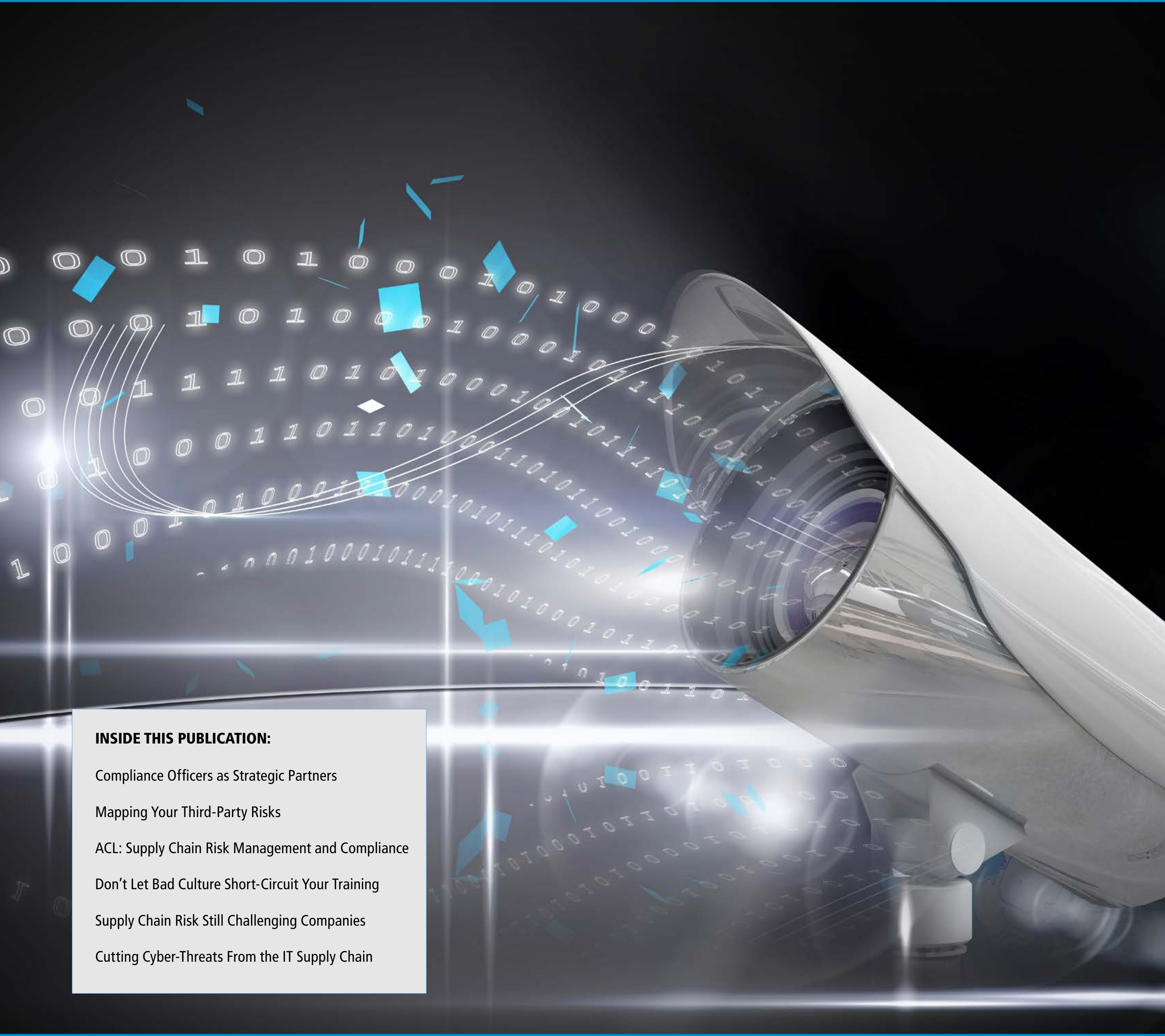
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Shining a Spotlight on

Supply Chain Risk Management

An e-Book publication sponsored by acl
transforming audit and risk

Inside this e-Book:

COMPLIANCE WEEK

Compliance Week, published by Wilmington Group 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.

acl™
transforming audit and risk

ACL delivers technology solutions that are transforming audit, compliance, and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Visit us online at www.acl.com

Compliance Officers as Strategic Partners

A recent report from PwC recommends ways that chief compliance officers can increase corporate strategic value

By Jaclyn Jaeger

One word that many people wouldn't use to describe the job of a chief compliance officer is "sexy," yet the role is quickly becoming one of the hottest positions within companies today.

As the regulatory and legal environment becomes more complex, compliance officers have more influence than ever before to affect corporate strategy and direction. "Who is the C-suite star of the future? We think it's the CCO," says Sally Bernstein, a principal with PwC.

Sounds great, right? One problem: A significant divide still exists between the business and the compliance function. "We often hear business folks say, 'Compliance folks just don't understand the business,' and we hear compliance folks say, 'I wish I could be more involved in the business,' " says Andrea Falcione, managing director in the performance GRC practice at PwC.

