



INSIDE THIS PUBLICATION:

Has the time arrived for a corporate overhaul of ERM?

What corporate meltdowns teach us about ERM

RSA: Business-driven risk management closes the gap of grief

Survey: Trials, tribulations of third-party risk management

Compliance clauses can keep third parties in line, regulators at bay

Learning to mitigate third-party risks

The international risk of compliance

Working toward a solution: Third-Party Risk Management

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. <http://www.complianceweek.com>

RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cyber-crime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to www.rsa.com

Inside this e-Book

Has the time arrived for a corporate overhaul of ERM?	4
What corporate meltdowns teach us about ERM	7
RSA: Business-driven risk management closes the gap of grief	12
Survey: Trials, tribulations of third-party risk management	16
Compliance clauses can keep third parties in line, regulators at bay	20
Learning to mitigate third-party risks	23
The international risk of compliance	25

Has the time arrived for a corporate overhaul of ERM?

Corporate approaches to risk management are not keeping pace with the velocity and complexity of risk in today's business environment. Is it time for an enterprise risk management refresh, asks **Joe Mont**.

Corporate approaches to risk management are not keeping pace with the velocity and complexity of risk in today's business environment, suggesting it's time for a refresh to traditional methods.

Nearly three-fourths of leaders at public companies, large organizations, and financial institutions say they've seen a marked increase in the volume and complexity of risk in the past five years, according to a new study out of North Carolina State University and the American Institute of Certified Public Accountants. Yet, only one-fourth believe their risk management processes are mature or robust enough to keep pace. The majority said they do not believe their handling of risk could be described as complete or formal approaches to enterprise risk management.

That suggests there's a big gap between the risk landscape and companies' ability to navigate it. "There's still a lack of clarity in how risk management should help me strategically," says Mark Beasley, a professor at NC State who led the study. "In so many entities, if you ask people 'tell me about risk management,' you hear 'that's the group that tells me I can't do X' or 'that's internal audit.' They don't see the value of risk management."

Deon Minnaar, a partner at KPMG who leads the

global practice around ERM and GRC, says he sees a lot of companies struggling with ERM. "Some ERM programs have become stale over time," he says. "It's become a little too much like a paper exercise to keep up."

Ash Noah, a vice president at the American Institute of Certified Public Accountants and a former CFO with global experience, says the interconnectivity of markets makes keeping up with emerging risks a particular challenge. "It's getting more difficult to look out and see what's coming at you," he says. "That's why it's getting more difficult to identify and manage risk, but it's all the more reason you need a systematized way to look at it."

Experts agree the time has come for companies to rethink their long-standing approaches to risk. For starters, it needs to be elevated in many cases. "In many organizations, risk has been relegated to middle level or upper middle level management," says Chris Ruggeri, principal at Deloitte who leads the strategic risk and reputation management practice. "That misses the fact that there are interdependencies in risk factors. Traditional ERM approaches don't consider the interdependencies across the risk spectrum. They look at each risk in isolation."

Stephen Zawoyski, U.S. ERM leader at PwC, says

ERM is too often seen as simply an exercise companies must endure. “It’s seen as an annual trip to the dentist,” he says. “Too many times it’s being done to comply with a request from the audit committee.” The key stakeholders in ERM—board, management, and internal audit—often have different expectations of enterprise risk management, he says, but many programs are not designed to satisfy the needs of all three groups.

Another problem, says Zawoyski, is ERM is often run by the internal audit department, which puts a negative connotation on ERM. He says that internal audit is asking: “What are all the things that can happen?”

The NC State study suggests some companies are trying to move in that direction, establishing management-level risk committees and even appointing chief risk officers, but they are still in the minority. “It’s the start of a trend, but it’s definitely not the majority,” says Zawoyski. It’s more prevalent in highly regulated industries, like financial services.

In addition to elevating the risk function to higher levels in the organization, companies also need to tie more closely their discussion of risk with their strategy, experts say. “Whoever is in charge of ERM needs a true seat at the table when it comes to strategy,” says Minnaar. Certainly, boards and senior management are already thinking about risk when they make critical decisions, but having the enterprise risk management voice at the table would formalize it, Minnaar says.

Ruggeri agrees that’s a missing element for many companies. “The mindset about risk has

been anything but strategic,” she says. “Risk is usually thought about in the context of something to be managed, mitigated, reduced, or eliminated. But it’s virtually impossible to eliminate all risk from business.”

Changing that mindset is another reason to elevate risk management, says Ruggeri. “It has to start at the top of the house,” she says. “It has to start in the C-suite at the board level.”

Jennifer Burke, a partner at Crowe Horwath in risk consulting, says she was surprised to see in the NC State study the extent to which ERM is still not tied to strategy-setting at the board level. She says boards should take a close look at risk right before their annual strategic planning gets started. “Having that conversation about risk management right before the strategic planning processes puts risk in mind,” she says.

COSO, the organization that gave capital markets a framework for internal control over financial reporting, is updating its separate framework on ERM. The board issued an exposure draft and is working through comment letters before finalizing the update. The new framework is expected to emphasize the importance of linking enterprise risk management to an organization’s strategy and performance.

That would be a useful tool for companies that recognize their risk approaches are in need of a reset, says Burke. “It will help organizations have a more tangible approach to ERM,” she says.

Zawoyski says the new framework will be useful both in elevating the risk discussion and in tying it to strategy and performance, but it won’t dictate

“In so many entities, if you ask people ‘tell me about risk management’ you hear ‘that’s the group that tells me I can’t do X’ or ‘that’s internal audit.’ They don’t see the value of risk management.”

Mark Beasley, Professor, NC State

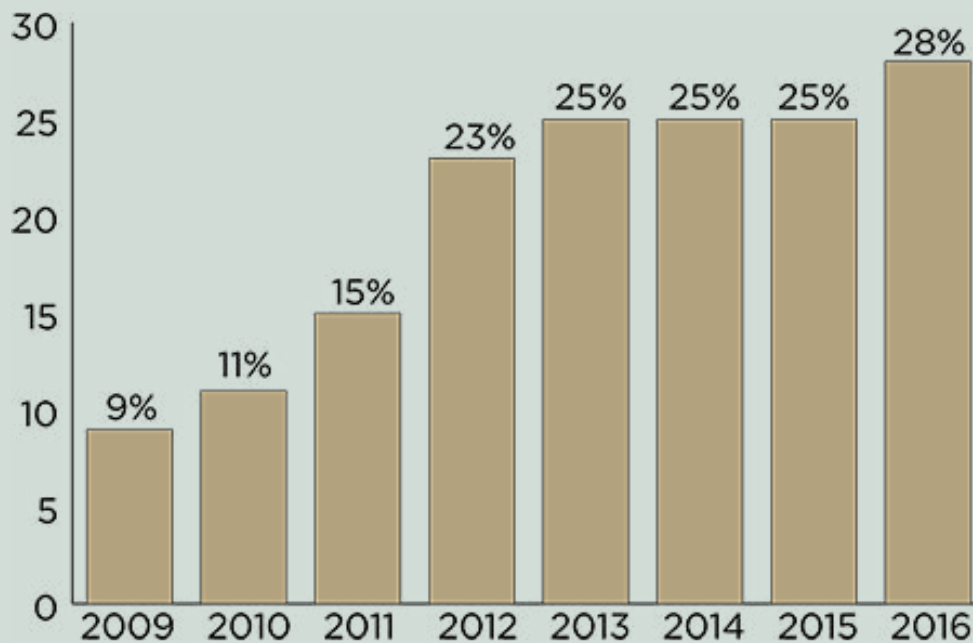
the exact mechanics of an ERM program. “It’s principles-based,” he says. “It’s not an implementation guide. It’s not going to tell you what your governance structure should look like, but that you need one and here’s its role and here’s what it needs to accomplish. So, it’s very scalable.”

