FOCAL POINT
DATA RISK

THE FUTURE OF INTEGRATED RISK MANAGEMENT

A guide to building and launching an integrated risk management program

A quiet but unmistakable shift is underway in the world of risk management and compliance.

A booming market of tools and services once marketed as "GRC" (Governance, Risk, and Compliance) has transitioned to a successor labeled "**IRM**" (**Integrated Risk Management**). In late 2017, this shift - from GRC to IRM - was cemented when Gartner officially moved beyond GRC to publish their first ever Magic Quadrant for Integrated Risk Management Solutions.

This transition is about far more than semantics or branding, though. There's a clear functional shift underway, and it's starting to gain more industry attention. The very boundaries of the organization are no longer clearly defined. Therefore, risks are not organization-specific, but initiative or process-specific (e.g. within a procurement process, IT security is not limited by organization boundaries to a single organization, but a group of business partners working together).

At its core, the move to Integrated Risk Management is a reflection of the shifting needs of today's digital businesses. New risks, new technologies, more complex regulatory requirements, and new demands from the business have forced the GRC market to evolve. Security and risk management leaders are no longer satisfied managing risks in silos (or even single organizations) – instead, they are looking to consider risks and compliance obligations holistically.

Integrated Risk Management (IRM)

A new approach to risk management that integrates risk activities from across an organization or group of organizations to enable better and more sustainable strategic decision making.

WHAT IS INTEGRATED RISK MANAGEMENT TODAY?

Simply put, it's a new approach to risk management that integrates risk activities from across an organization or *group of organizations* to enable better and more sustainable strategic decision making.

Or, as Gartner defines it, IRM is a set of practices and processes supported by a risk-aware culture and enabling technologies that improves decision making and performance through an integrated view of risk, sometimes across traditional organizational boundaries (e.g. integrated supply chain processes).

At a practical level, it means *putting every piece of risk data in context*. The problem with traditional risk management is that it evaluates and prioritizes risk in silos (sometimes looking at risk internally and not across the boundaries of the organization), making risk mitigation decisions without a complete understanding of competing risks, alternative solutions, or the relative significance to the organization or its business partners.

The goal of IRM is to break this mold, enabling the organization to measure the value of a risk management strategy against the relative value of applying the *same effort to mitigating a different risk* (i.e. evaluating the risk in context).

As an overly simplified example, is it better for the organization to spend $10,000 mitigating risk by implementing controls to keep software patches for a specific server up to date? Or would the organization see greater value from spending that same money mitigating risk Y, or risk Z?

Integrated Risk Management Maturity Model

The diagram below illustrates the journey from a risk management program operating in siloes to one that provides a 360° view of risk. A 360° view of risk allows you to examine all risks that will impact the organization, considering all applicable areas.

Let's use the concept of fourth parties as an example. Any impact from fourth parties on my business partners will have a direct impact on my business. In other words, the risks of my business partners are also my risks, and vice versa. My actions will have a direct impact on my business partners, or in some cases, multiple entities in a transaction community. Analyzing any one vendor without considering the broader business context will fail to deliver the insights needed to effectively manage that risk. So how can we, as business partners, address risk jointly?

A 360° view of risk allows you to examine all risks that will impact the organization.

Figure 1 | Integrated Risk Management Maturity

ZOOMING IN: THE IMPACT OF IRM TO A SPECIFIC RISK AREA

Of course, in day-to-day business, risk mitigation decisions are far more complicated than in the previous example. What IRM strives to do is establish a framework, often enabled with a technology tool-set, that allows you to consider multiple risk signals and understand the impact on specific business areas, as well as the downstream and upstream impacts, and then make strategic decisions about the relative severity of the risk and the priority of the remediation. Let's walk through the process.

We have adopted Gartner's CARTA approach (which emphasizes real-time, adaptive risk management) as the basis for our approach to integrated risk management. CARTA suggests that the risk management process be designed so that risk and trust factors are *continuously* evaluated *in context*. That is, each risk decision – whether to grant a user access, engage a vendor, etc. – is made based on the culmination of many risk mitigation actions (security controls, etc.) and risk factors (outside threats, etc.), and that the risk decision is *continuously* evaluated as these factors change over time.

