



A Get-It-Done Guide to ERM A Best Practices Approach



Executive Summary

In this white paper, we will offer a solution to a deep-rooted and often continuing problem facing many Risk Management professionals, namely: *“How do I get started and what do I need to do to build an impactful and sustainable ERM program in my company?”*

The truth of the matter is that many companies still a) lack even a basic, automated ERM platform or b) are saddled with an inflexible infrastructure that does not adequately meet their needs to provide an effective, focused process and responsive Board-level reporting business information and metrics. This leads to a wide range of use-case opportunities for ERM.

This White Paper Will Answer:

1. What is the Compelling Case for ERM?
2. Why Does DoubleCheck Believe An ERM Solution Is Needed?
3. What are the Key Features of the DoubleCheck ERM One Solution – an out-of-the-box Risk Register system?

With that said, this white paper has been designed as a reference point; a document to help guide ERM professionals through a “best practices” process that has been successfully honed for years, via working knowledge and experience, on how to establish a plan to deploy an ERM platform that will get you started or more agile... now!

It’s possible to fill this void by using a largely pre-configured, out-of-the-box solution based on subject matter expertise and composed of core features that are aligned with ERM “best practice” standards and guidance (e.g., ISO, NIST and COSO).

As a starting point, the decision should be made to focus on a small number of key risk attributes (causes, consequences, controls and key risk indicators) and select metrics (severity and likelihood, direction and velocity) that will enable the assessment and prioritization of risk action.

Key steps this paper will address

- Establish Risk Register
- Assign Risk Ownership
- Execute Risk Assessment
- Analyze results / prioritize risks
- Produce Board-ready reports



ERM professionals need a way to make it simple and easy to identify, define, and document risks, within the system and processes used to manage those risks.

Additionally, they will benefit from a partner who offers assistance when it’s needed. It’s like putting together a puzzle, with so many odd-shaped pieces and so many choices, and trying to assemble the picture. Sometimes it’s best to get help to complete the puzzle from those who have years of ERM knowledge, understanding, and experience. They can guide you through the basics and help you understand how all the pieces fit together.

Questions:

- **How do you get started and what do you need to do to build an impactful and sustainable ERM program in your company?**
- **What is the risk to you personally and/or to your company of either doing nothing, and hoping for the best...or just trying to get by with the status quo?**
- **How good do you need to be in this crucially important area?**

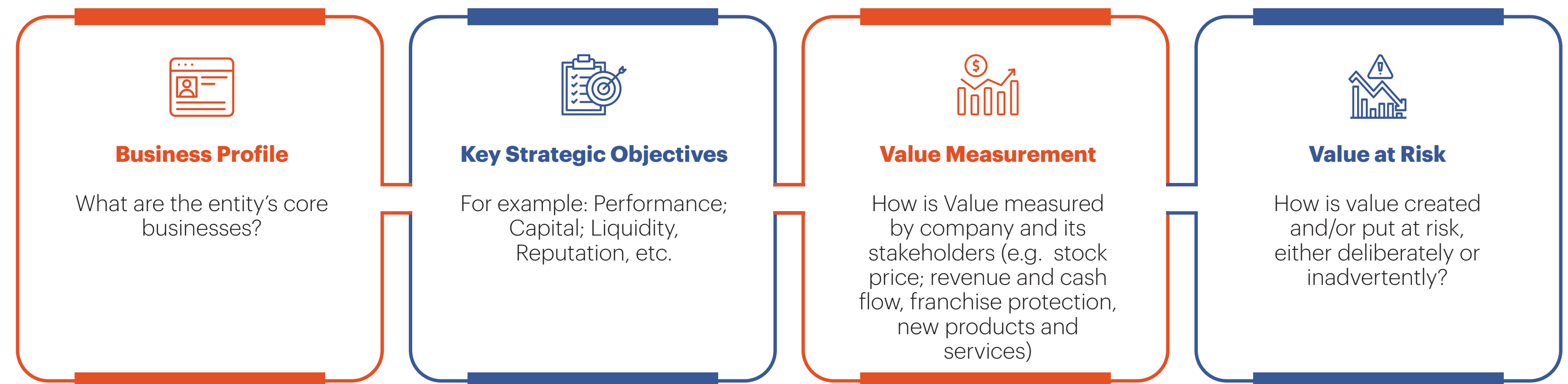
1. What is the Compelling Case for Enterprise Risk Management (ERM)?

In order to fully embrace ERM, there are three inextricably-connected elements that need to be fully understood at the outset:

- Overall Business Context
- Strategic Importance of ERM
- Tactical Execution of ERM

Overall Business Context

The very first step in the ERM journey is to understand and take into consideration the context surrounding the business basics – namely, who is the company and what does it do?



Strategic Importance of ERM: Link with Overall Business Goals and Objectives

Questions ERM Answers:

“If an unfavorable event happens, how will it impact the achievement of our business mission and our current strategic goals?”

“Which events are most likely and, of those, which would be most damaging?”

“What have we already done to compensate for, or prevent, them?”

“Do these mitigation measures work?”

Risk is best defined as the “effect of uncertainty on the achievement of objectives.” The successful management of risk is integrally connected to the achievement of the company’s strategic objectives. Support is needed from the organization’s leadership (people with holistic view of company) since they are the key decision-makers who establish budgets and allocate resources.

Risk is best defined as the “effect of uncertainty on the achievement of objectives.”

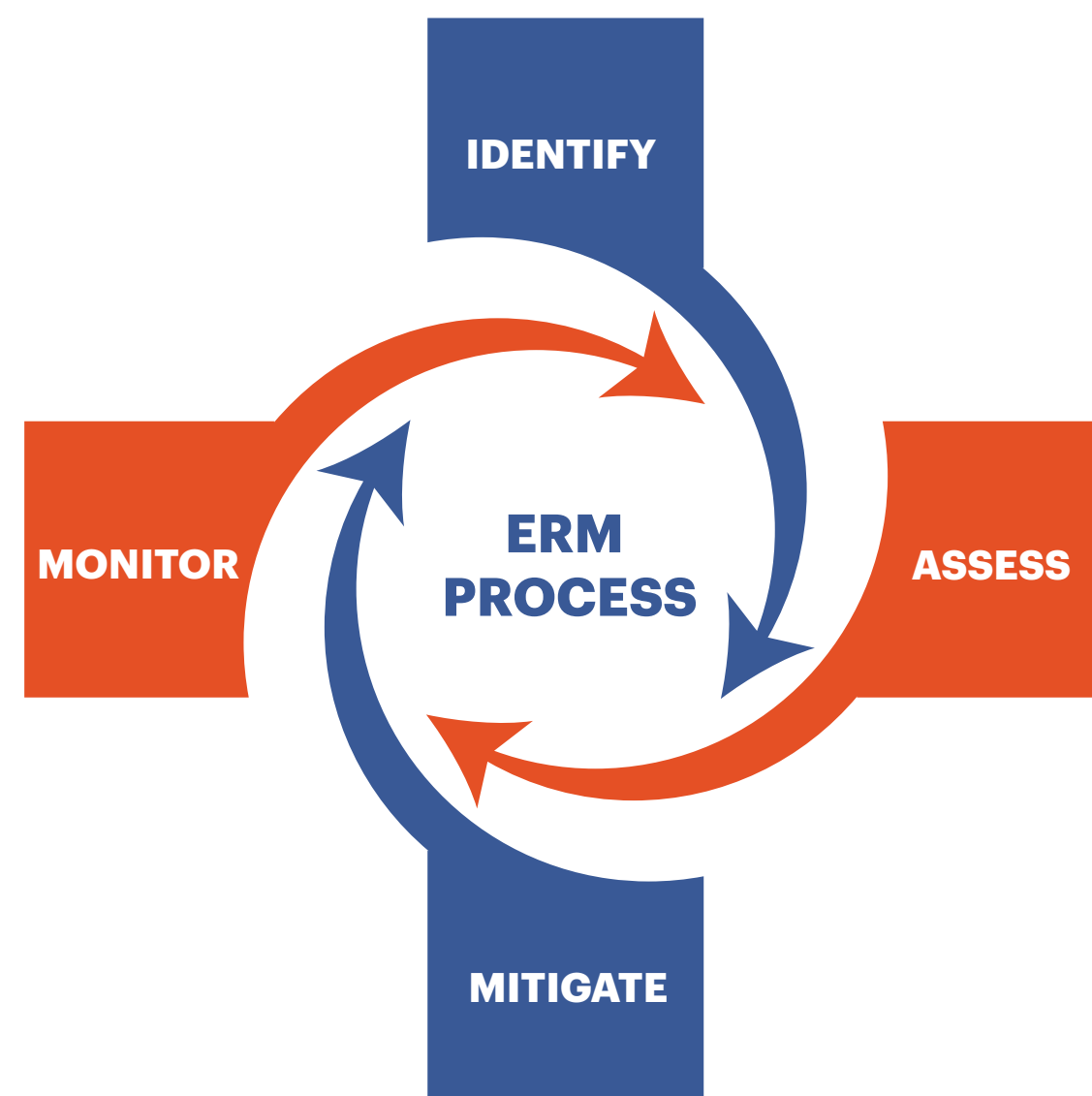
Enterprise Risk Management (ERM) is an essential discipline that needs to be installed, embedded, and inculcated into the organization in order to:

- Assure the active management of risks (i.e. the universe of company risks doesn’t manage itself).
- Set risk priorities and actionable resource allocation.
- Uncover organizational weaknesses.
- Expose hidden, value-add opportunities to exploit.
- Ensure ERM is not perceived as an adjunct to other corporate functions, like Compliance or Internal Audit.
- Establish ERM as a usable regimen, not as a stand-alone hypothesis, to realize its maximum impact.
- Enable the timely flow of risk information to company stakeholders who need to see it and be aware of it.



