Process and Procedures for Assessing Third Party Software & Service Providers

Acknowledgements
This document is the product of the Southeastern Universities Research Association and has been developed under the direction of the SURA IT Steering Group. Development of this document was led by Gary Crane, SURA Director of IT Initiatives with contributions from the following individuals (listed in alphabetical order):

Mark Cather - CISO, UMBC
Joanna Grama - Director of Cybersecurity and IT GRC Programs, Educause
Leo Howell - CISO, University of Oregon
Amy Kobezak - IT Risk Analyst, Virginia Tech
Bill Koffenberger - Director, Service and Contract Management, GWU
Brian Markham - Assistant VP, Information Security and Compliance Services, GWU
William Miaoulis - University Information Security Officer, Auburn University
Darlene Quackenbush - Info Security Officer/Planning, James Madison University

Target Audience
This document is intended to be used by an institution's IT management team and IT security staff to assist in the development of a process for evaluating cloud and third party vendor software and services with an emphasis on maintaining control of sensitive personal and institutional data. This document has been developed in conjunction with EDUCAUSE and is intended to assist in the development of an institutional process around the use of the Educause Higher Education Cloud Vendor Assessment Tools - HECVAT / HECVAT Lite: **https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool**

1.0 Introduction

Most universities have multiple departmental and individual entities capable of purchasing software and cloud services that have the potential to expose sensitive personal and/or institutional data. The rise in the availability and adoption of cloud services is dramatically increasing the potential for the unintended exposure of sensitive information. Universities must take steps to manage the risks associated with the unintended loss of confidentiality, integrity and availability of sensitive institutional and personal information that is processed and/or retained by third party and cloud service providers. Sensitive data stored in the cloud may include intellectual property (e.g. research data), confidential business information, usernames,

passwords, or highly regulated information such as protected health information, personally identifiable information, or financial data. Institutions may expose themselves to legal and financial liabilities by not having a documented process for managing the risk associated with reliance on the ability of third party and cloud service providers to protect their data.

1.1 Purpose

This document is intended to serve as a guide for an institution to implement a process for assessing the ability of third party software and service providers to meet institutional standards and follow Federal and state guidelines for security and accessibility BEFORE acquisition. The goal of this document is to share the current best practices of several SURA institutions in a form that can be easily updated, modified, and amended to meet individual institutional needs.

1.2 Scope

This document is intended to assist institutions with the implementation of a process for assessing the ability of third party software and service providers (cloud based or on-campus) to:

- Integrate properly with enterprise level applications;
- Adhere to institutional security requirements;
- Include proper security and protection controls for any sensitive institutional and personal data;
- Meet the needs of the campus population with disabilities;
- Identify and contain security gaps and implement compensating measures to mitigate risk.

2.0 Roles and Responsibilities

It is important to identify all the parties inside and outside your institution that may be involved in the acquisition of software or services that may expose institutional data and to identify their roles in evaluating the ability of software and service providers to meet institutional data security requirements. This section identifies the roles and responsibilities of many of the individuals and groups of individuals at a typical institution that may be involved in this process. It is important that all of the parties involved in the acquisition process work together to ensure that the institution's best interests are kept in mind throughout the procurement process.

2.1 Requesting Party: This is the party that is requesting the new tool or service. Instructions in the institutional purchasing process should provide guidance on who the Requesting Party should contact in order to begin a data security accessibility review of a requested tool or service.

2.2 Technology Services: This is the party that will conduct a technical review of a requested new tool or service. At many institutions this role is being filled by an individual with information security and/or risk management expertise. Many institutions have created the

position of Cloud Analyst within to be a point of focus for this activity within the IT Services unit. This person will review the requested new tool or service to ensure that it is compliant with institutional IT requirements and that the new tool or service can be properly integrated into the institution's infrastructure. This person may also work closely with Security and Compliance to address questions regarding the information security, privacy and accessibility components of a requested new tool or service.

2.3 Purchasing: This is the party that manages the purchasing process once a request to purchase a new tool or service is received. The purchasing department likely will review the requested purchase, serve as the initial point of contact for any RFPs or vendor inquiries, ensure that needed IT or other business reviews take place, manage any contracting processes, and serve as the primary business point of contact between the institution and the vendor.

