# ERM Practices, Risk Quantification and Risk Maturity

**FEI NE Wisconsin Chapter Meeting**
**April 18, 2018**

**Prepared by Aon Risk Solutions**
Global Risk Consulting | Risk Advisory Services

Empower Results®

# Enterprise Risk Management Defined

Empower Results®

# Defining Enterprise Risk Management

- The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value. – *COSO ERM Framework, September 2017*
- The discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders. – *Casualty Actuary Society*

## Enterprise Risk Management (ERM)

# Global factors driving improvements in risk management approaches

# Aon's Enterprise Risk Management Cycle


**Framework Design**
- Assessing an organization's ERM capabilities
- Leverage the Aon Risk Maturity Index
- Design a path to high risk maturity

**Framework Implementation**
- Strategic implementation of an ERM framework
- Develop a sustainable program to help the business meet objectives and strategic goals

**Risk Identification**
- Create an enterprise risk register
- Utilize surveys, interviews and workshops to elicit subject matter expertise and judgement

**Risk Assessment and Quantification**
- Prioritize and rank the organization's risks
- Develop quantitative risk estimates where data is available

**Risk Mitigation**
- Implement additional controls, targeted at the organization's top risks
- Develop plans to mitigate or accept risks

**Risk Reporting**
- Develop risk reports for management and the board that guide and inform strategic planning

# Critical Risk Management Questions

## Risk Awareness

- What are the key risks?
- What is the potential impact of these key risks?
- Which of business lines brings the most risk to the overall profile?
- Has the organization quantified any of its key risks? Which?
- How is risk information communicated to the Board and other key parties?
- How is the organization's risk profile changing?

## Risk Improvement

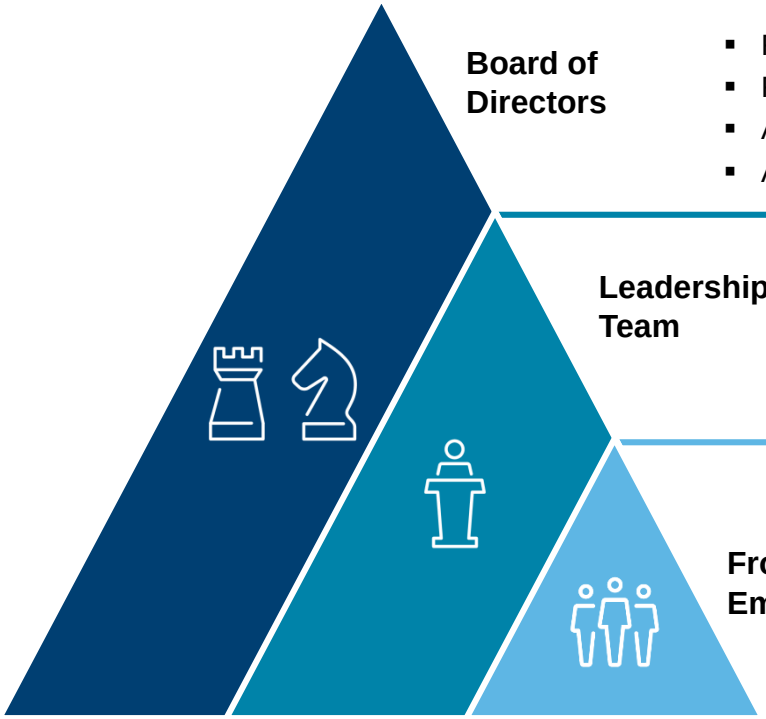
- What activities are in place to manage the key risks?
- Does the organization have the capabilities to execute this risk response strategy?
- What key metrics are used to monitor current risk exposure levels?
- Who is responsible for monitoring the completion of action plans?
- Did the mitigation activity yield the appropriate level of benefit for the cost?

## Risk Governance

- What is the organization's risk appetite?
- Is there a Risk Committee?
- Do employees understand their risk management roles?
- Where is the risk management department located in the organization?
- How does management incorporate risk into its strategy development?
- Is the organization taking an appropriate amount of risk?

# Providing risk information to key decision makers

A mature ERM program supports decision making by integrating effective risk identification and assessment approaches into existing governance structures and management processes



**Board of Directors**

- Reviews and confirms risk management policy and objectives
- Reviews and confirms organization's risk profile and risk appetite
- Aligns risk governance with overall strategy and shareholder expectations
- Accepts ultimate responsibility for overseeing risk governance

**Leadership Team**

- Develops risk appetite consistent with operating plans, metrics
- Determines risk management responsibilities
- Allocates resources and monitors risk management performance
- Discloses key risks and risk management performance

**Frontline Employees**

- Oversees risk management implementation
- Confirms risk management results
- Identifies and implements best practices
- Provides internal oversight, expertise and training

***Effective ERM programs will fit within organizational culture and management priorities***

# Additional considerations when designing an ERM framework

**Understand that organizations seek different levels of ERM sophistication**

- There are no off-the-shelf solutions. Every implementation strategy is different, and must support the organization's ERM goals and objectives

**Recognize that ERM is an investment**

- Establish clear expectations
- Understand the costs in terms of time and resources

**Understand and overcome typical ERM implementation challenges**

- Perception of ERM as "bolt-on, bureaucratic process" that is not needed as "risk is managed"
- Unclear ownership or lack of champion to lead the effort
- Management attention may be focused on more immediate / critical issues

**Leverage existing strengths and integrate ERM into existing and accepted management decision processes and structures**

