Solicitation UU184014613

Request for Proposal For Payroll/ Human Resource Information System

Bid Designation: Public

University of Utah

Bid UU184014613
Request for Proposal For Payroll/ Human Resource Information System

Bid Number	**UU184014613**
Bid Title	**Request for Proposal For Payroll/ Human Resource Information System**
Bid Start Date	**In Held**
Bid End Date	**Apr 9, 2024 5:00:00 PM MDT**
Question & Answer End Date	**Mar 29, 2024 5:00:00 PM MDT**
Bid Contact	**Matt Cooney** **Senior Buyer** **Purchasing** **801-585-5242** **mcooney@purchasing.utah.edu**
Contract Duration	**3 years**
Contract Renewal	**2 annual renewals**
Prices Good for	**120 days**
Bid Comments	**The purpose of this Request for Proposals (RFP) is to solicit proposals to enter into a contract with a qualified vendor to obtain a Payroll/ Human Resource Information System that encapsulates functions of payroll, time and attendance, as well as benefit management for the eight technical colleges of the Utah System of Higher Education (USHE).**

Item Response Form

Item	**UU184014613-01-01 - Request for Proposal For Payroll/ Human Resource Information System**
Quantity	**1 each**

Prices are not requested for this item.

Delivery Location

University of Utah
Utah System of Higher Education
Board of Regents Building, The Gateway
60 South 400 West
Salt Lake City UT 84101-1284
Qty 1

Description
The purpose of this Request for Proposals (RFP) is to solicit proposals to enter into a contract with a qualified vendor to obtain a Payroll/ Human Resource Information System that encapsulates functions of payroll, time and attendance, as well as benefit management for the eight technical colleges of the Utah System of Higher Education (USHE).

Request for Proposal
For Payroll/ Human Resource Information System

RFP # UU184014613

Issued March 15, 2024

University of Utah Contact:

Matt Cooney, Senior Buyer
University of Utah Purchasing Dept.
201 S. Presidents Circle Rm.170
Salt Lake City, UT 84112
Tel. (801) 585-5242
E-Mail: mcooney@purchasing.utah.edu

Questions regarding this RFP should be submitted through Periscope S2G (formerly BidSync:
https://www.periscopeholdings.com/s2g
Solicitation #: UU184014613
In the Question and Answer section

Version: 3.30.2023

TABLE OF CONTENTS

Instructions: Vendors must respond to all sections of this RFP, including sections 1 through 7. When a section does not request specific information and you agree to what it contains, you may use language such as "Sections 1.01 through 1.05, Understood and Agreed" in your response. State of Utah Procurement Code requires pricing be submitted separately from the technical proposal. Refer to Section 5 for instructions on how to organize your response.

SECTION 1 – PURPOSE OF RFP

1.01 Purpose of RFP. The purpose of this Request for Proposals (RFP) is to solicit proposals to enter into a contract with a qualified vendor to obtain a Payroll/ Human Resource Information System that encapsulates functions of payroll, time and attendance, as well as benefit management for the eight technical colleges of the Utah System of Higher Education (USHE), hereafter referred to collectively as "USHE". The companies submitting proposals in response to this RFP will hereafter be referred to as "Vendor." USHE is examining several alternatives of providing this Payroll/Human Resource Information System and may decide, after reviewing proposals submitted, not to enter into any agreement. While USHE is coordinating this procurement, it is intended that the actual contracts will be with the individual technical colleges.

1.02 Background. Enacted through Senate Bill 146 from the 2023 General Session of the Utah Legislature, Utah Code section 53B-1-402 newly requires the Utah Board of Higher Education to prioritize various areas for shared services implementation including human resources, payroll, and benefits administration. USHE technical colleges use diverse and unstandardized payroll processing systems. Payroll at the eight technical colleges is processed using five different payroll systems. Some systems are outsourced systems that provide services such as processing employee payments and filing taxes. Other systems only process payroll and payments, leaving tax filing to be done by the institution. Establishing a common vendor to provide payroll processing services for USHE technical colleges could result in cost savings and increased efficiencies.

Utah's technical colleges utilize various accounting/finance systems, including Microsoft Great Plains Dynamics, Microsoft Business Central, Sage MAS 500, Jenzabar, QuickBooks, and LINQ. It is desired that the proposed solution be compatible with most, if not all, of these systems.

Most of the technical colleges have contracted with the State of Utah Public Employees Health Program (PEHP) as their healthcare insurance provider as well as Utah Retirement Systems (URS) and Teacher's Insurance and Annuity Association (TIAA) for retirement benefit services.

As of 2012, Utah's technical colleges have opted out of the Social Security (SS) program and discounted FICA withholdings. This change affects only Full-time employees. Part-time employees continue to pay into the SS program. If a part-time employee moves in to a full-time position, they pay social security for the part of the year while they were part-time and receive (2) two W-2s for the year. The first for the period they were a part-time

employee and the second for the time they were a full-time employee. Each W-2 reflects the amount of SS withholding.

1.03 Definitions.

1.03.1 **Restricted Data** – As required by University Rule 4-004C and Rule 4-050B, any and all software maintaining, processing, or transmitting restricted data—defined as Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry (PCI) Data, Financial Information, and Donor Information —shall be subject to any IT-related requirements as indicated in the RFP document (for example, see Section 4.01.B).

1.03.2 This Payroll/ Human Resource Information System is to be obtained for the eight technical colleges of the Utah System of Higher Education, hereafter to be referred to as "USHE." These Technical Colleges are:

- Bridgerland Technical College – Logan, Utah
- Davis Technical College – Kaysville, Utah
- Dixie Technical College – St. George, Utah
- Mountainland Technical College – Lehi, Utah
- Ogden-Weber Technical College – Ogden, Utah
- Southwest Technical College – Cedar City, Utah
- Tooele Technical College – Tooele, Utah
- Uintah Basin Technical College – Roosevelt, Utah

1.03.3 The companies submitting proposals in response to this RFP will hereafter be referred to as "Vendor."

SECTION 2 – RFP DETAILS

2.01 Issuing office and RFP Reference Number. The Purchasing Department of the University of Utah ("Purchasing Department") is the issuing office for this RFP and all subsequent addenda relating to it. The reference number for the transaction is UU184014613. This number must be referenced on all proposals, correspondence, and documentation relating to the RFP.

2.02 Important Dates. The following dates are significant for this RFP:

RFP Dated and Issued	March 15, 2024
Pre-Proposal Conference	See Section 2.03
RFP Inquiry Questions Due	March 29, 2024 @ 5:00 PM, MDT
Proposals Due Date	April 9, 2024 @ 5:00 PM, MDT
Estimated Oral Presentations	April 22-26, 2024

2.03 Pre-Proposal Conference.
A pre-proposal conference will not be held for this RFP.

2.04 Inquiries. Questions arising subsequent to the issuance of this RFP that could have a significant impact on the responses to the RFP, should be submitted in the RFP Question and Answer Section, Solicitation # UU184014613 in Periscope S2G. All such questions should be received by **the Questions Due Date listed in Section 2.02.** Answers to questions will be posted on the Periscope S2G site. Bidders who select 'Notify me about this Bid' or 'Download Bid Packet' will receive email notification of any addenda, changes, or updates to the bid.

2.05 Submission Due Date.

Submit your proposal electronically through Periscope S2G by the Proposal Due Date and Time listed in Section 2.02.

Proposals submitted electronically through Periscope S2G may require uploading of electronic attachments. The Periscope S2G site will accept a wide variety of document types as Word, Excel, and PDF attachments but not all. You **MAY NOT** submit documents that are embedded (zip files), movies, wmp and mp3 files or password protected files, etc. Such actions may cause your proposal(s) to be deemed as "non-responsive". All cost documents must be attached as separate files.

When submitting an offer electronically through Periscope S2G, please allow sufficient time to complete the online forms and upload documents. The solicitation will end at the closing time listed in the offer. If you are in the middle of uploading your documents at the closing time, the system will stop the process and your offer will not be received by the system. It is recommended the submission process be completed the day prior to the due date, with the knowledge any changes/updates will be accepted through the due date and time.

Periscope S2G customer support may be contacted at (800) 990-9339 or S2G@periscopeholdings.com for guidance on the Periscope S2G site.

Vendors are responsible for ensuring their Periscope S2G registration information is current and correct. USHE and stakeholders shall not be responsible for missing or incorrect information contained in the vendor registration in the Periscope S2G site. Incorrect or missing vendor registration information may result in failure to receive notification from Periscope S2G regarding this procurement.

Proposals received after the due date and time will be late and ineligible for consideration. Following the deadline, the names of those responding to the RFP will be made public.

2.06 Time for Evaluation. All proposals shall remain valid for a minimum of 120 calendar days after the Proposal Due Date to allow adequate time for evaluation.

2.07 Multiple Stage Process. USHE reserves the right to conduct the RFP in a multiple stage process and narrow the number of Vendors that will move on to subsequent stages.

2.08 Oral Presentation. USHE may award a contract based on initial proposals received without discussion of such proposals with Vendors. However, USHE may require oral presentations to supplement their written proposal. These presentations may be scheduled, if required, by the Purchasing Department after proposals are received and prior to the award of the Contract. If requested, Vendors may present their proposed solution either in-person or through an on-line demonstration.

Based on preliminary total score, the evaluation committee may invite up to six (6) of the highest scoring proposals Any proposal not invited to oral presentations will not receive further consideration for award of a contract.

After the oral presentations and/or product demonstrations are complete, the committee shall be allowed to re-score the technical criteria as needed to reflect the information provided in the presentations or demonstrations. USHE reserves the right to reschedule or cancel oral presentations at any time at no cost to USHE.

2.09 Best and Final Offer. Best and Final Offer (BAFO) may be requested as part of this process from responsive and responsible proposals received.

2.10 Award of the Contract.

Upon completion of the evaluation process, USHE may award the contract ("Contract") to the highest scoring responsive and responsible supplier.

While USHE is coordinating this procurement, it is intended that the actual contracts will be with the individual technical colleges listed in 1.03.

Upon successful completion and award of this RFP as described above, USHE will post notice of an "intent to award" which shall be based upon completion of a mutually agreed upon contract.

The Purchasing Department is the only entity authorized to award a Contract for the proposed purchases.

2.11 Contract Period and Effective Date. The anticipated Contract term will be for a period of three (3) years, with an option to renew for two (2) additional periods of one (1) year each at USHE's discretion. The anticipated effective date of the Contract is July 2024.

2.12 Costs and Fees.
Cost for initial set up, data transfer, and cost of physical time clocks must be firm and considered as "all-inclusive". Variable processing costs, to include payroll processing, tax filing, and W-2 processing for the first or full term of three (3) years must also be firm based on the rate quoted.

A price increase may be requested sixty (60) days prior to end date of the current three-year term) and is subject to USHE approval. Vendor requests shall include detailed documentation explaining and supporting the price increase request. Price decreases shall be passed on to USHE immediately.

Send cost increase requests to: Russ Galt, Commissioner at the Utah System of Higher Education, russ.galt@ushe.edu.

2.13 New Technology

The awarded contract(s) may be modified to incorporate new technology or technological upgrades associated with the procurement item being solicited, including new or upgraded: (i) systems; (ii) apparatuses; (iii) modules; (iv) components; and (v) other supplementary items. Further, a maintenance or service agreement associated with the procurement item under the resulting contract(s) may be modified to include any new technology or technological upgrades. Any contract modification incorporating new technology or technological upgrades will be specific to the procurement item being solicited and substantially within the scope of the original procurement or contract.

SECTION 3 – SCOPE OF WORK

3.01 The basis of the RFP is to find a replacement payroll, timecard and benefit management system that can provide all College departments and campuses at each of the eight Utah technical colleges a system by which to easily manage their employees and prospective employees. It is anticipated that the system will have an integrated mobile app. It is also anticipated that the system will have the capability and compatibility to work with various accounting/finance systems.

3.02 Desired Specifications.

3.02.1 General Specifications

1. Proposed system is expected to be easy and intuitive to use so that an average person would have no difficulty entering, viewing, processing or reviewing timecards for themselves or those they are responsible for.
2. Proposed system must allow for both local and remote/internet access as well as access using a mobile app.
3. Proposed system must provide integrated functionality for time and attendance, payroll, benefit management, and human resource information system.
4. Provide employee portal allowing employees to review and print their tax, benefit, payroll, and time & attendance information including but not limited to pay stubs and W2 forms.

5. Offeror to explain if solution is Software as a Service (SAAS) or can be purchased and hosted on College's servers.
6. Proposed system is to provide report writing functionality allowing College to create, perform and export reports without assistance or special programming by Offeror.
7. Tracking for recruiting, and onboarding, including e-form completion, E-Verify, and I-9 forms. Electronic signature and storage of documents.
8. Preferred that solution offer applicant tracking system.
9. Preferred that solution offer Training & Performance management capabilities allowing for tracking of employee credentials, training, Learning Management System, performance reviews, etc.
10. Organizational Chart Module.
11. Offeror to describe how payroll and HR data from existing system will be stored and accessed for future reference.

3.02.2 Time and Attendance

1. Proposed solution must allow for various methods of time collection such as: computer based, mobile app, and physical time clock.
2. Physical time clock must be compatible with HID proximity iclass cards. In addition, they must allow employees the ability to view simple information such as total hours for day, week, pay period, and enter breaks or lunches via time clock display. Offeror to provide specifications and image of proposed physical time clock. Contractor may submit alternates.
3. Geofencing capabilities.
4. Time and attendance functionality should allow for rounding rules.
5. Input of employee schedules.
6. Provide employees with an internet-based web portal and mobile app to view timecard request and enter vacation, sick and comp time for approval.
7. Real time view and reporting.
8. Automated leave management processing (that includes the delegation of approval and rights).
9. Predetermined alerts for tardiness, missed punches, no entered time etc.
10. The Offeror to describe time and attendance abilities and features.
11. Ability to perform historical corrections

3.02.3 Payroll

1. Must allow for flexibility of monthly, bi-weekly, or semi-monthly payroll processing.
2. Unlimited pay codes.
3. Ability to have multiple pay rates for the same employee.
4. Ability to split pay between multiple cost centers.
5. Ability to run an off-cycle payroll.

6. Automated Vacation, Sick, and Comp time accrual management and customizable rules that include variable accrual polices based upon employee classifications.
7. System must be able to automatically convert overtime hours to comp time based on employee classification.
8. Real time and mock payroll preview, processing and review.
9. Standard and ADHOC payroll reports.
10. Affordable Care Act (ACA) compliance reporting.
11. Full Federal, State and local tax filing administration, including DWS/unemployment, and workers compensation.
12. New hire reporting.
13. Garnishment management and child support payments.
14. Direct deposit allowing for employee paycheck distribution (i.e. split up among more than one bank account).
15. W-2 preparation and availably for employee access via portal as well as paystubs for at least one previous year.
16. The Offeror to describe Payroll abilities and features.

3.02.4 Benefits

1. Allow online enrollment for annual benefit enrollment of employees.
2. Allow enrollment access for open enrollment; employee view to see all benefits they are enrolled in.
3. Ability to create Utah Retirement System contribution report.
4. Ability to work with TIAA and create contribution report.
5. Works with PEHP Health and Benefits Systems.
6. It is preferred, offered solution electronically connect with benefit provider.
7. Benefit reporting for internal use, as well as for remittance to various providers.
8. Automatically create payroll deduction (s).
9. Full-time benefited employees at technical colleges do not participate in Social Security, but do participate in Medicare. Offeror to describe how full-time benefited employees will be excluded from Social Security while part-time or otherwise unbenefited employees will participate in Social Security.
10. The Offeror to describe Benefit enrollment process, abilities and features.
11. The Offeror to describe Benefits abilities and features.

3.02.5 Mobile App

1. Proposed solution must provide employees with a mobile app for time collection, vacation/sick/comp time leave requests and approvals.
2. App should allow online enrollment for annual benefit enrollment of employees.

3. App should allow enrollment access for open enrollment; employee view to see all benefits they are enrolled in.
4. Employee should have access through the mobile app to perform such functions as change address, deductions, or direct deposit
5. The proposed mobile app should be compatible with both IOS and Android devices and via Intranet and Internet.
6. The Offeror to describe mobile app abilities and features.

3.02.6 Security

1. The system must offer robust security features to limit access of users to information relevant to their specific job duties and authority.
2. Security features must ensure that all employee records and confidential information are handled in accordance with all state and federal privacy and confidentiality laws.
3. SOC 2 report
4. The proposed solution must include multi-factor authentication capabilities
5. The Offeror to describe security features.
6. It is preferred that proposed system utilizes Microsoft Active Directory as account authentication and security roles.
7. An audit trail must be available for all transactions in the system outlining their creation, deletion, modifications and approvals, if applicable.

3.02.7 Workflow

1. The intention of the workflow is to facilitate and streamline the approval process of timecards, vacation/sick/comp time leave requests, and benefit enrollment through the system to ensure quick and timely processing of requests with minimal manual effort.
2. The proposed system must work in a hierarchy or manually forwarded.
3. At all times, requests must be visible to requestor as to its location and time in the workflow.
4. Workflow to allow for the use of a mobile app in the workflow as to creation and approval of requests.
5. The Offeror to describe the proposed system workflow abilities and features.

3.02.8 Compatibility with various accounting/finance systems

1. Proposed solution must be compatible with various accounting/finance systems, allowing simple upload of payroll expense data into the accounting/finance system.
2. Offeror to describe the compatibility of proposed solution to with accounting/finance systems.

3. Offered solution must be maintained to allow continued compatibility with accounting/finance systems with regard to upgrades, patches, versions or other updates to ensure continued compatibility.

3.02.9 Installation/Training/Warranty

1. Training is to take place at the main campuses of the various technical colleges. Training should commence immediately upon the completion of installation and calibration. The training should involve in-depth training for at least three (3) members of the college IT staff and should be sufficient to allow them to understand and operate all functions of the system as well as allow them to troubleshoot minor issues without technician intervention or assistance. Training for human resource and payroll personnel to allow them to understand and operate all functions of the system. Up to three (3) open forum meetings for end-users which includes a question and answer section, should also be performed to demonstrate to end-users the functionality and operations of the system so that they can take full advantage of system features. All training shall be included as part of initial fee for setup. It is expected that all training is provided by skilled and educated individuals on the processes and techniques necessary to perform technical training on the software.
2. As part of annual maintenance and support fee, Offeror to provide ongoing formal training, at least annually, for College Human Resource and Payroll personnel to inform them of new features and functionality.
3. The Offeror to define the system's warranty, length, terms and conditions and exclusions.

3.02.10 Service

1. The Offeror must provide technical phone support for proposed system at least during normal business hours of 7:00AM to 5:00PM Monday through Friday current Mountain time, excluding state and federal holidays, as part of annual support and maintenance fees.
2. Offeror must show what is and is not included in annual support and maintenance fee with regard to updates, technical support etc.

Additional services can be added within the nature and intent of the scope of work, if cost determined to be fair and reasonable, by amendment, signed by both parties.

SECTION 4 – PROPOSAL REQUIREMENTS

4.01 Mandatory Requirements. Mandatory requirements will be evaluated on a Pass or Fail basis. Requirements set forth in this section are mandatory and indicate the minimal requirements that must be addressed by the Vendor. Vendors must meet all mandatory requirements without qualification. If a Vendor is not able to meet a mandatory

requirement, the Vendor's proposal will be deemed as "non-responsive" and will not be further evaluated.

A. Vendor has reviewed "Attachment A – BAA Criteria and Requirements" and understands these provisions and requirements as they apply to the product or service referenced in Sections 1.01 and 3.0.

Yes _____
No _____

B. **Completion** of the HECVAT (full version) ***and*** University of Utah Prospective Supplier Technical Questionnaire addendum, hereafter referred to as "IT Questionnaire," is **required** to ensure University IT compliance. Failure to fully complete these questionnaires will render your proposal non-responsive and it will not be further evaluated.

Do you agree to provide your completed HECVAT (full or Lite version) ***and*** IT Questionnaire addendum with your proposal for review and evaluation?

Yes _____
No _____

C. Please indicate that your proposed technologies and services adhere to the current requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act, and if web-based, will conform to Level AA web accessibility standards in the most recent version of web content accessibility guidelines (WCAG 2.0) upon the implementation of the technology? If working toward compliance, please indicate that you agree to submit your plans and timeline with your proposal to become compliant along with the completed HECVAT (full or Lite version).

Yes _____ we are compliant with current requirements of Section 508.
or
Yes_____ we are actively working toward compliance and have provided our written plan in this proposal response. If your plans and timeline are not acceptable to the University of Utah, your proposal will not be further evaluated.
No _____

Business Confidentiality Claim: It is recommended Vendors indicate through a completed business confidentiality claim (BCC) form, any information that may be seen by the Vendor as confidential. More information regarding the BCC form and protected information may be found in Section 7.01 of this RFP.

4.01.1 By responding to this solicitation, Vendors are certifying that neither they nor their principals are presently debarred, suspended, proposed for debarment or ineligible for contracting by a governmental entity. Vendor is also agreeing to notify USHE within 30 days if suspended, debarred, or declared ineligible for contracting with a government entity. Additionally, Registration in SAM.GOV is required when federal funding sources are being used for payment of services. Vendors must provide a copy of your active

registration, including unique entity ID, confirming you have no exclusions. https://sam.gov/content/home

Minimum mandatory requirements.

a. The proposed system provides integrated functionality for time and attendance, payroll, benefit management, and human resource information system. Yes / No
b. Vendor has the ability to provide full ~~Full~~ Federal, State, and local tax filing and administration. Yes / No
c. Vendor has the ability to provide direct deposit allowing for paycheck distribution. Yes /No.
d. Vendor has the ability to prepare W-2s. Yes / No
e. Vendor has the ability and intends to provide training for human resource and payroll personnel to allow them to understand and operate all functions of the system. Yes / No

Evaluated Criteria

4.02 Evaluated Criteria.

4.02.1 Functionality **(50 Points)**

1. Functionality will be evaluated on how well proposed system and solution will meet desired specifications as outlined in Section 3 – Scope of Work.
2. Any inability on the part of the vendor must be noted.

4.02.2 Service/Maintenance. **(15 Points)**

Service maintenance will be evaluated on:

1. Warranty
2. Offeror to specify number of technicians with certified training and hands on experience.
3. Offeror to specify if annual maintenance and support are required.
4. Offeror to specify number of technicians with certified training and hands on experience.
5. Offeror to specify if annual maintenance and support are required.

4.02.3 Qualifications and Expertise of Staff. **(5 Points)**

Qualifications will be evaluated based on:

1. Years of experience and qualifications of sales staff, technicians, support and training staff assigned to this RFP.

4.02.4 Cost. **(30 Points)**

All costs are to be issued separately from the proposal.

