

**Brian Neary**  
**Chief Operational Risk Officer**  
**June 9, 2014**

**OPERATIONAL RISK —  
WHAT IS IT AND HOW CAN YOU MANAGE IT?**



# AGENDA





---



- **Introductions**
- **What is operational risk?**
- **How can you manage operational risk?**
- **Top and emerging operational risks**
- **Conclusions**

# EXAMPLES OF OPERATIONAL RISK FAILURES



|   | Company         | Impact  |
|---|-----------------|---|
|    | JP Morgan Chase | <ul style="list-style-type: none"> <li>• <b>Traders engaged in a hedging strategy causing mark-to-market losses of \$6.2 billion and cut more than \$20 billion off the bank's market value in 2012</b></li> <li>• <b>Regulatory penalties totaled &gt; \$1 billion</b></li> <li>• Inadequate risk culture and governance</li> <li>• Use of inadequately developed and implemented models</li> </ul>  |
|    | Target          | <ul style="list-style-type: none"> <li>• <b>Hackers entered the company systems via vendor access stealing 70 million individual customers data</b></li> <li>• <b>46% drop in net income for 4Q13 and loss of \$4.5 billion market capitalization</b></li> <li>• S&amp;P ratings downgrade and CEO resigns</li> </ul>   |
|   | Credit Agricole | <ul style="list-style-type: none"> <li>• <b>Due to technical problems, &gt;350,000 double payments totaling \$4.6 billion were processed</b></li> <li>• Human error and a programming bug were blamed for the event</li> </ul>  |
|  | Hewlett Packard | <ul style="list-style-type: none"> <li>• Shareholder lawsuit alleging negligence by the executives and directors during an acquisition of UK software company Autonomy Corporation which resulted in <b>an \$8.8 billion write-down</b></li> <li>• <b>HP's stock price fell causing billions of dollars in lost market value</b></li> <li>• It is anticipated that HP will payout \$1 billion in losses depending on the number of shareholders who join the lawsuit</li> </ul> |

# OPERATIONAL RISK—OVERVIEW



- Operational Risk Management (ORM) is a newer focus area and is still evolving within insurance companies; whereas, banks are required by their regulators to manage operational risk
- There is no consistency in the insurance industry for managing or even defining operational risk
- The NAIC ORSA discusses operational risk
  - Section 1: describe the insurer's framework for managing OR
  - Section 2: document operational risk exposure
- NAIC's Capital Adequacy Taskforce is taking steps to develop an RBC specifically for Operational Risk

- ***Basel definition for operational risk is:***  
***“the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”***
  - Process failure = write off of a large software project
  - People failure = claim employee sending payments to family members
  - Systems failure = failure of system to back up a shared drive
  - External events = Super Storm Sandy flooded offices and disrupted power
- Operational risk (OR) differs from other risks and are usually not willingly incurred
  - We get ***no reward from “taking” operational risk***
  - Not easily quantifiable with models (i.e. capital planning)
  - ***Operational risk is inherent throughout all firms. Operational risk cannot be fully eliminated***

# THE HARTFORD'S ORM FRAMEWORK IS BASED ON BASEL 11 PRINCIPLES



## *Eleven Basel Principles*

1. Establish a strong risk management culture
2. Implement a framework fully integrated within the firm's risk management processes
3. BOD should approve and review the framework
4. BOD should approve and review the risk appetite and tolerances
5. Develop a clear and robust governance structure with well-defined roles and responsibilities
6. Identify and assess operational risk in all products, processes, and systems
7. Ensure there is an approval process for all new products
8. Regularly monitor and report on operational risk exposures
9. Maintain a strong control environment
10. Have enterprise-wide business resiliency and continuity plans
11. Provide public disclosure to allow stakeholders to assess operational risk approach

