Cloud Vendor Security Risk Assessments: An Update from the HEISC Shared Assessments Working Group

Charles Escue, Indiana University

cescue@iu.edu

REN-ISAC

INTERNET2®

EDUCAUSE

Agenda

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

- HECVAT Promotion
- HEISC Shared Assessments working group
  - Project inspiration & collective vision
  - Phase I & Phase II deliverables
  - Current State
- Using the HECVAT in your institution
  - Leveraging community strength
  - Securing leadership buy-in
  - Early HECVAT adoption successes
- What's next for the HECVAT?
- Questions

Project inspiration came from many sources

Rapid Cloud Service Adoption

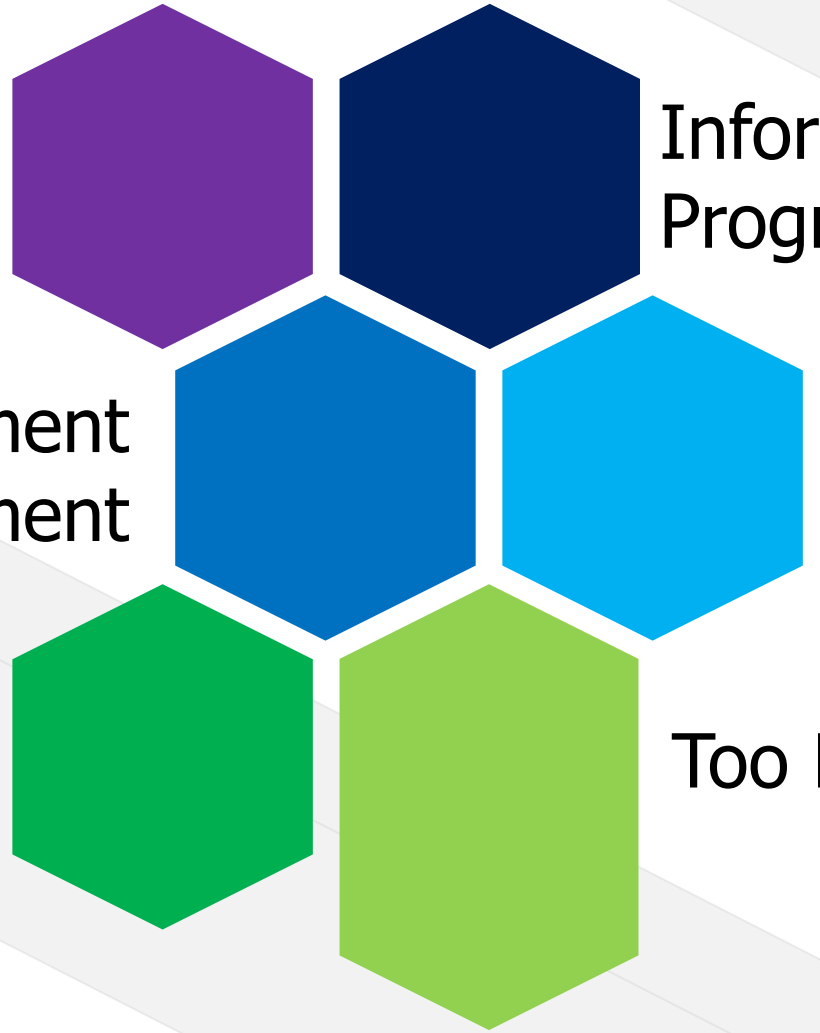
Information Security Programs Evolving Quickly

Enterprise Risk Management Program Development

Vendor Risk Management Program Development

Proper Assessment Becoming Burdensome

Too Much Going On!



Outlining the job to be done

Share work done at one organization with others

Create a space for finding/sharing existing assessments

Reduce unnecessary burden, focus on critical functions

Support the HigherEd information security community

Working group founders created a robust charter, quickly steering development efforts

Charter Objectives		
Standard Security Controls Document	Provide a tool to facilitate HE usage	Address unique operations of HE

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

So what has it taken to forge this new opportunity for collaboration?

