RSA®CONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Third-Party Cybersecurity and Data Loss Prevention

SESSION ID: DSP-W04A

Brad Keller
Sr. Vice President
Santa Fe Group

Jonathan Dambrot, CISSP
CEO, Co-Founder
Prevalent Networks

SHARED ASSESSMENTS

PREVALENT® networks

3rd Party Risk Management is a Hot Topic

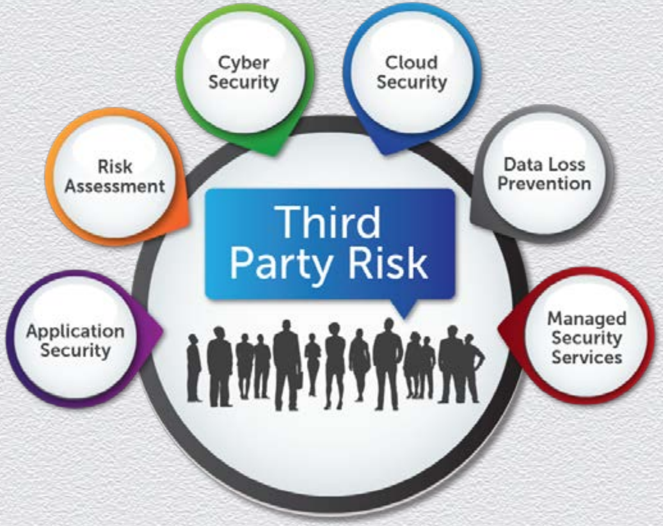
Third-Party Risk is one of the largest drivers of data

"If not managed effectively, the use of service providers may expose financial institutions to regulatory action, financial loss, litigation, and loss of reputation." *Federal Reserve WSJ 12/6/13*

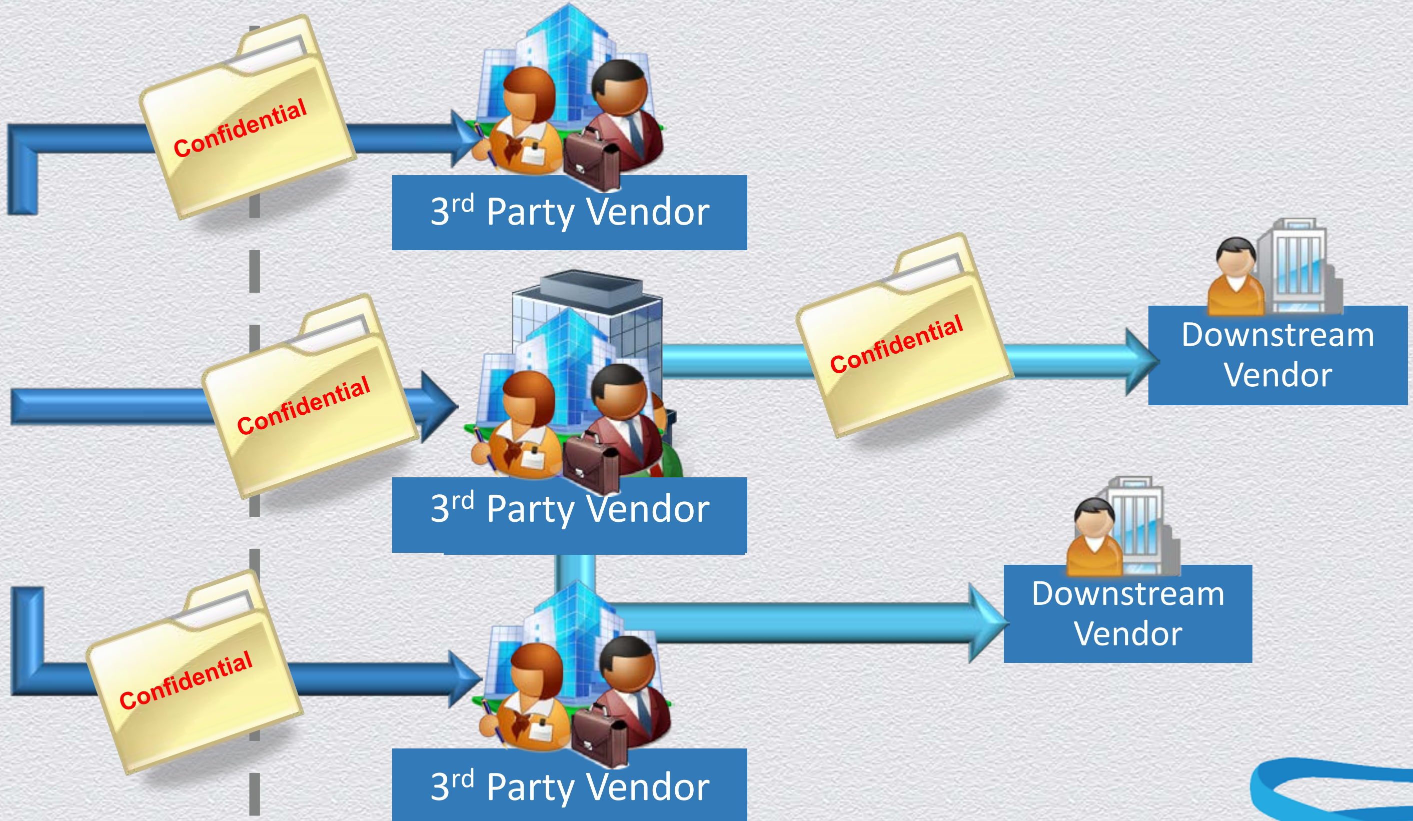
"Institutions under the jurisdiction of the CFPB will have to evaluate the risk profile of vendors and retain evidence of risk & compliance activities of those 3rd parties," *Risk & Compliance Journal 12/2/13*

