Learning Objectives

1. Learners will discover the differences between Enterprise Reliability Risk Management and Compliance Management through a brief presentation then demonstrate what they learned by their ability to successfully explain it to another learner during the workshop.

2. Learners will consider the differences between Top Down and Bottoms Up Enterprise Reliability Risk Management through a brief presentation then demonstrate what they learned by sharing their company’s approach with another learner during the workshop.

3. Learners will discover the problems with using Risk Matrices for Enterprise Reliability Risk Management through seeing an example, then demonstrate what they learned by sharing with other learners areas where they have seen Risk Matrices applied and how the problems can be avoided.
Learning Objectives

1. Learners will discover the differences between Enterprise Reliability Risk Management and Compliance Management through a brief presentation then *demonstrate what they learned by their ability to successfully explain it to another learner during the workshop.*

2. Learners will consider the differences between Top Down and Bottoms Up Enterprise Reliability Risk Management through a brief presentation then *demonstrate what they learned by sharing their company’s approach with another learner during the workshop.*

3. Learners will discover the problems with using Risk Matrices for Enterprise Reliability Risk Management through seeing an example, then *demonstrate what they learned by sharing with other learners areas where they have seen Risk Matrices applied and how the problems can be avoided.*
## Popular Models

### Reliability and Quality Management
- Identify Gaps in Reliability
- Hold Internal Audits for Objective Evaluation
- Maintain System for identifying Internal Controls
- Maintain System for validating Procedures for Ops/Planning
- Monitor Reliability
- Perform Annual Management Process Review for system to validate process, including all stakeholders
- Correct Reliability Issues
- Perform Corrective and Preventive Action measures including Root Cause Analysis/Problem solving
- Provide Reliability Training Program for Organization (including reliability and awareness)

### Risk Management
- Establish Risk Management
- Establish Reliability Risk Areas and Objectives
- Establish process to identify existing & emerging threats (risks)
- Establish risk response plans
- Evaluate Risks
- Evaluate the potential impact of the identified risks (likelihood of occurrence, detection, and impact)
- Mitigate Risks
- Mitigate and control risk
ISO 31000:2009

5. RISK MANAGEMENT PROCESS

5.3 ESTABLISH YOUR UNIQUE RISK MANAGEMENT CONTEXT

5.4 CARRY OUT YOUR RISK ASSESSMENT PROCESS

5.4.2 IDENTIFY YOUR ORGANIZATION'S RISKS

5.4.3 ANALYZE YOUR ORGANIZATION'S RISKS

5.4.4 EVALUATE YOUR ORGANIZATION'S RISKS

5.5 FORMULATE AND IMPLEMENT YOUR RISK TREATMENT PLANS

5.6 MONITOR AND REVIEW YOUR RISK MANAGEMENT PROCESS

ISO 31000 RISK MANAGEMENT ARCHITECTURE

Source: www.praxiom.com
Goals of ERM

Enterprise GRC Platforms

Figure 1. Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms

Source: Gartner (October 2012)
AEP’s GRC Journey - Background

- Varied collection of Risk Management techniques and tools
- Have a Chief Risk Officer
- Corporate risks viewed utilizing a top-down approach
- Implemented EMC’s RSA-Archer
  - Physical Security
  - NERC Compliance
  - Cyber Security
  - Internal Audits
GRC introduced new challenges

- New terminology for many – everything is a ‘risk’
- Viewing & relating financial risks with operational risks
- Policies must be restructured to become ‘workflow friendly’
- Consistency of implementation across lines of business
AEP’s GRC Journey - Opportunities

➢ GRC creates new opportunities

• Complete company-wide view of risks
  – Operational, financial, legal, compliance, etc.