- Committed, Action Oriented Work Group(s)
- A multi-phase development approach
- 19+ Contributing Organizations
- HE excitement, openness to change, feedback

Initial Contributors; Phase 1

- **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

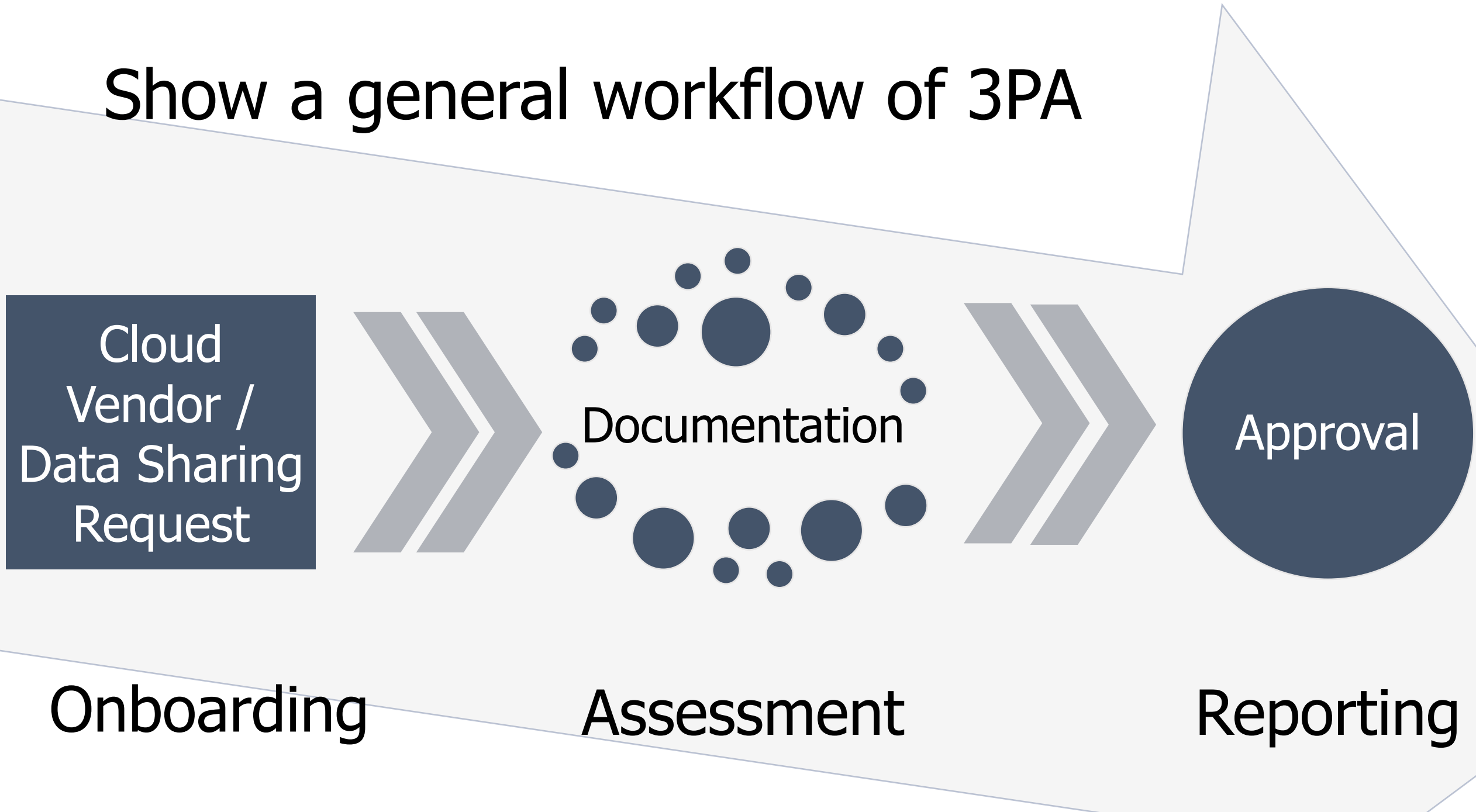
- Staff Liaisons from EDUCAUSE, Internet2, and REN-ISAC:
  - **Joanna Grama**
  - **Todd Herring**
  - **Nick Lewis**
  - **Kim Milford**
  - **Valerie Vogel**

