

NIST CSF Compliance Acceleration

The NIST Cybersecurity Framework provides a flexible way to manage and communicate cybersecurity risk. Drata helps centralize evidence, map controls, and automate monitoring to strengthen program maturity.



DISCOVER THE DRATA DIFFERENCE

► Prioritize Threat Exposure Using Risk Context

Drata connects NIST CSF outcomes to enterprise risks across governance, operations, and technology. As business priorities, assets, or third parties change, teams maintain a current view of how cybersecurity risk aligns to CSF functions, supporting clearer executive reporting and defensible responses to customer and regulatory scrutiny.

► Maintain Continuous CSF Alignment

Drata supports NIST CSF with continuously monitored controls and always-current evidence mapped to CSF outcomes. Teams maintain visibility into alignment as environments evolve, reducing reliance on point-in-time assessments and staying prepared for recurring executive reviews and stakeholder requests.

► Use AI to Summarize Security Posture Changes

Drata AI explains control test issues mapped to NIST CSF outcomes, including when controls behave unexpectedly. Teams gain clarity into what is occurring, why it affects enterprise risk alignment, and what to review next when preparing for executive updates, board discussions, or external risk communications.

► Scale Cyber Risk Governance Across Teams

Drata manages NIST CSF across global and regional programs within a single control-centric model. Teams maintain consistent risk language and governance across geographies while adapting to regional security expectations—supporting enterprise-wide alignment without fragmenting reporting or ownership.

ADDITIONAL CAPABILITIES

Align CSF Functions

Map NIST CSF functions and categories to controls with clear ownership across security domains.

Centralize Evidence

Unify NIST CSF evidence to support assessments, executive reporting, and ongoing oversight.

Link Risks to Controls

Surface CSF-aligned risks automatically when mapped controls fail to support timely response.

Automate Program Workflows

Route NIST CSF tasks, reviews, and remediation through custom workflows across responsible teams.

Share Security Posture

Publish NIST CSF aligned security documentation through Trust Center for customers and partners.

Answer Security Questionnaires

Respond to CSF-based security questionnaires using AI-assisted, human-reviewed responses.

TRUSTED BY 8,000+ GLOBAL CUSTOMERS

