Implementing a Control Self Assessment Framework

A case study of RLI Corp.
Welcome to Today’s Webinar

• Before We Begin
  – Sponsors
  – CPE Requirements
  – Demographic Polling Questions
  – Q&A Session

• Copyright: These materials are presented by The IIA. Use without expressed written permission of it is prohibited.
A Word from our Sponsors…

ERNST & YOUNG
Quality In Everything We Do
CPE Requirements

• Only registered participants are eligible to receive CPE credit.
• A series of polling questions will be posed throughout the presentation.
• You must respond to 70% of the polling questions to receive credit.
• Be sure to select the submit button, after making your answer selection.
• You must view the entire webinar.
• Early departure could result in decreased CPE award.
Demographic Polling Questions

1. How many viewers are watching the Webinar at your location?
   a) 1 – I am the only viewer
   b) 2 to 4 viewers
   c) 5 to 7 viewers
   d) 8 to 10 viewers
   e) More than 10 viewers
Webinar Participation

• Submitting Questions to the Presenter:
  – Type the question into the Q&A panel section.
  – Select the “Send” button.
  – We will have a dedicated question and answer session at the end of the presentation to address your questions.

• Technical Assistance
  – Type your issue into the Chat panel section to IIA Tech Support.
  – Select the “Send” button.
  – We will respond to your question privately.
Implementing a Control Self Assessment Framework

A case study of RLI Corp.
Presenters

Seth Davis CIA, CFA, CPCU, CFSA
Vice President, Internal Audit Services at RLI Insurance Company

Brooke Miller, CPA, CPCU, ARe, AIAF
Manager, Internal Audit Services at RLI Insurance Company
Overview

• RLI Background
• Evolution of Sox at RLI (Foundation for RCSA)
• IIA Guidance on CSA
• Risk Control Self Assessments (RCSAs)
  – Determined ideal process and expanded quarterly assessments from Sox financial controls to include operational and compliance risks and controls
  – Developed workflow tool (RISC)
• Enhancement of audit methodology to support management RCSAs/Future State
Polling Question #1

At what level in your internal audit career are you?

a) New to internal audit
b) Staff Auditor
c) Sr. Staff Auditor
d) Audit Manager
e) Audit Director
f) Chief Audit Executive
RLI Background
RLI Profile

- Headquartered in Peoria, IL
- Founded in 1961
- Specialty Property/Casualty Insurance company serving "niche" or underserved markets
- Traded on NYSE (RLI)
- Operates primarily in the United States with over 35 locations and more than 700 employees

- Ratings
  - A.M. Best Company: A+ Superior
  - Standard & Poor's: A+ Strong
<table>
<thead>
<tr>
<th></th>
<th>12/31/2009</th>
<th>12/31/2008</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invested Assets</td>
<td>$ 1,853</td>
<td>$ 1,659</td>
<td>11.7%</td>
</tr>
<tr>
<td>Prem/Reins Recoverable</td>
<td>420</td>
<td>442</td>
<td>-5.0%</td>
</tr>
<tr>
<td>Other Assets</td>
<td>266</td>
<td>318</td>
<td>-16.4%</td>
</tr>
<tr>
<td><strong>Total Assets</strong></td>
<td><strong>$ 2,539</strong></td>
<td><strong>$ 2,419</strong></td>
<td><strong>5.0%</strong></td>
</tr>
<tr>
<td>Unpaid Losses</td>
<td>1,147</td>
<td>1,159</td>
<td>-1.0%</td>
</tr>
<tr>
<td>Unearned Premium</td>
<td>313</td>
<td>335</td>
<td>-6.6%</td>
</tr>
<tr>
<td>Debt</td>
<td>100</td>
<td>100</td>
<td>0.0%</td>
</tr>
<tr>
<td>Other Liabilities</td>
<td>147</td>
<td>117</td>
<td>26.0%</td>
</tr>
<tr>
<td><strong>Total Liabilities</strong></td>
<td><strong>$ 1,707</strong></td>
<td><strong>$ 1,711</strong></td>
<td><strong>-0.2%</strong></td>
</tr>
<tr>
<td>Shareholders’ Equity</td>
<td><strong>$ 832</strong></td>
<td><strong>$ 708</strong></td>
<td><strong>17.5%</strong></td>
</tr>
<tr>
<td>Book Value Per Share</td>
<td><strong>$ 39.14</strong></td>
<td><strong>$ 32.98</strong></td>
<td><strong>18.7%</strong></td>
</tr>
</tbody>
</table>
## INCOME STATEMENT