The Office of the Comptroller of Currency (OCC) issued new standards and requirements for banks regarding the upfront and ongoing management of third party risk – *October 2013*

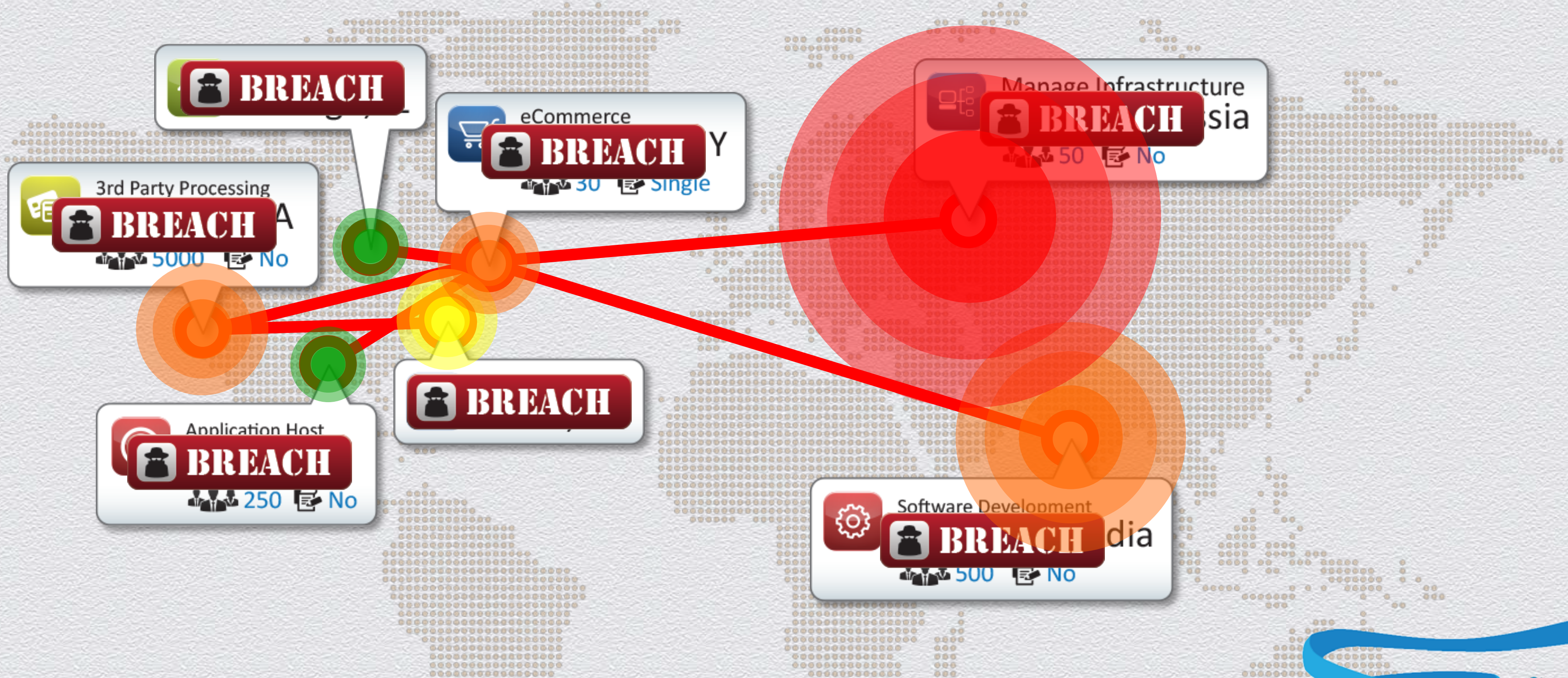
Improving vendor mgmt is a top security priority for institutions in 2014…Third-party relationships are becoming more complex as more functions are outsourced to the cloud – *Bank Info Security 11/2013*