2.4 Vendor: The entity that provides a requested new product or service.

2.5 Data Steward: Data stewards are specialists in understanding institutional data governance and use practices. Often data stewards are specialized within an institutional business area (e.g., business office, academic offices, etc.). They are charged with understanding which data business areas collect, how that data is used, and whether that use complies with institutional data governance policies. In the procurement process, the data steward helps understand how a requested new tool or service will use institutional data and whether that use complies with institutional policy.

2.6 University Legal Counsel: In the procurement process, University Legal Counsel may render advice on the process itself, contractual issues, or in any other matter in which vendor compliance with institutional policies and procedures may be in question.

2.7 Security & Compliance: In the procurement process, institutional security and compliance teams may render advice on the procurement process, and may assist Technology Services in reviewing a vendor's product or service to address questions regarding the information security, privacy posture and accessibility of a requested new tool or service.

3.0 Example Internal Processes: This section provides a set of links to existing documents currently in use at several SURA member institutions. This document will be routinely updated to include additional institutional process and procedure documents as they become available. To have a link to your institution's process added to this document please email your contribution to Gary Crane (gcrane@sura.org).

University of Delaware - Cloud Service Acquisition Procedure:

http://www1.udel.edu/security/policies/cloudserviceacquisition.html

University of Maryland, Baltimore County - Cloud/SaaS Solution Request Process and Cloud Solution Review Process:
https://drive.google.com/drive/folders/0B5DlE0e2uH0fcHFzdDNJOEVNWVU

North Carolina State University - IT Purchase Compliance
https://software.ncsu.edu/it-purchase-compliance/

University of Alabama in Huntsville - Cloud Services and IT Procurememt
https://www.uah.edu/images/administrative/policies/02.01.40-AA_OIT_Cloud_Services_and_Information_Technology_Procurement.pdf

Educause - Higher Education Cloud Vendor Assessment Tool (HECVAT) Updated
https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

4.0 Evaluating Service Providers

4.1 Identifying need for formal assessment (when do you need to invoke a process?)

- **Sensitivity of Data -** It is recommended that an institution develop a data classification standard and use this standard to define when a third-party assessment should be completed. For example, third-party vendors that are accessing public data, or non-sensitive, non-public data may not be subject to a formal assessment. It is strongly recommended that any vendor that will be accessing, processing or storing sensitive data should be evaluated for compliance with institutional standards for securing sensitive data.
- **New acquisitions (two points to invoke)** - both purchasing of software and acquisition of freeware. Partnership should be established with the Purchasing department to ensure that no purchase associated with access to sensitive data is made without an assessment. Partnerships should be established with data stewards and major applications system service owners to ensure that data feeds or system integration is not allowed with 3rd party systems without an assessment being done.
- **Renewals** - for the most part, it's difficult to not approve renewals of software or services that have already been integrated into the business process, however, a security assessment for existing services that interact with sensitive data could expose new risks associated with added features or functions, particularly if the service was not formally evaluated at initial acquisition. An application inventory system (e.g., Excel) should be

implemented showing appropriate renewal dates so that this conversation can start well before the renewal date.

4.2 Assessment Tools

EDUCAUSE has developed a pair of assessment tools (a long and a short version) that are freely available from the EDUCAUSE website:
https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

4.3 Interacting with the vendor

- **Initial contact** with the vendor should come from the department making the purchase. Adequate survey tools and specific guidance to the purchaser should be provided by the institution's security team so the departmental contact can collect the information required to properly complete a security screening of the vendor.
- **Follow-up contact** should be a conversation between the security team and the vendor's security team to avoid inefficiencies and mistranslation of technical information.

4.4 Verifying vendor responses

- Vendors should be asked to provide documentation and appropriate evidence (e.g., SOC 2 reports, ISO 27001/2 certification, validation of PCI DSS compliance, HIPAA compliance) to verify their responses. Vendors may request a NDA be signed prior to sharing these materials. The institution will have to decide on a case-by-case basis whether or not to sign a NDA with the vendor. The NDA process may prolong the assessment and ultimately hold up the procurement process.
- Level of risk should be determined by the type of data involved in the transaction. Risk is typically divided into at least two categories; High Risk and Low Risk.
    - **High risk systems/services** - typically, this represents a relatively small number of business critical applications that will need careful review of vendor qualifications. This should include systems or services that process or store regulated data (e.g., FERPA, HIPAA, GLBA, PCI, etc.), or any data that the institution has flagged as sensitive. The institutional IT security team should perform all reviews of vendor services that support high risk systems or services.
    - **Low risk systems** - typically this represents the largest category of reviews that must be done and includes all of the systems or services that are not considered high risk. Many institutions rely on the IT Security Team to complete these reviews, however, this can often result in a review bottleneck if this task is understaffed in the IT unit. With adequate guidance and training this task could be delegated to the department making the purchase. When security reviews are delegated outside of the IT Services unit a review process should be established that samples departmental reviews on a periodic basis to determine to ensure that

institutional standards are being met. This review process should also provide insights into which departments need further training or could be approved to conduct higher risk reviews.

