How a CISO Crowd-sourced a Successful Business Case for GRC

Security Veterans Share GRC Vendor Experiences and Tips on Gaining Buy-in for a Risk-based Security Approach

WISEGATE MEMBER CASE STUDY

wisegate

2303 Ranch Road 620 South I #135-165 I Austin, Texas 78734 I www.wisegateit.com

Introduction

Over the last decade, regulatory pressures have instilled within many organizations a compliance-based approach to information security. But now organizations must rethink their approach to security as sensitive data threats continue to proliferate and the federal government pushes forward risk-based frameworks, such as FISMA and NIST. In response to these changes, many chief information security officers (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.

To address these new responsibilities, CISOs are implementing GRC technologies and educating, collaborating and communicating with senior executives and their counterparts in groups across the organization. Making the shift from a compliance-based to risk-based approach can be difficult as it requires senior management and the C-suite to think differently about risk and stop handling compliance as a checklist. Creating the necessary understanding of risk, which often span legal, business operations, finance, and human resources, can be a big challenge for even the most seasoned CISOs.

This report features a case study of a CISO and Wisegate member—and details how she used the Wisegate community to crowd-source a successful GRC business case. Like all IT security leaders, Wisegate members face challenges managing the growing complexity of governance, risk and compliance (GRC)—and find benefits from the ability to confer with others—to get advice and learn from the experiences and successes of their peers.

There's no simple answer to the GRC dilemma and the right solution will vary from one company to the next based on company size, corporate culture, industry, regulatory requirements and IT infrastructure. Nevertheless, this case study is designed to help you understand common risk management issues and learn how one CISO built a successful business case for GRC with crowd-sourced answers to questions like:

73%

of senior IT leaders cite compliance requirements as a top driver for information security and risk management programs

SOURCE: Wisegate Community Poll

- *How do you engage the business in risk discussions?*
- *What tools do you use for risk assessments?*
- *Which criteria should we use to compare GRC providers?*

Meet the Case Study's featured CISO and Wisegate Member

"I belong to many associations for the purpose of networking, but the Wisegate community is extremely responsive and allows me to quickly find out how my peers are addressing industry challenges. Because it is a closed community, I can trust that I'll get solid advice."

Candy Alexander

Former CISO of Long Term Care Partners
Wisegate member since April 2012

- Volunteer member, International Board of Directors, ISSA
- Invited to White House to speak on importance of security awareness to President's Cyber-Czar staff
- Throughout career has held several positions as CISO with responsibility for corporate security programs

Challenge: Convince senior management to buy off on a new approach to risk management

Candy knew that a new approach to risk management was necessary to protect sensitive corporate data from evolving security threats and fully comply with new federal guidance for risk-based frameworks. To help her company successfully complete the transition from a compliance-based to risk-based security approach, Candy needed to further educate her senior management team on the differences between risk and compliance, and decide which Governance, Risk and Compliance (GRC) technology would best meet her company's unique needs.

> "It's a big challenge to move the business past the compliance 'checklist' mentality and help people across the organization understand all the potential risks found in the environment, such as data exposure, unauthorized access, proprietary information theft, etc."
>
> Candy Alexander, CISO

Like Candy, many Wisegate members face the same challenges building business acceptance for new risk-based management programs.

- *"My organization still has not had that "aha!" moment when the business understood the difference between risk and compliance. The business units still focus on making sure we are compliant with the necessary laws and regs rather than seeing the big picture of risk and protecting the data from it. Someday we will get there."*
- *"Unfortunately to understand risk, sometimes business people first need to feel the pain. After a big data breach, which makes headlines, it becomes much easier to move the company towards a risk-based approach. Hopefully, you can make the switch before you get to that point, but that takes commitment."*
- *"You have to find something that's important to the business—something that's tangible. It may be a common friction point that staff or business leaders often run up against, like password resets. When they ask, 'Why do we have to do this?' you have an opportunity to provide a meaningful example of compliance versus risk."*

Solution: Tap the collective wisdom of peers to test ideas and gain external perspective

Candy was overloaded with information from GRC vendors, but felt that her team lacked insight on what other companies were actually doing to overcome evolving compliance and risk challenges. To build a solid business case, Candy wanted more practical knowledge about how her peers were successfully engaging business leaders in risk discussions, which risk assessment tools were most popular and how vendor technologies really stacked up in real world deployments. Candy tapped the Wisegate community to gain real world advice and learn from the experience of other veteran security practitioners.

