Baldwin Wallace University Information Technology Standard

Issued by:	**Information Technology**
Title:	**Vendor Risk Assessment**
Number:	**ITS-BW-16-02**
Publish date:	**July 17, 2019**

A. Vendor Risk Assessment Process

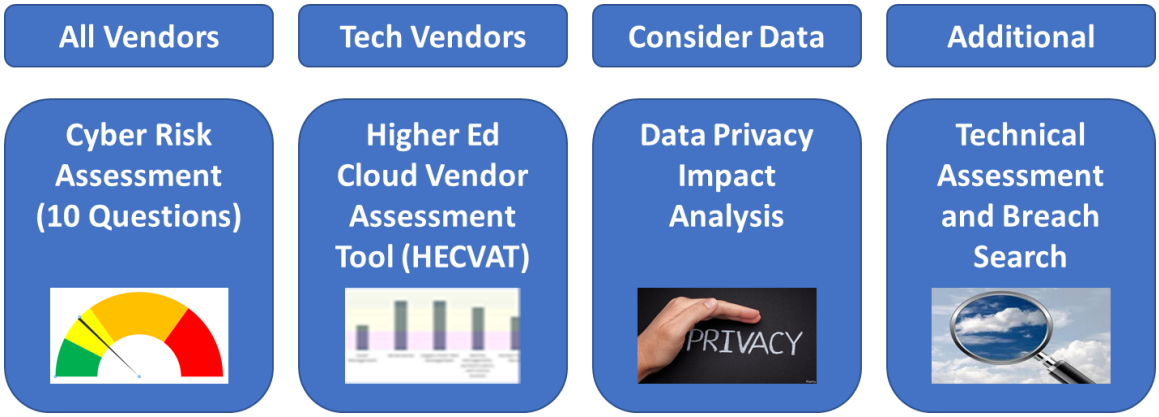
Applicability:

1. Baldwin Wallace University employees wanting a vendor to do business with Baldwin Wallace University shall ensure that each vendor is evaluated according to this process prior to contracting.

2. Vendors wanting to do business with Baldwin Wallace University shall ensure that a cyber risk assessment has been completed prior to performing services, providing products, or engaging with Baldwin Wallace University.

3. Baldwin Wallace University Procurement and Supply Chain groups are primarily responsible for ensuring that these assessments are performed prior to contract approval.

Process Summary:



Inputs to this process:

1. Inputs to this process include:

   - The project has been identified, and a project charter or request for information has been submitted that includes a detailed description of the expected services, solutions, or systems that will be provided.

   - It has been determined that a vendor qualifies for a risk evaluation to be performed.

   - This assessment will be used to gauge the cyber readiness and resiliency of organizations doing business with Baldwin Wallace University. Therefore,

documentation that supports the selected service, system, solution, or product is required and can be attached or stored in a folder with this assessment.

2. These assessments may require that a member from the Vendor's Information Technology or Security teams take part in the interview process. (or fill out the form directly)

    - As such, a host of information may be requested, reviewed, and attached, including but not limited to policies, charters, procedures, attestation of regulatory compliance, etc.

B. Evaluating Vendors

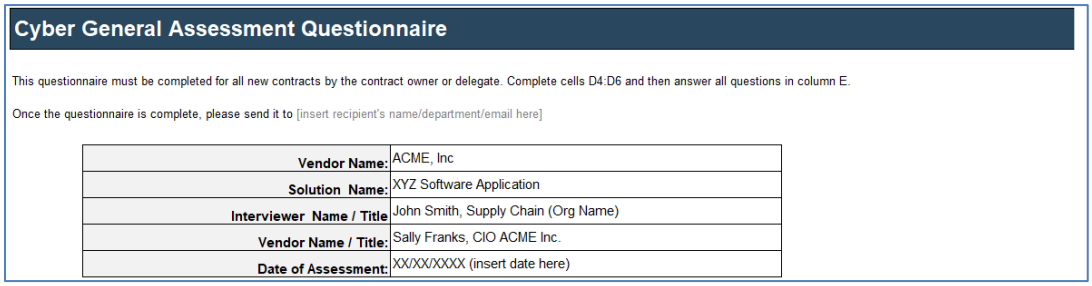
The Cyber Risk Assessment is a 10-question survey intended to depict the overall (general) cybersecurity posture of the vendor who is being considered to do work with Baldwin Wallace University.