1. Price to be proposed based on number of employees that receive a check per pay period.
2. Price must include migration and initial setup of all current employees to new system.
3. Price must include all training as specified.
4. Cloud based software solutions are preferred. Offeror to identify which components are SAAS. Offeror may submit alternate pricing options for review. Evaluation will be done for the most advantageous pricing as determined to meet the needs of the users.

SECTION 5 – PROPOSAL RESPONSE FORMAT

(For Cost Proposal submission see section 5.03)

5.01 Administrative Guidance. The information provided herein is intended to assist Vendors in the preparation of proposals necessary to properly respond to this RFP. The RFP is designed to provide interested Vendors with sufficient basic information to submit proposals meeting minimum requirements, but is not intended to limit a proposal's content or to exclude any relevant or essential data therefrom. Vendors are at liberty and are encouraged to expand upon the specifications to give additional evidence of their ability to provide the services requested in this RFP.

5.02 Technical Proposal Response Format. Proposals should be concise and in outline format. Pertinent supplemental information should be referenced and included as attachments. All proposals should be organized to comply with the following sections:

DETAILED RESPONSE. This section should constitute the major portion of the proposal and must contain **a specific response in outline form to each section in this RFP. Outline numbers should correspond, in order, to the section numbers contained in this RFP.** Specific emphasis should be placed on responding to the information requested in Sections 3 and 4 but all sections and items should be fully addressed. Narrative regarding options or alternatives with complete details including how those meet or exceed the RFP requirements should be included in the relevant section. Failure to provide written response to items indicated in this RFP will be interpreted by USHE as an *inability* by the Vendor to provide the requested product, service or function and may be deemed as "Non-responsive"

ADDITIONAL INFORMATION: Miscellaneous additional information and attachments, if any may be submitted by the Vendor.

5.03 Cost Proposal Response Format. **Pricing information MAY NOT be included in the technical portion of your proposal. Vendors must submit a separate cost proposal allowing costs to be evaluated independently of other criteria in the proposal. Inclusion of any cost or pricing data within the technical proposal may result in your proposal being deemed as "non-responsive."**

The cost proposal must be attached as a separate document and identified as "Cost Proposal" with your company name in Periscope S2G if your submission is electronic.

Failure to submit the cost proposal form included in this RFP may cause your proposal to be deemed "non-responsive." Incomplete cost proposal forms will receive zero cost points.

Standard Cost Formula: (Alternate formula may be used with Purchasing's approval.)

The following formula shall be used to determine the cost score: *Cost Points*((2-(proposed fee/lowest proposed fee)))*

SECTION 6 – PROPOSAL EVALUATION

6.01 Proposal Evaluation Criteria. The criteria to be used to evaluate proposals, listed with their relative weight in *points,* are as follows: Evaluation criteria must correspond with the proposal requirements listed in Section 4.

A. Responsive / Non-responsive- Vendors who are deemed as "responsive" to this request shall advance to further scoring as listed below. Vendors who are deemed as "non-responsive" shall not advance further in this request.

Evaluated Criteria (Section 4.02)	Points
Functionality	50
Service/Maintenance	15
Qualifications	5
Cost	30
Total	100

6.02 Evaluation Process. All proposals in response to this RFP will be evaluated as follows:

1. All proposals will be reviewed to determine their responsiveness to the requirements of the RFP. Non-responsive proposals (those not conforming to minimum RFP requirements) shall be eliminated from further consideration. Each Vendor bears the sole responsibility for the items included or not included in the response submitted by that Vendor. USHE reserves the right to disqualify any proposal that includes significant deviations or exceptions to the terms, conditions and/or specifications in this RFP at any time the deviations or exceptions are discovered.

2. Proposals will be reviewed and evaluated by the evaluation committee based upon the quality of information received and the information that supports the respondent's ability to meet or exceed the technical requirements stated in the RFP and is subject to all advancement criteria or multi-stage process stated. Proposals may be deemed non-responsive and disqualified at any stage of the process the disqualifying factor is discovered. At the conclusion of the technical evaluation, the Purchasing Department will evaluate the cost proposals according to the formula, published in Section 5.03 and in accordance with the Utah Procurement Code. **Cost scoring shall be based on**

the lowest responsive and responsible price offered meeting or exceeding all minimum requirements listed in this RFP. The points allocated to each cost proposal will be added to the corresponding proposal's total technical score.

3. Oral or product demonstrations may be required from eligible proposals.

   Based on preliminary total score, the evaluation committee may invite up to six (6) of the highest scoring proposals. Any proposal not invited to oral presentations will not receive further consideration for award of a contract.

   After the oral presentations and/or product demonstrations are complete, the committee shall be allowed to re-score the technical criteria as needed to reflect the information provided in the presentations or demonstrations. USHE reserves the right to reschedule or cancel oral presentations at any time at no cost to USHE.

   Proposals that do not meet the parameters will not be invited to oral presentations and shall receive no further consideration for contract award.

   USHE may choose to make an award directly from the responses received. USHE will be the sole judge as to the overall acceptability of any proposal or to judge the individual merits of specific provisions within competing offers.

4. Upon request, a Best and Final Offer (BAFO) may be requested as part of this process from responsive and responsible proposals received.

SECTION 7 - GENERAL PROVISIONS

7.01 Protected Information. Under the Government Records Access and Management Act, Utah Code §§ 63G-2-101 to -901, as amended ("GRAMA"), certain information submitted in the proposal(s) may be open for public inspection or disclosure. Pursuant to Section 63G-2-309 of GRAMA, any confidential information provided to the University which Vendor believes should be protected from inspection or disclosure must be accompanied by a written claim of confidentiality and a concise statement of reasons supporting such claim. A copy of the University's standard business confidentiality claim form may be found at (http://fbs.admin.utah.edu/download/purchasing/Business_Confidentiality_Claim_Form.pdf). **Non-specific statements of confidentiality (e.g., marking a document confidential or proprietary in a cover letter, header, footer or watermark) are insufficient to claim confidentiality under GRAMA.** All material contained in and/or submitted with the proposal becomes the property of the University and may be returned only at the University's option. Any confidentiality and non-use obligations applicable to the University as a consequence of the Contract will be subject in all cases to the University's obligations under GRAMA.

7.02 Incurring Costs. The University will not be liable for any cost which Vendors may incur in connection with the preparation or presentation of their proposal(s). Proposals should be concise, straightforward and prepared simply and economically. Expensive displays, bindings or promotional materials are neither desired nor required. However, these instructions are not intended to limit a proposal's content or exclude any relevant or essential data therefrom.

7.03 Addendum to RFP. In the event the University deems it necessary to revise this RFP in whole or in part, an addendum will be provided to relevant vendors.

7.04 Other Communications. During the RFP process (from the date of issue through the date of contract award or other final decision) the Purchasing Department is the sole source of official information regarding this RFP. All other communications, both spoken and written, which are received by any representative of the Vendor from other sources (such as employees in the using department) should be confirmed by the Vendor with the buyer in the Purchasing Department assigned to this RFP as being true and accurate prior to incorporating such information into their response. This refers to both formal and informal conversations and communications. Significant changes to the RFP will always be issued as a formal, written addendum.

7.05 Alternative Proposals. A Vendor may submit more than one proposal, each of which must follow the Proposal Response Format (section 5 herein) and satisfy the requirements of this RFP. The Vendor's primary proposal must be complete and comply with all instructions. The alternative proposals may be in abbreviated form following the Proposal Response Outline but providing complete information only for sections which differ in any way from those contained in the prime proposal. If alternative proposals are submitted, the Vendor must explain the reasons for the alternative(s) and its comparative benefits. Each proposal submitted will be evaluated on its own merits.

7.06 Authorized Vendor Representatives. The University reserves the right to require a change in the individual assigned to represent the Vendor if the assigned representative is not serving the needs of the University in an acceptable manner. This right shall carry forward through the response period and, with the successful Vendor, during the term of the Contract.

7.07 Award of Subcontracts. For each subcontract, if any, which the Vendor proposes to award, the Vendor shall specify in writing the proposed subcontractor's name and address, and the purpose of each subcontract. Any Vendor proposing subcontracts as a part of a proposal must explicitly state so in the proposal. Written approval by the Purchasing Department is required prior to the awarding of any subcontracts. Any Subcontractor shall be required to provide evidence to the University of the same insurance provisions and coverages as described in section 7.29 of this RFP.

7.08 Assignment. Vendor shall not assign or subcontract any portion of its obligations under the Contract without the prior written consent of the University Purchasing Department.

Assignment or subcontracting shall in no way relieve the Vendor of any of its obligations under the Contract.

7.09 Remedies; Governing Law; Venue. The laws of the State of Utah shall apply in all disputes arising out of this RFP, without application of any principles of choice of laws. The Contract will be governed by the laws of the State of Utah, without regard to conflicts of laws principles. Venue for any lawsuits, claims, or other proceedings between the Contract parties relating to or arising under the Contract shall be exclusively in the State of Utah. The Contract will not require either Vendor or the University to arbitrate any dispute arising under the Contract.

7.10 Compliance. The Vendor hereby agrees to abide with all applicable federal, state, county and city laws and regulations and to be responsible for obtaining and/or possessing any and all permits and licenses that may be required.

7.11 Cancellation. Inadequate delivery, unsatisfactory service or Vendor's failure to adhere to the Contract covenants may result in University's cancellation of the Contract. The Vendor shall be responsible for reimbursing the University for expenses incurred as a result of unacceptable service. In the event that either party determines that a material breach has occurred that would be cause for cancellation of the Contract, the party wishing to cancel shall notify the other party of the alleged breach in writing, and allow the other party thirty (30) days in which to cure the alleged breach.

If the alleged breach is not cured or substantial steps to cure the alleged breach are not taken within this period, the non-defaulting party may cancel the Contract at the end of said thirty (30) day period.

7.12 Acceptance of Services Rendered. The University, through its designated agents and representatives, will be the sole determining judge of whether services rendered under the Contract satisfy the requirements as identified in the Contract.

7.13 Anti-Collusion. The submission of a proposal constitutes agreement that the Vendor has not divulged its proposal to, or colluded with, any other offeror or party to a proposal whatsoever.

7.14 Indemnification; Limitations of Liability. The Contract shall provide the Vendor shall hold harmless, defend and indemnify the University of Utah and its officers, employees, and agents from and against any and all claims, losses, causes of action, judgments, damages and expenses including, but not limited to attorney's fees because of bodily injury, sickness, disease or death, or injury to or destruction of tangible property or any other injury or damage resulting from or arising out of (a) performance or breach of the Contract by Vendor, or (b) Vendor's use of University premises, or (c) any act, error, or omission on the part of the Vendor, or its agents, employees, invitees, participants, or subcontractors except where such claims, losses, causes of action, judgments, damages and expenses result solely from the negligent acts or omissions or willful misconduct of the University of Utah, its officers, employees or agents.

University is a governmental entity under the Governmental Immunity Act of Utah, Utah Code Ann., Section 63G-7-101 et seq., as amended (the "Act"). Nothing in the Contract shall constitute the University's waiver of any protections, rights, or defenses applicable to the University under the Act including, without limitation, the provisions of Section 63G-7-604 regarding limitation of judgments. Without limiting the generality of the foregoing, and notwithstanding any provisions to the contrary in the Contract, any indemnity obligations of University contained in the Contract shall be subject to the Act and are further limited only to claims that arise directly and solely from the negligent acts or omissions of University.

The University will not incur, as a consequence of the Contract or otherwise, any liability for the operations, acts, or omissions of Vendor or any third party, and nothing in the Contract shall be so interpreted or construed.

The Contract will include no limitations of liability, or exclusions or remedies, for any damages other than special, indirect or consequential damages.

7.15 Restrictions. Subject to the terms of this Section 7, all proposals must clearly set forth any restrictions or provisions deemed necessary by the Vendor to effectively service the proposed Contract.

7.16 Right to Reject. The University reserves the right to reject any or all proposals and to waive any informality or technicality in any proposal in the interest of the University.

7.17 Record Keeping and Audit Rights. Any Vendor providing goods or services under any Contract shall maintain accurate accounting records for all goods and services provided thereunder, and shall retain all such records for a period of at least seven (7) years following termination of the Contract. Upon reasonable notice and during normal business hours the University, or any of its duly authorized representatives, shall have access to and the right to audit any records or other documents pertaining to the Contract. The University's audit rights shall extend throughout the term of the Contract and for a period of at least seven (7) years thereafter.

7.18 Management Reports. Upon request the Vendor must be able to summarize and concisely report pertinent information to the University in a timely manner, throughout the duration of any Contract resulting from this RFP.

7.19 Further Agreements. In addition to a proposal, the University may from time to time require a Vendor to execute certain additional documents or agreements, including without limitation a Contract, for the purpose of clarifying the intention of the parties with respect to providing the goods or services hereunder.

7.20 Relationship of the Parties. In assuming and performing the obligations of any Contract, the University and any Vendor shall each be acting as independent parties and neither shall be considered or represent itself as a joint venturer, partner or employee of the

other. Vendor affirms that the Vendor or any employee in their organization does not have a conflict of interest or potential conflict of interest with the University of Utah.

7.21 Equal Opportunity. No Vendor of goods and/or services under this RFP or any Contract shall discriminate against any employee, applicant for employment, or recipient of services on the basis of veteran status, race, religion, color, sex, sexual orientation, age, disability, or national origin.

7.22 Taxes – Vendor's Responsibility. Vendors shall be responsible for and pay all taxes which may be levied or incurred against the Vendor in connection with the performance of any services under a Contract, including taxes levied or incurred against Vendor's income, inventory, property, sales, or other taxes.

7.23 Taxes - University is Exempt. The University is exempt from State of Utah sales and excise taxes (State of Utah Sales Tax Exemption number: 11874443-002-STC). Exemption certification information appears on all purchase orders issued by the University and such taxes will not apply to the University unless otherwise noted.

7.24 Tax Liens. By submitting a proposal, the Vendor certifies that neither it nor its principals are presently subject to an outstanding tax lien in the State of Utah. If the Vendor cannot certify this statement, the Vendor will submit to the University a written explanation for the review of the University. If the Vendor is subject to any outstanding tax lien in the State of Utah, the University may reject the Vendor's quote, bid, offer, or proposal in response to the request pursuant to UCA 63G-6a-905.

7.25 Health Insurance Portability and Accountability Act (HIPAA). The University of Utah Health Sciences Center is subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This transaction may fall under the jurisdiction of HIPAA and Vendor must comply with applicable state and federal HIPAA laws. If you have any questions, please contact the HIPAA Regulatory Office at 801-587-9241.

7.26 Debarment Clause. Vendor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract), by any governmental department or agency. If Vendor cannot certify this statement, attach a written explanation for review by the University. Vendor must notify the Director of Purchasing within 30 days if debarred by any governmental entity during the Contract period.

7.27 Status Verification System. If a Contract is awarded through this RFP for the physical performance of services within the State of Utah, Vendor or Vendor's agent, contractor, subcontractor or service provider is required to register and participate in the Status Verification System (E-verify) to verify the work eligibility status of Vendor's or Vendor's agent's, contractor's, subcontractor's or service provider's employees hired on or after July 1, 2009 and employed in the State of Utah, in accordance with UCA Section 63G-12-302.

7.28 Federal Exclusion. Vendor warrants and represents that Vendor, its officers, directors, and any employees or subcontractors providing goods or services under this Contract (i) are not currently excluded, debarred, or otherwise ineligible to participate in federal health care programs as defined in 42 U.S.C. § 1320a-7b (f) or to provide goods to or perform services on behalf of the federal government as either a contractor or subcontractor. This shall be an ongoing representation and warranty during the term of this Contract and Vendor shall immediately notify University of any change in the status of the representation and warranty. University may immediately terminate the Contract for cause in the event of a breach of this section or as a result of any material change in status of the representation and warranty. Notwithstanding any other provision in the Contract, Vendor shall defend and indemnify University and its officers, employees, and agents in connection with any and all claims, losses, causes of action, judgments, fines, damages, or other similar expenses, including reasonable attorney fees, resulting from a breach of this section.

7.29 Insurance. During the term of any Contract, and for a period of two (2) years following the expiration or earlier termination of the Contract for any reason, Vendor shall maintain the following insurance policies:

a) Commercial General Liability insurance with per occurrence limits of at least $1,000,000 and general aggregate limits of at least $2,000,000.
b) If applicable to Vendor’s operations or performance of the Contract, Cyber Liability, Professional Liability, Liquor Liability, Aircraft Liability and/or Business Automobile Liability insurance covering Vendor’s owned, non-owned, and hired motor vehicles with liability limits of at least $1,000,000 per occurrence.
c) All employee related insurances, in the statutory amounts, such as worker's compensation, and employer's liability, for its employees or volunteers involved in performing services pursuant to the Contract.
d) "Special form" property insurance at replacement cost applicable to Vendor’s property or its equipment and that contains a waiver of subrogation endorsement in favor of the University.

Such insurance policies shall be endorsed to be primary and not contributing to any other insurance maintained by the University.

If applicable, Vendor shall maintain and provide evidence of an employee dishonesty (fidelity) bond or other form of surety in the minimum amount of $100,000 which guarantees that the bond or surety will reimburse the University for any pecuniary loss that may be sustained by any act of fraud, dishonesty, forgery, theft, embezzlement, malfeasance, or misappropriation on the part of Vendor, or any of its employees, officers, directors, agents, contractors or subcontractors directly or indirectly. This bond shall be issued by a responsible surety company authorized to do business within the State of Utah, and shall be subject to the reasonable approval by the University as to form and content.

Vendor's insurance carriers and policy provisions must be acceptable to the University's Risk and Insurance Manager. The University of Utah shall be named as an additional insured on the Commercial General Liability, and if applicable, Aircraft Liability, and Liquor Liability insurance policy by endorsement. Vendor will cause any of its subcontractors, who provide materials or perform services relative to this contract, to also maintain the insurance coverages and provisions listed above.

If the coverage's described above are not in place at the time a proposal is submitted, Vendor should describe in detail what types and levels of coverage are in place currently, and clearly indicate Vendor's ability and willingness to obtain the above listed coverage's if required by the University.

Vendor shall submit certificates of insurance as evidence of the above required insurance to the University prior to the commencement of this Contract (mail to: **University of Utah Purchasing Department, Attn: Associate Director of Procurement and Contracting Services, 201 S. Presidents Circle Rm 170, Salt Lake City, UT 84112**. Such certificates shall indicate that the University will be given **thirty (30)** calendar day's written notice prior to the cancellation of coverage.

University carries insurance through the State Risk Manager of the State of Utah up to the limits required by the State Risk Manager of the State of Utah and applicable law. Nothing in the Contract shall require University to carry different or additional insurance, and any obligations of University contained in the Contract to name a party as additional insured shall be limited to naming such party as additional insured with respect to University's negligent acts or omissions.

7.30 Drug- Alcohol- Tobacco-Free Campus. The University of Utah is a drug-, alcohol-, and tobacco-free campus, with no smoking and/or use of any tobacco product on all University property and in any outdoor area controlled by the University. This rule is applicable 24 hours a day, 7 days a week. The campus will officially operate as tobacco-free as of July 1, 2018. University property includes any property owned, leased, or controlled by the University and includes but is not limited to: all buildings, vehicles, residential and recreational areas, athletic fields, parking lots, parking structures, streets, sidewalks, hospitals and clinics. All representatives of the awarded Vendor, including delivery and installation personnel, shall adhere to these requirements, including being free of the effects of these substances while on campus. Not adhering to these standards shall be considered a breach of any Contract or purchase order resulting from this solicitation. Please see the following link for more information regarding the University Rule. https://regulations.utah.edu/administration/rules/R3-300A.php

7.31 Contract Terms; Incorporation by Reference. Contract provisions shall be consistent with each provision of this Section 7 in all material respects. The Contract will incorporate by reference this Section 7. If any provision of this Section 7 conflicts with any provision of the Contract, the conflicting provision of this Section 7 shall control.

7.32 Public Contract Restrictions. If Vendor has 10 or more full-time employees and the total value of the any resulting Contract is $100,000 or greater, Vendor agrees not to engage in a Boycott of the State of Israel, as defined in Utah Code § 63G-27-102(2), for the duration of any resulting contract and further certifies that it is not currently engaged in an "economic boycott," as defined in Utah Code § 63G-27-102(5), and that Vendor will notify University in writing if it begins an "economic boycott" while any resulting Contract remains in effect.

Cost Proposal Form

Request for Proposal
For Payroll/ Human Resource Information System

RFP #:

Proposal Due: _____

Vendor Name: _____

Count	Item	Estimated # of Employees	Unit Price	Warranty, License, etc.	Extended Price	Total
1	**Cost per W-2**					
2	**Cost per employee receiving paycheck per pay period**					
3	**Cost per active employee not receiving paycheck per pay period**					
4	**Migration and Initial Setup**					
5	**Training**					
6	**Cost per Physical Time Clock**					
7	**Monthly administrative charge**					
8	**Other charges (please provide detail)**					
9	**Cost per add-on modules (please provide detail)**					
10						
					Total Cost Proposal	**$0.00**

No pricing information may be included in the technical portion of your proposal. The supplier must submit a separate cost proposal allowing costs to be evaluated independently of other criteria in the proposal. Inclusion of any cost or pricing data within the technical proposal may result in your proposal being judged as non-responsive. The Cost Proposal must be attached as a separate document on BidSync if your submission is electronic, or in a separate sealed envelope if you submit a hard copy of your proposal. With either method, please clearly label your Cost Proposal as such, along with the RFP # and your company name. This Cost Proposal Form must be completed and submitted in order for your proposal to be considered.

Formula to be used in evaluating your cost proposal: Cost Points*((2-(proposed fee/lowest proposed fee)))

BAA Criteria and Requirements

A Business Associate Agreement (BAA)[1] is required when information is shared with a company or person who is not a workforce member[2] of the University of Utah's HIPAA Covered Entity[3] **AND** the company or person, on behalf of the University, performs or assists in the performance of an activity involving the use or disclosure of **Protected Health Information (PHI).**

1. Will you be considered a Business Associate[4] as defined by the HIPAA Privacy Rule?
    a. What is a Business Associate?
        i. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.
2. Will the third party create, receive, maintain, transmit, or use **PHI**?
    a. The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI).[5]
    b. "Individually identifiable health information" is information, including demographic data, that relates to:
        i. the individual's past, present or future physical or mental health or condition,
        ii. the provision of health care to the individual, or
        iii. the past, present, or future payment for the provision of health care to the individual,
    c. and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[6]
        i. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).
    d. The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

If the product or service your company is providing is subject to these requirements, a signed BAA may be required prior to the execution of a contract.

