Anzenna

Anzenna Compliance and Security Framework Controls

NIST 800

The NIST 800 series provides widely adopted guidelines for securing information systems and protecting sensitive data. NIST 800-53, in particular, serves as the foundational security standard for U.S. federal agencies. It outlines a comprehensive set of controls designed to protect Controlled Unclassified Information (CUI), strengthen cybersecurity posture, and reduce the risk of data breaches and insider threats.

Security Framework Control Map

Anzenna empowers security teams with the context they need to investigate and mitigate insider threats – before they escalate.

CONTROL FRAMEWORK	CONTROL ID	HOW ANZENNA ADDRESSES THE CONTROL
NIST 800-53	AC-02(09) Account Management - Restrictions on Use of Shared and Group Accounts	Anzenna automatically generates the list of shared accounts along with MFA status based on usage
NIST 800-53	AC-02(11) Account Management - Usage Conditions	Anzenna monitors all accounts/users across various channels for information disclosure, risky and anomalous behavior including Identity, SaaS, External Breaches, Shadow IT, Password Reuse, Data Exfiltration, Device Posture, Device Apps, Browser Extension, Phishing Susceptibility and other criteria to create a risk score for every user/employee. Auto-remediation of high risk along with targeted user training can then be triggered based on findings.
NIST 800-53	AC-02(12) Account Management - Account Monitoring for Atypical Usage	Anzenna monitors all accounts/users across various channels for risky and anomalous behavior including Identity, SaaS, External Breaches, Shadow IT, Password Reuse, Data Exfiltration, Device Posture, Device Apps, Browser Extension, Phishing Susceptibility and other criteria to create a risk score for every user/employee. Auto-remediation of high risk along with targeted user training can then be triggered based on findings.
NIST 800-53	AC-02(13) Account Management - Disable Accounts for High Risk Individuals	Anzenna provides a list of high risk individuals based on activity and behavior (UBA). Organizations can take that list and disable high risk users via their IDP
NIST 800-53	AC-20 (03) Use of External Systems - Non-Organizationally Owned systems - Restricted Use	Anzenna provides visibility on external SaaS application usage and Shadow IT application usage. For SaaS application usage, Anzenna provides detailed information on Oauth scopes/ permissions granted along with the ability to revoke access with a single click.
NIST 800-53	AC-21 Information Sharing	Anzenna provides visibility on information that is externally shared (e.g. public shares, AI systems like chatgpt etc.). Organizations can review this information and either setup so users can self correct or mitigate offline.
NIST 800-53	AC-22 Publicly Accessible Information	Anzenna provides out of the box visibility on information that is externally shared (e.g. public shares, AI systems like chatgpt etc.). Organizations can review this information and either setup so users can self correct or mitigate offline.
NIST 800-53	AT-02 (1) Literacy Training and Awareness - Practical Exercises	Anzenna provides training workflows using which practical tranining can be initiated based on specific user mistakes. This makes the training more relevant and effective
NIST 800-53	AT-02 (2) Literacy Training and Awareness - Social Engineering and Mining	Anzenna provides training workflows using which practical tranining can be initiated based on specific user mistakes like falling for a phishing sumulation. This makes the training more relevant and effective
NIST 800-53	AT-02 (3) Literacy Training and Awareness - Insider Threat	Anzenna provides training workflows using which practical tranining can be initiated based on specific insider threats and mistakes. This makes the training more relevant and effective
NIST 800-53	AT-02 (4) Literacy Training and Awareness - Suspicious Communications and Anomalous System Behavior	Anzenna provides training workflows using which practical tranining can be initiated based on specific insider anomalous behavior. This makes the training more relevant and effective
NIST 800-53	AT-02 (5) Literacy Training and Awareness - Advanced Persistent Threat	Anzenna provides training workflows for fake application installs which provide insiders specific information on how to mitigate against these types of advanced threats