<table>
<thead>
<tr>
<th>($ millions)</th>
<th>12/31/2009</th>
<th>12/31/2008</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gross Premiums Written</td>
<td>$ 631.2</td>
<td>$ 681.2</td>
<td>-7.3%</td>
</tr>
<tr>
<td>Net Premiums Written</td>
<td>469.9</td>
<td>513.5</td>
<td>-8.5%</td>
</tr>
<tr>
<td>Net Premiums Earned</td>
<td>492.0</td>
<td>528.8</td>
<td>-7.0%</td>
</tr>
<tr>
<td>Investment Income</td>
<td>67.3</td>
<td>79.0</td>
<td>-14.8%</td>
</tr>
<tr>
<td>Loss Ratio</td>
<td>41.3%</td>
<td>46.7%</td>
<td>-11.6%</td>
</tr>
<tr>
<td>Expense Ratio</td>
<td>41.0%</td>
<td>37.5%</td>
<td>9.3%</td>
</tr>
<tr>
<td>Combined Ratio</td>
<td>82.3%</td>
<td>84.2%</td>
<td>-2.3%</td>
</tr>
<tr>
<td>Operating EPS</td>
<td>$ 4.70</td>
<td>$ 4.99</td>
<td>-5.8%</td>
</tr>
</tbody>
</table>
SUPERIOR UNDERWRITING RESULTS

COMBINED RATIO TRACK RECORD: Over the last 10 years RLI has outperformed the industry combined ratio by an average of 14 points.

*Source: Insurance Information Institute. Year-end ratio estimated.
RLI Internal Audit Services (IAS)

- Established in 2003
- Helped RLI become Sox compliant in 2004
- IAS took over Sox Administration in Q2 2008
- Adhere to IIA Standards and completed QAR in early 2008
Evolution of Sox at RLI
Polling Question #2

Has your organization implemented a Sox 404 assessment process (whether required or voluntary)

a) Yes
b) No
c) Don’t know
Evolution of Sox at RLI

- Developed an assessment methodology in 2004 to comply with Sox
  - Was bottom up due to lack of early Sox guidance
    - Included a large number of controls for testing
  - Required individuals in the business units to assess financial reporting controls
    - Internal Audit convinced the Audit Committee and exec mgmt that mgmt, not internal audit, owns the controls and, therefore, should assess these controls
  - Testing for most controls were quarterly
    - For Sox controls occurring more frequently than quarterly
    - Supports 302/906 certification by CFO/CEO
Evolution of Sox at RLI

• Developed an assessment methodology in 2004 to comply with Sox

  – Testing results were aggregated and reported to Executive management and the Audit Committee by a Sox Coordinator who reported to the Controller
  – Sub-certification of financial reporting control environment by VPs
Implications of AS/5 Effective in 2007

• Using guidance provided by the SEC and PCAOB (Auditing Standard 5), RLI “right-sized” the number of Sox financial controls to focus on those key controls which, if not operating effectively, could result in a material error

• This enabled us to make distinctions between key controls over financial reporting and non-key controls
Implications of AS/5

• Internal Audit led initiative to categorize controls as key vs. secondary under AS/5

• However, Sox Coordinator under Controller continued to have secondary controls assessed in the same manner as key controls

• New secondary controls weren’t being added by Sox Coordinator so we were inconsistent
Implications of AS/5

• By continuing to assess secondary Sox controls in the same manner as key controls, we were potentially spending unnecessary resources which may be better used in reviewing high risk Operational/Compliance processes.
Operational/Compliance Controls