---

[1] *See* 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).
[2] *Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. *See* 45 CFR § 160.103.
[3] Generally speaking, all operating units of University of Utah Health, Health Sciences, and Huntsman Cancer Institute, as well as other operating units that rely on access to protected health information to support those operating units, are considered part of the University's HIPAA Covered Entity. (See HIPAA Hybrid Entity Designation Statement for more information.)
[4] 45 C.F.R. § 160.103.
[5] 45 C.F.R. § 160.103.
[6] 45 C.F.R. § 160.103.

UNIVERSITY OF UTAH BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement"), effective this **_____day of _____, 202___** ("Effective Date"), is entered into by and between **XXXXXXXX** ("Business Associate"), and the University of Utah, a body politic and corporate of the State of Utah, ("Covered Entity") (each a "Party" and collectively the "Parties").

The Parties have previously executed or are considering execution of contractual arrangements through which Business Associate may access, use, or disclose Protected Health Information ("PHI") in connection with its performance of services ("Services") on behalf of Covered Entity. When used in this Agreement, the term "Underlying Agreement" means all current and future agreements between the Parties in which Business Associate may access, use, or disclose PHI in connection with its performance of Services. The Parties are committed to complying with the regulations found at 42 C.F.R part 2, with the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act of 2009, as codified at 42 U.S.C. § 17901 *et seq.* ("HITECH Act"), and any current and future regulations promulgated under HIPAA or the HITECH Act. HIPAA, the HITECH Act, and any current and future regulations promulgated under either are referred to in this Agreement as "HIPAA Rules" This Agreement sets forth the terms and conditions pursuant to which PHI (electronic and non-electronic) that is created, received, used, maintained, or transmitted by Business Associate from or on behalf of Covered Entity, will be handled between Business Associate and Covered Entity and with third parties during the term of the Underlying Agreement and after its termination. The Parties acknowledge that Covered Entity is engaged in the provision of both health care and health plan services. Nothing in this Agreement shall be interpreted as permitting comingling or other sharing of PHI between the distinct covered functions of Covered Entity unless otherwise permitted by applicable law.

DEFINITIONS:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the University of Utah

1. PERMITTED ACCESS, USE, AND DISCLOSURE OF PHI

a. Services. Pursuant to the Underlying Agreement, Business Associate provides Services for Covered Entity that may involve the access, use, or disclosure of PHI. Except as otherwise specified herein,

Business Associate may make use of Covered Entity's PHI as necessary to perform the services set forth in the Underlying Agreement. All other uses not authorized by this Agreement are prohibited. Further, Business Associate may only disclose PHI as authorized by this Agreement or as required by HIPAA Rules.

b. Business Activities of Business Associate. Unless otherwise limited or prohibited by this Agreement and provided such access, use, or disclosure of PHI would not violate HIPAA Rules if done by the Covered Entity, Business Associate may:

i. Use PHI for proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

ii. Disclose PHI to third parties for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate, provided that Business Associate represents to Covered Entity, in writing, that (i) the disclosures are required by law, or (ii) Business Associate obtained written assurances from the third party regarding its confidential handling of such PHI as required under 45 C.F.R. §§164.314 and 164.504(e)(4), and the third party notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Data Aggregation. Business Associate may provide data aggregation services relating to the health care operations of Covered Entity.

2. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PHI

a. Responsibilities of Business Associate. Business Associate shall:

i. Not access, use, or disclose PHI other than as permitted or required by this Agreement or as required by law.

ii. Use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent access, use, or disclosure of PHI other than as authorized under this Agreement.

iii. Report, in writing, to Covered Entity within five (5) business days any unauthorized access, use, or disclosure of PHI of which it becomes aware, including breaches of unsecured PHI as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware, and cooperate with Covered Entity in any mitigation or breach reporting efforts. Notwithstanding the foregoing, the Parties acknowledge that Business Associate is likely to experience security incidents that do not result in unauthorized access, use, or disclosure of PHI. The Parties agree that this paragraph constitutes notice to Covered Entity of any such unsuccessful security incident. By way of example, unsuccessful security incidents covered by this paragraph include firewall pings and port scans of Business Associate.

iv. In accordance with 45 C.F.R. §§ 164.308(b)(2) and 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to terms and conditions that are materially similar to those that apply to Business Associate with respect to such information.

v. Not export, or allow any agent or subcontractor to export, PHI for storage beyond the borders of the United States of America.

vi. With respect to any employee, agent, or subcontractor who has access to PHI from beyond the borders of the United States of America:

1. Ensure that any such individuals are bound by the terms and conditions of this Agreement or a subcontractor Agreement containing materially similar terms and conditions; and

2. Ensure that any such individuals are subject to the jurisdiction of the courts in the United States of America; and

3. Ensure that any such individuals have received current training on HIPAA Rules.

vii. As applicable, within ten (10) business days of a request from Covered Entity, make available PHI in a designated record set to Covered Entity, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524.

viii. As applicable, within ten (10) business days of a request from Covered Entity, make any amendments to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526.

ix. As applicable, maintain and make available the information required to provide an accounting of disclosures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528.

x. To the extent Business Associate carries out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

xi. Make its internal practices, books, and records available to the Secretary and to the Covered Entity for purposes of determining compliance with HIPAA Rules.

xii. Comply with minimum necessary requirements under the HIPAA Rules.

xiii. To the extent that in performing its services for or on behalf of the Covered Entity, Business Associate uses, discloses, maintains or transmits PHI that is protected by the regulations pertaining to substance abuse disorder treatment located at 42 C.F.R. part 2, Business Associate acknowledges that it is a Qualified Service Organization for the purpose of such federal law; acknowledges that in receiving, storing, processing or otherwise dealing with any such patient records, it is fully bound by the part 2 Regulations; and, if necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the part 2 Regulations.

b. Responsibilities of Covered Entity. Covered Entity shall:

i. Inform Business Associate of any limitations in the form of notice of privacy practices that Covered Entity provides to individuals pursuant to 45 C.F.R. §164.520, to the extent that such limitation may affect Business Associate's access, use, or disclosure of PHI.

ii. Inform Business Associate of any changes in, or revocation of, the permission by an individual to access, use, or disclose PHI, to the extent that such limitation may affect Business Associate's access, use, or disclosure of PHI.

iii. Notify Business Associate, in writing and in a timely manner, of any restriction on the access, use, or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect the access, use, or disclosure of PHI by Business Associate.

iv. Except if Business Associate will access, use, or disclose PHI for (and the Underlying Agreement includes provisions for) data aggregation, or management, administrative, or legal responsibilities of Business Associate, Covered Entity will not request Business Associate to access, use, or disclose PHI in any manner that would not be permissible under HIPAA Rules if done by the Covered Entity.

3. TERMS AND TERMINATION

a. Term. The Term of this Agreement shall commence on the Effective Date and shall terminate on the termination date of the Underlying Agreement or on the date Covered Entity terminates this Agreement for cause as authorized in Section 3(b), whichever is sooner.

b. Termination for Cause. Covered Entity may terminate this Agreement if Covered Entity determines Business Associate has violated a material term of this Agreement and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity.

c. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate agrees to return or destroy all PHI pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(J), if it is feasible to do so. If it is not feasible for Business Associate to return or destroy PHI, Business Associate will notify Covered Entity in writing. Said notification shall include: (i) a statement that Business Associate has determined that it is not feasible to return or destroy the PHI in its possession, and (ii) the specific reasons for such determination. Business Associate further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement to Business Associate's access, use, or disclosure of any PHI retained after the termination of this Agreement, and to limit any further access, use, or disclosure to the purposes that make the return or destruction of the PHI infeasible. If destroyed, Business Associate shall provide Covered Entity a written statement that confirms that all PHI in the possession of Business Associate has been eliminated. If it is infeasible for Business Associate to obtain any PHI from a subcontractor or agent, Business Associate must provide a written explanation to Covered Entity of the reasons therefor, and require the subcontractors or agents to agree to extend any and all protections, limitations, and restrictions contained in this Agreement to the subcontractors' or agents' access, use, or disclosure of any PHI retained after the termination of this Agreement, and to limit any further access, use, or disclosure to the purposes that make the return or destruction of the PHI infeasible.

d. Automatic Termination. This Agreement will automatically terminate without any further action of the Parties upon the termination or expiration of the Underlying Agreement.

4. INSURANCE AND LIABILITY

a. Insurance. Business Associate will procure and maintain in effect during the term of this Agreement: (1) Commercial General Liability insurance coverage with limits of not less than $1 million per occurrence and $3 million aggregate; (2) Professional Liability (Errors & Omissions) – including Technology insurance with limits of not less than $1 million per occurrence and $2 million aggregate; and (3) Cyber Liability/Data Security insurance with limits of not less than $1 million per occurrence. If requested, Business Associate will provide a certificate of insurance as evidence of continuous coverage of the insurance policies required above.

b. Liability. Business Associate shall reimburse Covered Entity for any fees or costs related to forensic investigation, breach notification, and credit monitoring, in each case as such fees or costs are actually and reasonably incurred and that arise from a data breach or security incident experienced by Business Associate and/or its subcontractors. Business Associate agrees to indemnify and defend Covered Entity as well as its trustees, officers, and employees for any costs, fees, fines, including reasonable attorney fees and court costs (collectively, "Losses"), arising from any settlement, judgment or government action, where such Losses are actually and reasonably incurred from a data breach or security incident experienced by Business Associate and/or its subcontractors.

5. MISCELLANEOUS

a. Survival. The respective rights and obligations of Business Associate and Covered Entity under this Agreement shall survive termination of this Agreement indefinitely.

b. Amendments; Waiver. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events. The Parties agree to take such action as is required to amend this Agreement from time to time as necessary to ensure compliance with the HIPAA Rules or other applicable law.

c. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

d. No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

e. No Agency Relationship. Nothing in this Agreement shall be interpreted to create an agency relationship between the Parties.

f. **Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below:**

If to Business Associate, to:

_____

_____

Attn: _____

Fax: _____

If to Covered Entity, to:

50 North Medical Drive

Salt Lake City, Utah 84132

Attn: Privacy Officer

Email: privacy@utah.edu

Fax: 801-587-9443

If Business Associate gives no address, Covered Entity may use the address for Business Associate on file with Covered Entity's Information Privacy Office.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

Business Associate

By: _____
(Signature)

_____
(Print Name)

Title: _____

Date: _____

UNIVERSITY OF UTAH

By: _____
(Signature)

Brent T. Wilson

Title: Chief Compliance Officer

University of Utah Health

Date: _____

EDUCAUSE

Shared Assessments Introduction

Campus IT environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As campuses deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many campuses have established a cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other campuses don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by campus customers, often answering similar questions repeatedly. Both the provider and consumer of cloud services are wasting precious time creating, responding, and reviewing such assessments.

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

The Higher Education Community Vendor Assessment Toolkit:
- Helps higher education institutions ensure that vendor 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 vendor services without increasing risks
- Reduces the burden that service providers face in responding to requests for security assessments from higher education institutions

The Higher Education Community Vendor Assessment Toolkit is a suite of tools built around the original HECVAT (known now as HECVAT - Full) to allow institutions to adopt, implement, and maintain a consistent risk/security assessment program. Tools include:
- **HECVAT - Triage**: Used to initiate risk/security assessment requests - review to determine assessment requirements
- **HECVAT - Full**: Robust questionnaire used to assess the most critical data sharing engagements
- **HECVAT - Lite**: A lightweight questionnaire used to expedite process
- **HECVAT - On-Premise**: Unique questionnaire used to evaluate on-premise appliances and software

The HECVAT (and Toolkit) 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 vendor provided 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

This Higher Education Cloud Vendor Assessment Toolkit 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).

Proceed to the next tab, Instructions.

HECVAT - Full | Instructions

Target Audience

These instructions are for vendors interested in providing the institution with a software and/or a service.
This worksheet should not be completed by an institution entity. The purpose of this worksheet is for the vendor to submit robust security safeguard information in regards to the product (software/service) being assessed in the institution's assessment process.

Document Layout

There are five main sections of the Higher Education Community Vendor Assessment Tool - Full, all listed below and outlined in more detail. This document is designed to have the first two sections populated first; after the Qualifiers section is completed it can be populated in any order. Within each section, answer each question top-to-bottom. Some questions are nested and may be blocked out via formatting based on previous answers. Populating this document in the correct order improves efficiency.
Do not overwrite selection values (data validation) in column C of the HECVAT - Full | Vendor Response tab.

General Information	This section is self-explanatory; product specifics and contact information. GNRL-01 through GNRL-15 should be populated by the Vendor.
Qualifiers	Populate this section **completely** before continuing. Answers in this section can determine which sections will be required for this assessment. By answering "No" to Qualifiers, their matched sections become optional and are highlighted in orange.
Documentation	Focused on external documentation, the institution is interested in the frameworks that guide your security strategy and what has been done to certify these implementations.
Company Overview	This section is focused on company background, size, and business area experience.
Safeguards	The remainder of the document consists of various safeguards, grouped generally by section.

In sections where vendor input is required there are only one or two columns that need modification, Vendor Answers and Additional Information, columns C and D respectively (see Figure 1 below). You will see that sometimes C and D are separate and other times are merged. If they are separate, C will be a selectable, drop-down box and any supporting information should be added to column D. If C and D are merged, the question is looking for the answer to be in narrative form. At the far right is a column titled "Guidance". After answering questions, check this column to ensure you have submitted information/documentation to sufficiently answer the question. Use the "Additional Information" column to provide any requested details.

Figure 1:

C	D	E
Vendor Answers	**Additional Information**	**Guidance**
No		Provide a brief description.

Optional Safeguards Based on Qualifiers

Not all questions are relevant to all vendors. Qualifiers are used to make whole sections optional to vendors depending on the scope of product usage and the data involved in the engagement being assessed. Sections that become optional have the section titles and questions highlighted in orange (see Figure 2). For this example, questions in the HIPAA section become optional based on the answer to QUAL-01.

Figure 2:

HIPAA - Optional based on QUALIFIER response.		Vendor Answers	Additional Information
HIPA-01	*Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?*		

Definitions

Institution	Any school, college, or university using the Higher Education Community Vendor Assessment Tool - Lite
Vendor Hosting Regions	The country/region in which the vendor's infrastructure(s) is/are located, including all laws and regulations in-scope within that country/region.
Vendor Work Locations	The country/region(s) in which the vendor's employees and sub-contractors are located.

Data Reporting and Scoring

To update data in the Report tabs, click Refresh All in the Menu tab. Input provided in the HECVAT tab is assessed a preliminary score pending review by the assessing institution.
Note for institution assessors and vendors: Until an institution assesses HECVAT responses, the scoring is incomplete. Assessors must complete Step 2 in the Analyst Report tab to convert qualitative responses to quantitative values. Once this step is complete, the scoring system is fully populated.

Proceed to the next tab, HECVAT - Full | Vendor Response.

Assessment Instructions For Risk/Security Assessors

1. **Begin** your assessment by selecting the Analyst Report tab
2. **Select** the appropriate security standard used in your institution (cell C10) before you begin.
3. **Select** compliant states for vendor responses in column G. **Yes** means compliant. **No** means not compliant.
   Note: Review the Analyst Reference tab for guidance and question/response interpretation.
4. **Override** default weights to meet your Institution's needs in column I.
5. **Navigate** to the Summary Report tab once all responses are evaluated and compliance indicated, as appropriate.
6. **Review** details in the Summary Report and based on your assessment findings, follow-up with vendor for clarification(s) or add the Summary Report output to your Institution's reporting documents.
7. **Connect** with your higher education peers by joining the EDUCAUSE HECVAT Users Community Group at https://connect.educause.edu.

HECVAT - Full | Vendor Response

Version 3.04

Vendor Response

DATE-01	**Date**	*mm/dd/yyyy*

General Information

In order to protect the Institution and its systems, vendors whose products and/or services will access and/or host institutional data must complete the Higher Education Community Vendor Assessment Toolkit (HECVAT). Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least data and metadata. Answers will be reviewed by Institution security analysts upon submittal. This process will assist the institution in preventing breaches of protected information and comply with Institution policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security Assessment and should be completed by a vendor. Review the *Instructions* tab for further guidance.

GNRL-01 through GNRL-08; populated by the Vendor

GNRL-01	Vendor Name	*Vendor Name*
GNRL-02	Product Name	*Product Name and Version Information*
GNRL-03	Product Description	*Brief Description of the Product*
GNRL-04	Web Link to Product Privacy Notice	*https://www.vendor.domain/privacynotice*
GNRL-05	Web Link to Accessibility Statement or VPAT	*https://www.vendor.domain/vpat*
GNRL-06	Vendor Contact Name	*Vendor Contact Name*
GNRL-07	Vendor Contact Title	*Vendor Contact Title*
GNRL-08	Vendor Contact Email	*Vendor Contact E-mail Address*
GNRL-09	Vendor Contact Phone Number	*555-555-5555*
GNRL-10	Vendor Accessibility Contact Name	*Vendor Accessibility Contact Name*
GNRL-11	Vendor Accessibility Contact Title	*Vendor Accessibility Contact Title*
GNRL-12	Vendor Accessibility Contact Email	*Vendor Accessibility Contact E-mail Address*
GNRL-13	Vendor Accessibility Contact Phone Number	*555-555-5555*
GNRL-14	Vendor Hosting Regions	*See Instructions tab for guidance*
GNRL-15	Vendor Work Locations	*See Instructions tab for guidance*

Instructions

Step 1: Complete the *Qualifiers* section first; responses in this section drive dictate question response requirements throughout the HECVAT Full.
Step 2: Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order.
Step 3: Submit the completed Higher Education Community Vendor Assessment Toolkit (HECVAT) to the Institution according to institutional procedures.

Qualifiers		Vendor Answers	Additional Information	Guidance	Analyst Notes
The institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented and allows for various parties to utilize this common documentation instrument. **Responses to the following questions will determine the need to answer additional questions below**.					
QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?			Standard Guidance	
QUAL-02	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)			The Institution views hosted solutions such as AWS, Rackspace, Azure, and other PaaS/SaaS offerings as third parties. If services such as these are used in your environment, respond "Yes".	
QUAL-03	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?				

QUAL-04	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?				
QUAL-05	Is the vended product designed to process or store Credit Card information?			Answer yes if your product handles PCI (Credit Card) information, either directly or via a third party	
QUAL-06	Does your company provide professional services pertaining to this product?			Answer yes if you provide consulting	
QUAL-07	Select your hosting option	2) Physical Co-location		N/A	
Company Overview		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.			N/A	
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?				
COMP-03	Do you have a dedicated Information Security staff or office?				
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)				
COMP-05	Use this area to share information about your environment that will assist those who are assessing your company data security program.			N/A	
Documentation		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?				
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?				
DOCU-03	Have you received the Cloud Security Alliance STAR certification?				
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)				
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?			.	
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?				

DOCU-07	Does your organization have a data privacy policy?				
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?				
DOCU-09	Do you have a documented change management process?				
DOCU-10	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?			If your answer is 'I do not know', select 'No'. If the VPATs/ACR is for an older version of the product or has not been updated, its information does not accurately reflect accessibility of the product under consideration.	
DOCU-11	Do you have documentation to support the accessibility features of your product?				
IT Accessibility		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
ITAC-01	Has a third party expert conducted an audit of the most recent version of your product?				
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?				
ITAC-03	Have you adopted a technical or legal standard of conformance for the product in question?				
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?				
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?				
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?				
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?				
ITAC-08	Can all functions of the application or service be performed using only the keyboard?				
ITAC-09	Does your product rely on activating a special ‘accessibility mode,’ a ‘lite version’ or accessing an alternate interface for accessibility purposes?				

Assessment of Third Parties		Vendor Answers	Additional Information	Guidance	Analyst Notes
THRD-01	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).				
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.			List each third party and why institutional data is shared with them. Format example: [Vendor] - Reason	
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?				
THRD-04	Do you have an implemented third party management strategy?			Robust answers from the vendor improve the quality and efficiency of the security assessment process.	
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)			Make sure you address any national or regional regulations	

Consulting		Vendor Answers	Additional Information	Guidance	Analyst Notes
CONS-01	Will the consulting take place on-premises?				
CONS-02	Will the consultant require access to Institution's network resources?				
CONS-03	Will the consultant require access to hardware in the Institution's data centers?				
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?				
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?				
CONS-06	Will any data be transferred to the consultant's possession?				
CONS-07	Is it encrypted (at rest) while in the consultant's possession?				
CONS-08	Will the consultant need remote access to the Institution's network or systems?				
CONS-09	Can we restrict that access based on source IP address?				

Application/Service Security		Vendor Answers	Additional Information	Guidance	Analyst Notes
APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?			This includes end-users, administrators, service accounts, etc. PBAC would include various dynamic controls such as conditional access, risk-based access, location-based access, or system activity based access.	
APPL-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?			This includes system administrators and third party personnel with access to the system. PBAC would include various dynamic controls such as conditional access, risk-based access, location-based access, or system activity based access.	
APPL-03	Does the system provide data input validation and error messages?				
APPL-04	Are you using a web application firewall (WAF)?				
APPL-05	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)			Include any in-house developed or contract development	
APPL-06	Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?			If the web application only works with a subset of modern supported browsers, please indicate that here	
APPL-07	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?			Select N/A if there is no mobile version of your app	
APPL-08	Does your application require access to location or GPS data?				
APPL-09	Does your application provide separation of duties between security administration, system administration, and standard user functions?				
APPL-10	Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?				
APPL-11	Have your developers been trained in secure coding techniques?				
APPL-12	Was your application developed using secure coding techniques?				
APPL-13	Do you subject your code to static code analysis and/or static application security testing prior to release?				
APPL-14	Do you have software testing processes (dynamic or static) that are established and followed?				
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?			Answer 'Yes' only if user AND administrator authentication is supported. If partially supported, answer 'No'. Ensure you respond to any guidance in the Additional Information column.	

AAAI-02	Does your solution support local authentication protocols for user and administrator authentication?				
~~AAAI-03~~	~~Can you enforce password/passphrase aging requirements?~~				
~~AAAI-04~~	~~Can you enforce password/passphrase complexity requirements [provided by the institution]?~~				
~~AAAI-05~~	~~Does the system have password complexity or length limitations and/or restrictions?~~				
~~AAAI-06~~	~~Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?~~				
~~AAAI-07~~	~~Does your organization participate in InCommon or another eduGAIN affiliated trust federation?~~				
AAAI-08	Does your application support integration with other authentication and authorization systems?				
~~AAAI-09~~	~~Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]~~			An answer of 'Yes' should be well-supported in the Additional Information column, and all elements of interest should be sufficiently addressed.	
AAAI-10	Do you support differentiation between email address and user identifier?				
~~AAAI-11~~	~~Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]~~				
~~AAAI-12~~	~~If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)~~				
AAAI-13	Does your application automatically lock the session or log-out an account after a period of inactivity?				
AAAI-14	Are there any passwords/passphrases hard coded into your systems or products?				
AAAI-15	Are you storing any passwords in plaintext?				
AAAI-16	Does your application support directory integration for user accounts?				
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?				
AAAI-18	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.			Ensure that all elements of AAAI-18 are clearly stated in your response.	

AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).			Ensure that all elements of AAAI-19 are clearly stated in your response.	
Business Continuity Plan		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
BCPL-01	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?				
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for impacted clients?				
BCPL-03	Is there a documented communication plan in your BCP for impacted clients?				
BCPL-04	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?				
BCPL-05	Are specific crisis management roles and responsibilities defined and documented?				
BCPL-06	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?				
BCPL-07	Does your organization have an alternative business site or a contracted Business Recovery provider?				
BCPL-08	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?				
BCPL-09	Is this product a core service of your organization, and as such, the top priority during business continuity planning?				
BCPL-10	Are all services that support your product fully redundant?				
Change Management		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
CHNG-01	Does your Change Management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?				
CHNG-02	Does your Change Management process also verify that all required third party libraries and dependencies are still supported with each major change?				
CHNG-03	Will the institution be notified of major changes to your environment that could impact the institution's security posture?				
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?				

CHNG-05	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?			List the current version you support and what percentage of customers are utilizing that version	
CHNG-06	Does the system support client customizations from one release to another?			Ensure that all relevant details pertaining to CHNG-06 are clearly stated in your response.	
CHNG-07	Do you have a release schedule for product updates?				
CHNG-08	Do you have a technology roadmap, for at least the next 2 years, for enhancements and bug fixes for the product/service being assessed?				
CHNG-09	Is Institution involvement (i.e. technically or organizationally) required during product updates?				
CHNG-10	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?				
CHNG-11	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?				
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?				
CHNG-13	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?				
CHNG-14	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)				
CHNG-15	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?				
Data		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
DATA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).				
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?				
DATA-03	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)				
DATA-04	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)				

DATA-05	Do all cryptographic modules in use in your product conform to the Federal Information Processing Standards (FIPS PUB 140-3)?				
DATA-06	At the completion of this contract, will data be returned to the institution and deleted from all your systems and archives?				
DATA-07	Will the institution's data be available within the system for a period of time at the completion of this contract?				
DATA-08	Can the Institution extract a full or partial backup of data?				
DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?				
DATA-10	Are these rights retained even through a provider acquisition or bankruptcy event?				
DATA-11	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?				
DATA-12	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?			Ensure that response addresses involatile storage and lists retention periods	
DATA-13	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?				
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)				
DATA-15	Are physical backups taken off site? (i.e. physically moved off site)				
DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?				
DATA-17	Are data backups encrypted?				
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)				
DATA-19	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?				
DATA-20	Does the process described in DATA-19 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?				
DATA-21	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?				
DATA-22	Will you handle data in a FERPA compliant manner?				

DATA-23	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) through any means?				
DATA-24	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)				
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?				
DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?			Please indicate which geographic regions you can provide storage in the Additional Info column.	
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?				
DCTR-04	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?				
DCTR-05	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?				
DCTR-06	Are your primary and secondary data centers geographically diverse?				
DCTR-07	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?				
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime Institute)?			Review the Uptime Institute's level/tier direction provided on their website if you need addition information	
DCTR-09	Is the service hosted in a high availability environment?				
DCTR-10	Is redundant power available for all datacenters where institution data will reside?				
DCTR-11	Are redundant power strategies tested?				
DCTR-12	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.			Ensure that all parts of DCTR-12 are clearly stated in your response.	
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?			State the ISP provider(s) in addition to the number of ISPs that provide connectivity.	
DCTR-14	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?				
~~DCTR-15~~	~~Are you requiring multi-factor authentication for administrators of your cloud environment?~~				

~~DCTR-16~~	~~Are you using your cloud providers available hardening tools or pre-hardened images?~~				
~~DCTR-17~~	~~Does your cloud vendor have access to your encryption keys?~~			Describe your key management practices.	
Disaster Recovery Plan		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).			Provide a valid URL to your current DRP or submit it along with this fully-populated HECVAT.	
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?				
DRPL-03	Can the Institution review your DRP and supporting documentation?				
DRPL-04	Are any disaster recovery locations outside the Institution's geographic region?				
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?				
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?				
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?				
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?				
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)			Ensure that all elements of DRPL-09 are clearly stated in your response.	
DRPL-10	Has the Disaster Recovery Plan been tested in the last year?				
DRPL-11	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?				
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?				
FIDP-02	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info				
FIDP-03	Do you have a documented policy for firewall change requests?				
FIDP-04	Have you implemented an Intrusion Detection System (network-based)?				

FIDP-05	Have you implemented an Intrusion Prevention System (network-based)?				
FIDP-06	Do you employ host-based intrusion detection?				
FIDP-07	Do you employ host-based intrusion prevention?				
FIDP-08	Are you employing any next-generation persistent threat (NGPT) monitoring?				
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?				
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?			In addition to stating your intrusion monitoring strategy, provide a brief summary of its implementation.	
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?				
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?				
PPPR-02	Do you have a documented patch management process?				
PPPR-03	Can you accommodate encryption requirements using open standards?				
PPPR-04	Are information security principles designed into the product lifecycle?				
PPPR-05	Do you have a documented systems development life cycle (SDLC)?				
PPPR-06	Will you comply with applicable breach notification laws?				
PPPR-07	Will you comply with the Institution's IT policies with regards to user privacy and data protection?				
PPPR-08	Is your company subject to Institution's geographic region's laws and regulations?			State the country that governs and regulates your company	
PPPR-09	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?				

PPPR-10	Do you require new employees to fill out agreements and review policies?				
PPPR-11	Do you have a documented information security policy?				
PPPR-12	Do you have an information security awareness program?				
PPPR-13	Is security awareness training mandatory for all employees?				
PPPR-14	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?				
PPPR-15	Do you have documented, and currently implemented, internal audit processes and procedures?				
PPPR-16	Does your organization have physical security controls and policies in place?				
Incident Handling		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HFIH-01	Do you have a formal incident response plan?				
HFIH-02	Do you have either an internal incident response team or retain an external team?				
HFIH-03	Do you have the capability to respond to incidents on a 24x7x365 basis?				
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?				
Quality Assurance		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
QLAS-01	Do you have a documented and currently implemented Quality Assurance program?			Provide a valid URL to your Quality Assurance program or submit it along with this fully-populated HECVAT.	
QLAS-02	Do you comply with ISO 9001?				
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?				
QLAS-04	Do you incorporate customer feedback into security feature requests?				
QLAS-05	Can you provide an evaluation site to the institution for testing?				
Vulnerability Scanning		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
VULN-01	Are your systems and applications regularly scanned externally for vulnerabilities?				

VULN-02	Have your systems and applications had a third party security assessment completed in the last year?				
VULN-03	Are your systems and applications scanned with an authenticated user account for vulnerabilities [that are remediated] prior to new releases?				
VULN-04	Will you provide results of application and system vulnerability scans to the Institution?				
VULN-05	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).			Ensure that all elements of VULN-05 are clearly stated in your response.	
VULN-06	Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?				
HIPAA		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-05	Have you conducted a risk analysis as required under the Security Rule?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-06	Have you identified areas of risks?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-07	Have you taken actions to mitigate the identified risks?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-08	Does your application require user and system administrator password changes at a frequency no greater than 90 days?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-09	Does your application require a user to set their own password after an administrator reset or on first use of the account?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-10	Does your application lock-out an account after a number of failed login attempts?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-11	Does your application automatically lock or log-out an account after a period of inactivity?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-12	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-13	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	

HIPA-14	Does your application provide the ability to define user access levels?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-15	Does your application support varying levels of access to administrative tasks defined individually per user?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-16	Does your application support varying levels of access to records based on user ID?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-17	Is there a limit to the number of groups a user can be assigned?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-18	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-19	Does the application log record access including specific user, date/time of access, and originating IP or device?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-20	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-21	How long does the application keep access/change logs?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-22	Can the application logs be archived?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-23	Can the application logs be saved externally?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-24	Does your data backup and retention policies and practices meet HIPAA requirements?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-25	Do you have a disaster recovery plan and emergency mode operation plan?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-26	Have the policies/plans mentioned above been tested?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-27	Can you provide a HIPAA compliance attestation document?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
HIPA-29	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.	
PCI DSS		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?			Refer to PCI DSS Security Standards for supplemental guidance in this section	

PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-04	Are you classified as a service provider?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-05	Are you on the list of VISA approved service providers?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-08	What payment processors/gateways does the system support?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-09	Can the application be installed in a PCI DSS compliant manner ?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-10	Is the application listed as an approved PA-DSS application?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?			Refer to PCI DSS Security Standards for supplemental guidance in this section	
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.			Refer to PCI DSS Security Standards for supplemental guidance in this section	

HECVAT - Full | Analyst Report

Version 3.04

Institution Assessment

Instructions

Step 1: Select the security framework used at your institution in cell B10. **Step 2:** Convert qualitative vendor responses into quantitative values, starting at cell G37. **Step 3:** Review converted values, ensuring full population of report. **Step 4:** Move to the Summary Report tab.

Vendor Name	Vendor Name			**Product Name**	Product Name and Version Information
Vendor Contact Name	Vendor Contact Name			**Product Description**	Brief Description of the Product
Vendor Contact Title	Vendor Contact Title			**HECVAT Version**	Full
Vendor Email Address	Vendor Contact E-mail Address			**Date Prepared**	mm/dd/yyyy

Step 1: Select your institution's security framework		

Report Sections	Max_Score	Score	Score %
Company	80	0	0%
Documentation	220	0	0%
Accessibility	225	0	0%
Third Parties	0	0	0%
Consulting	0	0	0%
Application Security	315	0	0%
Authentication, Authorization, and Accounting	245	0	0%
Business Contituity Plan	0	0	0%
Change Management	270	0	0%
Data	440	0	0%
Datacenter	290	0	0%
Disaster Recovery Plan	0	0	0%
Firewalls, IDS, IPS, and Networking	240	0	0%
Policies, Procedures, and Processes	300	0	0%
Incident Handling	45	0	0%
Quality Assurance	90	0	0%
Vulnerability Scanning	110	0	0%
HIPAA	0	0	0%
PCI-DSS	0	0	0%
		0	
Overall Score	**2870**	**0**	**0%**

				Analyst Notes	Step 2: Override/Correct Vendor Responses and Set Weights Per Institution's Use Case			
ID	**Question**	**Vendor Answer**	**Additional Information**	**(Will show in Col F on HECVAT tab)**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
Company Overview		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
COMP-01	Describe your organization’s business background and				Qualitative Question		15	
COMP-02	Have you had an unplanned disruption to this product/service in	0			No		10	
COMP-03	Do you have a dedicated Information Security staff or office?	0			Yes		15	
COMP-04	Do you have a dedicated Software and System Development team(s)?	0			Yes		25	
COMP-05	Use this area to share information about your environment that will				Qualitative Question		15	
Documentation		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?	0			Yes		20	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or	0			Yes		20	

DOCU-03	Have you received the Cloud Security Alliance STAR certification?	0			Yes		20	
DOCU-04	Do you conform with a specific industry standard security	0			Yes		20	
DOCU-05	Can the systems that hold the institution's data be compliant with	0			Yes		20	
DOCU-06	Can you provide overall system and/or application architecture	0			Yes		20	
DOCU-07	Does your organization have a data privacy policy?	0			Yes		20	
DOCU-08	Do you have a documented, and currently implemented,	0			Yes		20	
DOCU-09	Do you have a documented change management process?	0			Yes		20	
DOCU-10	Has a VPAT or ACR been created or updated for the product and version	0			Yes		20	
DOCU-11	Do you have documentation to support the accessibility	0			Yes		20	
IT Accessibility		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
ITAC-01	Has a third party expert conducted an audit of the most recent version	0			Yes		25	
ITAC-02	Do you have a documented and implemented process for	0			Yes		25	
ITAC-03	Have you adopted a technical or legal standard of conformance	0			Yes		25	
ITAC-04	Can you provide a current, detailed accessibility roadmap	0			Yes		25	
ITAC-05	Do you expect your staff to maintain a current skill set in IT	0			Yes		25	
ITAC-06	Do you have a documented and implemented process for	0			Yes		25	
ITAC-07	Do you have documented processes and procedures for	0			Yes		25	
ITAC-08	Can all functions of the application or service be performed using only the	0			Yes		25	
ITAC-09	Does your product rely on activating a special ‘accessibility mode,’ a	0			No		25	
Assessment of Third Parties		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
THRD-01	Do you perform security assessments of third party companies with	0	0		Yes		25	
THRD-02	Provide a brief description for why each of these third parties will	0			Qualitative Question		15	
THRD-03	What legal agreements (i.e. contracts) do you have in place with these	0			Qualitative Question		15	
THRD-04	Do you have an implemented third party management strategy?	0	0		Yes		15	
THRD-05	Do you have a process and implemented procedures for managing	0	0		Yes		15	
Consulting		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
CONS-01	Will the consulting take place on-premises?	0	0		No		15	
CONS-02	Will the consultant require access to Institution's network	0	0		No		15	
CONS-03	Will the consultant require access to hardware in the	0	0		Yes		15	
CONS-04	Will the consultant require an account within the Institution's domain	0	0		No		15	
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI,	0	0		Yes		15	
CONS-06	Will any data be transferred to the consultant's possession?	0	0		No		15	
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	0	0		Yes		15	
CONS-08	Will the consultant need remote access to the Institution's network or	0	0		No		15	
CONS-09	Can we restrict that access based on source IP address?	0	0		Yes		15	
Application/Service Security		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
APPL-01	Are access controls for institutional accounts based on structured	0	0		Yes		25	

APPL-02	Are access controls for staff within your organization based on	0	0		Yes		20	
APPL-03	Does the system provide data input validation and error messages?	0	0		Yes		20	
APPL-04	Are you using a web application firewall (WAF)?	0	0		Yes		25	
APPL-05	Do you have a process and implemented procedures for managing	0	0		Yes		20	
APPL-06	Are only currently supported operating system(s), software, and	0	0		Yes		25	
APPL-07	If mobile, is the application available from a trusted source	0	0		Yes		15	
APPL-08	Does your application require access to location or GPS data?	0	0		No		25	
APPL-09	Does your application provide separation of duties between security	0	0		Yes		40	
APPL-10	Do you have a fully implemented policy or procedure that details	0	0		Yes		10	
APPL-11	Have your developers been trained in secure coding techniques?	0	0		Yes		20	
APPL-12	Was your application developed using secure coding techniques?	0	0		Yes		20	
APPL-13	Do you subject your code to static code analysis and/or static	0	0		Yes		25	
APPL-14	Do you have software testing processes (dynamic or static) that	0	0		Yes		25	
Authentication, Authorization, and Accounting		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
AAAI-01	Does your solution support single sign-on (SSO) protocols for user	0	0		1		25	
AAAI-02	Does your solution support local authentication protocols for user and administrator authentication?	0	0		1		25	
~~AAAI-03~~	~~Can you enforce password/passphrase aging requirements?~~	~~0~~	~~0~~		Yes		~~20~~	
~~AAAI-04~~	~~Can you enforce password/passphrase complexity requirements~~	~~0~~	~~0~~		Yes		~~40~~	
~~AAAI-05~~	~~Does the system have password complexity or length limitations and/or~~	~~0~~	~~0~~		No		~~40~~	
~~AAAI-06~~	~~Do you have documented password/passphrase~~	~~0~~	~~0~~		Yes		~~25~~	
~~AAAI-07~~	~~Does your organization participate in InCommon or another eduGAIN~~	~~0~~	~~0~~		Yes		~~40~~	
AAAI-08	Does your application support integration with other authentication and	0	0		Yes		20	
~~AAAI-09~~	~~Does your solution support any of the following Web SSO~~	~~0~~	~~0~~		Yes		~~15~~	
AAAI-10	Do you support differentiation between email address and user	0	0		Yes		15	
~~AAAI-11~~	~~Do you allow the customer to specify attribute mappings for~~	~~0~~	~~0~~		Yes		~~20~~	
~~AAAI-12~~	~~If you don't support SSO, does your application and/or user~~	~~0~~	~~0~~		No		~~15~~	
AAAI-13	Does your application automatically lock the session or log-out an	0	0		Yes		15	
AAAI-14	Are there any passwords/passphrases hard coded into your	0	0		No		25	
AAAI-15	Are you storing any passwords in plaintext?	0	0		No		25	
AAAI-16	Does your application support directory integration for user	0	0		Yes		20	
AAAI-17	Are audit logs available that include AT LEAST all of the following; login,	0	0		Yes		25	
AAAI-18	Describe or provide a reference to the a) system capability to log	0			Qualitative Question		25	
AAAI-19	Describe or provide a reference to the a) system capability to log	0			Qualitative Question		25	
Business Continuity Plan		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
BCPL-01	Is an owner assigned who is responsible for the maintenance and	0	0		Yes		20	
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for	0	0		Yes		20	

1

BCPL-03	Is there a documented communication plan in your BCP for impacted	0	0		Yes		25	
BCPL-04	Are all components of the BCP reviewed at least annually and	0	0		Yes		25	
BCPL-05	Are specific crisis management roles and responsibilities defined	0	0		Yes		20	
BCPL-06	Does your organization conduct training and awareness activities to	0	0		Yes		20	
BCPL-07	Does your organization have an alternative business site or a	0	0		Yes		20	
BCPL-08	Does your organization conduct an annual test of relocating to an	0	0		Yes		20	
BCPL-09	Is this product a core service of your organization, and as	0	0		Yes		15	
BCPL-10	Are all services that support your product fully redundant?	0	0		Yes		25	
Change Management		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
CHNG-01	Does your Change Management process minimally include	0	0		Yes		20	
CHNG-02	Does your Change Management process also verify that all	0	0		Yes		20	
CHNG-03	Will the institution be notified of major changes to your	0	0		Yes		25	
CHNG-04	Do clients have the option to not participate in or postpone an	0	0		Yes		10	
CHNG-05	Do you have a fully implemented solution support strategy that	0	0		Yes		15	
CHNG-06	Does the system support client customizations from one release to	0	0		Yes		25	
CHNG-07	Do you have a release schedule for product updates?	0	0		Yes		15	
CHNG-08	Do you have a technology roadmap, for at least the next 2 years,	0	0		Yes		15	
CHNG-09	Is Institution involvement (i.e. technically or	0	0		Yes		15	
CHNG-10	Do you have policy and procedure, currently implemented, managing	0	0		Yes		20	
CHNG-11	Do you have policy and procedure, currently implemented, guiding	0	0		Yes		20	
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a	0	0		Yes		15	
CHNG-13	Do procedures exist to provide that emergency changes are documented	0	0		Yes		15	
CHNG-14	Do you have an implemented system configuration	0	0		Yes		25	
CHNG-15	Do you have a systems management and configuration strategy	0	0		Yes		15	
Data		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
DATA-01	Does the environment provide for dedicated single-tenant	0	0		Yes		15	
DATA-02	Will Institution's data be stored on any devices (database servers, file	0	0		No		25	
DATA-03	Is sensitive data encrypted, using secure protocols/algorithms, in	0	0		Yes		40	
DATA-04	Is sensitive data encrypted, using secure protocols/algorithms, in	0	0		Yes		25	
DATA-05	Do all cryptographic modules in use in your product conform to the	0	0		Yes		25	
DATA-06	At the completion of this contract, will data be returned to the	0	0		Yes		20	
DATA-07	Will the institution's data be available within the system for a period of	0	0		Yes		25	
DATA-08	Can the Institution extract a full or partial backup of data?	0	0		Yes		20	
DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained	0	0		Yes		15	
DATA-10	Are these rights retained even through a provider acquisition or bankruptcy	0	0		Yes		25	
DATA-11	In the event of imminent bankruptcy, closing of business, or retirement	0	0		Yes		15	
DATA-12	Are involatile backup copies made according to pre-defined schedules	0	0		Yes		15	

DATA-13	Do current backups include all operating system software,	0	0		Yes		20	
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)	0	0		Yes		20	
DATA-15	Are physical backups taken off site? (i.e. physically moved off	0	0		Yes		20	
DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone	0	0		No		25	
DATA-17	Are data backups encrypted?	0	0		Yes		15	
DATA-18	Do you have a cryptographic key management process	0	0		Yes		10	
DATA-19	Do you have a media handling process, that is documented and	0	0		Yes		20	
DATA-20	Does the process described in DATA-19 adhere to DoD 5220.22-	0	0		Yes		20	
DATA-21	Is media used for long-term retention of business data and	0	0		Yes		25	
DATA-22	Will you handle data in a FERPA compliant manner?	0	0		Yes		15	
DATA-23	Does your staff (or third party) have access to Institutional data (e.g.,	0	0		Yes		20	
DATA-24	Do you have a documented and currently implemented	0	0		Yes		20	
Datacenter		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?	0	0		Yes		20	
DCTR-02	Are you generally able to accommodate storing each institution's data	0	0		Yes		20	
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e.,	0	0		Yes		20	
DCTR-04	Are your servers separated from other companies via a physical	0	0		Yes		20	
DCTR-05	Does a physical barrier fully enclose the physical space preventing	0	0		Yes		25	
DCTR-06	Are your primary and secondary data centers geographically diverse?	0	0		Yes		20	
DCTR-07	If outsourced or co-located, is there a contract in place to	0	0		Yes		20	
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime	0	0		Qualitative Question		20	
DCTR-09	Is the service hosted in a high availability environment?	0	0		Yes		20	
DCTR-10	Is redundant power available for all datacenters where	0	0		Yes		20	
DCTR-11	Are redundant power strategies tested?	0	0		Yes		25	
DCTR-12	Describe or provide a reference to the availability of cooling and	0			Qualitative Question		20	
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?	0	0		Yes		20	
DCTR-14	Does every datacenter where the Institution's data will reside have	0	0		Yes		20	
~~DCTR-15~~	~~Are you requiring multi-factor authentication for administrators of your~~	~~0~~	~~0~~		Yes		~~20~~	
~~DCTR-16~~	~~Are you using your cloud providers available hardening tools or pre-~~	~~0~~	~~0~~		Yes		~~20~~	
~~DCTR-17~~	~~Does your cloud vendor have access to your encryption keys?~~	~~0~~	~~0~~		No		~~20~~	
Disaster Recovery Plan		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan	0			Qualitative Question		20	
DRPL-02	Is an owner assigned who is responsible for the maintenance and	0	0		Yes		15	
DRPL-03	Can the Institution review your DRP and supporting	0	0		Yes		25	
DRPL-04	Are any disaster recovery locations outside the Institution's	0	0		No		20	
DRPL-05	Does your organization have a disaster recovery site or a contracted	0	0		Yes		20	

