Frameworks and Assessment Tools

Below is a list of more cyber security frameworks and tools assessment information that can help you establish a better security standard for your organization. These both go hand in hand and can be applied in either order depending on where you are in your cyber security journey. Assessing your network using some various tools will allow you to choose one or more frameworks that can assist you and strengthen your cyber security posture. Also, after implementing these frameworks you can then again use the tools to test and evaluate implementation and possible changes and growth that needs to be addressed.

1. Frameworks - Cybersecurity defense can be neither an afterthought nor a half measure. Adequate protection against intrusions must be conducted within established frameworks that are scalable and measurable. The following resources can help you choose the right framework and testing tools for your organization.

   a. Security Frameworks and Implementation Guidance- These are some of the current frameworks and guidance for implementing frameworks. Developing frameworks will allow organizations to follow an organized path toward hardening their systems and increasing overall security and recovery.

   i. CIS- https://www.cisecurity.org/controls/

   ii. FCC Security Planner- https://www.fcc.gov/cyberplanner

   iii. ISO 27001- https://www.iso.org/isoiec-27001-information-security.html

   iv. NIST-800-53-https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

   v. NIST CI Resources- https://www.nist.gov/cyberframework/critical-infrastructure-resources

   vi. COBIT-5 https://www.isaca.org/

   vii. DOE Framework Implementation guide - http://energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance

2. Self-Assessment tools - Below is a list of tools that are available to organizations that provide testing and assessments of your current security posture.

   a. High-level assessments and starting points.

   i. Resources for Small and Medium business- This includes road maps and starting points for your business. - Cyber Security- Small Medium Business- https://www.us-cert.gov/resources/smb

ii. CISA Tools - https://www.cisa.gov/cybersecurity-assessments

1. The Cyber Resilience Review (CRR)
2. The Cyber Infrastructure Survey
3. External Dependencies Management (EDM)

iii. ISO 27001 checklist - https://www.dekra.us/media/dekra-cert-checklist-iso-27001-a4-en-v1.pdf?gclid=Cj0KCQiAs67yBRC7ARIsAF49CdXS5puBpZaKlpYXWrM9kQIWfEidxzSD0u5ne_0YuNtta66bj6kfLMsaAhp3EALw_wcB

b. Tools that will help mature a new cybersecurity program. (MID-Level)

i. CISA Tools - https://www.us-cert.gov/resources/ncats

1. The Phishing Campaign Assessment (PCA)
2. CISA offers vulnerability scanning (formerly known as Cyber Hygiene scanning)

ii. NIST Framework Assessment Information - https://www.nist.gov/cyberframework/assessment-auditing-resources

c. On-Site Assessment Tools that will help mature and established cybersecurity program. (Low-Level/Mature)

i. CISA Tools - https://www.cisa.gov/cybersecurity-assessments

1. A Risk and Vulnerability Assessment (RVA) - https://www.us-cert.gov/resources/ncats
2. Remote Penetration Testing (RPT)
3. The Validated Architecture Design Review (VADR)- https://www.us-cert.gov/resources/ncats
4. The Cyber Security Evaluation Tool (CSET®)