



## *UMassMemorial Health Care*

UMass Memorial Health Care is an integrated health care system providing the highest quality of patient care and experience. UMass Memorial Medical Center is the northeast region's trusted academic medical center, with over 10,000 employees committed to improving the health of the people of Central Massachusetts through excellence in clinical care, service, teaching, and research.

The UMass Medical network of care includes multiple hospitals, community-based physician practices, rehabilitation and behavioral health services, urgent care centers, and an accountable care organization dedicated to population health advances. UMass Memorial Medical Center is also the clinical partner of the UMass Medical School. The organization's physicians and staff teach tomorrow's physicians, nurses and other health care professionals, and participate in research efforts that bring patients the latest diagnostic and treatment protocols.

“As a leading healthcare institution, we align with industry-recognized frameworks and needed a solution that would simplify and scale our compliance and risk management initiatives, while also giving insights on these efforts from a risk perspective.”

- Bruce Forman, CISO, UMass Memorial Health Care

— BUSINESS CHALLENGE

## Scalable IT Risk Management Automated Assessment and Documentation

The UMass Memorial Health Care security program had a goal of implementing an integrated risk management approach to its governance, risk and compliance activities. The organization was relying on spreadsheets, text documents, and slide decks to manually manage IT risk and compliance assessments, working to assess against industry gold-standards such as the NIST Cybersecurity Framework and others.

The CISO originally considered developing an internal tool for IT risk management, control documentation and assessment, and other governance, risk and compliance (GRC) activities but decided to look for a platform that would fit their needs and offer more capabilities than they could develop, or may even think of, internally.

In researching possible solutions, the team realized that the traditional GRC platforms and modular IRM solutions would add to the complexity of their program instead of simplifying them. These solutions also lack the risk-centric view and metrics that the program needed to facilitate decision making and communication to non-security stakeholders. Adopting a risk-centric approach and using automation to simplify and accelerate their program is the key to program efficiency and performance - knowing this, the organization’s CISO set out to find a better solution than one they could buy or build.

SOLUTION: CyberStrong IRM

# IT Risk Management & Corporate Compliance Focus

## The CISO’s IRM Solution Priorities

	Risk quantification and analytics	Board-level reporting	Time to Implement	Automated risk mitigation plans	Real time risk prioritization
CyberStrong IRM	Yes	Yes	1-5 hours	Patented AI/ML/NLP	CVE to control mapping, scoring
In-house solution	No	No	6-9 months	None	None
Traditional GRC	No	No	9-12 months	Integrations	Integrations

## Outcomes from CyberStrong IRM

— ENSURED

Security of patient data with real-time risk and compliance measurement.

— AUTOMATED

Compliance and risk project workflow, assessment, remediation planning, and execution.

— REDUCED

The communication gap between security leadership and business management.

UMass Memorial Health Care chose CyberStrong to implement, automate, and scale their integrated risk management approach. Using the NIST Cybersecurity Framework as a starting point and including CyberStrong’s NIST 800-30 risk scoring, the team now automates previously overtaxing manual processes and manages IT risk and compliance assessment and documentation from one central location.

“We looked at other IRM platforms but they were overly complex, and the time-to-value was too long. It would have taken too much time and effort to spin up even just a small project. We needed a simple solution from which to manage our cybersecurity posture, and measure where we are against where we want to go using a scalable and easily managed platform.”

— Bruce Forman, CISO, UMass Memorial Health Care