DRPL-06	Does your organization conduct an annual test of relocating to this site	0	0		Yes		20	
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for	0	0		Yes		20	
DRPL-08	Is there a documented communication plan in your DRP for impacted	0	0		Yes		20	
DRPL-09	Describe or provide a reference to how your disaster recovery plan is	0			Qualitative Question		20	
DRPL-10	Has the Disaster Recovery Plan been tested in the last year?	0	0		Yes		25	
DRPL-11	Are all components of the DRP reviewed at least annually and	0	0		Yes		25	
Firewalls, IDS, IPS, and Networking		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?	0	0		Yes		25	
FIDP-02	Is authority for firewall change approval documented? Please list	0	0		Yes		20	
FIDP-03	Do you have a documented policy for firewall change requests?	0	0		Yes		25	
FIDP-04	Have you implemented an Intrusion Detection System (network-	0	0		Yes		25	
FIDP-05	Have you implemented an Intrusion Prevention System (network-	0	0		Yes		20	
FIDP-06	Do you employ host-based intrusion detection?	0	0		Yes		25	
FIDP-07	Do you employ host-based intrusion prevention?	0	0		Yes		20	
FIDP-08	Are you employing any next-generation persistent threat (NGPT)	0	0		Yes		20	
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?	0	0		Yes		15	
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?	0	0		Yes		20	
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS,	0	0		Yes		25	
Policies, Procedures, and Processes		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
PPPR-01	Can you share the organization chart, mission statement, and	0	0		Yes		20	
PPPR-02	Do you have a documented patch management process?	0	0		Yes		25	
PPPR-03	Can you accommodate encryption requirements using open standards?	0	0		Yes		20	
PPPR-04	Are information security principles designed into the product lifecycle?	0	0		Yes		15	
PPPR-05	Do you have a documented systems development life cycle	0	0		Yes		20	
PPPR-06	Will you comply with applicable breach notification laws?	0	0		Yes		15	
PPPR-07	Will you comply with the Institution's IT policies with regards to user	0	0		Yes		25	
PPPR-08	Is your company subject to Institution's geographic region's laws	0	0		Yes		25	
PPPR-09	Do you perform background screenings or multi-state	0	0		Yes		20	
PPPR-10	Do you require new employees to fill out agreements and review	0	0		Yes		20	
PPPR-11	Do you have a documented information security policy?	0	0		Yes		20	
PPPR-12	Do you have an information security awareness program?	0	0		Yes		15	
PPPR-13	Is security awareness training mandatory for all employees?	0	0		Yes		15	
PPPR-14	Do you have process and procedure(s) documented, and	0	0		Yes		15	
PPPR-15	Do you have documented, and currently implemented,	0	0		Yes		15	
PPPR-16	Does your organization have physical security controls and policies in	0	0		Yes		15	
Incident Handling		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HFIH-01	Do you have a formal incident response plan?	0	0		Yes		15	

HFIH-02	Do you have either an internal incident response team or retain	0	0		Yes		15	
HFIH-03	Do you have the capability to respond to incidents on a 24x7x365	0	0		Yes		15	
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen	0	0		Yes		15	
Quality Assurance		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
QLAS-01	Do you have a documented and currently implemented	0	0		Yes		10	
QLAS-02	Do you comply with ISO 9001?	0	0		Yes		15	
QLAS-03	Will your company provide quality and performance metrics in	0	0		Yes		20	
QLAS-04	Do you incorporate customer feedback into security feature	0	0		Yes		25	
QLAS-05	Can you provide an evaluation site to the institution for testing?	0	0		Yes		20	
Vulnerability Scanning		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
VULN-01	Are your systems and applications regularly scanned externally for	0	0		Yes		15	
VULN-02	Have your systems and applications had a third party security	0	0		Yes		20	
VULN-03	Are your systems and applications scanned with an authenticated	0	0		Yes		25	
VULN-04	Will you provide results of application and system vulnerability	0	0		Yes		25	
VULN-05	Describe or provide a reference to how you monitor for and protect	0	0		Yes		20	
VULN-06	Will you allow the institution to perform its own vulnerability testing	0	0		Yes		25	
HIPAA		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HIPA-01	Do your workforce members receive regular training related to the	0	0		Yes		25	
HIPA-02	Do you monitor or receive information regarding changes in	0	0		Yes		20	
HIPA-03	Has your organization designated HIPAA Privacy and Security	0	0		Yes		20	
HIPA-04	Do you comply with the requirements of the Health Information	0	0		Yes		20	
HIPA-05	Have you conducted a risk analysis as required under the Security Rule?	0	0		Yes		20	
HIPA-06	Have you identified areas of risks?	0	0		Yes		25	
HIPA-07	Have you taken actions to mitigate the identified risks?	0	0		Yes		20	
HIPA-08	Does your application require user and system administrator password	0	0		Yes		20	
HIPA-09	Does your application require a user to set their own password after	0	0		Yes		20	
HIPA-10	Does your application lock-out an account after a number of failed login	0	0		Yes		20	
HIPA-11	Does your application automatically lock or log-out an account after a	0	0		Yes		20	
HIPA-12	Are passwords visible in plain text, whether when stored or entered,	0	0		No		20	
HIPA-13	If the application is institution-hosted, can all service level and	0	0		Yes		20	
HIPA-14	Does your application provide the ability to define user access	0	0		Yes		20	
HIPA-15	Does your application support varying levels of access to administrative	0	0		Yes		20	
HIPA-16	Does your application support varying levels of access to records based	0	0		No		20	
HIPA-17	Is there a limit to the number of groups a user can be assigned?	0	0		Yes		20	
HIPA-18	Do accounts used for vendor supplied remote support abide by the	0	0		Yes		20	
HIPA-19	Does the application log record access including specific user, date/time	0	0		Yes		20	
HIPA-20	Does the application log administrative activity, such user account	0	0		Yes		20	

HIPA-21	How long does the application keep access/change logs?	0	0		Yes		20	
HIPA-22	Can the application logs be archived?	0	0		Yes		20	
HIPA-23	Can the application logs be saved externally?	0	0		Yes		20	
HIPA-24	Does your data backup and retention policies and practices meet	0	0		Yes		15	
HIPA-25	Do you have a disaster recovery plan and emergency mode	0	0		Yes		20	
HIPA-26	Have the policies/plans mentioned above been tested?	0	0		Yes		25	
HIPA-27	Can you provide a HIPAA compliance attestation document?	0	0		Yes		20	
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?	0	0		Yes		20	
HIPA-29	Have you entered into a BAA with all subcontractors who may	0	0		Yes		25	
PCI DSS		**Vendor Answer**	**Additional Information**	**Analyst Notes**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
PCID-01	Do your systems or products store, process, or transmit cardholder	0	0		Yes		20	
PCID-02	Are you compliant with the Payment Card Industry Data Security	0	0		Yes		20	
PCID-03	Do you have a current, executed within the past year, Attestation of	0	0		Yes		25	
PCID-04	Are you classified as a service provider?	0	0		Yes		20	
PCID-05	Are you on the list of VISA approved service providers?	0	0		Yes		20	
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	0			Qualitative Question		20	
PCID-07	Describe the architecture employed by the system to verify and authorize	0			Qualitative Question		10	
PCID-08	What payment processors/gateways does the system	0			Qualitative Question		10	
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	0	0		Yes		10	
PCID-10	Is the application listed as an approved PA-DSS application?	0	0		No		25	
PCID-11	Does the system or products use a third party to collect, store,	0	0		No		25	
PCID-12	Include documentation describing the systems' abilities to comply with	0			Qualitative Question		15	

HECVAT - Full | Analyst Reference

Connect with your higher education peers by joining the **EDUCAUSE HECVAT Users Community Group** at https://connect.educause.edu.

Instructions

Use this reference guide to assess vendor responses in relation to your institution's environment. The context of HECVAT questions can change, depending on implementation specifics so these recommendations and follow-up response are not exhaustive and are meant to improve assessment and report capabilities within your institution's security/risk assessment program.

Analyst tip #1: For any answer that is deem "non-compliant" by your institution, ask the vendor if there is a timeline for implementation, a sincere commitment to customer development engagement, and/or possible implementation of compensating control(s) that offsite the risks of another component.

Analyst tip #2: If a vendor's response to a follow-up inquiry is vague or seems off-point or dismissive, respond back to the vendor contact with clear expectations for a response. Responses that fail to meet expectations thereafter should be negatively assessed based on your institution's risk tolerance and the criticality of the data involved.

Analyst tip #3: The most important tip - reject a HECVAT from a vendor if; the vendor provides the institution with a insufficiently populated HECVAT; or the vendor responses are vague and/or do not answer questions directly; or significant discrepancies are found, making the HECVAT difficult to assess.

Qualifiers		Reason for Question	Follow-up Inquiries/Responses
Qualifier responses are meant to set the response requirements for a vendor and the intended use case. Since responses to these questions can make some question sections optional, vendors often answer sections partially, if they have the proper documentation. Depending on the security program maturity and risk tolerance of your institution, not all vendor responses will be relevant.			
QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	This qualifier determines the presence of PHI in the solution and sets the HIPAA section as required appropriately.	Reference the HIPAA section for follow-up review.
QUAL-02	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)	Vendors oftentimes use other vendors to supplement and/or host their infrastructures and it is important to know what, if any, institutional data is shared with fourth-parties. Responses to this qualifier set the response requirement for the Third Parties section.	Reference the Third Parties section for follow-up review.
QUAL-03	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	This qualifier determines the existence of a complete, fully-populated BCP, maintained by the vendor, and sets the Business Continuity Plan section as required appropriately.	Reference the Business Continuity Plan section for follow-up review.
QUAL-04	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	This qualifier determines the existence of a complete, fully-populated DRP, maintained by the vendor, and sets the Business Continuity Plan section as required appropriately.	Reference the Disaster Recovery Plan section for follow-up review.
QUAL-05	Is the vended product designed to process or store Credit Card information?	This qualifier determines the presence of PCI DSS in the solution and sets the PCI DSS section as required appropriately.	Reference the PCI DSS section for follow-up review.
QUAL-06	Does your company provide professional services pertaining to this product?	When consultants are given access to a system containing institutional data, the "sharing" of data is not in the same context as traditional data sharing (i.e. hosting, etc.) and thus, many of the HECVAT questions do not apply. When consultants have access to a system (onsite of via remote affiliate-type accounts), the Consulting section is most relevant.	Reference the Consulting section for follow-up review.
QUAL-07	Select your hosting option	Understanding the hosting environment may reveal infrastructure risks that may not be apparent by other means and provides context to the responses provided throughout this HECVAT.	Follow-up inquiries for hosting options will be institution/implementation specific.

Company Overview		Reason for Question	Follow-up Inquiries/Responses
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	Defining scale of company (support, resources, skillsets), General information about the organization that may be concerning.	Follow-up responses to this one are normally unique to their response. Vague answers here usually result in some footprinting of a vendor to determine their "reputation".
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.	If a vendor says "No", it is taken at face value. If you organization is capable of conducting reconnaissance, it is encouraged. If a vendor has experienced a breach, evaluate the circumstance of the incident and what the vendor has done in response to the breach.
COMP-03	Do you have a dedicated Information Security staff or office?	Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. The size of a vendor will determine their SO size, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.	Vague responses to this question should be investigated further. Vendors without dedicated security personnel commonly have no security or security is embedded or dual-homed within operations (administrators). Ask about separation of duties, principle of least privilege, etc. - there are many ways to get additional program state information from the vendor.
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Understanding the development team size (and capabilities) of a vendor has a significant impact on their ability to produce and maintain code, adhering to secure coding best practices. The size of a vendor will determine their use of dedicated development teams, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.	Follow-up inquiries for vendor team strategies will be unique to your institution and may depend on the underlying infrastructures needed to support a system for your specific use case.

COMP-05	Use this area to share information about your environment that will assist those who are assessing your company data security program.	For the 20% that HECVAT may not cover, this gives the vendor a chance to support their other responses. Beware when this area is populated with sales hype or other non-relevant information. Thorough documentation, supporting evidence, and/or robust responses go a long way in building trust in this assessment process.	This is a freebie to help the vendor state their "case". If a vendor does not add anything here (or it is just sales stuff), we can assume it was filled out by a sales engineer and questions will be evaluated with higher scrutiny.
Documentation		**Reason for Question**	**Follow-up Inquiries/Responses**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?	Standard documentation, relevant to institutions requiring a vendor to undergo SSAE 18 audits.	Follow-up inquiries for SSAE 18 content will be institution/implementation specific.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	Many vendors have populated a CAIQ or at least a self-assessment. Although lacking in some areas important to Higher Ed, these documents are useful for supplemental assessment.	Follow-up inquiries for CSA content will be institution/implementation specific.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	If a vendor is STAR certified, vendor responses can theoretically be more trusted since CSA has verified their responses. Trust, but verify for yourself, as needed.	If STAR certification is important to your institution you may have specific follow-up details for documentation purposes.
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	The details of the standard are not the focus here, it is the fact that a vendor builds their environment around a standard and that they continually evaluate and assess their security programs.	In an ideal world, a vendor will conform to an industry framework that is adopted by an institution. When this synergy does not exist, the interpretation of the vendor's responses must be interpreted in the context of the institution's environment. Follow-up inquires for industry frameworks (and levels of adoption) will be institution/implementation specific.
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	For institutions that collaborate with the United States government, FISMA compliance may be required.	Follow-up inquiries for FISMA compliance will be institution/implementation specific.
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?	Managing and protecting institution data is the reason organizations perform security and risk assessments. Privacy policies outline how vendors will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.	Inquire about any privacy language the vendor may have. It may not be ideal but there may be something available to assess or enough to have your legal counsel or policy/privacy professionals review.
DOCU-07	Does your organization have a data privacy policy?	Managing and protecting institution data is the reason organizations perform security and risk assessments. Privacy policies outline how vendors will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.	Inquire about any privacy language the vendor may have. It may not be ideal but there may be something available to assess or enough to have your legal counsel or policy/privacy professionals review.
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Managing and protecting a vendor's assets through appropriate human resource management is of the upmost importance. Knowing how roles and access controls are implemented (directed by policy) within a vendor's infrastructure during the onboarding and offboarding processes are indicative of how access control is regarded in other areas on the provider (vendor).	Unsatisfactory answers should be met with questions about access control authority, roles and responsibilities (of access grantors), administrative privileges within the vendor's infrastructure(s), etc.
DOCU-09	Do you have a documented change management process?	The lack of a change management function is indicative of immature program processes. Answers to this question can provide insight into how well their responses (on the HECVAT) represent their actual environment(s).	If a weak response is given to this answer, response scrutiny should be increased. Questions about configuration management, system authority, and documentation are appropriate.
DOCU-10	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	VPATs (Voluntary Product Accessibility Template) / ACRs (Accessibility Conformance Report, a completed VPAT) are standard accessibility reporting formats from the ITIC <https://www.itic.org/policy/accessibility/vpat>. They can be self-assessments from a vendor, though higher confidence is given if completed by expert third parties. It is important to confirm the version of the product tested and reported on for the VPAT matches the one under consideration.	Cross-reference Accessibility Conformance Reports (ACR) with any answers from ITAC-04 about product roadmaps for accessibility improvements.
DOCU-11	Do you have documentation to support the accessibility features of your product?	Has the vendor documented any additional information needed by users in order to create accessible products with the tool or platform? Are there tutorials, if needed, on how assistive technology users can best use the product (platforms tested and works best, shortcuts) etc.? In other words, are they taking care of the end users? Accessibility is more than completing checklists.	In-development
IT Accessibility		**Reason for Question**	**Follow-up Inquiries/Responses**
ITAC-01	Has a third party expert conducted an audit of the most recent version of your product?	Many vendors rely on their internal product knowledge and history to complete accessibility self-assessments of their own product rather than utilizing up-to-date, validated testing. Use of an expert, external specialist provides a more robust assessment of the product.	In-development
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	A combination of most responses to Q-03 would be ideal and a sign of a mature accessibility program. The goal of accessibility is ultimately usability by persons with disabilities, and so successful testing among that population indicates greater access. Expert staff and automated testing are important, but automated tools can only detect ~25% of issues so must be supplemented with additional methodologies. The use of overlays or plugins to help products 'automatically conform' with accessibility guidelines are presently inadequate and should impact scores negatively.	In-development

ITAC-03	Have you adopted a technical or legal standard of conformance for the product in question?	The Web Content Accessibility Guidelines (WCAG) <https://www.w3.org/WAI/standards-guidelines/wcag> from the W3C are widely accepted measures of accessibility conformance. WCAG AA conformance is the most common level of accessibility adoption, with preference given to the most recently released version: 2.1 (released 2018) or 2.0 (released 2008). Additionally, some federal or local requirements may incorporate or supplement the technical standards--including Section 508 <https://www.section508.gov/manage/laws-and-policies> of the Rehabilitation Act (U.S.), EN 301 549 <https://ec.europa.eu/eip/ageing/standards/ict-and-communication/accessibility-and-design-for-all_en.html> (E.U.) etc.	In-development
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	If products do not fully conform to accessibility standards, it is important that vendors have a roadmap specifying how they will work to achieve it. A roadmap with delivery timelines is best supported by evidence of prior delivery on such timelines. Analysts can better predict time to conformance and institutions can plan accordingly.	In-development
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	Having accessibility expertise within the staff supports the proactive development of accessible products. If staff lack sufficient accessibility expertise, then accessibility improvements may only be the result of the vendor reacting to issues or reports of access barriers submitted by clients of the vendor.	In-development
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Tracking and addressing technical issues is a natural part of any web or software product. Critical accessibility issues can cause a product to become unusable. Vendors should have a process to intake, triage and address accessibility issue reports. Vendors that treat accessibility as 'feature requests' for future versions of a product or as non-tracked bug reports (i.e. bug reports lacking accessibility tags) should score lower.	In-development
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	This question is designed to understand how accessibility is included in new versions and features of products, particularly with vendors that implement Agile or similar methodologies where software is updated frequently and continuously.	In-development
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	One critical accessibility requirement is the full use of a product using only the keyboard--no mouse or trackpad. This requirement is easy for a non-technical or non-accessibility expert to understand and verify.	In-development
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a 'lite version' or accessing an alternate interface for accessibility purposes?	Separate accessibility modes or interfaces are indicative of a product design creating an attempted 'separate but equal' environment for disabled users. In practice, separate modes or interfaces for accessibility almost never have feature parity and typically get new features less frequently and after the primary version. They therefore provide unequal experiences for disabled users compared with their non-disabled peers. Interfaces, overlays or extensions that create a separate experience or mimic such an environment should be avoided.	In-development
Assessment of Third Parties		**Reason for Question**	**Follow-up Inquiries/Responses**
THRD-01	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, vendor staff, and affiliates)that are used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of the integrity of their system(s). Questions about administrator access on end-user devices and other maintenance and patching type questions are appropriate.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	The sharing of institutional data to fourth-parties may increase the risk to the institutation and thus, we want to know who gets what data, when they get that data, and why they get that data.	Follow-up inquiries concerning third-party data sharing will be institution/implementation specific.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	Knowing the protections and legal agreements in-place for third-party data sharing may assists analysts in determininng residual risk.	Follow-up inquiries concerning legal agreements with third-parties will be institution/implementation specific.
THRD-04	Do you have an implemented third party management strategy?	Modern technologies allow for rapid deployment of features and with them, come changes to an established code environment. The focus of this question is to verify a vendor's practice of regression testing their code and verifying that previously non-existent risks are introduced into a known, secured environment.	If "No", inquiry if there are plans to implement these processes. Ask the vendor to summarize their decision behind not scanning their assets for vulnerabilities. Be sure that the vendor answers for both systems AND applications. Do not let good practices in one overshadow deficiencies in the other.
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)	Understanding a vendor's hardware supply chain can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment of the vendor's environment in more detail and/or expand the scope of the institution's assessment.	Follow-up inquiries concerning hardware supply chain will be institution/implementation specific.
Consulting - Optional based on QUALIFIER response.		**Reason for Question**	**Follow-up Inquiries/Responses**

CONS-01	Will the consulting take place on-premises?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-02	Will the consultant require access to Institution's network resources?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-06	Will any data be transferred to the consultant's possession?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-08	Will the consultant need remote access to the Institution's network or systems?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
CONS-09	Can we restrict that access based on source IP address?	Consultants are often used to implement, maintain, fix, and assessment technology environments. In these cases, third-party consultants have access to	Follow-up inquiries will be institution/implementation specific.
Application/Service Security		**Reason for Question**	**Follow-up Inquiries/Responses**
APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?	Understanding access control capabilities allows an institution to estimate the type of maintenance efforts will be involved to manage a system. Depending on the users, concerns may or not be elevated. The value of this question is largely determined by the deployment strategy and use case of the software/product/service under review. This question is specific to end-users.	Ask the vendor to summarize the best practices to restrict/control the access given to the institution's end-users without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
APPL-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Managing a software/product/service may rely on various professionals to administrate a system. This question is focused on how administration, and the segregation of functions, is implemented within the vendor's infrastructure.	Managing a complex infrastructure requires diligence in protecting access and authority. Unsatisfactory responses may indicate the lack of maturity with a vendor and/or a flat infrastructure with few individuals with broad authority. Inquire about separation of duties and look for areas of inappropriate functional overlap.
APPL-03	Does the system provide data input validation and error messages?	Input validation is a secure coding best practices so confirming its implementation is normally a high priority. Error messages (to the system and user) can be used to detect abnormal use and to better protect institutional data. Depending on the criticality of data and the flow of said data, an institution's risk tolerance will be unique to their environment.	Inquire about any planned improvements to these capabilities. Ask about their product(s) roadmap and try to understand how they prioritize security concerns in their environment.
APPL-04	Are you using a web application firewall (WAF)?	The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.	If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
APPL-05	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Understanding system requirements and/or dependencies (e.g., libraries, repositories, frameworks, toolkits, modules, etc.) can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment of the vendor's environment in more detail and/or expand the scope of the institution's assessment.	Follow-up inquiries concerning software supply chain will be institution/implementation specific.
APPL-06	Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?	Vendor responses to this question provides clarity on environment constraints that may exist and/or influence future development, configurations, infrastructure, etc. Although the vendor response may not directly affect end-users, the risks of the underlying infrastructure is better understood.	Follow-up inquiries for operating systems leveraged by the vendor will be institution/implementation specific.
APPL-07	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?	Distributing application via known, moderately vetted application platform decreases the chances of malicious code distribution. Standalone deployments (non-trusted sources) should be looked at more closely.	Ask the vendor why this deployment strategy is used. Ask if it is a restriction of the app store platform or some other environment restriction.
APPL-08	Does your application require access to location or GPS data?	Sharing location data significantly increases risk factors for users. It's important to understand if this is required.	Ask the vendor about the need for this requirement and understand any mitigation strategies that may be possible.
APPL-09	Does your application provide separation of duties between security administration, system administration, and standard user functions?	Managing a software/product/service may rely on various teams to administrate a system, in this question, it is security operations and systems administration. This question is focused on how system(s) administration, and the segregation of duties, are implemented in the vendor's organization, so that system administrators do not also have security responsibilities (e.g., monitoring, mitigating, reporting, etc.)	Ask the vendor to summarize their best practices for securing their system(s) administratively without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
APPL-10	Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?	Protecting administrative accounts is crucial to maintaining system integrity in any environment. This question is targeting privilege creep and unmanaged privileged acccounts to determine if the vendor properly	Ask the vendor to summarize their implemented policies and/or procedures
Authentication, Authorization, and Accounting		**Reason for Question**	**Follow-up Inquiries/Responses**

AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	Follow-up inquiries for IAM requirements will be institution/implementation specific.
AAAI-02	Does your solution support local authentication protocols for user and administrator authentication?	The purpose of this question is understand the vendor's authentication infrastructure so that additional questions can be formulated for the institution's use case.	The content of this response may or may not have value for the type of use case on the institution. Follow-up inquiries for authentication modes will be institution/implementation specific.
AAAI-03	Can you enforce password/passphrase aging requirements?	This question is primarily focused on account management capabilities that are built into a system. Although aging is not always required, a system that lacks commodity functionality may be lacking in other areas as well. Use the vendor's response to this question as a way to pivot to other questions, as needed.	The value of this question depends on your institution's policy on passwords, its use of 2FA, or any number of factors. Follow-ups for this question are unique to the institution.
AAAI-04	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Many institutions have policy focused on passwords/passphrases and this question confirms the capacity of a vendor's software/product/service to comply.	Follow-up inquiries for password/passphrase complexity requirements will be institution/implementation specific.
AAAI-05	Does the system have password complexity or length limitations and/or restrictions?	Many institutions have policy focused on passwords/passphrases and this question confirms the capacity of a vendor's software/product/service to comply.	Follow-up inquiries for password/passphrase limitations and/or restrictions will be institution/implementation specific.
AAAI-06	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	Account management can be a time-consuming part of an information system. Account reset capabilities, built into a system, can reduce burden on institutional support services.	Ask the vendor how end-users will be supported. Ask for training documentation or knowledgebase content. Confirm vendor and institution responsibilities in this support area (and others).
AAAI-07	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	This question defines the vendors scope of federated identity practices and their willingness to embrace higher education requirements.	If a vendor indicates that a system is standalone and cannot integrate with community standards, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
AAAI-08	Does your application support integration with other authentication and authorization systems?	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	If a vendor indicates that a system is standalone and cannot integrate with the institution's infrastructure, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
AAAI-09	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	Follow-up inquiries for IAM requirements will be institution/implementation specific.
AAAI-10	Do you support differentiation between email address and user identifier?	This questions allows an institution to know vendor system limitations and to help them gauge the resources (that may be needed to implement) required to successfully integrate the product/service with institution systems.	Follow-up inquiries for identifier requirements will be institution/implementation specific.
AAAI-11	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]	This questions allows an institution to know vendor system limitations and to help them gauge the resources (that may be needed to implement) required to successfully integrate the product/service with institution systems.	Follow-up inquiries for attribute mapping requirements will be institution/implementation specific.
AAAI-12	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases, a requirement for account protection purposes.	Ask the vendor about hardware and software options, future roadmap for implementations and support, etc.
AAAI-13	Does your application automatically lock the session or log-out an account after a period of inactivity?	This is a question to ensure account integrity and institutional data confidentiality.	Follow-up inquiries for inactivity protections will be institution/implementation specific.
AAAI-14	Are there any passwords/passphrases hard coded into your systems or products?	The response to this question can reveal the use (or not) of coding best-practices. If passwords/passphrases are hard coded into systems/productions, the vendor should provide robust details supporting why this is required.	Vague responses to this question should be met with concern. Repeat the question if first answer insufficiently - ask pointedly to ensure the vendor is not misunderstood.
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is end-user logs.	If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.
AAAI-18	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.	Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is system-related logs (e.g., including but not limited to - events, state changes, control modification, etc.).	If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.

AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	There are multiple components of this question - when assessing, ensure that the vendor responds to them all. Logs that are not properly managed may not be available when needed. The purpose of this question is to ensure that the vendor has a proper security mindset to ensure proper monitoring practices.	Follow-up inquiries for logging details will be institution/implementation specific.
Business Continuity Plan		**Reason for Question**	**Follow-up Inquiries/Responses**
BCPL-01	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	Having a BCP and maintaining/updating/testing a BCP are very different. Establishing a responsible party is fundamental to this process and this question looks to verify that within the vendor.	Follow-up inquiries for BCP responsible parties will be institution/implementation specific.
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
BCPL-03	Is there a documented communication plan in your BCP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
BCPL-04	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	It is expected that a vendor will maintain an accurate BCP to be tested at a regular interval. Any variance to this should be clearly explained. A vendor's response to this question can reveal the value that they place on testing their BCP (and possibly other aspects of their programs).	If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
BCPL-05	Are specific crisis management roles and responsibilities defined and documented?	As it relates to BCPs, a vendor's response will provide insight into their ability to properly response to business threats. A vendor that has not previously defined responsible parties and outlined realistic plans may not maintain the availability needed for the institution's use case or business requirement.	Follow-up inquiries for BCP roles and responsibility details will be institution/implementation specific.
BCPL-06	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	Understanding the maturity of a vendor's training and awareness program will indicate the value they place on protecting institutional data. BCP related awareness training should be prevalent, continuous, and well-documented.	If a vendor's BCP training and awareness activities are insufficient, inquire about other mandatory training, verify its scope, and confirm the training cycles.
BCPL-07	Does your organization have an alternative business site or a contracted Business Recovery provider?	In the event that a vendor's headquarters (primary location of operation) is no longer usable, an alternative business site may be needed to support business operations. Having an established (planned) alternative business site show maturity in a vendor's BCP.	Follow-up inquiries for alternative business site practices will be institution/implementation specific.
BCPL-08	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Testing a BCP is an important action that improves the efficiency and accuracy of a vendor's continuity plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
BCPL-09	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	The purpose of this question is understand the vendor's order of response if affected by a unplanned business disruption. If the software/product/service being assessed is a vendor's core moneymaker, the probability that restoration of the software/product/service will be top priority.	If it is not a core service, follow-up questions should be availability focused and institution/implementation specific.
BCPL-10	Are all services that support your product fully redundant?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
Change Management		**Reason for Question**	**Follow-up Inquiries/Responses**
CHNG-01	Does your Change Management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?	This question outlines a mature Change Management process. Changes should be analyzed for impact, officially approved, tested, and performed by authorized users.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses, as needed.
CHNG-02	Does your Change Management process also verify that all required third party libraries and dependencies are still supported with each major change?	This question is fundamentally about supply chain. The vendor should be able to document their procedures around tracking third party maintained libraries.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
CHNG-03	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Notification expectations should be set earlier in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	Unplanned and/or unexpected changes in a complex environment can introduce intolerable risks to the institution. Based on the operating environment of the institution, it may be necessary to postpone (or properly plan) the change to a system. The vendor's response should clarify their use of a "one code base" method or the ability to run multiple version concurrently.	Follow-up inquiries for software/product/service version releases will be institution/implementation specific.
CHNG-05	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?	Supporting multiple versions of a product is challenging. Understanding the vendor’s strategy and resources will provide insight into their ability to adequately support their customers.	Follow-up inquiries for the vendor’s support of concurrent versions will be institution/implementation specific.
CHNG-06	Does the system support client customizations from one release to another?	The vendor's software/product/service characteristics and the institution's use case will determine the relevancy of this question. The purpose of this question is to understand the underlying infrastructure and how it is maintained across all customers.	In cases where the software/product/service is customized for customer use cases, ensure the vendor's response covers all aspects of code migration, including backups, data conversions, local resources from the institution, etc., as it relates to code upgrades and/or version adoptions.

CHNG-07	Do you have a release schedule for product updates?	Answers to this question will reveal the vendor's ability to plan in the short term. This is valuable information for customers so they can anticipate updates and potential bug fixes.	Follow-up inquiries for the vendor's product update practices will be institution/implementation specific.
CHNG-08	Do you have a technology roadmap, for at least the next 2 years, for enhancements and bug fixes for the product/service being assessed?	Answers to this question will reveal the vendor's ability to plan for the future of their product.	Follow-up inquiries for the vendor's technology planning practices will be institution/implementation specific.
CHNG-09	Is Institution involvement (i.e. technically or organizationally) required during product updates?	The response to this question allows the institution to understand the information technology resources required to properly maintain the vendor's system. Initial acquisition and setup is important to assess, but the long-term maintenance (and the risks that come with it), should be clearly defined. Use the response to this question to pivot to other questions and/or verify other vendor responses.	Vague responses to this question should be investigated further. Ask for additional documentation for customer responsibilities (in the context of information technology/security).
CHNG-10	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	Answers to this question will reveal the vendor's knowledge of their IT assets and their ability to respond to notifications about their systems and software.	Follow-up inquiries for the vendor's patching practices will be institution/implementation specific.
CHNG-11	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	New vulnerabilities are published every day and vendors have a responsibility to maintain their software(s). The fundamental nature of operation will expose some risks to the system but it is crucial that a vendor recognize their responsibilities and have a plan to implement them, when this time arrives.	Follow-up inquiries for the vendors patching practices will be institution/implementation specific.
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It's also important for troubleshooting any problems that may occur as a result of the changes.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses, as needed.
CHNG-13	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. In the event of emergency changes, accountability and post-action review is expected.	Follow-up with a robust question set if a vendor cannot clearly state full-control of the integrity of their system(s).
CHNG-14	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	Hardware lifecycles and continuous software updates creates an always-changing landscape in information technology. The focus of this question is the integrity of a vendor's infrastructure. Mismanagement of system configurations can lead to breakdowns in layers of security.	It is expected that vendors should have robust documentation when it comes to configuration management. Vague answers to this question should be met with concern. Inquire about the device management tools in use, system lifecycles, complexity of systems, etc. and evaluate the response in the context of company capabilities (see Company Background section).
CHNG-15	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, vendor staff, and affiliates)that are used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of the integrity of their system(s). Questions about administrator access on end-user devices and other maintenance and patching type questions are appropriate.
Data		**Reason for Question**	**Follow-up Inquiries/Responses**
DATA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).	A vendor's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here so general follow-up is often needed. Understanding how a vendor segments its customers data (or doesn't) affects various other controls, including network settings, use of encryption, access controls, etc.). A vendor's response here will influence potential follow-up inquiries for other HECVAT questions.	Follow-up inquiries for dedicated single-tenant capabilities will be institution/implementation specific.
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	Systems that are directly exposed to public internet resources are at great risk than those that are not. Understanding the requirements for this configuration is important, particularly when assessing compensating controls.	Ask the vendor about their infrastructure and if there is a solution that eliminates the need for this environment.
DATA-03	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	The need for encryption in transport is unique to your institution's implementation of a system. In particular, the data flow between the system and the end-users of the software/product/service.	Follow-up inquiries for data encryption between the system and end-users will be institution/implementation specific.
DATA-04	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data encryption at-rest will be institution/implementation specific.
DATA-05	Do all cryptographic modules in use in your product conform to the Federal Information Processing Standards (FIPS PUB 140-3)?	Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases if which that is not the case, be sure to understand the vendor's infrastructure and the true security of a vendor's solution.	If the vendor cannot accommodate open standards encryption requirements, direct them to NIST's Cryptographic Standards and Guidelines document at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
DATA-06	At the completion of this contract, will data be returned to the institution and deleted from all your systems and archives?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. This questions allows the vendor to state their general practices when a customer leaves their environment.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.
DATA-07	Will the institution's data be available within the system for a period of time at the completion of this contract?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. This questions allows the vendor to state their general practices when a customer leaves their environment.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.

DATA-08	Can the Institution extract a full or partial backup of data?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. The vendor's response should verify if the institution can extract data or if it is a manual extraction by vendor staff.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.
DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	This question clarifies the operating model of a vendor and provides insight into the vendor-customer paradigm of a company. Knowing if the institution is of value to a vendor or if the institution's data is of value to a vendor should weigh heavily in the decision-making process.	If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
DATA-10	Are these rights retained even through a provider acquisition or bankruptcy event?	This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question - if vague, be sure to follow-up based on institutional counsel guidance.	If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
DATA-11	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question - if vague, be sure to follow-up based on institutional counsel guidance.	If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
DATA-12	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It’s also important for troubleshooting any problems that may occur as a result of the changes. Availability is the focus of this question.	An institution's use case will drive the requirements for backup strategy. Ensure that the institution's use case and risk tolerance can be met by vendor systems.
DATA-13	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	The purpose of this question is to define the scope of backup operations and the scope at which a vendor may readily recover when backup restoration is required.	Follow-up inquiries for backup content scope will be institution/implementation specific.
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)	When data is moved digitally (e.g., cloud provider, vendor-owned facility, etc.) offsite, the policies and implemented procedures are important to know. The protections implemented to prevent compromise will be technical in nature and should be well-documented.	Follow-up inquiries for offsite, digital backups will be institution/implementation specific.
DATA-15	Are physical backups taken off site? (i.e. physically moved off site)	When data is moved physically (e.g. HDD, print, etc.) offsite, the policies and implemented procedures are important to know. Unencrypted data taken outside secured areas introduces unnecessary risks.	Follow-up inquiries for offsite, physical backups will be institution/implementation specific.
DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
DATA-17	Are data backups encrypted?	The need for encryption at-rest (for backups) is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data backup encryption at-rest will be institution/implementation specific.
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)	Understanding how key management is handled and the safeguards implemented by the vendor to ensure key confidentiality in all components of a system(s) can provide insight into other complex details of a vendor's infrastructure. Use vendor responses to this question as a way to pivot to other infrastructure specifics, as needed to clarify potential risks.	Follow-up with the vendor to ensure that all components of the system are consider. This includes, system-to-system, system-to-client, applications, system accounts, etc.
DATA-19	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
DATA-20	Does the process described in DATA-19 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.	Follow-up inquiries for DoD 5220.22-M and/or SP800-88 standards will be institution specific.
DATA-21	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
DATA-22	Will you handle data in a FERPA compliant manner?	Standard documentation, relevant to institution implementations requiring FERPA compliance.	Follow-up inquiries for FERPA compliance details will be institution/implementation specific.
DATA-23	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) through any means?	Confidentiality is the focus of this question. Based on the capabilities of vendor administrators, the institution may require additional safeguards to protect the confidentiality of data stored by/shared with a vendor (e.g., additional layer of encryption, etc.).	If Institutional data is visible by the vendor's system administrators, follow-up with the vendor to understand the scope of visibility, process/procedure that administrators follow, and use cases when administrators are allowed to access (view) Institutional data.
DATA-24	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)	In the context of the CIA triad, this question is focused on confidentiality. Printed documents, mobile device use, and remote access are all relevant to this question. A vendor's response to this question will provide insight into their overall business process. Vendor business activity that pose additional security risks should be met with increased concern.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper customer data handling activity.
Datacenter		**Reason for Question**	**Follow-up Inquiries/Responses**

DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?	This question is relative to the response above. Understanding the ownership structure of the facility that will host institutional data is important for setting availability expectations and ensure proper contract terms are in place to protect the institution due to use of third-parties. If a vendor uses a third-party vendor to provide datacenter solutions, having that vendor's SOC 2 Type 2 provides additional insight. The ability to assess these "forth-party" vendors is based on your institution's resources. The vendor is responsible for providing this information - ensure that they handle their vendors properly.	Follow-up inquiries for additional vendor's SOC 2 Type 2 reports will be institution/implementation specific.
DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?	An institution's location will dictate what laws and regulations apply to them. As vendor's may not know where all of their customers may reside, it is imperative that vendors are able to accommodate geographic requirements for their customers. Although unfair to expect support for all geographic regions in common infrastructure/platform/software-as-a-service, it is expected that vendor's be absolutely clear about the regions they leverage and/or support.	If a vendor is unable to accommodate storing/processing institutional data within specific regions, ask them why they are unable to? Try to determine if its an infrastructure issue (scalability), a cost-reduction strategy (size/maturity), or some other issue.
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	Vendors that operate their own datacenter(s) can implement their own monitoring strategy. Use the vendor's response to this questions to verify/validate other responses related to ownership/co-location/physical security.	Follow-up inquiries for data center staffing will be institution/implementation specific.
DCTR-04	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.	Follow-up inquiries for system physical security will be institution/implementation specific.
DCTR-05	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.	Follow-up inquiries for system physical security will be institution/implementation specific.
DCTR-06	Are your primary and secondary data centers geographically diverse?	When planning for business continuity and disaster recovery, considering geographic diversity of a vendors operating environment will help analysts better understand risk due to widespread technical issues as well as weather and environmental considerations.	Follow-up inquiries for geographic diversity in datacenters will be institution/implementation specific.
DCTR-07	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime Institute)?	Standard documentation, relevant to institutions requiring a vendor to maintain a specific Uptime Institute Tier Level.	Follow-up inquiries for Uptime Institute Tier Level details will be institution/implementation specific.
DCTR-09	Is the service hosted in a high availability environment?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-10	Is redundant power available for all datacenters where institution data will reside?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-11	Are redundant power strategies tested?	Installing [potential] redundant power and regularly testing strategies to ensure they will work when needed are very different. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	Follow-up inquiries for redundant power testing details will be institution/implementation specific.
DCTR-12	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	Installing appropriate environmental controls is crucial to maintaining the integrity of the hosting site. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions	Follow-up inquiries for cooling and fire suppression systems will be institution/implementation specific.
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-14	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-15	Are you requiring multi-factor authentication for administrators of your cloud environment?	2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases, a requirement for account protection purposes.	Ask the vendor about hardware and software options, future roadmap for implementations and support, etc.
DCTR-16	Are you using your cloud providers available hardening tools or pre-hardened images?	In the context of the CIA triad, this question is focused on the integrity of a system (or set of systems).	Ask the vendor about their system lifecycle practices and security methodology.
DCTR-17	Does your cloud vendor have access to your encryption keys?	Understanding how key management is handled and the safeguards implemented by the vendor to ensure key confidentiality in all components of a system(s) can provide insight into other complex details of a vendor's infrastructure. Use vendor responses to this question as a way to pivot to other infrastructure specifics, as needed to clarify potential risks.	Follow-up with the vendor to ensure that all components of the system are consider. This includes, system-to-system, system-to-client, applications, system accounts, etc.
Disaster Recovery Plan		**Reason for Question**	**Follow-up Inquiries/Responses**

DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	In the context of the CIA triad, this question is focused on availability and is often in need of a follow-up. Understanding the maturing of a vendor's DRP can shed light on many other aspects of a vendor's overall security state.	A vendor may have a number of BCP elements defined so the vendor's response may not be binary. Assess the components of the plan and ask about timelines, follow-up commitments, etc. If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Having a DRP and maintaining/updating/testing a DRP are very different. Establishing a responsible party is fundamental to this process and this question looks to verify that within the vendor.	Follow-up inquiries for DRP responsible parties will be institution/implementation specific.
DRPL-03	Can the Institution review your DRP and supporting documentation?	General inquiry for documentation. As DRPs may contain some sensitive data, a robust summary is appropriate in lieu of a full DRP.	If the vendor states "No", you can ask for a summary, white paper, or blog. If unable to review the full plan, infer what you can from other DRP question responses.
DRPL-04	Are any disaster recovery locations outside the Institution's geographic region?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	In the event that a vendor's headquarters (primary location of operation) is no longer usable, a recovery site may be needed to support business operations. Having an established (planned) recovery site show maturity in a vendor's DRP.	Follow-up inquiries for disaster recovery site practices will be institution/implementation specific.
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-10	Has the Disaster Recovery Plan been tested in the last year?	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-11	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
Firewalls, IDS, IPS, and Networking		**Reason for Question**	**Follow-up Inquiries/Responses**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?	The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.	If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
FIDP-02	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info	Modifications to firewall rulesets can have significant repercussions. To ensure the integrity of the ruleset, this question targets the individual (or responsible party) for changes and the reasoning behind their authority.	Ensure that a separation of duties exists in network security configurations. Pay close attention to responsibility overlap in small organizations, where staff often fill multiple roles.
FIDP-03	Do you have a documented policy for firewall change requests?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Any change to a verified, known, secure environment should be carefully evaluated by stakeholders in a structured manner.	Follow-up inquiries for firewall change requests will be institution/implementation specific.
FIDP-04	Have you implemented an Intrusion Detection System (network-based)?	It is important to have detective capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	A security program with limited resources for event detection is not effective. Inquiries should include training for staff, reasoning behind not using IDS technologies, and how systems are monitored. Additional questions about a SIEM and other tool may be appropriate.
FIDP-05	Have you implemented an Intrusion Prevention System (network-based)?	It is important to have preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	A security program with limited resources for active prevent is inefficient. Inquiries should include training for staff, reasoning behind not using IPS technologies, and how systems are actively protected and how malicious activity is stopped.
FIDP-06	Do you employ host-based intrusion detection?	It is important to have detective capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	Ask the vendor to summarize why host-based intrusion detection tools are not implemented in their environment. What compensating controls are in place to detect configuration changes and/or failures of integrity?

