DO THEY MEASURE UP?
Assessing the Security Posture of 3rd Party Service Providers

David Escalante – Boston College
Shirley Payne – University of Virginia
Kevin Savoy – University of Virginia
Miguel Soldi - The University of Texas System

April 5, 2011, 10:30am
AGENDA

- Introduction – “Trust me, what could go wrong…?”
  - Why are 3rd Party Risk Assessments Important?
  - A Word About SAS 70
  - Available Options - Build, Adapt, or Adopt
- Shared Assessments
- The UVA Way
  - Concerns
  - Solutions
- Questions and Answers
“TRUST ME, WHAT COULD POSSIBLY GO WRONG?”

- Patient records stolen from vendor employee costs university 3.3 million
- Subcontractor employee assisting university with patient billing and collections is arrested and charged with identity theft
- Unbeknown to a university, patient records end up in a foreign country and are held up for ransom
- Your horror story here?
WHY 3rd PARTY ASSESSMENTS ARE IMPORTANT

- Contractual issues and assessment issues
- Increasing reliance on 3rd party service providers to maintain, manage, transmit, or store institution-owned data (i.e., Cloud, SaaS, etc)
- To assess and define the incremental risk to the institution of outsourcing a service or function prior to engaging a 3rd party service provider
- To ensure that adequate security controls are in place prior to finalizing any contract agreement

To Determine if They Measure Up to Your Standards
A WORD ABOUT SAS 70

- Designed basically for auditor-to-auditor communication
- It is not based on any security standard
- Objectives and parameters are stated by the client, not the auditor
- It is an audit report, not a certification (i.e., Can’t be “SAS 70 certified”)
- SAS 70 replacements - SSAE-16 and ISAE-3402 - do not fix any of these issues
AVAILABLE OPTIONS

- **Build**
  - Home-grown and tailor-made
  - Meets all institutional requirements for topics, level of detail, and format

- **Adapt**
  - Start with commercial or peer tool and modify to suit institutional needs
  - Not perfect but meets most institutional requirements

- **Adopt**
  - Use a commercial or peer tool as is
  - May not meet all institutional requirements
  - Quickest way to get started
AVAILABLE OPTIONS

- **Build**
  - Home-grown and tailor-made
  - Meets all institutional requirements for topics, level of detail, and format

- **Adapt**
  - Start with commercial or peer tool and modify to suit institutional needs
  - Not perfect but meets most institutional requirements

- **Adopt**
  - Use a commercial or peer tool as is
  - May not meet all institutional requirement
  - Quickest way to get started
WHAT IS THE SHARED ASSESSMENTS PROGRAM

Program created by industry leaders to provide a standardized, risk based approach to assess service provider control environments in a rational, cost-effective manner
ONE STOP SHOP

ISO 27002  PCI-DSS  HIPAA/HITECH
COBIT  AICPA  FFIEC
NIST  GLBA  UCF

TWO ASSESSMENT TOOLS
- The Standardized Information Gathering Questionnaire (SIG)
- The Agreed Upon Procedures (AUP)
ASSESSMENT TOOL: THE “SIG”

Standardized Information Gathering Questionnaire

- Replaces proprietary outsourcer questionnaires (1000s → 1)
- Excel format
- Complete picture of service provider controls
- Risk tiered
- Maps to standards (HIPAA, ISO, COBIT, PCI, NIST, FFIEC)
- XML supported
- Free download at www.sharedassessments.org
THE SIG VERSION 6 (2010)

- Procedures for cloud computing and SaaS
- Standards correspond to ISO, PCI DSS, HIPAA/HITECH, COBIT, NIST and FFIEC guidance
- New privacy procedures correspond with AICPA/CICA standards
- Scoring option for analysis and reporting
- Information Gathering Questionnaire Lite

©2010 The Shared Assessments Program. All Rights Reserved
THE SIG VERSION 6 – TAB TOPICS

The SIG Questionnaire covers the topics below and is available in two “flavors”:
- The complete SIG Questionnaire is very comprehensive and includes about 700 questions
- The SIG Lite Questionnaire covers “the basics” for each topic and includes about 90 questions