More Contributors; Phase 2

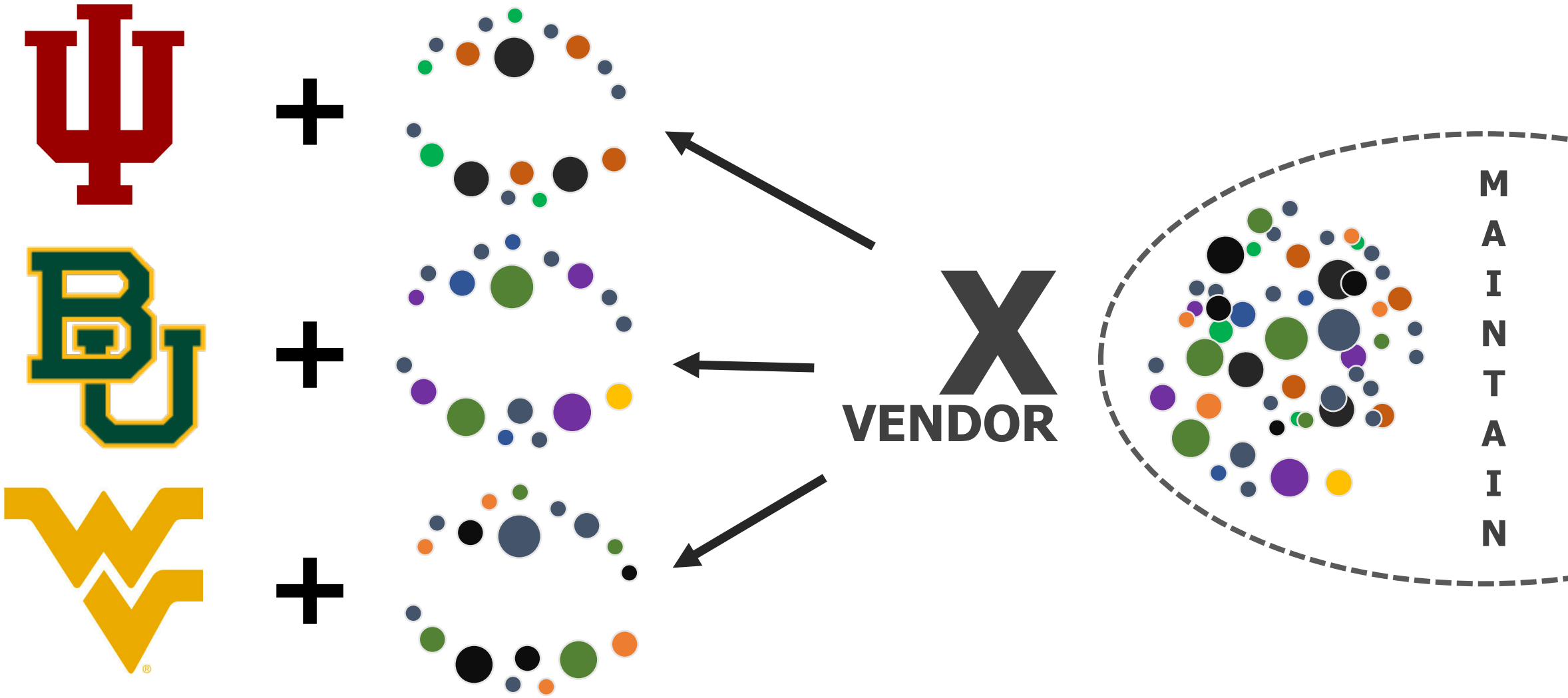
- **Jon Allen**, Baylor University
- **Samantha Birk**, IMS Global Learning Consortium
- **Jeff Bohrer**, IMS Global Learning Consortium
- **Sarah Braun**, University of Colorado – Denver
- **David Cassada**, University of California – Davis
- **Matthew Dalton**, University of Massachusetts Amherst
- **Charles Escue**, Indiana University
- **Kolin Hodgson**, University of Notre Dame
- **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**
  - **Todd Herring**
  - **Nick Lewis**
  - **Kim Milford**
  - **Valerie Vogel**

