maintained at a vendor site by another department (IT).

Monitoring Risks

After you set up your policies and control objectives and establish and implement your controls, you want to monitor your risks and determine where you stand and how your controls are mitigating your risks.

Testing controls

Your company should evaluate controls periodically (more frequently for high-risk or high-impact controls) to ensure that each control is operating effectively to mitigate the risk it was put in place to alleviate or remove. Testing can be performed automatically by continuous control monitoring software or manually by internal entities or a third party. These tests can be driven by risk, compliance, audit, or internal departmental teams, such as a security risk management team or a business unit's risk management team.

WARNING

The controls are in place to ensure the success of the business unit or the department. Therefore, it's in the business unit's, department's, process's, or application owner's best interests to ensure that the control is designed, implemented, and operating effectively. It is not somebody else's problem. Specifically, don't make an internal audit or compliance group solely responsible for testing and/or validating control effectiveness. Audit should be the last line of defense.

Measuring and quantifying risk

After your controls have been tested, it's time for numbers. There are two common ratings for risk:

- **Inherent risk:** Inherent risk is the risk that an event will occur and negatively impact your organization, given that there are no controls in place. Your company faces this risk by being in the type of business you're in, in the location you're in, and with the people you employ.
- **Residual risk:** Residual risk is the risk that remains after controls are put in place. It is impossible and undesirable to completely eliminate all risk, but you should try to alleviate as much of it as makes sense against the cost of the action it would take to mitigate it. Residual risk is the risk you're left with after you've developed mitigating controls.

Here's an example of the difference in the two risk measures: Having a website on the Internet poses an inherent risk. Hackers are constantly crawling the web looking for targets. This threat causes management to mitigate the risk by using controls such as firewalls, secure code practices, intrusion prevention systems, and backup systems. However, they don't completely remove the risk. What's left is the residual risk.

TIP

Don't spend more money mitigating a risk than the actual impact of that risk. There are many published and unpublished approaches to measuring risk. One simple way to evaluate the risk to an organization, process, or other entity is by plotting the impact of the risk (low, medium, high) and the likelihood of the risk's occurrence (low, medium, high) on a risk heatmap, as shown in Figure 3-2.

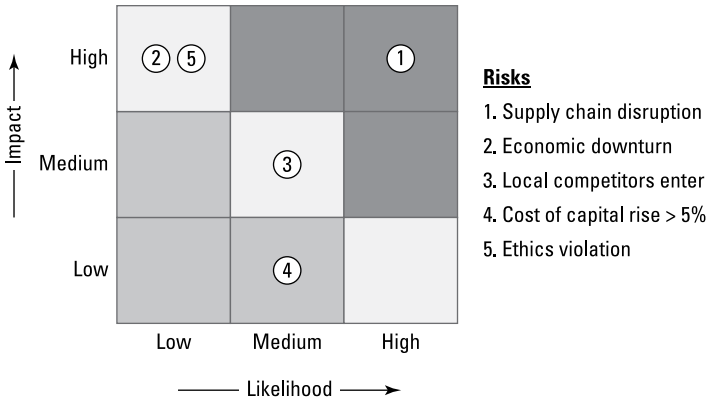

FIGURE 3-2: A risk heatmap.

REMEMBER

After you've properly evaluated all your risks and ranked them in accordance to their cost, business impact, and probability, you now must decide what to do about that risk. You can handle your risk in many ways. The primary techniques for managing risk include

- **Acceptance:** You and your organization decide that the risk likelihood and impact aren't significant enough to spend the time and resources to address the risk.

  For example, you note that the operating system (OS) on the server that runs the Voice-over-Internet-Protocol (VoIP) phones in your office is outdated and vulnerable. After further analysis, you discover that the VoIP application you're using doesn't work with the updated OS — upgrading would render the phone application useless. However, you note that this phone system is segmented from the rest of the environment and wouldn't allow an attacker to pivot into the internal network. Therefore, you decide to stay with the outdated OS, accepting the risk because, for now, the risk to your company isn't high.