4.5 Resolving conflicts or deficiencies with vendor responses

- From a security standpoint, the majority of conflicts that will arise relate to compensating controls that a vendor claims are sufficient to meet the spirit of the control in question. These issues often require specialized technical knowledge to make an appropriate judgement call. As such, the institutional IT security team should be responsible for working through these issues with the vendor and making a final go/no-go recommendation to the department acquiring the service.
- If the IT Security Team recommends a no-go and the Department still wants to proceed, then the data steward for affected data needs to be engaged and the decision to complete the purchase should be escalated to the appropriate authority.

4.6 Vendor approval

- **Security Assessment Result** - the outcome of any security assessment should result in a clear go/no-go recommendation, a list of reasons for any negative recommendations, and suggestions for possible resolutions for vendor deficiencies. Assessment results need to be made available in a timely manner and delivered to the appropriate parties (requesting department, purchasing, IT management …)
- **Integration & Data Sharing** - Any form of integration with existing systems, transfer or creation of new data, should be approved by the appropriate data stewards and system owners.
- **Workflow Approval** - an ideal process will involve a workflow with different stakeholders (security, accessibility, data stewards, etc.) being required to provide approvals. Delegations can be worked out as well.
- **Certificate** - departments should be given an official stamp of approval for the requested system or service with any relevant criteria such as expiration dates for the assessments and required reassessments.
- **Conditional Approval** - in some cases, the assessment result may be lacking but a conditional approval is given, allowing the vendor a clearly defined amount of time to correct a deficiency or mitigate a risk (e.g., vendor is in the middle of doing their SOC 2 cert and you allow them to provide details post-purchase).

4.7 Verifying vendor performance and appropriate implementation

- **Expiration date** - it is important to set an expiration date on certification to force a hard date for reassessment. Reassessment intervals will vary based on the level of risk associated with the service. Reassessment intervals should be agreed to prior to completion of purchase and should be included in the vendor purchase agreement.

- **Periodic update** - highly recommended that a periodic update be sent to the vendors (preferably via the department) to determine if any changes have taken place that could impact the assessment results and the state of security for the system or service.
- **External Factors** - changes in security standards, newly discovered security risks and other alerts should also be considered in the ongoing review process.

5.0 Tracking Vendor Performance and Resolving Problems

Vendor Management should generally begin as a process that guides sourcing and selection processes, enforces and tracks service delivery ensuring clear expectations and raising issues for collaborative remediation, and ultimately enabling clear separation when the engagement ends. The techniques used to track performance of vendors can borrow heavily from service management functions such as incident and change management; however, in the end successful vendor performance management will require clear and often measurable expectations that can be measured with exceptions managed through a clearly defined process. Contracts and agreements serve to guide performance and state objectives and are only impactful when the agreed terms are clear, unambiguous, measurable and reasonably attainable.

5.1 Vendor support and maintenance

Institutions should document support and maintenance expectations either based on a model such as ITIL suggested practice or simply organizing and defining key activities in the areas of incident, problem and change management or collectively service management. Additional best practices or processes could be added to increase specificity or document specific concerns or business needs that the vendor must support through their delivered solution.

An approach that may provide both the initial clarification of desired outcomes from the vendor provided solution as well as manage performance over time would involve using checklists or questionnaires that business units and technology support teams can use to document needs. As vendor support processes are considered, the mapping of institutional methods, expectations and needs should be mapped and compared to vendor service levels. Three critical focus areas include incident management, capability modifications or changes, major issue remediation and reporting.

While incident, change and problem management processes and procedures are increasingly commonplace and mature at most institutions, vendors may omit details of how these are managed or reference generic 'service levels' referenced from contracts or agreements. These referential documents are often fixed in content and general in nature. While these service levels may be workable in some instances, institutions should carefully evaluate how and where generic approaches need to be supplemented by specific processes. Escalation of incidents is one example where the defined criteria for escalation should be evaluated against the business needs

and institutional expectations. Technical escalations as well as management escalations are both critical elements to review. Status reporting to submitters and vendor managers should be defined and regular checkpoints established to ensure transparency and provide data to evaluate performance. Finally, tools and procedures should be reviewed for integration opportunities or potential conflicts.