Two recent surveys published by PwC underline how pronounced that divide is. According to PwC's 2015 Global CEO Survey, 78 percent of 1,322 chief executive officers named over-regulation as the top threat to growing the business. At the same time, only 35 percent of 1,102 respondents in PwC's 2015 State of Compliance survey reported that CCOs are involved in helping develop or implement corporate strategy.

Given the level of concern senior executives have about the effect the regulatory environment is having on their business, "this is a surprising disconnect," the PwC compliance survey stated. "CEOs should be turning to their CCOs for help in guiding that strategy."

Bernstein

For compliance executives who do participate in developing company strategy, 18 percent of respondents said they assist in the implementation of business strategy once decisions are made, while 15 percent said they address issues that arise after business strategy is implemented. Seventeen percent said they're not at all involved in developing or implementing business strategy.

Compliance officers could also use some guidance in that area. It's not that compliance officers don't want to play a strategic role in the business, Bernstein says, "but they don't have time, and they're not really sure how to do it."

So how, then, can compliance officers move beyond their traditional responsibilities of administering a program that complies with legal and regulatory requirements, toward a more strategic role in the business? "How do you contribute to helping the organization understand how they can manage these issues and still achieve its business objectives?" Bernstein asks.

> "If you bring people in from the business into compliance in a rotational manner, then your compliance function is going to have a better understanding of the business."
>
> Andrea Falcione, Managing Director, Performance GRC Practice, PwC

To help compliance officers answer that question, the PwC report recommends that CCOs increase their strategic value to their organizations in the following ways:

- » Express interest in participating in strategy decisions, and articulate to the CEO the strategic value that compliance can deliver.
- » Review the strategy plan and develop ideas for handling new or unusual compliance risks or for leveraging them to gain competitive advantage.
- » Forge close relationships with key business leaders through the company, and offer insights to help the business identify and mitigate risks related to compliance issues.
- » Define or redefine the scope of compliance across the organization, and build partnerships with compliance owners within the business to ensure that all issues are being managed effectively.
- » Implement efficiency initiatives to improve the effectiveness of the compliance function and reduce compliance-related costs.

"We don't expect the compliance officer to set strategy," Bernstein says. Rather, it's important for the compliance department to be a partner to the business leaders to help them achieve that strategy "versus historically being the Department of No," she says.

Prioritizing Risks

Compliance officers can also play a more strategic role by expanding their focus to include both current and emerging risks. The rising occurrence and cost of data breaches, for example, have increasingly driven many companies to rethink their approaches to managing cyber-security, which traditionally has been managed in a siloed fashion.

In fact, the plurality of respondents to this year's State of Compliance survey (47 percent) cited data security as their number one risk. This finding aligned with PwC's Global CEO Survey, where 61 percent of CEO respondents globally said they are "concerned about cyber-threats," including lack of data security.

These findings are a shift from the last two years of State of Compliance survey results, when compliance executives cited industry-specific regulations (31 percent), privacy and confidentiality (25 percent), and bribery and corruption (22 percent) as their top three risks.

Falcione

The report also found room for improvement in the way that risk assessments are managed. "What we're seeing in this area is a tremendous amount of overlap in terms of the types of assessments that are happening," Falcione says. For example, companies conduct an average of at least six separate compliance-related risk assessments: privacy assessments, ethics assessments, regulatory compliance assessments, and probably many more, she says.

Conducting too many assessments creates "risk assessment fatigue on the part of the business, because they're trying to get business done and drive revenue," Falcione says. Through better collaboration and better coordination of risk assessment activities, "the same people aren't being asked similar questions, or being asked to do similar things from a risk assessment perspective multiple times within a year," she says.

Operational Efficiency

Overlaps or gaps in the ways that companies perform testing and monitoring are another area where companies can help the business improve process efficiency and reduce costs. For example, many dashboards today consolidate data, making analysis easier and allowing broader coverage of testing. According to the report, however, only 10 percent and 6 percent of respondents, respectively, said they fully outsource their compliance testing and monitoring.

The plurality (44 percent) fully outsource hotline intake. Other outsourced activities were compliance training (15 percent), compliance auditing (13 percent), and investigations (10 percent).

"What areas of compliance risk management could you potentially outsource to a third party that could help drive efficiency?" Falcione asks. Companies in highly regulated industries such as financial services and life sciences have been more inclined to outsource these activities. Now, companies in less regulated industries are starting to think about that as a strategy, too, she says.

Moving Forward

As compliance becomes a more strategic partner to the business, the more important it's going to be for compliance officers to develop the compliance function within the business. "There are a lot of different ways for them to be focusing on this, and right now they're not," Falcione says.

One way to develop the compliance role is by encouraging short-term job rotations from the business into the corporate compliance function, which only 13 percent of respondents said they do. "If you bring people in from the business into compliance in a rotational manner, then your compliance function is going to have a better understanding of the business," Falcione says.

