Strategies for Streamlining Security Assessments using HECVAT
Presenters

Jon Allen
Interim CIO and CISO
Baylor University

Josh Callahan
Information Security Officer and CTO
Humboldt State University

Susan Coleman
Peer Assessment Program Mgr/Lead Security Analyst
REN-ISAC

Charlie Escue, CISSP
Extended Information Security Manager
Indiana University

Nick Lewis
Program Manager
Internet2
Welcome and Introductions
Welcome and Introductions

- Your name, your school, why you’re here
- Where are you in your cloud journey?
- When you say infosec, what do you mean?
- When you say cloud, what do you mean?
Report Out

• Are you using HECVAT? If not, why not?
• Summary of the discussion
• What do you want to get out of this workshop?
Resources

• HECVAT website:
  • https://www.educause.edu/hecvat

• Cloud Broker Index:
  • https://www.ren-isac.net/hecvat

• Session Resources:
  • SPC ‘19 Website

Workshop Slides: http://go.iu.edu/2aED
Workshop Demo: http://go.iu.edu/2aEu
Agenda

- Background
- HECVAT Overview
- Deep Dive on the Tool!
- Work Through an Assessment
- Vendor and Service Provider Aspects
- Lunch
Agenda

- Check-in after lunch
- Role playing game
- Developing a Comprehensive Vendor Assessment Program
- Campus Examples
- Group Consulting
- Wrap-up and Questions
Conference Session

- Will be a subset of this workshop
- Hoping you become an evangelist
- Bring peers and colleagues even in other areas
- Tuesday at 1:00pm
  Vevey 4, Second Floor Event Centre
Background
Cloud Strategy

- Do you have a cloud strategy?
- Is the concept still valid?
- Changes that the cloud caused
What the HECVAT!

- History
- Unique collaboration
- Ongoing Project
Campuses are rapidly adopting cloud services and deploying software systems

Assessing the risk for cloud services and software systems as quickly as possible

Developing vendor risk management programs

Developing enterprise risk management programs

Too much to do to effectively do it all!
The Job to Be Done

• How to as easily and quickly as reasonably possible share work done at one campus with other campuses
• Freeing up time & resources to dedicate back to critical information security functions
• Create a forum/space to share and find existing shared assessments
• Build on the existing higher education information security community sharing
• Ease vendor burden in responding to security and privacy product assessment requests
What the HECVAT!

The project is three years old

A win for schools and vendors

Simplify, Expedite, Improve Assessments
The HECVAT working group is the best!
Phase 3 Contributors

- Jon Allen, Baylor University
- Josh Callahan, Humboldt State University
- Charles Escue, Indiana University
- Jeff Hopkins, Purdue University
- Alex Jalso, West Virginia University
- Amanda Sarratore, Notre Dame
- Gary Taylor, York University
- Gene Willacker, Michigan State University
- David Zeichick, California State University-Chico
- Staff Liaisons from EDUCAUSE, Internet2, and REN-ISAC
  - Valerie Vogel, Nick Lewis, Todd Herring, Kim Milford, Susan Coleman
American University
Appalachian State University
Art Institute of Chicago
Baylor University
Berry College
Boston College
Bowling Green State University
Brown University
California Baptist University
California State University, all Campuses and System
Carnegie Mellon University
Carthage College
Champlain College
Clarkson University
Cornell University
Davidson College
Denison University
DeSales University
Drake University
Drexel University
Duquesne University
East Carolina University
Ferris State University
Foothill-De Anza Community College District
Franklin & Marshall College
Georgia Institute of Technology
Hillsborough Community College
Indiana University
Indiana Wesleyan University
John Carroll University
Kent State University
LeTourneau University
Linfield College
Marylhurst University
Miami University
Morgan State University
Northern Arizona University
Oakland University
Ohio Northern University
Oregon State University
Pepperdine University
Princeton University
Radford University
Rice University
Rutgers University
Southern Alberta Institute of Technology
Stony Brook University
Suffolk County Community College
Susquehanna University
Troy University
Truman State University
University of California, Davis
University of Delaware
University of Maine System
University of Maryland Baltimore
University of Massachusetts Amherst
University of Oregon
University of Portland
University of Richmond
University of Tennessee, Knoxville
West Virginia University
Western Carolina University
Western Michigan University
William & Mary
Williams College
Yavapai College
HECVAT Overview
Updates in the last year

