IT Risk Management Vendor Risk Assessment Procedure

Effective Date:
January 16, 2025

Category:
Security

Scheduled Review:
January 2, 2027

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Document Control

This procedure replaces, in its entirety, IT Risk Management Vendor Risk Assessment Procedure, dated January 2, 2025.

3. Purpose

This document establishes the requirements for IT Vendor Risk Assessment submission and procedure for review completion.

4. Procedure

Approved Submitter should submit a request to RA-OAITVENDORRA@pa.gov with as much of the information below that is available.

- Vendor name and overview of services to be provided, the business objectives and/or the business justification.
- Is this service deemed Critical for business operations?
- What is the classification of the Commonwealth data involved
- Will the data be processed, accessed, used, stored, transmitted, all, not sure. If yes, which actions?
- What is the business impact if a Data Breach occurred?
- What compliance requirements must you meet? None, CJIS, CHRIA, PHI/HIPAA, PII, IRS Pub 1075/SSA, Other? If Other, please provide requirement.
- Will this vendor provide network, infrastructure, PaaS or SaaS services?
- Provide a copy of the vendors SOC 2 Type II, ISO 27001 certification, SIG and/or other

relevant security documentation.

- Provide vendor StateRAMP and/or FedRAMP certificates
- Provide vendor Information Security Policy
- Provide vendor Pen Test Summary Report
- Provide any other relevant information pertaining to the vendor's Security & Compliance programs that would be helpful in evaluating how they manage their security
- Has the supplier provided an Accessibility Conformance Report (ACR) or a Voluntary Product Accessibility Template (VPAT)? If yes, please provide a copy. If the supplier doesn't have an ACR/VPAT for this product, email RA-OAAccessibility@pa.gov for other assessment options.
- Is there an SSLRA in place? If not, please reach out to RA-GSITSOFTWARE@pa.gov to start the process.
- Has a Data Retention Questionnaire been completed? If yes, please provide a copy. If no, please follow the guidance given in *The Records Management Policy* to complete a *System Design Review Form*.

A member of the GRC team will reach out if additional information is required or there are follow up questions.

Once the GRC team has completed the review, a documented approval/summary of findings will be shared with the approved submitter. If additional action is needed, that will be communicated within the review.

5. Contact

Questions or comments may be directed via email to OA IT Central.

6. Revision History

This chart contains a history of this publication's revisions.

Version	Date	Purpose of Revision
Original	1/6/25	Base Document
Revision	1/16/25	• Update accessibility requirement • Replaced old policy number with policy title • Added Document Control section