The Tactical Execution of ERM (via Risk Register)

The four-step ERM process (identify, assess, mitigate and monitor) is essential to the successful achievement of corporate business objectives, oftentimes by avoiding catastrophes or dereliction of duty.



This process needs to be tactically executed, on an iterative (day-in-and-day-out) basis, using a proportionate and reasonable risk register vehicle.

The risk register is foundational, collaborative, and value-oriented, for the following reasons:

Foundational

The risk register attribute “buckets” (causes, consequences, controls and key risk indicators) and metrics (severity and likelihood) allow the components of ERM actionability-identification, assessment, mitigation and monitoring-to be tracked.

Collaborative

Calls upon and engages all deputized individuals with ERM responsibilities and accountabilities

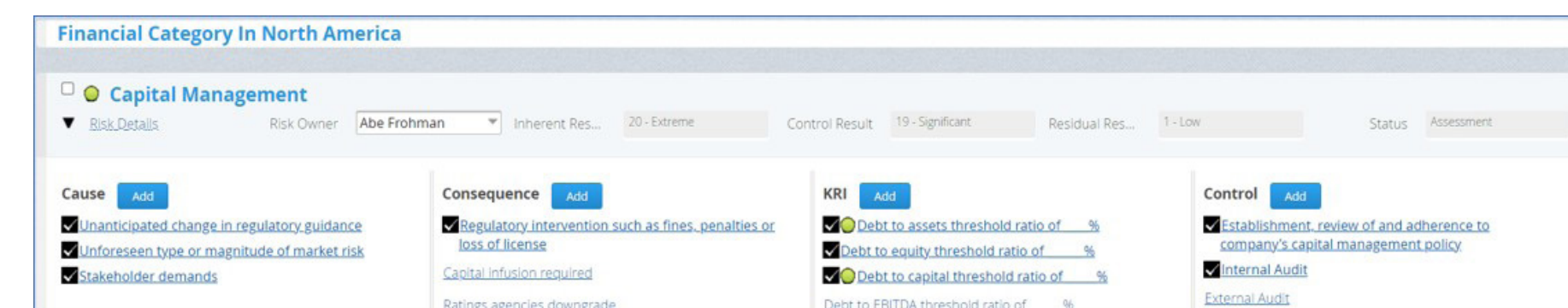
Value-Oriented

Satisfies varied needs across a wide spectrum of stakeholders, such as

- Board of Directors (governance)
- General Counsel and Internal Audit (compliance)
- Company Senior Management/ Leadership
- Middle Management
- All Remaining Employees
- Customers
- Partners
- Investors/Shareholders

More detailed discussion about the risk register (see Figure 1 below) will take place in Section 3 and in the Addendum section of this White Paper.

Figure 1



2. Why Does DoubleCheck Believe a New ERM Solution is Needed?

DoubleCheck is a prominent Governance, Risk and Compliance (GRC) solutions provider with an integrated suite of GRC products (see Slide 19), including those revolving around Enterprise Risk Management (ERM).

DoubleCheck firmly believes that a unified approach to GRC solutions allows a company to leverage GRC information across the enterprise. By linking key elements across risk, compliance, audit and policy management, DoubleCheck's solutions are able to streamline processes and maximize utilization of information dashboards and analytics that cross boundaries. Similarly, linked solutions reduce overlap, share overall insight, reuse work and tackle siloed GRC responses while securing what's private.

More specific to this White Paper, DoubleCheck knows the ERM world, fully understands the merits of ERM and believes in its importance as an essential discipline for all companies, allowing them to achieve their key business objectives. Having said that, DoubleCheck sees ERM voids that exist and challenges to full ERM acceptance.

Those shortcomings are best portrayed via two use cases that will likely resonate with ERM professionals when pinpointing problem areas within risk management. Specifically, the range of Use Cases is shown below:

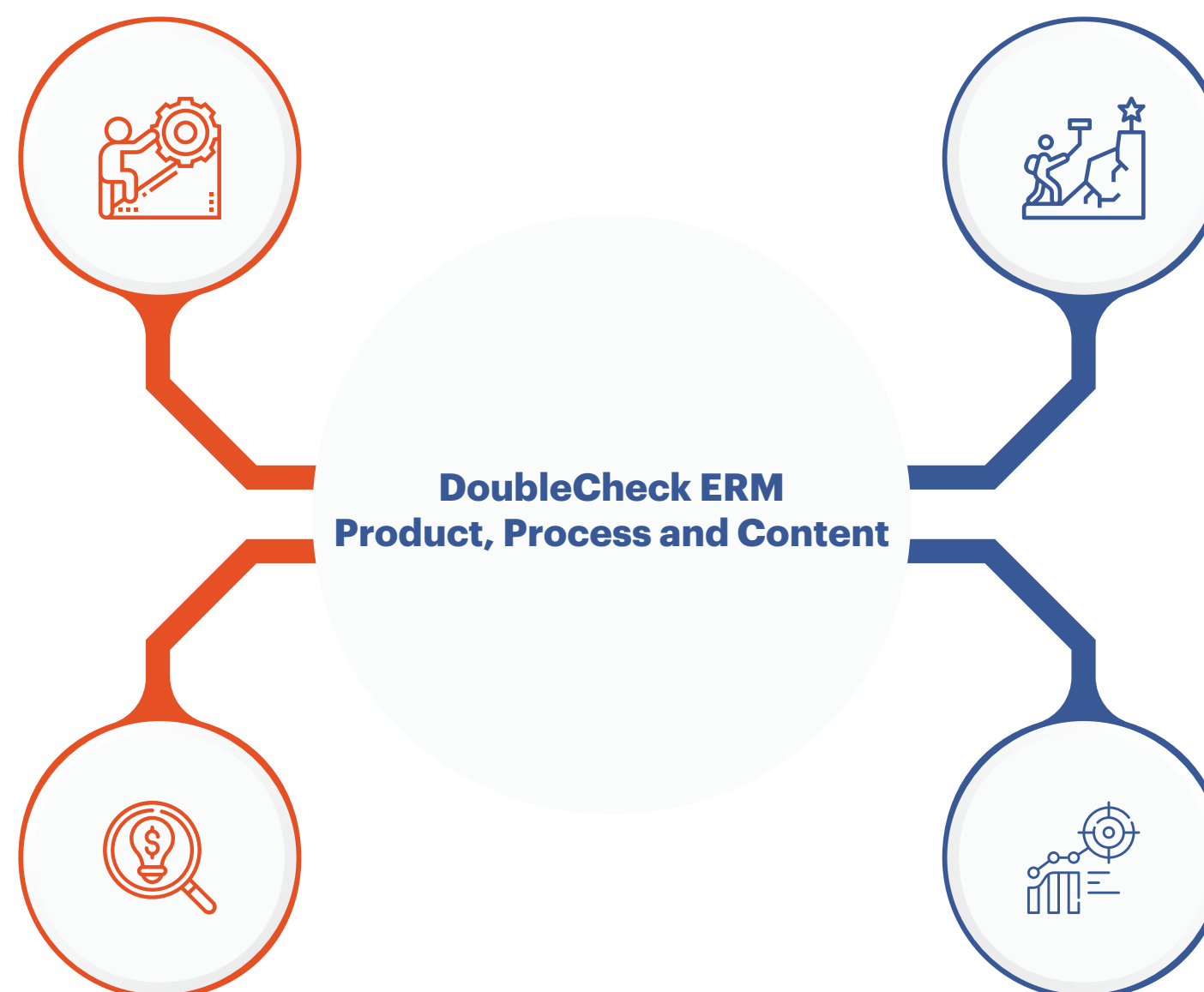
Use Case 1: No ERM Platform in Place

Challenge:

- Nothing in place for ERM
- Reliant on Excel/ Powerpoint E-mail/ Sharepoint
- No Organized, Integrated ERM Environment (Risk Controls, Risk Register etc.)

Opportunity/Need:

- Need for fully bundled ERM environment providing Products, Process & Content
- Fast, greenfield implementations
- Embedded Reporting & BI



Use Case 2: An Embedded GRC Infrastructure... But One That Is Not Delivering As Effectively As Needed

Challenge:

- Complex, rigid enterprise solutions in place
- User environment not streamlined for an agile ERM process
- User dependence on IT for ERM requirements... e.g. reports, workflows etc.
- Existing GRC system focuses on managing process-related risks instead of enterprise risks

Opportunity/Need:

- Streamlined, Cohesive ERM solution
- User managed, Embedded Reporting, Ad Hoc Flexibility, BI and ERM-specific project and Workflow Management

Use Case 1: No ERM Platform

If you have no real integrated platform system in place, any offering might seem like it would be an upgrade. But that's not exactly so. Part of the backstory for "no ERM is in place" is that its absence implies a lack of management concern over risk and perhaps a lack of understanding on how impactful ignoring enterprise risk management can be. In addition, there may be a real shortage of resources to address risk management, even if your executive team has concerns. A better approach might be to look at the operational processes that are critical to the organization. From a positive perspective, it's likely there are already "Plan B's" in place for some of the most critical operations, to assure some level of business continuity in the event of some disruption or incident. Use these as examples of enterprise risk management already in place. This list of recognized risks and actions could then be the germ of your first **enterprise risk register**. Offer that these discrete actions add value to the business, but would be more efficient, avoid duplication of effort and leverage overall efforts across the enterprise if a more centralized, managed approach were implemented. Point out that there's likely no consolidated risk register, no standardized means of assessing risk and evaluating priorities, leading to ineffective allocation of remediation resources. Controls, even when in place, may not be identified or aligned to the processes where they interact. There may be no way of tracking exceptions or evaluating requests for them. And of course, much of any activity may be siloed within specific functions or departments

Use Case 1: No ERM Platform in Place



Challenge:

- Nothing in place for ERM
- Reliant on Excel/ Powerpoint E-mail/ Sharepoint
- No Organized, Integrated ERM Environment (Risk Controls, Risk Register etc.)



