INVITATION TO PARTICIPATE:

The Healthcare Cybersecurity Benchmarking Study

Now Enrolling Participants for Wave 4 of the Landmark Study

The Benchmarking Study is the industry's first and only collaborative initiative to establish robust, objective, and actionable cybersecurity benchmarks to help healthcare organizations strengthen cyber resiliency and protect patient care from cyber threats. Co-sponsored by Censinet, KLAS Research, American Hospital Association (AHA), Health Information Sharing and Analysis Center (H-ISAC), Healthcare and Public Health Sector Coordinating Council (HSCC), and The Scottsdale Institute, Wave 4 expands the reach and impact of this initiative with new benchmarks for NIST Cybersecurity Framework 2.0 (CSF 2.0), the HHS Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs), and the NIST AI Risk Management Framework (AI RMF).

Value of Peer Benchmarking

- Compare cybersecurity program maturity and organizational performance to peers to understand 'gap-to-goal' and drive targeted improvement
- Improve enterprise coverage and compliance with 'recognized security practices' (e.g. NIST CSF 2.0) and with future HHS cybersecurity mandates (e.g. HPH CPGs)
- Justify cybersecurity investment to the Board to meet or exceed peer performance by targeting the most-critical, under-developed areas in program maturity
- Ensure the safe, secure adoption of AI across the organization with best practices from the NIST AI RMF

To participate in Wave 4 of The Healthcare Cybersecurity Benchmarking Study, contact us at benchmarks@censinet.com

Exclusive Benefits for Wave 4 Study Participants

Participation in Wave 4 of The Healthcare Cybersecurity Benchmarking Study entitles your organization free access to:

- Censinet RiskOps™ enterprise assessments and peer benchmarks for Organizational Metrics, NIST CSF 2.0, HPH CPGs, HICP 2023, and NIST AI RMF
- Executive Summary and Deep Dive Reports to be published in Q1 2025
- Board-ready dashboards and reporting for all enterprise assessments and benchmarks to help prioritize cybersecurity investment and resource planning

Participants in Wave 4 of the Benchmarking Study are required to complete enterprise assessments for Organizational Metrics, NIST CSF 2.0, and HPH CPGs by **November 15, 2024** to be eligible for these benefits.

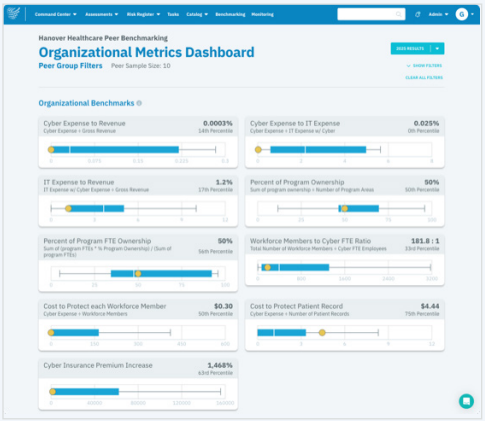
Completion of enterprise assessments for HICP 2023 and NIST AI RMF is optional.

Benchmarking Study Sponsors:

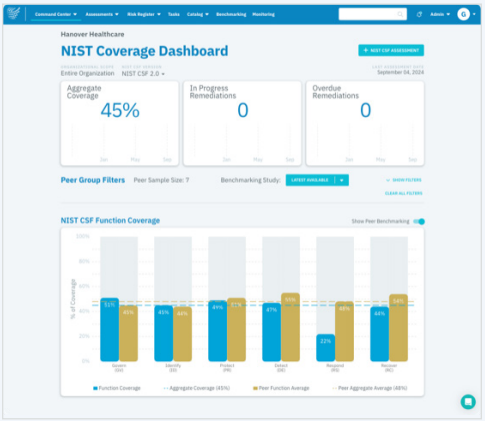
CENSINET® · KLAS RESEARCH · American Hospital Association™ Advancing Health in America · Health-ISAC™ Collaborating for Resilience in Healthcare · Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP · Scottsdale Institute COLLABORATION | EDUCATION | NETWORKING

Leverage Comprehensive Benchmarks to Transform Enterprise Cybersecurity

The Healthcare Cybersecurity Benchmarking Study enables your organization to: increase coverage of "recognized security practices" (e.g. NIST CSF 2.0); drive compliance with HPH CPGs; compare operational metrics against your peers to identify opportunities for greater cost efficiencies; and, ensure the safe, secure adoption of AI across your organization with best practices from the NIST AI RMF.

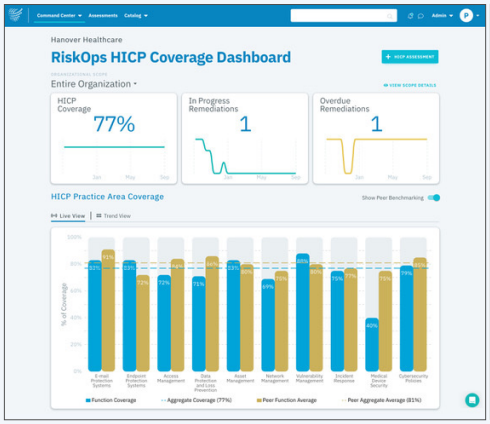


Organizational Metrics

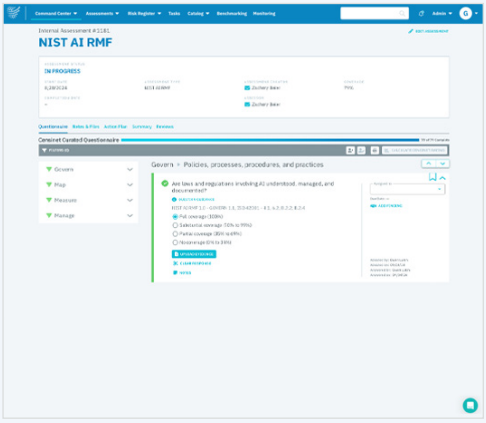


NIST CSF 2.0

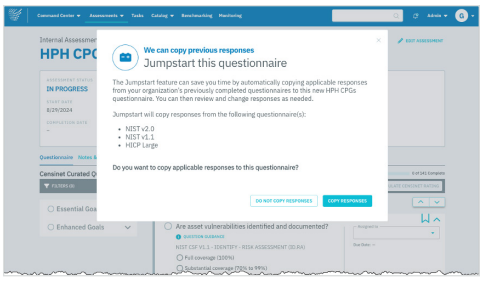
HPH Cybersecurity Performance Goals



HICP 2023



NIST AI RMF



"Jumpstart" Assessment Completion and Accelerate Time-to-Value

Wave 4 of the Benchmarking Study includes several product enhancements to expedite assessment completion and accelerate time-to-value, including the ability to "jumpstart" completion of questionnaires based on previously completed questionnaire responses for NIST CSF, HICP, and Organizational Metrics – **reducing assessment completion times by up to 90% based on availability of previously completed questionnaires.**

Stronger Together, We Can Make Healthcare Safer

To participate please contact benchmarks@censinet.com