- **Avoidance:** You and your organization decide to remove this risk from your risk sheet by getting rid of it altogether.

  For example, you have a legacy file server that you keep as a backup in case the main file server runs out of space. After analysis, it's noted that this backup file server is out of date and has a vulnerability that could give an attacker full control

of the computer. Rather than spending the resources to patch, your company opts to retire the system and get rid of the risk.

- **Mitigate:** You and your organization decide you can't take a system offline to patch it, but you can introduce compensating controls (other controls that have a similar or "compensating" risk reduction) to reduce the risk to a more acceptable level until you can patch them.

  For example, you notice that a large number of your manufacturing systems have a vulnerability that could allow an attacker complete control over the systems. From the manufacturing floor, the attacker could move laterally through your environment and into your databases and gain access to all your customer data. You can't schedule an upgrade until after the busy fall production season. You decide to use network segmentation to isolate the manufacturing equipment from the rest of your environment. This prevents attackers from getting to your data if they were to gain access to your manufacturing equipment.

- **Remediate:** You note that a couple of hundred servers are missing Microsoft patches. However, your patch management process works in a reasonable time frame, so you patch them and make that vulnerability go away.

- **Transfer:** You and your organization decide the best way to handle this risk financially and operationally is to make it someone else's problem and pass it on.

  For example, despite your team working tirelessly to secure your network, your team decides that a breach would be a very large hit financially, one that you could not recover from. You decide to pass that liability to someone else by purchasing cyber insurance. While you are required to pay premiums, you are able to sleep at night knowing that if a major breach were to happen, you are covered financially.

WARNING

When opting for cyber insurance, be warned about two things:

- Just because you have insurance now doesn't mean you can stop worrying about basic cyber hygiene.
- Make sure you read and understand your policy carefully. Some aspects related to cyberattacks may not be covered or require your company to uphold certain standards, such as performing a risk assessment or penetration test periodically.

Manual versus continuous monitoring

With the amount of effort required to monitor all these processes and digital assets to be sure they meet your control objectives, are you going to hire an army? No. You're going to apply a little digital transformation to your risk management program by using software that can continuously monitor things for you.

Many parts of the process that are performed today by using spreadsheets and emails can be automated. For example, your risk assessment, control testing, and Key Performance Indicator (KPI) and Key Risk Indicator (KRI) monitoring can all be done continuously with no manual overhead. After you have the monitoring built into your systems and have people enter risk data as they're doing their work, you can keep your understanding of risk up-to-date easily. This makes all the reporting you have to do much simpler, and the reports can be delivered as digital, interactive dashboards.

WARNING

It's not just about staying current. Manual processes have drawbacks. They're error-prone (because humans are), they're inefficient (manual data entry? Ugh.), and workers despise them. Employees avoid doing the work, cut corners, and burn out, so someone new has to be trained.

Note: Not all manual activities can be replaced by automation. However, if you have the right technology platform to support your risk management journey, you can progressively reduce the manual effort and move more of it into automation.

Developing Targeted Programs for Different Types of Risks

While it's important to look at your risk as a whole, it's also important to break down the maturity level in each of your risks. For example, consider the example of building a cybersecurity risk program from the ground up.

The best way to start developing any program is to look at your maturity for that risk area with an assessment. Maturity should be viewed from a high level. Think about where you stand now and where you want to be in three to five years. With attack landscapes

continually changing, it is difficult to plan out much further. Keep in mind that this three- to five-year plan is not set in stone and should be revisited at least yearly to determine if your company is heading in the right direction. This should also be continuously aligned to your company's strategic priorities.

TIP

Sometimes the strategy and maturity horizon in cybersecurity is measured in shorter terms than a typical strategic three- to five-year view because of the pace of change in risks, threat actors, and solutions. For this example, use the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) to evaluate your maturity. NIST CSF follows 108 different controls. At the conclusion of the assessment, your company receives an overall maturity score. It is graded on the following criteria: Identify, protect, detect, respond, and recover.

