Spirent Risk Assessment Solutions

NIST Cybersecurity Framework

Spirent Risk Assessment Solutions empower public and private organizations that manage critical infrastructures to take an active role in assessing and managing their infrastructure security risks in accordance with NISTs Cybersecurity Framework.

Critical Infrastructures Supply Chain

The National Institute of Standards and Technology (NIST) Cybersecurity Framework impacts all public and private organizations that manage critical infrastructures in the United States. The Framework encourages network equipment manufacturers, enterprises, service providers, government agencies and federal integrators to take an active role in risk management with the goal of improving the security posture of critical infrastructures.

Since the Department of Homeland Security (DHS) classifies critical infrastructure as companies in banking & finance, communications, critical manufacturing, defense industrial base, energy, emergency services, food & agriculture, healthcare, IT, utilities, and transportation—the framework impacts most industry sectors.

Although compliance with the Framework is optional, legal and accounting firms expect it to be widely adopted by the industry. Executives do not want to be in the position of going to court or being audited and found not in compliance with the framework.

In order to reduce and mitigate the risks associated with their critical infrastructures, organizations need to understand the Framework and assess their critical infrastructures and supply chain. Supply chains start with the Network Equipment Manufacturers (NEMs) who develop and deliver the network and security devices that manage critical infrastructures. Service providers, enterprises, federal integrators and government agencies need to feel confident that they understand the risks associated with deploying critical infrastructure components that are interconnected and protected by network switches, routers, load balancers, firewalls, Intrusion Prevention Systems and other security tools. The resiliency, stability and vulnerability of critical infrastructure components need to be assessed and tested.

Identify, Protect, Detect, Respond, and Recover

The Framework approach to risk assessment is based on five core functions that organize cybersecurity activities at their highest level.

The five functions are: **Identify, Protect, Detect Respond and Recover**. The functions represent the Framework Core. Each function is divided into categories, subcategories and references. The Framework categories and subcategories are groups of activities for a specific function that supports specific outcomes. References are lists of standards, guidelines and practices that are common across critical infrastructure sectors and help implement a subcategory activity.

Framework Identify Function

This function includes categories and activities related to Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy. The table below details the activities and identifiers for the Identify Function.

Core Function	Function Identifier	Category Identifier	Category
Identify	ID	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management

Spirent Risk Assessment solutions support the *Framework Identity Function* allowing network equipment manufacturers, service providers, enterprises, federal integrators and government agencies to:

- Assess physical devices and systems
- Assess software platforms and applications
- Assess external information systems
- Assess resiliency requirements for critical services
- Assess information security policy and security roles
- Assess vulnerabilities and threats
- Analyze potential impact of vulnerabilities

Framework Protect Function

This function includes categories and activities related to Access Control, Awareness & Training, Data Security, Information Protection Processes & Procedures, Maintenance and Protective Technology. The table below details the activities and identifiers for the Protect Function.

Core Function	Function Identifier	Category Identifier	Category
Protect	PR	AC	Access Control
		AT	Awareness & Training
		DS	Data Security
		IP	Information Protection Processes & Procedures
		MA	Maintenance
		PT	Protective Technology

Spirent Risk Assessment solutions support the *Framework Protect Function* allowing network equipment manufacturers, service providers, enterprises, federal integrators and government agencies to:

- Assess user identities and credentials
- Assess remote access elements
- Assess access permissions
- Assess network integrity
- Assess data-at-rest security
- Assess data-in-motion security
- Assess capacity and availability of networks and resources
- Assess data leaks
- Assess communications and control networks

Framework Detect Function

This function includes categories and activities related to Anomalies and Events, Security Continuous Monitoring, and Detection Processes. The table below details the activities and identifiers for the Detect Function.

