Strategies for Streamlining Security Assessments using HECVAT

PRESENTED BY:
Jon Allen • Joshua Callahan • Charles Escue • Nick Lewis • Kim Milford
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://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

• Cloud Broker Index:
  — https://www.ren-isac.net/public-resources/hecvat.html

• Session Resources:
  — https://baylor.box.com/v/Educause2018PreConf
Agenda

- Background
  - Cloud strategies
  - Internal Partners and collaborations
  - HECVAT
  - Walk through a HECVAT Assessment
  - Developing a Comprehensive Vendor Assessment Program
Agenda (continued)

- Comprehensive Vendor Assessment Programs
- Campus examples
- 9:30 am: Break
- Role playing game [or more discussion and consulting]
Conference Session

- Will be a subset of this seminar
- Hoping you become an evangelist
- Bring peers and colleagues even in other areas
Cloud Strategy

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

- History
- Unique collaboration
- Ongoing Project
Project Inspiration

- 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!

- Project is two years old
- Goal to simplify, expedite and create higher quality assessments
- A win for institutions and vendors alike
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
<table>
<thead>
<tr>
<th>Campus Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appalachian State University</td>
</tr>
<tr>
<td>Art Institute of Chicago</td>
</tr>
<tr>
<td>Baylor University</td>
</tr>
<tr>
<td>Berry College</td>
</tr>
<tr>
<td>Boston College</td>
</tr>
<tr>
<td>Bowling Green State University</td>
</tr>
<tr>
<td>Brown University</td>
</tr>
<tr>
<td>California State University System</td>
</tr>
<tr>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>Champlain College</td>
</tr>
<tr>
<td>Clarkson University</td>
</tr>
<tr>
<td>Cornell University</td>
</tr>
<tr>
<td>Davidson College</td>
</tr>
<tr>
<td>Denison University</td>
</tr>
<tr>
<td>DeSales University</td>
</tr>
<tr>
<td>Drake University</td>
</tr>
<tr>
<td>Drexel University</td>
</tr>
<tr>
<td>Duquesne University</td>
</tr>
<tr>
<td>Ferris State University</td>
</tr>
<tr>
<td>Foothill-De Anza Community College District</td>
</tr>
<tr>
<td>Franklin &amp; Marshall College</td>
</tr>
<tr>
<td>Georgia Institute of Technology</td>
</tr>
<tr>
<td>Indiana University</td>
</tr>
<tr>
<td>Indiana Wesleyan University</td>
</tr>
<tr>
<td>Kent State University</td>
</tr>
<tr>
<td>Linfield College</td>
</tr>
<tr>
<td>Marylhurst University</td>
</tr>
<tr>
<td>Miami University</td>
</tr>
<tr>
<td>Morgan State University</td>
</tr>
<tr>
<td>Northern Arizona University</td>
</tr>
<tr>
<td>Oakland University</td>
</tr>
<tr>
<td>Ohio Northern University</td>
</tr>
<tr>
<td>Oregon State University</td>
</tr>
<tr>
<td>Princeton University</td>
</tr>
<tr>
<td>Rice University</td>
</tr>
<tr>
<td>Rutgers University</td>
</tr>
<tr>
<td>Southern Alberta Institute of Technology</td>
</tr>
<tr>
<td>Stony Brook University</td>
</tr>
<tr>
<td>Susquehanna University</td>
</tr>
<tr>
<td>Troy University</td>
</tr>
<tr>
<td>Truman State University</td>
</tr>
<tr>
<td>University of California, Davis</td>
</tr>
<tr>
<td>University of Delaware</td>
</tr>
<tr>
<td>University of Maine System</td>
</tr>
<tr>
<td>University of Maryland Baltimore</td>
</tr>
<tr>
<td>University of Massachusetts Amherst</td>
</tr>
<tr>
<td>West Virginia University</td>
</tr>
<tr>
<td>Western Carolina University</td>
</tr>
<tr>
<td>Western Michigan University</td>
</tr>
<tr>
<td>Williams College</td>
</tr>
</tbody>
</table>

#EDU18
Phase 3 Deliverables

- Engage vendors
  - For HECVAT awareness
  - CBI participation
- Automated triage
Updates in the last year

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

- Added PCI DSS!
- CIS Critical Controls
- HIPAA
- ISO:27002:2013
- NIST Cybersecurity Framework
- NIST 800-171r1
- NIST 800-53r4
Our “sharing” objective has been modified

The Higher Education Cloud Vendor Assessment Tool (HECVAT) attempts to generalize higher education information security and data protection questions and issues for consistency and ease of use. Some institutions may have specific issues that must be addressed in addition to the general questions provided in this assessment. It is anticipated that this HECVAT will be revised over time to account for changes in cloud services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Cloud Vendor Assessment Tool:
- Helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, including some that are unique to higher education
- Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through cloud services without increasing risks
- Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions

The HECVAT was created by the Higher Education Information Security Council Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of third-party provided cloud services and resources. Over time, the Shared Assessments Working Group hopes to create a framework that will establish a community resource where institutions and cloud services providers will share completed Higher Education Cloud Vendor Assessment Tool assessments.

https://www.educause.edu/hecvat
https://www.ren-isac.net/hecvat

(C) EDUCAUSE 2018
This work is licensed under a Creative Commons Attribution-Noncommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).