# OPERATIONAL RISK— THE HARTFORD'S CATEGORIES



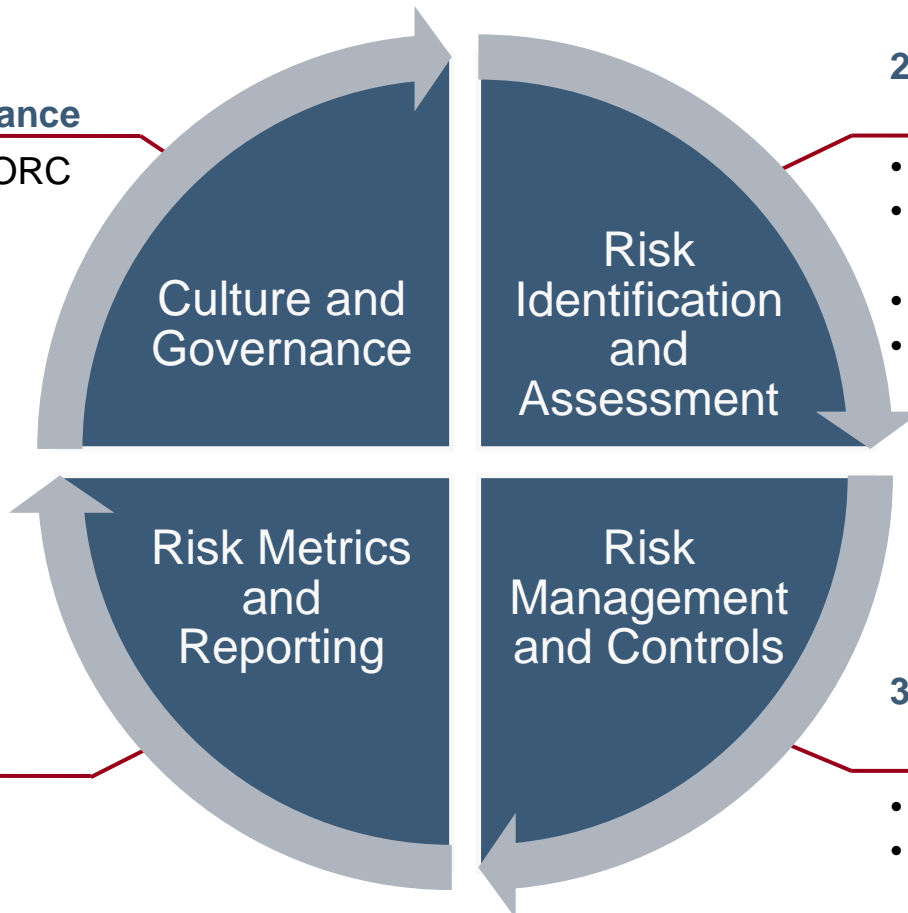
| Operational Risk                        | Definition   |
|---|--|
| Business Resiliency / Disaster Recovery | Inability to recover processes, technology and vendor capabilities in a timely manner                  |
| Compliance / Legal                      | Business is not conducted in compliance with legal regulations   |
| Fraud                                   | Controls do not prevent fraudulent activity  |
| Human Resources                         | Ability to retain key talent and prevent loss of corporate knowledge                                   |
| Information Protection                  | Protection of digital assets and information   |
| Information Technology                  | System stability and recoverability  |
| Process Quality                         | Critical processes not completed in a timely and/or compliant manner (claims, servicing, underwriting) |
| Vendor / Sourcing                       | Vendor over-concentration  |

# OPERATIONAL RISK— THE HARTFORD'S FRAMEWORK



## 1. Culture and Governance

- Committee structure (ORC within risk committee structure)
- Risk governors are assigned to all risk categories
- Policy and standards



## 2. Risk Identification and Assessment

- LOB self-assessments
- Top operational and emerging risk process
- Scenarios
- Risk library

## 4. Risk Metrics and Reporting

- Defined risk appetite and limits
- Dashboard reporting
- Loss aggregation (internal and external data)

## 3. Risk Management and Controls

- Mitigation actions
- Tools/Technology (Archer)
- Three lines of defense



# THE HARTFORD MANAGES RISK USING THREE LINES OF DEFENSE



| First Line of Defense  | Second Line of Defense   | Third Line of Defense  |
|--|--|--|
| Business / Functional Areas  | Risk Governors   | Internal Audit   |
| <ul style="list-style-type: none"> <li>• <b>Own and manage risk</b> within guidelines</li> <li>• <b>Identify, measure, and manage</b> risks</li> <li>• <b>Promote strong ethical culture</b> and risk / return thinking</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Establish risk tolerances, policies, and standards</b> for that specific risk</li> <li>• <b>Monitor limits and exposures</b> across the company</li> <li>• Ensure <b>appropriate resources</b> and focus on top risks</li> <li>• <b>Promote strong ethical culture</b> and risk / return thinking</li> </ul> | <ul style="list-style-type: none"> <li>• Provides <b>independent assurance to the Audit Committee</b></li> <li>• Validates that the 1<sup>st</sup> and 2<sup>nd</sup> lines of defense <b>reasonably mitigate significant risk</b> to the company</li> <li>• <b>Promotes strong ethical culture</b> and continuous improvement in control environment</li> </ul> |
| First Line of Defense Examples   | Second Line of Defense Examples  | Third Line of Defense Examples   |
| <ul style="list-style-type: none"> <li>• Claims Handling</li> <li>• Underwriting</li> <li>• Business Continuity Plans</li> </ul>   | <ul style="list-style-type: none"> <li>• Claims Quality Program</li> <li>• Quality Assurance Team</li> <li>• Business Resiliency Office</li> </ul>   | <ul style="list-style-type: none"> <li>• Audits adherence to controls (First Line)</li> <li>• Assesses control framework (Second Line)</li> </ul>  |