Opportunity/Need:

- Need for fully bundled ERM environment providing Products, Process & Content
- Fast, greenfield implementations
- Embedded Reporting & BI

and not offer benefit to the enterprise overall. In short, nobody is truly managing risk from a 40,000 foot level. In addition, it may be that regulatory and compliance obligations are difficult to meet, in the absence of these risk management basics.

All of this is a more powerful way to make a compelling argument from a business impact perspective to help explain and support the need for establishing enterprise risk management. From there, the issue of resources may well fall into place.

On Hand Resources

These rudimentary tools rely upon specific expertise and execution by someone who put it all together on his/her own. Even if done with skill, and well documented, they do not scale well, support facile shared input, secure sensitive data stored, and assure straightforward methods for identifying and gathering, assessing, mitigating, and monitoring risk. They just aren't up to the task. Instead, there needs to be powerful, but simple-to-use, tools to portray risk data in a business context for management to understand, address, and assign resources to appropriately mitigate the identified risks to an acceptable residual level. Also, users and program administrators need training to use the features of whatever ERM processes are put in place. And, of course, it all needs to be maintained and updated, both in process and content, as the business environment and risk profile of the enterprise changes.

Desktop tools like spreadsheets, small databases, and other office automation tools assembled in parts can offer some beginning steps to risk management, but fall far short of delivering the services needed to truly run an efficient, comprehensive program.

Use Case 2: An Embedded ERM Platform... But One That Is Not Delivering As Effectively As Needed.

This case is almost the polar opposite of Use Case 1. Here, there is an enterprise solution in place, if you can manage to understand it and put it to use. In this case, your only offered option is a “nuclear submarine”, when all you need is a reliable, agile PT boat to cross the waters before you.

Further, it may be built upon a large, centralized, and technologically complex foundation with powerful capabilities that rely upon dedicated expertise from IT resources outside the organization.

Sometimes, centrally developed and implemented ERM solutions grow to be so complex, inflexible, and difficult to operate, without extensive support and training, that they tie an organization up in knots and impede an organizational unit’s ability to operate them effectively. Further, they may be built upon a large, centralized and technologically complex foundation with powerful capabilities than rely upon dedicated expertise from IT resources outside the organization.

Often, these systems have been implemented at great institutional expense, and they consequently represent an accepted “standard” that everyone within the organization is expected to use. Adding other solutions may be viewed as unnecessary, wasteful, and redundant.

Use Case 2: An Embedded ERM Platform... But One That Is Not Delivering As Effectively As Needed.



Challenge:

- Complex, rigid enterprise solutions in place
- User environment not streamlined for ERM process
- User dependence on IT for ERM requirements... e.g. reports, workflows etc.
- Existing GRC system focuses on managing process related risks instead of enterprise risks



Opportunity/Need:

- Streamlined, cohesive ERM solution
- User managed, embedded reporting and BI, and ERM specific project and workflow management

In this complex and inflexible environment, the product may be in place, but its processes and content may not always meet the unit’s needs. Timely delivery of risk data, assessment reports, mitigation and remediation project status updates, and management of a specific risk register and related controls effectiveness may not be easily possible with the resources assigned within operating units. Inability to operate in an efficient fashion, to deliver accurate assessments dependent upon centralized IT resources that may or may not be able to make the changes needed in one area due to conflicts or processes in force elsewhere, may constrict or prevent

timely risk assessment, and defeat the ability of an organization to meet its “identify, assess, mitigate, and monitor” tasks. What local ERM resources really need is a solution that supports their reliable delivery of risk management practices upward to the larger enterprise, as well as the ability to operate without reliance upon centralized IT resource out of their control. In rigid environments, conversely, any specific configuration needed to address a specific need, or even the basic operation of these systems, often requires the intervention of, and coordination with, a centralized IT department. The central IT schedule and resource priorities may not match your business’ risk management obligations. Regardless, when you need specific reports, modifications to workflow parameters or escalations, email routing, or any other automated provisions of this ERM system, a request into a centralized IT department is necessary. And then you wait.

“Inability to operate in a timely fashion, to deliver accurate assessments dependent upon centralized IT ... may constrict or prevent timely risk assessment.”

On Hand Resources

But risk doesn’t wait. Risk management is essential and, in some instances, may be existential to company achievement of its goals and obligations to investors, clients, customers, and other stakeholders. Local organizations often have risk expertise to manage processes and specify content, but lack the tools to effectively deliver a comprehensive ERM program.

In order to be most effective, risk management needs to be embedded into the organization with deputized risk program participants who are local to the business unit, and understand its specific needs, methods, and operating style. They need to have the capability to manage and specify configuration changes to workflows, design reports, manage a risk register, align controls, and report on mitigation efforts. Timely ERM program delivery is crucial. Participants cannot rely upon spreadsheets or other desktop productivity tools to support input to a complex, inflexible system they are unable to modify or reconfigure to enable their management of processes and content. They need a solution that's simple to use, manage, and implement independently, yet one that will deliver the content, results and process support necessary to operate an effective risk management program.

Use Case Solutions

The best approach to these problems is to implement a fully-bundled, out-of-the-box ERM environment providing Product, Process & Content. Each element is vitally important. Product, in terms of the tools and automated services necessary to operate an ERM; Process, to enable easy implementation,

The best approach to these problems is to implement a fully-bundled, out-of-the-box ERM environment providing Product, Process & Content.

configuration and operation to work within your operating culture; and Content, to include controls and framework standards, a basic risk register, and more.

Such an ERM solution needs to be dependent upon little to support its presence, a "greenfield" kind of implementation. It needs to be a streamlined, cohesive ERM solution, managed by its users, that delivers all the essential product, processes, and content needed to proactively identify, assess, mitigate and monitor risk.

"...a "stand alone" out-of-the-box solution needs to enable local risk managers to set risk priorities and allocate actionable resources, expose hidden, value-add opportunities to exploit, and uncover organizational

This solution should have embedded reporting, BI and ERM-specific project and workflow management features to support local management and facilitate any reporting or compliance obligations present at a higher organizational level. A "stand alone" out-of-the-box solution enables local risk managers to set risk priorities and allocate actionable resources, expose hidden, value-add opportunities to exploit, and uncover organizational weaknesses. Such a solution should ideally offer a largely pre-populated risk register and align with leading controls standards and best practices as presented by ISO,

COSO, NIST, and others. And, as a final ask, it should enable the timely flow of risk information to company stakeholders who need to make informed risk management decisions, set priorities, and allocate resources at the enterprise level.

Sourcing a solution that fits these requirements, one that is straightforward to implement and without great reliance upon centralized IT resources, becomes the ultimate ERM goal. Proceeding from there will enable a localized solution, one that can expand easily in scope or scale as need arises, without re-implementation or wasteful re-work to operate an efficient and effective enterprise risk management program for an enterprise of any size or organizational relationship to an overarching entity.



3. What are the Key Features of DoubleCheck ERM One™ – An Out-Of-the-Box Risk Register System.

ERM One™, the out-of-the-box risk register solution that DoubleCheck has developed, is predicated on the understanding that there are three attributes of an effective ERM Solution (Product, Process and Content). These attributes, in combination, deliver the critical services, tools and capabilities that companies require to tactically execute upon the four elements of day-to-day risk management (Identify, Assess, Mitigate and Monitor) with efficiency and effectiveness.

DoubleCheck has structured the tool in a modular manner, with options available to add incremental GRC functions or advanced business intelligence (BI) capabilities to extend functionality.

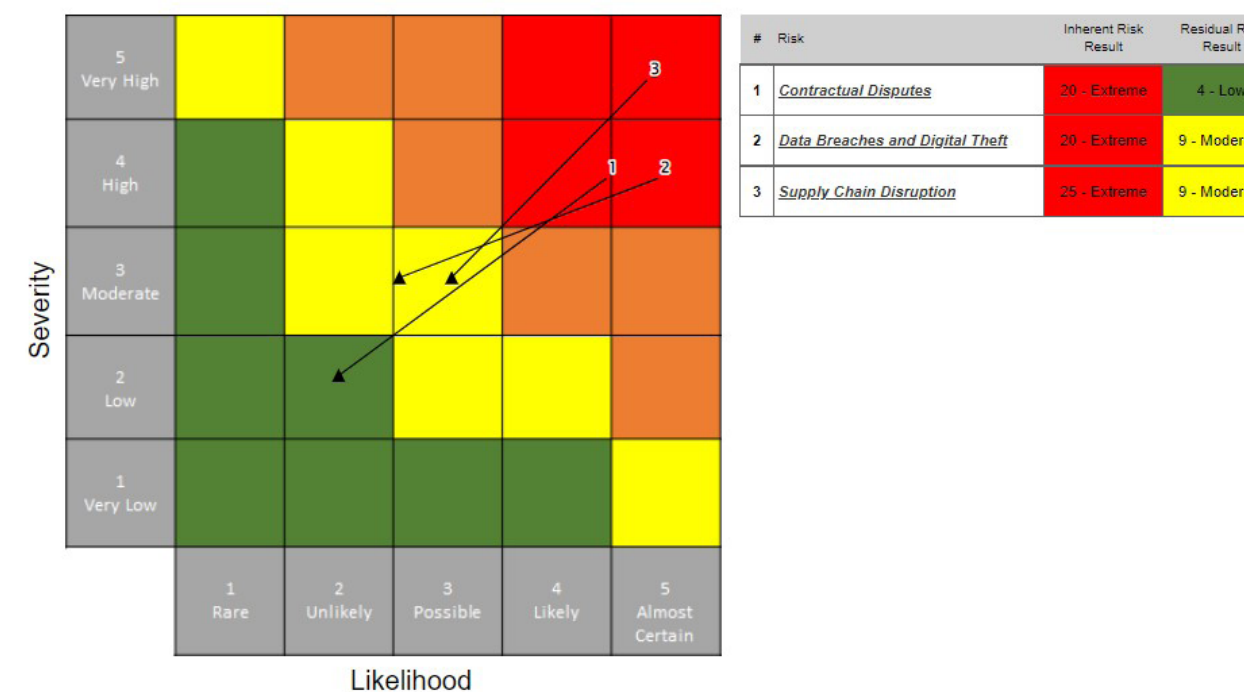
Further, services and features are highly integrated into one package. Reporting is embedded rather than independently aligned to content and processes, making the risk management practice a seamless effort rather than a disjointed one. It is delivered as an immediately-operational ERM platform, through a unified combination of its:

- **Product** – automated workflows; embedded business intelligence; project management; automated notifications; system generated heat maps, comprehensive risk reports, navigation through visualization; assessments; documentation management
- **Process** – risk identification, quantification, mitigation documentation, reporting and review
- **Content** – pre-populated (“running start”) risk universe, risk categorization, rating scales, individual controls by line of defense

Risk Arrow Heat Map

- indicates both inherent and residual risk values for each risk, and demonstrates the impact of controls. See Addendum section for larger image.

