DoubleCheck

DoubleCheck Webinar on Enterprise Risk Management (ERM) - Out of Box Risk Register Solution (ERM One™)

The Webinar Will Answer:

What is the Compelling Case for ERM?

Why Does DoubleCheck Believe a New ERM Solution is Needed?

What are the Key Features of that DoubleCheck ERM One™ Solution – an Out-Of-The-Box Risk Register System?

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

The Strategic Importance of ERM

The Tactical Execution of ERM

DoubleCheck

ERM is nothing without Context

Business Profile

What are the entity's core businesses?

Key Strategic Objectives

For example: Performance, Capital, Liquidity, Reputation, etc.

Value Measurement

How is Value measured by company and its stakeholders (e.g. stock price, revenue and cash flow, franchise protection, new products and services)?

Value at Risk

How is value created and/or put at risk, either deliberately or inadvertently?

ERM Mission Statement

The ERM mission statement is defined as "the process to identify, assess, mitigate and monitor all enterprise-wide risks that might impair the company's ability to achieve its strategic business objectives.

The Tactical Execution of ERM (Via Risk Register)

There are three attributes of an ERM solution (Product, Process and Content) that, 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.

Use Cases For A Fully Integrated DoubleCheck ERM One™ Solution

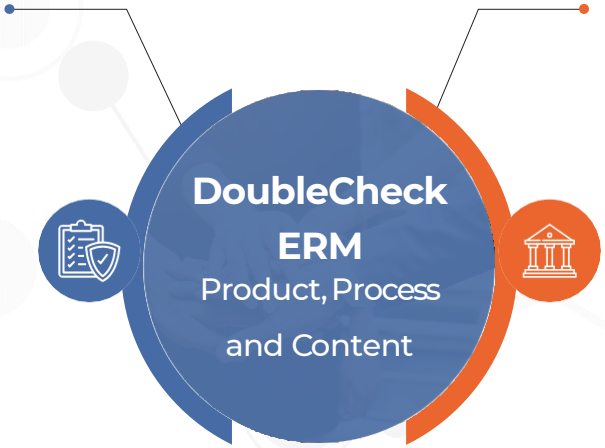
Case 1: No ERM Platform

Challenge:

- Nothing in place for ERM
- Reliant on Excel/PowerPoint/ email/SharePoint
- No organized, integrated ERM environment (Risks, Controls, Risk Register, etc.)

Opportunity/Need:

- Need for fully bundled ERM environment providing Product, Process & Content
- Fast, greenfield implementation
- Embedded Reporting and BI



Case 2: An Embedded ERM Infrastructure... But Ineffective

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

Case 1: No ERM Platform

Challenge:

- Nothing in place for ERM
- Reliant on Excel/Powerpoint/Email/SharePoint
- No organized, integrated ERM environment (Risks, Controls, Risk Register, etc.)

Opportunity/Need:

- Need for fully bundled ERM environment providing Product, Process & Content
- Fast, greenfield implementation
- Embedded Reporting and Business Intelligence tools

Case 2: An Embedded ERM Infrastructure… But Ineffective

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

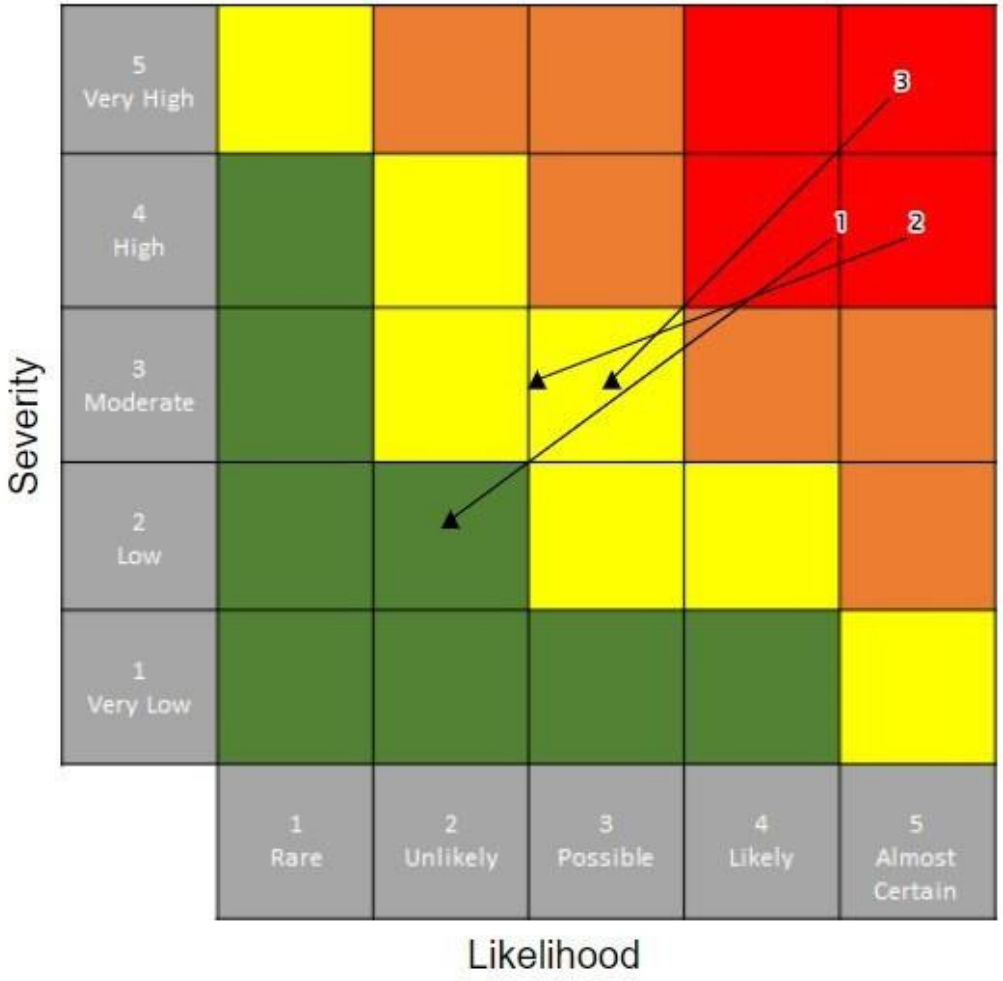
Opportunity/Need

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

..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 weaknesses.