- Operational and compliance risks and controls, which may pose a greater exposure than financial reporting risks, were not formally assessed with results reported to executive management
Operational/Compliance Controls

Processes for which we did not consider as key Sox controls included:

- Cat management data interfaces
- Succession planning
- Business Continuity
- Compliance with rate and form filings
- IRS limitations for retirement plans
- Etc.
Challenges with Existing Sox Coordinator

- Ineffective Sox Coordinator under Controller
  - Did not have a good understanding of risks/controls nor a vision of how to take advantage of AS/5 guidance
  - Ineffective hand-offs to Sox Coordinator
  - Doing nothing to replace ineffective assessment tool
Internal Audit Services Takes Over

In 2008, Internal Audit Services takes on oversight role for Sox with an idea to do things better - RCSA
IIA Guidance on CSA

Strong Support by the IIA for a CSA Framework
IIA Standards Support These Concepts

- 1100 – The internal audit activity must be independent, and internal auditors must be objective in performing their work
  - Internal audit should not be the only department assessing risks and controls as this is management’s responsibility

- 2120 – The internal audit activity must evaluate the effectiveness and contribute to the improvement of the risk management process
CSA is a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met.
CSA is a technique that adds value to the internal auditing profession. CSA can add value by increasing an operating unit’s involvement in designing and maintaining control and risk systems as well as identifying risk exposures and determining corrective action.
IIA’s Certification in Control Self-Assessment (CCSA)

• IIA offers a Certification in Control Self-Assessment with exam topics divided into 6 domains:
  – CSA Fundamentals
  – CSA Program Integration
  – Elements of the CSA Process
  – Business Objectives and Org Performance
  – Risk ID and Assessment
  – Control Theory and Application
CCSA Domain I – CSA Fundamentals

Emphasizes management’s responsibility for risk management and control

- Ownership and Accountability for Control – Senior management is charged with overseeing process of risk management and controls
- Reliance on Operational Expertise – CSA promotes evaluation of risks and controls by staff who do the work
- Control Awareness and Education – Education helps staff gain better understanding of risks and controls and how to identify them
## CCSA Domain I – CSA Fundamentals

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>Traditional Approach</th>
<th>CSA Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Business Objectives</td>
<td>Management</td>
<td>Management</td>
</tr>
<tr>
<td>Evaluation of risks and controls</td>
<td>Auditors</td>
<td>Mgmt/Auditors</td>
</tr>
<tr>
<td>Reporting</td>
<td>Auditors</td>
<td>Mgmt/Auditors</td>
</tr>
<tr>
<td>Validating Evaluation of risks and controls</td>
<td>Auditors</td>
<td>Auditors</td>
</tr>
</tbody>
</table>
CCSA Domain II – Program Integration

Focuses on the theories and techniques related to integrating a CSA program into an organization

– Alternative Approaches to CSA – No one CSA is best

– Cost/Benefit Analysis for Implementing CSA

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better risk awareness by management</td>
<td>Costs of facilitators to use CSA</td>
</tr>
<tr>
<td>Improved Controls</td>
<td>Loss of productivity</td>
</tr>
<tr>
<td>Improved Processes</td>
<td>Cost of software</td>
</tr>
<tr>
<td>More efficient use of audit resources</td>
<td>False sense of security if mgmt just go through motions</td>
</tr>
</tbody>
</table>
Presentation Techniques for Successful Integration – you need to sell this

- Clearly explain the purpose and benefits of CSA to group
- Encourage group participation
- Encourage feedback regarding the process
- Report results in a timely manner
CCSA Domain III – Elements of a CSA Process

Focuses on considerations in developing and implementing the CSA process

– Management’s Priorities and Concerns – May need to emphasize their duties in risk/control ownership

– Resource ID and Allocation
  • What type of assessment approach will be used
  • Who will facilitate
  • Who will train
  • Who are the testers
  • Who will report results
CCSA Domain III – Elements of a CSA Process

- Technology Supporting the CSA Process
  - Difficult to sustain in paper and report results
  - Need a tool to enable CSA process

