ASSURANCE MAPPING – CHARTING THE COURSE FOR EFFECTIVE RISK OVERSIGHT

AUGUST 30, 2012

Anthony Reyes, CIA, Director, Audit Services, Pinnacle West Capital Corporation
Nathan Ives, Senior Manager, E&Y
YOUR PRESENTERS

Anthony Reyes
Director, Audit Services
Pinnacle West Capital

Nathan Ives
Senior Manager
Ernst & Young
LEARNING OBJECTIVES

I. Assurance Mapping definition and the role it serves

II. Drivers for Assurance Mapping

III. Assurance Mapping development phases

IV. Assurance Mapping impacts on Internal Audit organizations

V. Example Assurance Map
I. ASSURANCE MAPPING DEFINITION AND THE ROLE IT SERVES
POLLING QUESTION #1

Is your organization planning (or has completed) an Assurance Mapping exercise?

A. Yes
B. No
C. Pending
PINNACLE WEST ASSURANCE MAPPING DRIVERS

• Complexity of nuclear power plant operations
• Existence of nuclear focused assurance function
• Significant number of external assurance activities
• End Goal: definition of internal audit scope
### WHO ARE THE DIFFERENT TYPES OF ASSURANCE PROVIDERS WITHIN AN ORGANIZATION?

<table>
<thead>
<tr>
<th>Management Assurance</th>
<th>Board of Directors</th>
<th>External Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compliance</td>
<td>• Internal Audit</td>
<td>• Independent Auditor</td>
</tr>
<tr>
<td>• Quality Assurance</td>
<td></td>
<td>• Government Regulators</td>
</tr>
<tr>
<td>• Self-Assessments</td>
<td></td>
<td>• Trade Associations (e.g. ISO)</td>
</tr>
</tbody>
</table>
INTERNAL AUDIT’S ROLE IN ASSURANCE

REF: IIA PRACTICE ADVISORY 2050-2 ASSURANCE MAPS

• Normally responsible for providing assurance over the entire organization, including:
  – Design and operating effectiveness of risk management processes
  – Management of “key” risks including the risk assessment process
  – Reporting of assessed risk and control condition
CONVENTIONAL OWNERSHIP OF ASSURANCE ACTIVITIES

- Internal Audit
- Risk Management (ERM) / Compliance
- Quality Assurance / Self-Assessments

Areas of Potential Inefficiencies
BALANCING ASSURANCE ACTIVITIES

• Mapping assurance coverage against the key risks of an organization.
WHAT IS AN ASSURANCE MAP

Identification, Analysis, and Intelligent Work Distribution

Key Organization Risk

Compliance Assurance Activities
Quality Assurance Activities
Internal Audit Assurance Activities
External Assurance Activities
II. DRIVERS FOR ASSURANCE MAPPING
POLLING QUESTION #2

What role would you envision that the CAE will play in an Assurance Mapping effort?

A. Own the process
B. Actively assist others in the creation of the Assurance Map
C. Primarily a user of the mapping exercise
WHY COMPLETE AN ASSURANCE MAP?

• Assist the Board in understanding and assessing the organization’s assurance process for key risks

• Identify areas where audit coverage could be enhanced through the annual plan

• Coordinate the assurance activities of an organization

• Promotes collaboration between executive management and the internal audit function

• Increases the credibility of internal audit within the organization
CAE ROLE IN ASSURANCE MAPPING

• Understand assurance requirements of the board as well as the organization

• Use as an input into audit planning and when providing an opinion, on organizational governance, risk management, and control processes

• Act as an assurance activity coordinator

• Assist (or drive) with the creation of the Assurance Map
III. ASSURANCE MAPPING DEVELOPMENT PHASES
POLLING QUESTION #3

Which phase of the Assurance Mapping development process do you see as the most critical for your organization to ensure success?

A. Aligning ERM and business unit risks
B. Linking risks to processes
C. Identifying assurance activities (internal and external)
DEVELOPMENT PHASES

• Align enterprise level (ERM) risks with business unit risks

• Establish the relationship between business unit risks and the relevant processes

• Identify assurance activities
ASSURANCE MAPPING COMPONENTS

Assurance Mapping enables visualization of the alignment between enterprise risks and their associated processes. Concurrently, it reveals the degree of assurance oversight applied to these processes.