FIDP-07	Do you employ host-based intrusion prevention?	It is important to have preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	Ask the vendor to summarize why host-based intrusion prevention tools are not implemented in their environment. What compensating controls are in place to detect malicious activity and to actively prevent its function.
FIDP-08	Are you employing any next-generation persistent threat (NGPT) monitoring?	This question is primarily focused on determining the maturity of a vendor's security program and their ability to implement and operate cutting-edge technologies. Investment in advanced technologies may indicate appropriate security program capabilities.	Follow-up inquiries for next-generation persistent threat monitoring will be institution/implementation specific.
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?	This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.	Follow-up inquiries for 24x7x365 monitoring will be institution/implementation specific.
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?	This question is primarily focused on the capability of a vendor's security program. Understanding the size and skillsets of a vendor (taken from other responses) is needed to determine the appropriateness of the vendor's response to this question.	Follow-up inquiries for intrusion monitoring will be institution/implementation specific.
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	Strong logging capabilities are vital to the proper management of a network. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk.	If a weak response is given to this answer, it is an indicator that a non-technical representative populated the document and response scrutiny should be increased. If a vendor does not answer appropriately, a follow-up request to have the question fully-answered is appropriate.
Policies, Procedures, and Processes		**Reason for Question**	**Follow-up Inquiries/Responses**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. Vendor's will share organizational charts and additional documentation of their security program, if needed. The point of this question is to verify vendor security program maturity or confirm other findings and/or assessments.	Vague responses to this question should be investigated further. Vendors unwilling to share additional supporting documentation decrease the trust established with other responses.
PPPR-02	Do you have a documented patch management process?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed according to policy. Additionally, it is expected that devices used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of their system patching strategy. Questions about patch testing, testing environments, threat mitigation, incident remediation, etc. are appropriate.
PPPR-03	Can you accommodate encryption requirements using open standards?	Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases if which that is not the case, be sure to understand the vendor's infrastructure and the true security of a vendor's solution.	If the vendor cannot accommodate open standards encryption requirements, direct them to NIST's Cryptographic Standards and Guidelines document at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
PPPR-04	Are information security principles designed into the product lifecycle?	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
PPPR-05	Do you have a documented systems development life cycle (SDLC)?	Mature product/software/service lifecycle management can position a vendor to sufficiently plan, implement, and manage systems that better protect institutional data.	Although withdrawn by NIST, the Security Considerations in the Systems Development Life Cycle (SP 800-64r2) document is an excellent resource to provide guidance to vendors (i.e. set expectations.) Follow-up questions to SDLC use will be institution/implementation specific.
PPPR-06	Will you comply with applicable breach notification laws?	This is a general inquiry to determine if the vendor is well-versed in applicable laws and regulations that apply in the institution's region of business operation.	If a vendor is vague in their response, follow-up with direct questions about doing business in your state/region/country and any laws that are pertinent to the institution.
PPPR-07	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	This is a general inquiry to determine if the vendor has reviewed the institution's policies and are committed to complying with them.	If a vendor is vague in their response, follow-up with direct questions about the institution's policies and ensure the expectation of compliance is clear with the vendor.
PPPR-08	Is your company subject to Institution's geographic region's laws and regulations?	This is a general inquiry to determine if the vendor is well-versed in applicable laws and regulations that apply in the institution's region of business operation.	If a vendor is vague in their response, follow-up with direct questions about doing business in your state/region/country and any laws that are pertinent to the institution.
PPPR-09	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	The use of detective and preventive controls in the hiring process serve a valuable role in protecting institutional data. As these are often HR documented policies, a vendor should have their practices well-documented and ready for review, upon request.	Ask the vendor is background checks and/or screening are conducted in any capacity, at any time during the employment period. Ask about the precautions they take to ensure the intellectual property is secured and inquire if user data is treated in an appropriate manner.
PPPR-10	Do you require new employees to fill out agreements and review policies?	Setting the expectation of performance and increase awareness of security-related responsibilities are part of these initial-hiring documents. Oftentimes these agreements and reviews are conducted during orientation for new employees.	If a vendor's practices are not clear, inquire about training requirements for employees, especially the frequency and scope of content.
PPPR-11	Do you have a documented information security policy?	The ability for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a vendor's security office will determine their capabilities during a security incident but the incident response plan will oftentimes determine their effectiveness. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.	If the vendor does not have an incident response plan, point them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
PPPR-12	Do you have an information security awareness program?	Setting the expectation of security-related responsibilities throughout an organzation is favored in an information security awareness program. Vendors without an information security awareness campaign should be met with scrutiny on how security policies	Follow-up inquiries for information security awareness programs will be institution/implementation specific.

PPPR-13	Is security awareness training mandatory for all employees?	Setting the expectation of security-related responsibilities throughout an organzation is favored in an information security awareness program. Vendors without an information security awareness campaign should be met with scrutiny on how security policies	Follow-up inquiries for information security awareness programs will be institution/implementation specific.
PPPR-14	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?	Protecting privileged accounts is crucial to maintaining system integrity in any environment. This question is targeting privilege creep and unmanaged privileged acccounts to determine if the vendor properly manages access control in their application/system environments.	Ask the vendor to summarize their implemented policies and/or procedures.
PPPR-15	Do you have documented, and currently implemented, internal audit processes and procedures?	The role of an internal auditor is to verify implemented controls and highlight areas in need of improvement. Vendors without internal audit processes and	Follow-up inquiries for internal audit processes and procedures will be institution/implementation specific.
PPPR-16	Does your organization have physical security controls and policies in place?	This question aims to understand the physical security state of the vendor's operating environment, and whether or not physical assets are appropriately	Follow-up inquiries for physical security controls and policies will be institution/implementation specific.
Incident Handling		**Reason for Question**	**Follow-up Inquiries/Responses**
HFIH-01	Do you have a formal incident response plan?	The ability for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a vendor's security office will determine their capabilities during a security incident but the incident response plan will oftentimes determine their effectiveness. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.	If the vendor does not have an incident response plan, direct them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
HFIH-02	Do you have either an internal incident response team or retain an external team?	The ability for the vendor to investigate security incidents is of the utmost importance. Reviewing alerts but then taking no action is not security, only compliance. Incident reports and indications of compromise must be reviewed by qualified staff and they must have the capability to investigate further, as needed.	If the vendor does not have an incident response plan, direct them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
HFIH-03	Do you have the capability to respond to incidents on a 24x7x365 basis?	The incident team structure (internal vs. external), size, and capabilities of a vendor has a significant impact on their ability to respond to and protect an institution's data. Use the knowledge of this response when evaluating other vendor statements.	If the vendor does not have an incident response team, direct them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	The capacity for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size and talent of a vendor's incident response team will determine their capabilities during a security incident. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.	If the vendor does not have an incident response plan, point them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
Quality Assurance		**Reason for Question**	**Follow-up Inquiries/Responses**
QLAS-01	Do you have a documented and currently implemented Quality Assurance program?	Integrity and availability are the focus of this question. The existence of a well-documented quality assurance program, with demonstrated and published metrics, may provide insight into the inner workings (mindset) of a vendor.	Institutions vary broadly on how QA is handled so any follow-up questions will be contract/institution/implementation specific.
QLAS-02	Do you comply with ISO 9001?	Standard documentation, relevant to institutions requiring a vendor to comply with ISO 9001.	Follow-up inquiries for ISO 9001 content will be institution/implementation specific.
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	This question is for institutions that tie metrics and service level agreements (SLAs) or expectations (SLEs) to security reviews. The implementation strategy and use case will indicate the relevancy of this question for security/risk assessment.	Follow-up inquiries for quality and performance metrics will be contract/institution/implementation specific.
QLAS-04	Do you incorporate customer feedback into security feature requests?	This is a general inquiry to determine if the vendor being assessed has done or is doing business with the institution as the time of assessment. Existing relationships, if present, can be reviewed for insights into a vendor and/or to verify other responses.	Many Higher Ed institutions are large enough that existing/former contracts exist with one entity of the college/university (e.g. School of X) but it is unknown to another. Question the vendor in-depth if you get a vague response to this question - combining licenses/purchases increases buying power.
QLAS-05	Can you provide an evaluation site to the institution for testing?	This question is used to gauge the importance of our industry (higher education) to the vendor.	This is a general information question - any follow-up will be institution/implementation specific.
Vulnerability Scanning		**Reason for Question**	**Follow-up Inquiries/Responses**
VULN-01	Are your systems and applications regularly scanned externally for vulnerabilities?	External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquire if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
VULN-02	Have your systems and applications had a third party security assessment completed in the last year?	External verification of system and application security controls are important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	Ask if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.

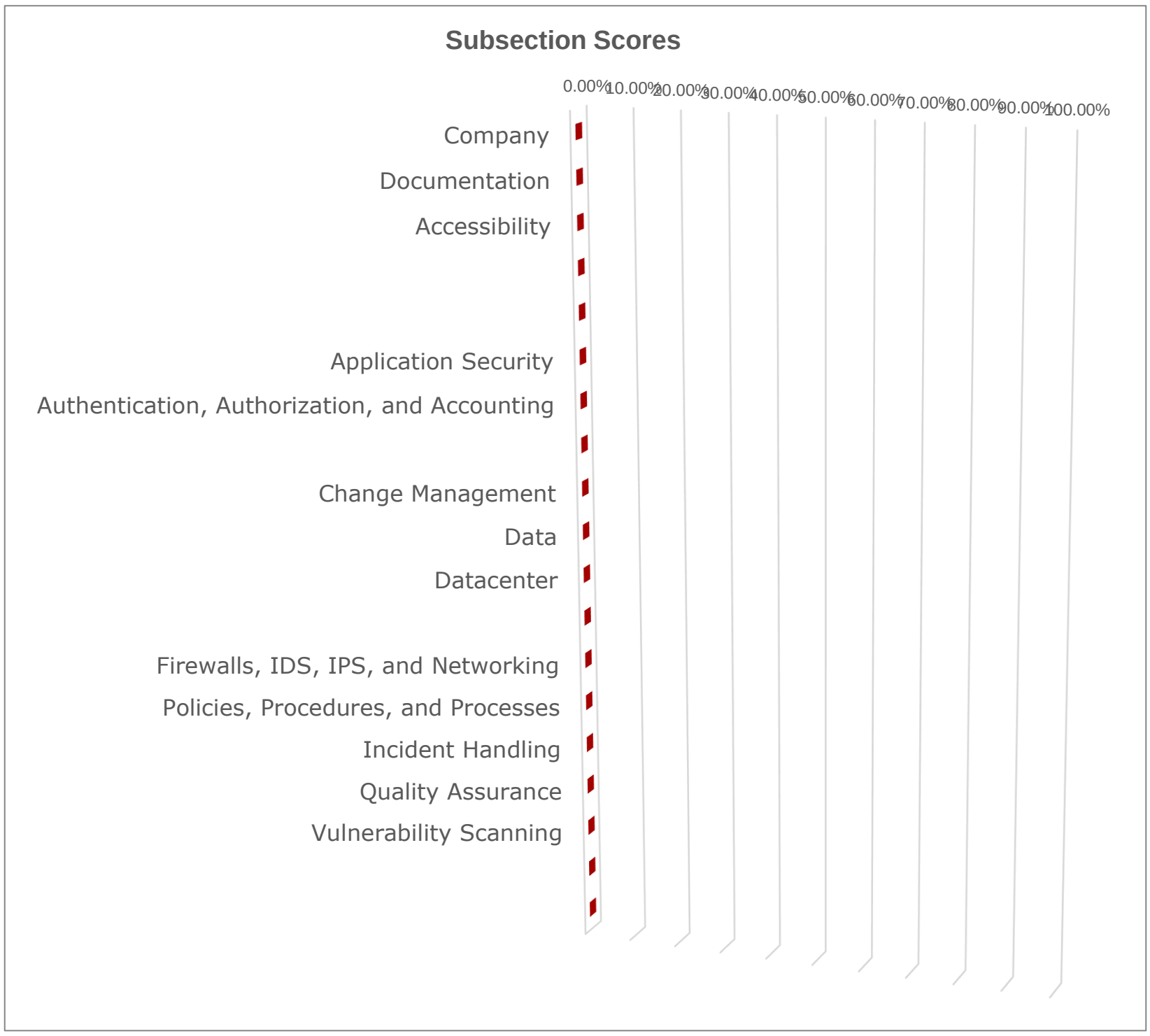
VULN-03	Are your systems and applications scanned with an authenticated user account for vulnerabilities [that are remediated] prior to new releases?	Modern technologies allow for rapid deployment of features and with them, come changes to an established code environment. The focus of this question is to verify a vendor's practice of regression testing their code and verifying that previously non-existent risks are introduced into a known, secured environment.	Ask if there are plans to implement these processes. Ask the vendor to summarize their decision behind not scanning their applications for vulnerabilities prior to release.
VULN-04	Will you provide results of application and system vulnerability scans to the Institution?	If a vendor is scanning their applications and/or systems, oftentimes an institution will want to review the report, if possible. Preferably, any finding on the reports will have a matching mitigation action.	If a vendor is hesitant to share the report, ask for a summarized version - some insight is better than none.
VULN-05	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications. Vendors should be monitoring for and addressing these issues in their products.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide Inquire about the tools a vendor uses, the interval at which systems are monitored/mitigated, and who is responsible for the process/procedure in place for this monitoring.
VULN-06	Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	Many Higher Ed institutions are capable of performing vulnerability assessments and/or penetration testing on their vendor's infrastructures. This question confirms the possibility of conducting these actions against the vendor's infrastructure.	Follow-up inquiries for vulnerability scanning and penetration testing will be institution/implementation specific.
HIPAA		**Reason for Question**	**Follow-up Inquiries/Responses**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-05	Have you conducted a risk analysis as required under the Security Rule?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-06	Have you identified areas of risks?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-07	Have you taken actions to mitigate the identified risks?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-08	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-09	Does your application require a user to set their own password after an administrator reset or on first use of the account?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-10	Does your application lock-out an account after a number of failed login attempts?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-11	Does your application automatically lock or log-out an account after a period of inactivity?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-12	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-13	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-14	Does your application provide the ability to define user access levels?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-15	Does your application support varying levels of access to administrative tasks defined individually per user?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-16	Does your application support varying levels of access to records based on user ID?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-17	Is there a limit to the number of groups a user can be assigned?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-18	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-19	Does the application log record access including specific user, date/time of access, and originating IP or device?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-20	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-21	How long does the application keep access/change logs?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.

HIPA-22	Can the application logs be archived?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-23	Can the application logs be saved externally?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-24	Does your data backup and retention policies and practices meet HIPAA requirements?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-25	Do you have a disaster recovery plan and emergency mode operation plan?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-26	Have the policies/plans mentioned above been tested?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-27	Can you provide a HIPAA compliance attestation document?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
HIPA-29	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	HIPAA	Refer to HIPAA documentation or your institution's Chief HIPAA Security Officer.
PCI DSS		**Reason for Question**	**Follow-up Inquiries/Responses**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-04	Are you classified as a service provider?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-05	Are you on the list of VISA approved service providers?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-08	What payment processors/gateways does the system support?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-10	Is the application listed as an approved PA-DSS application?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.	PCI DSS	Refer to PCI DSS documentation or your institution's treasurer's office.

HECVAT - Full - Summary Report

Version 3.04

Vendor	Vendor Name	
Description	Brief Description of the Product	



Non-Compliant Responses

		Institution's Security Framework	
Question	**Additional Info**	**0**	

Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	0	#REF!	#REF!
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)	0	#REF!	#REF!
Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	0	#REF!	#REF!
Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	0	#REF!	#REF!
Is the vended product designed to process or store Credit Card information?	0	#REF!	#REF!
0	0	#REF!	#REF!

HECVAT - Full | Standards Crosswalk - TO BE UPDATED IN 2023

Standards Crosswalk

	Qualifiers	CIS Critical Security Controls v6.1	HIPAA	ISO 27002:27013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS	Trusted CI
QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?								
QUAL-02	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)								
QUAL-03	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?								
QUAL-04	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?								
QUAL-05	Is the vended product designed to process or store Credit Card information?								
QUAL-06	Does your company provide professional services pertaining to this product?								
QUAL-07	Select your hosting option								
Company Overview		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.								
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?								
COMP-03	Do you have a dedicated Information Security staff or office?								
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)								
COMP-05	Use this area to share information about your environment that will assist those who are assessing your company data security program.								
Documentation		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?								
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?								
DOCU-03	Have you received the Cloud Security Alliance STAR certification?								
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)								
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?								
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?								
DOCU-07	Does your organization have a data privacy policy?								

DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?								
DOCU-09	Do you have a documented change management process?								
DOCU-10	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?								
DOCU-11	Do you have documentation to support the accessibility features of your product?								
IT Accessibility		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
ITAC-01	Has a third party expert conducted an audit of the most recent version of your product?								
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?								
ITAC-03	Have you adopted a technical or legal standard of conformance for the product in question?								
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?								
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?								
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?								
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?								
ITAC-08	Can all functions of the application or service be performed using only the keyboard?								
ITAC-09	Does your product rely on activating a special ‘accessibility mode,’ a ‘lite version’ or accessing an alternate interface for accessibility purposes?								
Assessment of Third Parties		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**

THRD-01	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).								
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.								
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?								
THRD-04	Do you have an implemented third party management strategy?								
Consulting - Optional based on QUALIFIER response.		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
CONS-01	Will the consulting take place on-premises?								
CONS-02	Will the consultant require access to Institution's network resources?								
CONS-03	Will the consultant require access to hardware in the Institution's data centers?								
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?								
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?								
CONS-06	Will any data be transferred to the consultant's possession?								
CONS-07	Is it encrypted (at rest) while in the consultant's possession?								
CONS-08	Will the consultant need remote access to the Institution's network or systems?								
CONS-09	Can we restrict that access based on source IP address?								
Application/Service Security		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?	0							
APPL-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?								
APPL-03	Does the system provide data input validation and error messages?								
APPL-04	Are you using a web application firewall (WAF)?								
APPL-05	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)								
APPL-06	Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?								

APPL-07	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?								
APPL-08	Does your application require access to location or GPS data?								
APPL-09	Does your application provide separation of duties between security administration, system administration, and standard user functions?								
APPL-10	Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?								
APPL-11	Have your developers been trained in secure coding techniques?								
APPL-12	Was your application developed using secure coding techniques?								
APPL-13	Do you subject your code to static code analysis and/or static application security testing prior to release?								
APPL-14	Do you have software testing processes (dynamic or static) that are established and followed?								
Authentication, Authorization, and Accounting		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?								
AAAI-02	Does your solution support local authentication protocols for user and administrator authentication?								
AAAI-03	Can you enforce password/passphrase aging requirements?								
AAAI-04	Can you enforce password/passphrase complexity requirements [provided by the institution]?								
AAAI-05	Does the system have password complexity or length limitations and/or restrictions?								
AAAI-06	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?								
AAAI-07	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?								
AAAI-08	Does your application support integration with other authentication and authorization systems?								
AAAI-09	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]								
AAAI-10	Do you support differentiation between email address and user identifier?								
AAAI-11	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]								
AAAI-12	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)								

AAAI-13	Does your application automatically lock the session or log-out an account after a period of inactivity?								
AAAI-14	Are there any passwords/passphrases hard coded into your systems or products?								
AAAI-15	Are you storing any passwords in plaintext?								
AAAI-16	Does your application support directory integration for user accounts?								
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?								
AAAI-18	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.								
AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).								
Business Continuity Plan		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
BCPL-01	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?								
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for impacted clients?								
BCPL-03	Is there a documented communication plan in your BCP for impacted clients?								
BCPL-04	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?								
BCPL-05	Are specific crisis management roles and responsibilities defined and documented?								
BCPL-06	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?								
BCPL-07	Does your organization have an alternative business site or a contracted Business Recovery provider?								
BCPL-08	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?								
BCPL-09	Is this product a core service of your organization, and as such, the top priority during business continuity planning?								
BCPL-10	Are all services that support your product fully redundant?								
Change Management		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
CHNG-01	Does your Change Management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?								
CHNG-02	Does your Change Management process also verify that all required third party libraries and dependencies are still supported with each major change?								
CHNG-03	Will the institution be notified of major changes to your environment that could impact the institution's security posture?								

CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?								
CHNG-05	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?								
CHNG-06	Does the system support client customizations from one release to another?								
CHNG-07	Do you have a release schedule for product updates?								
CHNG-08	Do you have a technology roadmap, for at least the next 2 years, for enhancements and bug fixes for the product/service being assessed?								
CHNG-09	Is Institution involvement (i.e. technically or organizationally) required during product updates?								
CHNG-10	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?								
CHNG-11	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?								
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?								
CHNG-13	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?								
CHNG-14	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)								
CHNG-15	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?								
Data		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
DATA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).								
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?								
DATA-03	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)								
DATA-04	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)								
DATA-05	Do all cryptographic modules in use in your product conform to the Federal Information Processing Standards (FIPS PUB 140-3)?								
DATA-06	At the completion of this contract, will data be returned to the institution and deleted from all your systems and archives?								
DATA-07	Will the institution's data be available within the system for a period of time at the completion of this contract?								
DATA-08	Can the Institution extract a full or partial backup of data?								

DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?								
DATA-10	Are these rights retained even through a provider acquisition or bankruptcy event?								
DATA-11	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?								
DATA-12	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?								
DATA-13	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?								
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)								
DATA-15	Are physical backups taken off site? (i.e. physically moved off site)								
DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?								
DATA-17	Are data backups encrypted?								
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)								
DATA-19	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?								
DATA-20	Does the process described in DATA-19 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?								
DATA-21	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?								
DATA-22	Will you handle data in a FERPA compliant manner?								
DATA-23	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) through any means?								
DATA-24	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)								
Datacenter		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?								
DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?								
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?								
DCTR-04	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?								
DCTR-05	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?								
DCTR-06	Are your primary and secondary data centers geographically diverse?								
DCTR-07	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?								
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime Institute)?								
DCTR-09	Is the service hosted in a high availability environment?								

DCTR-10	Is redundant power available for all datacenters where institution data will reside?								
DCTR-11	Are redundant power strategies tested?								
DCTR-12	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.								
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?								
DCTR-14	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?								
DCTR-15	Are you requiring multi-factor authentication for administrators of your cloud environment?								
DCTR-16	Are you using your cloud providers available hardening tools or pre-hardened images?								
DCTR-17	Does your cloud vendor have access to your encryption keys?								
Disaster Recovery Plan		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).								
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?								
DRPL-03	Can the Institution review your DRP and supporting documentation?								
DRPL-04	Are any disaster recovery locations outside the Institution's geographic region?								
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?								
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?								
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?								
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?								
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)								
DRPL-10	Has the Disaster Recovery Plan been tested in the last year?								
DRPL-11	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?								
Firewalls, IDS, IPS, and Networking		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?								
FIDP-02	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info								
FIDP-03	Do you have a documented policy for firewall change requests?								
FIDP-04	Have you implemented an Intrusion Detection System (network-based)?								
FIDP-05	Have you implemented an Intrusion Prevention System (network-based)?								

FIDP-06	Do you employ host-based intrusion detection?								
FIDP-07	Do you employ host-based intrusion prevention?								
FIDP-08	Are you employing any next-generation persistent threat (NGPT) monitoring?								
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?								
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?								
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?								
Policies, Procedures, and Processes		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?								
PPPR-02	Do you have a documented patch management process?								
PPPR-03	Can you accommodate encryption requirements using open standards?								
PPPR-04	Are information security principles designed into the product lifecycle?								
PPPR-05	Do you have a documented systems development life cycle (SDLC)?								
PPPR-06	Will you comply with applicable breach notification laws?								
PPPR-07	Will you comply with the Institution's IT policies with regards to user privacy and data protection?								
PPPR-08	Is your company subject to Institution's geographic region's laws and regulations?								
PPPR-09	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?								
PPPR-10	Do you require new employees to fill out agreements and review policies?								
PPPR-11	Do you have a documented information security policy?								
PPPR-12	Do you have an information security awareness program?								
PPPR-13	Is security awareness training mandatory for all employees?								
PPPR-14	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?								
PPPR-15	Do you have documented, and currently implemented, internal audit processes and procedures?								
PPPR-16	Does your organization have physical security controls and policies in place?								
Incident Handling		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
IH-01	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
IH-02	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A

IH-03	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
IH-04	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
Quality Assurance		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
QLAS-01	Do you have a documented and currently implemented Quality Assurance program?								
QLAS-02	Do you comply with ISO 9001?								
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?								
QLAS-04	Do you incorporate customer feedback into security feature requests?								
QLAS-05	Can you provide an evaluation site to the institution for testing?								
Vulnerability Scanning		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
VULN-01	Are your systems and applications regularly scanned externally for vulnerabilities?								
VULN-02	Have your systems and applications had a third party security assessment completed in the last year?								
VULN-03	Are your systems and applications scanned with an authenticated user account for vulnerabilities [that are remediated] prior to new releases?								
VULN-04	Will you provide results of application and system vulnerability scans to the Institution?								
VULN-05	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).								
VULN-06	Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?								
HIPAA		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?								
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?								
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?								
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?								
HIPA-05	Have you conducted a risk analysis as required under the Security Rule?								
HIPA-06	Have you identified areas of risks?								
HIPA-07	Have you taken actions to mitigate the identified risks?								
HIPA-08	Does your application require user and system administrator password changes at a frequency no greater than 90 days?								