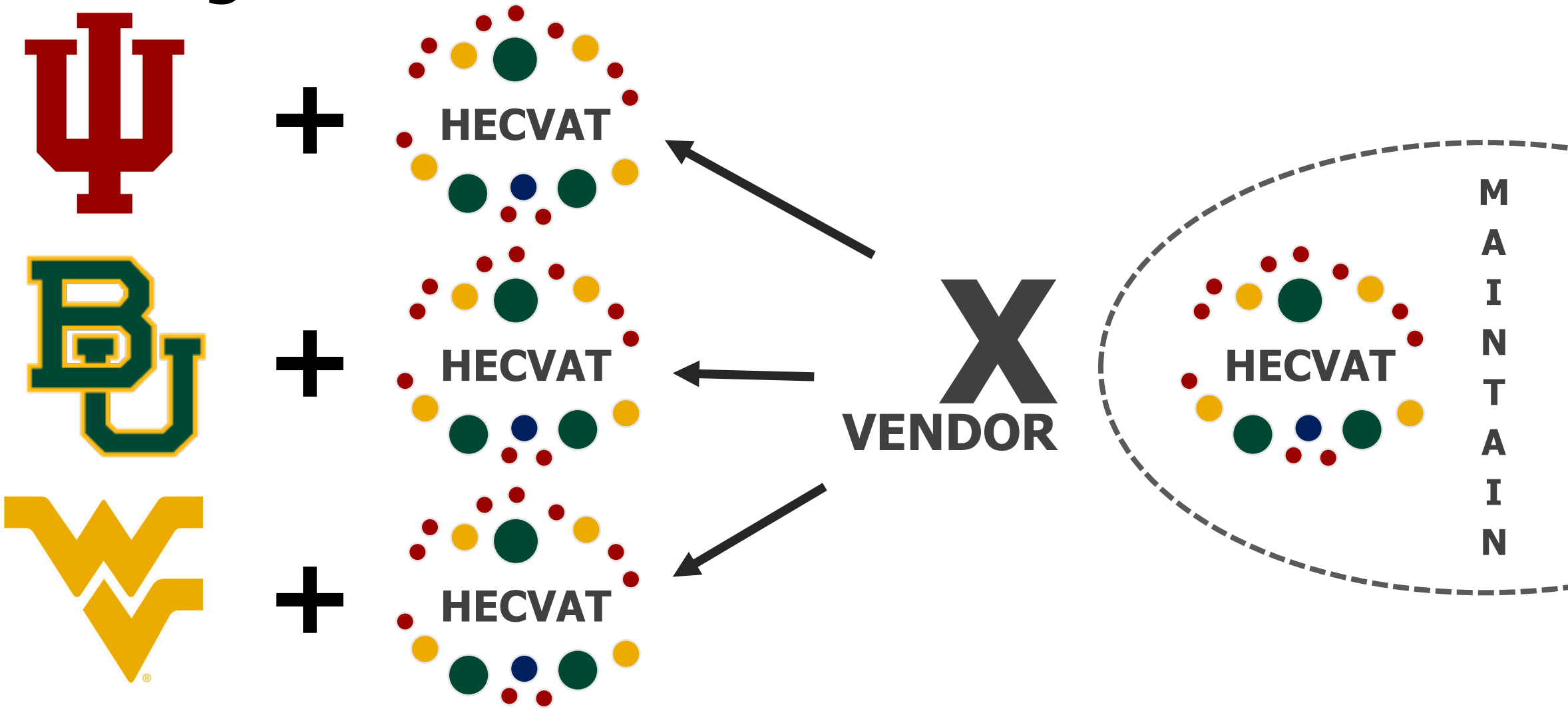
Show a general workflow of 3PA



We are all doing the same thing with minor changes to fit our environments



Using similar documentation facilitates HE sharing and reduces vendor burden



The Higher Education Cloud Vendor Assessment Tool (HECVAT), what is it?