Sample Vendor Support and Maintenance Questions

Tools and potential interoperability:
What tools and documented processes will be used for our engagement? What level of configuration is possible to map these to existing processes? Are there integration possibilities with existing tools to provide seamless support transitions between support teams?

How will requestors obtain updates on status at the individual ticket or request level? Does the institution have the ability to view requests and tickets individually or at the summary level? What typical interactions would end users or technical support staff have with the vendor support teams?

Actionable Reporting:
What aggregate reporting will be available to institutional management? How will service expectations or levels be measured against these data and what corrective actions can result? Does the institution have financial recourse if service levels are violated or breached? Who is responsible for tracking service level breaches and initiating appropriate actions (corrective actions, service or financial credits, escalations, etc.). What are the plans and needs for checkpoints and performance management meetings and how are institutional business expectations reflected in these contacts?

5.2 Vendor stability and acquisitions
Institutions should perform due diligence in ascertaining the financial and organizational fitness of a potential vendor. In addition to working collaboratively with procurement offices to leverage research sources and importantly lists of disbarred or banned vendors. Several items that can provide protections for the institution include contract provisions that assist in risk management and inform discussions regarding the stability and maturity of a vendor.

The following items should be reviewed and understood in any vendor agreement. Specific contract language examples included below are for illustration purposes only and should not be included in contracts with vendors without careful review by institutional legal counsel and purchasing and risk management offices:

***Suggestion / Example*: Require Up-To-Date Certificate of Insurance –** A certificate of insurance maybe a requirement of the institution's Risk. Management Office, but also provides verification of safeguards and vendor maturity.

[Example Agreement Language]

Certificate of Insurance ("COI") with proof of the following amounts of coverage:
The [UNIVERSITY NAME] is to be named as an additional insured on all liability policies, except for Workers Compensation. The foregoing insurance and limits of coverage are to be considered as minimum requirements under this Agreement, and in no way shall limit the Vendor's liability. Each policy of insurance shall be issued in a company or companies licensed to do business in the [UNIVERSITY STATE], maintaining a Best's rating of at least A-, VII, and shall provide for written notification to Customer at least thirty (30) days prior to termination. The correct certificate holders' name must be shown as: [OFFICIAL UNIVERSITY ADDRESS].

[UNIVERSITY] minimum requirements for Professional Services:
Workmen's Compensation/Employers' Liability: Statutory/$1M
Commercial General Liability: $1M
Automobile Liability: $1M
Umbrella Liability/Excess Liability: $2M
Proof of Professional Liability Coverage: Errors & Omissions/$2M

***Suggestion / Example:* Define and Document Mutual Indemnification**

[Example Agreement Language]

Each party shall be responsible for any and all costs, damages, claims, liabilities or judgments which arise as a result of the negligence or intentional wrongdoing of its employees or other agents. Any costs, including reasonable attorney's fees, for damages, claims, liabilities or judgments incurred at any time by one party as a result of the other party's negligence or intentional wrongdoing, or failure to perform any obligation undertaken or covenant made in this Agreement shall be paid for, or reimbursed by, the other party.

***Suggestions / Example*: Clarify Monetary Liability Clauses:**

[Example Agreement Language]

EXCEPT FOR DAMAGES ARISING FROM EITHER PARTY'S INDEMNIFICATION OBLIGATIONS SET FORTH ABOVE, Neither Party shall be responsible for, nor entitled to, any indirect, consequential (including lost profits) or punitive damages.

***Consideration*: Protection of Source Code in Escrow**

Institutions should evaluate the potential of vendors ceasing operations or support of a solution or service and consider how source code escrow could be used to reduce business interruptions. In the case of untested new to market vendors, software code escrow accounts and corresponding contract language governing use could provide an avenue for planned transition or service provision in the event of a catastrophic event impacting vendor operations.

5.3 Price controls

Universities can leverage negotiation techniques to seek the best value for services and licenses. Additionally, the following strategies can be leveraged to support cost control efforts:

Suggestion: **Clarity on details and deliverables** - Clearly defined scope and deliverables must be stated in the agreement. This means full understanding and documentation of needs and documented means to measure outcomes including deliverables.

