# Table of Contents

Background ........................................................................................................................................ 3  
Planning .............................................................................................................................................3  
Documenting the Terms and Conditions.............................................................................................5  
How to Conduct a Peer Review .............................................................................................................6  
Resources ........................................................................................................................................... 7
This paper was prepared by members of the Higher Education Information Security Council (HEISC) to provide guidance for conducting peer review assessments of higher education information security programs. Learn more about HEISC and the EDUCAUSE Cybersecurity Program.

**Background**

Information security represents an area of significant risk for higher education institutions, with every month bringing new accounts of security breaches. A single cyber event can involve tens or hundreds of thousands of lost records and result in costs — either through incident response or fines — in the millions of dollars. It can also negatively affect an organization’s reputation and customer relationships.

Periodic external reviews of higher education information security programs help ensure that resources are focused on the right items, a critical task given the rapidly evolving nature of cybersecurity and the limited resources available to most institutions. Reviews from subject-matter experts within the higher education community are often more efficient and relevant than those from commercial or government sectors, given that they begin with an understanding of the unique aspects and limitations of the higher education space and its business processes.

This toolkit can help institutions facilitate a do-it-yourself peer review assessment. In general, the process for conducting such an assessment includes these elements:

- Assessing your program’s needs to begin planning the peer review
- Documenting the terms and conditions
- Understanding how to initiate and conduct the peer review
- Leveraging current resources developed by the higher education community

**Planning**

The first step in conducting a peer review assessment is to comprehensively plan for it. Develop your assessment concept by considering the following elements:

- Understand your goals in engaging in a peer review assessment.
  - What do you hope to accomplish with the assessment?
  - How does it meet your information security programmatic goals?
• Understand the proposed scope of the assessment.
  ➢ What topics will the assessment cover? The more guidance you can provide on assessment coverage, the better your ability to identify a peer reviewer and ensure you will receive a deliverable that meets your needs.
  ➢ Will the assessment cover the institution’s entire information security program or only one unit or one specific area?

• Secure management’s support for the assessment.
  ➢ Who is supporting the peer review assessment? It could be one campus department, a cross-campus effort with multiple departments, or a regional effort supported by multiple institutions.
  ➢ Ensure that the institution’s legal counsel is involved with the engagement from the beginning.
  ➢ Reach out to the relevant areas that may be impacted by the assessment or its findings.

• Understand which internal staffing resources will be needed for the assessment.
  ➢ Who will be the primary point of contact for the entire engagement?
  ➢ What institutional information security team members (and others) will be required to participate in the assessment?
  ➢ What type of preparation will be required in advance of the assessment to provide the peer reviewer with an overview of the institution and its information security program?

• Think about the logistics of the peer review assessment. (Note that expectations should be managed up front, with appropriately sized outcomes — for example, producing conversation points or a heat map that emphasizes the top 10 areas to improve the program instead of a 100-page report, or agreeing to do a deeper dive into one specific known area of weakness in the program.)
  ➢ When will the assessment take place?
  ➢ Will the assessment be onsite or offsite (i.e., virtual)?
  ➢ When is the peer reviewer’s deliverable due?
  ➢ How will the institution respond to the final deliverable?
  ➢ What follow-up will be required from the institution?

• Think about selecting and compensating the peer reviewer.
  ➢ How will the peer reviewer be selected? Will it be someone recognized as an expert in a certain subject-matter area (e.g., NIST 800-171) or a peer
from a local institution or consortium? How will you select the best peer reviewer for the scope of the assessment?

- Will the peer reviewer be compensated or provided with an honorarium? (The peer reviewer will be expected to understand whether their home institution allows them to participate in a peer review during work status or whether the reviewer must be on leave from a regular job to participate in a peer review.)

- If travel for the engagement is required, how will it be managed for the peer reviewer? Will that person be reimbursed for travel?

**Documenting the Terms and Conditions**

It is critical that the terms and conditions of the peer review assessment be documented for both the institution engaging the assessment and the peer reviewer. This toolkit is written from the perspective that peer reviewers will be employees of higher education institutions. This means that in most instances, the legal counsel for the institution engaging the assessment and the peer reviewer’s home institution may require legal documents to memorialize the engagement.

Some terms and conditions that may need to be created include the following:

- A memorandum of understanding (MOU) or contract that outlines the scope of the peer review engagement, critical timelines, and other terms of the agreement
  - Will the engagement take place onsite, or will it be a virtual engagement?
  - What materials must be provided to the peer reviewer in advance of the assessment?
  - What deliverables are due to the institution being reviewed, and how should those deliverables be transmitted?
  - What is the duration of the engagement?
  - What are the financial terms, if any, of the engagement? How will the peer reviewer be compensated or reimbursed for travel expenses?
  - Should there be a limitation of liability for the parties?

- A non-disclosure agreement (NDA) to ensure that both the institution engaging the assessment and the peer reviewer maintain confidentiality about both the assessment process, any documents outlining the terms of the assessment, the assessment deliverables, and any other information learned during the course of the assessment
How to Conduct a Peer Review

This section outlines a simple peer review process. It includes guidance and recommendations on initiating a peer review, including practical recommendations for establishing scope and time frames, “keeping it simple,” and defining expected work products at the conclusion.