The Data Supply Chain



Who Moved My… Data? (based on a true story)



BREACH

3rd Party Processing

BREACH A

5000 No

eCommerce

BREACH Y

30 Single

Manage Infrastructure

BREACH sia

50 No

BREACH

Application Host

BREACH

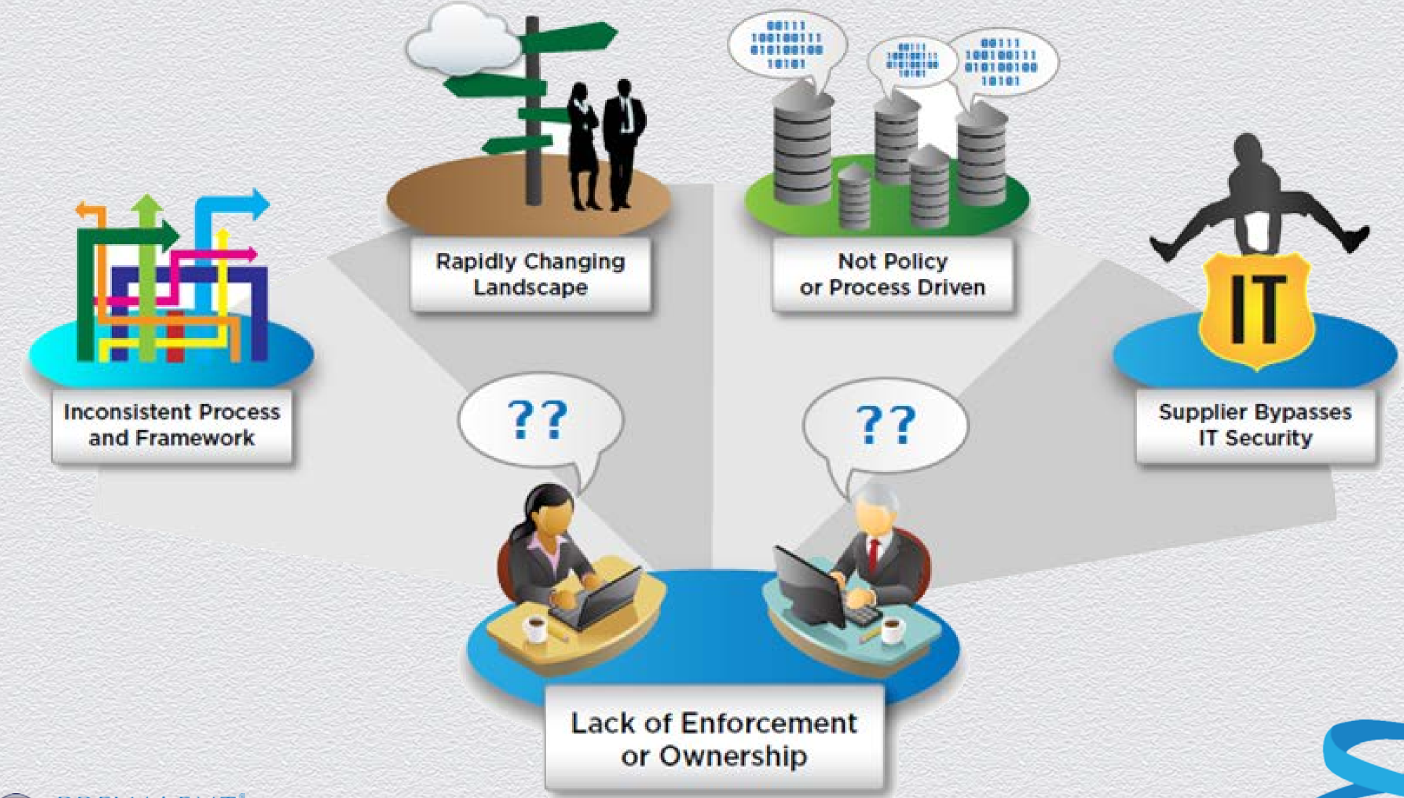
250 No

Software Development

BREACH dia

500 No

The Vendor Risk Management Problem



Rapidly Changing Landscape

Not Policy or Process Driven

Inconsistent Process and Framework

Supplier Bypasses IT Security

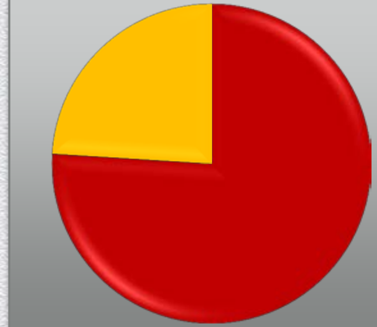
Lack of Enforcement or Ownership

Interesting Statistics

Only 24%

of respondents require third-party suppliers or partners to comply with baseline security procedures

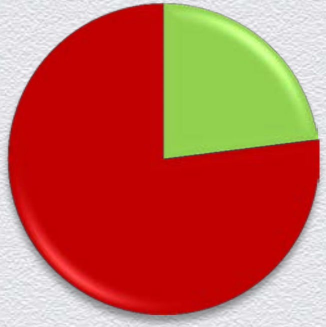