**Risk Categories:** High level Company corporate risk (ERM) groupings

**Nuclear Risk Universe:** Commonly 8 – 12 risk groupings specific to the Company

**Specific Risks:** Explicit risks linked to the nuclear organization

**Relationship:** Tie between specific risks and their associated processes

**Process Universe:** Nuclear business unit process model based on the Nuclear Energy Institute’s (NEI) Standard Nuclear Performance Model

**Internal / External Oversight & Assurance:** Scheduled assurance activities, noting frequency
ALIGN RISKS

- **Step 1:** Identify enterprise risk (ERM) categories
  (Operational, Financial, Reputational, Regulatory)

- **Step 2:** Document related business unit risks
- **Step 3:** List the focused organizational risks monitored for which mitigation actions are taken
ESTABLISH RISK TO PROCESS RELATIONSHIPS

• Step 4: Identify and document the business’s operational and supporting processes

• Step 5: For each key risk, identify and document all relevant processes
IDENTIFY PROCESS OVERSIGHT

- **Step 6:** Identify and document the business’s process assurance activities

<table>
<thead>
<tr>
<th>Process Universe</th>
<th>Internal Oversight &amp; Assurance</th>
<th>Internal Audit</th>
<th>Internal Oversight Organization 3</th>
<th>External Oversight Organization 1</th>
<th>External Oversight Organization 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Process 1</td>
<td>(Periodicity)</td>
<td>Client Audit 1</td>
<td>(Periodicity)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Process 2</td>
<td>(Periodicity)</td>
<td>Client Audit 2</td>
<td>(Periodicity)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Process n</td>
<td>(Periodicity)</td>
<td>Client Audit 3</td>
<td>(Periodicity)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Process n+1</td>
<td>(Periodicity)</td>
<td>Client Audit 4</td>
<td>(Periodicity)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Process 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Process</td>
<td>(Periodicity)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Process</td>
<td>(Periodicity)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Step 7:** Identify and document external organization’s process assurance activities
IV. ASSURANCE MAPPING IMPACTS ON INTERNAL AUDIT ORGANIZATIONS
BENEFICIAL INTERNAL AUDIT IMPACTS

• Improves Internal Audit’s effectiveness:
  – Focuses Internal Audit resources on the performance of risk-driven audits
  – Provides the opportunity to better leverage assessments by other internal groups
  – Elimination of redundant oversight activities
  – Reduction in the number of low value audits performed
  – Identifies the common processes in place to mitigate key risks

• Reduces Internal Audit’s impact on the business

• Provides for near and long-term assessment schedule planning

• Enables identification of near and long-term auditor knowledge, skills, and experience needs

• May lead to a standard risk definitions
  – Establish an overall assurance framework
CHALLENGES FACED

• Time consuming

• Must be periodically updated

• Coverage is dependent on assurance organizations outside of Internal Audit
V. EXAMPLE OF ASSURANCE MAP
# EXAMPLE - ENTERPRISE RISK (ERM) TO PROCESS RISK MAPPING

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Nuclear Risk Universe</th>
<th>Definitions</th>
<th>ID</th>
<th>Identified Nuclear Plant Specific Risks Within the Existing ERM Universe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational (OP)</td>
<td>Major Facility</td>
<td>An operational event that results in loss of life or significant facility/equipment damage.</td>
<td>633 Inherent Risk of Operating the Facility</td>
<td>123 Personnel / Industrial Safety</td>
</tr>
<tr>
<td>Plant Performance</td>
<td>Challenges</td>
<td>A failure to detect and remediate issues affecting unit reliability (overall capacity factor, forced outage factor, unplanned outage extensions, etc.), including both equipment and human</td>
<td>643 Nuclear Plant INPO Score Degradation</td>
<td>545 Lost Generation</td>
</tr>
<tr>
<td>Workforce Issues</td>
<td></td>
<td>Inadequate planning and execution of staffing strategies that ensure a qualified labor pool, robust succession plans, and effective employee</td>
<td>660 PWSCC of Reactor Vessel (RV) Nozzles</td>
<td>544 NRC Action Matrix Column / SCCI Degrad</td>
</tr>
<tr>
<td>Financial (FIN)</td>
<td>Financial Management</td>
<td>Inability to effectively forecast and manage business costs, creating financial exposure for the utility with potential negative consequences to financial planning and state regulatory</td>
<td>689 Succession Planning</td>
<td>234 Supply Chain - Inventory Management</td>
</tr>
<tr>
<td>Reputational (REP)</td>
<td>Governance Failure</td>
<td>Lack of appropriate governance structures. Failure to comply with legal, regulator, or ethics requirements resulting in significant impacts to the utility.</td>
<td>478 Cyber Security Program</td>
<td>233 Supply Chain - Strategic Sourcing</td>
</tr>
<tr>
<td>Regulatory (REG)</td>
<td>Loss of Favorable</td>
<td>Adverse changes in state or federal regulatory climate.</td>
<td>588 CTMT Sump Strainers, GL 04-02</td>
<td>36 New Physical &amp; Cyber Security Regs</td>
</tr>
<tr>
<td></td>
<td>Regulatory Environment</td>
<td></td>
<td>634 Potential New Emergency Planning Regs</td>
<td>635 Potential New Fatigue Rule Costs (Part 26)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>637 NRC Post Fukushima Orders</td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

† A quarterly rolup assessment of site operational performance information from all sources (internal and external) is also performed.