Core Function	Function Identifier	Category Identifier	Category
Detect	DE	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes

Spirent Risk Assessment solutions support the *Framework Detect Function* allowing network equipment manufacturers, service providers, enterprises, federal integrators and government agencies to:

- Assess that events are detected and analyzed to understand attack and target methods
- Assess incident alert thresholds
- Assess event monitoring devices
- Assess that malicious code is detected
- Assess that unauthorized mobile code is detected
- Assess vulnerability scans
- Assess detection processes

Framework Respond Function

This function includes categories and activities related to Response Planning, Communications, Analysis, Mitigation and Improvements. The table below details the activities and identifiers for the Respond Function.

Core Function	Function Identifier	Category Identifier	Category
Respond	RS	RP	Response Planning
		CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements

Spirent Risk Assessment solutions support the *Framework Respond Function* allowing network equipment manufacturers, service providers, enterprises, federal integrators and government agencies to:

- Assess that notifications from detection systems are investigated
- Assess that incidents are categorized consistent with response plans
- Assess that incidents are contained
- Assess that newly identified vulnerabilities are mitigated or documented as accepted risks

Framework Recover Function

The Framework Recover Function includes categories and activities related to Recovery Planning, Improvements and Communications. The table to your right details the activities and identifiers for the Recover Function.

Core Function	Function Identifier	Category Identifier	Category
Recover	RC	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Spirent Risk Assessment Solutions

Our next-generation test tools empower public and private organizations that manage critical infrastructures to take an active role in assessing and managing their infrastructure security risks. Every day, the critical infrastructure supply chain; network equipment manufacturers, enterprises, service providers, government agencies and federal integrators use our security and application test tools to assess the vulnerabilities of their infrastructure.

With the industries most intuitive test methodology, thousands of security exploits and applications, our next-generation test tools allow our customers to leverage the Framework's core functions: Identify, protect, detect, respond and recover to ensure the resiliency of their critical infrastructure.

Our next-generation test solutions validate that critical infrastructures and their components perform as intended and deliver the protection you expect, using the most intuitive and user friendly interface and test methodologies.

Real Apps such as ...

Business Apps
- MS Active Directory
- MS SharePoint
- Oracle
- WebEx

Communication Apps
- AIM
- Google Talk
- ICQ
- Jabber
- Rediff Bol
- Yahoo! Messenger

Games/Facebook Apps
- Armagetron
- Battlefield 1942
- FrontierVille
- World of Warcraft
- Zynga Poker

Peer-to-Peer (P2P
- BitTorrent
- Frostwire
- Gnucleus
- Gnutella

Social Networking
- Delicious
- Facebook
- LinkedIn
- Twitter

Streaming
- BBC iPlayer
- Hulu
- Metacafe
- Netflix
- Silverlight
- Skype

Known Security Attacks
- Adobe
- Apple
- Cisco
- Microsoft
- Oracle
- VMWare

Our next-generation test tools are present in almost every country and every lab providing network equipment manufacturers, service providers, enterprises, government agencies, and federal integrators with the:

- Ability to test critical infrastructures with realistic traffic that simulates real world applications and security attacks—with more than 3,000 applications including mobile apps
- Ability to detect, isolate and prevent—thousands of known and unknown security attacks and vulnerabilities including zero-day attacks
- Ability to operate under attacks, anomalies, variable loads and throughput conditions—keeping performance high while stopping attacks is critical

- Avalanche is the leading application and security test tool providing thousands of applications, security attacks, fuzzing attacks and performance testing, enabling users to test network security systems at line rate speeds while simulating daily business traffic to understand the impact of network faults and attacks on critical infrastructures.
- Spirent Studio Security is a testing solution purpose-built for validating security capabilities via fuzz testing, DDOS replication, vulnerability assessment and security capability verification.

Ordering Information

Due to the wide range of available system configurations, please contact your regional Spirent sales representative for detailed ordering information.

Spirent Global Services

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements. For more information, visit the Global Services website at www.spirent.com/gs or contact your Spirent sales representative.

AMERICAS 1-800-SPIRENT | +1-818-676-2683 | sales@spirent.com
EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 | emeainfo@spirent.com
ASIA AND THE PACIFIC +86-10-8518-2539 | salesasia@spirent.com

TESTED WITH SPIRENT