– PWC Third Party Risk Management April 2012



76% of data breaches

analyzed by TrustWave resulted from a third-party which introduced the security deficiencies that were ultimately exploited.

– Trustwave 2012 Global Security Report

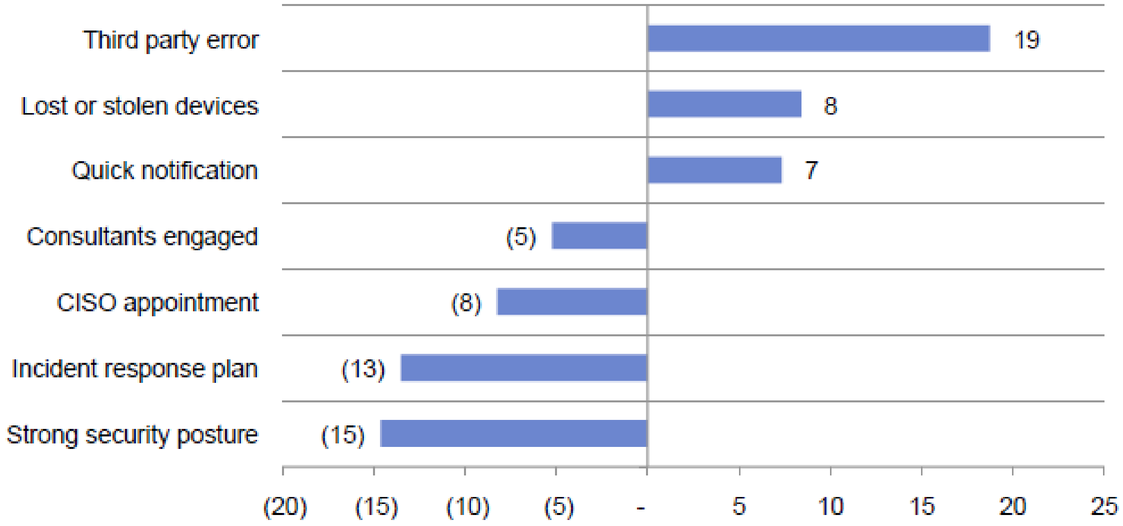


less than 1 in 5 enterprises are conducting security assessments from 3rd parties —Veracode 2012 State of Software Security Report

3rd Party Error and Data Loss Cost

As shown in Figure 9, a strong security posture, incident response planning CISO appointments and consulting support decreases the per capita cost of data breach (shown as negative numbers). Third party errors, lost or stolen devices and quick notifications increases the per capita cost of data breach (shown in positive numbers).