Using a cybersecurity framework, like NIST, helps identify certain areas your company could implement programs and will help you build out a long-term strategy for addressing cybersecurity risk. To help improve the various levels of maturity after a risk assessment, check out the programs in this section.

Asset management

A key aspect in the management of digital risk should be to understand all technology assets the company owns. This includes laptops, workstations, servers, routers, switches, VoIP phones, Internet cameras, IoT devices, databases, cloud assets, and applications. Typically, these should be tracked in a Configuration Management Database (CMDB) with necessary information like hostname, IP address, location, asset owner, and so on. This CMDB should also note the criticality of the system. For example, a critical server will be tracked more closely than something like a non-critical guest Internet kiosk. Remember, you can't defend what you don't know is there.

Vulnerability/patch management

A step that often follows asset management is review of the patching process. After you know all your assets, you can begin to understand what vulnerabilities are present in your environment. This step should consist of scanning all your assets and reporting back with the vulnerabilities. Make sure you have a way to keep up with dynamic and virtual assets that may come and go.

However, this part of the program is not over yet. Now is the most important and often overlooked step. What good is having all that vulnerability information if you don't do anything about it? A process should be put in place to properly evaluate your vulnerabilities, quantify their risk, prioritize remediation, fix, continuously monitor, and repeat. Automation can be your friend here as well.

Identity access management and privileged access management

Another process as part of a larger cybersecurity program is identity access management (IAM). For this program to be successful, you should evaluate the privileges of all your users and determine where they have access. Your organization should use the principle of least privilege, meaning that every user should only have access to accounts he or she absolutely needs to access, or needs to know. Privileged access management tools can help you implement and enforce these rules.

Employee training

A robust cybersecurity program is much more than just dealing with hardware and software. Employees are a large risk factor in cybersecurity incidents, so they should understand that the security of their organization is part of their jobs.

Employee training should be conducted continually throughout the year. This includes training on email phishing, social engineering (on social media as well as the phone), and even physical security, such as tailgating (following someone through a secure door).


TIP

Other typical programs targeted as specific types of risk include privacy, AI governance, model governance, third-party risk management, financial regulatory compliance, and product regulatory compliance.

Looking for Interconnected Risks

A whole lot of nuance goes into defining and differentiating risk. For example, technology, data risk, and cybersecurity risk can overlap depending on the structure of the organization. That's

why it's important to find interconnected risks and couple them to make them more manageable.

Take a look at a more complicated example about vendor risk. Your company uses an IT vendor to provide and manage a critical application and its infrastructure. This application is the main business-to-business (B2B) site for all your customers, and it processes credit card numbers. A few different risks stand out:

- **Operational technology risk:** The risk that the website crashes or doesn't work correctly
- **Data risk:** The risk of customer data being lost, abused, or mishandled
- **Vendor risk:** The risk of having a third party mishandle a primary portion of the revenue

These risks can all be rolled up into vendor risk because the operational technology and the data is being accepted and processed by the vendor. It is the vendor's responsibility to ensure the uptime of the application and to adhere to the Payment Card Industry Data Security Standard (PCI DSS). With that being said, evaluating your risk here can be made much simpler by reviewing the agreements with the vendor and rolling those risks up through vendor risk management. In other words, define your expectations in a service level agreement (SLA) and maintain this agreement over time.

Designing for Resiliency

Bad things can happen no matter how much mitigation and planning are put into a program. As your team is implementing your world-class risk management program, make sure it can roll with the punches. No matter how much emphasis or how much you minimize the risk, there should always be a Plan B.

How easily can an organization resume normal operations in the event of a negative event? Keep in mind the following examples of negative events and business resiliency:

- **Fire in the primary data center:** Have a redundant, high availability backup in the cloud or in an offsite data center in a different location that allows for a quick return to business as usual.

