HALOCKSecurityLabs

CASE STUDY

ISO 27001 Is Good Security and Good Business for National Law Firm

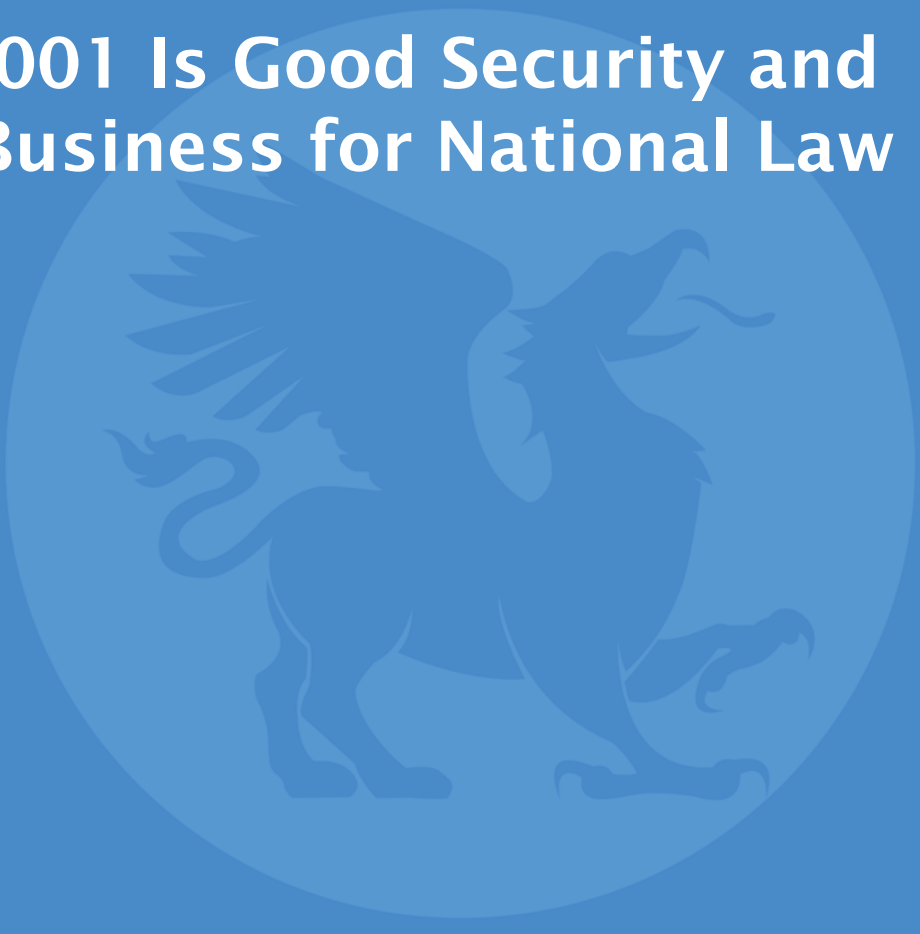
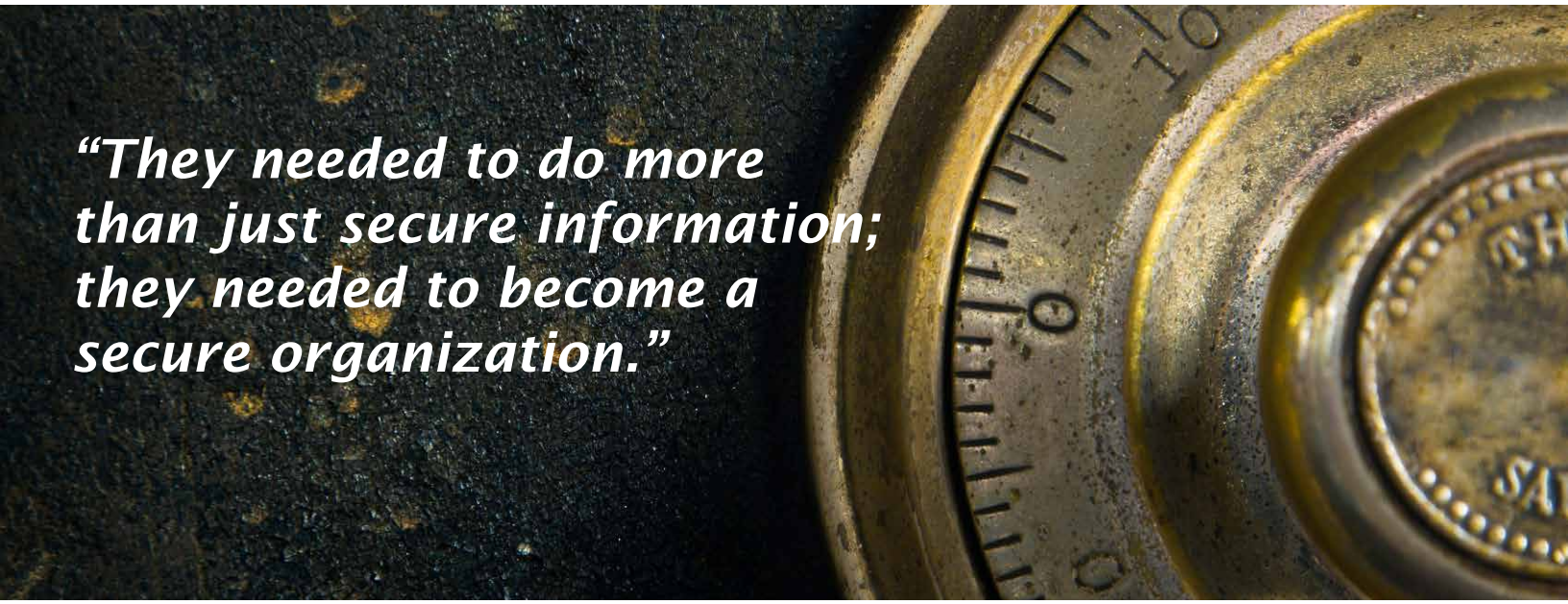