As in traditional, non-integrated risk management, each risk mitigation decision begins with an understanding of factors that increase and decrease a risk – Gartner terms these negative (increases risk) and affirmative (decreases risk) risk signals. These are indicators that can either raise or lower the potential risk of the action. Often, these risk signals are captured and managed in a domain-specific software solution (your IAM tool, for example). Most immature risk management programs stop here – making a risk decision after running these signals through company policy.

THE CARTA APPROACH

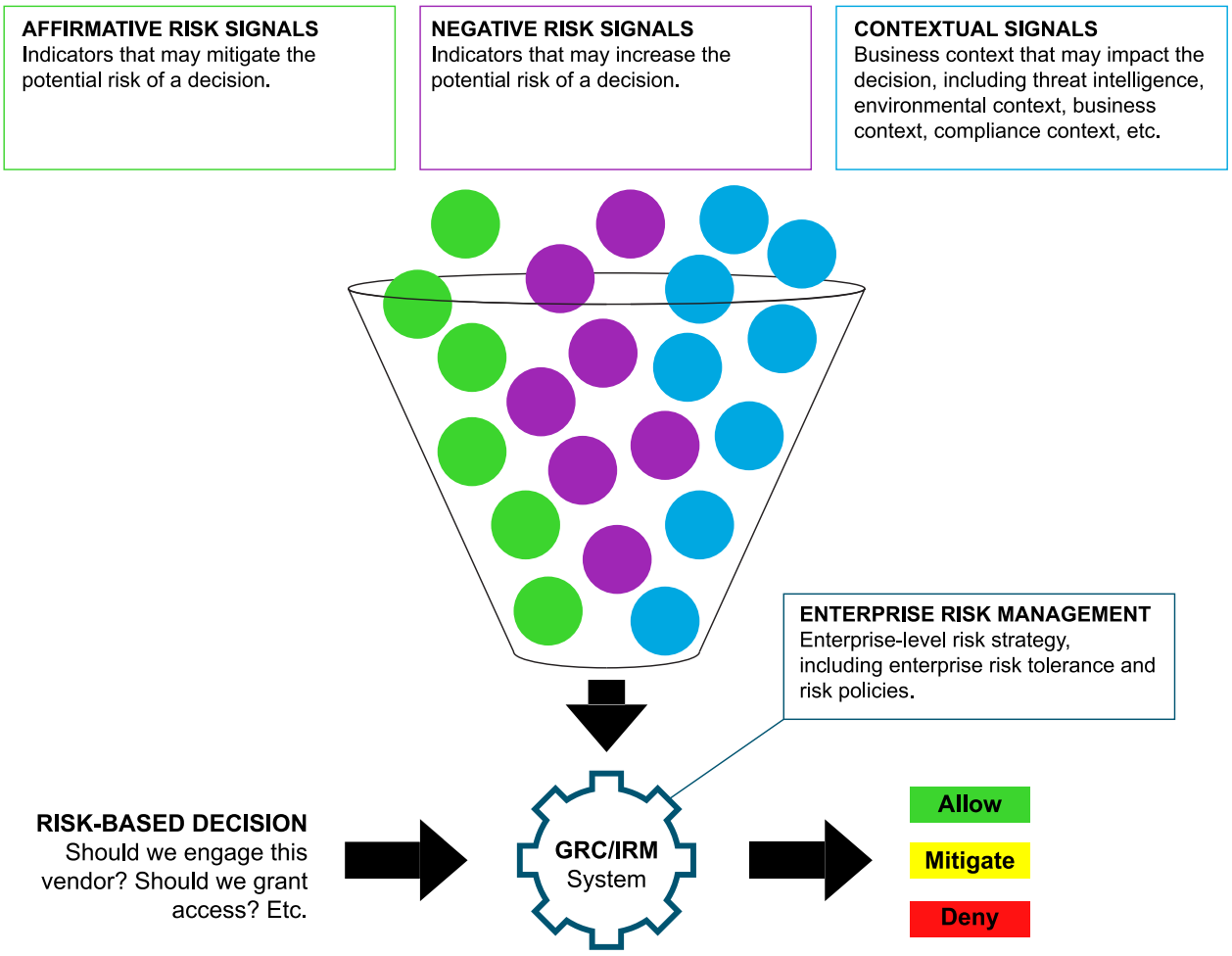
Read more on CARTA from Gartner.

LEARN MORE

For example, there is a vulnerability in the procurement application server. What will the negative and affirmative risk signals be?