The new framework will be a useful tool, says De-

loitte’s Ruggeri, but it won’t be a silver bullet. “It’s not a substitute for a holistic organization-wide mindset to risk management,” she said. “You can have the best processes in the world but if people follow them by rote and don’t gain the insights they are intended to provide, it fails to meet the mark.” ■

COMPLETE ERM IN PLACE

The chart below from the AICPA and NC State shows an increase from 2009 through 2012 with a leveling off for the subsequent three years in the percentage of organizations that claim they have a “complete formal enterprise-wide risk management process in place.”



Sources: AICPA; NC State

What corporate meltdowns teach us about ERM



Joe Mont talks to Steven Minsky, CEO of LogicManager, about how disruptive technology demands that businesses practice better governance and enterprise risk management.

In the modern world, everything is connected and risk is the common link.

Emerging technologies and new commerce models have transformed how businesses operate. Companies like Uber, AirBnB, Lyft, and Peapod are among the companies that have upended traditional business models. Customers can get a ride, book a hotel, and order groceries with just the push of a button. But with this convenience comes plenty of

risk, says Steven Minsky, CEO of LogicManager, a provider of risk management platforms and mentoring services. The rise of peer-to-peer networks, for example, put businesses directly in contact with the consumer, but also amplify traditional risks and add new threats to the mix.

We spoke to Minsky following IMPACT 2016, LogicManager's customer conference, held this year in Boston. Among the topics discussed at the event

“Companies need to reframe the conversation to accept that innovation brings risk, so how do they look at this through a risk management lens rather than focusing on regulatory barriers.”

Steven Minsky, CEO, LogicManager

were the risks inherent with emerging technologies and the evolving sharing economy. How can companies balance innovation with risk mitigation? The concerns encompass third-party risk management, performance integration, cyber-security, and risk reporting to the board.

A backdrop to these challenges is a shift in how compliance is viewed. New updates from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and International Organization for Standardization—including ISO 19600 and COSO's upcoming ERM update—emphasize a risk-based approach to compliance. In a broader view, the organizational understanding of the relationship between risk and compliance is changing.

Minsky offers the radical technology behind self-driving cars to underscore the butterfly effect that incubates risk for even traditional businesses. Consider auto insurance companies as an example.

“They have a fixed base of costs and with a reduced number of accidents they are going to have lower premiums,” Minsky says. “They are really investment companies, so that means they will have less money to invest. They must innovate to generate more revenue, somehow and somewhere.” The latter approach is where problems manifest. “Those new products are not going to have a history by definition,” he says. “They don't have 30 years of risk data.”

These, and other emerging issues must be approached as a risk management problem, not necessarily as a compliance problem, according to Minsky. “Companies need to reframe the conversation to accept that innovation brings risk, so how do they look

at this through a risk management lens rather than focusing on regulatory barriers,” he says.

LogicManager's website sums matters up succinctly: “In our 21st century business environment, everything is connected, and risk is the common link. Misconceptions about the role of risk management, and how to accomplish it effectively, have resulted in countless organizations falling victim to preventable disasters. Preventable, that is, if only those companies had established an effective ERM program.”

Illustrations of potentially preventable disasters were hardly in short supply throughout 2016. Looking back at the year that was may help understand the changing risk and compliance roadmap going forward. Minsky details a handful of corporate brouhahas to make his point.

Chipotle

Problems haunting Chipotle actually began in 2015, but continued to hurt the restaurant chain throughout the past year. A quick recap: In August 2015, 243 customers in California reported norovirus illnesses after eating at the restaurant; in December, another 143 customers reported food poisoning from a Boston-area location; E. coli-related sickness was later identified in 11 states.

The reputational damage has dragged down the company's financials ever since. The company has thus far settled with nearly 100 plaintiffs. In-store sales are down, and the stock price dropped 22 percent throughout 2016.

In many ways, Chipotle's troubles were a side effect of good intentions and customer-pleasing

innovation. The chain prided itself—and marketed accordingly—on a dedication to using fresh, locally sourced ingredients. The problem: Food safety management becomes far more difficult as the supply chain is decentralized.

The company failed to implement the risk management necessary to support its innovations, Minsky explains. A properly focused enterprise risk management solution might not have stopped the flow of tainted food, but standardized employee health protocols, testing, and preparation guidelines might have helped. At the very least, Chipotle would have been able to use its ERM software's reporting capabilities to evidence its risk program, verify control activities, possibly avoiding regulatory penalties and ongoing reputational harm in the process.

"Chipotle is not a story about lack of compliance. It is actually a story of innovation and not looking at the risks that go along with innovation," Minsky says. "What they did was a great innovation. Having a central distribution center, however, means you have one point of vendor management and food preparation oversight. When you move it to a thousand restaurants with local sourcing, you have a thousand points of food preparation oversight." Proper food preparation and vendor due diligence are not great mysteries to explore. "The question is how you do it at 1,000 different places. That is a governance problem."

Wells Fargo

The mother of all regulatory scandals in 2016 was Wells Fargo. Government investigations uncovered the widespread practice of opening unauthorized customer accounts and credit cards, a practice blamed (correctly or not) on harsh sales quotas. The damage thus far: \$185 million in fines, the loss of municipal business in some states, the resignation of its CEO, and 5,300 employees were fired.

To fully appreciate the bank's risk management woes requires a time trip back to 2009, when the Securities and Exchange Commission approved rules "to enhance the information provided to sharehold-

ers so they are better able to evaluate the leadership of public companies." In the following annual reporting and proxy season, those rules enhanced corporate disclosure regarding risk, compensation, and corporate governance matters.

Specifically, the SEC required disclosures in proxy and information statements about the relationship of a company's compensation policies and practices to risk management. It also required board-level accountability for enterprise risk management. Boards were required to disclose how their organizations identify risk and set risk tolerances.

Further back, in 2007, regulators released the Sarbanes-Oxley Audit Standard, which holds management accountable for the risk of misstated company financials. "The SEC disclosure rule is similar in the sense that it uses materiality, not specific risks, as a measure of what needs to be mitigated," Minsky wrote in a recent blog post. "It differs, however, in the sense that it applies to all risks, not only financial concerns, and does not take into account an organization's size. In other words, everyone should be concerned with ERM compliance. This leads to a fork in the road; organizations need to either adopt an effective risk management program or bite the bullet and disclose their ineffectiveness."

As for Wells Fargo's travails, Minsky has a variety of questions.

- » How could activities on this scale go unnoticed to management for 5 years? "Not knowing" isn't a valid excuse," he wrote recently. "It's negligence."
- » Why was there no compensation oversight for employee sales quotas and incentives?
- » Where were the risk assessments on these processes? What about internal audits of both the risk management process and governance oversight?
- » When Wells Fargo designed its sales incentive program, why didn't risk assessments reveal how unrealistic those sales goals were?
- » Were there mitigation activities to protect against customer account manipulation? If so, where

were the risk monitoring activities that would have picked up on the appearance of two million accounts over a five-year period?

Wells Fargo, in his assessment, offers yet another lesson that boards and senior management are responsible for the risk management effectiveness of their companies, no matter how vociferously they claim ignorance when problems are uncovered. A company can try to defend itself by claiming that rogue employees evaded internal controls. The argument falls apart, however, when robust controls are missing in action and board and executive oversight is lacking.

“This wasn’t about mean, old Wells Fargo putting up high sales targets,” Minsky says. “That’s a smoke-screen. When you are talking about 1.5 million unauthorized accounts, it is a failure of risk management, a failure in assessing the separation of duties, and a failure in assessing what those practices are and the effectiveness of the mitigation activities. It is a failure in risk management which is monitoring the controls against the risk.”