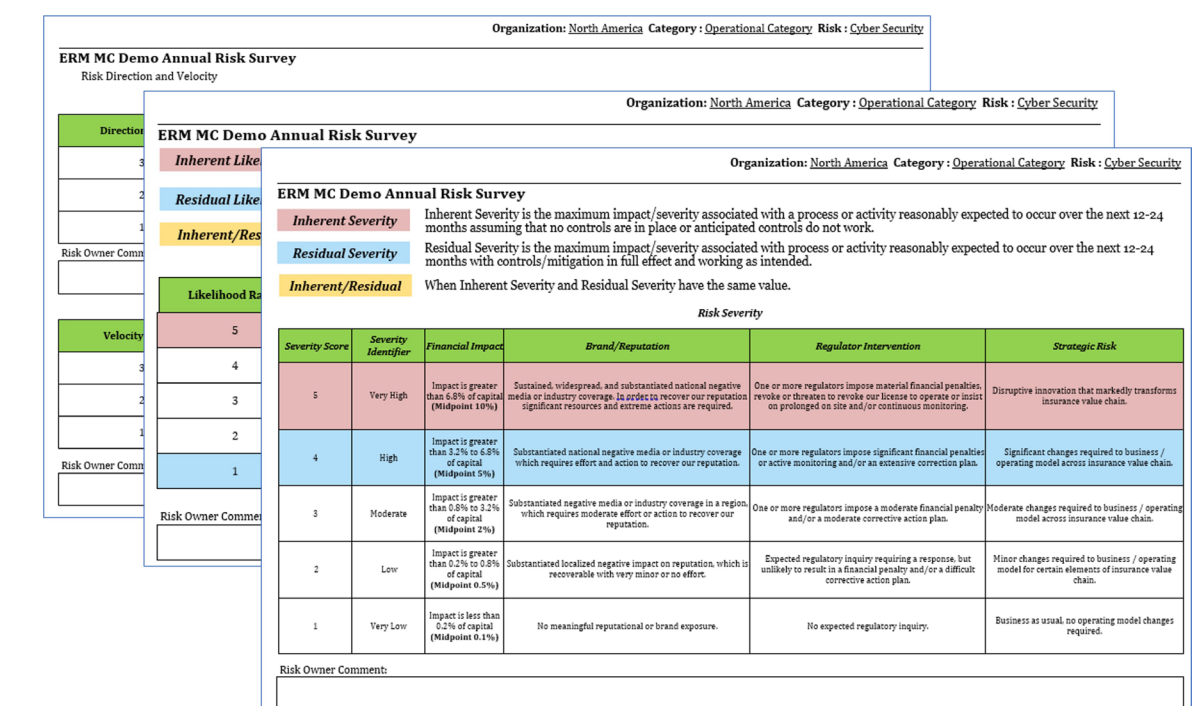
Figure 2



Comprehensive Risk Report

- shows a multi-page report that details all aspects of a particular risk, along with metric definitions so as to be easily understood by a non-ERM person. See Addendum section for a larger image.

Figure 3



DoubleCheck ERM One™ is, therefore, a defined, ready-to-use ERM solution with an install-to-operational potential timeframe of a mere 2-4 weeks.

DoubleCheck ERM One™ will take only 2-4 weeks to implement

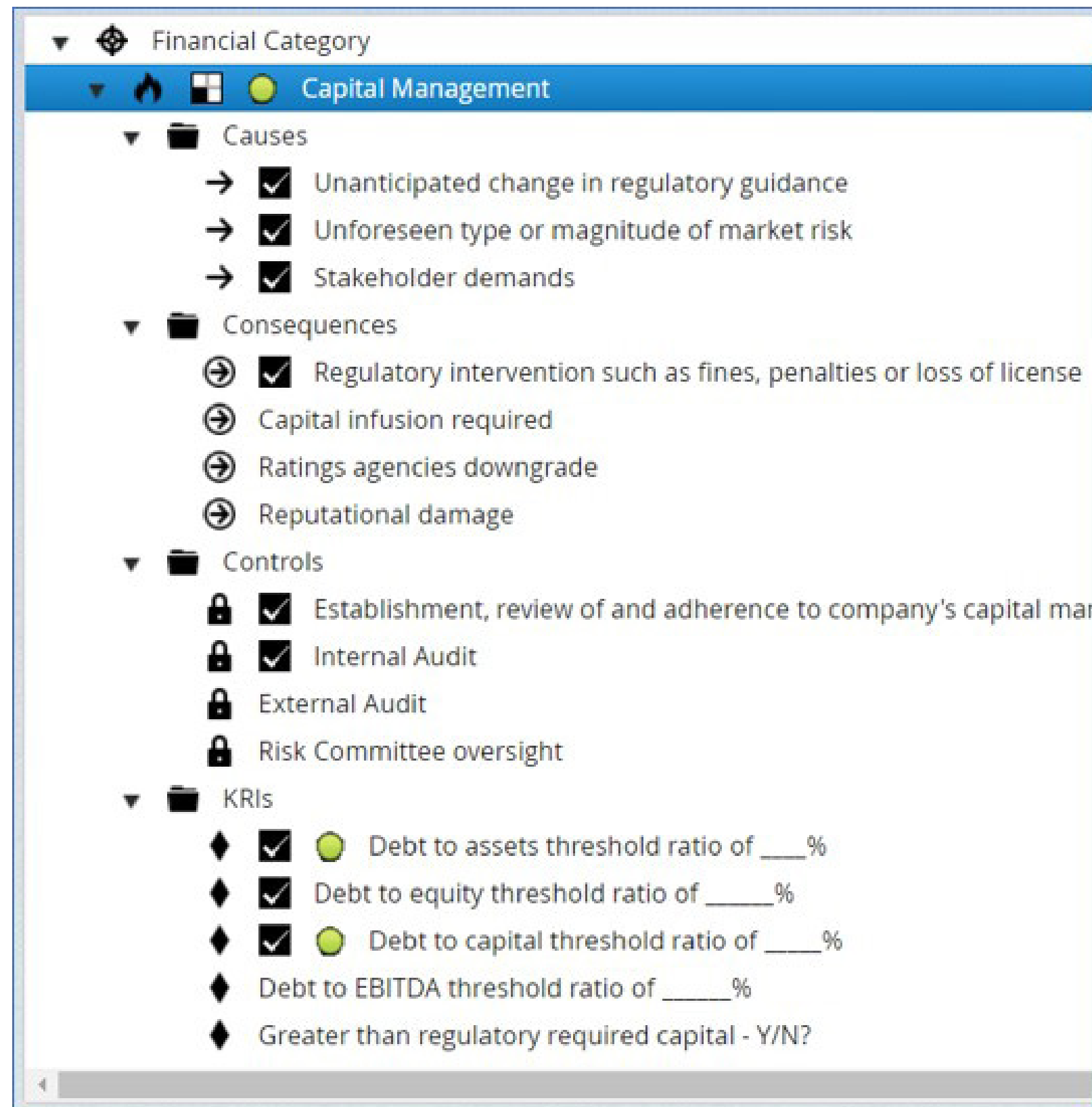
It is a largely turn-key application that is economic, intuitive and outcome-based.

It is designed to be flexible, not rigid and constraining, because DoubleCheck understands that the ideal, outcome-based risk management system needs to be agile and follow the dynamic nature of ERM itself.

With all this said, the top ten (10) reasons to choose the DoubleCheck ERM One™ solution are, as follows:



ERM Risk Content data view



Building A Risk Management Program Through the DoubleCheck ERM One™ Solution

When it comes to our business lives, we sometime find ourselves staring into a blank screen when establishing a risk management program. The process is actually straightforward.

Risk Process Done

- Establish Business Context
- Define Risks Within the Overall Universe
- Identify Risks
- Assess Risks
- Mitigate Risks
- Monitor Risks



Establish Business Context

Often overlooked, this is a vital beginning step to assure business relevance and promote meaningful dialogue with company leadership. Examine the business basics of your company, specifically who you are and what you do. In DoubleCheck's ERM One™, a company is guided by its risk universe in terms of four categories (Financial, Operational, Strategic and Business-Specific).

Define Risks Within the Overall Universe

There is art and craft to effectively doing this. If the universe is defined at too granular a level of specificity, the landscape become unmanageable, and conversely, if done too broadly, it evaporates into meaningless messaging. This is where your business context becomes your "North Star".

Expressing all risks in terms of their impact upon achievement of objectives is a way of establishing clear relevance to senior leadership, who will be responsible for allocating resources to your program to help mitigate and manage identified risks, and sponsor remediation efforts to manage them. This is the Identify process step to risk management.

Identify Risks

Key tasks are to:

- Detect and describe risks that could compromise the ability of the organization to achieve its business objectives.
- Establish ownership and accountability for each risk – one and only one owner deputized as subject matter expert (SME) for each risk.
- Clearly state business purpose which should fully weave in information on the inherent risks in the business.