- **Key employee leaves the organization unexpectedly:** Have policies, procedures, and processes in place that allow for a quick transition to new personnel. Reduce dependency on key employees with a rotation program.
- **Ransomware attack hits headquarters:** Segment your network so an attack in one area won't spread. Have an offline backup of your data and applications that can't be infected. This allows your company to restore affected machines from an uninfected system.

Contextualizing Digital Risk for Your Stakeholders

Business owners want to know the risks associated with their organization and how they're being managed. The information must be communicated in a way that the audience can relate to. It is often best to create two sorts of deliverables or dashboards — one for the risk owners and one for upper management and board members.

Risk owners

Risk owners are the people in charge of a business domain on a daily basis. Reports should be created with the understanding that these people interact with this risk on a daily basis. Reporting to the risk owner should include dashboards and reports with far more detail than for upper management. This level of detail enables these parties to understand the risk at hand and to be able to create or develop a proper solution from a more technical standpoint. In a sense, you're giving them the tools and insights to do their job. The dashboards and reports should be easy to access or ideally be embedded in that risk owner's daily processes and reports.

For example, if an IT service relies on a third party, the IT service owner should see the current risk posed by the third party as part of her daily dashboard.

Upper management and board members

Reporting risk to upper management and the Board should be different than reporting to your risk owners (see the preceding section). High-level reports and dashboards should explain risk in business terms that these stakeholders will understand: business impact, probability, and loss. The details help stakeholders make informed business decisions meant to drive the company forward. It should explain, at a high level, what the risk is, the likelihood of the risk's occurrence, and the impact if the risk were to happen.

IN THIS CHAPTER

- Trying not to boil the ocean
- Keeping your eyes on all the balls in the air
- Measuring your success
- Leveraging automation
- Planning for change

Chapter 4
Five Tips for Digital Transformation Success

This chapter gives you high-level, specific things to keep in mind when creating your risk management program to support your digital transformation. Implementing a program that leverages these tips and tricks helps your organization achieve greater risk reduction in less time and with fewer resources.

Crawl, Walk, and Then Run

Rome wasn't built in a day, and neither is a world-class risk management program. It is going to take time to get your program where you want it, and it will also require the right building blocks in place. With that being said, where you start depends on your organization. You could start with vendor risk, IT risk, enterprise-wide risk, or SOX compliance. The key is to inventory the different types of risks up front, and start looking for interconnected risks (connecting the dots). Soon, you can plan different risk projects in sequence or perform them in parallel. After you have the hang of these steps, implement automated indicators and controls. Have a plan in place for these steps from the beginning and make sure you don't fall prey to quick fix tools that won't support the longer term program.

The foundations and goals of the risk management program are what separate a good program from a great one. In Chapter 2, we describe some important foundational elements for the journey:

- A shared understanding of risk across the organization
- A sound risk and compliance culture
- Executive sponsorship
- A single source of truth

Now that some foundations and goals of the risk management program have been set, your business can begin to migrate from managing your risk with ad hoc manual processes to integrating risk into the day-to-day jobs of employees. As you begin to integrate the automated efficiency machine that you call your risk management program, think about strategy, people, process, and technology. These are covered in more detail in Chapter 2.

REMEMBER

Pick a couple of areas of risk and test out the process. You can't dive in with the entire risk program and fix it all right away. By slowly building out your risk program, piloting it with smaller groups, managing change, celebrating your wins, and demonstrating value, you're much more likely to succeed in your risk journey and establish a lasting culture of risk-informed business success.

Keep Your Eyes on All the Balls in the Air

After you've laid out a risk management vision, goals, and road map, it's time to embark on the journey. Now, as you go through this journey, there are typically multiple initiatives and parallel activities underway. These include (but are not limited to) the following:

- **Bringing different stakeholder groups on board:** Existing business functions and business units may be operating in different ways. The journey may include engaging with different groups to bring them on board.
- **Aligning business requirements:** Multiple internal stakeholder groups may have varying business needs that have to be rationalized without complicating the new processes.
- **Talent:** You must identify skill gaps and bring the right talent on board to support the various stages of your digital risk journey.