Wendy’s

In December 2016, fast food giant Wendy’s was served with the latest in a series of class-action and shareholder lawsuits over a data breach that compromised payment security at more than 1,000 franchises. The problem was ultimately traced to point of sale systems at those restaurants.

The interesting twist on a traditional cyber-attack was Wendy’s post-breach mea culpa. The corporation tried to distance itself from the breaches by showing that no company-owned stores were affected.

“This isn’t just a story of failed cyber-security. It’s also a story of failed vendor and third-party management,” Minsky says. “There’s a reason no company-owned stores suffered a breach, while more than 1,000 franchised locations were affected. Wendy’s maintained its own cyber-security processes. What it failed to do was ensure that all locations maintained the same standards.”

Cyber-security is not necessarily about compli-

ance, Minsky argues, “there are no laws in the world that are going to keep people safe. In fact, all the technologies to be safe pretty much exist. It is really a human problem.”

The majority of breaches occur because of weak, reused passwords and poor governance over password management. “It doesn’t really matter which technologies you use, there are still human beings with passwords,” he says. “Governance solves that problem very effectively for very little money, but people are still viewing it as a technology problem and spending millions—sometimes tens and hundreds of millions of dollars—on infrastructure and technology. Wendy’s had franchises with weak passwords, then they went out and bought tens of

Yes, there can be a compliance problem; but lack of compliance is in itself a governance problem.

Steven Minsky, CEO, LogicManager

millions of dollars of new point-of-sale equipment. It didn’t do anything because there was still a governance issue with passwords.”

The solution isn’t limited to technology. It is answering the question of how to take a policy and operationalize it, making it real for the employees.

The solution should not rest on the shoulders on the IT department and in-house security experts. “They can’t do it by themselves,” Minsky says. “[The rise of] Software as a service (SaaS) means that IT may not even know what is being used in the corporation. It used to be—and all the policies are still written this way—that IT knows everything and monitors everything. But in this day and age, 50 to 70 percent of the technology in some cases is no longer in house. How can IT even know what’s going on?”

The solution is to break down and bridge corporate silos. For example, incorporate the finance department into the security process because they know, definitively, what services they are buying, what the assets are, and what departments they are allocated to. “That’s what they do,” he says. “They pay for things and allocate them. They know the SaaS and devices in use. Because IT isn’t connected to finance, they might not even dream of going to them, not realizing they have a beautiful asset list, even if it is for a different purpose.”

Armed with an asset list from finance, combined with the IT department’s list of passwords, a company can begin to put governance to work with reminders and tasks for the process owners. ERM and GRC (governance, risk management, and compliance) systems can push tasks out to each of

the process owners. “Here is the devices, applications, and services your group is using; here is the list of employees who are mapped to them.” Should they have that access? Have they followed all the policies? When they change roles do they still need access?

Log-in walls can streamline the use of passwords and, by keeping employees from having to constantly update individual passwords—creating weak ones out of the necessity to remember them—stronger passwords will be the result.

“If you recognize it not as a technology problem to spend money on, but a governance problem to organize your people, that’s when you actually solve the problem for pennies on the dollar,” Minsky says. “Yes, there can be a compliance problem; but lack of compliance is in itself a governance problem.” ■

COSO FRAMEWORK

The following is from a LogicManager blog post on what CEO Steven Minsky sees as missing in the new, forthcoming COSO ERM Framework.

In my opinion, the following recommendations would make Enterprise Risk Management – Aligning Strategy and Performance more measurable and in line with statistically proven business processes. They are ordered from largest to smallest contribution to business value. For more details about each recommendation, please visit the full document on COSO’s feedback page:

1. The update needs to stress the crucial difference between risk outcome and root cause, as this distinction is vital to effective risk identification.
2. The “performance” attribute should be expanded so the update provides more support for internal initiatives, rather than emphasizing external elements.
3. The update should contain more actionable components regarding the integration of ERM into everyday activities.
4. The emphasis on engaging front-line management across all business areas should be quantified.
5. The framework should be substantiated with references/citations to established precedents: the SEC’s Proxy Disclosure Enhancement and the Yates Memo, for example. This would help educate management about the consequences of not effectively monitoring their risk management activities.

Source: LogicManager

Survey: Trials, tribulations of third-party risk management



Jaclyn Jaeger has the results of a new survey jointly conducted by Compliance Week and Crowe Horwath that explores the many trials and tribulations of third-party risk management programs.

A new survey conducted by Compliance Week and Crowe Horwath asked respondents to identify current challenges posed by third-party risk management programs. The answer? A litany of compliance woes: lack of technology to help manage workflow, lack of third-party participation, inability to produce meaningful reporting, and more.

“Overall, the survey tells us third-party risk management is continuing to evolve,” says Gayle Woodbury, managing director in Crowe Horwath’s risk consulting practice. “Although some companies have clearly moved beyond the basics in terms of maturity, many are still working through some foundational elements.”

According to the survey, 42 percent of 101 respondents cited third-party participation as one of their top challenges. In that aspect, robust communication can go a long way toward forging closer ties with third parties, both as it pertains to their participation in due diligence and ongoing monitoring efforts and willingness to work through rigorous contracting rules.

“Companies that have really good buy-in and good participation rates from their third parties have a really strong communication process,” Woodbury says. Clearly communicating expectations—as well as why and how the third-party risk management process works—is all the more important, given that third parties have multiple corporate customers, each with different processes and procedures required to satisfy their third-party risk management programs, she says.

Companies with mature third-party risk management programs are those that have built that rapport and mutual respect with their third parties, says Michele Sullivan, a partner in Crowe Horwath’s risk consulting practice. If managed well, that rapport can result in numerous benefits, including improved quality in the information that is shared and targeted consolidation of third-party capabilities, thus, resulting in potential cost savings realized by the company as well as potential revenue generation for the third party, she says.

Challenges

In addition to third-party participation, 39 percent of respondents cited “lack of technology to help management workflow” as another significant challenge.

When asked to identify what tools and technologies they use for third-party risk management, the majority of respondents said they use end-user computing—such as Excel, Access, or SharePoint. Moreover, the use of end-user computing was most common across the board for all kinds of purposes—performance scorecards, control assessments, contract administration, risk reporting, procurement, and more.

Of the respondents who said they use commercially available software, third-party/inventory was the most widely cited (34 percent), followed by contract repository (31 percent), issues management (24 percent), and risk reporting (23 percent). Others said they use it for things like sourcing/procurement, contract administration, and performance scorecards. Fewer respondents said they use an internally developed solution.

36 percent of respondents said the ability to produce meaningful reporting was also a pain point, which could be due to not having the necessary technology solutions in place. Also, when asked to identify what specific types of reporting their third-party risk management program produces, 48 percent of respondents cited “reporting to the board.”

Other common types of reporting cited by respondents included key risk indicators (38 percent), third-party performance scorecards (34 percent), and reporting to the senior operating committee (33 percent).

At the bottom of the list, only six respondents said they produce reports on “fourth-party and sub-contracting” risk. Woodbury says it’s not surprising that only a handful of companies produce fourth-party and sub-contracting reports, which would be reporting indicating the impact a third party’s own third parties or sub-contractors pose to the company, given that this is still an emerging area.

As we see companies’ third-party risk manage-

ment programs evolve and reach a level of maturity, “I think we will see those areas evolve, as well,” Woodbury says. “We’re seeing some companies reaching a level of maturity where they are identifying the same critical fourth parties or sub-contractors servicing multiple third parties of the company and, therefore, being identified as a higher risk to the company than some of the company’s own third-party relationships.”

