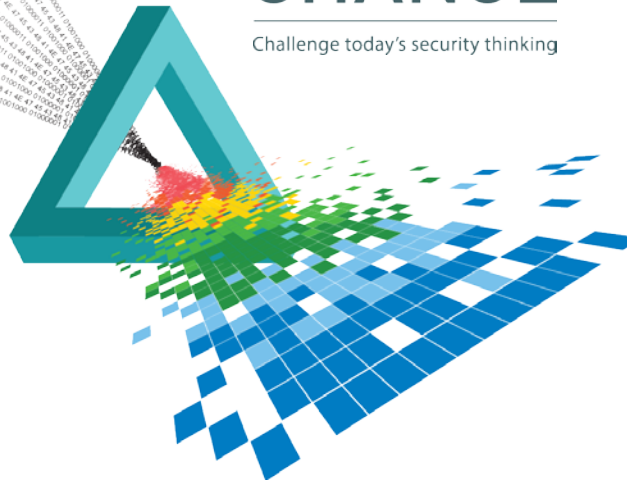
RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking



SESSION ID: GRM-F02

Peer Collaboration – The Next Best Practice for Third Party Risk Management

Robin M. Slade

EVP & COO
The Santa Fe Group & Shared Assessments Program

Introduction

- Q: How do we achieve standardization, efficiencies and cost savings in the third party risk assessment process?
- A: By agreeing that third party risk management is not a competitive issue.

Collective Intelligence

+ Industry Standard

= Improved Risk Assessment Process

The Environment

- Dependence on outsourcing critical services increases inherent risk
- Numerous and overlapping regulatory requirements and heightened expectation on assurance, including increased transparency regarding cybersecurity practices
- Boards and senior management involvement in the risk reporting process
- Proprietary methods for information gathering and assessments are inefficient, costly and lack standardization
- Risk areas continue to evolve and expand
- Threats are becoming increasingly more sophisticated

The Need – Robust Vendor Management Programs

- Evaluate, track and measure third-party risk
- Alignment of risk controls to corporate requirements to lessen exposure to risk from third (and fourth) parties
- Ensure compliance to regulations, standards and guidelines
- Consistent, robust and repeatable process
- Ongoing oversight program

The Problem

- Lack of standardized risk assessment processes by outsourcers
- Varying interpretation of regulations and differing risk appetites
- Service providers resources strained by outsourcers
  - Need to respond to diverse client information requests
  - Time and resource intensive onsite visits

The Solution – The Collaborative Onsite Assessment

- Top-tier US-based financial institution risk managers working collaboratively to improve the third party risk environment
- Leverage the collective intelligence to improve current standards for IT, privacy and data security controls
  - Shared Assessments Agreed Upon Procedures (AUP)
  - Service Organization Control (SOC) 2
- Utilize industry associations to foster collaboration and provide project management
  - Shared Assessments Program
  - Securities Industry and Financial Markets Association (SIFMA)

Project Goals - Creating Efficiencies

- Collaborate on Onsite Assessments of Key Third Parties
  - To the extent that common services are offered to multiple organizations in the financial services industry, evaluate the associated risk in a consistent, uniform manner
    - Leverage the Shared Assessments Agreed Upon Procedures (AUP), standardized testing procedures for onsite assessments, as the common risk assessment methodology
    - Reduce the time and expense of conducting multiple onsite vendor assessments
    - Ensure a standardized, robust, consistent, and repeatable evaluation of a vendor's risk posture

Project Goals - Improve the Framework

- Top tier financial institutions worked collaboratively to develop:
  - A “Superset” AUP framework for onsite assessments (Shared Assessments)
  - Development of a SOC 2 Plus (SIFMA)
- Both projects hold the same common goals – the development of a more robust and scalable risk assessment process that injects speed, efficiency and cost savings into the third party risk assessment process

Project Pilot: Collaborative Onsite Assessments

- Participants “piloted” the process of working collaboratively to assess key third parties for whom they share common shared services:
  - Pilot 1: Iron Mountain + 3 financial institutions
  - Pilot 2: Early Warning Services, LLC + 5 financial institutions
  - Pilot 3: Small Business Financial Exchange (SBFE)
- Superset AUP now meets all internal corporate requirements for many U.S. financial institutions, including key pilot participants:
  - JPMorgan Chase; Citigroup; Capital One; US Bank; Morgan Stanley; Northern Trust

Collaborative Assessment Pilot Approach

- Step 1: Determine participants
  - Select 3+ financial institutions to participate in a joint assessment
  - Select a vendor broadly used within the financial services industry
- Step 2: Scoping
  - Scope and location of services outlined by the vendor
  - Financial Institution participants agree to the scope and location of services
- Step 3: Selection of auditor
  - Participants agree to auditor to conduct the shared assessment
    - CPA or Non-CPA independent assessment firm may be used
- Step 4: Superset modifications
  - Leveraging the gap analysis developed in the mapping of requirements to AUP, auditor adds additional controls and testing procedures to create the Superset
  - Participants review and approve for accuracy and completeness