This file contains the Cyber Risk and Data Privacy assessments.

1. Typically, these forms are to be populated, executed, and owned by a representative/employee or designee of Baldwin Wallace University. Such as a trained, informed, and cyber aware supply chain or procurement representative.

2. The person filling out the form will herein be referred to as the "Interviewer".

3. The Interviewer should populate the top portion of the matrix with the vendor name, vendor representative's name/title, their name/title, and date of the interview:



Cyber General Assessment Questionnaire

This questionnaire must be completed for all new contracts by the contract owner or delegate. Complete cells D4:D6 and then answer all questions in column E.

Once the questionnaire is complete, please send it to [insert recipient's name/department/email here]

Vendor Name:	ACME, Inc
Solution Name:	XYZ Software Application
Interviewer Name / Title	John Smith, Supply Chain (Org Name)
Vendor Name / Title:	Sally Franks, CIO ACME Inc.
Date of Assessment:	XX/XX/XXXX (insert date here)

4. The Interviewer shall ask each of the questions on the sheet, indicating the vendor's answers to each:

    a. Choices for answers to questions include:

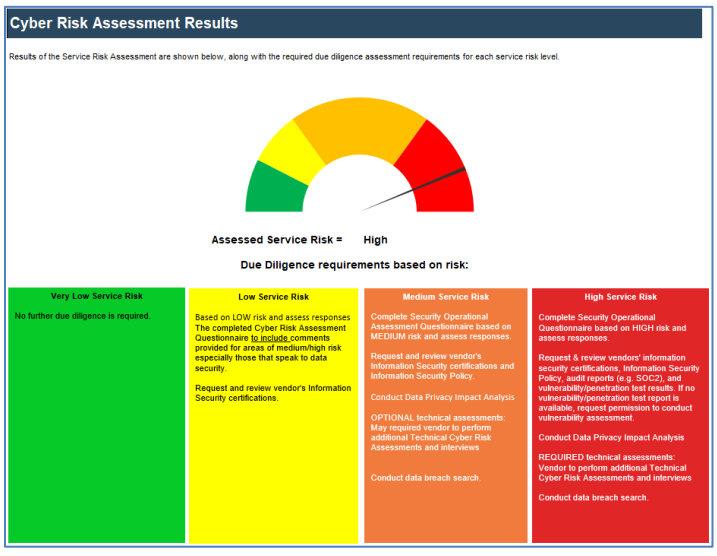
        - **N/A: Question is not applicable (requires a comment)**
        - **Low: As defined for each question**
        - **Medium: As defined for each question**

- **High: As defined for each question (requires a comment)**
- **No: Indicates a negative answer to the question (requires comment)**
- **Unsure: Indicates a level of uncertainty about the question (requires comment)**
- **Yes: Indicates a positive answer to the question (requires comment)**

5. Once all questions are answered, the weighted score column (F) will calculate the vendor's level of compliance and risk relative to Baldwin Wallace University's ratings.

#	Question	Guidance	Response	Weighted Score	Comments
1	What is the estimated one-time or annual (whichever is appropriate or higher) cost associated with the contract?	**N/A** = No cost **LOW** = $100,000 or less **MEDIUM** = Over $100,000 but less than $1,000,000 **HIGH** = $1,000,000 or more	High	0.1	
2	In the event of an extended service outage (i.e. one week or longer), what would be the estimated impact to business operations?	**N/A** = Negligible impact **LOW** = Minimal impact (i.e. minor impact to our customers, but likely no lost revenue) **MEDIUM** = Moderate impact (i.e. impact to our customers which may lead to lost revenue) **HIGH** = High impact (i.e. significant revenue loss, potential regulatory fines)	Medium	0.06	
3	To what extent will data received from the vendor (e.g. revenue, costs) affect our financial reporting process, such that a successful cyber attack on the vendor could impact our financial reporting obligations?	**N/A** = No possible impact **LOW** = Minimal impact (data obtained from vendor is not a direct input into financial reports) **MEDIUM** = Moderate impact (data obtained from vendor is a direct input into financial reports, but unlikely to be material) **HIGH** = High impact (data obtained from the vendor will be a direct material input into our financial reporting process)	High	0.15	
4	To what extent will the vendor be supporting or operating controls on our behalf which are required by compliance	**N/A** = None **LOW** = Vendor will be indirectly supporting our internal operations of compliance controls **MEDIUM** = Vendor will be directly supporting our internal operations of	Low	0.05	

