The IIA Risk Leadership Summit
22 August 2010

Brian Barnier
Brian@valuebridgeadvisors.com
Our Discussion Today

- Development Rational for ISACA’s Risk IT
- The IIA Market Positioning in Risk Management
- Opportunities for The IIA
Our Discussion Today

- Development Rational for ISACA’s Risk IT
- The IIA Market Positioning in Risk Management
- Opportunities for The IIA
### Key points in ISACA history

<table>
<thead>
<tr>
<th>ISACA formed</th>
<th>CISA</th>
<th>CISM</th>
<th>CGEIT</th>
<th>IT Assurance Framework</th>
<th>CRISC</th>
</tr>
</thead>
</table>

- **Val IT**: Based on COBIT 2006; updated 2008
- **Risk IT**: Based on COBIT 2009
- **86,000+ constituents; 160+ countries** 2010

©2009 ISACA/ITGI. All rights reserved.
Five focus areas of IT governance, created in the early 2000s, illustrate the role of risk management within ISACA’s IT governance approach.

Risk IT reflects enhancements to ISACA’s previous content in this area (formal frameworks and other guidance).
Knowledge Frameworks

- Risk IT was designed to extend and integrate the existing risk content in COBIT 4.1 and Val IT 2.0. By extension, it also reaches out to non-ISACA content previously mapped to COBIT or Val IT that is encountered by practitioners in their daily projects.
  - COBIT—first released in 1996—and now in version 4.1 released in 2007. The bulk of its risk management content is in the Plan and Organise (PO) 9 section. As a process model, other risk management content appears in related sections in Acquire and Implement, Deliver and Support, Monitor and Evaluate.

- The IT Governance Implementation and Continuous Improvement Guide (a third generation publication released in December 2009 at the same time as Risk IT) is not a framework but guidance on implementing all three frameworks together in an organization. This provides additional “connective tissue” between the three main frameworks.
IT Related Risk Management - Summary

- Various standards & frameworks available, but either:
  - Generic Enterprise Risk Management oriented
  - IT silo oriented
- No comprehensive IT Related Risk framework available
New common view of the three frameworks is used in both the Risk IT publications and the *IT Governance Implementation and Continuous Improvement Guide*.
Risk Management Requirements

• What are some essential qualities or features of a good (IT Related) risk management framework?
A. Comprehensive view on risk management, not only mechanical/technical
B. Specific for the subject matter, i.e. IT
C. End-to-end view on the subject matter, i.e. broadest view on IT related risks
D. Business oriented
E. Provide a continuous process, from risk identification to continuous monitoring and feedback
F. Cover all risk treatment options
G. Availability / Accessibility
## Comparison of Major Features

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk IT Principles</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always connects to business objectives</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Align the management of IT-related business risk with overall enterprise risk management</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Balances the costs and benefits of managing risk</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Promotes fair and open communication of IT risk</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Is a continuous process and part of daily activity</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Provides a detailed process model with management guidelines and maturity models</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td><strong>Additional Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability (to the general public)</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Comprehensive view on IT (related) risk</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Dedicated focus on risk management practices for specific IT areas (project management, service management, security, ...)</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Orange</td>
<td>Yellow</td>
<td>Green</td>
</tr>
</tbody>
</table>
CRISC

- Intended to recognize a wide range of IT and business professionals for their knowledge of enterprise risk and their ability to design, implement, monitor and maintain information system (IS) controls to mitigate such risk.
CRISC Domains

- Risk Identification, Assessment and Evaluation (31%)
- Risk Response (17%)
- Risk Monitoring (17%)
- IS Control Design and Implementation (17%)
- IS Control Monitoring and Maintenance (18%)
Our Discussion Today

- Development Rational for ISACA’s Risk IT
- The IIA Market Positioning in Risk Management
- Opportunities for The IIA
## Understanding the Space Example Content

Most is for Practitioner Audiences

<table>
<thead>
<tr>
<th>Conceptual / Framework</th>
<th>Managerial</th>
<th>Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4360, 31000, ARMS</td>
<td>Audit Standards (e.g., 2120)</td>
<td></td>
</tr>
<tr>
<td>COSO ERM</td>
<td>ITAF</td>
<td></td>
</tr>
<tr>
<td>Risk IT Framework</td>
<td>Auditing of IT Risk</td>
<td></td>
</tr>
<tr>
<td>Risk IT PG</td>
<td>Model Audit Guides (not risk specific)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practical</th>
</tr>
</thead>
</table>

© 2010 ValueBridge Advisors
Our Discussion Today

- Development Rational for ISACA’s Risk IT
- The IIA Market Positioning in Risk Management
- Opportunities for The IIA
Opportunities for The IIA for Auditors

- Sharpen audit-risk independence guidance
- Auditor’s Influence & Advocacy Guide for RM
  - Business Focus
  - Business Communication
  - Audit Relevance
- Formalize Auditing of Risk Management Guidance/Models
- Education on performance auditing in general and risk management in specific
- Future of Audit in the Content of Risk Management
Opportunities for The IIA for Non-Auditors

- Board members: How to Better Leverage Audit Teams
- Risk managers: How to Risk Assess Audit
- Risk managers: How to Partner with Audit
Opportunities for Cooperation with ISACA

- Shared Standards and Guidance on Auditing of Risk Management
- 2120 has no parallel in ISACA
- Consistent view on independence
- Consistent clarity on risk-based auditing, auditing of risk management, risk assessment of audit
- Shared guidance on auditing of risk management (new ISACA course including IIA guidance)
- Focus on intersection of business process and IT
Ongoing Learning….

- To join the group, contact: Brian@valuebridgeadvisors.com
  - Articles, whitepapers, chart of the month, risk pictures
  - Networking
  - Twitter @Brian_Barnier on risk management and green shoots