- ERM program must build upon existing strengths while closing identified gaps
- ERM activities must fit within the organizational culture

# Global Risk Management Survey Insights

Empower Results®

# 2017 Global Risk Management Survey Risk Ranking

## The majority of risks that organizations face are not fully insurable

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 Damage to reputation/brand | 2 Economic slowdown/slow recovery | 3 Increasing competition | 4 Regulatory/ legislative changes | 5 Cyber crime/ hacking/viruses/ malicious codes | 6 Failure to innovate/meet customer needs | 7 Failure to attract or retain top talent | 8 Business interruption |
| 9 Political risk/ uncertainties | 10 Third party liability | 11 Commodity price risk | 12 Cash flow/ liquidity risk | 13 Property damage | 14 Directors & Officers personal liability | 15 Major project failure | 16 Exchange rate fluctuation |
| 17 Corporate social responsibility/ sustainability | 18 Technology failure/ system failure | 19 Distribution or supply chain failure | 20 Disruptive technologies/ innovation | 21 Capital availability/credit risk | 22 Counter party credit risk | 23 Growing burden and consequences of corporate governance/ compliance | 24 Weather/natural disasters |
| 25 Failure to implement or communicate strategy | 26 Merger/acquisition/ restructuring | 27 Injury to workers | 28 Failure of disaster recovery plan/ business continuity plan | 29 Loss of intellectual property/data | 30 Workforce shortage | 31 Environmental risk | 32 Crime/theft/fraud/ employee dishonesty |
| 33 Lack of technology infrastructure to support business needs | 34 Inadequate succession planning | 35 Product recall | 36 Concentration Risk ( product, people, geography) | 37 Aging workforce and related health issues | 38 Accelerated rates of change in market factors and geopolitical risk environment | 39 Interest rate fluctuation | 40 Globalization/ emerging markets |
| 41 Unethical behavior | 42 Outsourcing | 43 Resource allocation | 44 Terrorism/ sabotage | 45 Climate change | 46 Asset value volatility | 47 Natural resource scarcity/ availability of raw materials | 48 Absenteeism |
| 49 Social media | 50 Sovereign debt | 51 Pandemic risk/ health crises | 52 Share price volatility | 53 Pension scheme funding | 54 Harassment/ discrimination | 55 Kidnap and ransom/ extortion | |

Insurable | Partially Insurable | Uninsurable

# Cyber risk continues to rise in importance

- Increased from #9 in 2015 to #5 in 2017, and ranks #1 across many organizations in North America
- Research by the Ponemon Institute supports the increase
  - Reported cyber incidents increased 64% from 2014 to 2015
  - Annual average cost of a cyber incident increased 24% from 2015 to 2016, up to $9.5 million
  - Phishing and social engineering attacks increased from 62% in 2015 to 70% in 2016
- The Government Accountability Office surveyed 24 federal agencies and found that between 2006 and 2015, the number of cyber attacks has climbed 1,300% - from 5,500 to 77,000 attacks per year
- Since 2005, higher education institutions in the US have been the victim of 539 breaches involving nearly 13 million student records
- Significant increase in demand for cyber insurance, with annual growth ranging from 30% to 50%
- Cyber attacks can destroy intellectual property, cause widespread property damage, and tarnish brand and reputation
- Cyber risks assessments should consider an organization's goals, technology, and vulnerable data as a starting point to identify associated risk and advise on the best mitigation strategy

# Stroz Friedberg's makes six predictions for Cyber

- Criminals harness IoT devices as botnets to attack infrastructure
- Nation state cyber espionage and information war influences global and political policy
- Data integrity attacks rise
- Spear-phishing and social engineering tactics become craftier, more targeted, and more advanced
- Regulatory pressures make red teaming the global gold standard with cyber security talent development recognized as a key challenge
- Industry first-movers embrace pre-M&A cyber security due diligence