Figure 9. Impact of seven factors on the per capita cost of data breach
Consolidated view (n=277).
Measured in US$



Source: 2013 Cost Data Breach Study; Ponemon Institute; May 2013

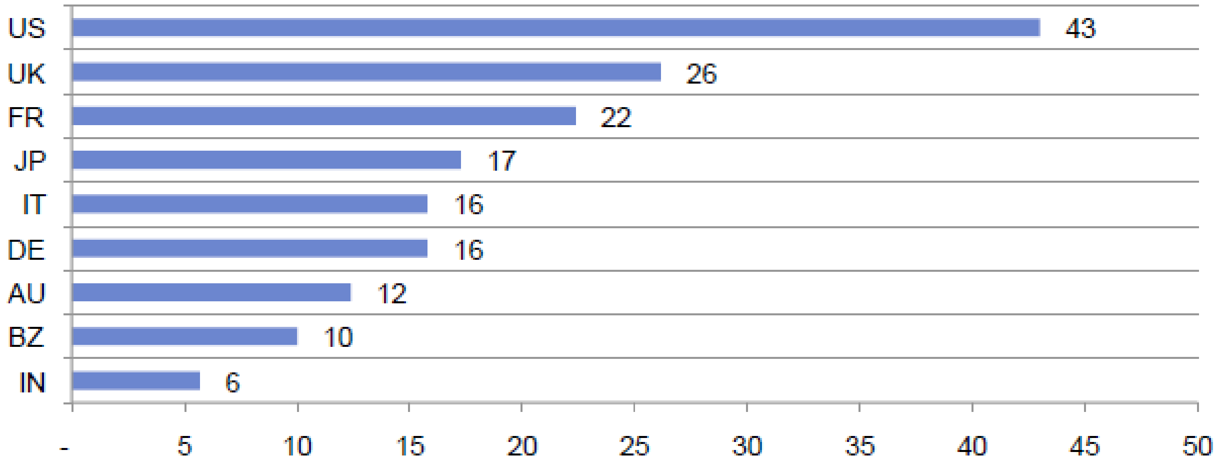
SHARED ASSESSMENTS

PREVALENT® networks

3rd Party Error and Data Loss Cost

Figure 11a, 11b and 11c show the factors that increased the cost of data breach, On average, third party errors increased the cost of data breach by as much as $43 per record in the US. In the case of Brazil and India, such incidents increased the cost by only $10 and $6, respectively.

Figure 11a. Third Party Error (US$)



Source: 2013 Cost Data Breach Study; Ponemon Institute; May 2013

Recommendations

- Assess before you buy!
- Understand and improve program maturity.
- Standardize your content.
- Automate wherever possible.
- Align with the business and other stakeholders.
- Get audit rights in contract.
- Move away from single, point-in-time assessment.
- Monitor regularly.

The “SIG”