6. The next worksheet, titled "Cyber Risk Assessment Results", depicts the relative risk for that vendor based on the attached criteria.



7. The needle will indicate the level of relative risk (these totals can be adjusted on the hidden "Calc's for Risk Assessment" sheet)

8. Based on the position of the needle, the Due Diligence is defined as follows

a. Very Low Service Risk (Green)

    i. No further diligence is required because no or very little risk to the organization or it's people, assets, and/or data exists.

    ii. Proceed to Data Privacy Impact Analysis (DPIA)

b. Very Low Service Risk (Yellow)

    i. The completed Cyber Risk Assessment is sufficient provided areas of interest include comments that mitigate interviewer concerns.

    ii. The interviewer may contact Information Security with any concerns that need clarification or further guidance.

    iii. All areas found to be Medium or High risk shall require a comment demonstrating mitigation of this question.

    iv. Additionally, the interviewer (or Information Security) may request additional attestation of compliance standards and certifications.

    v. If the vendor is an IT-based service that holds and/or processes BW data, then the interviewer may consider using the "Light Version" of the High Education Cloud Vendor Assessment Tool (HECVAT) developed by Educause and REN-ISAC (https://www.ren-isac.net/public-resources/hecvat.html) to completely define the vendor's risk to BW.

    vi. Proceed to Data Privacy Impact Analysis (DPIA)

c. Medium Service Risk (Orange)

    i. In addition to the completed Cyber Risk Assessment, a Medium score requires that the interviewer use the "Light Version" of the High Education Cloud Vendor Assessment Tool (HECVAT) developed by Educause and REN-ISAC (https://www.ren-isac.net/public-resources/hecvat.html) to completely define the vendor's risk to BW.

    ii. Optionally, the interviewer or Information Security may request additional attestation of compliance standards and certifications.

    iii. Optionally, the interviewer may request Information Security to perform a "Data Breach Search" on the internet for that vendor.

    iv. Proceed to Data Privacy Impact Analysis (DPIA).

d. High Service Risk (Red)

    i. In addition to the completed Cyber Risk Assessment, a High score requires that the interviewer use the "Light Version" High Education Cloud Vendor Assessment Tool (HECVAT) developed by Educause and REN-ISAC https://www.ren-isac.net/public-resources/hecvat.html to completely define the vendor's risk to BW.

    ii. Additionally, the interviewer (or Information Security) shall request additional attestation of compliance standards and certifications.

1. These shall include but not be limited to:

    a. Audit reports such as SOC 2 Type 1 and/or 2 Reporting

    b. Other information security certifications held by the Vendor

    c. Vulnerability and Penetration Testing Outcomes

    d. Vendor may be asked to perform vulnerability assessments

iii. The interviewer shall request Information Security to perform a “Data Breach Search” on the internet for that vendor.

iv. Proceed to Data Privacy Impact Analysis (DPIA)

C. Data Privacy Impact Analysis (DPIA)

The Data Privacy Impact Analysis (DPIA) is required to be performed by any organization that is subject to the EU General Data Protection Regulation (GDPR), which replaces the Data Protection Directive 95/46/EC, and is designed to:

- Harmonize data privacy laws across Europe,
- Protect and empower all EU citizens data privacy
- Reshape the way organizations across the region approach data privacy.

Additionally, a data privacy impact analysis is also required by any organization subject to the California Consumer Privacy Act or the CCPA or similar laws being drafted in the United States and abroad.