Suggestion: **Links between deliverables and payments** - Milestones that include defined activities/ deliverables to be attained at various checkpoints. Tying these to payments provides a financial incentive to perform.

Suggestion/ Example: **Change Management Process and Approvals for Services and Costs** - Direct statements concerning required approvals for changes in cost

[Example Agreement Language]

Prior written approval by [UNIVERSITY] is required for any additional costs above what is stated in this Agreement.

Consideration: Language that addresses budgeting processes that may impact availability of funds. Government funding sources and grantors may have specific language around price controls and multi-year commitments.

Consideration: In some cases, stable and predictable service delivery may be more assured through multi-year agreements, however, shorter-term agreements also provide benefits. Consider both benefits and risks from a probability and impact perspective:

- Transition Consideration – more frequent renewal terms may provide flexibility in changing vendors or solutions to alternate sources but benefits may be impacted by organizational agility on decision making, sourcing, implementation projects and business operations;
- Cost increase controls and renewal language with defined increases as opposed to multi-year agreements;
- Pace of business and technology changes and organizational change drivers and goals;

- What cancellation clauses are included – do the provisions sufficiently empower the university or are they more focused on the vendor. Consider how deliverables and performance can be linked to university rights to terminate a contract or engagement.

Suggestion/ Example: **Place Constraints on Travel & Miscellaneous Expenses**

[Example Agreement Language]

[The UNIVERSITY] will reimburse [insert vendor name] for actual, customary, and reasonable travel and miscellaneous expenses with supporting documentation. Travel expenses include meals, lodging and similar out of pocket expenses. [insert vendor name] shall use commercially reasonable efforts to minimize such expenses. Expenses will require prior written approval by the [UNIVERSITY] prior to being incurred by [insert vendor name] or submitted for reimbursement. Receipts are required for reimbursement of expenses.

Suggestion / Example: **Consider the potential impacts of Force Majeure clauses and related financial risks**

[Example Agreement Language]

Neither party shall be responsible for any failure or delay in its performance under this Agreement and any SOW due to causes beyond its reasonable control, including but not limited to, labor disputes, strikes, lockouts, shortages of or inability to obtain labor, energy, raw materials or supplies, war, riot, acts of terrorism, civil unrest, an act of nature (including but not limited to fire, flood, earthquakes or other natural disasters) or governmental action (including but not limited to any law, regulation, decree or denial of visas or residence permits). In the event that either party wishes to invoke force majeure, that party shall within ten (10) calendar days after the occurrence of the event of force majeure has become known to that party, send a written notice of such event to the other party.

The party claiming the benefit of the Force Majeure clause will: (a) take all reasonable steps to remedy or abate the Force Majeure and mitigate its effects on the other party; (b) keep the other party fully informed of such steps as have been taken and are planned; (c) meet its obligations under this Agreement and any SOW as far as is practical given the Force Majeure; and ***(d) where the party claiming the benefit of the Force Majeure clause is [the Provider], refund or credit [the Customer] the Charges to the extent the Services were not provided as a result of the Force Majeure.***

In the event that a force majeure event prevents either party's performance for a period of thirty (30) days, either party shall be entitled to terminate the Agreement and any SOW upon written notice to the other party. The provisions of this Section shall not apply to the payment of fees or

to any other payments due from either party for services already performed. The parties will work in good faith to prevent one party from unfairly benefiting from the force majeure event.

5.4 Data ownership and recovery (format, speed of recovery)

***Consideration*: Verifying standard contract provisions**
Some vendors will propose language that indicates that they will safeguard data at a level consistent with how they manage data. This clearly represents risk for the institution that does not fully understand the vendor's standards. Additionally, how will an institution know when these standards change and what recourse will they have to safeguard data.

Consideration: **Compatibility of service agreements with institutional standards**
Service agreements will need to address institutional data restrictions and definitions. One suggested approach is a standard Confidential Data Addendum, that can be leveraged for all contracts that involve storage of or access to various types of data.

Suggestion: **Create and synchronize data definitions**
The following examples define data at three levels. Definitions should map to institutional definitions.

