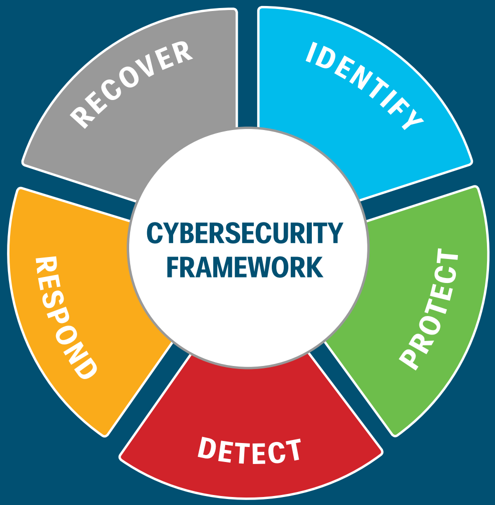
At-A-Glance
Cisco Public

Cisco and the NIST Cybersecurity Framework

From the largest federal agency to the smallest school district, every organization today is faced with managing cybersecurity risks effectively. How can you implement innovative, best practices approach to cybersecurity?

With so many security frameworks, it can be difficult to know where to start. For this reason, the National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF).

It enables organizations of all sizes to discuss, address, and manage cybersecurity risk. And it does this without reinventing the cyber wheel, referencing existing best practices through its functions: Identify, Protect, Detect, Respond, and Recover.



How Cisco helps you comply with NIST CSF

Cisco Security can help your organization adopt the Framework and use it to effectively manage cybersecurity risk. We help with all areas of the Framework, including the non-technical controls.

NIST for Security Risk Management

The Cybersecurity Framework has five functions to help organizations better manage security risk:

1. Identify develops an understanding of risk to systems, people, assets, data, and capabilities.
2. Protect ensures critical infrastructure services and contains the impact of cybersecurity events.
3. Detect identifies the occurrence of cybersecurity events.
4. Respond includes appropriate actions to take regarding a detected cybersecurity incident.
5. Recover identifies activities for resilience and to restore any capabilities/ services that were impaired due to a cybersecurity incident.

The breadth of our security and networking portfolio can help with important technical controls related to having the appropriate security technologies in place for aspects like access controls, threat detection or mitigation.

However, many of the CSF controls in the five functions are non-technical, related to training and preparation for staff along

with having the appropriate processes in place. Cisco Security will work with you to develop and implement the recommend training and processes to not only comply with CSF controls, but as importantly, make your security posture more effective.

The best source of Framework information is NIST itself. Materials are freely available from www.nist.gov/cyberframework.

Get Started

Get started with a free trial of one of our security solutions to accelerate your cyber risk management.

Go to Free Trial

Cisco Security and the NIST Cybersecurity Framework

		Technical Controls	Non-technical Controls
		Cisco	Cisco Services or Technology Partners
ID	Asset Management	✓	
	Business Environment		✓
	Governance		✓
	Risk Assessment	✓	✓
	Risk Management		✓
	Supply Chain	✓	✓
PR	Access Control	✓	✓
	Awareness Training		✓
	Data Security	✓	
	Info Protection Process		✓
	Maintenance		✓
	Protective Technology	✓	
DE	Anomalies and Events	✓	
	Continuous Monitoring	✓	
	Detection Process		✓
RS	Response Planning		✓
	Communications		✓
	Analysis	✓	
	Mitigation	✓	
	Improvements		✓
RC	Recovery Planning		✓
	Improvements		✓
	Communications		✓