The Shared Assessments Perspective on Effective Vendor Risk Assessment

Brad Keller, Program Director
The Shared Assessments Program
Shared Assessments Program

- Created in 2005, Shared Assessments has become the trusted authoritative source for vendor assessment and risk management.
- The Program focuses on the need for a standardized and objective vendor assessment methodology to help outsourcers meet regulatory and vendor risk management requirements while significantly reducing costs for all stakeholders.
Members of the Shared Assessments Program refine the Program’s Tools on at least an annual basis. New risk control areas are added, and existing risk areas are enhanced, by committees of risk professionals based on the issues they encounter every day.

Shared Assessments’ commitment to developing solutions based on member input is what keeps the Program Tools on the leading edge of third party risk assurance issues.
Shared Assessments Approach

- Substantially reduces the cost of vendor oversight and assessment by
  - Reducing the time and cost associated with processing multiple questionnaires in different formats
  - Standardizing supporting documentation
  - Eliminating redundancy of effort across business units
  - Reducing the need for on-site assessments
Program Tools: The “SIG” and “AUP”

- Standardized Information Gathering (“SIG”) Questionnaire
  - Uses industry best practices to gather and assess information technology, operating and data security risks (and their corresponding controls) in an information technology environment

- Agreed Upon Procedures (“AUP”)
  - Used by companies to evaluate the controls their service providers have in place for information data security, privacy and business continuity
Program Tools: The “SIG”

- Standardized Information Gathering Questionnaire
  - Developed using ISO 27001/2 for the framework methodology
  - Completing/reviewing one questionnaire instead of multiple (dozens? hundreds?) proprietary questionnaires
  - Provides a complete picture of service provider controls
  - Risk tiered scoring option for analysis and reporting
  - Standards correspond to ISO, PCI-DSS, HIPAA/HITECH, COBIT, NIST and FFIEC guidance
  - SIG Management Tool (SMT) facilitates questionnaire comparison(s) and version upgrades
Global Acceptance

- 26% of visitors to www.sharedessments.org are Outside the U.S.
- Top tool purchasers outside U.S. are located in the UK and India
Program Tools: SIG 2014

- Recent Enhancements
  - Mobile device security
  - Software application security
    - Facilitates assessment of service provider’s software development life cycle
  - Expanded privacy section
    - HIPPA/HITECH Regulations
    - Cross-border issues
  - Enhanced usability
    - Macro enabled for improved question filtering
    - Improved instructions and new Dashboard tab
Assessment Tools: The “AUP”

- Agreed Upon Procedures
  - Reduces or eliminates on-site assessments
  - Objective test of controls, validation of vendor self-assessment(s), and report of results
  - Companies view results in the context of their vendor risk management requirements
Recent Enhancements

- Incorporation of Cloud Computing risks from SIG
- Addition of controls to assess 4th Party risk
- AUP Report Template to facilitate concise reporting of on-site assessment results
Vendor Risk Management Maturity Model

- Defined the high-level components that should be present in a comprehensive vendor risk management process
  - Decomposed each high-level component into detail sub-components
  - Mapped the model to several commonly used frameworks to understand gaps and overlaps
  - Built the descriptions of the various levels of maturity leveraging the detail sub-components
  - Understanding the current state of vendor risk maturity allows conscious decisions to be made regarding where to use resources for the greatest benefit
Vendor Risk Management Maturity Model

- The maturity of your vendor risk management program should be related to the nature of your industry, size of organization, and criticality of the outsourced activity to your business.

- Establish program governance as a foundational, guiding element for other framework criteria.

- Identify the other framework elements that would provide the most benefit to your organization at the least cost.

- Reassess process maturity by measuring maturity over time to determine progress and benchmark with industry leaders, as appropriate.
Shared Assessments Annual Events

■ Shared Assessments Summit


■ May 19-21, 2014 - Pre-Summit Workshop and Summit
Learn More

- Website: www.sharedassessments.org
- Services and Education
  - Case studies
  - Enterprise Cloud Computing Guide
- Membership
  - Member Projects & Forums
- Email Brad Keller at brad@santa-fe-group.com