How to manage the risks in Digital Transformation

The new keys to a high-performance GRC program

Click to Continue >

icebergnetworks.com

Iceberg

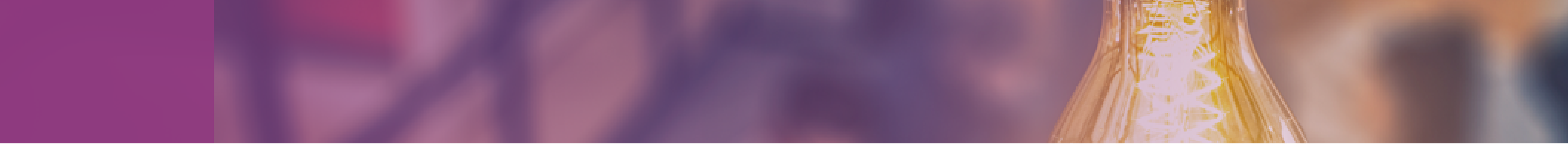
Calculated risk-taking is and has always been the essence of business and route to success, and a strong governance, risk and compliance (GRC) program is the right tool for managing non-financial and compliance risk.

But the rich opportunities in Digital Transformation have tempted many organizations to circumvent their GRC program – to rush into Digital Transformation projects without a clear picture of the new risks they are taking on and without the controls needed to manage those risks.

Ken McPherson, CEO of Iceberg Networks, discusses the risks that organizations are taking on when they take on Digital Transformation and the keys to a high-performance GRC program – one that identifies, quantifies, and qualifies those risks so businesses can make the fully informed decisions that support and drive your organization toward its goals. Done correctly, you can turn your GRC program into a true business enabler for digital transformation.

About the author

Ken McPherson has been at the helm of Iceberg Networks Corporation as the Chief Executive Officer and President since April 2014. Bringing more than 25 years of demonstrated experience in the information technology sector, Ken focuses on expanding Icebergs' business across North America and effectively establishing them as an industry leader in GRC programs, which includes Cyber Risk, Operational Risk and Vendor Risk solutions. Ken has helped many Fortune 500 organizations develop a better understanding of their risk posture – enabling them to make more informed business decisions. Ken is often invited to speak with and meet fellow Chief Executives that are trying to solve key board issues of how to gain a more accurate and aggregated understanding of the non-financial risks that effect their organization.



The new risks in Digital Transformation

Organizations must understand the depth and breadth of the risks in Digital Transformation and build that understanding into their GRC programs.

Cyber Risk

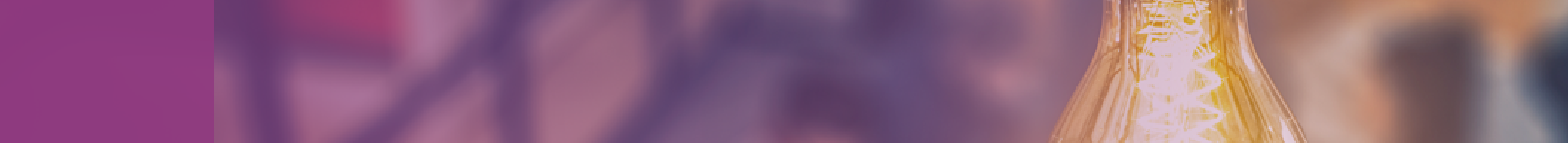
The experts, the observers and especially the victims of hacks and attacks all agree that cyber risk is the single most significant threat to business today.

With Digital Transformation, cyber risks that might once have been mitigated by simply beefing up a password regimen has metastasized into a dark industry that demands defensive systems as complex as the businesses they protect.

- **Cyber risk permeates the Cloud.** Loads running in the cloud are prime targets for cyber criminals. Data stored in the cloud are the spoils of a successful attack.
- **Cyber risk expands with the Internet of Things.** The billions of sensors and communications devices finding their way into every industry, our vehicles and our homes represent billions of points of illicit access to global networks and the arrival of 5G will only amplify this.
- **Cyber risk moves with every one of us on our mobile devices**, from network to network and from vulnerability to vulnerability.
- **Cyber risk only grows** as firms leverage artificial intelligence (AI) technologies and machine learning programs.

