

# FISMA & HIPAA Compliance for NIH Grant Holders



As a NIH grant holder, you may find you are required to be compliant with FISMA and/or HIPAA guidelines to maintain your grant, ensure continued funding and be eligible for future awards. But where do you start to build the processes, personnel and tools needed to effectively meet these guidelines in an efficient and timely manner? And once you're compliant, how can you ensure you maintain your status between audits and check points?

Building a governance, risk and compliance program can be a challenge, especially given the specialized knowledge needed to comply with regulations and the unique environments found at hospitals, research centers and other NIH grant holders. Success requires integrated processes, innovative technology, and risk management experts who understand your business needs and are qualified to work with you to establish an appropriate GRC program.

## The TalaTek Difference for FISMA, HIPAA and More

Our seasoned industry experts know regulations, frameworks and controls thoroughly, especially FISMA and HIPAA. Our proven process framework and assessment methodologies integrate with our FedRAMP-accredited SaaS technology, to build a program that measures risk and compliance across technical, operational and management controls.

Using our cloud managed service, TalaTek intelligent Governance and Risk Integrated Solution (TiGRIS), we integrate processes, workflows and control standards into a risk management program that enables you to keep pace with changing regulations, prove and sustain compliance, and demonstrate effectiveness to stakeholders.

Using our methodology, we can conquer requirements for multiple standards in an efficient manner. If you have FISMA, HIPAA and other compliance requirements, we enable you with a single, centralized system of record and artifacts library that easily leverages one set of controls for another. TiGRIS eliminates redundant effort and maximizes your investment and resources. NIH Grant holders faced with often overlapping FISMA and HIPAA requirements can build one integrated risk management program to address all their needs. Just as the Baylor College of Medicine – Human Genome Sequencing Center did, you can trust TalaTek to build the foundation needed to meet your risk, compliance and business goals.

“TalaTek brought a team of experts, sophisticated tools, vast experience and deep knowledge. We couldn't hire that.”

Kim Andrews  
Director of IT at BCM-HGSC

## Compliance Success at the Human Genome Sequencing Center at Baylor College of Medicine

As a NIH grant holder, the Baylor College of Medicine – Human Genome Sequencing Center (BCM-HGSC) is required to comply with FISMA guidelines, including NIST 800-37 and NIST 800-137. BCM-HGSC was required to demonstrate initial compliance on a tight

timeline and needed to quickly onboard deep expertise and process experience. BCM-HGSC also wanted to implement a risk management program to support the security authorization & assessment (SA&A) process, maintain their ATOs and sustain NIH funding.

BCM-HGSC called on TalaTek to help with their immediate need for FISMA compliance. “Because we were starting from ground zero, we needed a partner that could hit the ground running on FISMA, TalaTek did just that” says Kim Andrews, Director of Information Technology at BCM-HGSC. “TalaTek was able to meet a critical compliance requirement in a very tight timeline, enabling us to stay focused on our research.”

Today BCM-HGSC tracks compliance with over 300 Moderate NIST 800-53, Rev. 4.0 controls via continuous monitoring. TalaTek performed a gap analysis for BCM-HGSC's planned HIPAA implementation, including mapping HIPAA controls and requirements to FISMA controls currently implemented in the BCM-HGSC environment.

# FISMA & HIPAA Compliance for NIH Grant Holders



“ *Understanding risk is a partnership, we both bring deep knowledge. TalaTek helped us deepen our understanding of security.* ”

Kim Andrews  
Director of IT at BCM-HGSC

## Experts in Governance, Risk and Compliance

You can rely on the TalaTek team and our TiGRIS managed service to help you achieve efficient and repeatable risk and compliance management. Each member of TalaTek is an IT professional with industry-specific certifications and experience. This quality and expertise, combined with innovative technology, ensures the successful outcomes your organization requires. Contact us to learn how the TalaTek team can help you meet your unique FISMA and HIPAA requirements and more.

## About TalaTek

TalaTek delivers governance, risk and compliance solutions with a focus on people, processes and technology. By defining governance through risk and compliance goals that are aligned to business outcomes, the cybersecurity firm provides a secure foundation to strategically protect an organization's data and meet ever-expanding regulatory compliance and audit requirements. Through its FedRAMP-accredited managed service TiGRIS, TalaTek simplifies GRC for business and government. Visit [www.talatek.com](http://www.talatek.com) for more information and follow the company on Twitter and LinkedIn.