Compliance officers of tomorrow will also need more skill sets and experiences than traditionally has been required. "Data analysis experience, technology acumen, business operations experience, industry expertise, and other skill sets and backgrounds that could make the function more well-rounded—and better able to contribute to corporate strategy—are still not as well represented as they should be in today's compliance departments," the report stated. ■

STATE OF COMPLIANCE

The following is an excerpt from the 2015 State of Compliance Survey conducted by PwC.

Be aware of what "compliance" entails across the organization, as well as understand the scope of responsibilities.

The scope of the compliance function can vary significantly from one organization to the next, based on such factors as company size, sector, and culture, but there should be consensus on the definition of scope. Compliance officers and all others in the organization who oversee compliance obligations must not only understand the scope of their own responsibilities but also come to agreement on what compliance entails across the organization—from compliance with legal and regulatory requirements to meeting internal operational and other strategic obligations. Just as chief financial officers know where every dollar is spent but don't themselves spend every dollar, CCOs should know how their organizations manage all compliance obligations and issues throughout the company, even though they don't own all of the compliance responsibilities or mitigation activity.

Coming to an understanding of compliance obligations, where those obligations sit in the organization, and how they get tracked and reported is an important step in maturing the compliance program and enabling the compliance function to add more value to the organization. By understanding who manages which compliance obligations within the business, compliance officers can identify opportunities to add value enterprise wide.

In some sectors (e.g. financial services), CCOs may have a deep understanding of business operations; but in other sectors, CCOs may depend on so-called specialists in the business who have responsibilities to determine that the company is in compliance. CCOs should expect clear explanations from the business about how compliance is being managed and should not accept cursory assurances (e.g. "John is handling it").

Source: PwC.

Mapping Your Third-Party Risks

By Jaclyn Jaeger

Many third-party risk-management efforts start with the goal of providing full visibility over a company's universe of third-party relationships.

The trouble is that many companies still don't have a firm grasp on how to achieve that transparency, or even where to begin, exposing themselves to significant legal and compliance risks. "Companies often underestimate their universe of third parties," Randy Stephens, vice president of advisory services for NAVEX Global, says. Most tend to focus on traditional third-party relationships—such as suppliers, distributors, agents, and joint ventures, for example.

Stephens advises, instead, that they cast a broader net to include anyone who represents the company. These third parties might include suppliers' suppliers, resellers, subcontractors, and more.

Most global companies, however, have thousands—if not tens of thousands of third parties—and all of them must be monitored to ensure they adhere to the company's business practices. To efficiently and effectively get better control over a company's full universe of third-party relationships, the real difficultly is to "take that population of third parties and get it down to a manageable number," Graham Murphy, a principal in KPMG's U.S. forensic advisory services practice, says.

Stephens advises starting with a plan. Pull together an inter-departmental project team that includes regional and business leaders, as well as any country representatives, he says.

Next, identify the size and scope of your third-party universe—a task much easier said than done. "Most businesses procure services in a decentralized way," Walter Hoogmoed, a principal with Deloitte, says. Without any sort of master list, assembling an initial inventory of third parties involves leveraging multiple databases from multiple business units.

Develop a Matrix

Once you've gathered that master list, you'll want to separate high-risk third parties from low-risk third parties in order to more easily manage the third-party risk-management process, depending on which risk the company wants to focus on most. "If you want to concentrate on the FCPA, for example, you may want to eliminate domestic suppliers," Murphy says. "You should look at your third-party risk mitigation program as a part of your anti-bribery and anti-corruption program."

Criteria used to assess and rank the risks associated with each third party will vary by organization and may include:

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

Third parties that pose the greatest risk from an anti-bribery and corruption standpoint are those that have regular interaction with foreign government officials. "Because a company has political connections, it doesn't mean you don't do business with them; it may just mean you want to put processes and controls around that so you don't run afoul of anti-corruption laws," Murphy adds.

Another consideration when vetting third-party risk is to consider how frequently you use that particular third party. "You may want to eliminate those entities that you haven't done any business with over the last few years," Murphy says.

Triaging third parties helps set the wheels in motion for

ELEMENTS OF THIRD-PARTY RISK MANAGEMENT

Randy Stephens, vice president of advisory services for NAVEX Global, recommends a few basic steps toward developing an effective third-party risk management program.

Identify/Prioritize: Identify your universe of third-party relationships and prioritize by risk. Cast a broad net and include anyone who represents your company, especially those who have regular interaction with foreign government officials. Don't limit your search to suppliers, agents, and distributors.

Assess: Conduct due diligence on a risk-adjusted basis; uncover and assess risks. The FCPA Resource Guide states that the degree of appropriate third-party due diligence "may vary based on industry, country, size, and nature of the transaction, and the historical relationship with the third party."

Mitigate: Take steps to mitigate risk that was uncovered. This means checking multiple sanction lists, adverse publicity, the extent to which the third party might have relationships with foreign officials, and more.