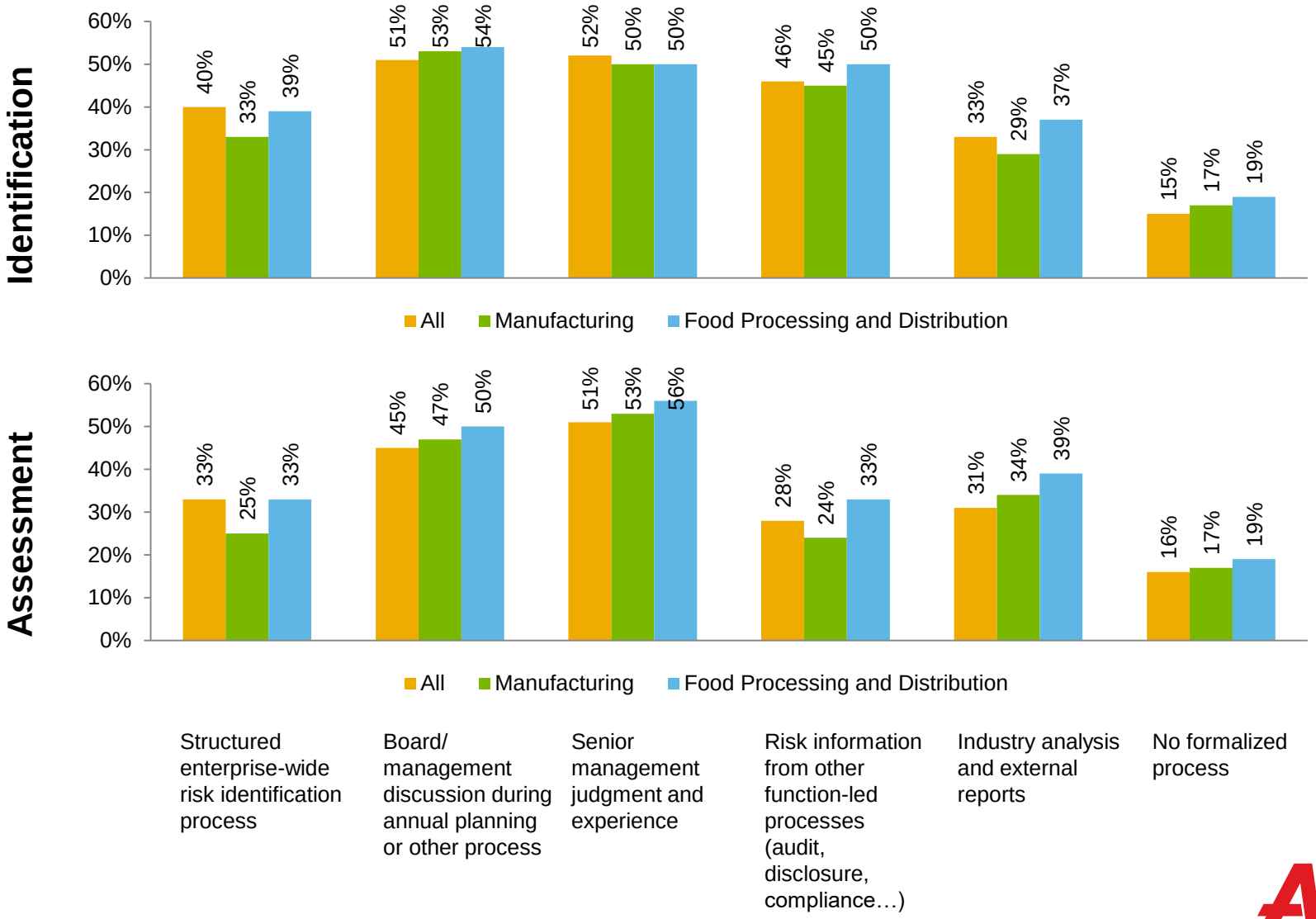
# Damage to brand and reputation remains a key concern

- Remained in the top three and #1 for many organizations despite being predicted to decline by respondents in 2015
- Brand and reputation damage can arise from several factors, including
  - Cyber crime
  - Defective products and services
  - Customer service issues
  - Fraudulent business practices
  - Corruption
  - Social media
  - Political crossfire
- Events can lead to challenges in cash flow and in attracting and retaining top talent
- Taking a close look at all risks that could damage an organization's brand allows for identification of vulnerabilities and focus on key areas of exposure

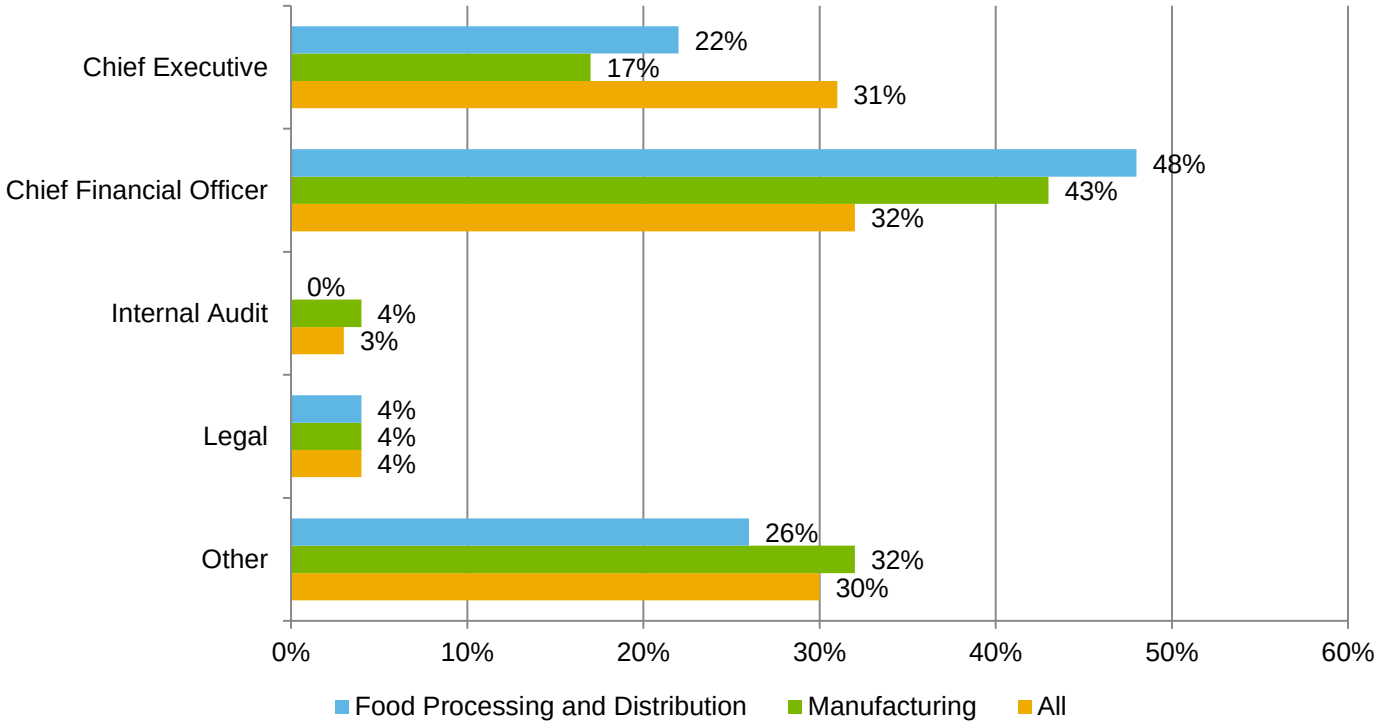
# Political risk/uncertainties has re-entered the top 10

