NIST Cybersecurity Framework 1.1

The NIST Cybersecurity Framework is a popular framework used to improve an organisations cybersecurity standards and manage the risk of cyber threats. This framework is a bit of an honourable mention because of its popularity and detail.

The framework provides guidelines on security controls & benchmarks for success for organisations from critical infrastructure (power plants, etc.) all through to commercial. There is a limited section on a standard guideline for the methodology a penetration tester should take.

Advantages	Disadvantages
The NIST Framework is estimated to be used by 50% of American organisations by 2020.	NIST has many iterations of frameworks, so it may be difficult to decide which one applies to your organisation.
The framework is extremely detailed in setting standards to help organisations mitigate the threat posed by cyber threats.	The NIST framework has weak auditing policies, making it difficult to determine how a breach occurred.
The framework is very frequently updated.	The framework does not consider cloud computing, which is quickly becoming increasingly popular for organisations.
NIST provides accreditation for organisations that use this framework.	*Intentionally left blank.*
The NIST framework is designed to be implemented alongside other frameworks.	*Intentionally left blank.*

Revision #1
Created 2023-02-11 20:37:38 UTC by Fettlaus
Updated 2023-02-11 20:37:58 UTC by Fettlaus