Baringa

POINT OF VIEW

Digital risk transformation: The three Vs of a successful risk management strategy

As organisations continue their digital journeys, the changing nature and volatility of risks demands an overhaul of risk management methods.

2023

Contents

Risk management can’t keep up

Introduction

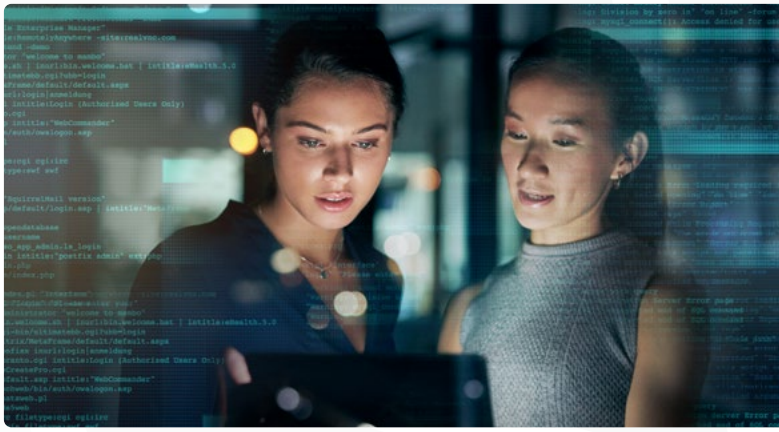
Global spending on digital transformation continues to grow and is expected to reach over USD3 trillion by 2025. This is driven by organisations as they join the global race to secure greater dominance in their respective industries. Organisations are fundamentally shifting their business models and changing how they engage their markets, including directly interacting with consumers through mobile apps or transacting in a more automated fashion through a web of API connectivity.

Whether you're working in the public or private sector, in financial services or manufacturing, it's hard to miss the large-scale technology-driven transformation happening around us. All organisations are on a journey to become digital businesses. Data is today the most strategically important asset across many sectors, and if advancing technology represents the spearhead of organisational transformation, data sits firmly at its heart.

A direct correlation exists between an organisation's ability to become more digital and its ability to organise its internal capabilities, thereby operating at a competitive pace and tempo of digital change. This has been proven through the significant rise in Agile delivery models that are much more aligned to 'customer obsession', 'business value' and 'end-to-end' product management. These changes have led to immense improvements in value creation, whilst removing organisational bottlenecks and constraints.

The problem-statement

Digitally maturing organisations are facing a seemingly insurmountable hurdle: the bottleneck presented by siloed risk management capabilities that haven't been able to keep up with the pace of complex technology-led change.



Expanding on the issue

The risks, associated with digital transformation, originate from across the domains of data privacy and technology, and cyber security – we refer to this as Digital Risk. These Digital Risks are becoming increasingly complex as organisations implement new technologies that are significantly more integrated with many more points of connectivity. Due to this entanglement of modern digital solutions, the nature of risk events has become obscured to the point of being unrecognisable. As a result, business leaders are no longer confident about the resilience of their digital solutions and the risk of cascading technology failure.

To enable digital innovation, operate at pace, and become value-additive, risk management capabilities need to operate at higher levels of maturity. In essence, risk management needs its own transformation. Without this, risk management capability will continue to diminish in value, and will inhibit the pace at which organisations can move to execute their digital strategy.

The solution

Moving away from a siloed approach of managing risk and taking a more integrated approach will lead to an outcome that is greater than the sum of its parts – not least by removing unnecessary spend and decreasing lead times.

In addition to taking a more integrated approach to risk management, organisations should measure their performance not only by the prevention or mitigation of loss events, but also by the quality of risk reduction, and the enablement of strategic benefits. If organisations don't measure performance through these additional lenses, the potential value of risk management capabilities is capped at minimising or preventing a loss, as opposed to creating a gain.

A strategic lens should be embedded in our approach to risk management

The challenge in risk management today is that you can too easily become out of touch with the wider strategic objectives of the digital agenda.

Without working in the context of a wider strategy, it's impossible to fully recognise and appreciate the relationship between risk and reward. Quite naturally, this leads to an overly risk-averse mindset where the potential reward is limited to a net-neutral outcome. This is to say, the reward is the prevention and mitigation of loss as opposed to *enabling* a strategic benefit.

Contemplate for a moment, the ability for cyber security related risk mitigation to enable a strategic benefit of 'enhanced consumer trust'. Keeping in mind that this strategic benefit influences how cyber security risk mitigations are implemented. For example, making access control overtly noticeable – but seamless – to the consumer to instil a sense of assurance. The subtle but important distinction is the mitigation of a risk *and* the promotion of a strategic benefit: enhanced consumer trust.

Will digital change introduce vulnerability if we fail to focus on risk management strategically? Possibly. Will it inhibit the ability to maximise the potential of risk mitigation by optimising cost and overheads? Absolutely. Does it prevent the ability for risk management to create a net-positive outcome like the example above? Definitely.

Old metrics are incentivising poor risk management behaviours

> *"Show me the incentive and I'll show you the outcome"*

The above quote from billionaire US investor Charlie Munger is particularly pertinent in this context. Organisations have implemented counterproductive incentives for risk management that undermines its core objective, which is: to garner a deep understanding of how risks could emerge within the business, digital solutions and processes, and to design sustainable and robust controls that will stand the test of time.

Bad incentives are leading to organisations over-indexing on the speed at which risk can be identified and understood across new digital technologies. While speed and quality are both clearly important, the former is achieved at the expense of the latter. This is because we have specific KPIs on the frequency and volumes of risk assessments, rather than the quality of risk mitigation that is typically introduced at a much later stage.