- Increased from #15 in 2015 to #9
- Reported risk readiness declined from 39% in 2015 to 27% in 2017
- Several geopolitical events over the last two years will likely have significant economic and social implications locally and globally
  - Brexit
  - Multiple elections
  - Political scandals
  - Rise of populism and trade protectionism
- Organizations need to consistently assess their political and security risks for all jurisdictions in which they operate to make informed decisions and protect operations and investments.

# Primary methods used to *identify* and *assess* major risks



# Who has responsibility for the risk management function?



# Establishment of policies on risk oversight and risk management

Has the Board of Directors or a Board Committee established policies on risk oversight and management?

| | All | Manufacturing | Food Processing and Distribution |
|---|---|---|---|
| Yes, formally | 43% | 37% | 43% |
| Partially / informally | 33% | 18% | 13% |
| No | 17% | 40% | 37% |
| Don't know | 7% | 6% | 7% |

Does the program have cross-functional input on key risks?

| | All | Manufacturing | Food Processing and Distribution |
|---|---|---|---|
| Yes | 71% | 68% | 83% |
| No | 29% | 32% | 17% |

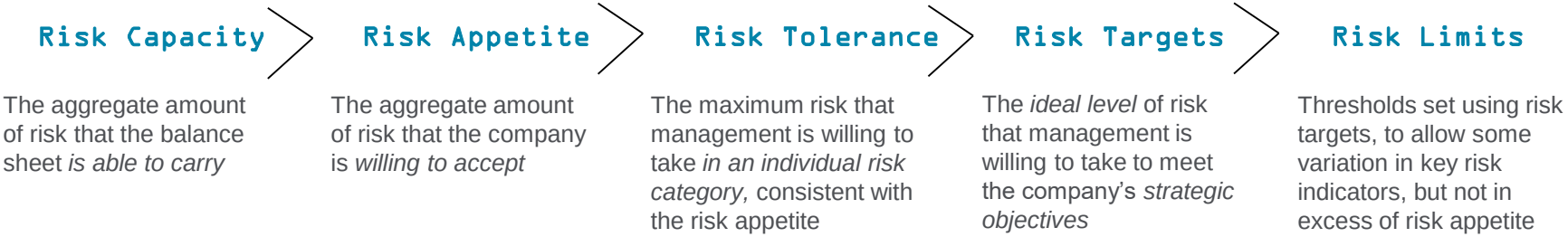
# Risk Quantification

Empower Results®

# Developing Risk Quantification

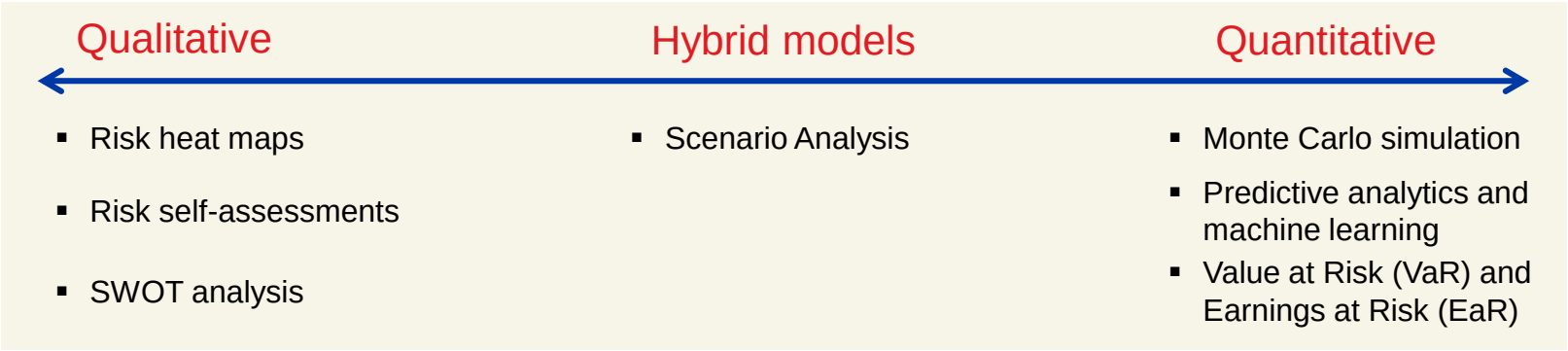
## A Consistent Approach to Understanding Risk

- In our experience, embedding risk analytics and risk quantification into an ERM program is critical to effectively answering the following key questions for the Board and Senior Management:
  - ✓ Are we focused on the risks most likely to impact our strategy?
  - ✓ Are we accepting the right level of risk?
  - ✓ How are our controls performing?
- To answer these questions, organizations make use of a range of qualitative methods and quantitative modeling techniques to better understand their risk exposure, and define the following concepts:



# Developing Risk Quantification

## Common Methods for Risk Quantification




- There are many different methods and models used to quantify risk and risk exposures. The table above presents some of the most commonly used, on a spectrum of qualitative through to quantitative.
- Importantly, there are advantages and disadvantages to each end of the spectrum:
  - *Qualitative methods* rely on the knowledge of subject matter experts, and can be used where no historical data exists. However, these approaches are often require significant time investments across the company
  - *Quantitative methods* are often more *predictive* than qualitative methods, and can be updated more quickly, but they rely on significant quantities of historical data, as well as understanding of the underlying models
- Aon works with clients to quantify their risks using the range of techniques shown above.