• Clear & consistent communication of risks

• Automated & timely risk reporting

• Ability to collect many opinions and points-of-view

• Direct lines-of-sight from requirements through tasks
  – Requirement ➔ Obligation ➔ Standard ➔ Procedure ➔ Task
Small Group Discussion 1

How does Enterprise Risk and Reliability Management differ from Compliance at our company?
Learning Objectives

1. Learners will discover the differences between Enterprise Reliability Risk Management and Compliance Management through a brief presentation then **demonstrate what they learned by their ability to successfully explain it to another learner during the workshop.**

2. Learners will consider the differences between Top Down and Bottoms Up Enterprise Reliability Risk Management through a brief presentation then **demonstrate what they learned by sharing their company’s approach with another learner during the workshop.**

3. Learners will discover the problems with using Risk Matrices for Enterprise Reliability Risk Management through seeing an example, then **demonstrate what they learned by sharing with other learners areas where they have seen Risk Matrices applied and how the problems can be avoided.**
Which Structure is Often Better for High Reliability at the Expense of Productivity?

**Organizational Structure and Its Influence (PMI®)**

<table>
<thead>
<tr>
<th>Project Aspect</th>
<th>Functional</th>
<th>Matrix</th>
<th>Projectized</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Manager’s Authority</td>
<td>Little or none</td>
<td>Low</td>
<td>Moderate to high</td>
</tr>
<tr>
<td>Resource Availability</td>
<td>Little or none</td>
<td>Low</td>
<td>Moderate to high</td>
</tr>
<tr>
<td>Who Manages the Project Budget</td>
<td>Functional manager</td>
<td>Functional manager</td>
<td>Mixed</td>
</tr>
<tr>
<td>Project Manager’s Role</td>
<td>Part-time</td>
<td>Part-time</td>
<td>Full-time</td>
</tr>
<tr>
<td>Project Management Administrative Staff</td>
<td>Part-time</td>
<td>Part-time</td>
<td>Part-time</td>
</tr>
</tbody>
</table>


© 2014 Global Knowledge Training LLC. All rights reserved.
Managing Systems

Functional organization  Project organization  Functional organization  Project organization

Knowledge

Mean level of knowledge

Time

Figure 14.11 Switching between functional and project organization.

Source: Advanced Systems Thinking, Engineering, and Management
By Derek K. Hitchins
## Top-down and bottom-up ERM

<table>
<thead>
<tr>
<th>Objective</th>
<th>What ‘good’ looks like</th>
</tr>
</thead>
</table>
| “Enable top management to make better risk/reward trade-offs” | - Insights on top 5 to 10 risks shaping future performance  
- Clarity on “big bets”  
- Major decisions supported with risk insights  
- Effective oversight of enterprise-wide risks  
- Risk dialogue among top management team |
| “Connect top management with the rest of the organization on risk matters” | - Top management involved in risk processes  
- Critical risk information surfaced in timely manner |
| “Ensure robust risk management across the organization” | - Exhaustive identification and prioritization of risks  
- Employees equipped to make the right risk-return trade-offs in day-to-day activities  
- Processes in place to enable risk oversight  
- Robust risk culture |

Lean Approach to ERM

**Bottom’s Up and Top Down Structure**

Source: *Kaizen Event Fieldbook* – Mark R. Hamel - 2010
1. Strategy deployment breakthrough objectives drive the need for kaizen.

2. Flow kaizen generates a value stream improvement plan (VSIP).

3. The VSIP prescribes relevant high-impact kaizen events.

4. Process kaizen events generate standard work and visual controls to help sustain the gains.

5. The lean management system (LMS) ensures process adherence and performance. Some of the LMS identified abnormalities and opportunities are feedstock for daily kaizen activities or formal kaizen events.