1. Institution determines the need for a peer review, outlines its goals for the review, and secures management support for the review.
2. Institution approaches a peer reviewer or vets several reviewers for best fit.
3. Peer reviewer selected.
4. Institutional point of contact identified for the engagement.
5. Institution and peer reviewer discuss scope and deliverables of engagement.
6. Institution and peer reviewer discuss peer review contract (e.g., fees, timeline, NDA if needed).
7. Scope and deliverables are established and agreed on.
8. Contract and all supporting documents are signed.
9. Begin pre-assessment (review prior to site visit).
   a. Institution provides self-study or assessment and previous benchmarks.
   b. Institution prepares supporting documents (policy, procedure, standards) and provides to reviewer.
   c. Supporting materials are reviewed, and follow-up questions and clarifications are settled.
10. Peer reviewer conducts onsite (or virtual) evaluation and discovery, including interviews and observations.
11. Peer reviewer develops deliverables and proposed action items.
12. Peer reviewer provides deliverables to institution’s point of contact.
13. Institution provides preliminary feedback or requests for revisions to deliverable (if needed).
14. Peer reviewer revises deliverables (if necessary).
15. Peer reviewer provides final deliverables to institution’s point of contact.
Resources

The [Higher Education Information Security Council](https://www.HEISC) (HEISC) and EDUCAUSE have created a number of resources that may be useful for peer review assessment activities. These resources, and their applicability in a peer review assessment, are outlined below.

- **HEISC Speakers Bureau**: This resource lists higher education professionals who are interested in speaking on various information security topics. These speakers may also be interested in serving as subject-matter expert peer reviewers.

- **EDUCAUSE Core Data Service**: Institutions that participate in the EDUCAUSE Core Data Service (CDS) have a number of institutional and information security measures available at their fingertips, both through the CDS Portal and through additional EDUCAUSE CDS-based research (e.g., yearly benchmarking reports, CDS data almanacs). This information could provide the basis for any materials that are provided to the peer reviewer in advance of the assessment.

- **EDUCAUSE Benchmarking Service**: The EDUCAUSE Benchmarking Service (EBS) is built on the Core Data Service database but broadens both audience and application. EBS provides capability reports that comprise maturity and deployment indices for IT governance, risk, and compliance, as well as information security. This information could be the basis of materials provided to the peer reviewer in advance of the assessment.

- **HEISC Budget Conscious Information Security Resources**: These resources provide budget-conscious advice for IT leaders and managers tasked with developing and delivering institutional information security programs and services. Three reports provide guidance on building resources on a budget, building institutional capability and sustainability, and formulating a capability roadmap to create a sustainable information security stance.

- **HEISC Information Security Program Assessment Tool**: Intended as a self-assessment tool, the HEISC Information Security Program Assessment Tool can be used by a peer reviewer to complete a review of an institution’s information security program. The tool uses International Organization for Standardization (ISO) 27002:2013, “Information Technology Security Techniques. Code of Practice for Information Security Management,” as its base framework. This tool, which is intended for use by an institution as a whole, includes a total of 101 questions; on average, it takes about two hours for an information security officer or equivalent — familiar with the local environment — to complete this tool.
• **HEISC Higher Education Cloud Vendor Assessment Tool**: Intended to be used by institutions to evaluate the purchase of cloud or third-party goods and services, the Higher Education Cloud Vendor Assessment Tool (HECVAT) can be used by a peer reviewer to complete a security and privacy review of institutional products and services. The HECVAT helps higher education institutions ensure that cloud and third-party services are appropriately assessed for security and privacy needs, including some that are unique to higher education, and provides a consistent, easily adopted methodology. The HECVAT comes in both long-form and lightweight versions.

• **HEISC Information Security Guide**: This resource provides practical approaches to preventing, detecting, and responding to information security problems in a wide range of higher education environments. This online guide is designed with colleges and universities in mind, balancing security with the need for an open, collaborative networking environment. A peer reviewer could use the Information Security Guide as a resource manual for topics within the information security body of knowledge. The guide includes mappings to popular standards such as the ISO, NIST, HIPAA, COBIT, PCI DSS 3.0, and the federal Cybersecurity Framework.

• **EDUCAUSE IT Risk Register**: This IT Risk Register was created to help institutional IT departments get their strategic IT risk-management programs off the ground. It is a sortable checklist that identifies common strategic IT risks and catalogues those risks according to common risk types and IT domains. It also contains a resource to help institutions conduct a qualitative risk assessment of the items listed in the register. A peer reviewer could use the risk register to conduct a high-level institutional risk assessment.

Other industry resources may be applicable in a peer review assessment engagement:

• **Research and Education Networking Information Sharing and Analysis Center** (REN-ISAC)

• **Office of the National Coordinator for Health Information Technology Security Risk Assessment Tool** (focused on elements of the HIPAA Security Rule)

• **Federal Financial Institutions Examination Council Cybersecurity Assessment Tool** (intended for assessing risk at financial institutions)

• **NIST Baldrige Cybersecurity Initiative** (a self-assessment tool to help organizations better understand the effectiveness of their information security program efforts)
The higher education community continues to identify collaborative ways to mitigate risk, and an assessment coordinated among peers is one approach that campuses can leverage. This toolkit is intended to serve as a starting point for colleges and universities seeking to improve and mature an existing information security program. Feedback is welcome and may be used to create a set of frequently asked questions in a future update of this resource. Please send comments or questions to security-council@educause.edu.