Table of Contents

ISO 27001 Is Good Security and Good Business

When a national law firm decided that securing their highly sensitive information and information systems was critical to their success, they turned to ISO 27001. By partnering with a security consultancy that specializes in the Information Security standard, they quickly realized that ISO 27001 was as much about smart business as it was about securing information.



Rausch, Sturm, Israel, Enerson & Hornik (RSIEH), a Milwaukee-based law firm that specializes in consumer debt collection is no stranger to information security requirements. As a debt collector, they are subject to numerous laws and regulations regarding communication with debtors and the handling of debtor records. And because their clients are consumer retailers and financial institutions their contracts are painstakingly detailed with requirements for proper stewardship of their customers' financial information. Add to that the rise of information security laws and regulations and the law firm's challenge with information compliance can appear overwhelming.

RSIEH, now certified to ISO/IEC 27001, realized that in order to respond well to these increasingly demanding requirements, they needed to do more than just secure information; they needed to become a secure organization.

ISO 27001 Demystified

ISO 27001 (also known as ISO/IEC 27001), is an international information security standard that was devised by the International Organization for Standardization (ISO) and the International Electrotechnical Commission. ISO 27001 is more than a list of technical security controls, but a comprehensive management system. The Information Security Management Systems (ISMS) that is described in ISO 27001 describes how to manage a secure organization.

When an organization becomes certified to ISO 27001, they are able to demonstrate that they secure information assets (information, technology, facilities, processes and people) according to risk management principles and security objectives. They undertake the following activities:

Plan – Assessing and Addressing Risk: An ISO 27001 certified organization declares what part of their organization will operate within ISO 27001 ISMS management processes (the "scope" of the ISMS). They then identify in-scope information assets within the boundaries of their ISMS, and document the organization's legal and contractual obligations for protecting those assets. The core repeating activity from this phase is the Risk Assessment. The organization needs to assess risks to their in-scope assets in light of their obligations and select security controls (from a set of 133 controls provided in the ISO 27001 standard as "Annex A") that reduce those risks to an acceptable level.

Do – Reducing Risk with Standard Controls: The organization's management then implements the controls that were selected during the Plan phase, ensuring that the controls are sufficiently documented and communicated to the organization. The implementation of each control should address the risks that were identified. The controls must be implemented in such a way that they can be measured to demonstrate their effectiveness.

Check – Overseeing Effectiveness: In the Check Phase the organization designs and conducts measures of the implemented controls and performs independent internal audits. Managers who "own" high-risk information assets must be aware of how the controls around those assets are performing. They are also informed of their assets' security through internal audits. An information security committee regularly reviews trouble areas and progress towards reducing risk and can make decisions to continuously improve security.

Act – Addressing Weaknesses: The executive committee (sometimes called a Risk Management Committee or an Information Security Committee) makes decisions to address security weaknesses that became evident in recurring measures and audit tests. These decisions can be educated, tactical and strategic because the strengths and weaknesses of the ISMS are known at the executive level, are aligned with the organization's risk, and are tied to their ability to fulfill their information security obligations.