<table>
<thead>
<tr>
<th>Business Information</th>
<th>Communications and Ops Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>Access Control</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Info Sys AD&amp;M</td>
</tr>
<tr>
<td>Security Policy</td>
<td>Incident Event and Comm Mgmt</td>
</tr>
<tr>
<td>Organizational Security</td>
<td>BC /DR</td>
</tr>
<tr>
<td>Asset Management</td>
<td>Compliance</td>
</tr>
<tr>
<td>Human Resource Security</td>
<td>Additional Questions</td>
</tr>
<tr>
<td>Physical and Environmental</td>
<td>Privacy</td>
</tr>
</tbody>
</table>

©2010 The Shared Assessments Program. All Rights Reserved
## SIG Lite

<table>
<thead>
<tr>
<th>Question/Request</th>
<th>Response</th>
<th>Additional Information</th>
<th>AUP Reference</th>
<th>SO Ref Num</th>
<th>SO Ref Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig LITE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### A. Risk Assessment and Treatment

| SL.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? | | A.1 IT & Infrastructure Risk Governance and Context | 4.1 | Assessing Security Risks |

### B. Security Policy

| SL.2 | Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? | | B.1 Information Security Policy | 5.1.1 | Information Security Policy Document |

| SL.3 | Have the policies been reviewed in the last 12 months? | | B.2 Information Security Policy Maintenance | 5.1.2 | Review of Information Security Policy |

### C. Organisational Security

| SL.4 | Is there an information security function responsible for security initiatives within the organization? | | C.1 Information Security Policy | 6.1.1 | Management commitment to information security |

| SL.5 | Do external parties have access to Scooped Systems and Data or processing facilities? | | C.2 Information Security Policy | 6.2 | External parties |

### D. Asset Management

| SL.7 | Is there an asset management policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? | | D.1 Information Security Policy | 7.1 | Responsibility for Assets |

| SL.8 | Are information assets classified? | | D.2 Information Security Policy | 7.2.1 | Classification Guidelines |

### E. Human Resource Security

| SL.9 | Are security roles and responsibilities of constituents defined and documented in accordance with the organization’s information security policy? | | E.1 Information Security Policy | 8.1.1 | Roles and responsibilities |

| SL.10 | Is a background screening performed prior to allowing constituent access to Scooped Systems and Data? | | E.2 Background Investigation Policy Content | 8.1.2 | Screening |

| SL.11 | Are new hires required to sign any agreements upon hire? | | E.3 Background Investigation Policy Content | 8.1.3 | Terms and conditions of employment |

| SL.12 | Is there a security awareness training program? | | E.4 Security Awareness Training Program | 8.2.2 | Information security awareness, education, and training |

| SL.13 | Is there a disciplinary process for non-compliance with information security policies? | | E.5 Security Awareness Training Program | 8.2.3 | Disciplinary process |

| SL.14 | Is there a constituent termination or change of status process? | | E.6 Security Awareness Training Program | 8.3.1 | Termination responsibilities |

### F. Physical and Environmental Security

| SL.16 | Are there physical security controls present in the building/area that contains Scooped Systems and Data? | | F.1 Physical Security Controls – Scooped Systems and Data | 9.1.1 | Securing offices, rooms, and facilities |

| SL.17 | Are visitors permitted in the facility? | | F.2 Physical Security Controls – Scooped Systems and Data | 9.1.2 | Physical entry controls |

### G. Communications and Operations Management

| SL.18 | Are there approved operating procedures utilized? | | G.1 Information Security Policy | 10.1.1 | Documented Operating Procedure |
### G. Communications and Operations Management

