COMPLIANCE GUIDE

How Zero Networks Helps with NIST CSF Regulation Requirements

The National Institute of Standards and Technology (NIST) is a U.S. government agency that develops widely recognized cybersecurity standards and guidelines. NIST's frameworks, such as the NIST Cybersecurity Framework (CSF), help organizations strengthen their security, manage cyber risks, and demonstrate compliance. Following and adhering to NIST is important because it provides a proven, structured approach to protecting sensitive data and critical systems—making it a benchmark for both public and private sector cybersecurity programs.

Modern microsegmentation solutions like Zero Networks directly align with the NIST CSF by automating and enforcing granular access controls, isolating critical assets, providing continuous monitoring, and supporting rapid incident response and containment. Plus, Zero faclitates compliance documentation and audit readiness – all whle bringing a Tier 4 implementation to the industry. This ensures a robust and comprehensive approach to cybersecurity.

Zero Networks enhances NIST CSF 2.0 Functional Categories through automated Zero Trust controls and adaptive microsegmentation, aligning with Tier 4 (Adaptive) implementation maturity.

Below is a breakdown of key NIST CSF Functions and Categories – and how Zero helps organizations stay in line with NIST.

Function: Govern (GV)

Requirement	Description	How Zero Helps
GV.SC: Cybersecurity Supply Chain Risk Management	Cyber supply chain risk management processes must be identified, established, managed, monitored, and improved by organizational stakeholders.	Zero automates third-party access restrictions and monitors external service usage through dynamic microsegmentation.
GV.OV: Oversight	Results of organization-wide cybersecurity risk management activities and performance should be used to inform, improve, and adjust the risk management strategy.	By providing real-time compliance dashboards and demonstrable evidence for policy enforcement audits, Zero supports actionable oversight.

Function: Identify (ID)

Requirement	Description	How Zero Helps
ID.AM-1: Asset Management Identify physical and software assets within the organization to establish the context for cybersecurity activities	Security teams must understand their organization's IT infrastructure, including hardware, software, and data assets, to manage cybersecurity risks effectively.	Zero provides visibility into all network assets, including devices, applications, and users. This real-time inventory helps organizations understand their attack surface and identify critical assets that require enhanced protection.
ID.AM (generalized)		Maps authorized network communications through automated baselines of IT, OT, and Cloud environments, including applications and users.
ID.RA: Risk Assessment	The cybersecurity risk to the organization, assets, and individuals is understood by the organization.	Continuously evaluating exposure risks through lateral movement prevention controls, Zero aligns with AbuseIPDB for automatic protection against high-risk sources.

Function: Protect (PR)

Requirement	Description	How Zero Helps
PR.AC-4: Access Control Manage access authorizations and authentication to assets and associated facilities	Organizations should implement robust access control measures to ensure that only authorized users and devices can access sensitive systems and data.	Zero implements granular network and identity-based segmentation with just-in-time multi-factor authentication (MFA) applied at the network layer, ensuring only authorized users and devices can access specific network segments or assets. This directly addresses the need for least privilege access and secure authentication
PR.DS-1: Data Security Data-at-rest is protected	Ensure that data stored within the organization is protected through encryption, access controls, and other security measures.	Zero Networks Segment creates micro-perimeters around workloads, applications, and data while enabling granular identity-based access controls. Zero automatically learns network behavior and generates segmentation policies, isolating critical assets and blocking unauthorized lateral movement, thus reducing the risk of unauthorized access to sensitive data at rest.

Function: Detect (DE)

Requirement	Description	How Zero Helps
DE.CM-7: Anomalies and Events Anomalous activity is detected	Monitor systems and networks for unusual or suspicious activities that could indicate a security breach or compromise.	Zero provides detailed, real-time insights into and granular control over network traffic, asset communication, and identity activity. It can integrate with SIEM or other Security Monitoring tools to stream granular activity details (both network and identity), as well as platform audit trails, thus supporting organizations in their threat/anomaly detection and response initiatives.

Function: Respond (RS)

Requirement	Description	How Zero Helps
RS.MI-1: Incident Management Response plan is implemented during an incident	Execute the incident response plan to manage and contain the impact of security incidents.	Zero enables rapid threat response and containment by automatically enforcing segmentation and access policies across a network. Its automated microsegmentation solution blocks lateral movement and isolates compromised segments, supporting swift containment and minimizing the blast radius of an attack.

Function: Recover (RC)

Requirement	Description	How Zero Helps
RC.IM-2: Improvements Improvements are made to the incident response plan based on lessons learned	Improve incident response strategies and plans based on insights gained from past incidents.	Zero provides detailed telemetry and reports of network, asset, and identity activity during incidents, facilitating post-incident analysis. This information helps organizations refine their segmentation policies and incident response plans to prevent future breaches. Its microsegmentation capabilities quickly quarantine threats, minimizing damage and making recovery much easier than it could otherwise be.

Additional CSF Categories Addressed

Requirement	Description	How Zero Helps
PR.PT-1: Network Segmentation	Segment the network based on risk.	Zero Networks automates network and asset microsegmentation, by leveraging the native components of each available system to create logical micro perimeters with the goal of reducing the organization's overall attack surface and ensuring strict separation of duties, environments, and business areas to meet compliance requirements. These capabilities allow organizations to protect every asset and workload at scale and minimize or mitigate any possible lateral movement.
DE.CM-1: Monitoring	The network is monitored to detect potential cybersecurity events.	Zero Networks provides continuous monitoring of network traffic, asset, and identity activity (e.g., user or service accounts), enabling organizations to have a near real-time audit trail of any connection or logon activity, while improving threat/anomaly detection and containment, minimizing the likelihood of a potential security incident.

Modern microsegmentation solutions like Zero Networks directly align with the NIST CSF by automating and enforcing granular access controls, isolating critical assets, providing continuous monitoring, and supporting rapid incident response—all while facilitating compliance documentation and audit readiness. This ensures a robust and comprehensive approach to cybersecurity.

Catalyze compliance and protect your network.

Try Zero today

ZERO. Networks