TPRM Vendor 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 see that security controls are operating as intended. Evidence can be submitted as part of the assessment or reviewed over Zoom.

Evidence requests may include some or all of the following:

Vendor Security Assessment (VSA)

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 from within the last 12 months, including any in scope applications)*
6. Network and Application Vulnerability scans *(Executive Summary from within the last month, including mobile devices if applicable)*
7. Remediation SLAs for identified vulnerabilities *(timeline for Critical/High/Medium/Low)*
8. Patch Management Policy & Schedule
9. Multi-Factor Authentication (MFA) evidence *(including mobile devices if applicable)*
10. Intrusion Detection/Prevention System (IDS/IPS) evidence
11. Encryption of data at rest
12. Encryption of data in transit
13. Data Loss Prevention (DLP) evidence
14. Data Protection & Retention Policy/Procedures
15. Data Destruction Policy/Procedures
16. Mobile Device Management (MDM) solution evidence *(if applicable)*
17. Mobile Application Password Requirements *(if applicable)*
18. Cloud Security Shared Responsibility Matrix *(if applicable)*
19. Container Security Policy *(if applicable)*
20. Secure Software Development Lifecycle (sSDLC) Policy/Procedures
21. Secure Code Review (SAST/DAST scans)
22. Open Source Security Policy/Procedures
23. Open Source Component List *(if applicable)*
24. Incident Response Policy/Procedures and evidence of recent exercise/test *(within the last 12 months)*
25. Third Party Risk Management Policy/Procedures
26. List of third parties with access to Zoom data *(if applicable)*