<table>
<thead>
<tr>
<th>Question/Request</th>
<th>Response</th>
<th>Additional Information</th>
<th>AUP Reference</th>
<th>ISO Ref Num</th>
<th>ISO Ref Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>59 G.6.2.0.3</td>
<td>Verification of receipt?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60 G.9</td>
<td>Are there external network connections (internet, extranet, etc.)? If so, is there:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61 G.6.1</td>
<td>Security and hardening standards for network devices (baseline configuration, patching, passwords, access control)?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62 G.9.1.1</td>
<td>Regular review and/or monitoring of network devices for continued compliance to security requirements?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63 G.9.2</td>
<td>Is every connection to an external network terminated at a firewall?</td>
<td></td>
<td>G.17 Network Security – Firewalls</td>
<td>10.6.3.a</td>
<td>Exchange Agreements</td>
</tr>
<tr>
<td>64 G.9.3</td>
<td>Are network devices configured to prevent communications from unapproved networks?</td>
<td></td>
<td>G.17 Network Security – Firewalls</td>
<td>11.4.6</td>
<td>Segregation in Networks</td>
</tr>
<tr>
<td>65 G.9.4</td>
<td>Do network devices deny all access by default?</td>
<td></td>
<td>G.17 Network Security – Firewalls</td>
<td>11.4.5</td>
<td>Segregation in Networks</td>
</tr>
<tr>
<td>66 G.9.6</td>
<td>Is there a process to request, approve, log, and review access to networks across network devices?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67 G.9.6.1</td>
<td>Do logs contain failed login attempts, disabling of audit logs, changes, timestamps, IP info, etc?</td>
<td></td>
<td>G.4 Network Logging</td>
<td>10.6.1.d</td>
<td>Network Controls</td>
</tr>
<tr>
<td>68 G.9.6.2</td>
<td>Is the overwriting of audit logs disabled?</td>
<td></td>
<td>G.4 Network Logging</td>
<td>10.6.1.d</td>
<td>Network Controls</td>
</tr>
<tr>
<td>69 G.9.6.3</td>
<td>Are the logs from network devices aggregated to a central server?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70 G.9.6.4</td>
<td>Are security patches reviewed and applied to network devices?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71 G.9.6.5</td>
<td>Is there an approval process prior to installing a network device?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73 G.9.10</td>
<td>Is there a process to prevent unauthorized devices from physically connecting to the internal network?</td>
<td></td>
<td>G.17 Network Security – Firewalls</td>
<td>11.4.6</td>
<td>Segregation in Networks</td>
</tr>
<tr>
<td>74 G.9.11</td>
<td>Are internal systems required to pass through a content filtering proxy prior to accessing the Internet?</td>
<td></td>
<td>G.3 Externally Facing Open Administrative Ports</td>
<td>11.4.6</td>
<td>Access Control Policy</td>
</tr>
<tr>
<td>75 G.9.12</td>
<td>Is there an approval process to allow extranet connections?</td>
<td></td>
<td>G.4 Network Logging</td>
<td>11.3.1.d</td>
<td>Policy On Use Of Network Services</td>
</tr>
<tr>
<td>76 G.9.13</td>
<td>Are insecure protocols (telnet) used to access network devices?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77 G.9.14</td>
<td>Is access to diagnostic or maintenance ports on network devices restricted?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78 G.9.15</td>
<td>Is there a separate network segment or endpoints for remote access?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79 G.9.16</td>
<td>Are firewall rules and network access control lists regularly reviewed?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
USING THE SIG IN HIGHER EDUCATION

- **PRO**: Provides a standardized framework to center 3rd party assessments on
  - Standards are more defensible than roll-your-own
  - Saves work of developing your own from scratch
  - Provides great detail, probably more than any effort you would develop yourself

- **CON**: Questions may not be appropriate (or may be inadequate) for your institution

- **CON**: Significant level of detail can be more work to go through

- **Note**: Shared Assessments BoF tonight from 8:30-10:00
ASSESSMENT TOOL: THE “AUP”

Agreed Upon Procedures

 Framework for auditing 3rd parties
   If already done and available, significant supplement to SAS-70 type documents

 Objective test of controls, validation, and report of results

 Outsourcers view results in the context of their risk management requirements

 Free download: www.sharedassessments.org

©2010 The Shared Assessments Program. All Rights Reserved
CONCERNS TO ADDRESS

- IT services outsourced without adequate risk assessments
- 3rd parties not contractually bound to consistent security/privacy standards; some not to any at all
- No means to assure compliance

Bottom line: unacceptable risks associated with use of 3rd parties for critical services and sensitive data handling
WE NEEDED TO...

