Moving From Compliance to Risk-Based Security: CISOs Reveal Practical Tips

CISO members of Wisegate discuss effective ways to start and maintain a successful risk-based security program

WISEGATE COMMUNITY VIEWPOINTS
Introduction

Security managers are working with senior executives and their counterparts in groups across the organization to move from a compliance-based approach to information security towards a risk-based approach. The shift requires senior management and the C-suite to think differently about risk and stop handling compliance as a checklist.

Many industries are under regulatory pressure, but the federal government is also pushing forward risk-based frameworks. Organizations interested in retaining government contracts will need to ensure they have the controls and processes in place to meet requirements outlined by risk-based frameworks such as FISMA and NIST.

The shift to a risk management approach has been brewing for some time. In a previous Wisegate report titled, “CISOs Share Advice on Managing Both Information Security & Risk,” CISOs from top companies discussed the impacts of evolving job requirements as they take on a more strategic and proactive role in risk management and privacy. Today’s CISOs are being asked to prioritize risks—by identifying which ones need to be addressed and which ones should be accepted as the cost of doing business.

In the latest Wisegate discussions, security executives across industries broadened previous conversations by taking a more in-depth look into the challenges of shifting towards risk-based information security. While no two risk programs are identical, Wisegate members identified the following key takeaways.

» **Compliance becomes just one factor in the risk profile.** Even in a risk-based program, compliance doesn’t go away entirely. The regulations are still there, but department heads and managers have to start thinking in terms of acceptable risk levels versus compliance requirements to mark off a checklist. It’s a change in language, and the moment when everyone understands the difference is an “ah-ha!” moment for the entire organization.

» **Tolerance for risk changes over time.** The organization’s risk tolerance is dynamic and fluid. The assessment plan and risk profile indicates the organization’s risk acceptance level at a point in time, but it is expected to change. It is also difficult for organizations to properly assess risk beforehand; frequent conversations about what department heads and senior management are comfortable with promotes awareness across all lines of business.

» **Making risk management work.** Risk management can be broken down into three distinct areas: strategic, tactical and operational. As organizations move to a risk-based approach, they can explore assessment platforms, work to create risk profiles and partner with third-party providers to perform risk assessments.
Compliance Becomes Just One Factor in the Risk Profile

Security professionals have to engage business counterparts in frequent discussions about risk and compliance, and understand that complying with a regulation doesn’t necessarily equate to being secure. There is also a need for multiple, ongoing conversations that address how compliance fits within the risk framework.

For many Wisegate members—which include senior security executives in leading and major corporations across various industry sectors— compliance was a good starting point to begin the conversation.

A CISO of a health insurance provider commented, "We have patient information, so HIPAA and HITECH are daily conversations around here. Having management understand the value of going beyond compliance requirements to reduce our overall operations risk was invaluable."

When asked why their organizations were implementing a risk management program, Wisegate Members unsurprisingly named compliance requirements as their primary reason.

What are the top drivers for your Information Security / Risk Management program?

- Compliance requirements: 73%
- Recent security incident, requiring external notification: 15%
- A recent security 'close call', without external reporting requirements: 21%
- The general threat landscape facing your business, technology, and employees: 47%
- It is the right thing to do, we prefer to initiate change rather than react to events: 47%
For organizations with federal contracts, realizing the need to be FISMA-compliant helps add momentum to their programs. While compliance remained the top driver, many organizations also experienced an "ah-ha!" moment that drove home the importance of a risk-based approach, according to some CISOs.

When Bad News Can be Good News—Negative Incidents as a Driver for Change

"Business people need to feel the pain. If you’re unfortunate enough to have something like a big data breach that makes the headlines, then that just might be the ah-ha! moment that moves the company towards a risk-based approach. But hopefully, you can address this before you get to that point," commented an information security manager from a large non-profit during a Wisegate roundtable discussion.

Looking at what happened to their peers can also make senior management pay attention. "The biggest ah-ha! moment was when other institutions had issues that caused them bad press, monetary fine, or a combination of the two—that certainly made people stand up and take notice," said one higher education CISO.

While negative incidents get the organization talking about risk assessments, the catalyst doesn’t necessarily have to be a data breach. An internal audit flagging poor access management and other regulatory drivers can also improve funding for risk management projects.

Mapping Compliance Requirements to Risk Frameworks

Not all frameworks and regulations are created equal. Some provide stronger controls and frameworks for implementing security. Others have boilerplate controls that are too vague to be of any use. One recommended approach is to first understand what controls the organization needs and then figure out whether they are already in place by performing a risk assessment.