Inventory controls

One surprising finding was that “completeness of inventory controls” didn’t rank higher, “because that is such a foundational element of a program,” Woodbury says. “You can’t assess and manage what you don’t know about.”

That finding might correlate, however, with the 36 percent of respondents who said that “identifying third-party relationships” still poses a challenge.

This could be an indication that some respondents to the survey simply aren’t that sure about what controls they should be putting in place as it concerns the completeness of inventory controls, Woodbury says.

Those controls will vary depending on the types of third parties that the program covers. There is no silver bullet answer or one tool to put in place that’s going to scour your third-party universe. “You have to look in different places,” Woodbury says. “Some of them aren’t always super intuitive.”

Nearly all respondents (96 percent), for example, said they use traditional vendors, such as products and service providers. With traditional third parties, where the company is paying the vendor directly, one area to focus on is payment controls. “You can look at accounts payable, corporate card spend, expense reports, or procurement card spend,” Woodbury says.

THIRD-PARTY CHALLENGES

Challenges facing your firm’s third-party/vendor risk management program (select all that apply):



Sources: Compliance Week; Crowe Horwath

With non-traditional third parties, including revenue sharing or those collecting money on behalf of the company, such as debt collectors, however, you might need to pay closer attention to non-customers paying or sending money to the company. “You may need to look at some of the accounting and revenue recognition processes and follow the money that way,” Woodbury says.

Another survey finding that was surprising, Woodbury says, is the small number of respondents who said they use “internal change-of-use monitoring” (to identify if the company has changed how it’s utilizing third parties). “I expect that’s something we’re going to see shifting over the next few years, especially as new tools and technology come out and companies look for ways to narrow the focus of assessments to drive sustainability,” she says.

Monitoring when a new network communication port is opened or when a request for a physical access badge is requested can help ensure accuracy and completeness of the inventory. “Companies should be asking themselves if they have mechanisms to identify when these things happen,” Woodbury says.

Centralized vs. decentralized

Respondents were also asked which operating model best describes their third-party risk management program. A variety of answers were provided including, but not limited to:

- » Centralized in procurement (21 percent);
- » Decentralized: risk management embedded within each business unit (18.7 percent);
- » Hybrid, with centralized components in procurement (16.5 percent);
- » Centralized in operational risk management/enterprise risk management (15.4 percent); or
- » Hybrid, with centralized components in operational risk management/enterprise risk management (14.3 percent).

Centralizing third-party risk management in procurement may not always be the best option. The tendency in many companies has been a migration

away from having third-party risk management centralized in procurement, Sullivan says. “Often, procurement’s metrics in terms of success are focused primarily on spend and aren’t necessarily aligned to holistic management of risks presented by third parties,” she says.

Just a few respondents said they have a centralized or hybrid model in IT or information security. “There is not a right answer across the board,” Woodbury says. It will completely depend on the company’s size, structure, and the overall maturity of its third-party ERM program, among other factors.

Also, respondents were asked whether the procurement and contracting functions were integrated with the third-party risk management program. Nearly half of them responded that both the procurement and contracting functions are indeed integrated.

However, the second highest number of respondents (21 percent) answered “no” and further said they don’t have plans to integrate procurement or contracting, which could be a mistake. “We’ve seen it works really well and drives efficiencies for many companies that have those functions really well aligned, because procurement and contracting are critical pieces of the third-party management cycle,” Woodbury says.

Overall, survey respondents that rated their third-party risk management programs as most mature commonly utilize procurement, contracting, and third-party risk management technologies. In addition, they tended to incorporate continuous monitoring tools and completeness and accuracy of inventory controls, and they have expanded their programs to cover traditional vendors, non-traditional third parties, fourth parties, and others.

“Third-party risk management is as much about the journey as the destination,” Woodbury says. “It’s important to learn as you go and continue to build upon a solid foundation, increasing your coverage and improving your precision in understanding and managing the risks presented by your third-party relationships.” ■



Compliance clauses can keep third parties in line, regulators at bay

Even small firms have gone global and rely on a broad network of business partners. Those relationships, however, bring with them risks and potential regulatory hazards. **Joe Mont** discusses adding compliance and ethics clauses to contracts.

No organization is an island unto itself. Vendors, distributors, suppliers, sales agents, and other third parties are all part of an extended “family” that will expand its risk profile.

Regulators, in the United States and abroad, are increasingly holding companies responsible for their partners’ problems, with the sins of sub-contractors visited upon the prime. Domestically, the government’s growing focus on money laundering, corruption, bribery, and violations of the False Claims Act enhance the risk of mammoth fines, lost contracts, and personal liability.

A baseline strategy for minimizing third-party risks is the use of compliance and ethics clauses in the contracts that establish ground rules for a business relationship. Drafting effective clauses, and ensuring that everyone adheres to them, was the focus of a recent panel discussion during the annual meeting of the American Bar Association’s Business Law Section in Boston.

The process is not as simple as merely laying out policies on paper. They need teeth, specificity, context, and enforceability.

“One of the really difficult things is how to get your global partners to buy into the fact that they need to comply with some of the United States ethics and compliance laws. We have had particular difficulty when a company puts in very broad language: ‘You will comply with all U.S. laws and regulations,’ ” says Thomas Coulter, head of the law firm LeClair-Ryan’s government contracts practice area. “Their response, ‘I’m not doing that and I don’t know what they are.’ ”

A particular concern for government contractors is escalating enforcement of the False Claims Act, a law dating back to the Civil War that imposes liability on those who defraud governmental programs. “The FCA has really grown and morphed into the government’s secret weapon,” Coulter says.

Government contractors have mandatory disclosure obligations whenever they become aware of credible evidence that an FCA violation (or other ethical lapses or law-breaking) has occurred. “Part and

parcel to that is that you need to implement a rather extensive set of internal controls, so that you have an ethics program and a mechanism for employees to report any impropriety they see,” Coulter says. An expansion of the FCA in 2009 makes the requirement even more problematic.

The law now includes a qui tam provision that allows non-governmental parties, including employees to file actions on behalf of the government and receive a portion of any recovered damages. “That’s really where your company starts to see the FCA in action,” Coulter says.

The end result is costly, up to \$1 million or more in investigation, document collection, and compliance costs, he says. And, aside from actual damages, “it’s the penalties that are the killer.”

He cites a recent case where the settlement included \$14 million in damages, but also penalties in excess of \$350 million because every invoice that contained a request for payment that the government considered invalid added upwards of \$11,000 to the total.

Preventing this expensive problem ties back to the need for ethics and compliance clauses in contracts, extending in-house best practices throughout the supply chain.

“Really, all you can do is have a robust compliance policy and constant training to make sure you have the kind of environment where employees feel that they can talk to their supervisors and utilize the hotline you have to set up,” Coulter says. “You want supervisors who know what the issues are and are constantly monitoring problems. The best thing you can do is know you have a problem early on. You may be in a position where you need to start an investigation, talk to other employees, and get to the government before the employees do.”

What are the goals that guide ethics and compliance clauses? Government expectations help establish the template. For example, guidance on the Foreign Corrupt Practices Act issued by the Department of Justice and Securities and Exchange Commission detail expectations for third-party due diligence

that include exercising audit rights as needed and obtaining annual compliance certifications.

Suggested items to include in a contract:

- » Certifying that no employees or their close family members had been government officials in the past three years;
- » establishing audit rights;
- » the use of an independent monitor;
- » prohibiting bribes and presenting anything of value to a government official;
- » demanding accurate books and records and on-demand compliance certifications;
- » and the right to terminate the agreement and recall funds.

Clauses may also require disclosing business and personal relationships, conflicts of interest, campaign contributions, ongoing or past internal and government investigations, and private settlements.