- Reporting Techniques and Consideration
  - Frequency
  - Audience
  - Detail
  - Remediation
  - Follow-up
CCSA Domain IV – Business Objectives and Organizational Performance

Focuses on processes for developing business objectives and monitoring organizational performance

– Objective Setting –
  • Tie to mission, vision, values
  • Risks should relate to goals/objectives

– Performance Measures
  • KPI’s
  • KRI’s
CCSA Domain V – Risk Identification and Assessment

Focuses on including risk as a critical component of the CSA process

– Risk Theory
  • Link between goals, risks and controls
  • Inherent vs. residual

– Risk Models/Framework
  • COSO ERM
  • Proprietary models
CCSA Domain V – Risk Identification and Assessment

Risk Management Techniques

- Transfer – i.e. third party processing of credit cards to avoid PCI exposure
- Manage – traditional control design and evaluation
- Accept – management can and should accept some level of risk; Importance is transparency of this ownership with CSA supports
Focuses on theory and methods to assess internal control as part of a CSA

- Corp Governance, Control Theory and Models
  - Management establishes and owns controls – not internal audit

- Techniques for Evaluating Controls
  - Do testers get to decide?
  - Is it all or nothing?

- Control Documentation Techniques
  - Narratives
  - Workflows
  - Templates
Risk and Control Self Assessments

Determined Ideal Process
Polling Question #3

Has your organization identified and implemented a control self-assessment methodology?

a) Yes
b) No
c) Don't know
Key Concepts

• Management
  – establishes goals and objectives
  – monitors and manages risks which may prevent them from achieving their goals
  – monitors and assesses controls to mitigate risks

• Internal Audit can and should support management in their efforts
Opportunity

• We saw an opportunity to utilize the Sox workflow and structure to begin formalized assessments of operational/compliance controls.
• Made a presentation to management in early 2009 to get buy-in of project.
Goals for Risk and Control Self Assessment

- Create greater transparency and consistent terminology around risks and controls between audit and management
- Support ERM across the organization through risk as well as control ownership and review
Goals for Risk and Control Self Assessment

• Provide Executive management and Board with more timely assessment of controls by management – not just Sox

• Deploy an assessment tool that management could use to house and review their self assessments.
Recommendation to Management

1. Develop Risk and Control Self Assessment (RCSA) approach which would contain business objectives, risks, controls in the business units and support the corporate ERM initiative
2. Implement an assessment approach for key operational and compliance controls
3. Discontinue testing of secondary controls
Decision

• Executive management agreed to:
  – Require assessment of secondary Sox controls in case key controls failed.
    • Assessment effort of secondary controls would decrease from quarterly to annually
  – Begin requiring annual assessment of non-financial controls as part of RCSA
    • High risk operational and compliance controls tested annually
  – Decided to phase in over time as part of completing audits.
Next step

- Needed to sell to Home Office and Product Vice Presidents
  - Convince them why a control self assessment process would benefit them and their department.
- Internal Audit supported management with creating risk assessment for their areas through the completion normal audit risk assessments.
Gained Efficiency

• Implementing the new methodology where we test secondary/non-key Sox controls annually resulted in a 25% reduction in time spent on the assessments.

• As audits are completed and risk and control self assessments are expanded to include operational and compliance controls, the time spent will increase.
# Risk Grid

## Risk Ranking Grid

<table>
<thead>
<tr>
<th>Severity</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;$1M</td>
<td>5</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>≤$1M</td>
<td>4</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>≤$500K</td>
<td>3</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>≤$250K</td>
<td>2</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>&lt;$50K</td>
<td>1</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
</tr>
<tr>
<td>Slight</td>
</tr>
<tr>
<td>Likely</td>
</tr>
<tr>
<td>Highly Likely</td>
</tr>
<tr>
<td>Expected</td>
</tr>
</tbody>
</table>

Source: RLI

www.theiia.org
Two Phases of Risk and Control Self Assessment

- Phase 1 - Management review/approve
  - Process documentation
  - Business Objectives, Risks, and Design of Controls (RCSA)
- Phase 2 - Test the effectiveness of controls
  - Tested Quarterly
    - High Risk Financial
  - Tested Annually
    - High Risk Operational/Compliance Controls
    - Medium (Secondary) Financial Controls
## Risk and Control Review and Assessment Frequency