# HOW DO YOUR COMPANIES MANAGE RISK?

---



## Top and Emerging Operational Risks

- What are 2-3 top operational risks at your company?
- How do your top risks compare to the surveys?
- Are there any risks that surprised you in the surveys?
- Are there any risks you identified not included in the surveys?
- Do your companies have a process for identifying and top and emerging operational risks?

# RECENT SURVEYS OF TOP AND EMERGING RISKS



## North American CRO Council

1. **Cyber Attacks**
2. Chronic Fiscal Imbalance
3. **Negative Regulatory Implications**
4. Liquidity Crisis
5. **Terrorist Acts**
6. **Critical System Failure**
7. **Data fraud / Theft**
8. Systemic Financial Failure
9. Unmanageable inflation/deflation
10. **Extreme Weather**

## Allianz

1. **Business interruption**
2. **Natural catastrophes**
3. **Fire, explosion**
4. **Changes in legislation and regulation**
5. Market stagnation or decline
6. **Loss of reputation or brand value (social media)**
7. Intensified competition
8. **Cyber crime, IT failures, espionage**
9. **Theft, fraud, corruption**
10. Quality deficiencies, serial defects

## Protiviti

1. **Regulatory Changes and heightened regulatory scrutiny**
2. Economic Conditions in the Market
3. Political leadership in markets
4. **Succession challenges**
5. **Cyber threats**
6. **Organic growth**
7. **Resistance to change**
8. **Information security**
9. Volatility in global financial markets
10. **Uncertainty with ACA**

## Aon

1. Economic slowdown / slow recovery
2. **Regulatory / legislative changes**
3. Increasing competition
4. **Damage to reputation / brand**
5. **Failure to attract or retain top talent**
6. Failure to innovate / meet customer needs
7. **Business interruption**
8. Commodity price risk
9. Cash flow / liquidity risk
10. Political risk / uncertainties

The operational risks from the surveys are shown in bold/blue

North American CRO Council – *Quarterly Meeting (September 2013) Topic: Emerging Risks* (insurance industry); Allianz – *Risk Barometer on Business Risks 2014* (international corporate insurance); Protiviti – *Executive Perspectives on Top Risk for 2014* (multiple industries to include financial services); and Aon *Global Risk Survey for 2013*










# AN OPERATIONAL RISK THE HARTFORD IS MONITORING—CYBER RISK



Targeted, advanced threats are on the rise across industries

Persistent threats can now include nation state sponsored attacks

Misuse of systems and information places companies at risk

|   | Company                            | Impact   |
|---|------------------------------------|--|
|    | Financial Services Industry        | <b>Distributed Denial of Service (DDoS) attacks on the rise targeting banks and other Financial Services organizations</b> including: BoA, JP Morgan, Wells Fargo, Webster Bank, US Bank and PNC |
|    | Neiman Marcus                      | More than 1.1 million customers were affected in the recent hack of high-end retailer Neiman Marcus, the company has finally revealed.   |
|    | Target                             | On 10 January 2014, Target admitted that 70 million customers had had their personal information stolen  |
|    | Yahoo                              | File of unspecified vintage <b>contained about 400,000 Yahoo and other company users names and passwords</b>   |
|    | Sony Playstation                   | <b>77 million network accounts and millions lost in revenue</b>  |
|    | RSA Security                       | Possibly <b>40 million employee records stolen</b> . EMC has spent <b>at least \$66 million on remediation</b> .   |
|   | Apria Healthcare                   | 11,000 patients records <b>exposed on stolen laptop</b> .  |
|  | Oregon Health & Science University | USB drive with data on thousands of patients was <b>stolen from the home of an employee</b> .  |
|  | Toyota                             | Toyota <b>contractor accused of logging into the toyotasupplier.com website</b> without authorization and spending hours downloading proprietary plans for parts, designs, and pricing.          |

# SUMMARY



- The management of operational risk within insurance companies is still evolving
- Operational risk is inherent throughout all firms. Operational risk cannot be fully eliminated
- We have developed an operational risk framework aligned with Basel to ensure we identify, assess, control, and mitigate operational risk
- An important part of our framework is our process to identify top and emerging operational risks
- As operational risk has become recognized as a distinct risk category, ***the value of effectively managing operational risk has increased***

# QUESTIONS

