Higher Education Cloud Vendor Assessment Tool

Assessing security and privacy risks in third party services

Internet2 Global Summit - Joanna Grama EDUCAUSE; Kim Milford REN-ISAC; Nick Lewis Internet2

REN-ISAC

INTERNET2

EDUCAUSE

HECVAT INSTITUTIONS ROCK!

Agenda

1. Project inspiration and the “job to be done”
2. Phase I work and completion
3. Phase II deliverables and current status
4. Questions

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

Evolving information security programs as quickly as possible

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

This is a big project--so it was divided into two phases.

Phase I contributors

- Jon Allen, Baylor University
- John Bruggeman, Hebrew Union College, Jewish Institute of Religion
- Charles Escue, Indiana University
- Karl Hassler, University of Delaware
- Craig Munson, Minnesota State Colleges & Universities
- Mitch Parks, University of Idaho
- Laura Raderman, Carnegie Mellon University
- Sandy Silk, Harvard University
- Staff Liaisons from EDUCAUSE, Internet2, and REN-ISAC
  - Joanna Grama
  - Valerie Vogel
  - Nick Lewis
  - Todd Herring
  - Kim Milford

Phase I Deliverable

Create a cloud services assessment questionnaire/template that can be used to surface a short executive summary for review & sharing.

Collaboration between Internet2, EDUCAUSE, REN-ISAC and its members.

The Higher Education Cloud Vendor Assessment Tool (“*HECVAT” if you are cool*), was published October 2016.

https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

A little history about what brought us here

Objective from Working Group Charter

- Create a cloud services assessment questionnaire/template that can be used to surface a short executive summary for review & sharing
- Provide a comprehensive vendor evaluation tool geared towards higher education use/consumption

Creative Efforts

- Many existing questionnaires but none that covered the broad range of subjects to the degree needed in Higher Ed

The humble beginnings of what became the HECVAT

First draft

Merged the existing questionnaires from Carnegie Mellon University and Indiana University

Filled in group-defined gaps with other institutions questions

Baylor University, Hebrew Union College, University of Delaware, Minnesota State Colleges & Universities, University of Idaho, and Harvard University

Refinement

Performed a gap analysis between the pre-HECVAT and the Consensus Assessments Initiative Questionnaire (CAIQ)

The HECVAT is a spreadsheet, we used tabs

Introduction

Communicating the Higher Ed vision for shared assessments

Sharing Objectives & Tool Instructions

Description of sharing tiers (4) and an overview of the tool functionality

Overview of Qualifiers (and their linked Optional sections)

Cloud Vendor Assessment Tool

The main attraction!

HECVAT and How We [want to] Share It

By completing the Higher Education Cloud Vendor Assessment Tool, cloud service providers understand that the completed assessment may be shared among higher education institutions.

Four Tiers of Sharing

Assessment template and discussion regarding the assessment process

List of service providers assessed and contact information of service providers

Completed assessment (vendor answers intact)

Security report created by this Higher Education institution

There Are Various Sharing Options (Vendor Selected)

Item	Default Sharing Permission	Default Sharing Audience
Assessment template and discussion regarding the assessment process	OK to share	Public
List of service providers assessed and contact information of service providers	OK to share	Higher education institutions only
Completed assessment (vendor answers intact)	None, Opt-in by service provider only	None, unless opt-in. If a service provider opts-in, the sharing is within higher education institutions only
Security report created by this Higher Education institution	None, Opt-in by service provider only	None, unless opt-in. If a service provider opts-in, the sharing is within higher education institutions only

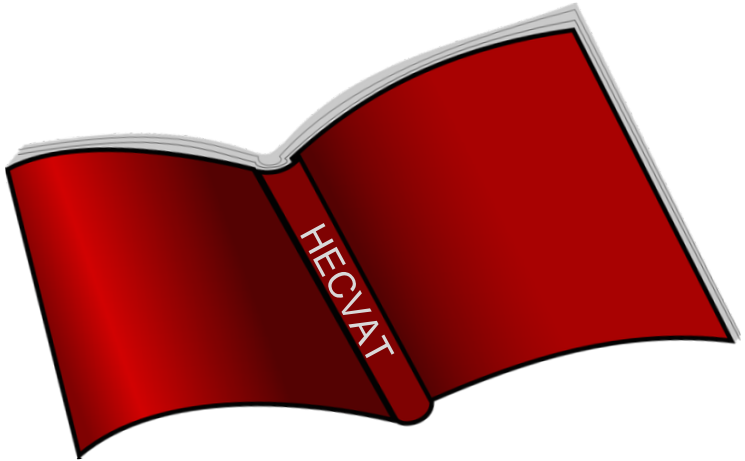
Read The * Manual!