- Updated HECVAT Questionnaire
- Crosswalk Updates
- Cloud Broker Index (CBI)
Phase 3 Deliverables

• Engage vendors
  • For HECVAT awareness
  • CBI participation
• Automated triage
HECVAT Improvement Debrief

Crosswalk
Score
Assess
Report
Standardize
Crosswalk

- Added PCI DSS!
- CIS Critical Controls
- HIPAA
- ISO:27002:2013
- NIST Cybersecurity Framework
- NIST 800-171r1
- NIST 800-53r4
Call to Community

- Commit to HECVAT
- Allow referencing
  - https://docs.google.com/forms/d/e/1FAIpQLSe7utsnnriOh_ARp-szZ5sVgN7sak6m-94rFuf0QkgoSMK5SA/viewform
- Educate Vendors
- Give feedback
Future Direction - Phase 4

- Governance
- Strategies
- Workplan

- Contract Language
- Report Templates
- Documentation
- "On-Prem" HECVAT

- Partnerships
- Privacy
- Accessibility
- Other SMEs

- Collaboration
- Communications
- Feedback
- Outreach
Deep Dive On Using The Tool
The use of Data Zones makes the HECVAT an international tool.

### Definitions and Data Zones

<table>
<thead>
<tr>
<th>Institution</th>
<th>Any school, college, or university using the Higher Education Cloud Vendor Assessment Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institution Data Zone</td>
<td>The country/region in which an Institution is located, including all laws and regulations in-scope within that country/region.</td>
</tr>
<tr>
<td>Vendor Data Zone</td>
<td>The country/region in which a vendor is headquartered and/or serves its products/services, including all laws and regulations in-scope within that country/region.</td>
</tr>
</tbody>
</table>

Customers from different regions may expect varying protections of data (e.g. GDPR); this is the Institution Data Zone. Vendors may handle data differently depending on the country or region where data is stored, this is the Vendor Data Zone. As a vendor, if your security practices vary based on your region of operation, you may want to populate a HECVAT in the context for each security zone (strategy). That said, Institutions from different data zones may still use vendor responses from other state Data Zones. If your security practices are the same across all regions of operations, indicate "All" in your Vendor Data Zone.

**Example A:** If vendor ABC is headquartered and stores data in Canada, and provides services to only customers in Canada, ABC should state "Canada" in both Data Zone fields.

**Example B:** If vendor ABC is headquartered and stores data in Canada, and additionally provides services to customers in the United Kingdom, ABC may want to assure customers in the United Kingdom that their data is handled properly for their region. In that case, ABC should state "Canada" in the Vendor Data Zone and "United Kingdom" in the institution Data Zone.

**Example C:** If your security strategy is broad and doesn’t fit this statement model, provide a brief summary in each field and the Institution’s Security Analyst can assess your response.
Vendor guidance improves responses

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Vendor Answers</th>
<th>Additional Information</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOCU-01 Have you undergone a SSAE 16 audit?</td>
<td>No</td>
<td></td>
<td>Describe any plans to undergo a SSAE 16 audit.</td>
</tr>
<tr>
<td>DOCU-02 Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?</td>
<td>Yes</td>
<td></td>
<td>Please include a copy with your response and include a URL for the published assessment.</td>
</tr>
<tr>
<td>DOCU-03 Have you received the Cloud Security Alliance STAR certification?</td>
<td>No</td>
<td></td>
<td>Describe any plans to obtain CSA STAR certification.</td>
</tr>
<tr>
<td>DOCU-04 Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)</td>
<td>No</td>
<td></td>
<td>Describe any plans to conform to an industry standard security framework.</td>
</tr>
<tr>
<td>DOCU-05 Are you compliant with FISMA standards?</td>
<td>Yes</td>
<td></td>
<td>Indicate level, agency issuing ATO, and necessary details on ATO. If using FEDRamp, please indicate the supporting details.</td>
</tr>
<tr>
<td>DOCU-06 Does your organization have a data privacy policy?</td>
<td>No</td>
<td></td>
<td>Describe your plans to provide a data privacy document.</td>
</tr>
</tbody>
</table>
Vendor response expectations were clarified

