Assessing the Risks of Outsourcing

Patricia Rowlett, CISA, CISSP
PROWLE Enterprises, LLC

ISACA Atlanta Geek Week
August 2011

Session Agenda

- What are the risks?
- What are the activities?
- Can standardization help?
- Wrap up

Definitions

Vendor Assessment

The activities conducted to assess the handling of your data as it is being processed by another organization.

IT Service

Any information technology process performed by another organization.

What are the Risks?

- **Your** data will not be secured consistent with **your** business requirements.
- **Your** data will not be available when **you** need it.
- **Your** data will not be processed with controls consistent with **your** business requirements.
- **Your** data will not be retained consistent with **your** business needs, contracts.

Additional Risks

- You will not be able to conduct business if the vendor goes out of business.
- Your data will not be isolated from other organization's data (it will be comingled) and thus not isolated from their risks.
- Your data will not be accessible to only those with a business need to know.

Bottom Line

"The bottom line is that using a cloud provider can significantly increase the risk of a security incident and can increase all the costs, legal remedies and other losses that follow such a breach."

"Every Silver Cloud Has a Dark Lining," ISACA Journal, Volume 3, 2011.

Three Questions

- What upfront activities do you do?
- What assessment activities do you do?
- Who does what?

Upfront Activities

- Do you put assessment requirements in your RFP's?
- Do you put assessment requirements in your contracts and SLA's?
- Do you put audit provisions in your contracts?
- Do you involve compliance and/or audit when selecting the services to outsource?

Assessment Activities

- Questionnaires
- Service Level Agreements (SLA)
- SAS 70 or other audits?

How much do you rely on SAS 70s?

You: "Do you have a SAS 70"

Your Service Provider: "Yes"

You: "Thank you"

Do you evaluate…

Security of data – in transit and at rest

Compliance Needs

Incident handling

Operational Practices

Availability of data and systems

Provider's assessment process

Who does what?

- Who develops the questionnaires and ensures they are consistent with current compliance requirements?
- Who administers the questionnaires? (sending to providers and tracking the responses)
- Who evaluates the responses?
- Who monitors the remediation efforts?
- Are all of these assessments performed by the same group or are they performed throughout the organization?

What if you are the service provider?

- What information are you letting out of your control?
- Who tracks the information sent for consistency?
- Is Audit or Compliance involved in the assessment process?

Risks of the Assessment

- Does the assessment truly address the risk?
- Are the activities and their supporting controls clearly identified?

What about vendors who outsource to other vendors?

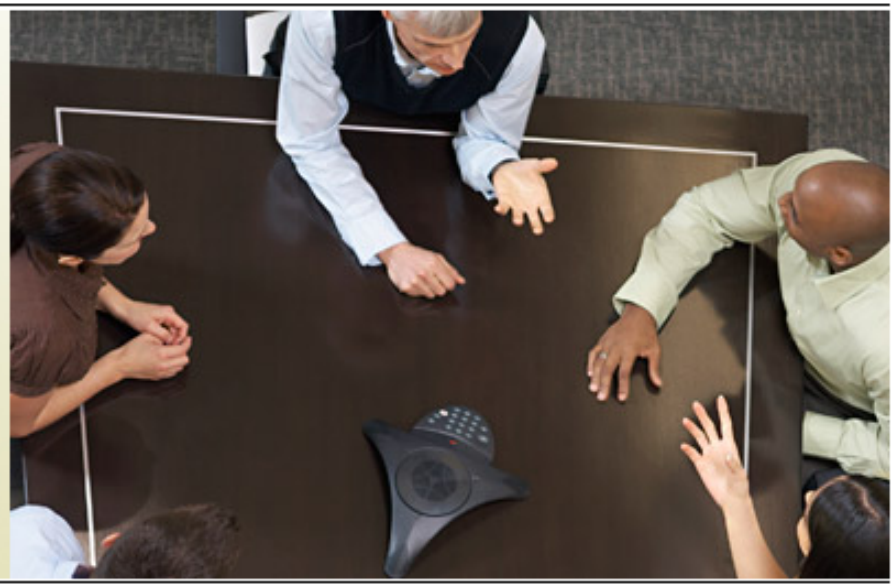
Standardization

- What can be standardized?
- Is it possible?
- Shared Assessments - one industry's attempt to standardize the assessment of outsourced activities.

SHARED® ASSESSMENTS

HOME ABOUT US MEMBER PROJECTS DOWNLOAD MEMBERS EVENTS

Setting the Standards for Vendor Assessments



THE BANK OF NEW YORK MELLON

SOME OF OUR MEMBERS

"The tools and relationships we've gained from Shared Assessments offer real value to CVS Caremark, ensuring rigor in our evaluations of

The Shared Assessments Program

Shared Assessments is a member-driven, industry-standard body that injects speed, efficiency and cost savings into the service provider control assessment process.

Download Current Version Now

Who is Shared Assessments?

- The old Banking Industry Terminology (BITS) Financial Services Roundtable
- Created by financial institutions (including insurance industry) and the "Big 4"
- Pilot completed in 2005 and version 1 launched in 2006
- Includes both national and international organizations

www.sharedassessments.org

Why Shared Assessments?