CONTROL FRAMEWORK	CONTROL ID	HOW ANZENNA ADDRESSES THE CONTROL
NIST 800-53	AT-02 (6) Literacy Training and Awareness - Cyber Threat Environment	Anzenna provides training workflows across all threat types which can be used to provide awareness training on the cyber threat environment relevant to the employee activity in question
NIST 800-53	AU(13) Monitoring for Information Disclosure	Anzenna monitors all accounts/users across various channels for information disclosure, risky and anomalous behavior including Identity, SaaS, External Breaches, Shadow IT, Password Reuse, Data Exfiltration, Device Posture, Device Apps, Browser Extension, Phishing Susceptibility and other criteria to create a risk score for every user/employee. Auto-remediation of high risk along with targeted user training can then be triggered based on findings.
NIST 800-53	CA-7 (04) Continuous Monitoring - Risk Monitoring	Anzenna continuously monitors and remediates accounts, user and app level risks within the enterprise
NIST 800-53	CA-7 (05) Continuous Monitoring - Consistency Analysis	Anzenna's continuous monitoring & remediation across a wide range of organizational risks ensures consistency in security policy controls.
NIST 800-53	CA-7 (05) Continuous Monitoring - Automation Support for Monitoring	Anzenna's monitoring is continuous and automated across a wide range of organizational risks
NIST 800-53	CA-7 (03) Continuous Monitoring - Trend Analysis	Anzenna provides ongoing trend analysis of the risks in the enterprise along with detections and remediations for new threats like AI
NIST 800-53	CM-08(01) System Component Inventory - Updates During Installation and Removal	Anzenna provides a continuous inventory of all user installed applications which automatically updates during installation and removal
NIST 800-53	CM-08(03) System Component Inventory - System component Inventory	Anzenna provides a continuous inventory of all issued devices and user installed applications which automatically updates during installation and removal
NIST 800-53	CM-08(04) System Component Inventory - Accountability Information	Anzenna provides a continuous inventory of all devices and user installed applications which automatically updates during installation and removal with owner information.
NIST 800-53	CM-08(06) System Component Inventory - Assessed Configurations and Approved Deviations	Anzenna continuously monitors device configurations and installed applications for risk and deviation from compliance standdards
NIST 800-53	CM-08(07) System Component Inventory - Centralized Repository	Anzenna provides continous inventory of all devices and installed applications
NIST 800-53	CM-11 (03) User Installed Software - Automated Enforcement & Monitoring	Anzenna automatically inventories and scores all user installed applications, risk scores them. Risky applications can be automatically remediated
NIST 800-53	IA-02 (01) Identification and Authentication - MFA for privileged accounts	Anzenna automatically monitors MFA status for privileged accounts and highlights the non-compliant ones
NIST 800-53	IA-02 (02) Identification and Authentication - MFA for non-privileged accounts	Anzenna automatically monitors MFA status for non-privileged accounts and highlights the non-compliant ones
NIST 800-53	SI-04 (02) System Monitoring - Automated Tools and Mechanisms for Real-time Analysis	Anzenna is a people SIEM that continously monitors multiple tools and correlates and remediates relevant risks across them for proactive defense

CONTROL FRAMEWORK	CONTROL ID	HOW ANZENNA ADDRESSES THE CONTROL
NIST 800-53	SI-04 (16) System Monitoring - Correlate Monitoring Information	Anzenna continously monitors multiple tools and correlates and remediates relevant risks across them for proactive defense
NIST 800-53	SI-04 (19) System Monitoring - Risks for Individuals	Anzenna continuously monitors risky users and users on a watchlist with available automated remediations
NIST 800-53	SI-04 (20) System Monitoring - Privileged Users	Anzenna continuously monitors privileged risky users and users on a watchlist with available automated remediations
NIST 800-53	SI-04 (21) System Monitoring - Probationary Periods	Anzenna continously monitors users on a watchlist with available automated remediations
NIST 800-53	IR-04(06) Incident Handling - Insider Threats	Anzenna continously monitors for insider threats and provides information to manage investigations and incidents
NIST 800-53	IR-04(07) Incident Handling - Insider Threats Intra-Organization Co-ordination	Anzenna continously monitors for insider threats and provides information including exportable data to manage investigations and incidents
NIST 800-53	IR-09 Incident Handling - Information Splillage Response	Anzenna continously monitors for insider exfiltrating information maliciously or accidentaly along with the ability to block and/or train insiders
NIST 800-53	PM-12 Insider Threat Program	Anzenna is a comprehensive platform that allows organizations to implement & maintain an insider threat program
NIST 800-53	SC-07(10) Boundary Protection - Prevent Exfiltration	Anzenna continously monitors for insider exfiltrating information maliciously or accidentaly along with the ability to block and/or train insiders