Digital Transformation is Changing your Business: Is your Approach to Risk Intelligence Changing, too?

A Frost & Sullivan White Paper
Introduction .................................................................................................................................................................... 3
Digital Transformation is Remaking Business—and Risk................................................................. 4
Are your GRC Policies Ready for the New Workplace? ................................................................. 5
Risk Calculation for the Digital World ............................................................................................... 6
Best Practices for Selecting and Deploying a Modern GRC Solution ........................................ 7
Conclusion........................................................................................................................................................................ 8
INTRODUCTION

New digital technologies are emerging at an unprecedented rate and changing the way we work and live. Digital transformation impacts every line of business, every job role and every industry. It impacts everything from manufacturing and production to office work and customer service, replacing mundane tasks with automation to free up employees to focus on work that benefits from uniquely human skills and interaction.

But as organizations transform everything from technology to business processes, they must also reassess how they quantify and calculate risk. That means rethinking their governance, risk and compliance (GRC) programs to adjust to new regulations and risk-management needs. In today’s business environment, the line between cyber risk and business risk disappears. Effective risk management practices will address the two equally, offering a single threat assessment to security professionals and executives as needed.

Opportunity requires risk. Avoiding it is not an option but mitigating it is. Having a clear-eyed, quantitative picture of where risk lies will allow you to stay ahead in an increasingly competitive market.

As a result, many organizations must re-evaluate their approach to GRC. Even companies that deployed state-of-the-art tools just a few years ago may need a refresh, since those applications may not cover the wide spectrum of regulations, threats and compliance requirements in place in today’s digital marketplace. It is especially important to deploy tools that can put a dollar figure on risk. That makes it easier to sell the C-suite on the need for GRC tools, and it will also help you calculate ROI on an ongoing basis as your business models and technology deployments change.

This paper will look at how Digital Transformation is changing business and the way companies must evaluate risk; present an overview of GRC, including the capabilities it has traditionally included; highlight the need for specific risk calculation to be added to the mix; and offer best practices for choosing and deploying a modern GRC solution.
DIGITAL TRANSFORMATION IS REMAKING BUSINESS—AND RISK

Driven by continuous connectivity in an always-on world, Digital Transformation is enabled by a raft of new technology. Big Data and advanced analytics, the Internet of Things (IoT), artificial intelligence (AI) and machine learning are all transforming the way business gets done, often automating manual processes and taking human beings out of the day-to-day equation or shifting their responsibilities to higher-level, value-added roles. The benefits are measurable and significant, and include dramatic increases in productivity, customer satisfaction, return on investment and the company's bottom line.

According to a recent Frost & Sullivan survey of almost 2,000 IT decision makers around the world, elements of Digital Transformation are impacting every aspect of their business and rearranging their IT priorities. The top challenge for IT departments continues to be dealing with security concerns (32% of respondents), but those threats are consolidating around cybersecurity in particular. The next biggest challenge is aligning IT with business strategies (28%), which often moves front-and-center as companies start to automate processes that have historically been ad-hoc and manually driven. Interestingly, 23% of respondents selected improving digital presence as a major challenge, which again speaks to the influence of DT; these executives know that tech is changing their markets—they just don’t know how to embrace this new way of working.

As they consider how to address these concerns, executives must also consider how new technology is affecting risk. Take the Internet of Things. Companies are embracing this merger of tech and business to boost customer service, collect usage data, and optimize field and on-site operations. Deployments are moving from “watching and learning” to mid- or large-scale trials (of more than 500 devices) and embedding IoT into core services and products (35% and 34% of respondents, respectively). In addition, 40% of respondents say they are already deploying next-generation solutions. But as they collect and analyze more and more data—and then use that information to transform business processes—companies must reconsider how that impacts the risk associated with the relevant tasks, technology and data.

Or consider that 61% of respondents say watches are the number-one wearable device used for business purposes in their organizations, followed by badges (48%) and clothes (45%). The BYOT trend is also prominent—an average of 37% use personally owned smartphones, 35% use personally owned laptops and 26% use personally owned tablets. In fact, 44% of respondents expect to increase their usage of BYOD. Almost half of the respondents claim that their organization fully enforces a BYOD policy. And almost two-thirds use consumer calling services like Skype in the workplace.
When asked, “How critical are the following investments for your organization’s digital transformation success over the next 5 years?” data analytics and communications/collaboration tools integration with other business software (Microsoft Office, Google G-suite, CRM, ERP, vertical apps) came out ahead. About 75% of the respondents rated these two solutions as either somewhat important or very important.