PROBLEM

No Directions + 100’s of Questions = Insufficient Vendor Responses

ANSWER

We provided a Manual [in the form of an “**Instructions**” tab]!



Target Audience

Optional Safeguards Based On Qualifiers

Document Layout

General Info

Sharing Selections

Documentation

Company Overview

Initially, there are four use case specific sections...

Section	# of ?s	Summary
Third Parties*	4	When a vendor (third party) uses a third party to support their product it is important to document vendor security assessments, any legal agreements, and general use case information. Section requirement based on Qualifier.
Consulting*	11	Controlled through a Qualifier. Vendor assessments for consulting services only require only a subset of questions to be answered; the remaining become optional.
PCI DSS*	12	Controlled through a Qualifier. The PCI DSS section is required when PCI DSS regulated data is shared.
HIPAA*	32	Controlled through a Qualifier. The HIPAA section is required when PCI DSS regulated data is shared. The largest section.

Although pioneering and useful, the HECVAT's scope is specific and it has some limitations

The tool is long and we recognize this could be cumbersome for low risk evaluations

Requires significant resources to properly digest and analyze vendor responses

May not be appropriate for vendor engagements using lower-level data classifications

Phase II

Phase II started in March 2017

Deliverables include:

- Feedback Gathering
- HECVAT Lite
- Crosswalk to standards
- Vendor expectations paper
- Sharing expectation paper
- Sharing infrastructure/proof of concept

Phase II contributors

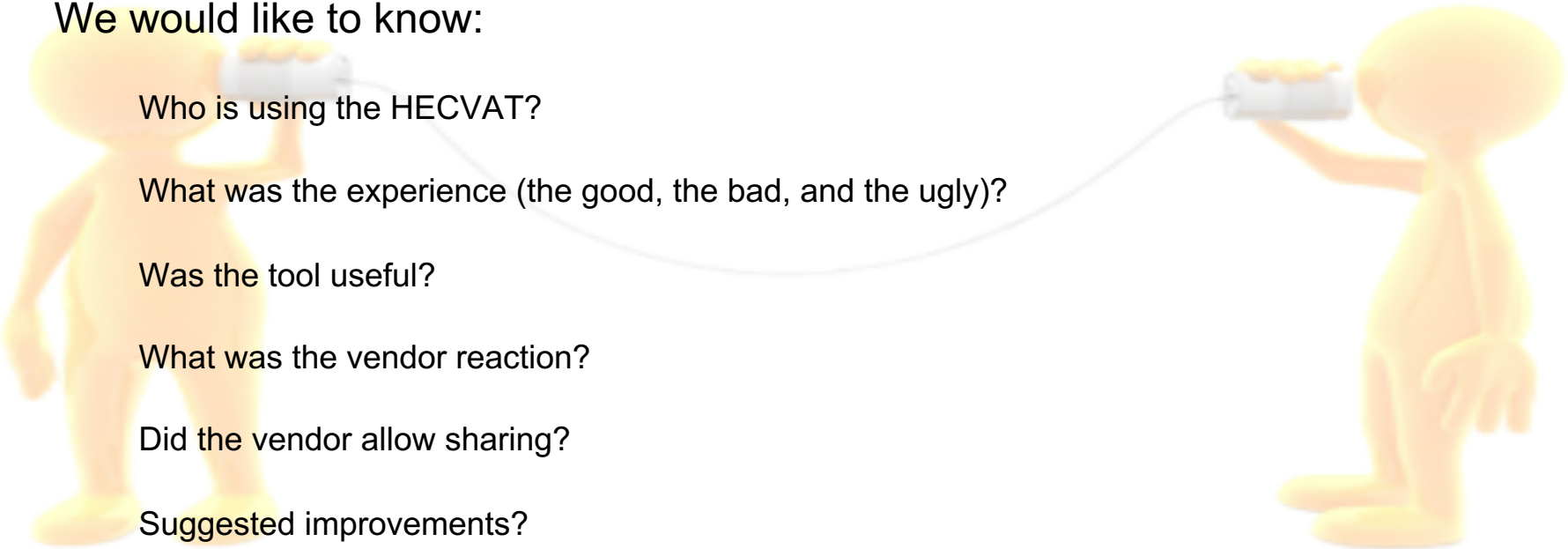
- Jon Allen, Baylor University
- Matthew Dalton, University of Massachusetts Amherst
- Charles Escue, Indiana University
- Kolin Hodgson, Notre Dame University
- Tom Horton, Cornell University
- Leo Howell, North Carolina State University
- Alex Jalso, West Virginia University
- Wyman Miles, Cornell University
- Staff Liaisons from EDUCAUSE, Internet2, and REN-ISAC
    - Joanna Grama
    - Valerie Vogel
    - Nick Lewis
    - Todd Herring
    - Kim Milford