HIPA-09	Does your application require a user to set their own password after an administrator reset or on first use of the account?								
HIPA-10	Does your application lock-out an account after a number of failed login attempts?								
HIPA-11	Does your application automatically lock or log-out an account after a period of inactivity?								
HIPA-12	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?								
HIPA-13	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?								
HIPA-14	Does your application provide the ability to define user access levels?								
HIPA-15	Does your application support varying levels of access to administrative tasks defined individually per user?								
HIPA-16	Does your application support varying levels of access to records based on user ID?								
HIPA-17	Is there a limit to the number of groups a user can be assigned?								
HIPA-18	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?								
HIPA-19	Does the application log record access including specific user, date/time of access, and originating IP or device?								
HIPA-20	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?								
HIPA-21	How long does the application keep access/change logs?								
HIPA-22	Can the application logs be archived?								
HIPA-23	Can the application logs be saved externally?								
HIPA-24	Does your data backup and retention policies and practices meet HIPAA requirements?								
HIPA-25	Do you have a disaster recovery plan and emergency mode operation plan?								
HIPA-26	Have the policies/plans mentioned above been tested?								
HIPA-27	Can you provide a HIPAA compliance attestation document?								
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?								
HIPA-29	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?								
PCI DSS		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:27013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**	**Trusted CI**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?								
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?								
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?								

PCID-04	Are you classified as a service provider?								
PCID-05	Are you on the list of VISA approved service providers?								
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?								
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.								
PCID-08	What payment processors/gateways does the system support?								
PCID-09	Can the application be installed in a PCI DSS compliant manner ?								
PCID-10	Is the application listed as an approved PA-DSS application?								
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?								
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.								

EDUCAUSE

Acknowledgments

The Higher Education Information Security Council Shared Assessments Working Group c
vision and significant talents to the conception, creation, and completion of this resource

Members that contributed in 2020, 2021, and 2022:
- Mary Albert, Princeton University
- Jon Allen, Baylor University (HECVAT Users CG chair)
- Jill Bateman, Ohio University
- Vince Bonura, Fordham University
- Gwen A. Bostic, Western Michigan University
- Josh Callahan, Cal Poly Humboldt
- Meryl Bursic, Cornell University
- Christopher Cashmere, University of Nebraska
- Jiatyan Chen, Stanford University
- Tom Coffy, University of Tennessee, Knoxville
- Doug Cox, University of Michigan
- Michael Cyr, University of Maine System, IT Accessibility CG Co-Chair
- Glenn Dausch, Stony Brook University
- Suzanne Elhorr, American University of Beirut
- Charles Escue, Indiana University (HECVAT Users CG co-chair)
- Laura Fathauer, Miami University [OH]
- Sean Hagan, University of Alaska
- Greg Hanek, Indiana University
- Tania Heap, University of North Texas
- Lori Kressin, University of Virginia
- Avinash Kundu, EAB Global, Inc.
- Dennis Leber, UTHSC
- Thierry Lechler, UCF
- Sung Lee, Howard Community College
- Matthew Long, University of NebraskaMary McKee, Duke University
- Jeff Miller, University of Central Oklahoma
- Steven Premeau, University of Maine
- Laura Raderman, Carnegie Mellon University
- Mark Rank, Cirrus Identity
- Nicole Roy, Internet2
- Carmen Schafer, University of Missouri
- Kyle Shachmut, Harvard University, IT Accessibility CG Co-Chair
- Eudora Struble, Wake Forest University
- Kate Tipton, California State University at Northridge
- Jeffrey Tomaszewski, University of Michigan
- Luke Watson, Virginia Tech
- Todd Weissenberger, University of Iowa
- William Wetherill, University of North Carolina Wilmington
- John Zage, University of Illinois- National Center for Supercomputing Applications
- Deb Zsigalov, Tennessee Technological University

Members that contributed to Phase IV (2019) of this effort are:
- Jon Allen, Baylor University (working group chair)
- Matthew Buss, Internet2
- Josh Callahan, Humboldt State University
- Andrea Childress, University of Nebraska
- Tom Coffy, University of Tennessee
- Susan Coleman, REN-ISAC
- Susan Cullen, CSU Office of the Chancellor
- Michael Cyr, University of Maine System
- Debra Dandridge, Texas A&M University
- Niranjan Davray, Colgate University
- Charles Escue, Indiana University
- Carl Flynn, Baylor University
- Ruth Ginzberg, University of Wisconsin System
- Sean Hagan, Yavapai College
- Daphne Ireland, Princeton
- Brian Kelly, EDUCAUSE
- Amy Kobezak, Virginia Tech
- Nick Lewis, Internet2
- Sue McGlashan, University of Toronto
- Hector Molina, East Carolina University
- Mark Nichols, Virginia Tech
- Laura Raderman, Carnegie Mellon University
- Kyle Shachmut, Harvard University
- Bob Smith, Longwood University
- Kyle Smith, Georgia Tech
- Christian Vinten-Johansen, Penn State University
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase III (2018) of this effort are:
- Jon Allen, Baylor University
- Josh Callahan, Humboldt State University
- Susan Coleman, REN-ISAC
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Jefferson Hopkins, Purdue University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Amanda Sarratore, University of Notre Dame
- Gary Taylor, York University
- Valerie Vogel, EDUCAUSE
- Gene Willacker, Michigan State University
- David Zeichick, California State University, Chico

Members that contributed to Phase II (2017) of this effort are:
- 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
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Kolin Hodgson, University of Notre Dame
- Tom Horton, Cornell University
- Leo Howell, North Carolina State University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Wyman Miles, Cornell University
- Kim Milford, REN-ISAC
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase I (2016) of this effort are:
- Jon Allen, Baylor University
- John Bruggeman, Hebrew Union College, Jewish Institute of Religion
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Karl Hassler, University of Delaware
- Todd Herring, REN-ISAC
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Craig Munson, Minnesota State Colleges & Universities
- Mitch Parks, University of Idaho
- Laura Raderman, Carnegie Mellon University
- Valerie Vogel, EDUCAUSE

Higher Educat
Change Log

HEISC Shared Asses

Version	Date
v0.6	8/4/2016
v0.7	8/14/2016
v0.8	8/15/2016
v0.9	8/16/2016
v0.91	8/24/2016
v0.92	8/25/2016
v0.93	8/26/2016
v0.94	8/26/2016
v0.95	9/21/2016
v0.96	9/23/2016
v0.97	9/26/2016
v0.98	10/6/2016
v1.00	10/17/2016
v1.01	11/16/2016
v1.02	11/21/2016
v1.03	11/23/2016

v1.04	4/22/2017
v1.05	4/28/2017
v1.06	10/24/2017
v2.00	10/13/2018
v2.01	11/1/2018
v2.02	1/25/2019
v2.03	3/19/2019
v2.04	4/29/2019
v2.10	10/4/2019
v2.11	11/21/2019
v3.0	12/17/2021
v3.01	2/4/2022
v3.01	3/4/2022
v3.01	3/7/2022
v3.02	3/9/2022
V3.02	3/14/2022
v3.03	3/31/2022
v3.03	5/1/2022

v3.03	5/11/2022
v3.03	5/11/2022
v3.03	5/11/2022
v3.03	5/11/2022
v3.03	5/11/2022
v3.03	5/27/2022
v3.04	2/6/2023

ion Community Vendor Assessment Toolkit -

sments Working Group

Description of Change
Merged initial comments and suggestions of sub-group members.
Completed base formulas for all Guidance fields. Changed Qualifier formatting to make questions readable (and optional).
Added SOC2T2 question to datacenter section.
Added Systems and Configuration Management section, added MDM, sep. management networks, system configuration images, Internal audit processes and
Added input from WG meeting on 8/22, removed RiskMgmt section, added question ID's, and removed dup network question.
Added Introduction, Sharing Read Me, and Acknowledgements tabs and content. Also updated report specifics in Documentation.
Integrated grammatical corrections set by Karl, fixed a minor formula error in a guidance cell.
Added Instructions tab, adjusted question ID background color, updated DRP/BCP copy error.
Changed document title to HECVAT. Integrated KDH input.
Added input from NL, 36 modifications across all sections.
Updated Sharing Read Me tab with final language and options table.
Sharing Confirmation section added, updated instructions, updated Sharing Read Me tab, fixed a ton of conditional formatting issues.
Finalized for distribution.
Corrections for grammar, conditional formatting, and question clarification.
Added tertiary services narrative question (DNS, ISP, etc.).
Grammar and spelling cleanup.

Minor layout change in preparation for HECVAT-Lite split
Changed University mentions to Institution; final version before SPC 2017
Added standards crosswalk and Cloud Broker Index (CBI) information
Major revision. Visit https://www.educause.edu/hecvat for details.
Minor calculation revision in Summary Report scoring.
Cleaned up old question references, added Excel backwards compatibility through named ranges, and fixed analyst report view.
Summary Report scoring issues fixed (calculation ranges in the Questions tab, synchronized calculation steps for reporting in both the Full and Lite versions of the
Repaired versioning issues
Updated name, converted question text on Standards Crosswalk tab to vlookups, added Analyst Reference, fixed external links
Updated SSAE 16 to 18. Fixed reference to Standards crosswalk on Summary Report.
Substantial update, see blog post at https://er.educause.edu/articles/2021/10/hecvat-3-0-launches-to-outer-space
Fixed VLOOKUP formulae between Analyst Report and Question tabs that were causing inconsistent results, fixed max score calculation on Values tab. Updated
Fixed Duplicate questions CHNG-14 and PPR-06. Included analyst notes column linked from Analyst Report to main HECVAT Tab, corrected Analyst report display
Fixed Analyst Guidance for CHNG-14 and PPR-06
Corrected Analyst report display of AAA-18, Fixed Compliant answer to DATA-01
Corrected Analyst override scoring and Values scoring table handling of Qual-0x optional sections.
CHNG05-07 incorrectly showed as Qualitative on Analyst report. DCTR08 and 12 incorrectly showed as Quantitative
DCTR 13-16 using wrong data validation list

CHNG-13 and CHNG-14 were duplicate questions, deleted and reordered
PPR-06 and APPL-13 were duplicates, deleted APPL-13 and renumbered
Fixed quantitative/qualitative incorrect listings on Analyst report and HECVAT tab
Fixed AAAI-04-05 and DRPL 04 answers
Fixed IH-04 guidance
Acknowledgments updated - 2020, 2021; Instructions tab updated; numerous guidance updates
Numerous scoring fixes and grammar refinements.

Brief product description:

Company Legal Name:
Product Name and Version:
Contact Name and Information:

Instructions:
Please complete all Scored Criteria questions.

General Questions - Cloud Based

Focus Area	Sub Focus Area	Assessment Question	Supplier Response	Notes
Contracts	Quality Assurance	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?		Scored Criteria
Contracts	Quality Assurance	In the last 12 months, have you engaged an independent auditing firm to examine and report on your organization's controls (e.g. SOC 2 engagement performed in accordance with SSAE-16 or a SAS-70 audit)? If so, please provide a copy of the most recent Type II audit report.		Scored Criteria
Contracts	Quality Assurance	Is a documented data sanitization process in place for disposal or retirement of storage devices? Does this process adhere to DoD 5220.22-M, NIST SP 800-88, ISO 20000 and/or ISO 27000?		Scored Criteria
Contracts	Quality Assurance	Please provide a list of current implementations of a similar size and nature to that proposed for The University of Utah. Would the infrastructure supporting the proposed solution be shared with other clients? If so, what elements and how many clients are in a shared environment?		Scored Criteria
Contracts	Quality Assurance	If your performance commitments are not met, what options do we as the customer have? Can we receive financial compensation for missed performance metrics? Is there an additional cost to the customer in order to adjust performance? (E.g. for hardware changes needed to improve performance.)		Scored Criteria
Contracts	Company Overview and Background	Describe what controls are in place to ensure that The University of Utah can continue business without interruption or undue hardship in the event that your organization goes out of business or the contract is terminated.		Scored Criteria
Contracts	Service Level Agreements	Do you carry cyber-risk insurance to protect against unforeseen service outages or data that is lost or stolen?		Scored Criteria
Contracts	Service Level Agreements	Do you offer clear SLAs in writing? Can we review SLAs that exist for other customers? Can we review your base SLA?		Scored Criteria
Contracts	Service Level Agreements	Does your SLA address data loss and data integrity issues?		Scored Criteria
Contracts	Data	Are ownership rights to all data, inputs and outputs retained by The University of Utah?		Scored Criteria
Contracts	Data	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?		Scored Criteria
Contracts	Data	Are ownership rights retained through a provider acquisition or bankruptcy event?		Scored Criteria
Contracts	Data	Is there a charge for ingress or egress of data?		Scored Criteria
Contracts	Data and Applications	Is the software code put in escrow to be made available to the University of Utah in the event of a bankruptcy?		Scored Criteria
Disaster Recovery	Recovery Prioritization	Can your organization commit to a Recovery Time Objective of 24 hours in the event you experience a disaster or significant business disruption?		Scored Criteria
Disaster Recovery	Recovery Prioritization	Can your organization commit to a Recovery Point Objective of 24 hours in the event you experience a disaster or significant business disruption?		Scored Criteria
Disaster Recovery	Plans	Is an owner assigned who is responsible for the maintenance and review of the Disaster Recovery Plan?		Scored Criteria
Disaster Recovery	Plans	Are all components of the disaster recovery plan reviewed at least annually and updated as needed to reflect change? Please describe that process.		Scored Criteria
Disaster Recovery	Plans	Does your organization have a comprehensive Disaster Recovery Plan?		Scored Criteria
Disaster Recovery	Plans	Is there a defined problem/issue escalation plan for impacted clients?		Scored Criteria
Disaster Recovery	Plans	Is there a documented communication plan for impacted clients?		Scored Criteria
Disaster Recovery	Plans	Do we have the opportunity to review your Disaster Recovery Plan(s) and supporting documentation?		Scored Criteria
Disaster Recovery	Testing	Please indicate the last time that the disaster recovery plan was tested and provide a summary of the results.		Scored Criteria
Disaster Recovery	Testing	Does your organization perform fully integrated end-to-end testing? If not, please describe the scope of your DR testing.		Scored Criteria
Disaster Recovery	Testing	Do the documented test results identify your organization's actual recovery time capabilities for technology and facilities?		Scored Criteria
Disaster Recovery	Testing	Based on your most recent disaster recovery test, what was your actual recovery time?		Scored Criteria
Disaster Recovery	Testing	Does your organization's executive management review and sign-off on documented test summaries, which include test objectives, results, and recommendations?		Scored Criteria

Brief product description:

Company Legal Name:
Product Name and Version:
Contact Name and Information:

Instructions:
Please complete all Scored Criteria questions.

General Questions - Cloud Based

Focus Area	Sub Focus Area	Assessment Question	Supplier Response	Notes
Disaster Recovery	Off-Site Capabilities	Does your organization have a disaster recovery site or a contracted disaster recovery provider?		Scored Criteria
Disaster Recovery	Off-Site Capabilities	What type of availability does your disaster recovery site provide? (hot/cold)		Scored Criteria
Disaster Recovery	Off-Site Capabilities	What is the distance (in miles) of the disaster recovery site from the primary technology location?		Scored Criteria
Disaster Recovery	Off-Site Capabilities	Are back-up files, information and materials to restore and operate key computing environments stored at the alternate site for ready access by authorized personnel?		Scored Criteria
Disaster Recovery	Backups	Are back-ups of the operating system software, utilities, security software, application software and data files necessary for recovery stored at the DR site or another off-site location?		Scored Criteria
Disaster Recovery	Backups	If stored at another off-site location, what is the distance (in miles) between the primary site and off-site location?		Scored Criteria
Disaster Recovery	Backups	Please describe the process for backing up the servers on which the service resides. Are backup copies made according to pre-defined schedules and securely stored and protected?		Scored Criteria
Disaster Recovery	Backups	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?		Scored Criteria
Disaster Recovery	Backups	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?		Scored Criteria
Disaster Recovery	Backups	If desired, can the University of Utah extract a full backup? At what frequency?		Scored Criteria
Network	General	Where are CDN service nodes or datacenters located?		Scored Criteria
Network	General	Does service have peering agreements with research/education networks (Internet2, NLR, TransitRail, etc.)?		Scored Criteria
Network	General	Does service use advanced IP protocols (IPv6, IP Multicast, etc.)?		Scored Criteria
Network	General	Describe the bandwidth requirements for connections between your systems and The University of Utah users.		Scored Criteria
Network	General	Describe the typical duration of transactions.		Scored Criteria
Network	General	Describe TCP/IP ports used between the service and any client or system that The University of Utah operates.		Scored Criteria
Network	General	Please explain your approach to firewall usage, policy, and management. Please include the following details: a) Basis and specificity for access filtering b) Default allow or default protect c) Change control procedures (e.g., who can change rules, how changes are tracked and verified) d) Self-service administration through an API, management console or both e) Firewall audit logging — every change is logged with the user, the time and the type of change		Scored Criteria
Accessibility	Web Accessibility	In the past 18 months, have you completed a Voluntary Product Assessment Template (VPAT) to self-assess the accessibility of your application? If so please provide a copy.		Scored Criteria
Accessibility	Web Accessibility	In the past 18 months, have you engaged an independent firm to evaluate the accessibility of your application? If so, please provide a copy of the audit report.		Scored Criteria
Operational	Availability	How does your organization measure availability? Does the definition of downtime start the minute the outage occurs (i.e., is there a minimum time, such that, any outage less than the minimum is not counted)?		Scored Criteria
Operational	Availability	What are the procedures to recover systems, applications, and data from operational failures? What is your method for testing recoverability component level versus full restore, etc.?		Scored Criteria
Operational	Availability	Will you voluntarily inform The University of Utah of a service disruption?		Scored Criteria
Operational	Performance	How do you monitor and respond to alerts regarding the performance of your service?		Scored Criteria
Operational	Performance	Are network, processor, and database performance monitoring procedures established to identify capacity and performance trends?		Scored Criteria
Operational	Performance	Has your software been load tested? How many concurrent users will it support?		Scored Criteria
Operational	Performance	Do you conduct performance and latency tests annually and share the outcomes with customers?		Scored Criteria

Brief product description:	

Company Legal Name:		Instructions:
Product Name and Version:		Please complete all Scored Criteria questions.
Contact Name and Information:		

General Questions - Cloud Based

Focus Area	Sub Focus Area	Assessment Question	Supplier Response	Notes
Operational	Performance	Are the following performance metrics part of the standard service and are they reported on in five-minute intervals or less? - CPU utilization - Memory utilization - Network I/O performance - Database performance - Disk I/O performance - Average disk queue length		Scored Criteria
Operational	Data Center	Which data centers will be used to serve our application?		Scored Criteria
Operational	Data Center	Do you own your data centers or lease them? If the latter, from whom?		Scored Criteria
Operational	Data Center	Are the data centers staffed 24 hours a day, seven days a week (24x7)? What staff is on-site?		Scored Criteria
Operational	Data Center	What physical security measures are in the data center?		Scored Criteria
Operational	Data Center	Is there redundant power? Batteries? Generators? How often are they tested?		Scored Criteria
Operational	Data Center	What cooling and fire suppression systems are available?		Scored Criteria
Operational	Data Center	How many Internet service providers (ISPs) do you buy connectivity from? Are they on separate telephone company entrances to the facility?		Scored Criteria
Operational	Data Center	At what tier level is your data center (as defined by the Uptime Institute)?		Scored Criteria
Operational	Integration	What type of integrations do you support? (API, web service, flat files, etc…)		Scored Criteria
Operational	Integration	Do you need development level access into our systems for the setup/configuration work?		Scored Criteria
Operational	Integration	Do you have documentation regarding the integration architecture?		Scored Criteria
Operational	Integration	Can you supply a working sample request and the expected response messages?		Scored Criteria
Operational	Integration	What is the SLA response time on reported integration errors?		Scored Criteria
Operational	Integration	Can you access the request/response message when there is an error?		Scored Criteria
Operational	Integration	Do you support user/password in the request to secure the integration?		Scored Criteria
Operational	Integration	Do you have a test environment for integrations?		Scored Criteria
Systems Support	Application General	Is your product or solution a beta version?		Scored Criteria
Systems Support	Application General	Is there a process to do real-time performance scaling to ensure we have adequate performance during peak usage times? If so, please describe the process.		Scored Criteria
Systems Support	Application General	Scalability – How does the solution design and infrastructure support growth and scale to multiple sites, nationally and globally?		Scored Criteria

Utah System of Higher Education

Technical Colleges

Fiscal Year 2023

Summary of Payroll Information

Software Systems	Bridgerland Technical College	Davis Technical College	Dixie Technical College	Mountainland Technical College	Ogden-Weber Technical College	Southwest Technical College	Tooele Technical College	Uintah Basin Technical College
Financial Information System (FIS)	Jenzabar	MS GP Dynamics	MS GP Dynamics	MS Business Central	Sage MAS 500	QuickBooks	QuickBooks	LINQ
Range ot total employees receiving a paycheck each pay period	275 - 413	377-431	150-225	320-475	253 - 327	115 - 170	79 - 113	150-170
Average number of employees receiving a paycheck each pay period	334	398	193	425	284	130	100	163
Total number of active full-time employees	169	229	109	227	148	70	53	103
Total number of active part-time employees	282	239	110	327	145	100	103	62
Total number of pay codes	1,895	38	28	59	14	14	73	60
Total number of benefits offered per FT employee (benefit & deduction codes)	74	28	39	29	22	50	81	70
Total number of W-2 issued for 2023	496	574	271	704	391	188	173	184
Total number of physical time clocks	14	8	-	-	-	-	-	5

Question and Answers for Bid #UU184014613 - Request for Proposal For Payroll/ Human Resource Information System

Overall Bid Questions

There are no questions associated with this bid.