TPRM Risk Assessment: Evidence Request List

A key component to the Third Party Risk Management (TPRM) assessment process is the evidence review. The purpose is to verify the assessment responses provided and validate that security controls are operating as intended. Evidence requests may include some or all of the following:

Vendor Risk Assessment (VRA)

1. Network Architecture Diagram
2. Data Flow Diagram *(if exchanging data)*
3. Independent industry certification/audit report/risk assessment *(examples include: SOC2 T2, HITRUST, ISO 27001, PCI DSS)*
4. Information Security Policy
5. Penetration Test *(Executive Summary & status of findings from within the last 12 months, including any in scope applications)*
6. Monthly execution of Network and Application Vulnerability scans
7. Remediation SLAs for identified vulnerabilities *(remediation timeline for Critical/High/Medium/Low)*
8. Patch Management Policy & Schedule
9. Multi-Factor Authentication (MFA) evidence
10. Intrusion Detection/Prevention System (IDS/IPS) evidence
11. Encryption of data at rest & transit
12. Data Loss Prevention (DLP) evidence/Email Security/ Data movement restriction
13. Data Protection & Retention Policy/Procedures
14. Data Destruction Policy/Procedures
15. Mobile Device Management (MDM) solution evidence *(if applicable)*
16. Secure Software Development Lifecycle (sSDLC) Policy/Procedures
17. Secure Code Review (SAST/DAST scans can also be included
18. Open Source Security Policy/Procedures *(if applicable)*
19. Incident Response Policy/Procedures and evidence of recent exercise/test *(within the last 12 months)*
20. Third Party Risk Management Policy/Procedures

Note: TPRM will accept a SOC2 Type2 Certification and/or SIQ Questionnaire in lieu of our customized assessment, but may require additional items that cannot be validated.