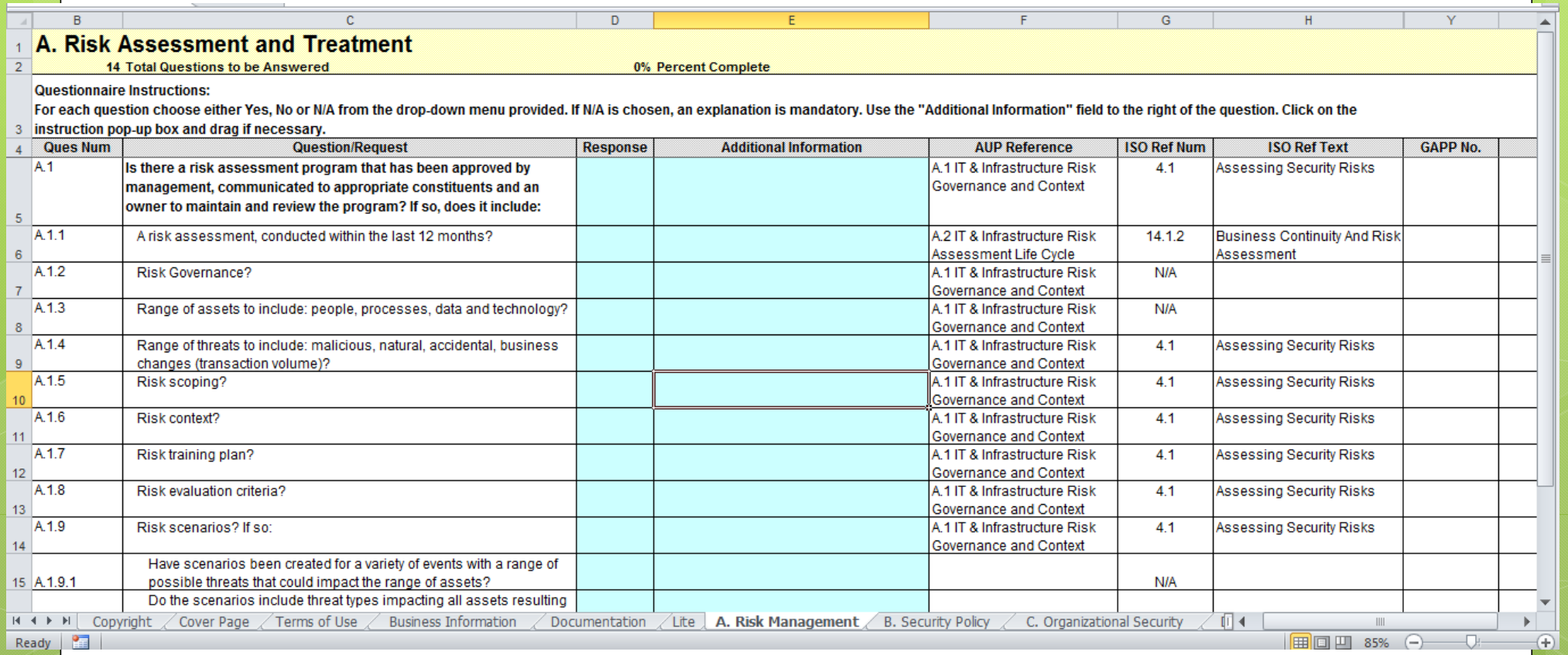
"These founding organizations saw the need for a standardized and objective vendor management assessment methodology that would help outsourcers meet regulatory and risk management requirements while significantly reducing costs for all stakeholders."

http://www.sharedassessments.org/about/

What are the tools?

- Agreed Upon Procedures (AUP)
- Standard Information Gathering Questionnaire (SIG) including
- Targeted Business Continuity & Privacy Questionnaires

Example



A. Risk Assessment and Treatment

14 Total Questions to be Answered — 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.
A.1	**Is there a risk assessment program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program? If so, does it include:**			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.1	A risk assessment, conducted within the last 12 months?			A.2 IT & Infrastructure Risk Assessment Life Cycle	14.1.2	Business Continuity And Risk Assessment	
A.1.2	Risk Governance?			A.1 IT & Infrastructure Risk Governance and Context	N/A		
A.1.3	Range of assets to include: people, processes, data and technology?			A.1 IT & Infrastructure Risk Governance and Context	N/A		
A.1.4	Range of threats to include: malicious, natural, accidental, business changes (transaction volume)?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.5	Risk scoping?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.6	Risk context?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.7	Risk training plan?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.8	Risk evaluation criteria?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.9	Risk scenarios? If so:			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks	
A.1.9.1	Have scenarios been created for a variety of events with a range of possible threats that could impact the range of assets?				N/A		
	Do the scenarios include threat types impacting all assets resulting						

Copyright | Cover Page | Terms of Use | Business Information | Documentation | Lite | A. Risk Management | B. Security Policy | C. Organizational Security

Ready — 85%

What works & what doesn't

What works	What doesn't work
Standard set of questions to allow easy comparison from year-to-year or vendor to vendor.	Length of time to complete – One-size-fits-all approach doesn't really fit!
One set of responses to provide to many recipients.	More subjectivity or analysis may be needed beyond the yes/no responses.
Input from all aspects of the industry.	Many augment the 'standard set of questions' making the standardization moot!

Wrap Up

- Know your risks
- Ensure you provide for the risks before you engage in business
- Clearly define your assessment responsibilities
- Ensure your assessment activities assess your risks

Contact

Patricia Rowlett, CISA, CISSP
PROWLE Enterprises, LLC
patricia.rowett@prowle.us
www.prowle.us