Baldwin Wallace University Information Technology Guideline

Issued by:	**Information Technology**
Title:	**Quick Reference Guide for Vendor Evaluation**
Number:	**ITG-BW-16-02**
Publish date:	**July 17, 2019**

A. Quick Reference Guide

Vendor Assessment
Quick Reference.xlsx

Baldwin Wallace University Vendor Risk Assessment Guide					
Area	**High Service Risk**	**Medium Service Risk**	**Low Service Risk**	**Very Low Service Risk**	**Implementation**
All Vendors	Business owner must insure the a Cyber Risk Assessment has been completed by a qualified person and risks identified are properly managed based on the resulting score and the guidance given in the risk mitigation section of this guide. All contracts must include the relevant sections of the IT Security Exhibit.				* Complete the initial 10 question cyber risk assessment spreadsheet as found in ITS-BW-16-02 Vendor Risk Assessment. * The IT Security Exhibit for contracts can be found in ITS-BW-16-01 Information Security Exhibit.
Technology Vendors (e.g. Software and/or Cloud Services)	Business owner must insure the using the "Light Version" of the High Education Cloud Vendor Assessment Tool (HECVAT) is completed to fully define the vendor's risk to BW and identified risks are properly managed based on the resulting score.				* HECVAT is developed by Educause and REN-ISAC and can be found at https://www.ren-isac.net/public-resources/hecvat.html.
Solutions requiring the processing of PII (Personally Identifiable Information)	Business owner must insure the DPIA (Data Privacy Impact Analysis) is completed and by a qualified person risks identified are properly managed based on the resulting score.				* Complete the DPIA spreadsheet as found in ITS-BW-16-02 Vendor Risk Assessment.
Risk Mitigation	Require Vendor to complete the "Light Version" of the High Education Cloud Vendor Assessment Tool (HECVAT) to fully define the vendor's risk to BW and identified risks are properly mitigated based on the resulting score. Request & review vendors' information security certifications, Information Security Policy, audit reports (e.g. SOC2), and vulnerability/penetration test results. Conduct data breach search.	Require Vendor to complete the "Light Version" of the High Education Cloud Vendor Assessment Tool (HECVAT) to fully define the vendor's risk to BW and identified risks are properly mitigated based on the resulting score. OPTIONAL: Request and review vendor's Information Security certifications and Information Security Policy. OPTIONAL: Conduct data breach search.	The completed Cyber Risk Assessment is sufficient provided any areas of medium or high risk include comments that mitigate interviewer concerns. Interviewer may, at their discretion, contact Information Security with any concerns that need clarification or further guidance.	No further due diligence is required.	* HECVAT is developed by Educause and REN-ISAC and can be found at https://www.ren-isac.net/public-resources/hecvat.html. * Suggested breach and vendor evaluation tools can be found in ITG-BW-16-02 Vendor Evaluation Research Tools. * If additional assistance is required contact the CIO or CISO.
Contract Approval Requirements	* President of University * CIO * Requesting Department Head	* CIO * Requesting Department Head	* Requesting Department Head	* Requesting Department Head	N/A