<table>
<thead>
<tr>
<th>Type of Risk</th>
<th>In RCSA For Review/Approval?</th>
<th>Testing Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk Financial (i.e. Key Sox Controls)</td>
<td>Yes</td>
<td>Assessed Quarterly (assuming control takes place more frequent than quarterly)</td>
</tr>
<tr>
<td>Medium Risk Financial (i.e. Secondary Sox Controls)</td>
<td>Yes</td>
<td>Assessed annually</td>
</tr>
<tr>
<td>High Risk Operational or Compliance Controls</td>
<td>Yes</td>
<td>Assessed annually</td>
</tr>
<tr>
<td>Medium Risk Operational or Compliance Controls</td>
<td>Yes</td>
<td>No assessment required in RISC</td>
</tr>
<tr>
<td>Low Risk Financial, Operational, or Compliance Controls</td>
<td>No</td>
<td>No assessment required in RISC</td>
</tr>
</tbody>
</table>
Polling Question #4

Does your organization use an automated tool to perform Sox 404 assessments?

a) Yes
b) No
c) Not/Applicable (not Sox compliant)
d) Don’t know
Risk and Control Self Assessments

Developed Workflow Tool
Technology Challenges

• The assessment tool in place at the time had some serious drawbacks
  – Off the shelf product purchased when first implemented Sox
  – Ineffective Sox workflow
    • Narratives not updated until the end
  – Confusing to users
  – Repetitive approvals
  – Unstable application
  – Difficult to add risk and control characteristics
  – Very limited on changes
Enhanced Assessment Tool

- Obtained several RFPs for applications but found they were either too expensive and/or required customization.

- Partnered with IT to develop a SharePoint based solution called RISC (RLI Internal System of Controls) to ensure it met our assessment needs as tool should conform to our process, not the other way around.
Key Components of RISC tool

- Narrative
- RCSA
  - Risk and Control Self Assessment
- Quarterly Assessment Workflow and Approvals
- Electronic Evidence
RISC Fields

• RISC tool mirrors risk assessments performed during audits and captures more effective data elements than previous tool including:
  – COSO Components
  – CoBIT components
    • Organized IT processes by CoBIT domain
      – Plan and Organize
      – Acquire and Implement
      – Delivery and Support
      – Monitor and Evaluate
    • Identified the domain processes applicable for each control
  – Account categories
Benefits of New Assessment Tool

• RISC tool provides proper workflow which requires review and approval of process narratives and Risk and Control Self Assessment (RCSA) Matrix
  – Makes no sense to test controls if process and risks have changed
  – Once process and risks/controls have been approved, the assessment process is initiated
Old tool workflow

Assessment Manager
- Logs in and kicks off assessment

Process Documenter
- Logs in again to click “complete process” which automatically delivers task to assessment manager.

Assessment Manager
- Review and submit assessment for approval

Process Documenter
- Updates/evaluates controls
- Creates and sends out tests
- Numerous things to change/click
  - e.g. “change evaluation period”

Process Approver
- Approve/reject process
- Process returned to process documenter

Assessment Approver
- Review and approve/reject assessment and all related processes/controls/tests

Tester
- Complete tests
- Submit to Process Documenter for Approval

Process Documenter
- Approve/disapprove tests.
- Evaluate/Complete controls
- Attach narrative
- Submit process for approval

Assessment Manager
- Log in again to “complete process”
**Control Admin (Internal Audit)**
- Sets quarter testing period and starts testing

**Process Owner**
- Must first review narrative and make updates
- Updates RCSA (Risk and Control Self-Assessment)
- All changes to these items are routed to the Internal Control Director

**Internal Control Director (Internal Audit)**
- Will review and approve changes made to narrative and RCSA
- When all items approved, an e-mail notification is sent to the Process Owner

