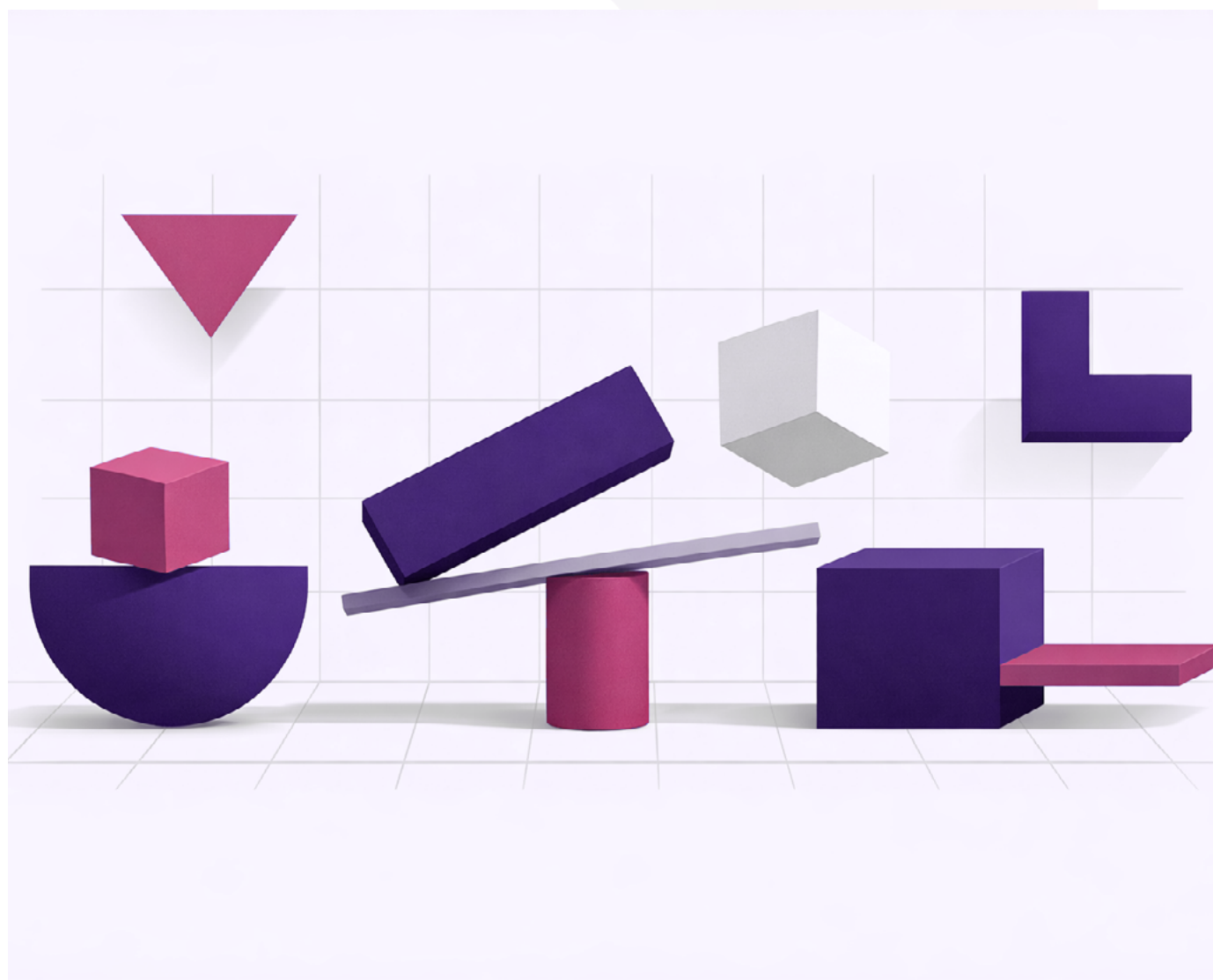


Point of View

7 Counter-Intuitive Ways To Elevate Your Enterprise Risk Management Capabilities



BRINGING FLEXIBILITY TO ENTERPRISE RISK MANAGEMENT

When it comes to Enterprise Risk Management (ERM), there is no shortage of frameworks, lifecycles, and benchmarks. These tools are helpful to have, of course, and provide key foundational concepts that can be invaluable as organizations establish ERM programs and formalize risk management processes. But in the end, nothing can substitute for common sense and knowing when you need to depart from the 'rules', which can only come from establishing, operating, and upleveling many programs across many industries. In this article, we will share some tips and tricks we have gained over the years, some of which may not align with conventional wisdom.