A CISO of a healthcare organization described during a roundtable discussion how an insurance company mapped HIPAA and HIPAA HITECH requirements against the controls required by NIST800-53:

"A mapping shows the controls that we have in place, such as access controls, and the relevant HIPAA reference. That’s been very helpful from the auditor standpoint, but from an operational standpoint, we aren’t focusing only on HIPAA."

A security executive from a medical services organization compared compliance to a lens, saying the set of controls can be viewed from a compliance perspective as well as risk. After verifying a system was compliant, the next step was to assess actual security.
“The first lens looks at the control and says, ‘yes, it’s there,’ or ‘no, it’s not or it’s not applicable.’ That’s the compliance way of asking, ‘Hey, is there a lock on the door?’ ‘Yes.’ Then I go back and I grade it again for maturity, saying, ‘That lock is kind of weak. I’d rather move these systems from this office with the weak lock into a bunker that has armed guards.’ As far as the law is concerned, my system’s behind a locked door, only three people have a key, and I’ve got tracking to see who can get in there, but when I look at that and have a conversation with my CIO, we say, ‘That’s just not as secure as we’d want it to be. We need to move these systems.’"

The first assessment determines where the controls exist and creates a gap analysis to identify the missing areas. The second assessment looks at the controls that need to be there and assesses whether they are sufficient. If not, the security team has to assess the risk of not using the stronger controls.

**Tolerance for Risk Changes Over Time**

It’s impossible to apply security controls across the board. No one has the resources to do that nor would it necessarily be good for the organization as a whole. So security professionals must conduct risk assessments to identify areas that are high priority for the organization. The problem is, not many business stakeholders—department managers, team leads, and senior executives—are used to thinking about security as part of a risk conversation.

**Use a Baseline Document as a Starting Point**

Several security executives commented that their counterparts in other parts of the organization didn’t have a clear view of what was an acceptable level of risk and couldn’t define their risk tolerance until they could look at something concrete. Many CISO members of Wisegate agreed that having a document as a starting-point facilitates these discussions. But it was also cautioned, “Don’t try to get it perfect. Don’t try to cover everything. It’s much more important to get a starting point and start the discussions.”

Once the organization creates an executive risk baseline document with the controls identified and the baseline clearly marked, then security and the leaders of the various lines of business can sit down each month and decide which controls may need a second look. Through the document, the stakeholders and senior managers can clearly see what it means to ease up on some controls and make changes as necessary.
Actual Incidents Help Illustrate Risk

One security manager in the healthcare sector discussed how their organization’s tolerance for risk changed after several laptops were stolen. Once there was a clear example of risk, it was easier to understand the risk of not doing anything.

“We had a couple of laptops stolen. Fortunately, none of them had HIPAA data, but it was a wakeup call, a shot across the bow. If that had happened in another division, we’d have a crisis. Their risk tolerance changed instantaneously because the abstract became real.”

A director of information security at a financial services firm described how the senior executives in his organization wanted to be notified about everything.

“When we were deciding what to escalate up to our executive team—what level of information and what metrics—they initially said they wanted to see everything. When we showed them what ‘everything’ was, they understood the volume. The conversation then became focused on finding the right level, such as, ‘The system is down for 10 minutes. We don’t really care about that. Let us know if it’s down for an hour.’”

Risk tolerance is hard to define, which is why it’s important for the security team to work alongside line of business partners so that they can collectively work through the assessment and keep the conversation going on a regular basis. Definitions, thresholds and tolerance levels eventually get clarified, and the division manager and executive leadership will know when something carries too much risk.

In an ideal scenario, the security team would work with all levels of the organization—starting with the C-suite, then the managers and continuing all the way down to the end-users—to clarify the balance between security and risk, and to understand what makes users scream in frustration.

“The exercise consists of going through and tightening the screws and saying, ‘If we set this up in the way that it makes the most sense based on security, we would have three gateways and it would require three log-ins.’ Then you’ll get feedback from the executives saying, ‘We don’t want to remember three different log-ins.’”

A director heading up security at an investment bank said, ‘Looking at impact levels—what people are willing to accept—sometimes is the right place to start.”

Some Employees are Riskier Than Others

Every employee doesn’t pose the same level of risk to the organization. Executives can have a higher acceptable risk profile—such as the ability to run unapproved software,
share data and use more assets—than end-users or lower-level managers. The risk profiles can be organized into a color-coded organizational chart like the one shown below.