Monitor: Even if your due diligence process did not turn up any red flags or issues with your existing or newly on-boarded third parties, resist the desire to close the book. Continuous monitoring and periodic re-screening is necessary to identify risk events, keep information current, and ensure policy compliance remains in force.

Source: Randy Stephens, NAVEX Global.

how much due diligence to perform on each third-party relationship moving forward. “Based on the inherent risk of that relationship, you might do more rigorous control testing,” Hoogmoed says. For some third parties, a due diligence questionnaire might suffice, whereas others might require on-site audits, he says.

Then determine who actually owns the risk. Who is purchasing from that third party? Who is approving payment to that third party?

“Every line of business has some sort of procurement, operation, or relationship manager that deals with third parties on a day-to-day basis,” Hoogmoed says. “The business manager that runs the business process should own the risk and be accountable for the exposure associated with that third party.”

Remediation Measures

Once a company has mapped out its total universe of third-party relationships, the next step is to continuously monitor third parties to ensure that you are catching and addressing any new risks.

Many companies still perform this task on an ad hoc basis. “They don’t have a process in place to address third-party risk from a holistic standpoint,” Murphy says. “A lot of companies, for example, are managing the process on Excel spreadsheets, and it becomes very difficult to manage from that perspective.”

Conducting risk management from a manual process standpoint makes it difficult to capture all third parties and the level of risk that each one poses. As a result, Murphy says, “a lot of companies right now are looking to technology-enabled solutions and putting systems in place to really help take them from a manual process to an automated process.”

Some third-party risk-management solutions automate the assessment and monitoring of a company’s third parties, screening for issues related to sanction and watch lists, politically exposed persons lists, and adverse media, for example.

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. “You may decide to, in the worst case scenario, terminate the relationship,” Murphy says.

In addition, companies should conduct a thorough onboarding process when going through a shift in business operations, or a merger or acquisition. A company that is expanding into an emerging market, for example, will want to ensure that it understands all the permits and licenses needed to build new facilities in that region. “Where you can run afoul of the law is by having an agent or third party do a lot of the gathering of that information for you,” Murphy says.

“Companies can outsource the function, but they cannot absolve themselves of any responsibility,” Murphy adds. “So you want to make sure agents and those acting on your behalf have a good reputation and prior experience.”

The risks associated with third parties will continue to grow more prevalent as more multinational companies turn to third parties. According to a third-party risk report conducted by NAVEX Global, 92 percent of more than 300 respondents indicated that they would either increase the use of third parties over the next year, or weren’t sure. Only 8 percent expected to reduce their reliance on third parties.

An effective third-party risk-management program doesn’t require an unlimited budget or sophisticated tools, but it does need to be reasonably tailored to the company’s level and type of third-party risk. By not monitoring third parties, and failing to document due diligence processes, companies expose themselves to significant legal, financial, and reputational risk. ■

RISK-BASED DUE DILIGENCE

Below, NAVEX Global outlines how firms should assess third parties.

For myriad financial and flexibility reasons, companies are relying more and more on third parties. The recent waves of [Foreign Corrupt Practices Act] enforcement actions demonstrate that third parties are often the source of inappropriate payments under the FCPA. The FCPA Guidance makes it clear that a risk-based due diligence process will be considered when assessing the effectiveness of a company’s compliance program. Luckily, “... the degree of appropriate due diligence may vary based on industry, country, size and nature of the [third party] transaction, and the historical relationship with the third-party ...” So one size doesn’t have to fit all, but you need to have some level of documented risk-based due diligence commensurate with your risk.

Some of the issues that might be considered red flags:

- Industry
- Corruption Index for the country in which the third party is operating
- Large size or sensitive nature of the transaction
- No history of past relationship with the third party
- Abnormally high commission or compensation
- Lavish gifts and entertainment expenses
- Third parties making unexpected, unreasonable, or illogical decisions
- Unusually smooth processing of matters where the individual does not have the expected level of knowledge or expertise

Source: NAVEX Global.

Supply chain risk management and compliance

Simplifying a complex process

By John Verver, CPA, CISA, CMC, Strategic Advisor to ACL

For many organizations, the entire supply chain process is becoming increasingly complex and time-consuming to manage. In some cases, and particularly in some industries such as manufacturing, there is often a massive and intricate web of third-party entities involved in providing components, sub-components and services. Failures in the supply chain can have a disastrous impact on financial performance as well as corporate reputation.

There are many different types of risks that can cause damage if improperly managed, including those relating to non-compliance with ever-increasing regulations. Just consider the impact that quality issues like defective airbags or ignition keys have had on many auto manufacturers. The total costs of recalls, liability claims, fines and penalties, as well as the damage to brand and future sales, have become staggeringly large.

The combination of supply chain risks such as supply continuity, component quality, use of child labor, conflict minerals legislation, bribery and corruption, environmental damage and product toxicity—when spread across thousands or tens of thousands of suppliers and sub-suppliers and other third parties—is daunting for any risk manager to consider. And that's just in manufacturing.