The RSIEH ISO Story

I think the most challenging part of implementing ISO 27001 is getting your team to switch their mode of thinking from 'getting things done' to reducing identified risks," says Garrick Olejnik, RSIEH's Chief Information Security Officer. "We had been in the mode of responding to clients and General Counsel who gave us a list of things to do to secure information. We would see some odd security requirements in those lists and we would ask our clients, 'does this control really help secure your information? Because we would need to apply a lot of effort without a lot of benefit.' And we found that, to the best of their intentions, they wouldn't always know the answer to those questions and we would negotiate some resolution between us. We did our best to get these information security controls right, but in the end, security was resolved as a negotiation. In hindsight it may not have been the best way to address actual risk."

"CMR 17.00 and the PCI DSS were telling us that we had to use a risk-based approach to securing information … So if we were going to live up to our responsibilities, we needed an information security management system."

Greg Enerson
Managing Partner / Co-CEO

Greg Enerson, RSIEH's General Counsel, noticed something lacking about their current approach to information security. "The laws and requirements that we were responding to, like Massachusetts CMR 17.00 and the PCI DSS, were telling us that we had to use a risk-based approach to securing information. To my mind, that's the law and the credit card industry telling us that we are responsible for identifying and managing our risk, not them. They can't tell us how to secure our information. So if we were going to live up to our responsibilities for securing their information, we needed an information security management system."

"HALOCK was already working with RSIEH when they asked us about ISO 27001," said Jim Mirochnik, a partner at Chicago-based HALOCK Security Labs. "RSIEH had a very significant client who had broadcast to their debt collectors that they were raising the bar. If you wanted to do business with them, you had to be compliant with ISO 27001." Mirochnik recognized something about the RSIEH leadership that gave him confidence that ISO 27001 was right for them. "We can bring organizations through ISO 27001 implementation and certification. We can bring them part-way so they get 80% of the benefit from maybe 60% of the effort, in essence being compliant without being certified. But RSIEH was serious. They knew that a data breach could really hurt them and their clients, and they knew that certification would set a high bar that they would be forced to surpass and raise every year. That certification would set them apart from their peers. They were all in and we would see them through to completion."

RSIEH and Halock partnered in the beginning of 2011 with a goal of getting certified to ISO 27001 in 18 months. “One of the initial activities we did with HALOCK was the risk assessment. That was eye-opening,” says Olejnik. “Imagine bringing every manager who is responsible for debtor information that moves through a law firm into interviews about what they are responsible for, how data moved from one stage to the next, what controls they had in place, what could go wrong, and what would be the impact to the organization if it did go wrong. When you spend that amount of time thinking through what could go wrong with information, that was educational, to say the least.”

Chris Cronin, Principal Consultant at Halock Security Labs, conducted RSIEH’s first risk assessment. “Risk assessments are as much about educating management as they are about laying the groundwork for an ISMS. When you meet with conscientious people who are focused on getting their work done well, and you shift their attention a little bit to the potential consequences of things going wrong, they are ready to re-prioritize their management focus immediately. They are ready and willing to take action and address those risks.”

“They got ISO 27001 from the outset. They saw what it could do for their business to differentiate themselves to their clients.”

Cronin noticed right away that RSIEH understood how ISO 27001 was about good business in addition to measurable security. “Within our first few conversations, they said, look, we need to focus on Confidentiality, Integrity and Availability of information. Absolutely. But we need the ISMS to also ensure that everything we do with debtor information is right. We need to also understand the likelihood and impact of missing client work standards. Let’s add another column to our risk assessment; ‘Process Compliance.’ They got ISO 27001 from the outset. They saw what it could do for their business to differentiate themselves to their clients.”

“We get a steady stream of requirements and audits from our clients. They really are trying their hardest to stay within the law and they need us to treat their customers, who are now debtors, with respect,” said Bill Sturm, CEO of RSIEH. “So our clients give us a set of rules we need to follow, in addition to existing regulations, to make sure that happens. If I am investing in ISO 27001, and it is going to help me know whether I’m in compliance with security rules or not, it better do the same for letting me know if I’m fulfilling my obligations to my clients. If it can’t do that then it’s not the best investment for us.”

Within weeks, Sturm knew that he had made the right investment. “Almost all of the risks we identified were about process compliance; fulfillment of our client obligations. We found our share of security and compliance issues at risk, and we knew right away how to address them. But we got our managers to really understand what could go wrong with data and the impact it could have on our business, on our clients and on the people we talk to everyday. That’s what we were looking for. That’s what we needed.”