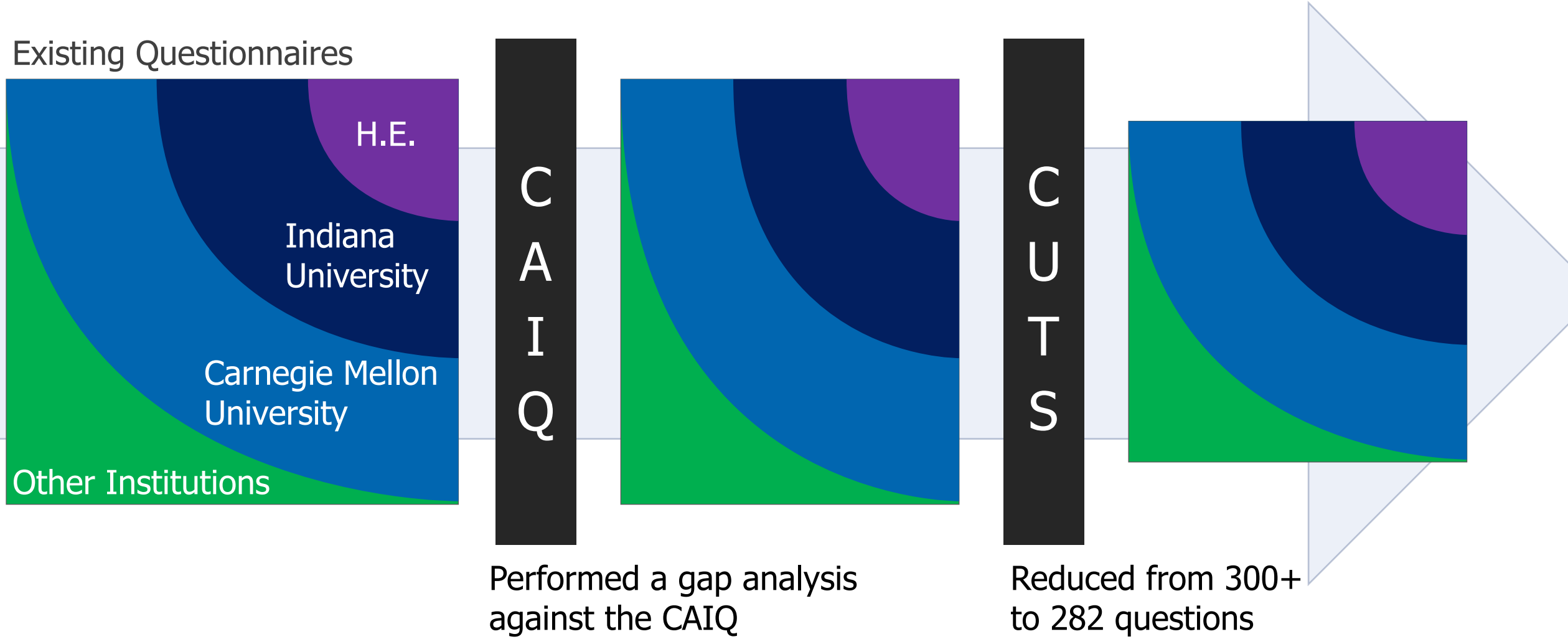
v1.06

A tool used to improve efficiency and consistency in vendor assessments within HE

A holistic document that covers our common operating environments in HE

An avenue to state HE expectations for security to vendors offering services in the cloud

So how did the HECVAT come to life?

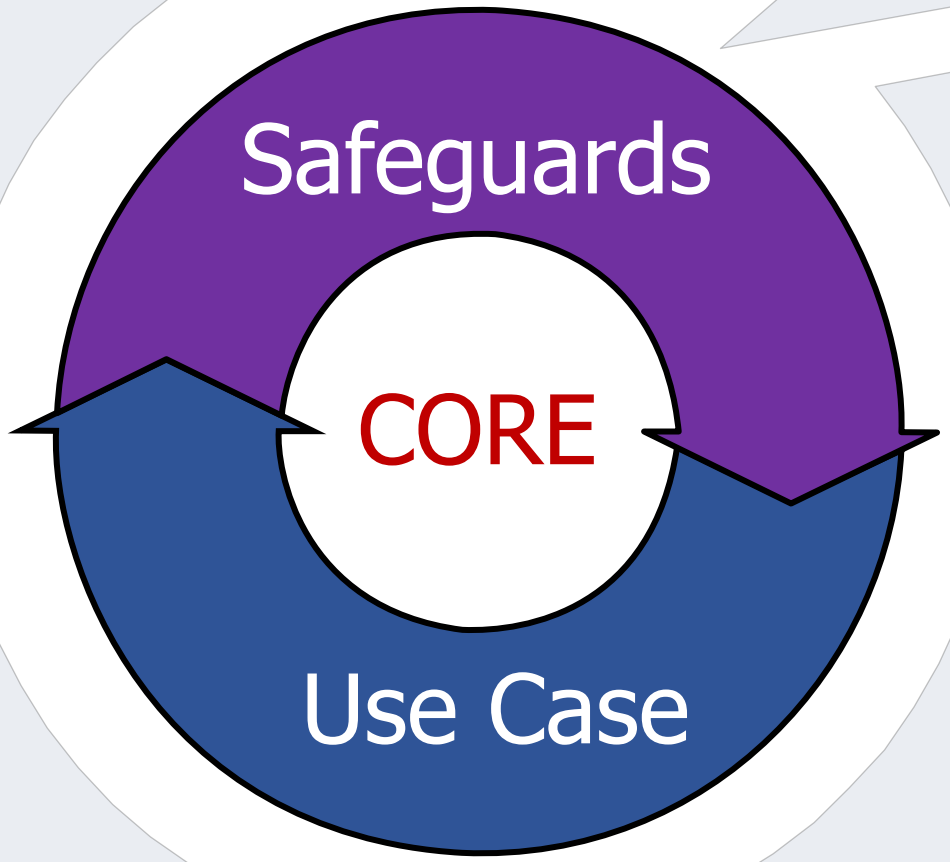


Performed a gap analysis against the CAIQ

Reduced from 300+ to 282 questions

Generally, there are three information gathering goals

General Information
Sharing Disclosure
Qualifiers*
Documentation
Company Overview



