

## New York University's Medical Center

### Automating Information Risk Management

Taking the pain out of the compliance process

HIPAA, COBIT, SOX, and FISMA. These acronyms may not mean much to the average person but to those employed in the federal, healthcare or financial sectors, they are quite familiar. To someone with a C in his or her title-CEO, CSO, or CIO- risk assessment and compliance requirements have likely been the cause of a few nightmares and at least a few headaches. While information security is a goal of each of the previously mentioned standards, the path to reach that goal can be long and arduous for the organizations mandated to follow it.

### The Sore Point

Hai Ngo is the Chief Information Security Officer for New York University's Medical Center (NYUMC) and is responsible for defining and implementing the processes necessary for maintaining regulatory compliance. The Medical Center is comprised of the NYU hospital and NYU medical school and employs about 20,000 people. As Ngo explains, the scope of activities that take place at NYU Medical Center-medical education, health care, and scientific research- necessitate the maintenance of several regulatory standards.

"As one of the nation's premier centers of medical excellence, we're accountable to a variety of mandates," said Ngo. "NYU Medical Center provides healthcare which necessitates following HIPAA regulations. We also receive federal research grants and must undergo audits of our financial records so we are bound by FISMA. Add to that COBIT and FDA regulations plus our accreditation requirements and it becomes obvious how complex our risk management and compliance processes become."

The risk assessment process required that Ngo and his team maintain a comprehensive, updated list of regulatory requirements and best practices guidelines. They would then need to gather information from each department at NYUMC to measure against these requirements. Once the data was gathered and assessed, reports needed to be generated that illustrated how each department was meeting or not meeting compliance standards, what risks they were vulnerable to and what remedial courses of action, if any, were required. Until now, Ngo had utilized his internal staff to execute risk assessment projects and compliance audits but the process was extremely labor and time intensive given the size of NYUMC-40 buildings-and the IT infrastructure. A typical risk assessment project could take anywhere from 6 weeks to 3 months and sidelined Ngo's staff from performing their other day-to-day tasks.

### Search For A Cure

Earlier this year, Ngo began researching possible software solutions that might help in streamlining the risk assessment and compliance process at NYUMC. Familiar with the industry, he looked at about five different products and finally settled on a software package that would help him automate most of the processes he had previously performed manually. Modulo Risk Manager™, developed by Modulo Security, was the software Ngo selected for deployment.

"I was looking for a solution that would offer an open framework so that I wouldn't have to perform separate assessments," said Ngo. "It was also important to be able to distribute and collect data seamlessly and of course, be easy for people outside of the IT department to use."



**NYU Medical Center**  
NYU School of Medicine & NYU Hospitals Center

"Deploying Risk Manager and thereby automating the information risk management and regulatory compliance processes at NYUMC has been a successful initiative"

"We hope to expand the software roll-out to apply this automated model to several different areas"

**Hai Ngo**  
Chief Information Security Officer for  
New York University's Medical Center  
(NYUMC)

# Success Story

## New York University's Medical Center

### Administering The Treatment

Ngo has customized Risk Manager to fit his specific needs at NYUMC. First, he “mapped” out the business components to be audited and determined the scope of the project. In this case, the project would be limited to NYUMC's financial system which consists of five systems and twenty servers. Ngo then defined the assets to be assessed, including people, processes, technologies, and physical environment. This process could be further streamlined by importing information directly from existing Active Directory™, Excel™, or XML files.

Next, the specific audit standards that Ngo needed to measure his data against, such as HIPAA, COBIT, and FISMA, were imported. Risk Manager already contained more than 10,000 built-in “controls”, otherwise known as best practices guidelines as well as an associated list of threats and threat-agents, so Ngo simply needed to choose which ones were relevant for his project and department by identifying his audit standards. He could also add to or edit the controls if needed. The controls could then automatically be converted to scripts or questions for use in data collection.

“It's important to have a repeatable process in place to manage risk and compliance across the environment,” affirmed Ngo. “I need to be able to collect and document measurable evidence in order to respond to internal audits and give our executives a metric of where we stand risk-wise as well as monitor how we control IT.”

With a defined scope in hand and online, Ngo and his team then began the process that usually makes IT management groan-gathering the data to be analyzed.

However, Ngo was able to automate that process using Risk Manager, instantly collecting answers to about 70% of the questions required for the assessment.

“I was able to do everything via securely encrypted email and the controlled-access website,” he said. “The data was automatically collected and then stored without requiring me to put software on every computer. Another bonus is that if I'm entering or analyzing information and the computer crashes or I become otherwise disconnected, I don't lose anything. The software 'remembers' where I left off.”

Of course, once the data is in hand, it must be analyzed and measured against multiple regulations and assessed for potential security vulnerabilities. Modulo Risk Manager is capable of assessing information security risk and also offers suggestions and courses of action to mediate those risks.

“If I had to measure all the data collected against all of the compliance standards we need to meet, it would take forever. Through automation, I was able to reuse 80-90% of the data collected for testing compliance to the different regulations. The measurement values were already built-in; I just had to apply the data.”

Once the data is collected, risks identified, and compliance levels measured, reports can be quickly generated (within minutes) for each standard required. Reports can also be generated during any stage of the project, allowing for quick and painless status updates.

Contact us  
(212) 922-1789

[www.modulo.com](http://www.modulo.com)



NYU Medical Center  
NYU School of Medicine & NYU Hospitals Center

### Prognosis?

Deploying Risk Manager and thereby automating the information risk management and regulatory compliance processes at NYUMC has been a successful initiative, according to Ngo. So successful, in fact, that his department hopes to widen the use of the software to other departments, such as research, where information security is always a high priority.

“We hope to expand the software roll-out to apply this automated model to several different areas,” he asserted.

“We go through so many compliance and accreditation audits in a year that it would be extremely helpful to more intensively apply this process to enterprise risk management.”

Aside from further customization of the software features, combining web and software deployment, and widening the project scope to include non-IT related systems, Ngo and the management team have been extremely pleased with the decision to implement Risk Manager for assessing risk and ensuring regulatory compliance.

“The flexibility and ease of use of the product we chose to deploy paired with its automated assessment and documentation features have saved us a significant amount of time,” asserted Ngo. “I don't know how the process could have gone any better.”