The Process Book

More than identifying risks, ISO 27001 is about managing risk by applying a set of standard security controls and overseeing their effectiveness. "That was the next challenge," said Olejnik. "We put together this comprehensive list of risks. Some important, some we could accept. But still a list like we've never had before. So how do we manage it?"

RSIEH immediately put into practice a monthly executive meeting called the Information Security Committee (ISC). Using a Process Book – an agenda-driven status review document – the ISC was able to schedule, assign and oversee implementation efforts for managing the risks they identified. For controls that were already in place, they could see if they were being tested. If they were not being tested, then they could put measures or audits in place. And if measured controls were not passing performance metrics such as "number of people who went through information security training divided by number of people hired," then management knew to correct the problem right away.

"I'll be honest. The last thing I need is another meeting," said Enerson. "Scratch that. The last thing I need is to violate requirements. So if I'm in another meeting, it better get to the point, it better let me know what's going wrong, and it better give me a basis to take corrective action. The Process Book did that. I liked it. You know what I liked more? The fact that our BSI ISO 27001 auditor liked it too."

"We invented the Process Book," Mirochnik said with a grin. "Our clients can't be expected to take on something as trans-formative as ISO 27001 without having a way to manage it. We had to design some easy way for them to – within a single meeting – see what is working and what isn't in the ISMS. RSIEH has to know where to apply their efforts, make their decisions, and close the meeting knowing that their decisions will be carried out. And if they're not carried out, they'll know at their next ISC meeting. It's right there in the Process Book."

"I have to make decisions on a daily basis about the business," said Sturm. "That Process Book gives me a real look at where we're at with our security obligations. If I make a decision to address a non-conformance or invest in a security device, I know what the effect on risk will be. I see trends of my risk going down month by month based on the decisions I've made."

"The most challenging part of implementing ISO 27001 is getting your team to switch their mode of thinking from 'getting things done' to reducing identified risks"

Rick Olejnik
Chief Information Officer

On Compliance and Good Business

When asked about ISO 27001 as an investment, Sturm was quick to respond, "Absolutely, absolutely a great investment. This is where the industry is going. It's where the world is going. We tell our clients, or even prospective clients that we're certified and it's an entirely new conversation. We've had clients ask us to expand our operations to more states because we are meeting their needs. And remember, not just securing the data. We're working within their strict processing requirements in a measurable way. Today we stand out, and that means more business."

"I know we're applying due diligence," says Enerson. "I can see we are applying due care. You throw a statute or requirement at us and we'll catch it, integrate it, measure it and fix it if it strays. That's what we're supposed to do by law, and that's what we do."

Olejnik added, "My responsibilities for protecting information and keeping things operating have always meant that at some point or other I've had to go to these guys and ask for money. Sometimes my pitch works and sometimes it doesn't. Using the ISMS though, we know why we're spending money. It's right there in our prioritized risk register. It's how we know we can get that control into compliance, or the impact of that threat reduced to something we can digest."

"And you can't get to this point without having a partner who's done this before," Sturm added. "We know people who've tried and they've failed. The concepts can be a little challenging to grasp at first. Knowing how to make things work in a practical way . . . . that's something that someone with experience is going to have to show you. We could not have done this without HALOCK. They know the security part of it. They have compliance down cold, and they know the ISMS requirements and how to make them achievable. Another big pay-off to partnering with them was that they know how the certification audit will go, so everything they help you implement is done so the certification auditor will understand it. Yeah, I don't see how you could get this done without a partner."

"It's where the world is going. We tell our clients that we're certified and it's an entirely new conversation. You can't get to this point without having a partner who's done this before.

Bill Sturm
Co-CEO

ABOUT HALOCK SECURITY LABS

HALOCK Security Labs is a new breed of information security professional services firms. HALOCK is a hybrid firm; the attributes of this new category include professional services organizations that have the necessary personnel to combine strategic security consulting and compliance with technical security architecture and implementation services. To truly be a security partner, it is necessary to have these combined capabilities in an integrated approach to servicing clients.

In addition to its strategy of Purpose Driven Security™, HALOCK works with clients to integrate security in all elements of IT. HALOCK is well positioned to partner with clients to assess, strategize, re-mediate, and build strong Security Programs.

ABOUT RSIEH

RSIEH is a debt collection law firm headquartered in Wisconsin with offices in 13 states and a nationwide network of firms for clients seeking additional coverage. In service of premier multi-state law firms, RSIEH operates facilities with state-of-the-art data management, software, imaging, call center and analytics.

HALOCK Security Labs

1834 Walden Office Square, Suite 200, Schaumburg, IL 60173

WWW.HALOCK.COM