The ABA panelists suggested that clauses be crafted after a risk-based assessment that addresses the following questions:

- » Do you need to even use a third party?
- » Where is the third party located and what will it be doing for your business?
- » How much due diligence has been executed on the entity?
- » How closely will your organization interact with the third party?
- » What are the applicable laws?
- » What is the length of your relationship?
- » What risk will audit rights mitigate and who will conduct the audit?
- » What is the scope of an audit, and what will you do with any findings?
- » Should you consider required ethics and compliance training rather than inserting a compliance clause?

Questions must also be asked before agreeing to accept contractual clauses. Do you have the means to conduct the due diligence necessary to make the

certifications? Do the disclosures expose sensitive business operations, investigations, or settlements? What will the cost of complying with the requirements be? How invasive and cumbersome will the audit be?

Don't expect that size matters when it comes to government enforcement or the need for compliance clauses. "Many companies incorrectly think they are too small and that FCA investigations only go after the Boeings and Lockheeds of the world," says Margaret Cassidy, founder of Cassidy Law, which specializes in the compliance risks of operating in a global marketplace.

Training is an important consideration and a demand that can be passed to, or facilitated for, third parties, says Fernanda Beraldi, corporate counsel and ethics and compliance director, Latin America, for Cummins Inc.

She recommends "robust clauses to require that employees, distributors, and sales agents" receive necessary compliance training and that the educational programs are certified on at least an annual basis.

Coulter recommends "pre-training," and advising a potential partner that "these are the things you are going to need to do if you want to work with us."

"From an outside counsel and CCO's perspective, it is always easier to say, 'Let's just have one standard and one standard only, and we will make it the highest ethical standard.' Practically speaking, that doesn't work," says Edwin Broecker, a partner with law firm Taft Stettinius & Hollister.

"Avoid the one-size-fits-all mentality," says David Ackerman, chief compliance officer for Sound Income Strategies, a registered investment advisory firm. "That is something everybody tries to default to because it is cheaper, but it is also a way to get into a lot of trouble. Really take a step back, look at the FCA, look at the FCPA, look at the Dodd-Frank Act, and try to generate [clauses] that are consistent across all of these regulations. Then, do your best to train, train, train. The more training you do the greater the likelihood of compliance and the easier it is going to be to point to a specific bad actor as opposed to a systemic problem at the company." ■

Learning to mitigate third-party risks

Many companies struggle with how to achieve full transparency into the breadth and depth of their third parties, exposing themselves to significant risks. **Jaclyn Jaeger** reports.

Most firms by now understand the escalating risks that third parties pose to their business and are ramping up their third-party risk management efforts accordingly. Even still, many struggle with how to achieve full transparency into the breadth and depth of their third parties, exposing themselves to significant legal and compliance risks.

Global companies must closely monitor thousands—if not tens of thousands—of third parties to ensure each one adheres to the company's business practices. It should come as no surprise, then, that many still get stuck on the first step toward effective vendor governance—identifying all the vendors the company uses. According to a third-party risk management benchmark report conducted by NAVEX Global, 11 percent of 321 respondents polled said they still don't know how many third parties they manage.

"As a first step, you've got to figure out who your third parties are," says Randy Stephens, vice president of advisory services for NAVEX Global. "If you don't know who is representing your company, then you cannot possibly assess risk accurately."

This means paying attention to not just traditional third-party relationships—agents, suppliers, distributors, and joint ventures, for example—but virtually anyone who represents the company. These third parties might include consultants, service providers, suppliers' suppliers, dealers and resellers, sub-contractors, and more.

At many firms, different departments, units, and locations all have preferred vendors and suppliers, so it makes sense to pull together an inter-departmental team that includes regional and business lead-

ers—risk, compliance, legal, HR, and procurement, for example—to identify the size and scope of your third-party universe. Assembling an initial inventory of third parties involves leveraging multiple databases from multiple business units.

After compiling a master list, the next step is to separate high-risk third parties from low-risk third parties to better manage the third-party risk management process. Criteria used to assess and rank the risks associated with each third party will vary by company and may include:

- » Country of operation where service is provided
- » Nature of third-party relationship and services provided
- » Type of industry
- » Length of the third-party relationship
- » Degree of involvement with foreign government officials

While many companies are still building a comprehensive third-party risk management program, most (68 percent) are conducting at least basic screening of their third parties prior to engaging with them, according to the NAVEX report. Furthermore, companies that use an outsourced provider to help manage their third-party due diligence programs also reported significantly higher program satisfaction ratings than those who do not.

These ratings apply in multiple areas, including:

- » Compliance with legal and regulatory demands: 78% compared to 65%

- » Ensuring a culture of compliance: 65% compared to 44%
- » Documentation management: 49% compared to 41%
- » Program defensibility: 52% compared to 41%
- » Overall program: 53% compared to 32%

The top external challenge relating to third parties—cited by 51 percent of respondents—is getting them to certify compliance with the firm’s policies. The second and third top challenges were “training third parties on our policies and compliance requirements” and “getting third parties to enforce our ethics and compliance policies in their organizations,” cited by 48 and 41 percent of respondents, respectively.

Stephens recommends selecting a sample of your highest-risk third parties and asking them to provide a syllabus of the types of training they provide. “To the extent that they don’t conduct their own training, provide them with online training,” he says.

An effective third-party risk management program, the NAVEX report stated, should include standardized documentation, recordkeeping methodology, timelines, well-defined expectations in terms of behavior and communications, and an ability to reassess engagements on a continuous basis.

Once a company has mapped out its total universe of third-party relationships, it’s important to continuously monitor third parties to ensure that you are catching and addressing any new risks.

“You don’t want to do that with all your third parties,” says Todd Boehler, vice president of product strategy for GRC software provider ProcessUnity. “You only want to do that with the ones that you deem as posing the most risk to your business.”

Companies generally discover “red flags” or other potentially negative third-party information via multiple channels, but the most common way is through internal due diligence monitoring, as cited by 62 percent of respondents in the NAVEX report.

Ranking second, 41 percent said they discover such issues through regulatory or legal action, “which may indicate that many organizations fail to use screening mechanisms and safeguards,” the report said.

Some third-party risk solutions automate the assessment and monitoring of third parties, screening for issues related to sanction and watch lists, politically exposed persons lists, and adverse media, for example. “It would be very difficult for individuals to look through that amount of data,” says Stephens.

Even when organizations get all of their third parties to certify compliance with their policies, those same organizations go back to square one when new service providers come on board, says Stephens. That’s where an automated process can best serve the companies with respect to monitoring and auditing.

Furthermore, the NAVEX report found that companies that use an outsourced third-party due diligence providers discover more “red flags” or other potentially negative third-party information than those who don’t. They uncovered, for example, more politically exposed persons, government investigations, adverse media reports, and more.

Other avenues of continuous risk mitigation may include performing additional due diligence, exercising audit rights, providing third-party training on topics such as anti-bribery and conflicts of interest, and requesting annual compliance certifications.


One area where there is room for improvement is getting ethics in compliance better aligned with advances in technology, whether that means other parts of the business working closer with compliance, or seeking the help of outside experts to drive analytics. “It’s the biggest challenge, but it’s also the biggest opportunity,” says Don Fancher, national and global leader for Deloitte’s forensic services.

An emerging best practice is tracking and analyzing internal data with external data, including from third-party vendors or third-party suppliers, says Fancher. Those that analyze this combined data can better identify specific risks “not only as they may be happening, or historically as they have happened, but, hopefully, you can actually begin to see predictive scenarios of where risks may emerge,” he says.