LESSON 1:

NO ONE IS MAKING YOU DO ERM. DO IT ANYWAY

01

Industries in the U.S. have a wide range of regulatory drivers for their risk management functions: Internal Audit, SOX, Cyber Security, Safety, and, of course, Compliance. All of these have regulations and oversight bodies that make focused programs necessary. ERM however, does not. Even though public companies may have requirements to report risks to their leaders and in disclosures, how they do so is not mandated. This results in some organizations viewing ERM as optional, or a "nice to have".

So why should you do it? Do it to uplevel the intelligence of your organization. Be the business that knows what is coming down the road and knows that they're focusing attention in the right areas. Implement ERM so you know whether the money you invested in a risk mitigation plan is actually making a difference. Know that before you go boldly towards a new strategy, you've thought through what could go wrong and planned for it. And know that your stakeholders have confidence that you know all of these things.

LESSON 2:

ALL SECOND LINE FUNCTIONS ARE EQUAL, BUT SOME ARE MORE EQUAL THAN OTHERS

02

Anyone who has worked in risk management is familiar with the Three Lines model. In this model, the first line consists of businesses that own the risks; the third line consists of Internal Audit, which provides assurance for risk management; and in between them is the second line, consisting of all functions dedicated to risk management. In this model, each function is independently responsible for providing the structure, approach, and expertise to manage its domain of risk, whether it's cybersecurity, compliance, talent, or other areas.

All of these roles are critical and certainly benefit from internal subject matter expertise. But running parallel to them all is ERM, tasked with identifying second line risks and elevating the most significant to leadership. A model in which every second line function operates independently misses the value ERM can bring as a standard setter. ERM's cross-functional view and unique connections to both leadership and business lines make it uniquely positioned to provide an informed focus on business-critical cross-domain risks.

When ERM is made central to second line operations, it is ideally positioned to develop enterprise-wide risk management frameworks, including a risk taxonomy, risk rating criteria, reporting templates, mitigation templates, and input into the capital allocation process. This standardization enables more efficient risk functions, apples-to-apples comparisons of risk, and clearer risk information for leaders. Why miss out on the benefit that centralization can bring?

LESSON 3:

A BIGGER COMMITTEE IS NOT ALWAYS BETTER

03

When launching a risk committee, the most common approach is to look for full coverage. You start with a list of every function or risk area, you find the right representative for that area, and they are voluntold to be on the committee. This results in a broad range of expertise on the committee, often with 15 or more members, but it can also lead to low engagement.

Don't do that. At least, not if you want your risk committee to be effective.

Instead of getting every possible representative on your committee, focus instead on getting the right individuals on the committee, even if that's just 3 or 4. These individuals should be employees who want to be there. They should be bold and willing to speak freely, be familiar with risk management, have good visibility into the operation, understand that risk has upsides and downsides, and possess a strong understanding of the organization's strategic goals. Finally, they should be well-connected, which can help make up for a smaller committee size. If these key individuals are sufficiently engaged in the decision-making, information sharing, and cultural tone-setting that comes with a committee, they can bring in other key individuals when it counts.

LESSON 4:

THE INFORMATION FLOWING DOWN MAY BE AS IMPORTANT AS THE INFORMATION FLOWING UP

04

No risk management framework is complete without reporting. We all know that getting the right information to leaders at the right time, with the right data, is vital for the decision making and confidence building that ERM enables.

What may be just as important, though, is what information comes back down the organizational ladder. When surveyed about what works and doesn't work in ERM, business and risk leaders alike describe many ERM programs as a "black box." Risk leaders provide a transparent upward-facing view of the strengths, weaknesses, and areas of concern within their domains through reporting, risk assessments, and other ongoing activities. However, they often don't receive feedback from leadership on what was prioritized, why choices were made, and what decisions will be made moving forward.

Programs that successfully close this loop and facilitate a flow of information from leaders back to businesses are more likely to experience higher engagement in future efforts. Additional benefits may include increased transparency during risk assessments and more sophisticated analyses by risk leaders who take organizational priorities into account. This information flowing back down should be unfiltered and can include which top risks were prioritized, which mitigation efforts were seen as valuable, and where leaders want to invest more in mitigation.

LESSON 5:

SKIP INHERENT LIKELIHOOD

05

Let's engage in a thought experiment. Picture what it would look like if your organization had no cybersecurity. No passwords, no MFA, no firewalls. How would you characterize the likelihood of a cyberattack in those circumstances? Is there a number high enough on the rating scale? That's what we're asking leaders to do when we rate inherent risk. At the end of the day, ERM aims to understand where we are exposed and where we need to change our approach. These goals are muddled, not enabled, by trying to picture a world without controls.