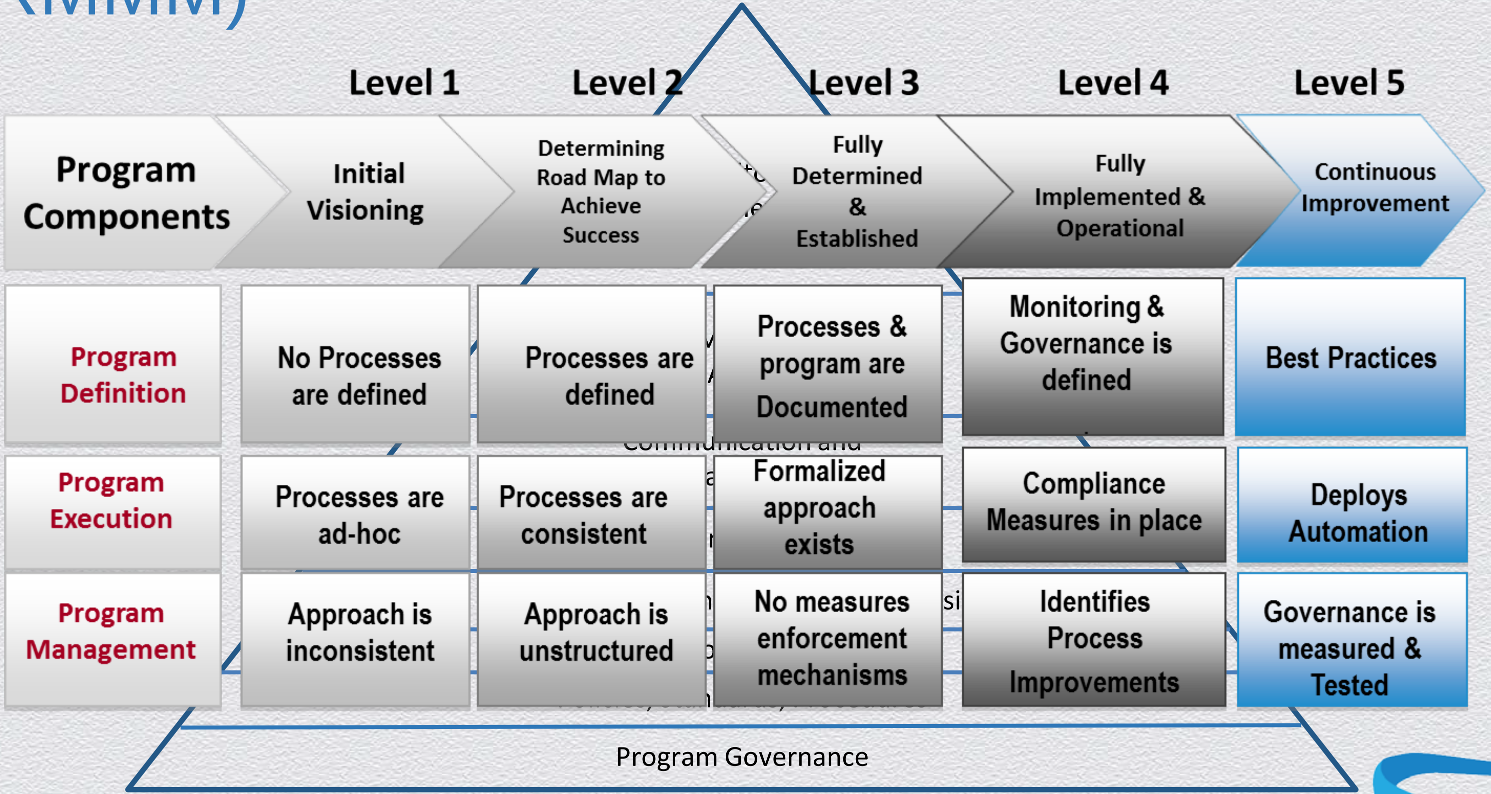
- Standardized Information Gathering Questionnaire
  - Replaces proprietary outsourcer questionnaires (1000s to 1)
  - Complete picture of service provider controls

NEW for 2014 - an entirely new section for assessing a vendor’s software security development lifecycle, and the expansion of questions related to service provider outsourcing (fourth-party risks).

Shared Assessments Tools and Other Considerations

- The 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.
  - New for 2014 - a new AUP Report Template allows users of the AUP to track the results of an AUP assessment and generate a clear and concise report of assessment results.
- The Vendor Risk Management Maturity Model (VRMMM)
  - Incorporates vendor risk management best practices into a usable model, which can be used to assess the current and desired future state
  - New for 2014 - New enhancements to the VRMMM include the ability to score program components to indicate those areas that are currently under development and provide tracking of program improvements over time. The Model now includes a dashboard that displays scores for each component; each foundational program area; and, an overall maturity score for the program.

Vendor Risk Management Maturity Model (VRMMM)



	Level 1	Level 2	Level 3	Level 4	Level 5
Program Components	Initial Visioning	Determining Road Map to Achieve Success	Fully Determined & Established	Fully Implemented & Operational	Continuous Improvement
Program Definition	No Processes are defined	Processes are defined	Processes & program are Documented	Monitoring & Governance is defined	Best Practices
Program Execution	Processes are ad-hoc	Processes are consistent	Formalized approach exists	Compliance Measures in place	Deploys Automation
Program Management	Approach is inconsistent	Approach is unstructured	No measures enforcement mechanisms	Identifies Process Improvements	Governance is measured & Tested

The Future of 3rd Party Risk

- Vendor Risk to 3rd Party Oversight
  - Security + Operational Risk + SLA Management
- Big Data Analytics and Continuous Monitoring
- Application Security In The Spotlight
- Additional Regulatory and Privacy Coverage
- Additional Sharing Among Peers
  - AUP Pilots
  - ISACs

RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank you!

Come Visit Us at Booth #1038