DoubleCheck provides the mechanism for risk owners to describe their risks within the overall risk universe and establish both inherent and residual likelihood and severity for every risk. Pre-configured risk categories and a pre-populated risk register offer a clear jump start to this process, yielding accurate, comprehensive, and quality findings.

Once you've built your preliminary set of risks to objectives, you are well advised to share the list with stakeholders who can add detail and specificity with respect to core disciplines.

These should include, but not specifically be limited to, IT, Finance, Audit, Operations, Product Development, Support Services, Procurement, Third Party Management, Regulatory Compliance, and Facilities.

Assess Risks

If there is one activity that best personifies the iterative, tactical-execution core of ERM, it's the risk assessment!

- Risk Assessment builds out metrics based upon risk owner perceptions – likelihood, severity, direction and velocity.
- Relies on experience as well as analytical and intuitive thinking by the risk owner.

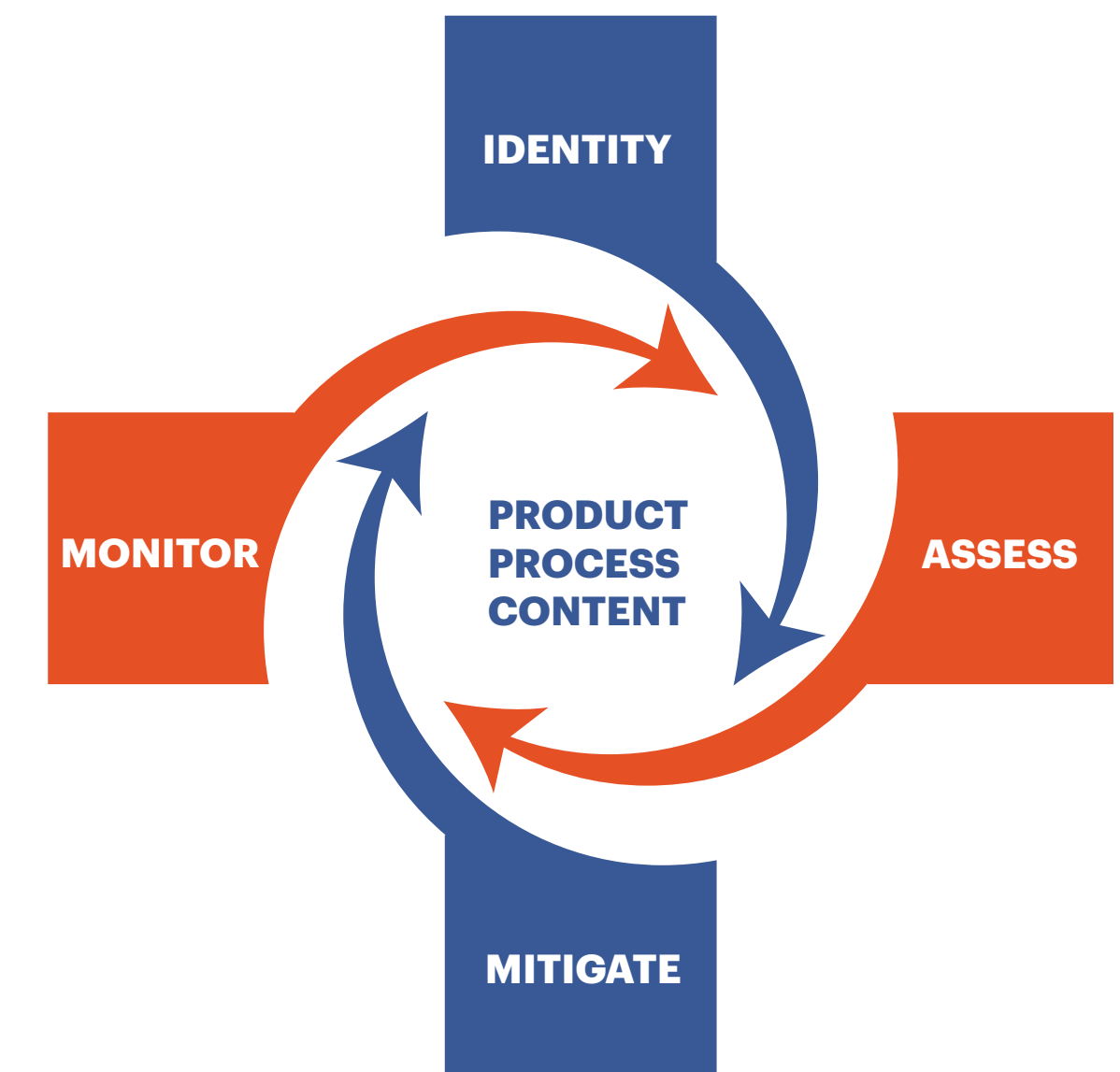
This is the action step that is derived from and drives mitigation and helps prioritize monitoring that leads, in turn, to actionability. This is where your risk "health" is determined. If your risk register is a thermometer, this is where you take your company's temperature.



DoubleCheck ERM One™ enables measurement approaches involving complex performance indicators, to be communicated succinctly in a common business language. DoubleCheck's ERM One™ rating scales and its intuitive, built-in survey management processes help you manage assessment efficiently, while optimizing subject matter expert resources.

The register, and any frameworks or further control questions, or other content you might have applied to supplement the register, are your key tools now to assess where your risk is well addressed and where additional resources are most urgently needed. The findings of the assessment define your current state, in the context of your business' needs and goals, and drive your program's response. The features of the tools you use to do this, through your GRC platform or whatever else you might use, are all focused upon a review of the content of the register, a determination of risk to your business by qualified individuals within it, a second estimation of the effectiveness of any controls implemented to address that risk, and an estimate of remaining, residual risk in place. Those qualified reviewers also need to consider the impact

upon your business, the potential velocity, or speed that a risk can manifest itself to maximum effect, and reflect those professional judgements in your risk scoring mechanisms. In brief, the end result is that snapshot in time, for wherever you have examined, of the risk state of your business.



Mitigate Risks

What do you do in order to actively manage risks in your universe?

- Design and implement a range of mitigation measures to reduce the likelihood and severity associated with each risk source to an appropriate residual risk level,
- Ensure that primary responsibility for risk control rests in the daily and first line of defense activities in the business units, profit centers and support units,
- Establish additional risk management and control responsibilities in the second line of defense, oversight functions that monitor effectiveness and escalate issues as appropriate,
- Provide checks on 1st and 2nd line activities through third line independent challenge, validation and assurance.

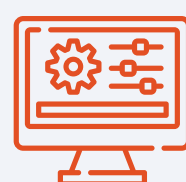


DoubleCheck ERM One™ provides a mechanism to individually describe each control and assign a line of defense - first, second or third - to each of those mitigation measures. With embedded reporting and BI tools, you will always know the state of your mitigation efforts.

Monitor Risks

Keeping a current, accurate understanding of risk status is a blend of reporting, comprehension, judgement, and decision making. Your Board of Directors, and any related committees, are accountable for addressing and managing risk to their shareholders, regulators, customers, and other stakeholders. ERM is a primary vehicle and tool that provides them with the information, guidance and confidence to make quality decisions to manage and mitigate risk effectively. Without this indispensable vehicle that allows and promotes absolute risk transparency, the value of risk management across your enterprise cannot be fully realized. Monitoring as a process includes:

- Analysis and clear communication of risk matters to all key internal and external stakeholders, including risk takers, business leaders, regulators and the Board of Directors.
- Particular emphasis on risks that are: a) material and b) those that might be changing and/or emerging.