Almost every industry has its own complicated version of supply chain and third party risks. Moving beyond the initial stages of the supply chain also means considering the risks related to distribution of goods and services through wholesalers and distributors that complete the chain of supply through to the customer.

Of course, the importance of effective supply chain risk management (SCRM) and compliance is generally well understood by those responsible for the area, as are the primary activities involved in the process. The challenge is: how do you make this into a process that works well and consumes the least amount of time and resources?

In many organizations, SCRM processes have evolved over time to reflect new business lines and products, as well as new regulatory requirements. Many processes are supported by systems that have grown in a haphazard way, using a combination of manual procedures, spreadsheets and certification processes, often spread across various corporate silos and regions. Producing one overall corporate view of the status of SCRM and the extent of risk involved, consistently and reliably, may just not be feasible using homegrown tools and techniques.

The opportunity for many organizations that find themselves in this situation is to re-think and simplify processes, making them more consistent and dependable. These processes should be driven by technology that is not only designed for this purpose, but also can do things, such as continuously monitor activities and risk indicators, which are not practical with older tools and techniques.

Transforming SCRM

There are various ways that current technology can support this transformation in supply chain risk management and compliance, by better supporting key stages. The following are some examples of the ways that the technology can be used to organize and connect the entire SCRM process:

Identification of risks

The challenge is to comprehensively identify risks throughout the supply chain, categorize them in a consistent way, and show the inter-relationships and dependencies among risks. These risks include risks relating to regulatory compliance failures. SCRM should normally be one major part of an overall risk management process within an organization. So, risks should also be capable of being categorized and included among a broader set of enterprise and functional risks. Trying to manage all of this through systems of spreadsheets is inevitably an inefficient, unreliable and frustrating process.

Supply chain risks are not static, and an additional component of creating a complete risk universe is the identification of new risks. Data analysis technologies can play a key role in identifying new risk trends and indicators. For example, supplier shipments can be tracked against POs to detect increasing delays in meeting delivery dates for critical product components, as well as increasing instances of sub-standard quality.

Risk assessment

As a consistent risk universe is established and maintained by risk owners throughout the supply chain process, an assessment process takes place. This is usually based on determining probability and extent of impact and takes into account aspects of corporate risk tolerance. The assessment also takes into account the nature of the controls in place to mitigate risks, together with ongoing assessments of control effectiveness.

The practical challenges of using traditional techniques in this process are significant. For example: trying to not only keep on top of what controls are in place to address compliance risks for regulations such as conflict minerals, employee health and safety, environmental protection and FCPA, but also how the extent of risk is impacted when weaknesses are detected in the effectiveness of controls.

SCRM technology simplifies the process by specifically linking the risks to related and over-lapping controls, including instances where multiple controls and risks are inter-linked. The results of automated monitoring of activities to assess control effectiveness can also be tied directly back to risks to provide updated assessments.

Controls

The design and description of control processes is critical to determining whether they are effective and can be understood by control owners and those involved in audit and compliance reviews. Control systems can include automated routines that prevent or flag transactions and activities that are likely to be damaging.

As with many other aspects of risk management and compliance, there are increasing numbers of external control and compliance frameworks that can be used to support the design and implementation of controls. By using software to manage and connect items identified as applicable within the specific controls' framework, it is easy to get a comprehensive view of how external requirements are being addressed.

Surveys and certification

Obtaining and collating responses from control owners based on questionnaires and certification sign-off is typically a very resource-intensive process and full of delays. Automation of this process through technology can dramatically reduce the effort involved, not only in timely collection of responses but also in the analysis of the types of responses. Common use cases for this could include, for example, individual employees confirming their understanding of sanction lists and that relevant controls have been tested to determine that no business takes place with vendors on a list.

Monitoring

Ongoing monitoring of supply chain control effectiveness is usually very difficult to achieve when wholly dependent on manual testing and review activities. Big data analysis technologies increasingly play a key role in SCRM monitoring, using a combination of tests designed to provide indicators of control breakdowns, together with predictive and statistical analytics that identify potential risks for which no controls currently exist.

A lack of effective monitoring is often where SCRM process break down in practice, since even the best-designed controls are often ignored or circumvented, for a variety of reasons.

Investigation and issues management

A common area of breakdown in SCRM processes is the response to problems and control exceptions that are revealed through monitoring processes. The questions are often around who is responsible for addressing an issue, the status of follow-up, and how much risk exposure exists from delays in response.

Current technologies provide workflow capabilities so that, for example, individuals receive emails informing them of issues that need to be addressed. A failure to respond appropriately within a given time period results in an escalation of an issue, so that a more senior manager is automatically notified.

Reporting

One of the biggest challenges of using traditional spreadsheet or other homegrown SCRM system is getting an overall insightful overview of the state of supply change risks and the ways they are being managed.

This is where a well-integrated technology driven approach produces large, highly visible benefits. Visual and quantified dashboards provide senior management with reliable, consistent assurance and understanding whenever needed.