<table>
<thead>
<tr>
<th>Qualifiers</th>
<th>Vendor Answers</th>
<th>Additional Information</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qual-01 Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qual-02 Does the vended product host/support a mobile application? (e.g. app)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qual-03 Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qual-04 Do you have a Business Continuity Plan (BCP)?</td>
<td>No</td>
<td></td>
<td>Respond to as many questions in the Business Continuity section as possible.</td>
</tr>
<tr>
<td>Qual-05 Do you have a Disaster Recovery Plan (DRP)?</td>
<td>No</td>
<td></td>
<td>Respond to as many questions in the Disaster Recovery section as possible.</td>
</tr>
<tr>
<td>Qual-06 Will data regulated by PCI DSS reside in the vended product?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qual-07 Is your company a consulting firm providing only consultation to the Institution?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Aligning reports to industry standards assist in the HECVAT integration process

### HECVAT: Assessment Report for Analysts

#### Version 2.0

<table>
<thead>
<tr>
<th>HEISC Shared Assessments Working Group</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor Name</strong></td>
<td><strong>Product Name</strong></td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Product Name and Version Information</td>
</tr>
<tr>
<td><strong>Vendor Contact Name</strong></td>
<td><strong>Product Description</strong></td>
</tr>
<tr>
<td>Vendor Contact Name</td>
<td>Brief Description of the Product</td>
</tr>
<tr>
<td><strong>Vendor Contact Title</strong></td>
<td><strong>HECVAT Version</strong></td>
</tr>
<tr>
<td>Vendor Contact Title</td>
<td>Full</td>
</tr>
<tr>
<td><strong>Vendor Email Address</strong></td>
<td><strong>Date Prepared</strong></td>
</tr>
<tr>
<td>Vendor Contact E-mail Address</td>
<td>mm/dd/yyyy</td>
</tr>
<tr>
<td><strong>Institution's Security Framework</strong></td>
<td><strong>NIST Cybersecurity Framework</strong></td>
</tr>
</tbody>
</table>

#Security19
The Analyst Report provides function to move qualitative results into quantitative

<table>
<thead>
<tr>
<th>ID</th>
<th>Question</th>
<th>Vendor Answer</th>
<th>Compliant?</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP-01</td>
<td>Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>COMP-02</td>
<td>Describe how long your organization has conducted business in this product area.</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>COMP-07</td>
<td>Use this area to share information about your environment that will assist those who are assessing your company data security program.</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>APPL-07</td>
<td>What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution’s data?</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>APPL-09</td>
<td>Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>APPL-10</td>
<td>Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>APPL-12</td>
<td>Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>APPL-13</td>
<td>Are there any OS and/or web-browser combinations that are not currently supported?</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
The new HECVAT scoring function provides an excellent starting point for evaluation efforts.

<table>
<thead>
<tr>
<th>ID</th>
<th>Question</th>
<th>Additional Info</th>
<th>High Risk</th>
<th>Category</th>
<th>C_Answer</th>
<th>Required</th>
<th>V_Answer</th>
<th>Compliant</th>
<th>Weight</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOCU-01</td>
<td>Have you undergone a SSAE 16 audit?</td>
<td>0</td>
<td>FALSE</td>
<td>Documentation</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>DOCU-02</td>
<td>Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?</td>
<td>0</td>
<td>FALSE</td>
<td>Documentation</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>DOCU-03</td>
<td>Have you received the Cloud Security Alliance STAR certification?</td>
<td>0</td>
<td>FALSE</td>
<td>Documentation</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>DOCU-04</td>
<td>Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)</td>
<td>0</td>
<td>TRUE</td>
<td>Documentation</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>DOCU-05</td>
<td>Are you compliant with FISMA standards?</td>
<td>0</td>
<td>FALSE</td>
<td>Documentation</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>DOCU-06</td>
<td>Does your organization have a data privacy policy?</td>
<td>0</td>
<td>TRUE</td>
<td>Documentation</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>THRD-01</td>
<td>Describe how you perform security assessments of third party companies</td>
<td>0</td>
<td>TRUE</td>
<td>Third-Parties</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>THRD-02</td>
<td>Provide a brief description for why each of these third parties will have</td>
<td>0</td>
<td>TRUE</td>
<td>Third-Parties</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>THRD-03</td>
<td>What legal agreements (i.e. contracts)</td>
<td>0</td>
<td>TRUE</td>
<td>Third-Parties</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>THRD-04</td>
<td>Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.</td>
<td>0</td>
<td>TRUE</td>
<td>Third-Parties</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
</tbody>
</table>
The Summary Report gives a quick view of a vendor's security state
Automated Triage – Live Demo!