All these technologies are changing how companies do business across the organization. Wearables and the IoT affect everything from production lines to transportation and supply chains; BYOT trends impact knowledge work and office culture; and everything changes customer service. Of course, no new technology comes without problems. The top concerns regarding IoT deployments are security/privacy (49% of respondents), the cost of integration (39%) and the time it takes to develop solutions (36%).

Missing from that list? Risk. Because while companies recognize that security and data management issues are paramount, they don’t always recognize that cyber threats are only one component of business risk.

Of course, it’s important to address cybersecurity risks by connecting security practices with risk and compliance functions across the enterprise. But it’s just as important to establish the relationship between business risk and IT risk and ensure business security priorities are consistently addressed. That requires bridging the gap between people and technology by creating repeatable processes that identify emerging risk conditions quickly and correctly. And once you’ve done all that, you must concretely explain the impact of IT and cybersecurity risk to senior management—in financial terms. That will then allow you to prioritize risk mitigation according to the relevant business and financial impacts.

**ARE YOUR GRC POLICIES READY FOR THE NEW WORKPLACE?**

GRC describes a company’s integrated strategy for managing corporate governance (how senior executives manage the organization), enterprise risk management (ERM, the processes used to identify, analyze and respond to risks to the company’s business goals) and compliance with regard to regulatory requirements. Essentially, GRC aims to ensure the company meets its business objectives with minimum risk, while also allowing it to maintain the values and culture its leaders or shareholders support. A GRC initiative will likely include most or all lines of business across the organization, as well as legal, finance, HR, compliance and the C-suite.
Rather than fearing risk, business leaders must position their companies to seize market opportunities whenever and wherever they arise. Risk management isn’t just about avoiding damage; by allowing companies to take chances and mitigate the cost of failure (and there will be failure!), risk management ensures bold companies will prosper while other, less aggressive players will not. The key is to leverage technology to support—and even redefine—the company’s strategic objectives, while promoting employee productivity, increasing revenues and positively impacting the bottom line. To do that, decision makers need immediate, accurate and relevant data; only then can they make the right decisions and pursue the right opportunities at any given moment in time.

A good GRC program will allow the company to take a global, encompassing approach to this effort; effectively share information across the organization; and improve operational efficiency and minimize waste. Just as importantly, it will mitigate risk, ensuring that the organization and its employees are not vulnerable to penalty (financial or otherwise) in the course of doing business.

But as the workplace changes in the face of Digital Transformation, so must risk analysis—and not all GRC systems are up to the task. If your company is undergoing any technological change—including the use of the Internet of Things, artificial intelligence, machine learning, advanced analytics and big data, and more—the way you identify, assess and mitigate risk is almost certainly not where it needs to be.

**RISK CALCULATION FOR THE DIGITAL WORLD**

Businesses have always had to assess and manage risk, but the increasingly digital nature of the workplace puts added pressure on business and IT managers alike. New technology can no longer be separated from the market conditions that affect companies on a consistent basis; in this chicken-and-egg relationship, it is unclear just how much tech is influencing economics, and vice versa. As a result, companies must look at risk as the intersection of the digital world and the physical one, and eliminate any barriers that make it hard to manage the two at once.

Indeed, it is important to remember that cyber risk is no longer limited to traditional IT departments and products. For starters, the majority of businesses today rely on technology to run their entire back-end operations, from finance to HR to Research and Development and IP. Threats, therefore, don’t just affect discreet data sets, networks or endpoints—they can quite literally take down the entire operation. Throw in sensors and beacons, smart watches and artificial intelligence, and you suddenly increase the number of potential threat vectors significantly. Add consumer technology to the mix (which is not built for enterprise security), as well as a rash of increasingly mobile employees and the need to embrace cutting-edge technology before it has been market tested, and the risk potential skyrockets.

