Information Security Plan

2022 Security Plan Template - Vulnerability Report Questionnaire

Updated March 2022

2022 Vulnerability Report Questionnaire

VR-001. What systems or applications does the agency perform vulnerability assessments and scans on prior to Production implementation? Check all that apply.

- IoT (Network Connected) Devices
- Mobile Applications
- Network Devices
- Servers
- Web Applications
- Workstations

VR-002. How often does the agency conduct web application vulnerability scanning?

- Never
- Prior to implementation only
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc
- Continuously

VR-003. How often does the agency conduct network vulnerability scanning?

- Never
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc
- Continuously

VR-004. How often does the agency perform network penetration testing?

- Never
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-005. How often does the agency perform web application penetration testing?

- Never
- Prior to Implementation
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-006. How often does the agency perform .mobile application penetration testing?

- Never
- Prior to Implementation Only
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc
- N/A, we do not have mobile applications

VR-007. How often does the agency perform physical/environmental penetration testing?

- Never
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-008. How often does the agency inventory devices connected to the network?

- Never
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-009. How often does the agency review data/information flow designs to ensure that controls are still effective and that vulnerabilities are identified and addressed?

- Never
- Prior to Implementation Only
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-Hoc

VR-010. How often does the agency perform wireless vulnerability assessments?

- Never
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-011. How often are independent third-party security assessments conducted?

- Never
- Prior to Implementation Only
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-Hoc

VR-012. How often are security self-assessments conducted?

- Never
- Prior to Implementation Only
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-Hoc

VR-013. What is the percentage of agency coverage in these assessments?

- 0 to 10%
- 10 to 25%
- 25 to 50%
- 50 to 75%
- 75 to 90%
- 90 to 100%

VR-014. How often does the agency conduct social engineering (phishing, etc.) simulation testing or assessments?

- Never
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-015. How often does the agency patch applications?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-016. How often are the agency's servers patched?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-017. How often does the agency patch network equipment?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-018. How often does the agency patch workstations?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-019. How often does the agency patch infrastructure components (firmware, drivers, etc.)?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-020. What is the percentage of agency compliance with application patching?

- 0 to 10%
- 10 to 25%
- 25 to 50%
- 50 to 75%
- 75 to 90%
- 90 to 100%

VR-021. What is the percentage of agency compliance with server patching?

- 0 to 10%
- 10 to 25%
- 25 to 50%
- 50 to 75%
- 75 to 90%
- 90 to 100%

VR-022. What is the percentage of agency compliance with network equipment patching?

- 0 to 10%
- 10 to 25%
- 25 to 50%
- 50 to 75%
- 75 to 90%
- 90 to 100%

VR-023. How often does the agency conduct audits of unnecessary or unapproved software and/or services?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-024. On average, approximately what percentage of vulnerabilities identified during assessment are remediated between assessment periods?

- 0 to 10%
- 10 to 25%
- 25 to 50%
- 50 to 75%
- 75 to 90%
- 90 to 100%

VR-025. Does the agency document vulnerability/patching exceptions?

- Yes
- No
- Sometimes

VR-025.a. (If Yes) How often are exceptions re-visited?

- Never
- Weekly
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-hoc

VR-026. Does the agency have any known production system vulnerabilities that cannot be patched or remediated?

- Yes
- No

VR-026.a. (If Yes) Select the reason(s) for operating with identified vulnerabilities.

- No patch exists
- Patching would disrupt operations/availability
- Risk acceptance, vulnerabilities deemed insignificant
- Risk acceptance, mitigating controls deemed sufficient
- Risk acceptance, remediation efforts targeted for completion within the next Fiscal Year
- Other

VR-026.b. Select the challenge(s) preventing remediation of identified vulnerabilities.

- Lack of funding/resources
- Lack of knowledge/skills to remediate
- Other

Additional Comments:

Optional: provide any additional comments regarding the vulnerability report or your organization's vulnerability management practices.