Deliverable: Feedback Gathering

One of the most important Phase II deliverables

We would like to know:

- Who is using the HECVAT?
- What was the experience (the good, the bad, and the ugly)?
- Was the tool useful?
- What was the vendor reaction?
- Did the vendor allow sharing?
- Suggested improvements?
- Gather testimonials



Deliverable: HECVAT Lite

- The HECVAT is a mere 284 questions
  - This includes qualifying questions for HIPAA and PCI opt-in
- The HECVAT Lite project is to create a very lightweight version of the HECVAT for use in special situations
  - Short on time? Short on personnel to review? Short on budget? Short on risk?
- Current “lite” version is 57 questions; hope to pare it down more

Deliverable: Crosswalk to Standards

Understanding how HECVAT questions compare to industry standards is useful

Did we mention, 284 questions? That is a lot to crosswalk.

For the next HECVAT revision, we plan to crosswalk to as many standards, at a high level, as possible.

Currently we are reviewing, ISO 27002:2013; NIST SP 800-53 Controls; NIST SP 800-171 Controls; NIST Cybersecurity Framework; CIS 20 Critical Security Controls (ver 6.1); HIPAA Security Regs; PCI DSS Regs

Deliverable: Vendor Expectations Paper

Do vendors *really know* what higher ed wants with respect to security/privacy information for their products/services?

The goal of this *very short* paper (or blog post) is to provide concrete advice to vendors about the types of information and documentation we expect from them

Other possible items to address:

- Can we specify that our expectation is that vendors in the our industry will use the HECVAT (e.g., like the InCommon Federation for authentication)
- Can we also make the case for the HECVAT? (A vendor is completing one assessment, not many, for higher education institutions)

Deliverable: Sharing Infrastructure

Assumption: We want to be good sharers; sharing is caring.

What does a sharing infrastructure look like?

- Are we sharing completed HECVATs or are we sharing an institution's assessment of a particular vendor/service
- What about metadata?
- Who runs the infrastructure?

Desired end state vs. realistic sharing

- What is the minimum viable product w/r/t sharing?

Addresses the barriers to sharing

Questions for You

Have you used the HECVAT? Take our survey and share your feedback please! https://www.surveymonkey.com/r/PQSLMBK

What are your reactions?

Do you know of other organizations doing something similar that we can talk to?

What is your highest priority in terms of the HECVAT deliverables we discussed?

Questions for Us?

Timeline for completing Phase II: EOY 2017

Thank You!

Internet2 Global Summit - Joanna Grama EDUCAUSE; Kim Milford REN-ISAC; Nick Lewis Internet2

Please be sure to complete the session evaluation so that we can improve our presentation next time!