When cyber risk manifests as a cyber breach – when systems are compromised, and data is stolen – the consequences range from reputational damage to fines to the potentially devastating impact of operational disruption. But though these cyber risks are complex, they *can* and *must* be managed if the enterprise is to reap the outsized benefits of Digital Transformation.

By proactively understanding an organization's business architecture and leveraging GRC assessment technology and remediation workflows, can position firms well to prevent a



successful attack. At the same time, an efficient and well implemented security incident and vulnerability response management program can minimize the impact of a potential breach.

A high-performance GRC program does just that. It *enables* the business benefits by exposing and providing the means to manage the cyber risks in Digital Transformation.

3rd Party Risk

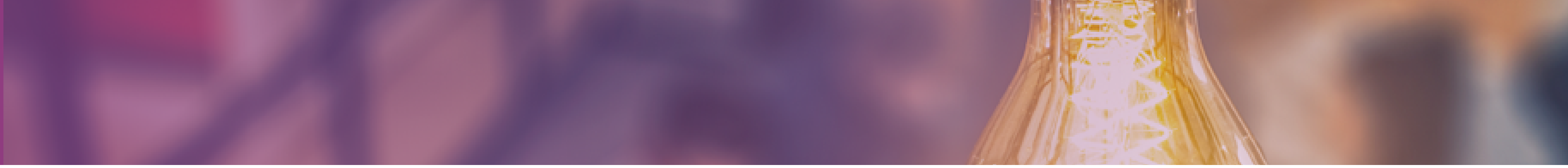
As challenging as it is to enumerate, measure and manage cyber risks faced from within an enterprise, few enterprises operate in a digital vacuum. And Digital Transformation only multiplies the electronic interconnections among enterprises as more and more data are collected, shared and traded through formal and ad hoc networks of customers and partners, websites and apps. Today, no enterprise is an island.

And as with every business to business relationship, arrangements made on the basis of mutual benefit bring with them 3rd party risk (and often 4th party and 5th party risk too).

No business would choose a logistics provider on the strength of lower costs alone. That kind of decision requires a high degree of confidence that shipments will arrive at their destinations on-time, safe and secure, whatever the price paid. Yet something similarly risky is happening when companies take on unexamined partners as a function of Digital Transformation. Too often, decisions are being made almost solely on the basis of cost reduction or the promise of market expansion without an in-depth understanding of the risks to systems and data introduced by new partners and technologies, and by *their* extended networks of partners and technologies.

By implementing a successful 3rd party or vendor risk management GRC program, an organization can make more confident decisions around third party relationships in a shorter time period, which in turn can help organizations drive new revenue streams or help drive down costs in the supply chain. This fact alone adds context around why we see 3rd party or vendor risk management as the most sought after and implemented GRC use case in the marketplace today.

A high-performance GRC program solves this challenge. It *enables* the business benefits by exposing and providing the means to manage the 3rd party risks in Digital Transformation.



Operational Resilience

Of all the bad things that can follow a failure to manage the risks in Digital Transformation, none are so dire as a threat to an enterprise's viability. Most estimates contend that 60% of businesses go *out* of business within 6 months of suffering a cyberattack.

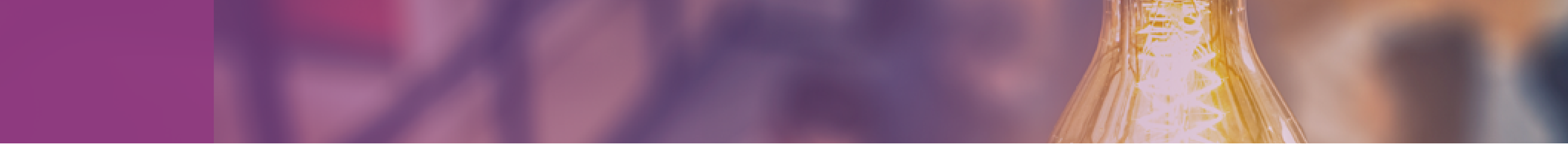
New businesses, particularly those funded through venture capital, tend to have an outsized appetite for risk. As these businesses mature (assuming they survive) into self-funding and even profitable organizations, the tolerance for risk shrinks. But no matter where an enterprise sits on this continuum, none can tolerate a prolonged disruption in their operations.