We have seen examples of this in our recent past with a series of similar outages in financial services[1]. In essence, we're undermining high-quality risk mitigation by rewarding the speed at which we aim to identify, understand and measure risk. It isn't working.

1 https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf

The business case for Digital Risk

The business case for Digital Risk

To better enable our organisations to fully realise the benefits of a modern business, Digital Risk management needs to be fully embedded within digital transformation, and to operate with a mandate to not only mitigate a loss event, but also contribute to a strategic benefit.

If approached in this way, organisations can improve the **value** *protected* by Digital Risk capability, increase the **velocity** at which this value is created, and significantly improve the **veracity** of risk management capability.

Value

Customer outcome: better **protect** value at risk, and **create** value through effective Digital Risk management.

Maximising second order effects through Digital Risk

When traditional risk management practices are applied disparately or in silo we become tunnel visioned and are unable to appreciate the many-to-many relationship between business risks and their mitigating controls. For example, when approaching risk management in silos, we apply an overly simplistic approach of applying cyber controls to cyber risks, and architectural controls to availability risk.

For example, when mitigating a risk associated with the stability of a digital product, decreasing software-related defects through better quality code, together with being able to seamlessly re-deploy code into production, are key controls that can also materially minimise the risk associated with a cyber breach, as a second order effect.

Maximising second order effects is all about aligning incentives and creating a mutually beneficial outcome. For example, when mitigating a risk associated with the stability of a digital product, decreasing software-related defects through better quality code, together with being able to seamlessly re-deploy code into production, are key controls that can also materially minimise the risk associated with a cyber breach, as a second order effect.

Business leaders should challenge themselves on whether they're maximising the potential of Digital Risk management.

Aligning strategic objectives of risk and digital transformation

The objectives of Digital Risk need to be better aligned to the objectives of digital transformation, which focusses on the ability to not only preserve the standing of the business, but also attain market share, all whilst optimising operating costs.

By aligning the objectives of Digital Risks to the objectives of digital transformation, we create an acute focus on promoting strategic objectives as a deliberate outcome of risk mitigation.

When adopting this mindset, risk mitigation can help the business to enter new markets by achieving regulatory compliance, and increase market share by improving consumer trust, through enhanced resilience, privacy, and security control, in addition to achieving a first-mover-advantage by releasing new, secure digital products to market quicker. This type of value-add is every bit as important, if not more so, than minimising the likelihood and impact of a loss event, such as a data breach.

Velocity

Customer outcome: better work in **lockstep** with digital change, and **streamline** the identification and management of Digital Risk.

Improve the maturity of risk management to meet the pace of digital change

Most organisations face a challenge in terms of available capacity for skilled individuals, such that effective risk management cannot be sustainably deployed and embedded across a broad portfolio of digital change. By 2025, it's expected that there will be a shortfall of 2.5 million cyber security professionals, with similar numbers reported for privacy and data professionals.

The only way to overcome this shortfall of skilled individuals effectively is to invest in capabilities that enhance the efficacy of risk management practices without increasing demands on time.

1

Ways of working:

Consider establishing Digital Risk as an enduring value-stream within the business that has a mandate of supporting digital change from conception to launch. This should be combined with defined risk management accountability across specific digital change initiatives so as to enable risk management practices to scale.

2

Adopt automation:

Security-as-code and compliance-as-code are simple but powerful examples of how Digital Risk management can be scaled and sustained across the business from an implementation perspective, whilst minimising overheads, costs and human error. As a second order effect, this will provide the added benefit of increased staff retention, as skilled individuals will be able to focus their time on more specialist and high-value matters, which will help to improve motivation.

3

Assurance:

Many business leaders have experienced the surprising amount of time it can take to answer the simple question: are our controls operating as intended? This is often due to the extensive manual overhead needed to gather evidence and evaluate controls. Business leaders should accelerate their implementation of technologies that enable better automation and orchestration of control operations and assurance.

Veracity

Customer outcome: addressing risk **cohesively** to improve the **precision** of applied risk management.

Large-scale digital transformation presents an opportunity for business leaders to futureproof their approach to risk management

One of the most common and fundamental challenges we observe across industry is the incompatibility between already fragmented digital, data and technology control environments and ways of working. As organisations become digital businesses, the nature of risks, how and where they emerge, and the way in which risk events ripple across the business is changing in a manner that our existing control environments cannot easily accommodate. For this reason, our approach to Digital Risk needs to evolve with the business. Existing ways of working won't provide the necessary value, without disproportionate amounts of investment, human capital, and a high-risk appetite that may be out of kilter with market expectations.

To enhance the precision of risk management in our digital business, we need to establish an environment of cohesive risk mitigating controls that integrates Digital Risk. This is driving many organisations towards zero-trust cyber security approaches, the use of compliance-as-code, increased automation, and consolidation of control within the network. From a people perspective, this is supported by high-performing risk management practices that are tightly integrated within the digital agenda, and work towards contributing to strategic gains as well as risk mitigation.

Organisations that have adapted their Digital Risk management capabilities are better positioned to reach their strategic goals earlier, whilst maximising the potential offered by digital technologies.

We set out to build the world's most trusted consulting firm – creating lasting impact for clients and pioneering a positive, people-first way of working. We work with everyone from FTSE 100 names to bright new start-ups, in every sector. We have hubs in Europe, the US, Asia and Australia, and we can work all around the world – from a wind farm in Wyoming to a boardroom in Berlin.

Find us wherever there's a challenge to be tackled and an impact to be made.

We'd love to hear from you enquiries@baringa.com
Or visit baringa.com

Baringa Partners LLP
62 Buckingham Gate
London
SW1E 6AJ
United Kingdom