Range from
Application Security to
Vulnerability Scanning

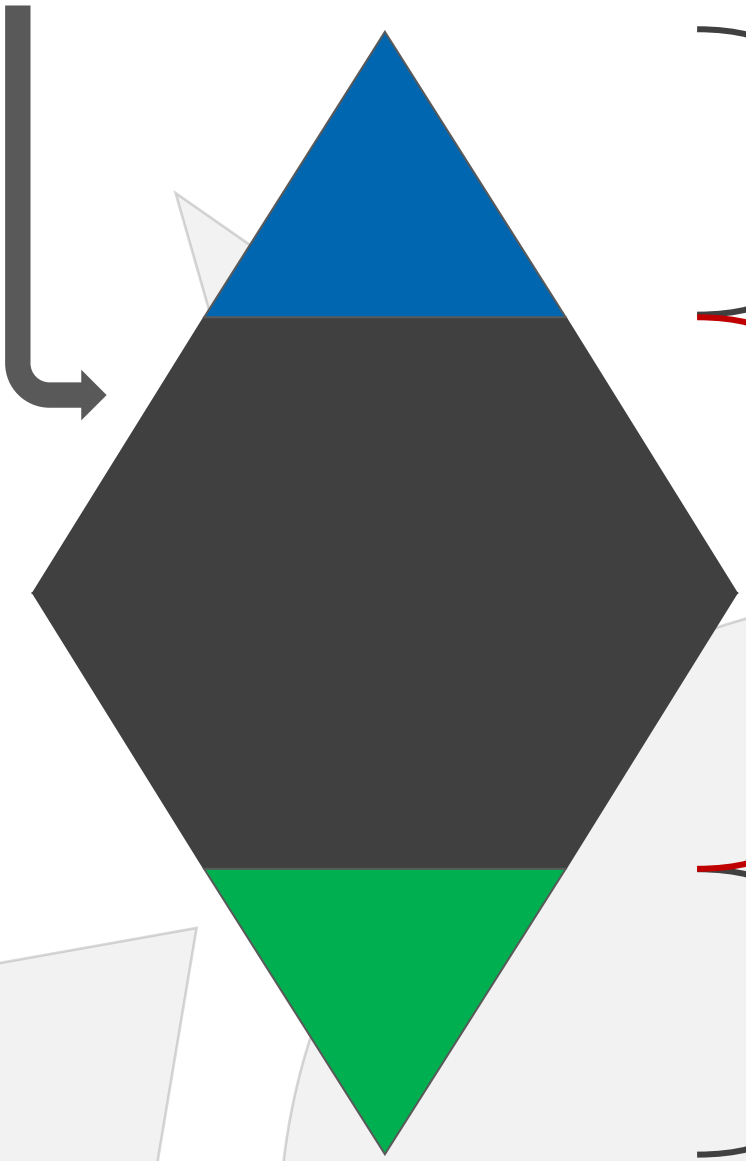
Third (Fourth) Parties *
Consulting *
PCI DSS *
HIPAA *

The HECVAT covers a broad range of safeguard groups

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

What can the HECVAT do for your organization?

10/**80**/10



Onboarding

Assessment

Reporting

There are many factors in successfully adopting the HECVAT at your institution

The HECVAT's scope is specific and it has some limitations

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

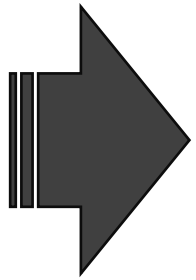
Requires committed resources to properly digest and analyze vendor responses

Can be cumbersome for low risk evaluations

Making the HECVAT usable for many institutions meant making it smaller

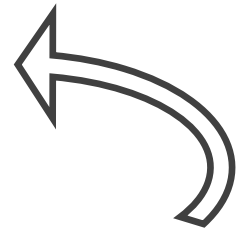
282

HECVAT



81

HECVAT Lite



Short on time? Short on personnel to review? Short on budget? Short on risk?