- **Rolling out multiple use cases:** At any given point in time, you may be rolling out and taking some use cases live with pilot groups or broader audiences while ramping up the next use cases.
- **Training and change management:** Business users and participants must be educated about the revised and new processes. See the later section "Plan for Change" for more on this.
- **Stakeholder communication:** All key stakeholders must be closely engaged and aligned throughout the journey.

This list is just some of the common activities in your risk management journey. Your own journey will differ based on your organization's vision and digital priorities. With all these different types of activities underway at the same time, it's essential to treat this as a program with holistic program governance rather than as an isolated project. Establish periodic reviews, steering committees, independent reviews, and other controls to ensure the program's success.


TIP

If your organization doesn't have employees with the right skills for certain aspects of the journey, get help from advisory and implementation partners who understand your business as well as your technology platform of choice.

Measure Success

Your organization needs to understand that this investment is paying off. Find meaningful metrics that show off what you implemented. Show how this state-of-the-art program generates tremendous business value through increased efficiencies, drastically minimized risk, happier employees, and transparency so stakeholders can understand the risk into your organization. Find metrics such as

- **Risk reduction:** How well does the program identify and mitigate the key risks to the enterprise?
- **Efficiency:** How many employee hours have been cut down or how much cost efficiency has been accomplished to achieve the same result as before?

- **Adoption and culture:** Are stakeholders pleased with the new processes? Are they using risk information to inform their decisions?
- **Transparency:** What percentage of the risks identified have been remediated or addressed? How quickly are they being remediated?

Leverage Automation to the Hilt

Not everything can or should be automated, but find ways to continue to automate. There's no need to manually perform expensive and time-consuming tasks like control monitoring, risk monitoring, remediation tracking, and continuous risk assessments. Also, the 100-question surveys about a department's compliance status are a thing of the past. With the right technology, many of these can be streamlined or automated.

REMEMBER

Don't forget to look at communications processes: Automation can provide detailed and high-level dashboards and generate reports for all audiences.

Plan for Change

The purpose of the risk management journey is to enable your business users, executives, and the Board to make risk-informed decisions on their digital transformation journey. Therefore, the ultimate goal and success of the program depend on how well employees and executives understand their new digital risks, take ownership of the risks, and leverage risk intelligence as part of their daily operations.

This cultural transformation requires as much attention, or even more, than all other aspects of the risk management journey. A well-designed change management program helps employees understand, commit to, accept, and embrace the inevitable changes to their daily processes. Proper change management processes include engagement, education, feedback cycles, and coaching to reduce the resistance and cost that come with organizational transformation.

servicenow

Go from hair on fire to calm, cool and collected.

Are you ready to transform the way you handle security and risk? You can when you bring security, risk, and IT together, on one platform—the Now Platform®. Suddenly, you're able to see and prioritize security incidents, vulnerabilities, and enterprise risks more quickly than ever—and with new certainty. You're able to monitor and reduce your risk exposure with real-time visibility. And you respond faster using workflows, automation, and orchestration. On the Now Platform your enterprise can stay safe, stay alert, and do it all with ease and simplicity.

Visit **servicenow.com/securityandrisk** to learn more.

Make the most of your digital transformation

With more products, relationships, and revenues depending on more digital capabilities, risk isn't something just for IT or the compliance guy. We are all on the frontline, and we can all help our companies avoid mistakes and problems. This book introduces you to important topics like privacy, cyber risk, and third-party risk, so you can get smarter about data and technology risks. The goal: wise, risk-aware decisions that help your business safely transform.

Inside...

- Key risks of digital transformation
- Risk management basics
- Getting started with your program
- Technology considerations for digital risk
- Tips, tricks, and traps to learn from

servicenow

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-69248-5
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.