Rather than rating a risk by inherent likelihood, consider a criteria like "Residual Likelihood" or "Vulnerability." These criteria, when developed and trained on properly, can provide a view of which risks are most likely to impact us, considering everything we're actually doing to prevent them. This provides a much crisper view of where more risk response is needed and bypasses the need for complicated scoring methodologies and matrices.

LESSON 6:

SUSTAINABILITY RISKS MAY BE MORE RELEVANT THAN YOU REALIZE

06

As organizations look to identify and assess sustainability-related risks, whether it's through Climate Risk Assessments, Materiality Assessments, or other reporting efforts, they face a range of challenges to successfully integrating these risks into existing ERM efforts. Differing taxonomies, diverse stakeholders, extended timelines to impact, and misaligned impact criteria can all lead to a disconnect from your enterprise risk register. Failing to account for sustainability risks properly, however, can leave a gap in your risk reporting and fail to satisfy stakeholders' desire to know that these risks are considered and managed.

No enterprise risk exists in isolation, and each risk has a set of drivers that cause it and its potential impacts. In many cases, these drivers may have a sustainability component; therefore, the risk they're driving should be considered a sustainability-related risk. Severe drought can cause supply chain disruptions. Severe heat can increase safety risk. Climate migration can lead to market disruption. While none of these sustainability components may be material in and of themselves, it is important to consider them part of a broader risk that may well be material. Once you have identified these climate drivers, you can fold them into your reporting to demonstrate that sustainability is considered and to drive attention to these issues.

LESSON 7:

DON'T TECH ENABLE... YET.

07

Any risk leader drowning in slides and spreadsheets can tell you the value of tech enablement. The efficiency, visibility, insights, and organization that come from a well-designed and well-implemented GRC technology can be game-changing, and these tools should absolutely be brought in at the right time. What you shouldn't do, though, is let the acquisition of a new technology – even just a module of a larger platform used elsewhere in the organization – drive the creation or formalization of an ERM capability. Substance should come first, enablement second.

In order to have a value-adding and sustainable ERM capability, it is vital that the program drives the tool, and not the other way around. Before any ERM tool can be successfully implemented, you first need a defined ERM framework (taxonomy, criteria, scoring, aggregation methodology, etc.). When tools are implemented without that framework in place, implementers will often default to an “out of the box” approach to move the project along. This can result in a program that is not fit for its purpose, doesn't provide value, and will lead to either a) the technology being abandoned or b) a costly reconfiguration.

By no means is it necessary to delay tool implementation for a significant length of time, but it's essential to pick the right time. Select and implement your tool based on what your ERM goals are, what your framework is, and what's the right fit. Look for providers and implementers who truly understand ERM and can help you make the right decisions throughout, rather than going to a default.

Finding What Fits For Your Program

Like all rules, none of these will always apply to every organization. Sometimes conventional wisdom works, and each program is different. But as you embark on launching, re-launching, or enhancing an ERM program, remember to ask the right questions, challenge the assumptions, and bring along the right team for the journey.

About Uniquis Consultech:

Uniquis Consultech is a global tech-enabled consulting company that specializes in Accounting & Reporting, Governance, Risk & Compliance, Sustainability & Climate, and Tech Consulting. The Company is co-founded by consulting veterans Jamil Khatri and Sandip Khetan and backed by marquee investors such as Nexus Venture Partners, Sorin Investments, and UST. Anu Chaudhary, a global sustainability and climate specialist with over 25 years of experience, serves as the Global Head of Sustainability & Climate Consulting.

Uniquis has a global team of 700+ professionals led by 85+ Partners & Directors across eleven offices in the USA, the Middle East, and India. The company serves more than 400 clients, including marquee names in each of the markets it operates in.

Uniquis is committed to leveraging technology and an integrated global delivery model to provide best-in-class consulting services to its clients.

About Our Governance, Risk & Compliance Services:

Our GRC practice partners with organizations as they continue to deal with the dynamic governance, risk, and compliance landscape and navigate today's complex business environment. We seek to prepare business leaders and their teams to identify and manage risks, strengthen governance across levels, ensure end-to-end compliance, design & test internal controls, anticipate and assess any disruptions, and help build business resilience. We help to deploy platforms aimed at digitization and automation of an organization's GRC functions.

A Team That You Can Trust To Deliver



Nagaraj Uchil
*Partner, Global Head
of GRC*



Matt Solomon
Managing Director, GRC

Scan this code to find
more content like this



Visit us at www.uniquis.com

or follow us on