Collaborative Assessment Pilot Approach

- Step 5: Assessment prep
  - Auditor and Service Provider narrow the AUP to the specific services being assessed
- Step 6: Assessment performed
  - Auditor schedules and conducts an onsite assessment using the narrowed Superset AUP
- Step 7: Post assessment
  - Auditor presents the findings from the assessment to the service provider
  - Service provider presents comments and observations to auditor in response for inclusion into the report
  - Auditor presents final report to all participants
  - Financial institutions meet separately with service provider to review and agree upon remediation plan(s) for any issues or findings

Pilot Lessons Learned

- More robust framework developed with broader risk domain coverage than individual proprietary practices
- More robust controls testing process
- Efficiency gained through one assessment by multiple banks
- Enhanced communication and improved relationship between financial institutions and third party service providers
- Assessors are completely independent of participating banks
- Each participant able to view report based on their unique risk environments

Benefits Summary

- Increased rigor, consistency, efficiency and cost savings in the control assessment process for both the outsourcing organizations and the service provider
- Larger Tier 1 and 2 service providers would benefit most immediately from participating in collaborative assessments
- For mid and small size institutions who cannot necessarily dedicate a high level of resources to meet the changing regulatory and evolving risk environment, there exist tangible cost savings and personnel efficiencies benefits through use of a consistent, reliable tool
- More robust control sets developed through collective intelligence are expected to drive improvements in service provider programs

Continuous Efforts and Improvements

- Next Steps:
  - Ongoing development and refinement of the Superset AUP to ensure additional robustness by expanding the collective intelligence to include additional financial institutions
  - Develop and broaden the collaborative onsite assessment program including project management services
  - Release the enhanced Superset AUP Program Tool mid 2015
  - Promote adoption of the Program's Superset AUP as a best practices standard for each industry or sector as they are developed.

Apply What You Heard Today

- Understand that third party risk management is not a competitive issue
  - Form cooperative relationships and open the lines of communication with your counterparts at other organizations
  - Get involved in industry associations and public-private partnerships
  - Adopt a standardized framework to keep current with new regulatory requirements and changing risk control areas
  - Outsourcers: Consider working collaboratively with other companies to perform collaborative onsite assessments
  - Service Providers: Understand what organizations share common services and encourage them to perform a collaborative onsite assessment

Questions?

For More Information…

Contact:

Robin Slade

EVP & COO

972-347-1627

robin@santa-fe-group.com

Appendix

Shared Assessments Program

- Setting the standard in U.S. vendor risk assurance since 2005, now expanding internationally
- Created by leading financial institutions, the Big 4 accounting firms, and key service providers to:
  - Standardize an objective framework for outsourcers to gather service provider information through a repeatable and consistent evaluation process
  - Raise the bar on third party risk management by creating a comprehensive onsite security evaluation process, regardless of who performs the assessment (CPA, independent assessment firm, internal assessor)
  - Ensure a means for keeping current with the latest regulations, standards and new risk control areas
  - Create efficiencies and reduce costs for all stakeholders

Shared Assessments Program Tools

- Methodologies for managing the vendor risk lifecycle
  - Two complementary tools to document service provider management of information security controls
    - Standardized Information Gathering (SIG) questionnaire
    - Agreed Upon Procedures (AUP) – standardized testing procedures for onsite assessments
  - "Trust, but verify" approach to conducting third party assessments
    - Trust = SIG: Uses industry best practices to gather and assess information technology, operating and data security risks (and their corresponding controls) in an information technology environment
    - Verify= AUP: Used by companies to evaluate the controls their service providers have in place for information data security, privacy and business continuity

Shared Assessments Program Tools

- The Program Tools are aligned to:
  - ISO 27001, 27002
  - COBIT
  - NIST Cyber Security Framework (CSF); Computer Security Incident Handling Guide (NIST.SP.800-61r2)
  - PCI-DSS
  - OCC-2013-29; Merchant Processing Handbook
  - Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
  - FFIEC Appendix J
  - DOJ Breach Procedures
  - AICPA Incident Response Procedures
  - HIPAA Incident Response Reporting Procedures
  - US CERT – Federal Incident Notification Guidelines
  - CMS Medicare and Medicaid EHR Incentive Program, “Meaningful Use”

Shared Assessments Program Tools

- International “add on” components under development to align with international regulatory standards and guidance, including:
  - Hong Kong Monetary Authority (HKMA)
  - European Central Bank (ECB)
  - Asia-Pacific Economic Cooperation (APEC)
  - Monitory Authority of Singapore (MAS)
  - German Federal Financial Supervisory Authority (BaFIN)
  - Bundesbank/Central Bank of Germany (BuBA)
  - Financial Conduct Authority (FCA)
  - Financial Services Authority (FSA)
  - Financial Market Supervision Act (FINMA)
  - Commission de Surveillance du Secteur Financier (CSSF)
  - EU Data Protection Directive