- Collecting the data
- Assessing the risk
- Example going through automated scoring
- How to convert and do scoring
- Look on weighted questions
LIVE DEMO!
Working Through An Assessment
10am Break and Feedback Check – return at 10:30am
Working Through An Assessment Continued
Working With a Vendor/Service Provider
SPs and Vendors Using the HECVAT

• Why it’s so important for them and the community
• Help us sell this to SPs and vendors
SPs and Vendors Including HECVAT

• SP/vendors including the HECVAT questionnaire in their tool(s)
  • The licensing allows this for free
  • Potentially in GRC/ITGRC tools
  • Managing the questionnaire files and workflows across campus
    • Could be one of many different files collected
SPs and Vendors Completing the HECVAT

- Benefits to the SP/vendor
- Benefits to the campus
- Benefits to the community
- All save time for each other’s benefit!
- More details
Vendor Partner Value

- Shows engagement in the procurement conversation
- Reduce redundant use or staff
- Increase quality of assessments
- Differentiation in the marketplace
- Being seen as engaged with the community
- Getting contacts at potential customers
Working With a Vendor/SP

- How to work with the vendor/SP
- Share with them the list of campuses
- Engage the workgroup or the community
Vendor Partner Value

@SonaSystems

@renisac You saved us many hours this week. Two universities sent their own security evaluation forms. We convinced them to accept our completed HECVAT instead.

6:05pm · 25 Jul 2018 · Twitter Web Client

2 REPLIES 1 RETWEET 4 LIKES
SPs using HECVAT in their ecosystems

• Used for the SPs using or integrating with their tools
• They can help us improve the security of their partners
Phase 4

- Working group deliverables
- Develop more community resources
- Documentation
  - What kind of additional documentation you’re looking for or would be helpful?
HECVAT & the CBI

• CBI = Cloud Broker Index
• HECVAT Phase 2
• Convenience
• Single source
• Balance accessibility with privacy
Service Providers Using HECVAT

16 Service Providers with 22 HECVATs!
Service Providers Incorporating HECVAT

5 Service Providers (so far)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product Name</th>
<th>Date of Inclusion</th>
<th>Vendor Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantiv Solutions</td>
<td>DecisionDirector for HECVAT</td>
<td>October 30, 2018</td>
<td><a href="https://advantiv.com">https://advantiv.com</a></td>
</tr>
<tr>
<td>Salty Cloud, PBC</td>
<td>Isora</td>
<td>May 8, 2019</td>
<td><a href="https://saltycloud.com">https://saltycloud.com</a></td>
</tr>
<tr>
<td>Swivl, Inc</td>
<td>Swivi Cloud</td>
<td>March 1, 2019</td>
<td><a href="https://cloud.swivl.com">https://cloud.swivl.com</a></td>
</tr>
<tr>
<td>ThirdPartyTrust</td>
<td>ThirdPartyTrust</td>
<td>April 1, 2019</td>
<td><a href="https://thirdpartytrust.com">https://thirdpartytrust.com</a></td>
</tr>
</tbody>
</table>
HECVAT & the CBI

REN-ISAC proactively reaches out to vendors

Universities working with certain vendors provide facilitation
- Please send vendors to us!
- hecvat@ren-isac.net
- We can provide scripted outreach as needed

Vendors come to REN-ISAC requesting participation
Cloud Broker Index (CBI)

Public
- Hosted and linked on REN-ISAC web site

Public2
- Vendor hosts, REN-ISAC links

Semi-Public
- Vendor hosts, REN-ISAC links
- Vendor hosts behind firescreen, sends the link and information

Private
- Vendor controls, REN-ISAC links
- Vendor keeps private, send instructions on how people can request
12pm Lunch – Return at 1pm
Questions and Discussion when returning from lunch
Enterprise File Sync & Share
Selection Roleplay
Setting the Scene

• What university are you?