NEGATIVE SIGNALS	AFFIRMATIVE SIGNALS	CONTEXTUAL SIGNALS
How severe is the vulnerability?	Third-party access is limited to very specific low risk areas.	How critical is this system - was a business impact analysis done?
Are there any open incidents or findings related to this server?	Very strong Segregation of Duties management.	What type of information is kept in the system?
Do any third parties have access to the server?	Very strong application controls are in place.	

Figure 2 | Integrated Risk Management Model



This integrated model considers both domain-specific and general risk factors to make the decision, informed by an understanding of critical risk areas from across the business. Decisions are made on a micro level in real-time, considering all of the same factors.

For most organizations, realizing a truly integrated, adaptive risk management posture will require significant technology improvements, including:

- A centralized hub for management (in many cases, GRC or IRM software)
- The ability to measure context-based risk signals (in many cases, more advanced point solutions)
- Significant integration between applications, allowing disparate risk sets to feed into your centralized hub

These are real hurdles, but they shouldn't stand in the way of progress toward this end. Without a doubt, the field of risk management is moving toward integration and toward adaptive, dynamic, risk-based decision making. Leading organizations will begin integrating as soon as they're able, adopting new techniques and technologies to give them an edge over their competition.

HOW TO START YOUR INTEGRATED RISK PROGRAM

With IRM, the value of the program increases as more risk activities are brought into view, because it allows business leaders to make *enterprise-level and community* decisions about which risks to mitigate, and which to accept or transfer.

There are many important risk areas to consider as part of your Integrated Risk Management program, and there are often connections and interdependencies among them. As you break down siloes and improve control and visibility over one risk area, you often improve decision-making and business intelligence in other areas.

Similarly, integrating risk areas allow you to ask more strategic questions about the nature of your business risk, and how risk in one part of your business impacts other parts of the business.

- **But where should you start as an organization?**
- **Should you take baby steps, by adapting an IRM approach for a single risk area, or jump in all the way, working toward a 360° IRM program?**
- **What is your most pressing risk area, and how does it impact other parts of your business?**

In today's environment, critical risks are rarely confined within a silo, but knowing the point of origin can help you build an effective plan for managing it. In the end, however, success with IRM is less about where you start, and more about having a reliable framework that is managed through an appropriate governance structure.

"Without a doubt, the field of risk management is moving toward integration and toward adaptive, dynamic, risk-based decision making."

APPLYING AN IRM APPROACH

Some examples of where you can apply an integrated risk management approach in an organization are:

Identity Risk Management

IdRM is the set of processes to mitigate the access risk in an organization through the Identity Access Management process (infrastructure for creating, maintaining, and using digital identities). When integrated within the broader technology risk posture of the organization, it will provide substantial improvements in an organization's ability to measure and mitigate overall enterprise risk.

Third-Party Risk Management

Managing complex vendor supply chains is one of the biggest challenges facing security and risk management leaders today. Recent third-party breaches and new compliance mandates make the issue even more pressing.

Strategic question: What is the impact on business continuity management or identity access management if the third-party risk for a particular vendor is high?

Business Continuity Management

The ability to identify, respond to, and recover from business disruptions is critical to the success of the modern digital business.

Strategic question: Does the business impact analysis align with the overall risk assessment of the organization or the risk profile for key third parties?

Corporate Compliance Management

The job of compliance managers only becomes more complicated as new regulations, like GDPR, come into effect, and organizational compliance requirements (social and environmental responsibility, for example) begin to accumulate.

Strategic question: What is the impact of incidents on my compliance obligations?

To learn more about integrating Identity Management, check out our whitepaper, *Rethinking the Identity Risk Equation.*

DOWNLOAD

IT Risk Management

The risk associated with new and growing technologies continues to evolve. The Internet of Things (IoT), machine learning, social media, big data, and mobile devices (among many others) disrupt traditional risk management models and present new challenges for enterprise decision makers.

Strategic question: What is the impact of vulnerability management on IT risk?

Depending on your organization, you may also consider other key risk areas, like legal management and audit management, for inclusion in your Integrated Risk Management program.

THE BENEFITS OF INTEGRATED RISK MANAGEMENT

In a fully mature IRM program, these sub-domains should roll up into centralized reporting tools and dashboards, allowing business leaders to leverage insights from all risk areas for better decision making.