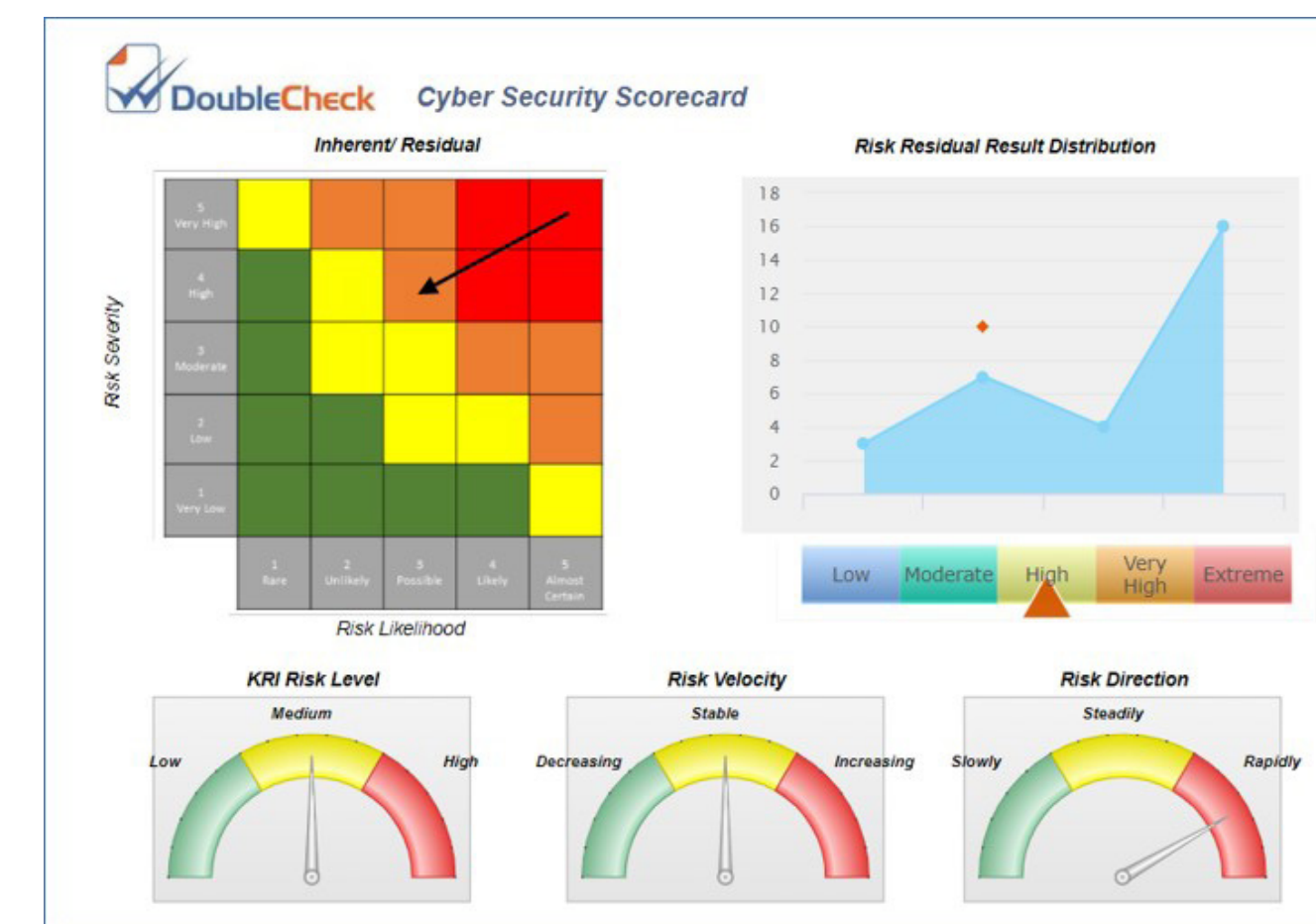


DoubleCheck ERM One™ facilitates the active monitoring process of ERM through established KRI's. DoubleCheck's, proven, Board-level configured reports and scorecards assure that your executive team will be well positioned to make informed risk management decisions. Everyone needs to be on the same page with regard to the ERM message. The very design of the DoubleCheck ERM One™ is established with that end in mind.

Risk Scorecard:

Provides an overall status of a particular risk. See Addendum for larger image.

Figure 4



The DoubleCheck Standard of Excellence

This white paper offers guidance on many risk management issues. All of them point towards the benefit of utilizing a quality ERM tool to support execution. DoubleCheck understands that three attributes of ERM (Process, Product, and Content) are essential to delivering the critical services, tools, and capabilities companies require to manage risk (Identify, Assess, Mitigate, and Monitor) with efficiency and effectiveness. Further, its services and features are highly integrated into one package, and reporting is embedded within, rather than dependent upon independently aligned content and processes, making the risk management practice a seamless effort rather than a disjointed one. Whether out-of-the-box core functionality, or a more expansive, yet tailored implementation, DoubleCheck ERM One™ offers products, processes, and content on an agile, configurable, and scalable platform, designed to support all your enterprise risk management needs, wherever your company may be on the ERM use-case spectrum.



Questions and Answers about DoubleCheck ERM One Solution: Proactive Anticipation of Potential Concerns

- **Question:** How does the DoubleCheck view of ERM stack up against prominent ERM standards?

Answer: The DoubleCheck ERM One™ principles, particularly the four-step tactical execution process (identify, assess, mitigate and monitor) is in solid alignment with both the International Organization of Standardization - ISO 31000 (Risk Management Principles and Guidelines) - and with four (4) key releases on ERM over time by the Committee on Sponsoring Organizations, or COSO, (2004, 2012, 2013 and 2017).

- **Question:** What is the degree of DoubleCheck help that will be provided in the initial installation of the tool itself?

Answer: As much as needed. Assistance will be totally individualized.

- **Question:** Extent of interaction in the first year or two of activity – for instance, running the initial surveys?

Answer: DoubleCheck offers a wide range of help desk services, including a White Glove Helping Hands approach to system administration and user support.

- **Question:** Could DoubleCheck actually act as our outsourced Risk Manager, taking direction from us but doing all the real work?

Answer: Very simply, yes. DoubleCheck has done so in the past and could take on that role in the future.

- **Question:** What about emerging risks? How are they handled in the tool?

Answer: This is a common question. The ability to include emerging risks is vital to the dynamic strength of the ERM program, whether the addition of an emerging risk is prompted during the standard risk assessment process or as a one-off special risk identification exercise. The

DoubleCheck ERM One™ tool is able to accommodate either emerging risk approach equally well.

- **Question:** You've mentioned cyber and third party risk management as branches of core ERM? Would others (e.g. climate risk) be handled in exactly the same way?

Answer: Yes; the core, disciplined ERM process does not deviate from risk to risk. The process works for the entire universe of risks as well as any emerging risks.

- **Question:** Can we download reports into separate tools we have like Power BI? Is there a way that the DoubleCheck tool can do that and be a fully-integrated solution? If so, please describe the Business Intelligence (BI) platform that is included.

Answer: Yes! However, there is no need to do so. The DoubleCheck BI fully-embedded platform is extremely robust and able to handle all of your reporting needs and desires.

- **Question: What about ad-hoc reporting?**

Answer: This is one of the strongest elements of the DoubleCheck value-add proposition – our ability to listen to the client’s real needs and customize a reporting solution that meets that company’s unique needs. DoubleCheck understands that no two clients have precisely the same needs. An agile, ad-hoc reporting capability is a vital delineator.

- **Question: You hear so much about a client’s wishes, wants or needs? How can DoubleCheck ERM One™ work to address all of our ERM concerns?**

Answer: We believe that, with DoubleCheck, you’ll find a trusted business partner who works with you from the very beginning and provides continued support. As a result, with DoubleCheck ERM One™, you’ll be enabled to:

- *Get the right information in front of the right people,*
- *Respond faster in order to proactively mitigate risks, and*
- *Create compelling visualizations to easily analyze data and share with executive leadership.*



About DoubleCheck Suite of GRC Services

If you are looking for enterprise software that can support your Compliance, Risk, Audit or Enterprise needs, DoubleCheck can help. We offer highly configurable solutions that can be tailored to your company's users, data and processes. We offer embedded Business Intelligence features that give you the dashboards and reports you and your management wants. DoubleCheck works as your partner to deliver solutions that support your business processes, not the other way around.

Compliance

- Financial (SOX, PCI)
- Industry (NERC, HIPAA)
- Department (HR, IT)
- Approvals and Certifications

Audit

- Program definition base on client specific scoring
- Management review, overrides to final plan
- Engagement Planning
- Electronic Workpaper Management
- Issue and Remediation Management

Double Check's Integrated Suite of GRC Products

Governance

- Policy Definition
- Policy Renewal
- Demonstrable
- Performance

ERM

- Identify Risk and Drivers
- Assess Risk and Consequences
- Prioritize Risk Mitigations
- Monitor Risk via KRIs
- Include Functional Risks such as Financial, Cyber Security, Third-party, or IT Risk

Risk Owner Workbench

- Displays the metrics and associated Causes, Consequences, KRI's and Controls for a risk, within a Risk Category

Figure 1

Financial Category In North America

☐ **Capital Management**

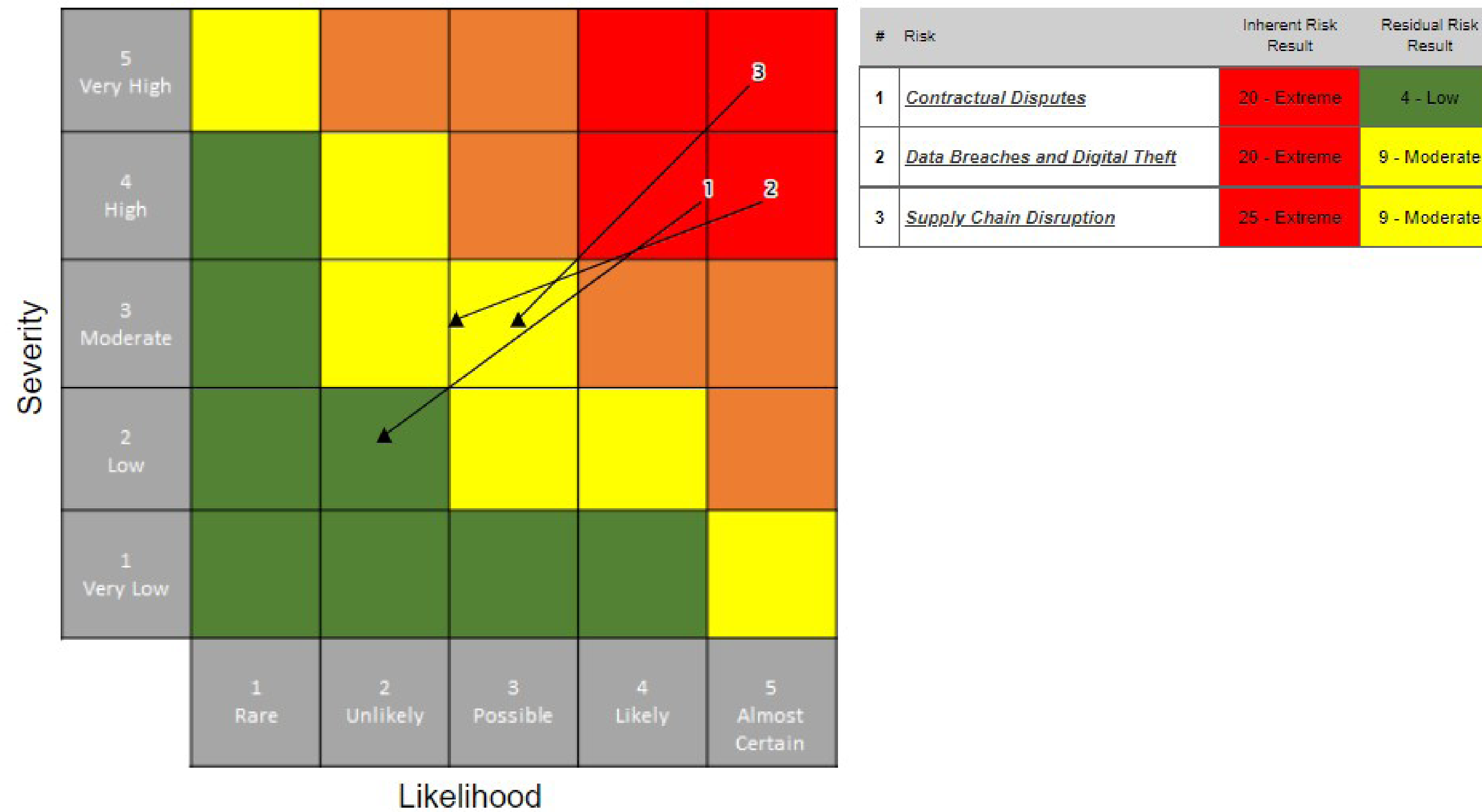
▼ Risk Details
Risk Owner: Abe Frohman
Inherent Res...: 20 - Extreme
Control Result: 19 - Significant
Residual Res...: 1 - Low
Status: Assessment