* A semi-annual rolup assessment of site corrective action and root cause analysis data is also performed.
# EXAMPLE – PROCESS TO ASSURANCE ACTIVITY MAPPING

## Process Universe

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations Program</td>
<td>(24 months)</td>
<td>(Ongoing)</td>
<td>(24 months)</td>
<td>(O / P / C / A / B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental Monitoring Program</td>
<td>(24 months)</td>
<td>(Ongoing/Quarterly)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance Program</td>
<td>(24 months)</td>
<td>(Ongoing)</td>
<td>(24 months)</td>
<td>(P / C / A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Management Program</td>
<td>(24 months)</td>
<td>(Ongoing)</td>
<td>(24 months)</td>
<td>(P / C / A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide Material &amp; Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Material Control Program</td>
<td>- Quality Assurance Controls</td>
<td>X</td>
<td>(B-annual)</td>
<td>(P / T / S)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Procurement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Inventory Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract Control Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Monitoring &amp; Improvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Assessment and Benchmarking Program</td>
<td>(24 months)</td>
<td>(Ongoing)</td>
<td>(24 months)</td>
<td>(P / C / S / A / B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Independent Oversight Program</td>
<td>OA Group</td>
<td>X</td>
<td>(24/48 months)</td>
<td>(A / I / B / P)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire Protection Program</td>
<td>(24/36 months)</td>
<td>(Ongoing)</td>
<td>(24 months)</td>
<td>(P / T / C / A / T)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Security Program</td>
<td>- Cyber Security Planning</td>
<td>X</td>
<td>(24 months)</td>
<td>(Cyber security rules are being developed.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Business Systems</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Technology Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document Control Program</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative Control Program</td>
<td></td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records Management Program</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Services Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensing and Compliance</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources Program</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(24 months)</td>
<td>(P / C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Human Resources Functions</td>
<td>X</td>
<td>(B-annual)</td>
<td>(24/48 months)</td>
<td>(Periodic)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Communications Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility Management Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Key - Level of internal assurance derived from activity:

- **High**: Those process areas routinely assessed by NQA and nuclear plant management.
- **Medium**: Those process areas not routinely assessed by either NQA or nuclear plant management.
- **Low**: Those process areas not routinely assessed by either NQA or nuclear plant management.

### Periodicity:

- **O - Ongoing**: A - Annual
- **P - Periodic**: 18 - 18 months
- **C - Conditional**: B - Biennial
- **Q - Quarterly**: 24 - 24 months
- **S - Semi-annual**: T - Tri-annual

These assessments focus on areas based on plant performance, industry trends, and management discretion. All other audits are based on predefined performance requirements as established by law/regulation.
### EXAMPLE – EXECUTIVE / BOARD LEVEL ASSURANCE MAP

<table>
<thead>
<tr>
<th>Core Processes</th>
<th>Enabling Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate the Plant</td>
<td>Performance Monitoring &amp; Improvement</td>
</tr>
<tr>
<td>Maintain the Plant</td>
<td>Training</td>
</tr>
<tr>
<td>Provide Material &amp; Services</td>
<td>Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>Information Management</td>
</tr>
<tr>
<td></td>
<td>License &amp; Permits</td>
</tr>
<tr>
<td></td>
<td>People, Business &amp; Support Services</td>
</tr>
</tbody>
</table>

#### Operational
- Operations Program
  - Maintenance Program
    - Work Management Program
- Corrective Action Program
- Leader Training Program
- Security Program
- Document Control Program
- Employee Concerns Program

#### Financial
- Material Control Program
  - Contract Control Program
- Fire Protection Program
- Records Management Program
- Information Services Program
- Human Resources Program
- Facility Management Program

#### Reputational
- Environmental Monitoring Program
- Independent Oversight Program
- Industrial Health and Safety Program
- Administrative Control Program
- Licensing and Compliance Program
- Communications Program

Note: Programs depicted may be associated with multiple risk categories but are shown within the most relevant category.
FINALIZING ASSURANCE MAP

Once the Assurance Map is completed:

• Identify gaps in assurance coverage
• Determine areas of redundant oversight
• Isolate low value monitoring activities
• Optimize the internal audit plan and management’s assessment activities
• Update the audit universe and multi-year audit plan leveraging the Assurance Map
IMPORTANT LESSONS LEARNED

Following these practices improves Assurance Map accuracy and gains organization buy-in:

• Obtain the Assurance Map’s contents from those directly responsible:
  – Leverage corporate risk identification as an input to the Assurance Map
  – Partner with business unit executives to identify organization specific risks
  – Work directly with line organization managers to identify business processes and oversight activities

• Validate the map’s accuracy from operational managers up to corporate executives

• Update the Assurance Map on a periodic basis
PRESENTERS

Anthony Reyes
Director, Audit Services
Pinnacle West Capital Corporation
(602) 250-2636
anthony.reyes@pinnaclewest.com

Nathan Ives
Senior Manager
Ernst & Young LLP
(678) 920-9926
nathan.ives@ey.com