By using analytics to predict what risks an organization company may face, Fancher says, “that can go a long way toward averting a bigger problem, or even avoiding a problem altogether.” ■

The international reach of compliance

The challenges facing global compliance programs are only getting more complex, writes **Bill Coffin**, with money laundering, fraud, KYC, sanctions, and cyber-risk leading the way.

n March 9, the International Compliance Association held an Open House in Manhattan to celebrate the opening of its New York office. Founded in the United Kingdom in 2001, the ICA has members in more than 112 countries. It has also become the world's foremost compliance training organization, issuing more than 120,000 compliance certifications globally in concert with the University of Manchester and International Compliance Training, its dedicated training arm.

Pekka Dare, director of the ICT, spoke on the pressing need for compliance training by underscoring the increasingly global scope of major compliance issues such as corruption, money laundering, cyber-risk, and more.

Money laundering. Property has become the safe haven of choice for criminals around the world, Dare noted, with New York and London becoming the top money laundering centers because of their perpetually hot real estate markets. (Separately, both Miami and Vancouver have also seen their real estate markets hijacked somewhat by illicit buyers. This appears to be a trend poised for truly global expansion.) China is the top source for illicit capital outflows by a large margin, with Russia also a major player. Corrupt public officials in both countries are especially fond of investing in New York, Dare said, because it's such a stable, high-priced market. A \$1 billion purchase doesn't exactly stand out in the Big Apple, whereas in Dublin, it will. Plus, there is a large community of professional enablers in New York—lawyers, real estate agents, and even banks—

that are willing to facilitate dirty purchases for bad people. Organized crime loves to legitimize assets, Dare noted, so this problem is definitely not going away any time soon. What is especially important to note is how the international community is trying to respond to the issue, and how compliance officers can be sure that companies in the financial services, legal, and real estate industries don't get caught up in money laundering efforts.

Global issues. The Panama Papers revelation last year is still making waves around the world. The scale of illicit capital and tax evasion brought to light by the hacked documents of Panamanian law firm Mossack Fonseca was truly shocking, Dare said. What is more, it shone a light on persistent compliance problems, such as how many jurisdictions, prevent disclosure of the true ownership or control of companies, making true know-your-customer impossible. Where does the customer really get their wealth from, and how can you, the compliance officer, deal with that? Depending on where the third party is, the truth is, it might not be possible to deal with it fully unless you don't do business with such jurisdictions. Now, it might be tempting to immediately think of oft-maligned offshore destinations such as the British Virgin Islands when thinking about difficulties identifying a third party's ultimate beneficial owner. But according to a recent World Bank report, Dare noted, the U.S. and the UK were tagged as the top jurisdictions for illicit corporate structures.

Sanctions and screening. This is one of the most heavily geopolitical risks a compliance officer can

face, especially in areas of ongoing volatility (such as Russia and the Crimean Peninsula, where political instability is by no means settled; or Iran, where companies have the go-ahead to do business there but banks are simply unwilling to touch the area for fear of accidentally violating still-sanctioned areas of the country's economy). Evolving hazards include technologies such as swift messages, a way to move money instantly from peer to peer without the use of a bank, often through mobile technology such as smartphones.

One of the ways to address this is through technology, since there are steep international rules on maintaining certain levels of information quality on payment messages to spot terrorists or sanctioned individuals. Dare noted how screening technology can spot seemingly innocuous names and words from sanctions lists (such as "Azam," an Iranian ship) on transactions that otherwise look legitimate. Looking closer at those clues can uncover what is, in fact, an illicit payment being made to a sanctioned party that if facilitated completely, would draw in whatever financial center that helped to move the money.

To show how complex that risk can be, Dare showed an example of a transfer scheme originating with the Lebanese Canadian Bank, which at its height was channeling some \$200m a month in a circuit that consistently diverted some of these funds to Hezbollah. The money began its trip in the U.S. in the form of used cars exported to Western Africa, where cash-intensive economies make it easy to convert assets to cash. That money then went to Colombia to buy drugs, which then sent the drugs back to Africa, and from there into Europe for retail sale. The proceeds from the drug trade went back once again to Africa where they commingled with proceeds from the used car trade from the United States. From there, the money, went to a number of financial exchange houses, one of which was Lebanese Canadian bank. As it disperses funds, some of them went into the coffers of Hezbollah, which used them to carry out criminal and terrorist acts. That, Dare, noted, is how a complicated system of otherwise ordinary transfers can easily ensnare a clueless financial institution into a serious third party risk

situation if it is not aware of what to look for, or if it does not have the apparatus in place to check the details of its transactions.

Financial crime prevention. Many of these compliance risks feed into the changing threat of serious and organized crime, which Dare noted is becoming less traditional, less driven by hierarchy, and more cellular in its structure (small groups acting with relative independence to each other, forming a loose network). To protect consumers, themselves and society at large, Dare said, compliance programs are working to better understand the rapidly evolving types of financial crime, as well as to creating a more holistic approach to financial crime prevention to facilitate swifter response to it.

The key to all of this, Dare, explains, is for compliance officers to understand the different kinds of financial crime they are likely to encounter. Financial, corporate, and business frauds, for example, can take form in insurance fraud, banking fraud, bust-out fraud, and mortgage fraud. Electronic crime and data security includes not just protecting physical security of data but also its encryption and how humans come into contact with it. Investigation, prosecution, and recovery requires a human touch to know when something amiss is at hand; a good understanding of criminal psychology can help determine when internal fraud is ongoing, as well as what might be motivating it (greed, a perceived grudge against the company, etc.). And tech risks include a host of new issues including virtual the licensing of cryptocurrencies and the scale of cybercrime.

With so many risks to face, one might be tempted to think that perhaps this is a bad time for compliance, but Dare suggests it is quite the opposite. This is a golden age for compliance programs and compliance officers, he said. Never before have compliance professionals had so much opportunity not just to serve their organizations and protect them against serious risks, but they can help to make the world a better place by preventing and holding back the kinds of new crime that threaten everybody around the world, whether they have a compliance department or not. ■