• Consider the parameters of your university

• Brainstorm and select a name for the campus
Scenario Detail

• Our CIO has asked us to select a File Sync & Share Solution for the enterprise

• Or, select a new solution!
Your role at your Campus

• Study the product cards for your role
What product do you choose?

- Study Product card for your role.
- Discuss pros and cons of each with colleagues.
- Vote based on each role and consider the results.
- Come to consensus decision.
Oh those pesky users...

- Chose 2-3 Scenario cards
- Discuss if/how this changes your decision.
- Capture changes.
Lessons Learned

• Group discussion and report back

• What product did you choose?

• Did that change with the scenarios?
Oh those infosecurity people...

- Where can you find efficiencies?
- How to do this for hundreds of cloud services?
Community Perspective

• How do we share this significant work across the community?
• CBI
• Badging
• Others?
2:30pm Break – return at 3pm
Developing a Comprehensive Vendor Assessment Program
Higher Education Cloud Vendor Assessment Tool (HECVAT): Streamlining Security Risk Review

Five steps to protecting security and privacy in the cloud

“Bench”mark 1
Institution A uses HECVAT responses to ensure its service provider partners are protecting institutional systems and data appropriately.

“Bench”mark 2
Institution A wants to move to the cloud for a new LMS and identifies Wprovide123.com to fulfill that need.

“Bench”mark 3
Institution A checks the Internet2 Cloud Services listings and the REN-ISAC Cloud Broker Index to see if Wprovide123.com has completed a HECVAT questionnaire for its LMS product. It has not.

“Bench”mark 5
Institution B is looking for a new LMS, sees that Wprovide123.com has a HECVAT listed on the REN-ISAC Cloud Broker Index and contacts Wprovide123.com about its product.

HECVAT Benefits
For Institutions:
- Consistent Security Review Process
- Cost and Resource Savings

For Service Providers:
- Cost and Resource Savings
- Lead Generation

During the procurement process, Institution A encourages Wprovide123.com to complete a HECVAT for its LMS product, and to list that HECVAT in the REN-ISAC Cloud Broker Index.

Kim Milford (REN-ISAC) and Joanna Grama (EDUCAUSE)

www.educause.edu/hecvat

#Security19
Campus Partnerships
Increase Campus Involvement

- Success is dependent on campus involvement
- Shorten the review cycle
- Improve the quality of responses
Using HECVAT in Procurement
Campus Procurement

• How does campus procurement work from the IT Department perspective?

• IT Department, Information Security, and Procurement at times work closely on campus wide projects
HECVAT in Procurement

- How are campuses including HECVAT in their procurement?
- Procurement may collect the questionnaire for the infosec team to review
- Some campuses are including HECVAT in annual reviews, renewals, etc.
HECVAT in Procurement

1. Product identified
   CAMPUS DEPT

2. Procurement notified of details
   CAMPUS DEPT

3. Vendor HECVAT requested
   PROCUREMENT

4. Completed HECVAT sent to
   IT Security
   PROCUREMENT

5. Vendor notified of status
   PROCUREMENT

6. Approved?

   - Yes
     Contract engagement begins
     PROCUREMENT

   - No
     Summary findings to Data Stewards
     IT SECURITY

   HECVAT review
   IT SECURITY
Contracts

• Frame the conversation
• A key security control
• Service addendum - Top 3
Contracts - Top 3

- Location of data
- Security compliance expectations
- Notification of breach
Managing Vendor Risk

- Information Security is one aspect of managing Vendor or 3rd Party risk
- Campuses are now including information security requirements in their agreements
- HECVAT is one potential component
Assessment Report

- HECVAT gathers the information
  - Provides triage
- Communicating risk and recommendation
- Sets expectations for business and technical implementation
Example Report

- Project Overview
- Point of Contact
- System Description
Example Report continued

- Supported technologies (optional)
- System administration and authentication
- Data security
Example Report continued