- Enhance project-based risk assessment
- Preserve the institution’s legal rights regarding protection and use of its data
- Increase assurance that audit compliance would persist over the long term
UVA SOLUTION #1

- Standard security, privacy, and audit risk assessment tool for IT projects
  - addresses risks associated with projects of all types, particularly those involving 3rd parties
  - supplements and integrates with the university-wide IT Security Risk Management Program that departments already use to assess risks to all IT assets critical to their missions
COMPLEXITIES

- Two central security offices (Academic Division, Medical Center)
- Existing models & standards¹ did not fit our need
- Fear of “extra work” for IT project teams

¹ Ex: NIST SP 800-39 Managing Information Security Risk
PROJECT SECURITY RISK ASSESSMENT TOOL COMPONENTS

1. Describe outsourcing plans
   - Helps determine requirements to include in RFP and negotiated contracts

2. Indicate data classification
   - Determines baseline security requirements to address during project

3. Describe data access requirements
   - Helps determine if additional (beyond baseline) access controls must be applied

4. Conduct data risk assessment
   - Helps determine if additional (beyond baseline) data protection requirements must be applied
5. Establish security architecture plan
  • Ensures network/server security architecture is designed and its implementation is scheduled in a timely manner

6. Describe audit strategy
  • Incorporates system capabilities for work flow audits and security event logging

7. Categorize planned information systems
  • Correlates new system to critical business functions of user departments

8. Describe mission continuity requirements
  • Determines if user departments must alter their mission continuity plans to accommodate new system
UVA SOLUTION #2

- Standard security, privacy and audit contract language tool
  - used for contractual agreements with 3rd parties receiving institutional data and/or providing key IT services
  - informed by Data Protection Contractual Language resource developed by the Higher Education Information Security Council
  - leverages the NACUA/CSG Shared Services Working Group Model Contract effort
COMPLEXITIES

- Two central security offices and two procurement offices (Academic Division, Medical Center)
- Alignment with pre-existing Business Associates Agreement for HIPAA-covered data
- Accommodation of grant obligations and data sharing agreements among research collaborators
- Vendor resistance to on-site audit reviews
CONTRACTUAL LANGUAGE TOOL

- Common set of data-related terms and conditions
  - Mandatory and recommended T&Cs
  - Extension of existing general T&C boilerplates
- Selection varies depending upon nature of procurement
- Wording adjustments may be necessary for individual procurements
- Not complete replacement for consultation
CONTRACTUAL LANGUAGE TOOL

- Definitions
- Rights and license in and to university and end user data
- Intellectual property rights/disclosure
- Data privacy
- Data security
- Data integrity
- Audits
- Data compromise response
- Response to legal orders, demands or request for data
- Data retention, disposal, and legal holds
- Data transfer upon termination or expiration
- Compliance with applicable laws and customer policies
- Subcontracting
- Survival of terms
APPROACH THAT MADE WORK DOABLE

- Cross disciplinary task forces:
  - Project risk assessment tool developed by Security, Audit, Application Development, System Architecture
  - Contractual language tool developed by Security, Audit, Procurement, Legal Counsel

- Leveraged national level resources
  - Power in many institutions specifying same requirements

- Well-understood need for timely risk assessment and strong data protection agreements – critical for us and for our vendor partners
ADDITIONAL RESOURCES

- **BOF Session on Shared Assessments Tool:**
  Tonight, 8:30 PM - 10:00 PM, Texas Ballroom AB/Fourth Level

- **EDUCAUSE Data Protection Contractual Language Toolkit**

- **CSG-NACUA Shared Services Working Group – Model Contract**

- **UVa Project Security Risk Assessment Tool**
  [http://itc.virginia.edu/security/riskmanagement/project](http://itc.virginia.edu/security/riskmanagement/project)

- **UVa Data Protection Contractual Language Tool**
  [http://itc.virginia.edu/security/dataprotection/contracts](http://itc.virginia.edu/security/dataprotection/contracts)
QUESTIONS AND ANSWERS
THANK YOU