This Higher Education Cloud Vendor Assessment Tool is brought to you by the Higher Education Information Security Council, and members from EDUCAUSE, Internet2, and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).
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 vary 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>Vendor Answers</th>
<th>Additional Information</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Please include a copy with your response and include a URL for the published assessment.</td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Describe any plans to obtain CSA STAR certification.</td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Describe any plans to conform to an industry standard security framework.</td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></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>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></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>The Institution conducts Third Party Security Assessments on a variety of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>third parties. As such, not all assessment questions are relevant to each</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>party. To alleviate complexity, a &quot;qualifier&quot; strategy is implemented and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>allows for various parties to utilize this common documentation instrument.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>**Responses to the following questions will determine the need to answer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>additional questions below.**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualifiers</td>
<td>Vendor Answers</td>
<td>Additional Information</td>
<td>Guidance</td>
</tr>
<tr>
<td>QUAL-01 Does your product process protected health information (PHI) or</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>any data covered by the Health Insurance Portability and Accountability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QUAL-02 Does the vended product host/support a mobile application? (e.g.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>app)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QUAL-03 Will institution data be shared with or hosted by any third</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>parties? (e.g. any entity not wholly-owned by your company is considered</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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

<table>
<thead>
<tr>
<th>HEISC Shared Assessments Working Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
</tr>
<tr>
<td>Vendor Contact Name</td>
</tr>
<tr>
<td>Vendor Contact Title</td>
</tr>
<tr>
<td>Vendor Email Address</td>
</tr>
<tr>
<td>Institution's Security Framework</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Product Name and Version Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Description</td>
<td>Brief Description of the Product</td>
</tr>
<tr>
<td>HECVAT Version</td>
<td>Full</td>
</tr>
<tr>
<td>Date Prepared</td>
<td>mm/dd/yyyy</td>
</tr>
</tbody>
</table>
The Analyst report provides function to move qualitative results into quantitative scoring

<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>Please rate the vendor's answer</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>Please rate the vendor's answer</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>Please rate the vendor's answer</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>Please rate the vendor's answer</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>Please rate the vendor's answer</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>Please rate the vendor's answer</td>
</tr>
</tbody>
</table>
The new HECVAT scoring function provides an excellent starting point for evaluation efforts.
The Summary Report gives a quick view of a vendor's security state
HECVAT - Demo

- Consolidate the power of higher education
- Shorten the review cycle
- Improve the quality of responses
Developing a Comprehensive Vendor Assessment Program
Increase Campus Involvement

- Success is dependent on campus involvement
- Shorten the review cycle
- Improve the quality of responses
Campus Partnerships

- Procurement
- Legal
- Audit
- Campus Departments
Contracts

- Frame the conversation
- Four corners all that matter
- A key security control
- Service addendum (example)
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.
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
Cloud Broker Index

https://www.ren-isac.net/ hecvat/cbi.html
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 Wprovidet23.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 Wprovidet23.com has completed a HECVAT questionnaire for its LMS product. It has not.

**“Bench”mark 4**
During the procurement process, Institution A encourages Wprovidet23.com to complete a HECVAT for its LMS product, and to list that HECVAT in the REN-ISAC Cloud Broker Index.

**“Bench”mark 5**
Institution B is looking for a new LMS, sees that Wprovidet23.com has a HECVAT listed on the REN-ISAC Cloud Broker Index and contacts Wprovidet23.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

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

www.educause.edu/hecvat
HECVAT & the CBI

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

10 Service Providers with 15 HECVATs!
HECVAT & the CBI

- REN-ISAC proactively reach out to vendors
  - Please send vendors to us!
  - hecvat@ren-isac.net
  - We can provide scripted outreach as needed

- Universities working with certain vendors provide facilitation

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

Public: *Hosted and linked on REN-ISAC web site*
- Vendor sends completed assessment to HECVAT@REN-ISAC.net

Public2: *Vendor hosts, REN-ISAC links*
- Vendor sends the link to completed questionnaire

Semi-public: *Vendor hosts, REN-ISAC links*
- Vendor hosts behind paywall, sends the link and information

Private: *Vendor controls, REN-ISAC links*
- Vendor keep private, send instructions on how people can request
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
Vendor Partner Value

Sona Systems
@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
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
Campus Examples
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.
The HECVAT elevates our leaders confidence and improves collaboration.
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.
Call to Community

- Commit to HECVAT
- Allow referencing
- Educate Vendors
- Give feedback
Future Direction

Phase 4 - 2019

Brainstorm on ideas for the next phase

Engage with existing working group members and new members to develop workplan.

We want your input!
Consulting and Discussion
Feedback and Questions

Survey:

https://www.surveymonkey.com/r/6LMNLFZL
Please take a moment to evaluate this session
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