No matter the source or precise nature of the risk in Digital Transformation, keeping that risk within tolerance thresholds informed by the potential impact on organizational viability is the goal.

By mapping out the business processes into a GRC program that allows for proactively building, testing and validating resiliency plans and crisis management prepares a firm for quick responses, and minimal exposure to an inevitable outage in today's digital reality.

A high-performance GRC program does just that: It enables the benefits of Digital Transformation by providing a structured way to consider the risk in relation to the organization's ability to withstand and/or respond to an operational disruption and an informed framework within which to make the critical important business decisions.

Cyber risk, 3rd party risk and the threat to organizational viability are the evolving top-line risks to manage in Digital Transformation. And while IT departments have an important role to play, these risks and the GRC programs required to manage them belong on the agenda of every executive management and board meeting.



The new keys to high-performance GRC

GRC first emerged as a set of tools and processes used to ensure organizational compliance with the regulations that govern business activities. It evolved into a risk-based program, as organizations needed to understand “what may happen”.

And today, with new global privacy legislation, GRC programs now are helping with the need for better data protection.

Subsequently, a high-performance GRC program goes further; weaving the proactive management of cyber, operational and business risks into the very fabric of organizational decision-making, including and especially the far-reaching decisions involved in Digital Transformation.

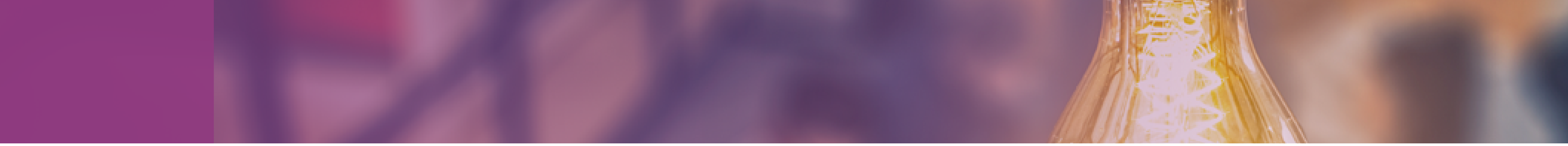
And today’s most successful organizations do not rely solely on the risk management protocols employed by IT managers when making strategic decisions around Digital Transformation.

But if effective, pan-organization risk management goes beyond compliance and IT risk, what steps should an organization take to ensure early and ongoing GRC success?

GRC or IRM?

With the rapid rise of Digital Transformation, the risk management community is at a crossroads – taking a look at where it has been and where it is headed – and a healthy debate has developed. Some argue that GRC should be replaced by Integrated Risk Management (IRM). Others argue that GRC and IRM are different names for the same thing.

At Iceberg Networks, we see GRC and IRM working together to accomplish the same goals. In our practice, vertically and horizontally integrated risk management is the principle that guides the design, development and implementation of the high-performance GRC Programs our clients rely on to guide them through the risks in Digital Transformation.



Make GRC an Executive Function

Facilitate the *vertical* integration of strategic and operational risk.

Do this by bringing GRC practices and oversight into the boardroom. Some organizations have done this by elevating the risk management function into the C-suite thereby to ensure that the quantified and qualified ramifications of every strategic business decisions are understood and managed at the operational level, and vice versa.

As an executive function, GRC is much more than a collection of defensive tactics. Decisions made or declined on the strength of “gut feelings” (or worse, held in undecided suspension while the opportunity slips away) give way to structured deliberations and the GRC program becomes a strategic business enabler – a transparent, auditable process for weighing the benefits in every opportunity against the risks each presents to the organization.