[Example Agreement Language]

a. *Confidential Information means all information and data provided to Service Provider that is protected by statute or regulation, or is protected by University policies, contracts, or designation in any medium or form. Confidential Information includes Personally Identifiable Information, as hereinafter defined, relating to students, faculty, staff, users of University services and facilities, and information about the University's network and information technology infrastructure. More specific laws and policies govern certain types of information, such as the Family Educational Rights and Privacy Act (FERPA), which protects personal information about current and former students, the Health Insurance Portability and Accountability Act (HIPAA), which governs the use of protected health information, the Gramm-Leach-Bliley Act (GLBA), which protects personal financial information, and other statutory or regulatory requirements. Confidential Information also includes credentials (e.g., passwords, PKI certificates) to protect systems containing Confidential Information. By way of illustration only, some examples of Confidential Information include: personally identifiable information from student educational records, social security numbers, bank account numbers and other personal financial information, and medical information.*

b. Personally Identifiable Information includes, but is not limited to: (i) personal identifiers such as name, address, phone number, date of birth, social security number, and student or personnel identification number; (ii) personally identifiable information contained in student education records as that term is used in the Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. § 99.3; (iii) protected health information as that term is defined in the Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 160.103; (iv) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; (v) nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. § 6809; and (vi) other financial account numbers, access codes, driver's license numbers; and state- or federal-identification numbers such as passport, visa, or state identity card numbers.

c. Restricted Information means all information and data provided to Service Provider excluding Confidential Information that must be protected from unauthorized access, use, or disclosure due to proprietary or privacy considerations. Restricted Information is limited to members of the University community who have a legitimate need to for such information. By way of illustration only, some examples of Restricted Information include: employment data, payroll records, and university telephone and directory information.

***Consideration*: Intellectual Property and Data - Ensuring data ownership clarity**
Many agreements will address intellectual property ownership – almost always emphasizing the vendor's ownership. Some institutions have specific work for hire and other provisions around intellectual property ownership. In addition to ensuring thorough understanding of these more traditional intellectual property concerns, clear definitions and statements regarding data ownership, particularly for confidential or restricted data, are important considerations for agreement reviewers. In any event, ensure that violations have meaningful penalties or provide flexibility from the institutional perspective.

***Suggestion*: Link data safeguards to specific standards –**

- Center for Internet Security - see http://www.cisecurity.org
- Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/
- National Institute for Standards and Technology - see http://csrc.nist.gov
- ISO/IEC 27000-series - see http://www.iso27001security.com/

***Consideration*: Data Storage**.

Data storage restrictions should reinforce the location of stored data and emphasize that data storage should be limited to agreed systems, servers, and locations. Provisions outlining restrictions on transfers or copying data should be noted such that they cover the likely use cases or misuse cases including convenience copies and flexible access needs facilitated by making copies.

***Consideration*: Data Encryption**
Provisions for the encryption of data at rest or in transit should be considered and required as appropriate to the data classification and associated risks.

***Consideration*: Data Transmission**
Data transmission restrictions or guidance should be consistent with the types of data and associated risks. Institutions may want to ensure that data is only transmitted between locations or providers as agreed to in writing and define the methods and technologies required for transmission.

Consideration: **Disaster Planning, Testing and Service Resumption**
As with force majeure language, the definition of disaster recovery and service restoration terms are critical to ensuring services and minimizing operational impacts. Based on the sensitivity of the data and the criticality of the business operations supported by the solution, disaster recovery requirements including defined procedures, expectations, testing transparency and active engagement should all be defined in agreements. In considering these elements, the tradeoffs between cost and resiliency will determine what is reasonable.

Consideration: **Data Recovery and Re-use**
The design of a solution or service may dramatically limit or facilitate the retrieval of data for use in other systems. Standards can provide a starting point, but many solutions based on standards will still produce unstructured data that is impossible to use without schema and other knowledge that vendor will generally be unwilling to share. Even with the inherent barriers, institutions should define how they will extract data or be provided with data, the format of the data and where possible information that would facilitate effective use of the data in a new environment. Leveraging software code escrow can also provide a potential solution to being able to make extracted data usable. As institutions consider how their data should be accessible and how it would be usable independently from the vendor solution, they should consider early in service design the likely need to migrate to a new version or product and identify ways to design solutions with these needs in mind.

5.5 Continuous verification that additional modules have not been added

***Consideration*: Application and Configuration Changes**

To seek greater transparency related to application changes impacting functionality, user interfaces and capabilities, it is important to understand how these activities are managed and communicated. In shared services solutions there are added implications. One important item to look for is that service providers may bundle services or describe services through references from agreements to websites. In some cases these references are not contractually binding and the services not specifically governed by a contract.