# Aon's Risk Quantification Capabilities

## Example 1: Business Impact Study

**Client Need**

- Aon was engaged by a large supermarket chain to support the risk, technology, and insurance teams to assess a range of business risks, evaluate performance, and model the potential financial loss exposure for the purpose of informing decision making on investment in risk mitigation and transfer (insurance).

**Client Objectives**

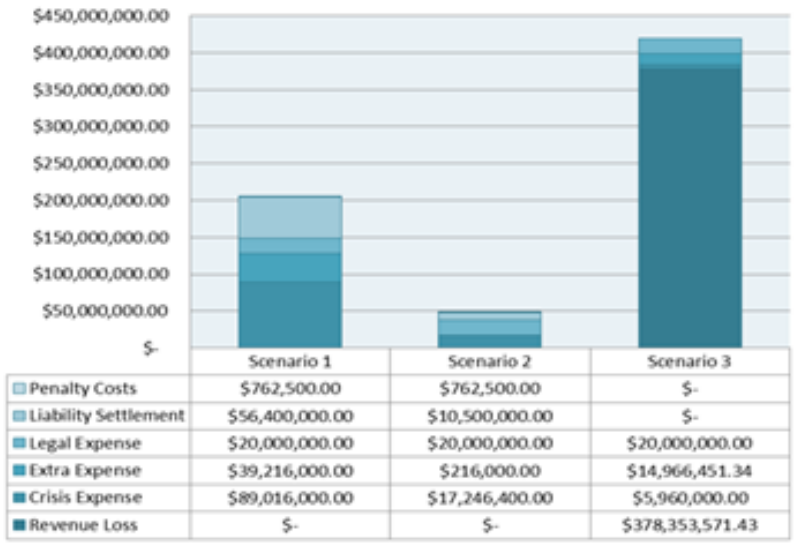
- Achieve a thorough understanding of the business risks and efficiency of controls
- Evaluate the financial exposures from the identified risks
- Ensure adequate board oversight of risks facing the business
- Provide meaningful input toward the business strategy
- Define an effective risk transfer strategies with the objective of protecting shareholder value
- Provide the basis for an effective insurance market submission to obtain sufficient market capability

**Solution**

- Aon performed a business risk assessment with key Security, Technology, And Commercial teams to prioritize business risks for the financial analysis and identify key security vulnerabilities
- Aon generated an appropriate financial model to determine the monetary impact of each identified risk scenario in both 'Estimated Maximum Loss' (EML) and 'Probable Maximum Loss' (PML) terms

# Aon's Risk Quantification Capabilities

## Example 1: Business Impact Study

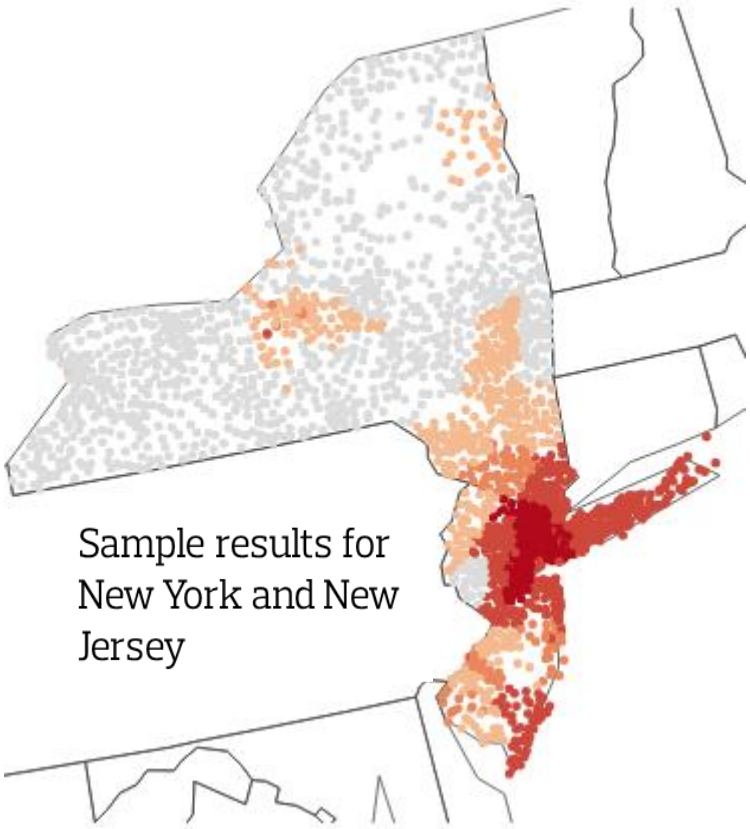




| | Scenario 1 | Scenario 2 | Scenario 3 |
|---|---|---|---|
| Penalty Costs | $762,500.00 | $762,500.00 | $- |
| Liability Settlement | $56,400,000.00 | $10,500,000.00 | $- |
| Legal Expense | $20,000,000.00 | $20,000,000.00 | $20,000,000.00 |
| Extra Expense | $39,216,000.00 | $216,000.00 | $14,966,451.34 |
| Crisis Expense | $89,016,000.00 | $17,246,400.00 | $5,960,000.00 |
| Revenue Loss | $- | $- | $378,353,571.43 |