Cause	Consequence	KRI	Control
Add <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Unanticipated change in regulatory guidance <input checked="" type="checkbox"/> Unforeseen type or magnitude of market risk <input checked="" type="checkbox"/> Stakeholder demands 	Add <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Regulatory intervention such as fines, penalties or loss of license Capital infusion required Ratings agencies downgrade 	Add <ul style="list-style-type: none"> <input checked="" type="checkbox"/> ● Debt to assets threshold ratio of ___ % <input checked="" type="checkbox"/> Debt to equity threshold ratio of ___ % <input checked="" type="checkbox"/> ● Debt to capital threshold ratio of ___ % Debt to EBITDA threshold ratio of ___ % 	Add <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Establishment, review of and adherence to company's capital management policy <input checked="" type="checkbox"/> Internal Audit External Audit

Risk Arrow Heat Map

-Indicates both inherent and residual risk values for each risk, and demonstrates the impact of controls.

Figure 2



Comprehensive Risk Report

-A multi-page report that details all aspects of a particular risk, along with metric definitions so as to be easily understood by a non-ERM person

Figure 3

Organization: <u>North America</u> Category : <u>Operational Category</u> Risk : <u>Cyber Security</u>
<p>ERM MC Demo Annual Risk Survey Risk Description, Causes, and Consequences of Risk</p>
Risk Description
Risk associated with the compromise of company information that impacts the confidentiality, integrity, or the availability of that information due to targeted or non-targeted, <u>internal</u> or external information security threats.
Causes of Risk
<ol style="list-style-type: none"> 1.Malware / Ransomware infecting desktops, laptops, servers and preventing business processes 2.Phishing scams and visiting exploited web sites where malware can be pushed to the user 3.Internal or external threat actor who exploits vulnerabilities to disrupt business processes 4.Social engineering against employees to trick them into malicious actions 5.Security/privacy breach where confidential, corporate and/or client sensitive information has been lost, stolen, or inappropriately disclosed, either accidentally or deliberately 6.Inappropriate access to systems and applications 7.More extensive use of third-party cloud-based services, and ease of use of moving sensitive information to the cloud by non-technical staff
Consequences of Risk
<ol style="list-style-type: none"> 1.Regulatory fines and other enforcement actions 2.Significant legal expenses 3.Civil penalties 4.Business interruption/restriction 5.Reputational damage leading to business impact 6.SEC filing that includes material risk

ERM MC Demo Annual Risk Survey

Risk Controls and Key Risk Indicators

Risk Controls

1st Line

- 1.Restricted system access
- 2.Change Management Process
- 3.Encryption on Workstations
- 4.Encryption on Removable Media
- 5.Identifying lost/stolen devices
- 6.Critical Vulnerabilities - External Servers
- 7.Critical Vulnerabilities - Internal Servers
- 8.Regular scans are conducted of estate to confirm anti-virus is fully implemented on all devices. Effective actions are taken to remediate any deficiencies in an appropriate timescale.
- 9.Review of operating system and database management security systems

2nd Line

- 1.Risk Committee - Oversight and Review

3rd Line

- 1.Internal Audit
- 2.External Audit

Key Risk Indicators

- 1.Compliance breaches - cyber security _____
- 2.Data breaches - _____
- 3.Unauthorized access - _____
- 4.Business disruption from cyber-attacks - _____ threshold
- 5.Local regulatory issues related to cyber - Y/N

ERM MC Demo Annual Risk Survey

- Inherent Severity** Inherent Severity is the maximum impact/severity associated with a process or activity reasonably expected to occur over the next 12-24 months assuming that no controls are in place or anticipated controls do not work.
- Residual Severity** Residual Severity is the maximum impact/severity associated with process or activity reasonably expected to occur over the next 12-24 months with controls/mitigation in full effect and working as intended.
- Inherent/Residual** When Inherent Severity and Residual Severity have the same value.

Risk Severity

Severity Score	Severity Identifier	Financial Impact	Brand/Reputation	Regulator Intervention	Strategic Risk
5	Very High	Impact is greater than 6.8% of capital (Midpoint 10%)	Sustained, widespread, and substantiated national negative media or industry coverage. <u>In order to</u> recover our reputation significant resources and extreme actions are required.	One or more regulators impose material financial penalties, revoke or threaten to revoke our license to operate or insist on prolonged on site and/or continuous monitoring.	Disruptive innovation that markedly transforms insurance value chain.
4	High	Impact is greater than 3.2% to 6.8% of capital (Midpoint 5%)	Substantiated national negative media or industry coverage which requires effort and action to recover our reputation.	One or more regulators impose significant financial penalties or active monitoring and/or an extensive correction plan.	Significant changes required to business / operating model across insurance value chain.
3	Moderate	Impact is greater than 0.8% to 3.2% of capital (Midpoint 2%)	Substantiated negative media or industry coverage in a region, which requires moderate effort or action to recover our reputation.	One or more regulators impose a moderate financial penalty and/or a moderate corrective action plan.	Moderate changes required to business / operating model across insurance value chain.
2	Low	Impact is greater than 0.2% to 0.8% of capital (Midpoint 0.5%)	Substantiated localized negative impact on reputation, which is recoverable with very minor or no effort.	Expected regulatory inquiry requiring a response, but unlikely to result in a financial penalty and/or a difficult corrective action plan.	Minor changes required to business / operating model for certain elements of insurance value chain.
1	Very Low	Impact is less than 0.2% of capital (Midpoint 0.1%)	No meaningful reputational or brand exposure.	No expected regulatory inquiry.	Business as usual, no operating model changes required.

Risk Owner Comment:

ERM MC Demo Annual Risk Survey

- Inherent Likelihood** Inherent Likelihood that a significant risk event (Inherent Severity = 3 & up) will occur from this risk source over the next 12-24 months assuming no controls are in place or controls do not work.
- Residual Likelihood** Residual Likelihood that a significant risk event (Inherent Severity = 3 & up) will occur from this risk source over the next 12-24 months with controls/mitigation in full effect and working as intended.
- Inherent/Residual** When Inherent Likelihood and Residual Likelihood have the same value.

Risk Likelihood

Likelihood Rating	Likelihood Identifier	Full Description
5	Almost Certain	Significant event is expected to occur (once every year).
4	Likely	Significant event will probably occur over the stated time frame (once every 5 years).
3	Possible	Significant event might occur under specific conditions (once every 10 years).
2	Unlikely	Significant event could occur at some time but is not probable (once every 25 years).
1	Rare	Significant event is very unlikely to occur (once every 50 years).

Risk Owner Comment:

ERM MC Demo Annual Risk Survey

Risk Direction and Velocity

Risk Direction

Direction Rating	Direction Identifier	Full Description
3	Increasing	Likelihood of a significant residual (after controls) event is increasing
2	Stable	Likelihood of a significant residual (after controls) event is stable
1	Decreasing	Likelihood of a significant residual (after controls) event is decreasing.

Risk Owner Comment:

Risk Velocity

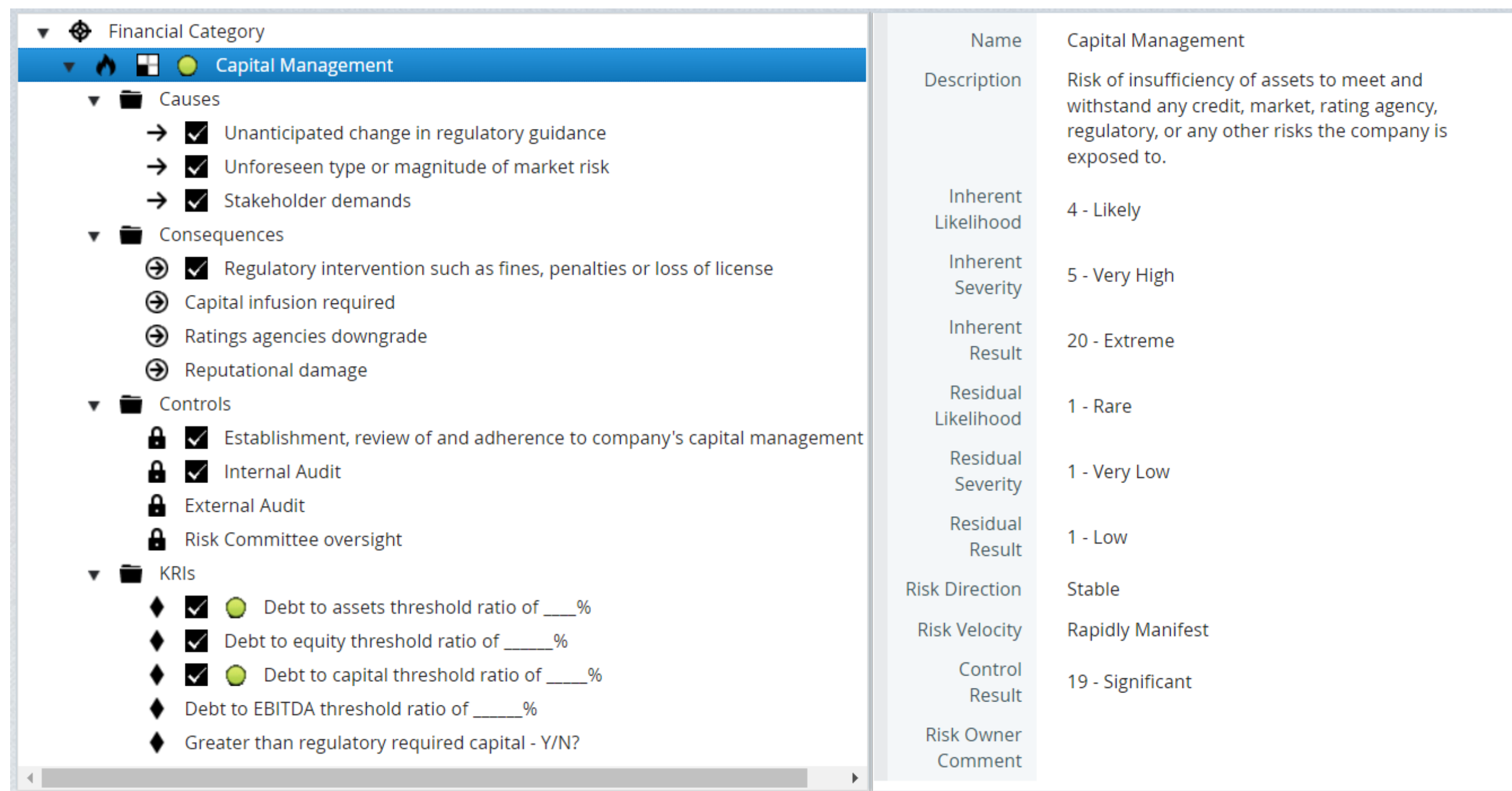
Velocity Rating	Velocity Identifier	Full Description
3	Rapidly Manifest (e.g., a natural catastrophe)	A significant risk event from this risk source would manifest itself very quickly
2	Steadily Emerge (e.g., the 2007-2008 credit crisis)	A significant risk event from this risk source would likely emerge on a steady basis, over time
1	Slowly Emerge (e.g., regulation such as Sarbanes Oxley)	If a significant risk event from this risk source were to occur, it would emerge slowly

Risk Owner Comment:

ERM Risk Content Data View

-Displays hierarchy of data within the system

Figure 4 (expanded view)



The screenshot displays the 'Financial Category' section, expanded to show 'Capital Management'. The left pane shows a hierarchical tree view with the following structure:

- Financial Category
 - Capital Management
 - Causes
 - Unanticipated change in regulatory guidance
 - Unforeseen type or magnitude of market risk
 - Stakeholder demands
 - Consequences
 - Regulatory intervention such as fines, penalties or loss of license
 - Capital infusion required
 - Ratings agencies downgrade
 - Reputational damage
 - Controls
 - Establishment, review of and adherence to company's capital management
 - Internal Audit
 - External Audit
 - Risk Committee oversight
 - KRIs
 - Debt to assets threshold ratio of ___%
 - Debt to equity threshold ratio of ___%
 - Debt to capital threshold ratio of ___%
 - Debt to EBITDA threshold ratio of ___%
 - Greater than regulatory required capital - Y/N?

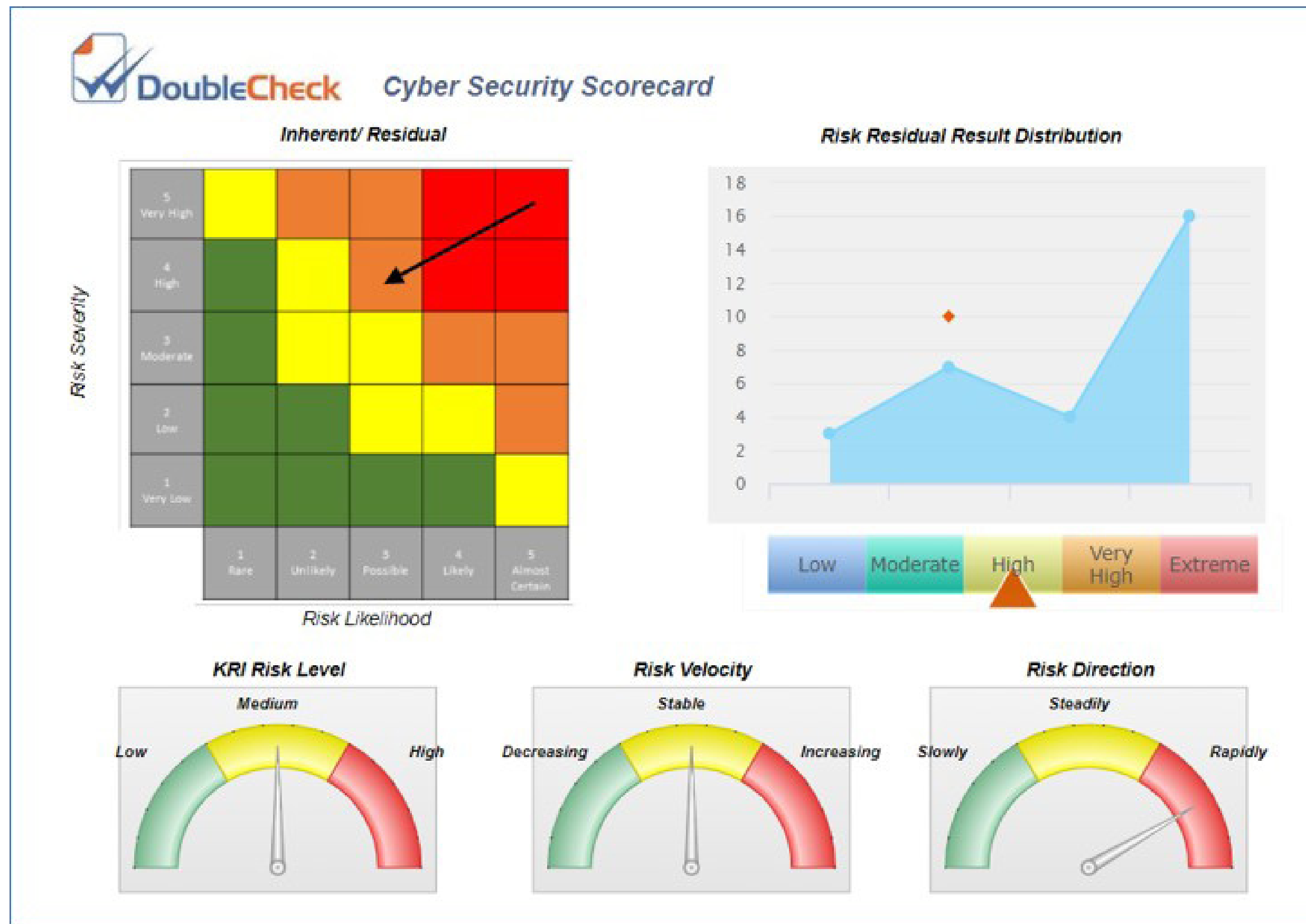
The right pane provides detailed information for the selected 'Capital Management' risk:

Name	Capital Management
Description	Risk of insufficiency of assets to meet and withstand any credit, market, rating agency, regulatory, or any other risks the company is exposed to.
Inherent Likelihood	4 - Likely
Inherent Severity	5 - Very High
Inherent Result	20 - Extreme
Residual Likelihood	1 - Rare
Residual Severity	1 - Very Low
Residual Result	1 - Low
Risk Direction	Stable
Risk Velocity	Rapidly Manifest
Control Result	19 - Significant
Risk Owner Comment	

Risk Scorecard

-Displays key Risk components such as Inherent vs Residual heatmap, Risk Residual Results Distribution, KRI Risk Level, Risk Velocity and Risk Direction

Figure 5



Additional ERM One™ Resources

To access additional ERM One™ resources:

- Webinar
- Free trial
- Blogs

Please visit: [DoubleCheck ERM One™](#)

THANK YOU!

About the Authors

Michael Cawley

Mike is a risk management executive with a 35 year record of broad and diversified accomplishment in the strategic and tactical elements of corporate enterprise risk management (ERM). He performed day-to-day development and execution of a risk management program that covered all elements in the identification, assessment, mitigation and monitoring of all exposures within the corporate risk universe. Specific experience involved being a corporate risk manager for a service-related conglomerate (15 years) and then a biopharmaceutical manufacturer (10 years) before assuming an ERM governance and disclosure leadership role (10 years, through 2021) for a major worldwide financial entity. Currently, Mike serves as a Subject Matter Expert (SME) in an advisory role for ERM Best Practices for the advancement of DoubleCheck's new ERM One™ application.

Contributors:

Simon Goldstein

Simon Goldstein is an accomplished senior executive blending both technology and business expertise to formulate, impact, and achieve corporate strategies. As a former senior manager of Accenture's IT Security and Risk Management practice, and an experienced change agent, he has led efforts to achieve ISO2700x certification and HIPAA compliance, as well as held credentials of CRISC, CISM, CISA. Simon, an accomplished writer, also provides insightful information and experience on a monthly basis as part of DoubleCheck's published blogs.

Tim Ihde

Tim has over 30 years experience as a senior engineer / project lead designing operating systems and multi-threaded web and server-based applications, at companies such as AT&T Bell Laboratories, UNIX System Labs, Novell, and Hewlett Packard. For the past 15 years he has been the Chief Technology Officer of DoubleCheck Software, leading a team developing distributed Risk Analysis and Management software.

CONTACT INFO



101 Gibraltar Drive, Morris Plains, NJ 07950



sales@doublechecksoftware.com



www.doublechecksoftware.com



1-973-984-2229 OR 1-888-299-3980