Integration into ERM

While it is important to be able to look at the entire SCRM process holistically, it is also important to be able to put it into the context of enterprise-wide risk management. Achieving a truly enterprise-wide approach to risk management can itself be an overwhelming undertaking. While the process challenges can be great, they are surmountable when driven by technology.

For many organizations it makes sense to be able to manage supply chain risk management and compliance using the same basic processes and technology that drive risk and compliance in other areas of the organization. This, of course, allows senior management and the executive suite to gain a broad view of corporate and organizational risk management—and to see where SCRM fits into the overall picture.

Technology helps keep things simple

As with any aspect of risk management, the basic steps of an SCRM process themselves are not particularly complicated. What makes things complicated is the volume and detail of issues to address, and all their inter-connections, as well as managing the process and people's roles in an efficient way. As with any critical business process area that is being transformed and now driven by the right technology, it's hard to imagine how SCRM can become a really manageable process without taking a technology-driven approach.

The question for many organizations is how long to continue to make do with an SCRM system that has been patched together over the years. Consider at what point it makes sense to invest in an integrated technology-driven approach that can dramatically reduce the resource burden of managing supply chain risks. ■

Don't Let Bad Culture Short-Circuit Your Training

NAVEX Global says 37 percent of 677 ethics and compliance professionals think "employee cynicism about culture change efforts" is the top training threat

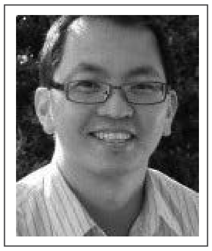
By Jaclyn Jaeger

A compliance training program is only as strong as the corporate culture for which its stands upon, and yet several cultural-related concerns that threaten to undermine training program effectiveness continue to persist.

According to NAVEX Global's 2015 Ethics and Compliance Training Benchmark Report, 37 percent of 677 ethics and compliance professionals polled said the top threat to training program effectiveness was "employee cynicism about culture change efforts." Close behind was fear of retaliation, at 35 percent.

"When there is disconnect between the message and the reality, cynicism will fester and grow," says Ingrid Fredeen, vice president of online learning content for NAVEX Global. "Distrust is much more present in an organization where actions are not aligned with the words."

Even if a company has a perfectly polished Code of Conduct and says it prohibits retaliation, nothing triggers employee cynicism in the workplace more than when supervisors and middle manager don't practice what they preach. Disconnect can be created when supervisors mishandle or downplay complaints or employee allegations, for example; that perception is supported by the findings of the survey: 26 percent of ethics and compliance professionals cited it as a concern.


Lin

The findings suggest that companies may not be doing as good of a job as they believe in getting middle managers to embody the message that their company doesn't tolerate retaliation. That means they must keep reinforcing the message, says Jimmy Lin, vice president of product management and corporate development at The Network. "You're not going to see overnight success," he says.

Middle managers who don't demonstrate ethics and compliance behaviors also add to employee cynicism and serve as a barrier to effective compliance training. "They should be visibly modeling values-based behavior," says Marsha Ershaghi Hames, practice leader of education solutions at LRN. Middle management misbehavior was a concern cited by 34 percent of ethics and compliance professionals in the NAVEX survey.

Another factor that can undermine compliance training efforts is when "disciplinary measures are inconsistent or non-existent," which 32 percent of ethics and compliance professionals cited as another top threat to training program effectiveness. Employee cynicism is "a symptom of a culture that either isn't saying the right thing, or is saying the right thing but not supporting it," Fredeen says.

Senior leaders also play an integral role. "Tactics such as linking performance ratings, promotions, and pay to corporate values are a step in the right direction, but senior leaders must also provide appropriate executive level support for the program and hold middle managers accountable," the NAVEX report said.

Senior leaders can also foster corporate culture by playing a "very visible role not only in talking the talk but walking the talk," Ershaghi Hames says. That means finding opportunities to insert themselves into the conversation and "not just be a formal talking head—really make themselves approachable and integrated into day-to-day dialogue of the business."

Ethics and compliance professionals who responded to the survey likewise stressed the importance of senior leadership engagement. Nineteen percent said that when senior leaders don't communicate the importance of the company's values, that also threatens to undermine compliance training effectiveness.

> "When there is disconnect between the message and the reality, cynicism will fester and grow. Distrust is much more present in an organization where actions are not aligned with the words."
>
> Ingrid Fredeen, VP of Online Learning Content, NAVEX Global

One hallmark of an effective training program is a "deliberate focus on the culture," Ershaghi Hames says. "Employees have to feel like there is a consistent and authentic commitment to the program."

Training Engagement

The good news, the report finds, is that most ethics and compliance professionals want to foster a healthy corporate culture—how to get there is what perplexes them. When asked to force-rank their top ethics and compliance training objectives, for example, a plurality of respondents (46 percent) cited "creating a culture of ethics and respect" as their top objective, followed by complying with laws and regulations (37 percent).