# Aon's Risk Quantification Capabilities

## Example 2: Predictive Analytics Case Study

- Aon designed a pre-loss general liability model to identify high loss potential zip-codes for a retailer expanding its global footprint
- The model used claim costs for ~1,500 zip-codes and demographic information, such as
  - Population density
  - Household size
  - Average income
  - Local unemployment rates
  - Ambulance costs
  - Heart failure rates
- Using this information, the model estimated a "score" (like a FICO score) for every zip-code in the US, and used these scores to assign each zip-codes to a different cost category.
- Validation testing on independent data indicated that
  - The top two cost categories cover 13% of zip-codes, with expected costs 2x to 3x the national average
  - High cost categories are located in both large city centers and lower population areas throughout the US
- Similar modeling could be performed for other business metrics, such as store turnover or revenue, where appropriate data is available.



# Risk Maturity

Empower Results®

# Aligning risk and value with the Aon Risk Maturity Index


- **Purpose:** Innovative tool for organizations to assess risk management capabilities; provides immediate feedback in the form of a rating and comments for improvement
- **Audience:** Senior risk and finance leaders of organizations across every industry with annual revenues in excess of $250MM USD
- **Assessment Focus:** Corporate governance, management decision processes and risk management practices; 125 questions organized into 40 components that align with 10 characteristics of risk maturity
- **Insights:** Research partnership with The Wharton School will drive insights on the relationship between risk management and performance

Risk Maturity Is Associated With Value

- Researchers at the Wharton School at the University of Pennsylvania and the Aon Centre for Innovation and Analytics have identified strong relationships between an organization's Risk Maturity Rating and its performance
- Organizations with higher risk maturity enjoy
  - ***Stronger*** stock price performance
  - ***Reduced*** stock price volatility over time
  - ***Stronger*** return on equity performance
- Research findings also evidence a direct relationship between risk maturity levels and the relative resilience of an organization's stock price in response to significant events in the financial markets

# Risk Maturity is a measure of the robustness, sophistication, and resilience of an organization's enterprise risk management framework


The set of policies and organizing structures in place that guide and support a risk management process across the organization:

- Organizational structure, including roles and responsibilities
- Risk appetite and tolerance statements
- Policies and procedures for risk management and key activities

The methodology, tools and techniques an organization uses to identify, analyze, measure, manage and monitor its key risks:

- Risk assessment and prioritization exercises
- Defined key risk and performance indicators
- Qualitative and quantitative risk analysis approaches

The approach and tools used to include risk, risk management and risk-return information into management decision processes:

- Budgeting and forecasting techniques
- Cooperation among compliance, internal audit, risk management
- Influence of risk sensitivity on financing, business decisions

The practices utilized internally and externally to raise awareness and enhance understanding of risk and risk management:

- Disclosures and regulatory filings
- Board/management reporting frameworks and templates
- Benchmarking

**Evaluation Framework**

Each framework component is rated using Aon's ERM evaluation criteria prior to calculation of clients' overall ERM rating

Components and the overall ERM framework are assigned one of the following ratings:

- Advanced
- Operational
- Defined
- Basic
- Lacking/Initial

# 10 Characteristics of Advanced Risk Maturity

| | |
|---|---|
| 1 | ***Board-level understanding of and commitment*** **to risk management as a critical factor for decision making and for driving value** |
| 2 | A ***senior-level executive*** who drives and facilitates key risk management processes and development |
| 3 | ***Transparency*** of risk communication |
| 4 | A risk ***culture that encourages full engagement and accountability*** at all levels of the organization |
| 5 | ***Identification of existing and emerging risks*** using internal and external data and information |
| 6 | ***Participation of key stakeholders*** in risk management strategy development and policy setting |
| 7 | Formal collection and incorporation of operational and financial ***risk information into decision making and governance processes*** |
| 8 | ***Integration of risk management insights into human capital processes*** to drive sustainable business performance |
| 9 | Use of ***sophisticated quantification methods*** to understand risk and demonstrate added value through risk management |
| 10 | A move from focusing on risk avoidance and mitigation to ***leveraging risk and risk management options that extract value*** |

# Aon Risk Maturity Index

## Levels of Maturity


The organization has a well developed ability to identify, measure, manage and monitor risks. Risk management processes are dynamic and adapt to changing risks and business cycles:

- ✓ A formal statement of risk appetite is in place and guides decision making
- ✓ Risk information is explicitly considered in decision-making processes
- ✓ Analytics are consistently applied, and incorporate qualitative and quantitative techniques
- ✓ Risk management provides a competitive advantage, with a focus on optimizing business performance


There is a clear understanding of the organization's key risks and also a consistent execution of activities to address these risks; some functional areas may employ more sophisticated techniques

- ✓ The set of loss and tolerance guidelines are predetermined or developing
- ✓ Explicit consideration of risk and risk management information is taken in key decisions
- ✓ Analysis is consistently applied, incorporating both qualitative and quantitative techniques


The organization understands and is addressing its key risks; capabilities to measure, manage and monitor risks are in place but may be inconsistent across the organization

- ✓ Guidelines for loss and risk tolerance are less developed
- ✓ Risk and risk management information is considered informally / implicitly in decision making
- ✓ Analysis is consistently applied, with a focus on qualitative approaches


There is inconsistent understanding, management and monitoring of key risks across the organization; capabilities to consistently identify, assess, manage and monitor risks are limited

- ✓ Risk management activities occur at the functional level rather than the enterprise level
- ✓ Risk management activities emphasize compliance
- ✓ Risk and risk management information is considered informally or implicitly in decision making, often on an ad hoc basis


The organization identifies and addresses risks within silos only. Components and activities of the risk management process are limited in scope and are implemented in an ad-hoc manner.

