VESTIGE
Digital Investigations

NIST Framework

An Overview

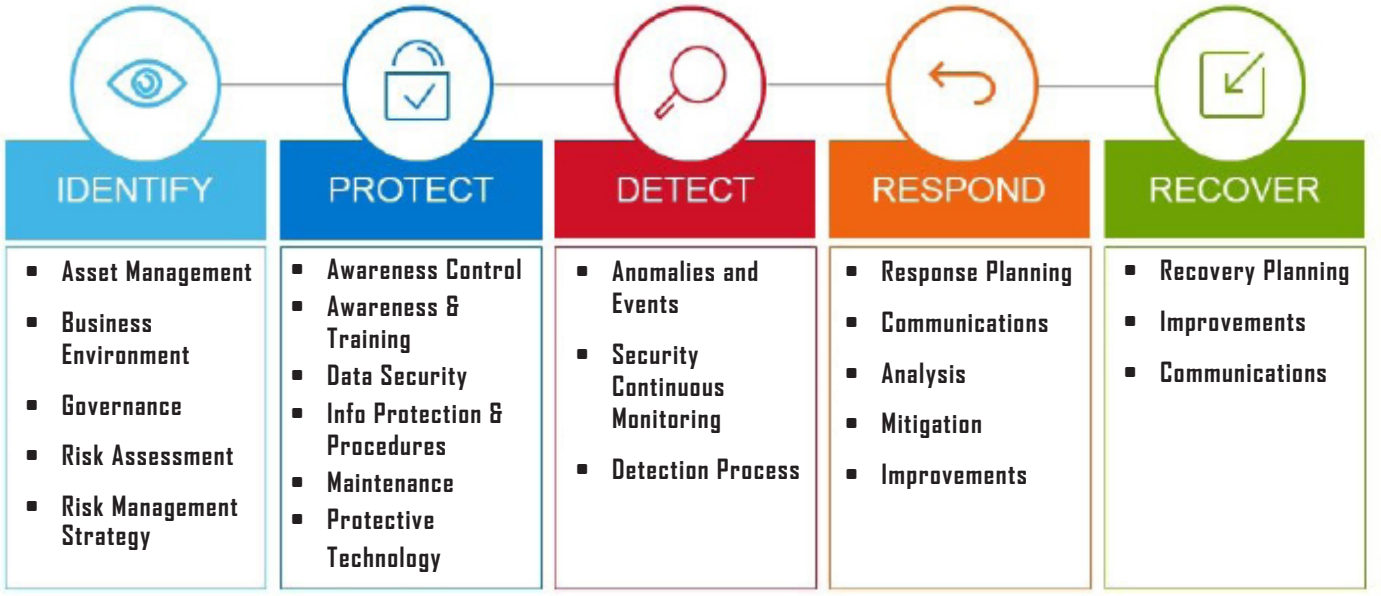
The NIST CyberSecurity Framework was developed by the U.S. Department of Commerce's National Institute of Standards & Technology to help organizations to better understand and improve their management of cybersecurity risk.

This leading, voluntary, public-private framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The CyberSecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST is not the only framework from a cybersecurity standpoint, however, at Vestige we prefer it because it has a more holistic approach to securing your environment from a security standpoint.

It focuses on more than just prevention. While on the surface an organization's goal should be to prevent cyber attack, the reality is we can never prevent everything. Therefore, focusing on other aspects becomes equally important.

NIST is arranged in five domains



It is not equally balanced across all five, but there is representation in each of these areas.

The issues organizations often have is that they spend all of their resources on the prevention and become dismayed when they still fall victim to a cyber attack. Having exhausted their resources, there is nothing left to detect a cyber attack in a timely fashion, let alone adequately respond when an incident or breach arises.

Organization's that adopt the NIST CyberSecurity Frameworkand meet its 98 control objectives spread amongst the five domains are not only well protected from a preventive standpoint, but have the tools, processes and resources to detect and respond in a manner that is more expeditious and cost effective.

Contact Vestige today to discuss your CyberSecurity needs.

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com