**Assign Color-Coded Risk Profiles Across the Organization**

This particular type of organizational chart is a visual way to get different members of the company thinking about risk. Every name on the organizational chart hierarchy is inside either a red, yellow, or green box on this chart. The colors indicated the amount of risk each person pose to the company (red—show-stopper; green—no/low risk).

**Making Risk Management Work**

During the roundtable discussions, Wisegate members stressed the importance of having frequent discussions about risk tolerance and existing controls, even on a monthly basis. The conversation needs to involve key stakeholders in the organization, including the CEO, COO, CFO and other C-suite executives, human resources, IT, business support and business unit executives.

Risk management programs need to have top-down buy-in, and a risk executive must be willing to take charge of the entire program.
As one security director said, "If you have executive support, risk management can work, but it’s not something that you’re going to be able to just flip a switch and have it start working. There are a lot of conversations that need to occur, and people need to agree on baselines, scoring and a lot of other elements."

**Collect Data Regularly for Most Up-to-Date View**

In the discussions, CISOs and director-level security professionals said there should be at least two full-blown assessments a year, one of which should be a true penetration test and the other scrutinizing all existing controls.

The results of the penetration test, financial control audits, system tests and evaluation, and any other assessment data should be combined to get a full overview of the organization. The assessments help each line of business understand the risks associated with their projects and initiatives and ultimately transforms what used to be just a compliance audit into a risk management program.

A senior security executive described the importance of having an initial risk questionnaire for a manager to complete when starting up a new project so that risk can be adequately assessed. Answers to questions about types of data being accessed, architecture, and user access help the organization create a preliminary risk profile for the new initiative. The questionnaire can also be overlaid against NIST or similar controls.

"We started by saying, 'What do we need to know before we can develop a risk profile? And what are the red flags—those things that get our complete undivided attention if somebody says it during a new project meeting?' We broke it down into five or six questions and said, 'If we get certain answers to these five or six questions, we will need to be more involved with the project going forward.'"

Even if the resulting risk profile doesn’t trigger a flag, everyone can proceed with full awareness of the potential risk—while still small—associated with the new project.

**Treat Risk Management as an Evolutionary Process**

Wisegate members agree that it is helpful to approach the transition from compliance to risk-based security as an evolutionary process. Wisegate member Jeff Bardin identifies, in the graphic below, different levels organizations go through while building processes and frameworks.
Jeff explains, “Risk is just a phase in the evolution of security. Once built in, security will be just as seat belts, brakes and air bags are on automobiles—standard features and functionality. Risk today is no more than an opportunity for the organization to waive due diligence and due care.”
Approach Risk Management from Varying Points of View

Risk management should be looked at from varying points of view including: strategic, tactical, and operational.

Three Levels of Risk Management

Risk management from strategic, tactical, and operational points of view.

1. **Strategic**—At this level, focus is on the lines of business and their individual objectives. The question to ask is, “How it will affect the company’s three-year and five-year plans?” Security managers should sit down with their counterparts across the organization—including HR, IT, finance, operations and other divisions—to talk about existing risks. Everyone should weigh in on what they feel is acceptable, transferable or can be mitigated. The goal is to create a thorough risk impact analysis so that executives know the objectives.

2. **Tactical**—The security team is primarily concerned with performance and how the organization is doing against the risk controls, but the business objectives are still paramount. Managers and executives may be willing to take more risks, but the auditors generally suggest a more cautious approach. Some point between the two is the baseline for the organization’s acceptable level of risk. With the baseline in place, it’s time for the executives to discuss in which areas they are willing to take on more risk.

3. **Operational**—This is where risk assessments, SDLC, continuous monitoring, risk profiles, and controls are all built. The operational level should consider what compliance controls are in place, find the gaps, and identify new tools to add.

Explore Risk Assessment Methodologies and Tools

Security teams are adopting various governance and control frameworks, and it was clear at the roundtables that members are using a mix of controls and frameworks, instead of relying on just one. Examples include using modified ISO 27000 controls alongside CoBIT. The HITRUST framework is already mapped to ISO, NIST 800-53, PCI, and HIPAA/HITECH, making it easier to work with.
Which governance or control frameworks have your organization adopted, even if loosely (assume centralized model)?