> "Typically, we have one shot with the business to get a program accepted. If we fail, it may take an extraordinary amount of time to recover—if at all possible. My involvement in Wisegate allowed me to take the lessons learned from peers and successfully apply them in our business."
>
> Candy Alexander, CISO

Getting Started with Wisegate Online Content

Candy started her research online by exploring existing Wisegate community content, which included member discussions, polls and product reviews. Below is a sampling of some of the information that Candy found useful.

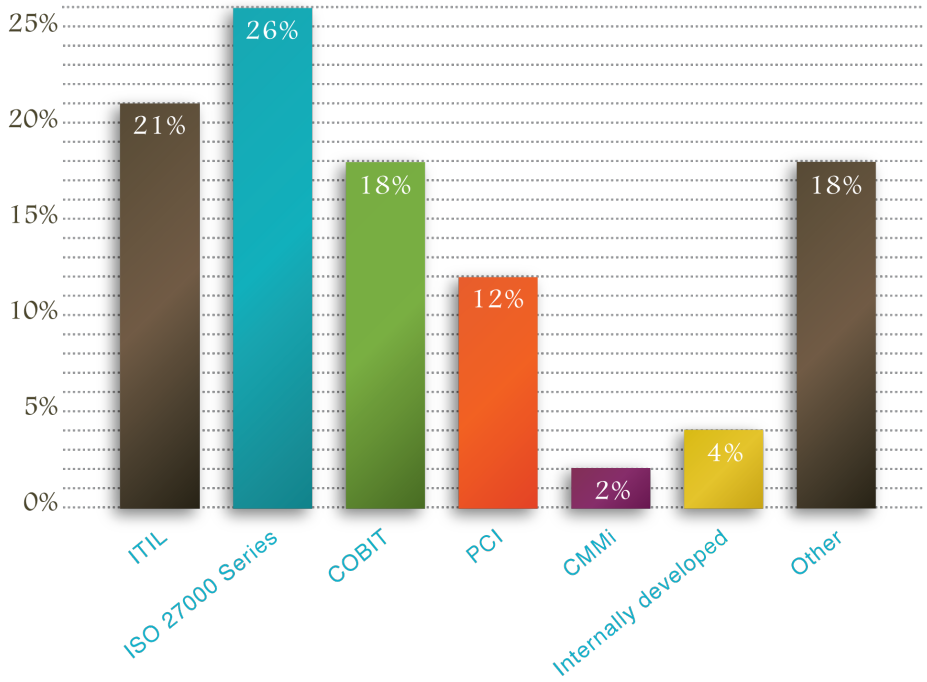
Online Discussions

"What tools are you using to help with risk assessment?"

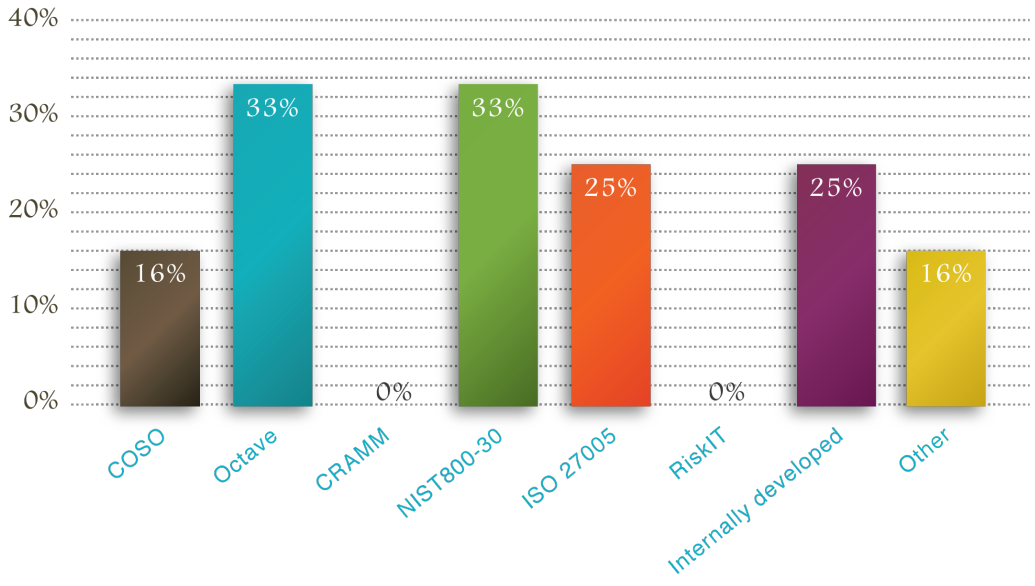
- *"We use Citicus ONE software (which leverages the FIRM risk management methodology developed through the Information Security Forum). We have extended the scope and use of the software steadily over the years and integrated it increasingly in processes such as portfolio management, continuity management and service level management."*
- *"We are currently evaluating new vendors to assist us with this process, but so far the most comprehensive Enterprise Risk Assessment platform we have come across is called WolfPAC for our type of financial services organization. For 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. We have worked with a vendor by the name of TraceSecurity in the past and they have done a decent job for us as a mid-sized financial institution."*
- *"We conduct homegrown audits using ISO 27k as a framework."*
- *"There are many tools out there for use. An ISO27001/2 tool may help you measure risk—control driven, Q&A and you can modify your risk areas as well."*
- *"We use Binary Risk Assessment and OCTAVE Allegro."*

Online Polls

Which governance or control frameworks have your organization adopted?