Suggestion/ Example: Documented Change Management Processes

Documented processes and required approvals should be included in purchase orders and agreement terms and conditions.

[Example Language from Purchase Order Terms and Conditions]

The PO, when accepted as indicated herein, may not be modified, amended, rescinded, or in any way varied, except by a writing signed by the parties.

Suggestion/ Example: Documented Change Management Processes

[Example Agreement Language]

This agreement when accepted as indicated herein, may not be modified, amended, rescinded, or in any way varied, except by a writing signed by the parties.
[UNIVERSITY] may incur additional costs:

1) *[UNIVERSITY] is impacted because vendor makes changes to its' Terms and Conditions at anytime without Notice to [UNIVERSITY]*
2) *[UNIVERSITY] impacted because vendor makes changes to features and functionality without notice (impacts [UNIVERSITY] users/systems)*
3) *Contractual changes that affect both parties (e.g. changes to price, delivery schedule, quantity, nature of deliverables, key personnel, or terms and conditions)*

Suggestion/ Example: Documented Change Management Processes for Professional Services

[Example Agreement Language]

Prior written approval by [UNIVERSITY] is required for any additional costs above what is stated in this Agreement.

6.0 Identifying Total Cost of Ownership of 3rd Party Vendor Services

In the Spring of 2015 Educause released a framework for identifying the total cost of ownership (TCO) for both cloud-based and on-premises IT services. Educause has graciously allowed

SURA to reference this Framework for inclusion in this document. Below is an excerpt from the introduction to the Educause TCO Framework followed by a link to the full document:

"One of the common justifications for moving to cloud services is cost savings, but the data are often insufficient to support such claims due to the inherent challenges in effectively identifying and comparing the total cost of ownership (TCO) for both cloud-based and on-premises fulfillment of IT services. Pertinent costs for on-premises services are often hidden, are partially visible, or unaccounted for because they are not part of the requesting department's budget (e.g., electricity, space, staffing, etc.). The ability to effectively compare TCO is essential to understanding the complete impact on our institutions and the attendant shifts in costs as we migrate to the cloud. Clarity about TCO also underscores the strategic shifts in IT service delivery that higher education is experiencing.

To address the challenge of fully understanding costs and to facilitate data-based decisions, the ECARTCO Working Group has created a TCO framework. Appropriate application of the TCO framework will help institutions effectively understand and analyze all costs associated with running a system or service on premises versus moving it to the cloud. The framework enables more accurate identification of the cost to a specific department, as well as the cost to the institution as a whole. However, the framework is not a silver bullet; often case, the decision to select one option or another may include other factors that make up the full business case, such as capital investment required, staff skillsets, security, privacy, etc. In this TCO framework, our goal is to incorporate all the significant factors impacting the total long-term investment into a solution. Additionally, we want to determine and identify the key stakeholders who are responsible for funding the expense."

ECAR Total Cost of Ownership for Cloud Services - A Framework:
https://library.educause.edu/~/media/files/library/2015/4/ewg1503-pdf.pdf

Additional Resources

EDUCAUSE, Higher Education Cloud Vendor Assessment Tool - **HECVAT / HECVAT Lite:** **https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool**

EDUCAUSE, Information Security Guide - Vendor and Third-Party Management
https://spaces.internet2.edu/display/2014infosecurityguide/Vendor+and+Third-Party+Management

EDUCAUSE Center for Analysis and Research, Total Cost of Ownership for Cloud Services - A Framework:
https://library.educause.edu/~/media/files/library/2015/4/ewg1503-pdf.pdf

Acronyms

CISO - Chief Information Security Officer

FERPA - Family Educational Rights and Privacy Act is a federal privacy law that gives parents certain protections with regard to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules.

GLBA - The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.

HIPAA - Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information.

ISO certification - ISO is an independent, non-governmental international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. ISO/IEC 27001 is the relevant standard that provides requirements for an information security management system (ISMS).

ITIL - formally an acronym for Information Technology Infrastructure Library, is a set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.

NDA - Non-disclosure Agreement

PCI - Payment Card Industry

PCI DSS - The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that organizations that accept, process, store or transmit credit card information maintain a secure environment.

SOC 2 - SOC 2 is an auditing procedure that ensures that service providers securely manage client data to protect the interests of your organization and the privacy of its clients.

TCO - Total Cost of Ownership