This may sound difficult to achieve – and it is – but leading organizations are moving in this direction because of the long-term benefits it offers to the business:

- Strategy-based (not just compliance-based) decision-making and planning
- Reduction in disparate risk management point solutions
- Centralized, accurate reporting
- Fewer risk management "blind spots"

But perhaps most importantly, knowing your risks across the business creates opportunities – for cost-savings, competitive advantages, and alignment. And as a business leader, creating these opportunities allows you to add value to your organization above and beyond risk mitigation.

Even if your organization is not ready to begin a full-blown IRM revolution, you can begin taking small steps to improve your risk visibility by leveraging the tools you already have in place.

ABOUT FOCAL POINT

Focal Point Data Risk, a leading cybersecurity services provider, helps companies secure the future of their business. By integrating market-leading consulting, technology integration, and cyber workforce development services, Focal Point provides an end-to-end solution for security leaders looking to future-proof their companies against threats, changing data protection laws, and growing workforce shortages. From the server room to the board room, Focal Point enables companies to build stronger, smarter, and more resilient cybersecurity programs that can scale at the pace of business growth. Focal Point works with the largest and most innovative companies in the U.S., including 6 of the top 10 companies by revenue and more than half of the Fortune 50. For more information about Focal Point, please visit focal-point.com.

QUESTIONS?

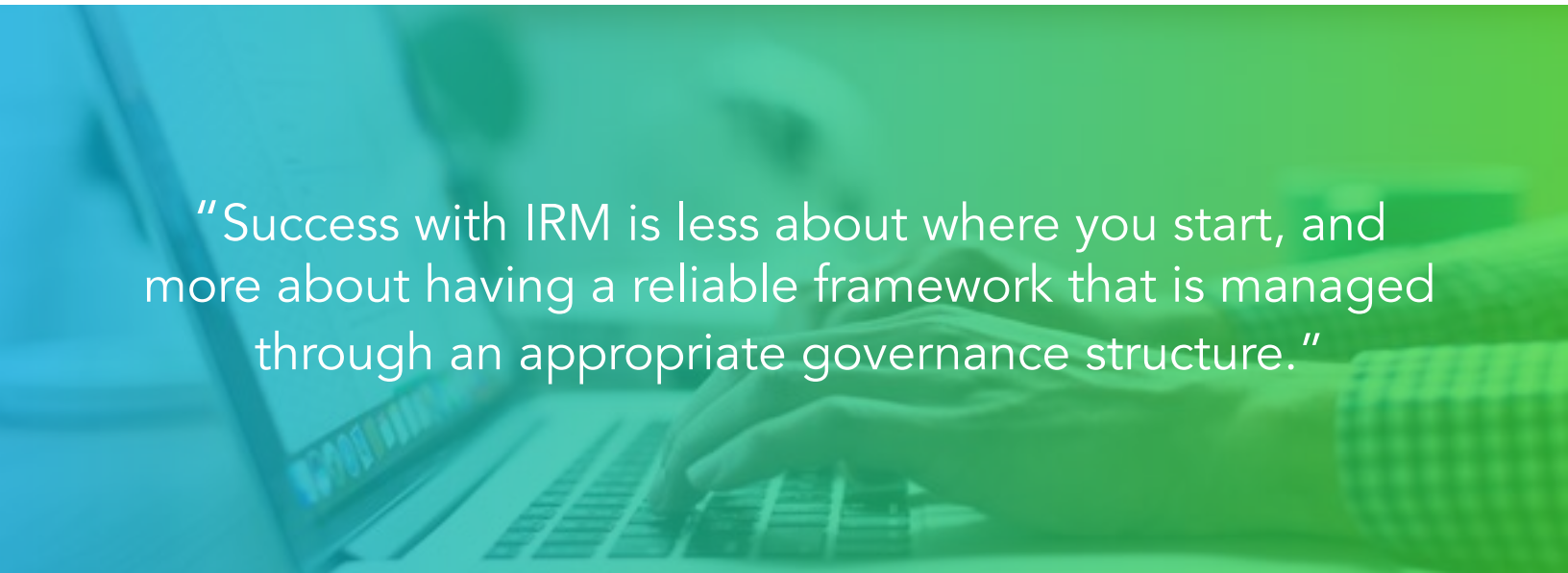
Focal Point is ready to help. We have helped organizations of all sizes implement and optimize their integrated risk management programs to better protect their most critical data:

813-402-1208

info@focal-point.com

focal-point.com

CONNECT WITH US



FOCAL POINT

DATA RISK

Focal Point Data Risk® is a registered trademark of Focal Point Data Risk, LLC.