BUSINESS-DRIVEN SECURITY™

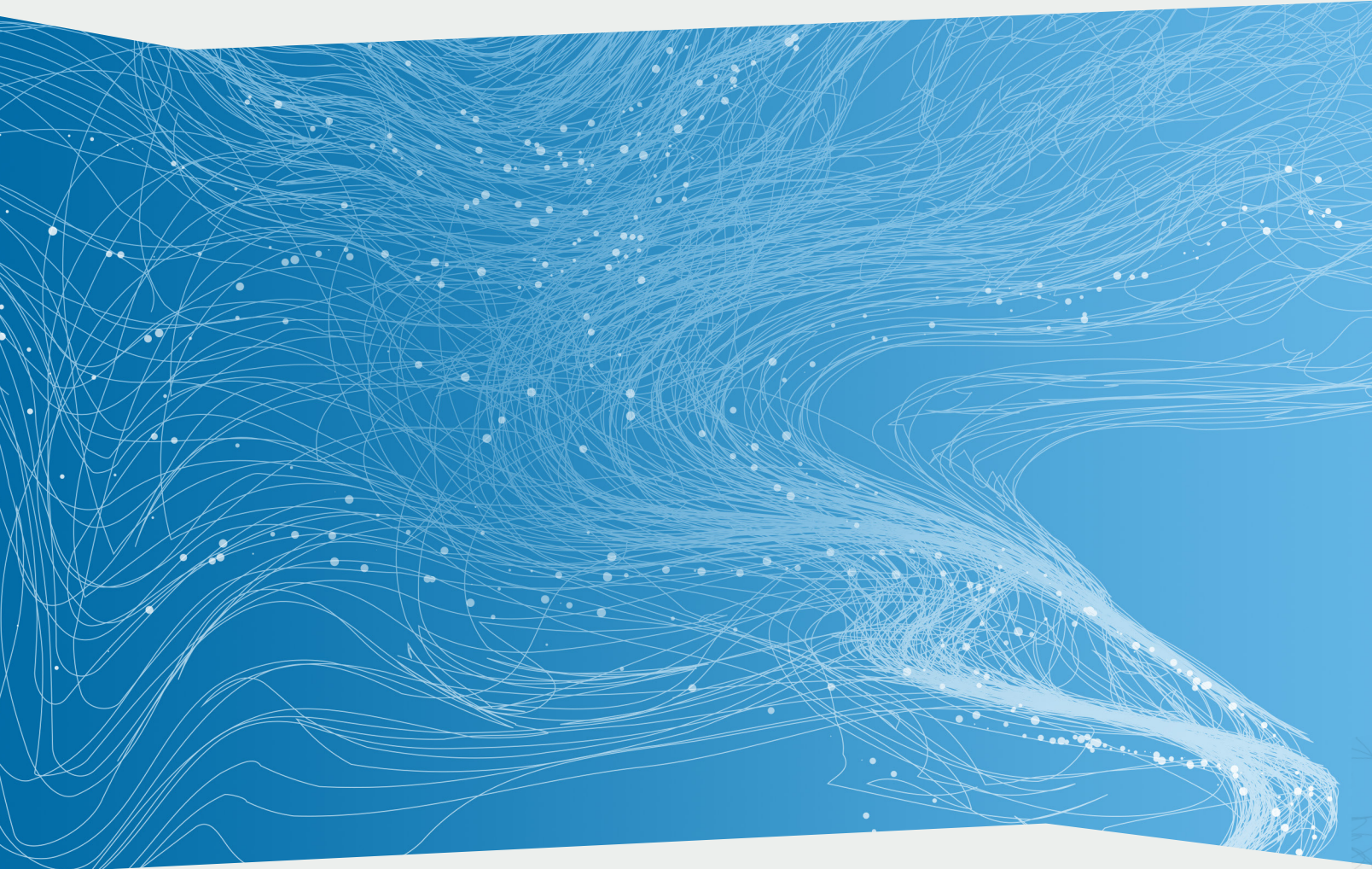
KNOW WHICH RISK IS WORTH TAKING



ARCHER® BUSINESS
RISK MANAGEMENT

Moving forward means not letting risk hold you back. RSA Archer empowers organizations of all sizes to respond to risk with data-driven fact. A single, configurable platform gives you a broad view of your risk management picture so you can implement processes that are right for you, based on industry best-practices. And when you know your risk, you can accomplish just about anything.

rsa.com/risk



WHITEPAPER

BUSINESS-DRIVEN RISK MANAGEMENT CLOSES THE GAP OF GRIEF

GRC CAPABILITIES HELP TRANSLATE
SECURITY RISKS INTO BUSINESS TERMS

OVERVIEW

Evidence is mounting that organizations can reduce the cost of breaches and increase security efficiency by proactively managing risk.

Organizations that hold a legacy perspective of security are at a disadvantage. In response to the latest security threats, these organizations often purchase the latest security gadget or system. For each new threat, there may be a new box. But each box is a security silo. Rather than providing integrated and complete coverage, point solutions create network blind spots, areas where the organization can't monitor user and system activity. So despite these security investments and perhaps even because of them, organizations still find it difficult to put security details in business context in real-time or to respond appropriately when information security vulnerabilities and incidents are identified.

As a result, security leaders are unable to understand and communicate security details as business risk. RSA calls this the "Gap of Grief".

We believe that the solution to the Gap is Business-Driven Security™, an approach to translate security risk into business language that business leaders and Board Members can understand and act upon. Business-Driven risk management in the form of a Governance, Risk and Compliance (GRC) solution plays a major role. In fact, GRC as a concept is at a point of evolution – moving ever closer to the business to truly transform risk management into a strategic enabler. RSA's vision of a Business Risk Management platform takes GRC capabilities into the next generation with the ability to translate any risk into actionable intelligence to improve business decisions. This evolution falls directly in line with Business-Driven Security.

Business Risk Management solutions are about more than security. Security risk is just one piece of operational risk, which is in turn just one piece of enterprise risk. A Business-Driven Risk Management solution provides an accurate, aggregated, and timely view of all enterprise risk – whether that risk is associated with people, processes, technologies, third parties, regulations, or something else – and provides a unified response to any security incident. In other words, it delivers organization-wide visibility, so security and business leaders can work together to proactively prioritize and manage risk.

In addition, Business-Driven Risk Management solutions enable an organization to extract more value from existing security investments by integrating with other systems and using the logs and data they generate.

By understanding and communicating information security in terms of the impact to the overall business, organizations can make better business decisions and more efficiently allocate the human and capital resources that manage information security.

CHALLENGES ABOUND

The world has changed. The attack surface has exploded; no longer do we have a clear, defensible perimeter secured simply by establishing preventative controls. The threat landscape is broader in scope, more sophisticated and targeted and new regulations are emerging around the world.

- **The scope and frequency of attacks continue to grow.**
- **Organizations, executives, and Board Members are increasingly held accountable** for failing to adequately manage information security.
- **Information security regulations are becoming more onerous.** Regulations increasingly focus on the infrastructure on which the information is stored, processed, and transmitted. Fines for compliance failures are growing. In addition, overlapping regulations can differ significantly in their approach to a problem.

THE SECURITY FUNCTION IS NOT SET UP TO WIN

The IT security function, as it exists in many organizations, is not effective.

- Many security teams cannot communicate security risk in a language that business leaders understand.
- This creates a disconnect between security teams and business leaders which leads to poor decisions about how to prioritize human and capital resource investments to protect and manage information risk.
- Many organizations do not fully understand where they have material exposure to information security risk, the significance of the risk, or what is being done to manage it.

INCREASED INTEREST FROM BUSINESS LEADERS

These days, about 70% of Boards of Directors are asking for increased senior executive involvement in risk oversight, according to a survey by the American Institute of Certified Public Accountants (AICPA). (See 2016 The State of Risk Oversight, AICPA.) For large or public companies, that figure is 88%.

In the event of a breach, CEOs and Board Members want to actively manage risk. They want to connect the breach to a system or asset and they immediately want to understand business impact. A Risk Management solution is invaluable in providing the information the CISO requires for those C- and Board-level conversations.

BOARD INVOLVEMENT MAY DECREASE BREACH COSTS

A recent study found that Board involvement reduced breach costs by about \$6 for each compromised personal record. (See 2016 Cost of a Data Breach Study: Global Analysis, Ponemon Institute.) With Ponemon reporting global average number of records impacted by a breach at 23,834, this translates to \$143,000 in savings per breach. Clearly, organizations that communicate security information in terms of business risk are reaping the benefits.

The study also identified many other Risk Management factors that decrease breach costs, including:

- Data governance improvements.
- Formal incident response planning.
- Business continuity planning.
- Mature compliance practices that reduce regulatory examination time and associated fines.

Yet, only one in four respondents in the 2016 AICPA survey felt that their organization had a complete risk management process, showing that although better methods and tools are available, the companies that use them have a clear advantage over 75% of the competition.

SECURITY QUESTIONS FROM BUSINESS LEADERS

Business leaders simply want confidence that their security teams have effective control of security risk.

Frequently-asked CEO questions include:

- Have high priority assets been prioritized for threat detection and response?
- Where is this information handled, stored, processed, transmitted, and archived? How are weaknesses identified, threats detected, and incidents resolved?
- In the absence of controls and risk transfer, what is the likelihood that this important information can be stolen, altered, destroyed, or inaccessible for a period of time? What is the impact to the organization?
- How does our information security risk compare to the organization's other risks?
- Are any of these risks of enough significance to warrant devoting human and capital resources to mitigate and transfer the risk?
- Where significant risks have been identified, are the committed human and capital resources adequate to meet objectives?