# What You Receive for Participating

Risk Maturity Rating

According to your answers, your organization is at a **(2) Basic Level** of Risk Maturity. In Aon's experience, organizations at similar levels of Risk Maturity have found value in the following activities to develop their risk management capabilities:


The chart above displays the distribution of Risk Maturity Ratings globally and reflects responses from risk and finance leaders from more than 260 organizations.

Click here for information on Risk Maturity Ratings

Click here for information on the 10 Characteristics of Advanced Risk Maturity

**Activities to Enhance Risk Maturity:**

Developing awareness of risk and risk management at executive and Board levels through educational presentations on specific topics (e.g., risk appetite and tolerance, risk reporting, etc.)

Appointing a risk management leader, executive champion and committee to lead development of the organization's risk management framework

Developing enterprise-level risk assessment tools with appropriate detail regarding risk drivers, risk tolerances and risk management practices

Expanding understanding of the human capital drivers of risk

Reviewing existing governance structures to ensure appropriate documentation and assignment of risk management and oversight

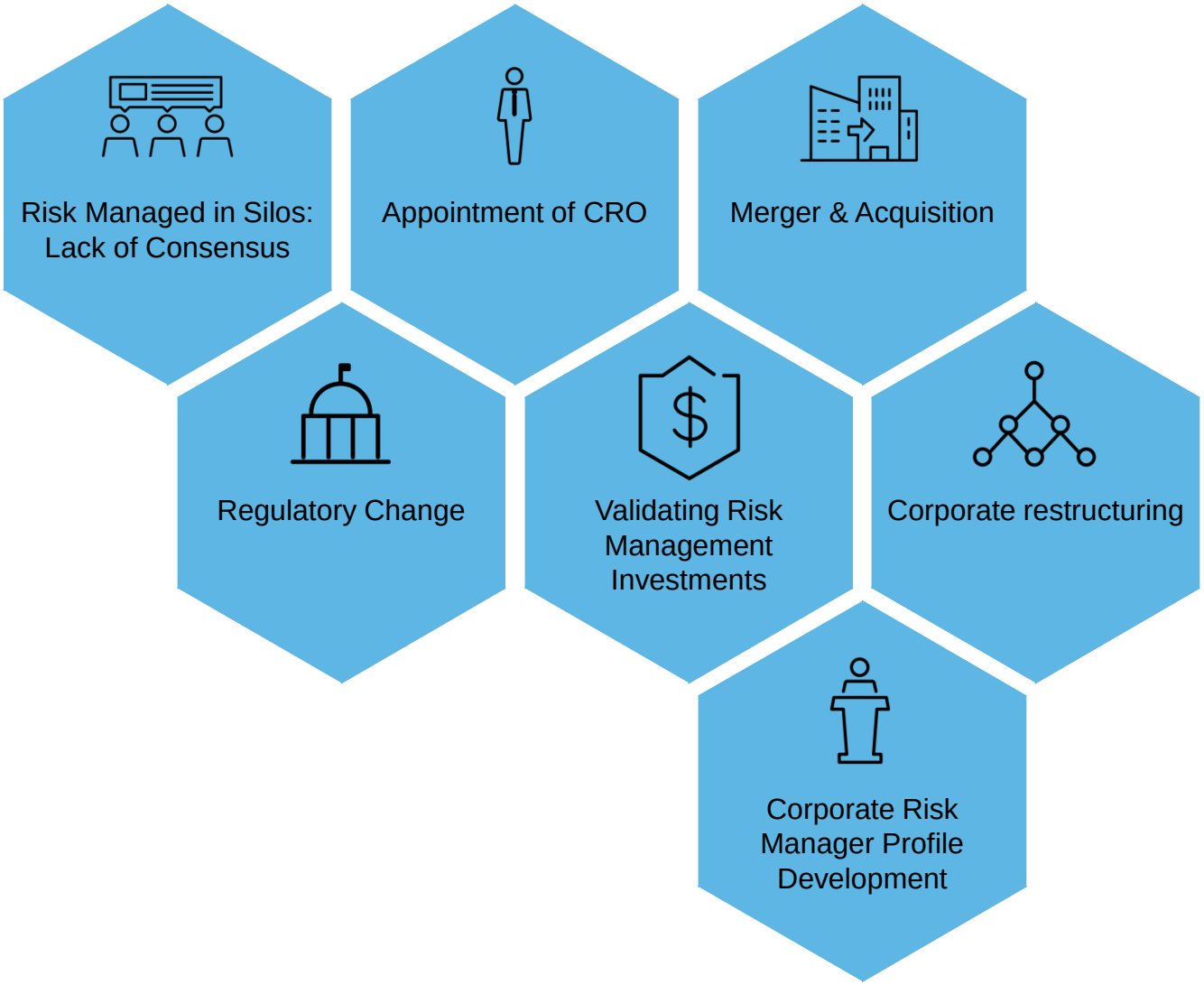
Confirming executive and Board-level risk reporting requirements and expectations

*Disclaimer:*
*Results reflect participant's self-assessment of organizational activities and capabilities using the Aon Risk Maturity Index. It does not represent an evaluation performed by Aon or Wharton School.*