REN-ISAC

INTERNET2

EDUCAUSE

...and sixteen security safeguard sections

Application/Service Security

Authentication, Authorization, and Accounting

Business Continuity Plan *

Change Management

Data

Database

Datacenter

Disaster Recovery Plan *

Firewalls, IDS, IPS, and Networking

Mobile Applications *

Physical Security

Policies, Procedures, and Processes

Product Evaluation

Quality Assurance

Systems Management & Configuration

Vulnerability Scanning

Generally, there are three information gathering goals

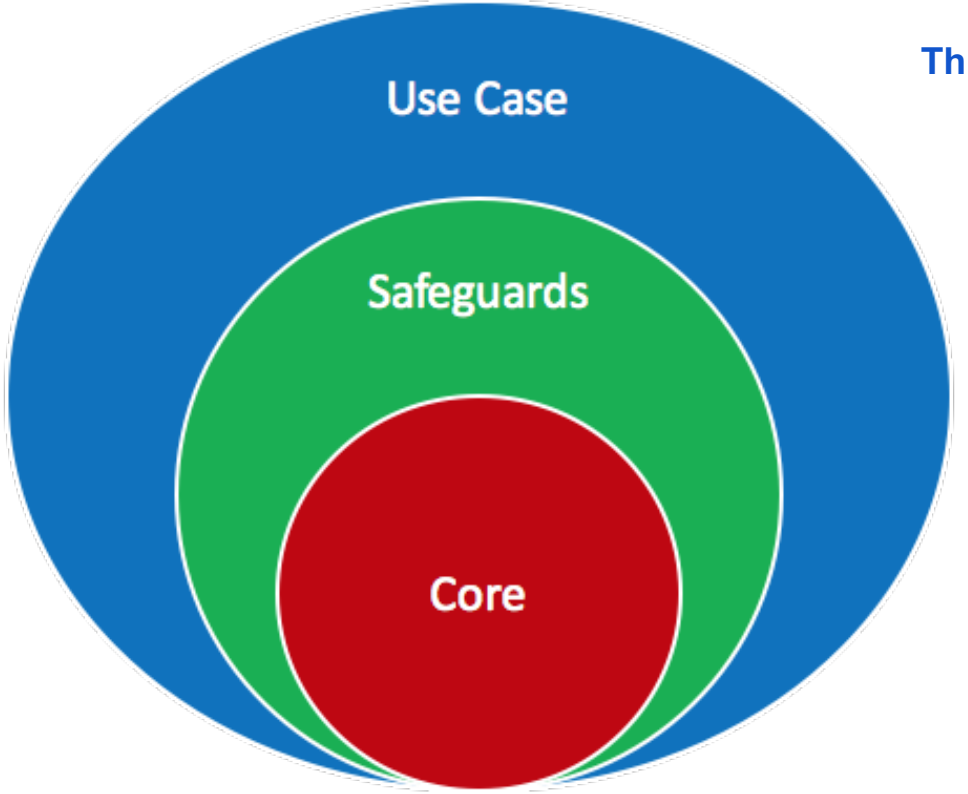
General Information

Sharing Disclosure

Qualifiers*

Documentation

Company Overview



Third (Fourth) Parties *

Consulting *

PCI DSS *

HIPAA *

More details on the next slides

Data and Security Focused Questions

Let’s take a look at the sections in general groups, starting with Data & Application

Section	# of ?s	Summary
Application/Service Security	22	Topics of redundancy, access control, user management, system components (including supporting systems), architectures, diagrams, and system validation are a few of the topics covered by this section.
Data	31	The largest safeguards section, this one is all about the data; transport, encryption, storage, destruction, etc. You name it.
Database	2	Database encryption capabilities is what we want to know.
Mobile Applications*	10	Controlled through a Qualifier. When a vendor’s product includes a mobile app, support (software and hardware), distribution strategy, network protections, and functionality are outlined in detail in this section.

Most deterrent and preventive controls are in Physical

Section	# of ?s	Summary
Datacenter	19	Ownership, geographic diversity, ISP redundancy, Uptime Institute tier levels, physical segmentation, and monitoring efforts are just a few topics covered in the DC section.
Physical Security	6	Physical access controls, system monitoring capabilities, and equipment access details are collected here.

Sections that address the overall operational and response structure of a vendor are in Planning

Section	# of ?s	Summary
Business Continuity Plan*	12	Controlled through a Qualifier. See title.
Change Management	15	Patching, server maintenance, security mitigation strategy, release timing, assurance testing, and emergency action documentation efforts are the focus of this section.
Disaster Recovery Plan*	14	Controlled through a Qualifier. See title.
Policy, Procedures, and Processes	23	Security organization sizes/capabilities, secure development strategies, established SDLC implementation(s), formal Incident Response plans, and general HR issues are broadly covered in this catch-all.

Technically, most sections can be technical, but the Technical group is reserved for only the techy-ist

Section	# of ?s	Summary
Authentication, Authorization, and Account	19	All questions related to IAM, AAAI, password/passphrase, MFA, and access control can be found here.
Firewalls, IDS, IPS & Networking	12	Network security practices, monitoring, IDS/IPS strategy, and auditing details are collected here.
System Management & Configuration	4	Summaries for general system management, segmentation, MDM strategy, and secured images are the focus here.
Vulnerability Scanning	9	Straight-forward. Details for server and application level vulnerability scanning for the system are collected here. Timely, relevant scans are necessary; timelines and recent activity/response is crucial to environment understanding.

In the land of misfits, there lies the Other section

Section	# of ?s	Summary
Product Evaluation	2	Many institutions expressed the expectation for vendors to accommodate security feature requests and the ability to have a testing environment (especially for enterprise-class systems).
Quality Assurance	5	Although an outlier, the QA section allows institutions to measure a vendor's Higher Ed environment awareness and general performance metrics.

Deliverable: Sharing Expectations Paper

The goal of this *very short* paper (or blog post) is to provide concrete advice to vendors about the types of information and documentation we expect them to share when we evaluate their services for security and privacy.

We will also explain the value of a sharing framework like the HECVAT, and encourage campuses and vendors to use the tool.