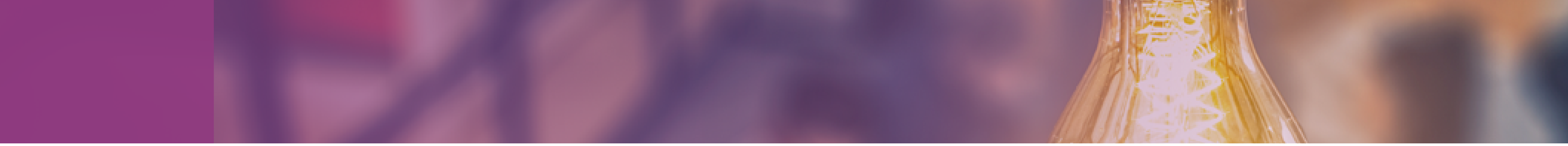
In the age of Digital Transformation, a high-performance GRC program requires more than executive sponsorship – it requires active executive engagement that now includes the Board, the “C” suite, the Audit Committee, and the Business Leaders.

Normalize Cross-Functional Communications

Facilitate the *horizontal* integration of risk management across organizational functions.

Do this by implementing a single risk taxonomy and a consistent approach to measuring both the scale and scope of the risk *and* the potential impact on the organization.

Ultimately, it is the growth and cost-reduction opportunities, the risks involved and the potential impacts across multiple organizational functions that make most Digital Transformation decisions *strategic*. But too often, GRC programs flounder because the compliance team uses one set of measures while the security team uses another, and operations a third, and internal audit a fourth, and all use terms and terminology that are unique to their siloes of expertise. The confusion is exacerbated when Digital Transformation decisions reach across functions boundaries, e.g., when moving a critical business process to a cloud services provider introduces cyber, operational, audit, compliance and 3rd party risks. And when the confusion leads to ill-considered business strategies, the impact on the organization can be devastating. This example alone further emphasizes the need for executive engagement discussed earlier.



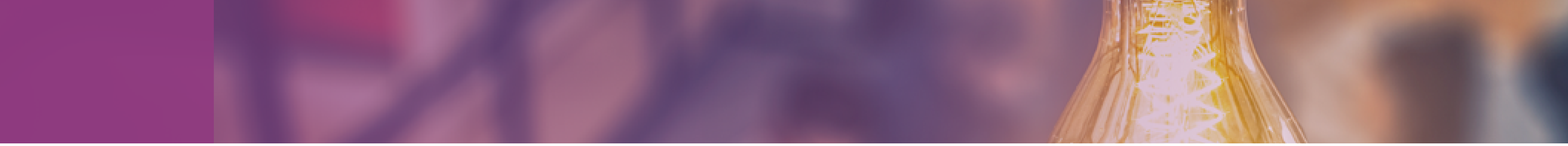
A high-performance GRC program requires cross-functional collaboration that can drive a shared language and harmonized metrics to help break down risk management siloes and ensure that every Digital Transformation decision considers the costs and benefits to every operational function that may be affected.

Deliver Actionable Data

Do this by implementing standardized risk management technology and tools to deliver consolidated data to support the risk management actions at every level of the organization in a translated business context that each function understands.

A GRC program that is focused on identifying the risks accomplishes the critical first step of the mandate. A high-performance GRC program prioritizes risks according to the potential impacts and maps them to the organizational functions affected and communicates the results in context that each recipient understands. A high-performance GRC delineates the courses of action that may be taken to mitigate the risks and/or the impacts and monitors the progress of all risk management action.

A capable but flexible risk management technology platform that supports the unique needs of each operational function and implements a shared language and harmonized risk metrics provides the foundation. The best platform implementations provide actionable, understandable risk data that support the capture and communication – through notifications, dashboards and customized reports – to enable all stakeholders to confidently make more informed and effective business decisions.



Next steps

Managing the new risks in Digital Transformation requires a high-performance GRC program that senses, measures, prioritizes, communicates and accelerates the action required to manage those risks. While creating such a program has its challenges, the returns will always justify the effort. The outcome is then a strong, efficient strategic decision-making regime, enhanced operational resilience and improved organizational performance which are all exceptional indications of the organization’s commitment to their stakeholders.

About Iceberg

Iceberg helps organizations plan, deploy and support successful implementations of Governance, Risk Management & Compliance (GRC) solutions. Iceberg's team of consultants, developers and subject matter experts offers a full lifecycle of services, including executive workshops, implementation and integration, and support services. We are also a value-added partner for North America's leading GRC software platforms.

For more information please contact us at
info@icebergnetworks.com or call **855-595-0808 x261**.

icebergnetworks.com

Iceberg