**Tester**
- Completes tests assigned and submits for approval

**Process Owner**
- Approved/rejects tests
- Submits completes process testing results to Executives

**Process Executive**
- Reviews a report detailing unacceptable control tests and giving drill down capability to all controls tested.
RCSA screen

• Access narrative
  – Versioning of Word document in SharePoint
• Export risks and controls to Excel for easy review
• Make changes/updates directly to tool
  – Process Owners can decide what quarter(s) works best for testing and select that quarter
RCSA Approval

• After reviewing and updating controls and risks and updating the narrative, process owners submit RCSAs to the Internal Control Director for approval

• Internal Control Director reviews changes to verify all changes are clear and do not need clarification.
# RCSA Approval

## Publish RCSA - Process Owner

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Test Frequency</th>
<th>Test Period</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control: HR-103</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR-103 (Modified)</td>
<td>Annually</td>
<td>Q3</td>
</tr>
<tr>
<td><strong>Control: HR-107</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR-107</td>
<td>Quarterly</td>
<td>Q1, Q2, Q3, Q4</td>
</tr>
<tr>
<td><strong>Control: HR-106</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR-106</td>
<td>Annually</td>
<td>Q1</td>
</tr>
<tr>
<td><strong>Control: HR-125</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Process:** Human Resources - Retirement Benefits

[www.theiia.org](http://www.theiia.org)
# RCSA Approval

## Original

### Control Details

<table>
<thead>
<tr>
<th>Published</th>
<th>Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Number:</strong></td>
<td>EN-100</td>
</tr>
<tr>
<td><strong>Control Description:</strong></td>
<td>The Code of Conduct is reviewed by the Board of Directors and all employees who attest that they have read and understood the Code.</td>
</tr>
<tr>
<td><strong>SOX Control:</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Updated

### Control Details

<table>
<thead>
<tr>
<th>Published</th>
<th>Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Number:</strong></td>
<td>EN-100</td>
</tr>
<tr>
<td><strong>Control Description:</strong></td>
<td>Annually, the Code of Conduct is reviewed by the Board of Directors and all employees who attest that they have read and understood the Code.</td>
</tr>
<tr>
<td><strong>SOX Control:</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Control tests

• Once the RCSA is updated and approved, process owners can send out tests.
• When tests are completed, a task is sent to the process owner to approve.
• Once all tests are completed and approved, the entire RCSA and test results are sent by a task in the tool to the Process Executive for Approval.
Submit RCSA for Approval

Send Processes to Executive for Approval

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Test Evidence</th>
<th>Test Result</th>
<th>Tester Name</th>
<th>Test Status</th>
<th>Test Period</th>
<th>Test Frequency</th>
</tr>
</thead>
</table>
| Control Number: **EN-102**  
EN-102 | Test Pending | Pending Approval | Pen Setz | Q4 | Annually |
| Control Number: **EN-104**  
EN-104 | Test Pending | Pending Approval | Tyler Peterson | Q4 | Annually |
| Control Number: **EN-105**  
EN-105 | Test Pending | Pending Approval | Pen Setz | Q4 | Annually |
Dashboard

- The Internal Control Director can monitor the status of the RCSAs and testing through an easy-to-read dashboard.
## Dashboard

### Current Quarter

<table>
<thead>
<tr>
<th>Start Date</th>
<th>End Date</th>
<th>Quarter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/1/2010 12:00 AM</td>
<td>12/31/2010 12:00 AM</td>
<td>Q4</td>
</tr>
</tbody>
</table>

### Processes

<table>
<thead>
<tr>
<th>Processes</th>
<th>RCSA Approval</th>
<th>Acceptable Tests</th>
<th>Unacceptable Tests</th>
<th>Approved Tests</th>
<th>Rejected Tests</th>
<th>Pending Tests</th>
<th>PE Process Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actuarial Reserving</td>
<td>Draft</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>Bank Reconciliations, Law, Maui Jim, Miscellaneous Accounting</td>
<td>Draft</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td>Branch Administration</td>
<td>Draft</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>Capital Administration</td>
<td>Draft</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>Cash Management</td>
<td>Draft</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>-</td>
</tr>
</tbody>
</table>
User Feedback

