



# **Comparison of Cybersecurity Security Controls – NIST Cybersecurity Framework vs. ETSI TR 103 305-1 V2.1.1**

# Cybersecurity Controls Comparison

## NIST Cybersecurity Framework vs. ETSI TR 103 305-1



Security Control	NIST Cybersecurity Framework	ETSI TR 103 305-1
Asset Management	√	
Business Environment	√	
Governance	√	
Risk Assessment	√	
Risk Management Strategy	√	
Supply Chain Risk Management	√	
Identity Management, Authentication and Access Control	√	√
Awareness and Training	√	√
Data Security	√	√
Information Protection Processes and Procedures	√	
Maintenance	√	
Protective Technology	√	
Anomalies and Events	√	√
Security Continuous Monitoring	√	√
Detection Processes	√	√
Analysis	√	√
Mitigation	√	√
Improvements	√	
Recovery Planning	√	√
Improvements	√	
Communications	√	
Inventory of Authorized and Unauthorized Devices		√
Inventory of Authorized and Unauthorized Software		√

# Cybersecurity Controls Comparison

## NIST Cybersecurity Framework vs. ETSI TR 103 305-1



Security Control	NIST Cybersecurity Framework	ETSI TR 103 305-1
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers		√
Controlled Use of Administrative Privileges		√
Maintenance, Monitoring, and Analysis of Audit Logs		√
Email and Web Browser Protections		√
Malware Defenses		√
Limitation and Control of Network Ports, Protocols, and Services		√
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		√
Boundary Defense		√
Controlled Access Based on the Need to Know		√
Wireless Access Control		√
Account Monitoring and Control		√
Application Software Security		√
Penetration Tests and Red Team Exercises		√