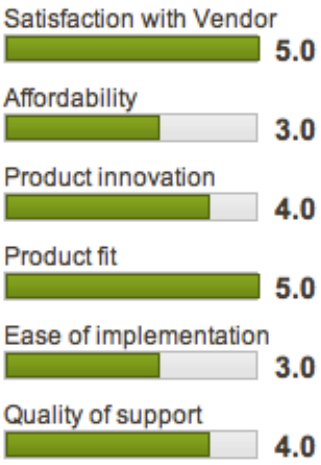
Which IT risk assessment methodologies does your organization use?



Vendor Reviews

IT Risk Management and IT GRC Tools

Archer (RSA) eGRC



"The product is more than just a tool, it is a framework and as such you can do anything with it that the software allows. Unlike its competitors, who provide a product where you have to hope and wait for updates in the next release, you release what you want, when you want."

"The cost of ownership is higher than others."

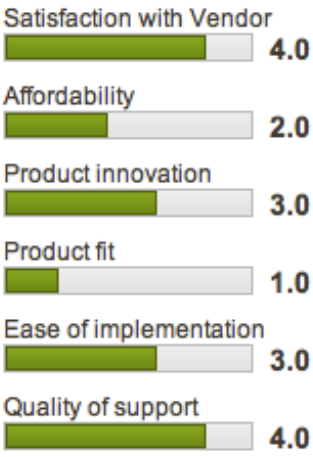
"This tool requires care and feeding. A program around GRC must be in place with proper policies, procedures and workflow. If you do not have procedures and workflow around GRC, it can be easy to use what is built-in."

Agiliance RiskVision Open GRC

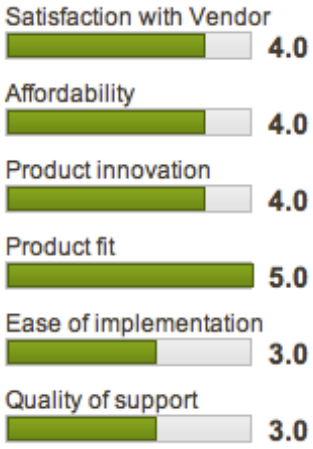
"The product just wasn't a great fit for us. It was a full-blown GRC solution, so it was fairly expensive for us. We just needed it for privacy compliance, but it really wasn't well suited for that purpose."

"Implementation was fairly expensive—given the limited amount we were implementing. We had to pay them to try to get the tool to work for what we needed."

"We should have probably stepped out of it two years before we did. You just have to know when to stop throwing good money after bad."



Symantec Control Compliance Suite



"Overall, we were satisfied with the product and vendor. We did have some issues with quality of support during implementation, but some of that was due to the complexity of the product and insufficient training and skillsets on our end."

"It's very important to think about the strategic things you want to accomplish and carefully develop those goals into business requirements; then translate those business requirements into technical requirements to see if the system is going to deliver what you expect."

Taking a Deeper Dive with a Live Wisegate Hosted Roundtable Call

To share her experiences and gain even more detailed information from her peers, Candy asked Wisegate to host a live roundtable session. During the roundtable call, *"Moving Security Programs from Compliance to Risk Based Approach,"* Candy led the discussion and received many valuable insights from her peers about what was working and just as importantly, what wasn't.

Present Risk vs. Compliance as a Continuum

To help engage business leaders in risk discussions, one member recommended presenting compliance as a baseline along a risk continuum.

A CISO for a state healthcare agency explained, *"In my definition, risk falls along a scale. Compliance requirements set the minimum risk that the governing bodies are allowing for your organization. Start from the baseline and then take a risk-based approach—setting the bar at the level your organization feels secure with. The idea is—don't set a level of security that doesn't meet the baseline or else you have compliance issues, plus you're probably not secure because those baselines are the minimum level of security that you should have inside your organization."*

He continued, *"My biggest problem with this approach, which is probably opposite from most, is that I have too conservative of an organization. The businesses have a tendency to*

take a very risk averse position, and sometimes we have to get them off the board a bit because if we implemented the controls that they'd like to see, it would make the systems unusable. While it makes a lot of sense from a security point of view, you have to get them off the baseline and come up a little bit on the risk in order to allow the functionality of the organization to exist."