1. This form may be filled out by any persons deemed appropriate by the Information Security Director/CISO.

2. Typically, the DPIA is filled out by a subject matter expert, and business owner of the technology being implemented, or change is made to the data. The data steward should be well-positioned to understand both the technological change being proposed, as well as the impact of that technology on the business function, specifically, the impact to personally sensitive data or personally identifiable data. Additionally, one should consider the impacts on all types of sensitive data classified above Level 1 in accordance with the Data Classification approach described in Appendix A: Data Classification Strategy.

3. This questionnaire is to be filled out by the Departmental owner, Information Technology SME, or Designee to arrive at the amount of residual risk that may remain after assessing the protections that are afforded by applied controls. This "Residual Risk" is then to be assessed based on a High, Medium, or Low basis and seeks approval from specific members of the security/information technology leadership teams to move forward. This analysis shall be performed prior to engaging a technology vendor, prior to a technical change to the existing technical environment, or anytime changes are made to technologies that could feasibly impact sensitive data.

4. Begin by filling out the demographical information at the top of the form with the vendor name, vendor contact's name/title, their name/title and date of the qualified person filling out the form:

Data Privacy Impact Analysis

This questionnaire is to be filled out by the Departmental owner, Information Technology SME, or Designee to arrive at the amount of residual risk that may remain after assessing the protections that are afforded by applied controls. This "Residual Risk" is then to be assessed based on a High, Medium, or Low basis and seeks approval from specific members of the security/information technology leadership teams to move forward. This analysis shall be performed prior to engaging a technology vendor, prior to a technical change to the existing technical environment, or anytime changes are made to technologies that could feasibly impact sensitive data.

Vendor Name:	ACME, Inc
Vendor Representative:	XYZ Software Application
Completed By:	John Smith, Supply Chain (Org Name)
Vendor Name/Title:	Sally Franks, CIO ACME Inc.
Date of Assessment":	XX/XX/XXXX (insert date here)

5. The Interviewer shall ask each of the questions on the sheet, indicating the vendor's answers to each:

Choices for answers to questions:

N/A:	Not Applicable
NONE:	Not provided, not required, does not require input
DEFINED:	Defined and provided in the comments section
High:	Indicates the highest ranking as defined for each of the boxes
Medium:	Indicates median ranking as defined for each of the boxes
Low:	Indicates the lowest ranking as defined for each of the boxes

6. Each section is designed to drive down to the final Residual or Remaining Risk (R2) for this technical change.

Box 1 Consequence Statement: Identify the Consequence of a compromise statement in the comments Choices: N/A, NONE, DEFINED.

Box 2 Vendor Data Privacy Known Risk Exposure: Determine the relative risk to data based on the consequence statement provided (see Data Classification Standard Worksheet). Identify specific risks related to the consequences in the Comments section. Choices: High, Medium, Low as defined.

Box 3 Cyber or Privacy Controls incorporated: Identify and define controls used to mitigate risks as identified in the consequence statement. Identify specific controls in the Comments section. Choices: High, Medium, Low as defined.

Box 4 Residual or Remaining Risk (R1) after Controls are implemented: After applying controls identified in question 3 above, what risks remain or are introduced that could impact sensitive data. NOTE: This question should measure BOTH the likelihood of occurrence, as well as the impact should it occur. Choices: High, Medium, Low as defined.

Box 5 Additional Actions or Controls: Process changes, personnel oversight, compensatory controls, technologies to be implemented, or additional steps to be taken to ensure data is adequately protected against cyber compromise. List each control in the comments section. Choices: High, Medium, Low as defined.

Box 6 Residual or Remaining Risk (R2) after Additional Actions/Controls are implemented: After applying controls identified in question 3 above, what risks remain or are introduced that could impact sensitive data. NOTE This question should measure BOTH, the likelihood of occurrence, as well as the impact should it occur. Choices: High, Medium, Low as defined.

Box 7: Outcomes: Determine what, if any, remaining approvals for this change are required based on the R2 Ranking. Choices: High, Medium, Low as defined.