

BIITOPS AS AN ENABLER FOR NIST COMPLIANCE



The NIST (National Institute of Standards and Technology) Cybersecurity Framework provides organizations with a comprehensive foundation for managing and reducing cybersecurity risks. BiitOps' DataLake and functionality actively support several core areas of the NIST framework, making it a significant enabler for organizations seeking to achieve or maintain NIST compliance.



IDENTIFY (ID)

Asset Management (ID.AM)

BiitOps delivers comprehensive asset management support through:

- Automatic and continuous collection of asset information
- Centralized “Single Point of Trust” for all asset data
- Detailed overview of hardware, software, and configurations
- Precise asset tracking through dual timestamp technology
- Historical documentation of changes in the asset landscape

Business Environment (ID.BE)

- Provides management with data-driven insights into IT infrastructure status
- Enables strategic resource prioritization based on current data
- Supports understanding of IT landscape complexity

Risk Assessment (ID.RA)

- Identifies deviations from desired configurations through Desired State dashboards
- Provides continuously updated overview of security-critical configurations
- Tracks changes in system configurations that may affect security levels

PROTECT (PR)

Access Control (PR.AC)

- Tracks user rights and privileged accounts
- Documents group memberships and their changes over time
- Monitors local administrator rights

Data Security (PR.DS)

- End-to-end encryption of all collected data
- Encryption of BiitOps data directly on client/server
- Collected data remains encrypted during transmission and storage
- Decryption occurs only during API requests and exclusively in memory

Information Protection (PR.IP)

- Maintains complete history of configuration changes
- Enables audit of security policies and their implementation
- Supports change management through precise documentation

Phone: +45 7199 2645
sales@biitops.com
www.biitops.com



DETECT (DE)

Anomalies and Events (DE.AE)

- Identifies deviations from standard configurations
- Tracks unauthorized changes in system settings
- Documents timing of changes through dual timestamp technology

Security Continuous Monitoring (DE.CM)

- Continuous monitoring of system configurations
- Automatic verification of security settings
- Ongoing validation of compliance with security policies

RESPOND (RS)

Analysis (RS.AN)

- Provides rapid access to historical data during security incidents
- Enables precise mapping of changes over time
- Supports root cause analysis through detailed change history

Mitigation (RS.MI)

- Quickly identifies deviating systems requiring action
- Supports effective prioritization of mitigating actions
- Validates the effect of implemented security measures

RECOVER (RC)

Recovery Planning (RC.RP)

- Documents system configurations for rapid restoration
- Supports verification of restored systems
- Enables comparison between before and after states



BUSINESS BENEFITS

1. Reduced Compliance Costs

- Automated data collection minimizes manual effort
- Fewer resources spent on audit preparation
- Faster response to audit requests

2. Improved Risk Management

- Proactive identification of configuration deviations
- Data-driven prioritization of security measures
- Better foundation for security investments

3. Streamlined IT Operations

- Automation of compliance-related tasks
- Faster problem identification and resolution
- Reduced time spent on manual documentation

4. Enhanced Security Posture

- Continuous validation of security configurations
- Rapid response to security incidents
- Documented compliance with security standards

Phone: +45 7199 2645
sales@biitops.com
www.biitops.com



CONCLUSION

BiitOps offers a robust platform that actively supports organizations' work with NIST compliance.

Through automated data collection, secure storage, and comprehensive reporting capabilities, BiitOps provides organizations with the tools they need to implement and maintain NIST-based security controls. The unique dual timestamp technology and centralized data storage ensure not just compliance, but also enable organizations to work proactively with their security level.