To achieve that objective, however, a check-the-box training program will not suffice. "They need to look for training that is engaging, informative, that is helpful and relevant—not just the least expensive, easiest, most simplistic solution on the market," Fredeen says. Whether they're building a compliance training program or buying one, she says, "they have to look for something that will really resonate with employees."

One compliance training tactic that many companies are adopting today is awareness campaigns on social media platforms like Jive, Yammer, or Chatter to foster ongoing, dynamic discussions online, including internal discussions about integrity and compliance topics. "It's not just about trying to shove training in someone's face," Lin says. It's about creating conversations that naturally become part of the culture of the organization, he says.

Employees should also be involved in the training. "If employees don't feel engaged enough in the conversation and in the topic, if the subject matter isn't really relevant to them, that also can make it very challenging for the training to have any kind of impact on their behavior," says Pat Harned, chief executive officer of the Ethics and Compliance Initiative, an information resource for ethics and compliance officers. "Having employees talk about situations that have happened to their peers, things that have actually happened in their company, makes it more real for them."

Harned

Focus groups are another way to include employees in a positive way and avoid one-way conversations, Ershaghi Hames says. Questions to ask employees during those focus groups, could include, "Do you feel your manager is approachable? Do you feel you can communicate openly without fear of retaliation?" Answers to those questions will help paint a clearer picture of the corporate culture, she says.

Many companies are now also establishing "speaking up campaigns," Ershaghi Hames says. In one particular case, for example, a company began to notice through its employee engagement survey that trust levels in leadership was dropping.

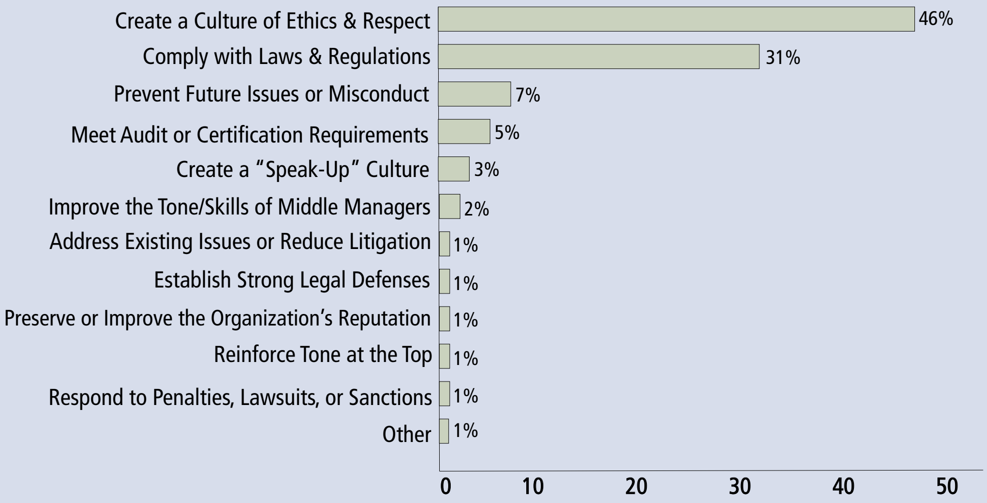
To get to the bottom of why this was happening, LRN helped the company develop a campaign "to take the concept of speaking up and speaking out on the road," Ershaghi Hames says, and directly to the employees of their manufacturing plants. What they found was that by talking openly about anti-retaliation and the importance of speaking up through focus groups and interviews where the issues existed, managers learned more than they ever would have through a campaign strategy developed at corporate, she says.

Through that experience, Ershaghi Hames says, the company was able to develop more targeted awareness around anti-retaliation: why it's important to culture, how to collaborate and communicate more cohesively, and how it's connected to their Code of Conduct. "By connecting a lot of this back to the business, it became more integrated in the day-to-day 'how we live and what is our purpose,' " she says.

Culture is one of the biggest factors that drives employee behavior and employees' perception of a company's culture. So it's important that both senior and middle management alike can maintain the company's message that unethical or non-compliant behavior will not be tolerated. Being consistent, fair, and responsive to employee concerns will go a long way toward mitigating employee cynicism and foster a strong ethical culture. ■

TRAINING OBJECTIVES

Respondents to NAVEX Global's 2015 Training Benchmark Report were asked, "Which Ethics and Compliance Training Objective Is Most Important for Your Organization?" Their responses are below.



Source: NAVEX Global.

Supply Chain Risk Still Challenging Companies

While 90 percent of respondents to a survey on supplier compliance have a supply chain compliance program, nearly 50 percent still had incidents of supplier non-compliance

By Joe Mont

Rare is the business these days that can afford to be cavalier about the regulatory scrutiny on its supply chain. Rarer still is the enterprise not working hard to gain more visibility into its extended family of vendors and suppliers.

But are they doing what needs to be done effectively and efficiently?

A recent survey of companies by MetricStream on managing, measuring, and monitoring supplier compliance found that even though more than 90 percent of respondents have a supply chain compliance program in place, nearly 50 percent have still suffered from recent incidents of supplier non-compliance.