Talk About Risk in the Context of Business Continuity

To business people, the thought of discussing threats and information risk can be very intimidating. In order to break the ice, members agree it can be helpful to start the discussion from a business continuity perspective, which is the worst-case scenario. From this point of view, the business is more open to talking about risk tolerance and the cost of mitigation.

A senior security manager for a non-profit suggests, *"Ask, 'What is it about your department and your activities that you're worried about?' Or, 'What keeps you awake at night?' There's always one little thing that makes the department think, 'If this fails, we're in big trouble.' Once you find out what that is, use it to define the conversation and prioritize your efforts."*

Create a Risk Profile at the Beginning of Each New Project

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 to five or six questions and said, 'If we get 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.

Deliver Good News, Before Bad

No matter how adeptly or diligently controls are implemented, the results of a gap analysis or audit will almost always reveal outstanding actions. But constantly focusing attention on

the open items can overwhelm business units. Often it is easier to build support by focusing on the successes and progress of your initiatives before being the bearer of bad news.

An information security manager explained, *"You're always left with a list of things that still have to be done. No one likes to look at that. It's always, 'Here's the stuff you haven't done.' And, 'Here's the extra work you're going to have to do.' I find that it works better if I highlight the fact that we're not starting at point zero by saying something like, 'There's 100 things on the list and we've accomplished 87 of them. We're down to the final 13.' That helps people feel a little bit better about what's left to do rather always focusing on those few things that haven't been done."*

Take a Collaborative Approach

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 are looking for problems. The way to diffuse this tension is to make the conversation inclusive and collaborative. Find out what is important to 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.

"If we come to a point in time where the business is surprised or perceives that we're telling them they can't do something, or saying what they're doing is wrong, as a business leadership team, we've failed," commented a senior security officer.

A director of information technology from the banking sector further explained, *"We always go forth with the intent to meet our business units' expectations, but negotiate with them along the way to layer in proper security controls as we implement solutions."*

An information security officer from the health care industry added, *"You have to overcome the 'old security manager' reputation of saying 'No' and show that you're all about 'business enablement.' I tell my managers that I'm here to not only help them to do business, but to do business securely. I see the security manager's job as the 'enablement of secure lines of business communication.' But we have to keep in mind that security should be in alignment with the value of the data. Putting in gates and security for low levels of information will be perceived as overkill. Layering security based on information value is a key concept to get across to management."*

Lessons Learned: There are no right or wrong answers

> "The right approach has to do more with the organization itself, the business it operates and the risks inherent to that operation. Ultimately the right tool and approach depends mostly on the security professional and what he or she feels most comfortable using to 'tell the story'."

Candy Alexander, CISO

> "Be consistent and persistent in making the business understand that compliance is only a piece of the puzzle. Additional information risks may be found in the environment—and work with the business to understand their risk tolerance."

Candy Alexander, CISO

Benefits Realized: Saved time, money and potential heartache from a bad decision

Wisegate enabled Candy to speak directly with other senior IT security practitioners to get an honest assessment of the vendor landscape and select the right GRC partner in a reduced timeframe—saving time, money and potential heartache from a bad decision. Additionally, she implemented many of the ideas she gained from her peers to improve senior management's understanding of why a risk-based approach was necessary and help them become actively involved in making better risk-based security decisions.

> "Using Wisegate I was able to connect with peers and get meaningful data. This allowed me to actually show my CEO how we stack up against other companies—making justification of my GRC recommendations much easier. I can honestly say it saved us months of pouring through endless amounts of vendor hype and failed attempts of implementing a program that may not have fit our business."

Candy Alexander, CISO

About Wisegate

Being part of the Wisegate expert network keeps senior IT practitioners abreast of evolving strategies and informed on which approaches their peers find effective. In-depth discussions on the challenges and strategies that can be helpful to explore when planning a move from a compliance-based to risk-based security approach and other relates issues continues online at www.wisegateit.com.

Wisegate is a private, practitioner-based Information Technology (IT) research service for senior IT professionals that lets them tap directly into the most valuable source of technology information: the collective intelligence and experiences of their peers.

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 professionals. Wisegate makes working in IT rewarding and fulfilling by putting technology professionals in control of valuable information.

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

wisegate

2303 Ranch Road 620 South

#135-165

Austin, Texas 78734

PHONE 512.763.0555

EMAIL info@wisegateit.com

www.wisegateit.com