Many institutions have some assessment capability; how can the HECVAT fit in?

- Understanding how HECVAT questions compare to industry standards is useful
- Standards mapping enable smoother adoption of the HECVAT
- Phase 2 contributors spent countless hours creating the crosswalk of six initial standards

CIS 20 Critical Security Controls (v6.1)
HIPAA
ISO 27002:2013
NIST Cybersecurity Framework (CSF)
NIST SP 800-53r4
NIST SP 800-171r1

Staff Liaisons from EDUCAUSE, Internet2, and REN-ISAC truly support the effort!

CLOUD BROKER INDEX

NET+

COMMS & THE REST

Indiana University was one of the first adopters of HECVAT; we saw immediate improvement

Pilot use began October 2016

Exclusive use of HECVAT for all third-party assessments began January 2017

HECVAT-Lite released in May 2017; used in RFP process when appropriate

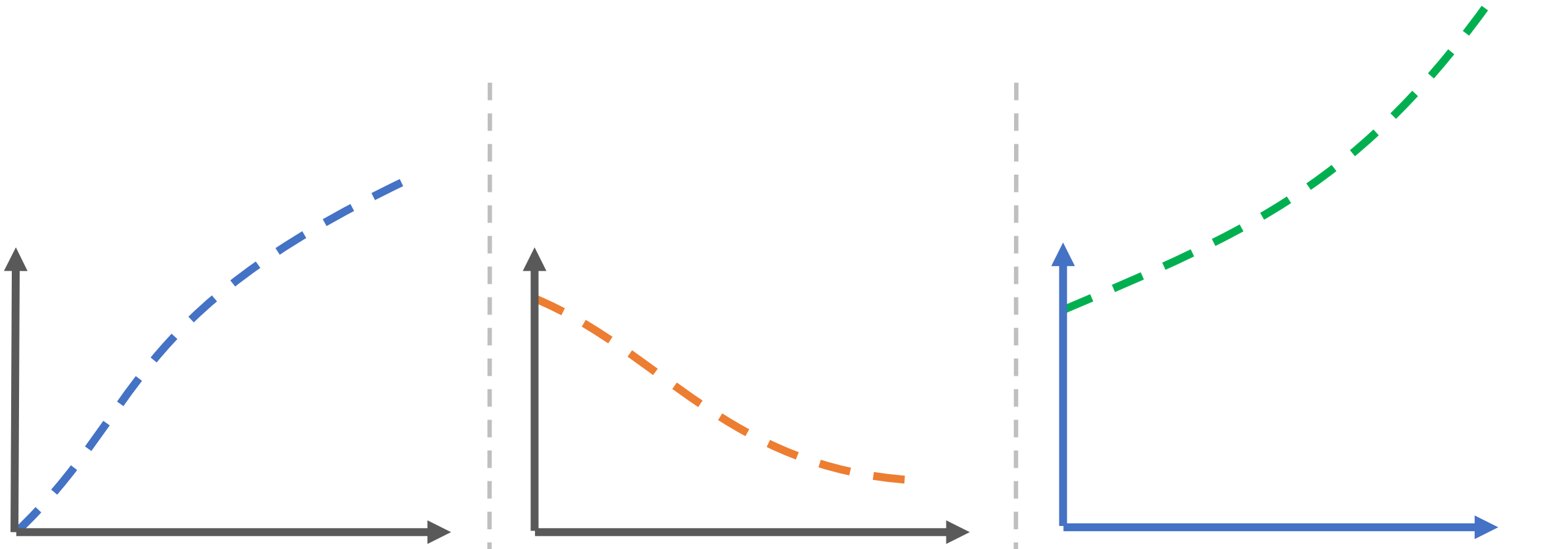
As of September 2017, we have received **34** populated HECVATs

Next Step: Matching HECVAT standards crosswalk to IU program

After That: Improve assessment reporting for HECVAT standards

HECVAT & HECVAT-Lite V1.06 released October 2017

What will Phase 3 efforts focus on?



Cloud Broker Index Support and Usage

Obstacles to adopt HECVAT at your institution

HECVAT & HECVAT-Lite Use and Participation

Questions?

Cloud Vendor Security Risk Assessments:
An Update from the HEISC
Shared Assessments Working Group

Charles Escue, Indiana University

cescue@iu.edu