Source: *Kaizen Event Fieldbook* – Mark R. Hamel - 2010
Uptime % requires detailed knowledge of: Likelihood of Risks causing issues AND internal controls to enable uptime!
Four Rooms of Change – Claes Janssen

Change House

AEP’s GRC Journey - Framework

Authoritative Sources  
(e.g., NERC Standards, NIST, CERT-RMM, RTO Protocols / Manuals)

Control Standards

Policies

“Logical groupings of Obligations – Generally summarized at the Standard or Requirement Level”

Obligations

“Unambiguous statements of what is required to be created to demonstrate compliance”

Control Procedures

“Describe how obligations are being met”

Tasks

“Individual assignments with due dates to execute Control activities (e.g., run reconciliation report)”

Evidence

• Documents  
• Reports  
• Raw Data

Control Assessments

“Activities completed to ensure obligations are being met – per the methods defined in the Control Procedures”
AEP’s GRC Journey - Progress

➢ To date focus has been on automating workflow for compliance activities
  • CMEP
  • Data Requests
  • RSAW development
  • Self-Certifications

➢ With CIP v5 - implementing controls within GRC to ensure compliance down to the task level
AEP’s GRC Journey - Design

Figure 1: The Top Down/Bottom Up Risk Management Approach
Source: Utilizing RSA Archer Risk Management 5.0 Solution – Practitioner’s Guide
Connecting the Top and Bottom

Key Questions

- Can assumptions made at the strategic level be corroborated with empirical operations evidence? (i.e., Is the perception of risk accurate?)
- Are executives worried about the right things and prioritizing appropriately?
- How well is the organization staying within the bounds of its risk tolerance?
- How effective is the risk function in consistently identifying risks?
- Is the risk function covering the proper portion of the enterprise with detailed risk assessments?
Small Group Discussion 2

- How do the ERM methods discussed compare to what we are doing at our company?
- Who owns Top-to-Bottom Enterprise Risk and Reliability Management at our company?
Learning Objectives

1. Learners will discover the differences between Enterprise Reliability Risk Management and Compliance Management through a brief presentation then *demonstrate what they learned by their ability to successfully explain it to another learner during the workshop.*

2. Learners will consider the differences between Top Down and Bottoms Up Enterprise Reliability Risk Management through a brief presentation then *demonstrate what they learned by sharing their company’s approach with another learner during the workshop.*

3. Learners will discover the problems with using Risk Matrices for Enterprise Reliability Risk Management through seeing an example, then *demonstrate what they learned by sharing with other learners areas where they have seen Risk Matrices applied and how the problems can be avoided.*
What Wrong with Risk Matrices?

- **Poor Resolution.** Typical risk matrices can correctly and unambiguously compare only a small fraction (e.g., less than 10%) of randomly selected pairs of hazards. They can assign identical ratings to quantitatively very different risks (“range compression”).

- **Errors.** Risk matrices can mistakenly assign higher qualitative ratings to quantitatively smaller risks. For risks with negatively correlated frequencies and severities, they can be “worse than useless,” leading to worse-than-random decisions.

- **Suboptimal Resource Allocation.** Effective allocation of resources to risk-reducing countermeasures cannot be based on the categories provided by risk matrices.

- **Ambiguous Inputs and Outputs.** Categorizations of severity cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g., frequency and severity categorizations) and resulting outputs (i.e., risk ratings) require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks. These limitations suggest that risk matrices should be used with caution, and only with careful explanations of embedded judgments.

### Flawed Risk Matrix Example

**Example**

<table>
<thead>
<tr>
<th>Qualitative model</th>
<th>Quantitative reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>0</td>
</tr>
<tr>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>H</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(Occurrence, Detection, Harm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3,3,3)</td>
</tr>
<tr>
<td>(2,2,5)</td>
</tr>
</tbody>
</table>

How Likely is this Risk to Occur?  
How Likely will be Detect It?  
How Much Harm Could it do?

(3,3,3) → 27  
(2,2,5) → 20  
(M,M,M) → M  
(M,M,H) → H

Categorical qualitative is awkward

Double Check the Math…

3/5 * 3/5 *3/5 = 0.22 Medium??
2/5 *2/5 *5/5 = 0.16 High??

Source: *Probabilistic Risk Analysis with Hardly Any Data* – Scott Ferson and Kevin Shoemaker – Applied Biomathematics – Stony Brook University - 2013
Where have I seen issues with Risk Matrices?

What else about ERM would I like to learn about at future Conferences or in other engagements?
Questions & Answers

Forward Together • ReliabilityFirst