**What is NIST?**

NIST: It’s stand for the National Institute of Standards and Technology. NIST different from other bodies that issue guidelines, such as the ISO, which focuses on risk control. NIST is more focused on data security than procurement.

**What Does NIST Do**

NIST outlines how data should be protected. This includes providing standards that govern the security measures needed to protect data, as well as shore up the systems and tools used to ensure data safety.

**NIST Compliance Benefits**

NIST compliance comes with several benefits to both an organization and the people it serves.

First, it ensures a more secure infrastructure for the organization. With a strengthened infrastructure, it is more difficult for cyber threats to penetrate and disturb the day-to-day operations of various teams and individuals.

**Who Should Comply?**

NIST Any company that does business with the United States government should comply with NIST. This includes agencies within the U.S. government, as well as businesses and individuals that the government may hire to perform work on projects.

**NIST Cybersecurity Framework**

The NIST Cybersecurity Framework outlines all the ways data needs to be protected to create a more secure organization

It is composed of five steps:

**Identify**: In this step, the data and systems that need to be protected are identified. This often involves those that fall under the jurisdiction of specific legislation designed to protect consumers, patients, or sensitive information.

**Protect**: In the protection phase, the team puts security measures into place to safeguard the data. These will often involve specific tools, hardware, and software designed to address common security concerns. However, it may also involve getting stakeholders and employees on board so everyone can work together to guard sensitive data and systems.

**Detect**: In the detection step, tools and policies are designed to discover an incident when it happens. This requires enhanced visibility into the various systems, networks, and devices used by the organization. It may also include applications that manage data or interface with it in the course of regular business.

**Respond**: The response phase requires a company to devise a plan for responding to a threat. The plan will include the different methods used to mitigate the threat, as well as which tools will be used. An organization’s response mechanism may include intentional redundancies designed to approach a threat from multiple angles, such as redundant firewalls or antivirus software.

**Recover**: In the event an attack penetrates the network, the process outlined by NIST also includes ways of helping an organization recover as quickly as possible. This may include recovering data from backups, regaining control of workstations, or spinning up parallel devices. Recovery may also include resiliency measures and tools that ensure the company has as little downtime as possible.

# Top 10 Security Controls in NIST SP 800-53

The top 10 security controls in NIST SP 800-53 include:

**Access control**: Ensures only authorized users have access privileges.

**Audit and accountability**: Involves a system of checks and balances to ensure proper protection.

**Awareness and training**: Ensures team members are given the pertinent security controls training, including how these controls protect their systems.

**Configuration management**: Ensures all configurations address the latest needs of the system without compromising security.

**Contingency planning**: Involves creating a plan that provides different options in case your security controls do not perform as expected.

**Identification and authentication**: Focuses on ensuring users and devices have valid identification and the rights they need to access systems and data.

**Incident response**: Orchestrates the steps and tools used when there is a breach.

**Maintenance**: Necessary for keeping the system up-to-date and functioning as it should.

**Media protection**: Involves protecting the physical media used to store data, such as hard drives and servers.

**Personnel security**: Ensures people that manage sensitive systems and data are protected from cybercriminals who may target them.