- Application auditing
- Solution overview
- System
  - Hosting
  - Software
  - Content
  - On premise needs
Example Report continued

• Assumptions

• Security risks

• Recommendations
Example Report continued

- Related documents
- Summary
Review Process

• Submission
• Review
• Security Review
• Departmental Approval
Annual Reviews

• What do you need to do on a regular basis?
• Just gathering updated docs and looking for changes?
• What’s your risk tolerance and how is the SP being used on your campus?
Annual Reviews continued

- For high risk services (based on the data or operational impact), devote more resources
  - Review contracts and documentation
- For all including low risk, gather updated docs and update contact information
Annual Reviews continued

- There are tools in this space that you might want to explore
  - Cloud based tools that we’re working with in the HECVAT WG
  - GRC and ITGRC tools
- Automation, internal lists, etc
How to handle cloud integrations

- Integrating 3rd party tools into cloud services
- Assessing the security around the integrations
Other aspects

- Use InCommon, campus SSO, or campus AD
  - Implement MFA for cloud services
- Get logs into your SIEM/logging tool
- Other monitoring of the service
  - Network performance
- Secure implementation guide from vendor/SP
- SaaS, PaaS, IaaS, XaaS, and beyond
Even more aspects!

- VPAT and ADA/503 compliance
- Actual functionality evaluations!
- Significantly more aspects outside of cloud security related aspects
- Network performance
- BCDRP
- Privacy
- Don’t give up!
Case Study Examples
NET+ Case Study
How NET+ uses HECVAT

- Included in NET+ service validation
- Used by the service validation campuses to assess the security of the SP
- Annually requesting updates by the advisory board planned in future
- Encouraging SPs to list themselves in the CBI
- Examples....
NET+ information security aspects

- SSAE16, CAIQ, ISO27001, and other security docs
- Incident response
- Contracts
- Transition
- APIs
- Metadata
Baylor University Case Study
Indiana University
Case Study
The early years of assessment were primarily performed ad-hoc

Original safeguard questionnaire(s) had a technical focus

Our old ways couldn’t keep up with the new reality
We moved away from pure technical
to include strategy and business operations

• Needed a way to assess RFP responses more efficiently
• The needs of our data stewards grew with service adoption
  and with it, our process
After adopting the HECVAT, IU prioritized risk assessment process improvements

- **Standardization**: Has become a factor in our security strategy. Focusing on training to ensure analyst proficiency.
- **Operations**: Community defacto is increasing trust internally. Improved consistency across assessments.
- **Reporting**: Like many schools, we do not have a “perfect” report. HECVAT charts provide context to our data stewards.

2018 2019

Phase 4 deliverable
The HECVAT elevates our leaders confidence and improves collaboration
Working with our security peers in the community will increase our capabilities.
California State University Case Study
How We Got Here

The Problem

The 23 campuses in the system and our Chancellor’s Office have widely varying IT procurement processes. Additionally, we often use different definitions.

The Goal

We set out to develop a common vendor assessment process that produces a risk ranking. This would allow subsequent campuses to review that score and decide if the solution falls within their risk appetite.

That led us to a common set of procurement forms and to standardize on asking for the HECVAT.
Let’s Play 300 Questions!

One challenge was the length, both filling out and reading – could we automate the scoring?

We started with a separate scoring spreadsheet that could read a filled HECVAT and produce some numerical scoring and
Consulting!
Group Consulting

• Did we get to all of your questions from the beginning of the day?
• Any vendors/SP’s that you want advice on engagement
Questions & Feedback

security-council@educause.edu
Session Evaluations

There are two ways to access the session and presenter evaluations:

1. In the online agenda, click on the “Evaluate Session” link.

2. From the mobile app, click on the session you want from the schedule > then click the associated resources > and the evaluation will pop up in the list.
Resources

• HECVAT website:
  • https://www.educause.edu/hecvat

• Cloud Broker Index:
  • https://www.ren-isac.net/hecvat

• Session Resources:
  • SPC ’19 Website

Workshop Slides: http://go.iu.edu/2aED
Workshop Demo: http://go.iu.edu/2aEu

#Security19
Additional Resources

• Information Security Guide
  • Vendor and 3rd Party Risk:

• Data Protection Contractual Language