Top 10 Reasons to Choose the DoubleCheck ERM One™ Solution

Risk Arrow Heat Map



#	Risk	Inherent Risk Result	Residual Risk Result
1	*Contractual Disputes*	20 - Extreme	4 - Low
2	*Data Breaches and Digital Theft*	20 - Extreme	9 - Moderate
3	*Supply Chain Disruption*	25 - Extreme	9 - Moderate

Comprehensive Risk Report

Risk Survey Report

Organization: North America

Operational Category Risk: Cyber Security

Risk Owner: Abe Forhman

Comprehensive Risk Report - Page 1

Organization: North America **Category :** Operational Category **Risk :** Cyber Security

ERM MC Demo Annual Risk Survey

Risk Description, Causes, and Consequences of Risk

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, internal or external information security threats.

Causes of Risk

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

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

Comprehensive Risk Report - Page 2

Organization: North America **Category :** Operational Category **Risk :** Cyber Security

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

Comprehensive Risk Report - Page 3

Organization: North America **Category:** Operational Category **Risk:** Cyber Security

ERM MC Demo Comprehensive Risk Report

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. In order to 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:

Comprehensive Risk Report - Page 4

Organization: North America **Category :** Operational Category **Risk :** Cyber Security

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:

Comprehensive Risk Report - Page 5

Organization: Testing **Category:** Operational Category **Risk:** Cyber Security

ERM MC Demo Comprehensive Risk Report

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

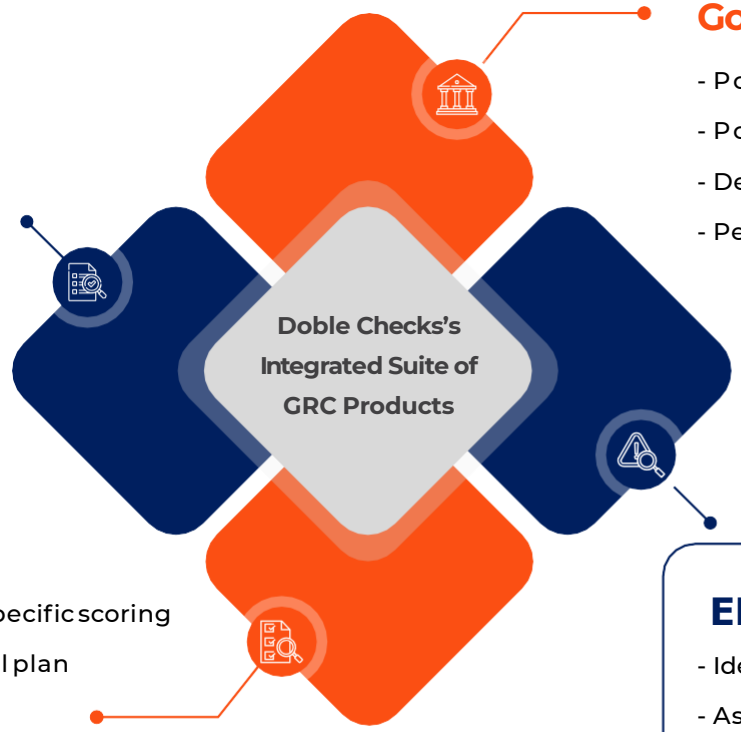
Velocity Rating	Velocity Identifier	Full Description
3	Rapidly Manifest (e.g., a natural catastrophe)	A significant risk event from this risk source would manifest itself very quickly
2	Steadily Emerge (e.g., the 2007-2008 credit crisis)	A significant risk event from this risk source would likely emerge 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:

Double Check's Integrated Suite of GRC Products

Compliance

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



Governance

- Policy Definition
- Policy Renewal
- Demonstrable
- Performance

Audit

- Program definition based on client specific scoring
- Management review, overrides to final plan
- Engagement Planning
- Electronic Workpaper Management
- Issues & Remediation Management

ERM

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

DoubleCheck

DoubleCheck ERM Webinar Summary

- **Background:** DoubleCheck is a prominent Governance, Risk, Compliance (GRC) solutions provider, one who knows the ERM space well
- **Belief:** DoubleCheck supports the fact that ERM is a vital discipline, one that is integrally connected to the achievement of a company's corporate objectives
- **Challenge/Opportunity:** DoubleCheck sees considerable ERM underutilization, ranging from companies with no ERM structure in place at all to companies who are saddled with an ERM system that is inflexible/inefficient

- **Response:** To seize upon that opportunity, DoubleCheck has proactively designed an innovative, turnkey ERM solution (ERM One™) with:
  - risk structure pre-configuration
  - risk content pre-population
  - risk process integration
  - modular construction, capable of significant functional enhancement
  - embedded reporting and robust business intelligence (BI)
  - navigation through visualization
  - alignment to ERM standards and best practices

Additional ERM One™ Resources

To access additional ERM One™ resources:

- White Paper
- Free trial
- Blogs

Please visit:

DoubleCheck ERM One™ webpage

THANK YOU!