• We distributed a user survey after the first quarter of testing and received good feedback
  – Many users felt system was easier to use and was intuitive
  – Liked the electronic evidence feature
• Did receive some good suggestions that resulted in some final tweaking/changes before the next quarter of testing.
Polling Question #5

Does your audit department share its risk assessments with management?

a) Yes
b) No
c) Don’t know
Enhancement of Audit Methodology to support RCSA’s
Enhance Risk Assessment Process During Audits

• Historically, risk assessments were conducted as part of each audit to develop a risk-based audit program. However, the risk assessments were not shared with management to obtain their input and agreement.
Enhance Risk Assessment Process During Audits

• Current audits are typically 12 weeks broken into two six-week phases – one for planning and one for testing/reporting
  – During the planning phase, the audit team will complete narratives and workflows, conduct walkthroughs, complete a risk assessment, complete an audit program, and issue an engagement memo
Enhance Risk Assessment During Audits

- At the end of the planning phase, the audit team will meet with management to review the risk assessment which provides several benefits:
  - Obtain their input on risks and controls
  - Helps avoid disputes on whether control concerns identified during the audit are important as we obtained agreement as to the underlying risks
  - Helps to establish ownership of the risks at the conclusion of the audit
Enhance Risk Assessment During Audits

• Challenges when sharing with management
  – Confusion of inherent vs. residual risk
  – Confusion between risks and audit issues
  – Length of time required by management to review risk assessment
Migrating Risk Assessments to Management

At the conclusion of the audit, all risks that are medium or high (which is the same ranking used when reporting issues to Executive management and the Audit Committee) are uploaded into the RISC tool.
Migrating Risk Assessments to Management

• Each quarter Management will review and approve their process narrative which covers operational, compliance, and financial aspects of their area

• Each quarter management will review and approve the risks and controls in their area
Migrating Risk Assessments to Management

• Annually management will test the controls to ensure they are operating effectively to mitigate the high operational and high compliance risks as well as non-Sox controls
  – Partner with management to determine quarter that is most convenient to test these controls

• Sox controls are assessed quarterly
Future State

• Continue to populate non-financial risks and controls in RISC tool for quarterly review, approval, and appropriate assessment

• Enhance the quarterly sub-certification to include non-financial risks and controls to provide executive management and the board with overall assurance

• Continued updates to RISC as we mature in our process
  – Risk Management Maturity
  – Add residual risk
Key Points

- Leverage the IIA Guidance
- Management owns risks/controls
- Obtain exec buy-in
- Have mgmt review process, risks and design of controls first
- Identify type and frequency of tests
- Implement process first then tool as enabler
- Do a phased in approach to learn and modify
Questions?

Seth Davis – Seth.Davis@rlicorp.com

Brooke Miller – Brooke.Miller@rlicorp.com
CPE Certificates

• Registered participants who have met the CPE requirements will receive their CPE Certificate and a speaker evaluation by e-mail in approximately ten business days.
Webinar Playback

• Paid attendees of this live Webinar can access the playback at no cost by contacting our Customer Support Team at +1 407 937 1111 or by sending an e-mail to elearning@theiia.org.
Upcoming IIA Webinars

• Establishing Accountability and Transparency Through Performance Auditing
  – December 9, 2010

• Optimizing Value From Your Organization’s Business Relationships: Trust, but Verify
  – December 16, 2010
Upcoming IIA Virtual Seminars

- Enterprise Risk Management: An Introduction
  - starts December 6, 2010

- Operational Auditing: Advanced
  - starts December 6, 2010
Thank You to Our Principal Partners!!!

<table>
<thead>
<tr>
<th>ACL</th>
<th>Deloitte</th>
<th>pwc</th>
</tr>
</thead>
<tbody>
<tr>
<td>protiviti</td>
<td>Robert Half</td>
<td>CCH® TeamMate</td>
</tr>
<tr>
<td>Grant Thornton</td>
<td>Ernst &amp; Young</td>
<td>IDEA</td>
</tr>
</tbody>
</table>

www.theiia.org