Insight Into Risk Maturity Ratings Globally

Comments for Improving Rating

# Triggers to re-examine an organization's risk maturity



# Risk Maturity Case Study

Empower Results®

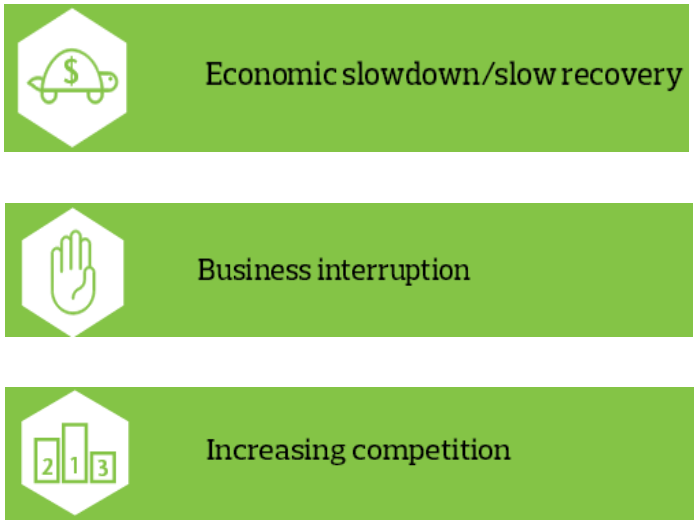
# Case Study: Industrials

The newly appointed Chief Risk Officer (CRO) of an American industrials company sought to evaluate existing risk management capabilities and develop a strategic path forward to align risk and business practices.

Developing Manufacturing Solutions for:

- Construction
- Infrastructure
- Mining
- Manufacturing
- Energy
- Utilities

Self identified significant risk factors

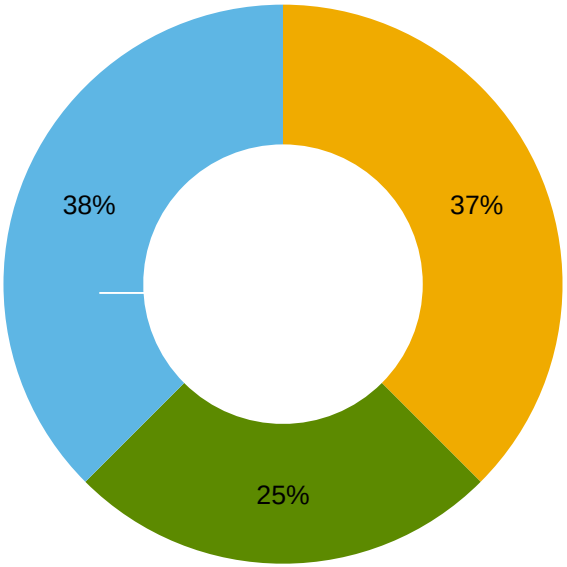


# Case Study: Industrials

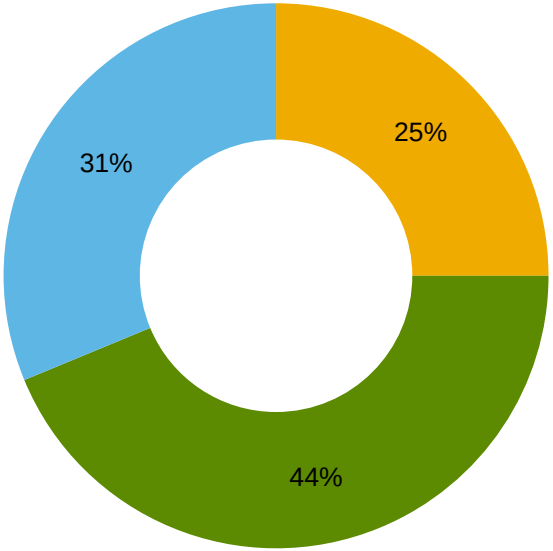
| | |
|---|---|
| **EH&S** | 1.5 Initial to Basic |
| **Executive Leadership** | 2.5 Basic to Defined |
| **Finance** | 2.5 Basic to Defined |
| **Human Resources** | 3.5 Defined to Operational |
| **Information Technology** | 1.5 Initial to Basic |
| **Legal & Compliance** | 2.5 Basic to Defined |
| **Risk Management** | 1.5 Initial to Basic |

## Key Divergence of Opinions

**Content of Management Communication (Performance / Strategy)**




**Communication of Risk Assessment Results Between Risk Functions**




- Consistent at an enterprise level
- On an ad-hoc basis / in silos
- Rarely or never / inconsistent

# Case Study: Industrials

Aon conducted a workshop with the executive leadership team and developed a roadmap for ERM implementation:

| | |
|---|---|
| *1. Formalized Risk Team* | Formalized team to identify, assess, and monitor risk issues across the organization as well as define consistent terminology |
| *2. Risk Mapping* | A formalized risk identification and assessment process to capture current and emerging risks from across the business |
| *3. Risk Dashboards* | Mechanism to integrate risks and provide visibility across the organization, as well as reporting to the Board |
| *4. Loss Collection / Reporting* | Leverage loss event collection to analyze events and drive awareness, agreement, and identification of improvement opportunities |

# Resources and Contacts

## Resources

Aon Global Risk Management Survey 2017

http://www.aon.com/2017-global-risk-management-survey/

Aon Risk Maturity Index

http://www.aon.com/rmi/

## Contacts

Derrick Oracki

Director, Risk Advisory Services

t: +1.202.429.8539

derrick.oracki@aon.com