The most effective and efficient way to protect against cyber threats across the entire organization is to quantifying digital risk. For years, cybersecurity has not mandated much, if any, financial accountability; it’s typically considered a technical issue for the MIS team to manage and design. But today, the lines between cyber risk and business risk are blurred, if they exist at all. Executives and their boards have a fiduciary duty to manage cyber risk as it impacts the broader business—recognizing in the process that no company can be 100% secure and therefore prioritizing risk is paramount to success.

But it is not enough to simply identify potential risks to the business; rather, it is critical to put a dollar value to those threats, allowing decision makers to decide which risks to take, which to prevent and how much to spend on each endeavor based on clear and meaningful data.

**Qualitative** risk analyses—using scales or color codes, for instance—do not enable smart, well-informed decisions. They create a guessing game of their own, in which executives rely on what are essentially subjective assessments tied to language that makes them feel reliable. They are not specific enough to prioritize investment and action
so it can be difficult if not impossible to distinguish between two (or several) risks that have a common “level” (say, three events labeled “red”), making it equally difficult if not impossible to decide which one to address first. Qualitative analysis also doesn’t allow for understanding how risk can be multiplied. And it forces analysts to either downplay or exaggerate real risk to fit into the categories at hand.

A *quantitative* approach to risk analysis ensures that executives get the most accurate and specific information available—literally in dollars and cents, allowing them to make decisions based on real numbers that will impact the bottom line. This is done by using a standard set of practices that don’t leave the assessment up to any one analyst; users know the information has been culled from a group of known processes, with certain required inputs and algorithms. That allows them to compare various risks across the organization and then prioritize the ones that either pose the biggest threat or offer the greatest reward.

**Three questions to ask:**

- What are the top cyber risks and how exposed is my company?
- Which risk-management investments offer the highest ROI?
- Are we investing enough or too much in cyber risk management?
BEST PRACTICES FOR SELECTING AND DEPLOYING A MODERN GRC SOLUTION

In today’s world, risk management is not only required to fend off cybersecurity and other threats, it’s also a key differentiator that can deliver significant competitive advantage. But while many companies have established risk-management processes in one or two areas of the business, that typically leads to duplication on the one hand and gaps on the other. To get a complete and accurate picture of corporate risk requires a complete and accurate set of processes across the organization. So the first step is to look for a GRC solution that can ensure accountability across the organization.

When looking for a quantitative risk management solution, the first order of business is finding one that fits into a broader GRC program—after all, you don’t want to rip-and-replace your current software, but you do want to incorporate your quantitative data into your other GRC processes as needed. Make sure the software considers both loss event frequency (how often, over a defined period of time, a risk will result in a loss) and loss magnitude (the monetary cost of a loss event). A bell curve that shows a range of possible outcomes, with their associated probability, adds credence to the endeavor. And software that allows input from subject-matter experts ensures you can defend the results to anyone within your organization.

CONCLUSION

Technology is dramatically changing how all companies do business—and so is the way they assess and mitigate risk. Smart businesses are rethinking their GRC processes and software to incorporate flexible, enterprise-wide programs that take into account the ways in which Digital Transformation is impacting the business and which quantify risk and opportunity in a way that clearly shows where threats (and possible rewards) lie.

In the current climate of global competition and relentless change, one bad decision can result not just in hard-dollar costs, but also in a loss of reputation that goes viral and delivers significant long-term consequences. At the same time, being too cautious can deliver its own problems, notably opportunity costs no business can afford today. Smart companies are quantifying risk in the digital age to ensure their executives can make the most effective and impactful decisions—today and into the future.

FAIR (Factor Analysis of Information Risk) is a model to codify and monetize risk by identifying and defining the elements that contribute to risk in relation to reward. The relationship between each element is measured mathematically and assigned a dollar value, making it possible to express risk in financial terms. That makes it easier to treat cybersecurity the way you would any other business planning effort, allowing you to prioritize, calculate ROI and deploy the most cost-effective solutions. Software that employs the FAIR methodology uses data collected from your business combined with pre-populated data from your industry and other relevant factors. It then presents the results in charts that are easy to read, understand and act upon.
Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community.

Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
3211 Scott Blvd
Santa Clara CA, 95054