- Where technology vulnerabilities and weaknesses have been identified, is the organization prioritizing remediation efforts based on the areas of highest business risk? Who is responsible?
- If an incident occurs, how bad could things get? Can the security team identify which information was breached, by whom, and in what time-frame? What are the potential repercussions?
- How do security risks impact the business? How might security team collaboration with the business improve corporate performance?

If security leaders are unable to clearly and readily answer these questions, business leaders may conclude that investments in technology and people are being spent without understanding the big picture of information security and business risk.

Technical answers, made in the absence of business context, widen the Gap of Grief.

STUCK IN THE GAP OF GRIEF

The benefit of communicating with business leaders is clear. The questions a security team will be asked are known. and yet, the thought of the CEO walking up the hallway pains many CISOs, in part because business leaders have a skewed perspective of how to prioritize risks.

A recent survey of executives found that 59% are concerned with their organization's ability to stay operational following a data breach involving high-value information assets, such as trade secrets and confidential corporate information. (See The Cybersecurity Risk to Knowledge Assets, Kilpatrick Townsend and Ponemon Institute.) However, 53% indicated their senior management's greater concern is a breach involving credit card information or Social Security numbers. Notice the disconnect? For most leaders, protecting consumers from fraud is a higher priority than protecting the organization from threats that could very well force it to close the doors.

These grim facts demonstrate that security leaders with advanced technical knowledge are having a difficult time discussing in straight-forward business terms how to prioritize information security risks, assess the impact of security on organizational strategies and objectives, justify resource expenditures, and encourage business units to mitigate risk.

POINT SOLUTIONS CREATE BLIND SPOTS

Organizations sometimes feel the pressure to respond to a narrow set of threats with a point solution. Because organizations are buying, vendors have obliged with a proliferation of such tools. Although they may perform as claimed against select threats, they create blind spots in networks where user or system activity is not fully monitored.

Without full visibility, many organizations simply can't accurately identify their highest risks. Therefore, security leaders can't deliver risk-based recommendations to the business leaders and Board Members that have fiduciary responsibility to manage risk.

A COMMON BUSINESS RISK MANAGEMENT FRAMEWORK PROVIDES A HOLISTIC VIEW

Often, organizations don't understand the benefits of bringing together their patchwork of security, compliance, and governance efforts into a single Business Risk Management framework that expands governance, risk and compliance activities. Business Risk Management is the next evolution of GRC – a step beyond implementing processes in reaction to compliance requirements towards a metamorphosis of risk management into an enabler of the business.

What exactly is a Business Risk Management platform? It is a set of capabilities that provides a common framework or platform to address three fundamental enterprise needs:

- **Governance.** The manner in which senior executives direct and control the organization.
- **Risk management.** A set of processes used to manage issues that might prevent the organization from meeting its objectives.
- **Compliance.** An organization's efforts to adhere to laws, regulations, standards, policies, and contracts.

A Risk Management solution enables an organization to catalog all elements and their interrelationships to manage risk and compliance obligations in a way that is not just defensive but also energizes the organization's business objectives. These elements may include strategies and objectives, products and service, policies and procedures, authoritative and regulatory sources, business processes and sub-processes, third parties, and IT infrastructure elements (web services, IT software applications, IT systems, databases, and data stores), risks, and controls. In addition, the solution engages deep into the Lines of Business, which are sometimes referred to as "the first line of defense," to better align risk management processes with business operations.

The increased visibility leads to better business decisions, more efficient allocation of human and capital resources, renewed focus on the organization's mission, and peace of mind.

BUSINESS-DRIVEN RISK MANAGEMENT

While no organization can completely eliminate risk, applying Business-Driven Security enables organizations to more intelligently direct limited resources to the security risks that have the greatest business impact. This is the core reason for the shift from GRC to Business Risk Management – to factor business impact into decision-making at a much more detailed level.

Working with security leaders, business executives and Board Members can ensure that risk management is consistent with the organization's risk appetite, adheres to strategies, and meets objectives.

A Business-Driven Business Risk Management solution can enable organizations to:

- Identify critical assets, where each resides, its level of criticality, and how it should be prioritized.
- Assess the level of information risk.
- Understand where to apply limited resources to control information risk, to ensure that organizations are not over- or under-controlling risks.
- Monitor and manage the information risk on an on-going basis.
- Respond to new threats and incidents as thoughtfully and quickly as possible.

RSA'S APPROACH TO BUSINESS RISK MANAGEMENT

The RSA Archer® Suite empowers organizations to manage multiple dimensions of risk on one configurable, integrated software platform. With RSA Archer solutions, organizations can efficiently implement risk management processes using industry standards and best practices, to significantly improve their business risk management maturity.

RSA's approach to Business Risk Management goes beyond event and incident management to establish a risk management foundation. The RSA Archer Suite provides organizations with access to a holistic view of security and business risks so attention can be directed to analysis and strategic problem solving. By improving the quality of information, organizations are improving the quality of their decisions.

The RSA Archer Suite serves as an aggregation point to consolidate governance, risk, and compliance information of any type. It allows technical and non-technical users to automate processes, streamline workflow, tailor the user interface, and report in real-time.

The RSA Archer Suite integrates with a range of other security technologies including point solutions and RSA's other Business-Driven Security Suites.

By leveraging information from existing security systems, the RSA Archer Suite helps organizations get a better return on their existing investments in security technology.

CONCLUSION

Business-Driven Security is an approach to information security risk management that focuses on communicating security details such as risk and incident response in terms that can be understood by an organization's top business leaders.

The RSA Archer Suite is specifically built to support Business-Driven Security. It powers conversations between security and business leaders by providing excellent dashboard views, actionable metrics, and better control.

With the RSA Archer Suite, security risk is depicted in a manner that can be compared with the organization's other risks, regardless of their type or source. This visibility into risks allows security leaders to answer questions from business leaders about security risk, priorities, and incident response. The improved visibility also allows compliance teams to address questions about the organization's compliance posture.

By understanding information security risk, compliance risk, and business risk within a single framework, CISOs, C-Suite executives, and Board Members can make better business decisions and ensure that the organization's objectives are met.

In a new spirit of collaboration, all parties can play a more proactive role in protecting what matters most to the organization.

BUSINESS-DRIVEN SECURITY SOLUTIONS FROM RSA

RSA is a leader in advanced cybersecurity solutions delivering Business-Driven Security™ so organizations of all sizes can take command of their evolving security posture in this uncertain, high-risk world.

Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

More specifically, RSA is the ONLY company that enables the three most critical elements of a sound security strategy: rapid detection and response, control at the user access level, and business risk management. No other company does this.

The **RSA Archer® Suite** empowers organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform.

The **RSA® Fraud & Risk Intelligence Suite** is a centralized fraud prevention platform that uniquely blends continuous monitoring, risk-based authentication and fraud intelligence to deliver rapid insight into cybercrime attacks. Leveraging data from your business and other anti-fraud tools, the RSA Fraud & Risk Intelligence Suite enables organizations to greatly improve detection and response to fraud incidents across digital channels without impacting the customer experience.

The **RSA SecurID® Suite** enables organizations of all sizes to accelerate their business while minimizing identity risk and delivering convenient and secure access to the modern workforce. The RSA SecurID Suite leverages risk analytics and context-based awareness to ensure the right individuals have the right access, from anywhere and any device.

The **RSA NetWitness® Suite** is a threat detection and response platform that allows security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. By aligning business context to security risks, RSA NetWitness Suite provides the most advanced technology to analyze, prioritize, and investigate threats making security analysts more effective and efficient.

ABOUT RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.

The information in this publication is provided "as is." Dell Inc. or its subsidiaries make no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA 02/17 White Paper

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.