A director of identity access management at a financial institution said:

“The reality of these standards and others is that we found adhering to some of the controls next to impossible for various reasons (culture, business maturity, lack of mature SDLC, etc.) so we usually implemented some and others were home-grown based on a good set of policies, standards, and procedures... ‘loosely coupled’ is a good way to put it.”

In the medical sector, there is no single framework that contains all the compliance rules, prompting the security team to identify a handful that could be cobbled together to meet all requirements. “I use the NIST framework with the ISO controls overlaid with HIPAA controls, PCI controls, a couple of contractual obligations and I’ve created a framework that’s got about 177 controls.”

CISOs are adopting various risk assessment methodologies and tools to conduct audits and assessments. The results are in line with the earlier risk management report.
Which IT risk assessment methodologies does your organization use, even if loosely?

In an online poll, Wisegate members identified the following risk assessment tools and vendors as being helpful: Citicus ONE, WolfPAC, OCTAVE Allegro, and Binary Risk Assessment. Some of the CISOs said they relied on homegrown audits using ISO 27000 for a framework because they weren’t impressed with the level and depth of content from commercial providers.

Wolfpac appeared to be commonly used by financial institutions to compile and document risk assessments. It allows for the production of a comprehensive risk assessment report that can be used for regulatory requirements as well as an executive summary that can be used for board reporting. Some CISOs praised the platform for its comprehensive features:

"Wolfpac should be a jumping-off point to address regulatory issues then expanding upon it into a comprehensive IT Risk Management program. It is definitely not a cure-all but if small or mid-size financial institutions aren’t using anything and were looking for something to address regulatory concerns or cited contraventions, I would recommend it."

Others remained skeptical of WolfPAC’s capabilities.
“One thing I have noticed with Wolfpac is that it is not quantitative in any shape or form. It is opinion based Q&A that leads to the assessment. Unless it has changed, that was my impression as recently as last fall. Therefore, I don’t believe it is in fact comprehensive. It does have acceptance with auditors but this demonstrates a problem overall with how things work. I have seen financial organizations use Wolfpac and pass their audit / assessment, but have significant technical and procedural issues bordering on material. Then again, this can be said about many methods/tools (Garbage In, Gospel Out).”

While OCTAVE Allegros was also a popular choice, it may be too complex for some organizations.

“In terms of straight IT risk assessments, we have used OCTAVE Allegro in the past but have found even this simplified version of OCTAVE can bog down small(er) IT departments. Because of this, I have generally gone with an outsourced and slightly less complex solution.”


**Tips for Success**

Business units, such as human resources, IT, support staff, business unit leads, and even end-users can be suspicious of risk management programs--considering them to be a form of witch-hunt through which security teams were looking for problems, CISOs said. The way to diffuse this tension is to make the conversation inclusive and collaborative. Find out what is important to the end-users and their manager and what slows them down while working. Use that as a starting point to answer why things have to be a certain way and how things can be better.

“Ask end users, ‘What is it about your department and your activities that you’re worried about?’ There’s always one little thing out there that makes the department think, ‘Oh, my God, if this fails, we’re screwed,’” said a senior security manager.

“If we come to a point in time where the business is surprised or perceives that we’re basically saying, ‘You can’t do something’ or ‘What you’re doing is wrong,’ as a business leadership team, we’ve failed.”
In Closing…

From the Wisegate roundtables, it was clear that risk management programs provide organizations with a lot of flexibility, but implementation still requires a tremendous amount of effort. A risk-based approach doesn’t eliminate compliance requirements, and C-level executives, security managers and division heads have to learn to communicate their objectives so that collectively everyone can agree upon the right balance. Risk management requires buy-in from the top-down so that there is support for new initiatives and processes.

Being part of the Wisegate expert network keeps senior IT practitioners abreast of evolving strategies and informed on which approaches other CISOs find effective. An in-depth discussion of the challenges and tactics that can be helpful to explore when moving from compliance to risk-based security continues at Wisegate.

Wisegate is an IT expert network and information service that provides senior-level IT professionals with high quality research and intelligence from the best source available—the collective knowledge of IT leaders from across the industry.

Through live roundtable discussions, detailed product reviews, online Q&A and polls, and timely research reports, Wisegate offers a practical and unbiased information source built on the real-world experience of veteran IT professionals. No analyst theories or vendor bias to cloud the information, just clear and straightforward insight from experienced IT leaders.

Would you like to join us? Go to wisegateit.com/request-invite/ to learn more and to submit your request for membership.