Even a single slip-up can be disastrous in the current regulatory environment. Bank regulators have made abundantly clear that financial institutions bear responsibility for the actions and deficiencies of the third parties they use. Federal and state laws regarding conflict minerals, human trafficking, and child labor affect the manufacturing sector and beyond. Activist scrutiny, customer concerns, reputation risk, and class-action lawsuits are all unwanted supplements to an enforcement action.

How do non-compliant vendors and suppliers still manage to fall through the cracks? The reasons vary. Many are globally disparate and have suppliers of their own—and those fourth or fifth parties can still haunt you directly. Companies may also focus on immediate regulatory priorities (conflict minerals, for example), while neglecting broader issues. Others may have such a fractured, siloed system of vendor management that a holistic view of risk is nearly impossible.

Stephens

"Doing nothing is not an option," says Randy Stephens, vice president of advisory services for NAVEX. "No matter how challenging it is, you need to find ways to break it down into its component parts and get started."

Ditch the Paper

The complexity of the third-party universe means that overseeing your supply chain manually is virtually impossible. Still, says Gary Barraco, senior director of supply chain solutions for Amber Road, a provider of global trade management software, nearly 50 percent of the manufacturing companies he talks to manage their vendors with spreadsheets, Word documents, or even e-mail.

GRC software vendors abound, eager to help companies automate their processes, but Barraco finds it can be useful to let personnel hold onto their spreadsheet security blanket, configuring a back-end system that can seamlessly import and export data into those documents.

There are strategic benefits to moving away to manual processes. "Upstream visibility helps with downstream proactivity," Barraco says. Tracking a vendor's suppliers, for example, can let a company keep tabs on its inflow of raw materials, flagging discrepancies that could lead to a shipping delay. Transparency into supplier capacity levels can also raise red flags. If a vendor's capacity is 100,000 units per year and your company's order is for 150,000, questions need to be asked about where the remainder of the units are coming from and who they are outsourced to.

Get Everyone at the Table

At many companies, different departments, units, and locations all have preferred vendors and suppliers. A proper risk assessment needs to consider a company as a whole, not the sum of its parts, even if that might initially lead to conflicts.

> "If you get your due diligence back and everything looks great, with green lights all across the board, that itself might send you a red flag. Don't rely completely on the process; still apply common sense and question things your instincts tell you don't make sense."
>
> Randy Stephens, VP of Advisory Services, NAVEX

"You may always have people in your organization who will argue that they need to use their guy," Stephens says. "A compliance officer needs to be able to stand up to them and say they can use them, but they need to be able to demonstrate the same rationale and same due diligence process applied to any undertaking with a third party. They are gong to have to demonstrate a business need and that they don't add risk, just like anybody else."

Stephens recommends that each external vendor be assigned an in-house point person for oversight. "That person knows they are going to be on the hook if somebody gets out of line," he says.

Convening the entire team helps everyone understand the need for evaluating, monitoring, and establishing policies and controls for vendors both new and old. "Get in a room with the stakeholders in your company and whiteboard out where all the potential third parties can exist," Stephens advises. Although most data can be gleaned from accounts payable information and internal databases, this exercise will help fully map the supply chain and provide the opportunity to rationalize their third parties and eliminate duplicate services.

> "Regulators are going to ask how well you really have your arms around your supply chain and vendor chain. The wrong answer is going to lead to a more egregious audit and examination."
>
> Sean Cronin, VP of Field Operations, ProcessUnity

Think Like a Regulator

When engaging in third-party management, "think and act like a regulator," says Sean Cronin, vice president of field operations for GRC software provider ProcessUnity. That requires a focus on established standards, controls, expectations, and demands for transparency.

"That's what the regulators are really looking for, because you cannot avoid vendors that may have ulterior or bad motives," he says. "Regulators are going to ask how well you really have your arms around your supply chain and vendor chain. The wrong answer is going to lead to a more egregious audit and examination. You want to show that you are managing this process proactively and are self-policing."

Be a Diplomat

Organizations may need to be difficult with unresponsive or recalcitrant vendors, but a little bit of diplomacy can go quite a long way to build the sort of relationship you want. "Years ago, the model would have been to go in and say, 'You work for me, I'm going to tell you what to do, and if you don't like it I'm going to stop doing business and go somewhere else'," Barraco says. "If you keep doing that you will eventually run out of places to source from."

Just as compliance officers have had to convince their companies to view them as a useful ally rather than an obstacle, supply-chain management needs to adopt a similar mission statement. "The best way to remediate health and safety issues is not to just go in like a bull and say you are taking over," Barraco says. "Go in and say you are there to help and work with them. Nine times out of 10, the factory would love to have the same compliance standards and operate properly."

Trust, but Verify

As always, use a risk-based approach to judging your vendors and business partners. "It's not the people you have dealt with for years and years and have a great relationship with who are likely to cause you a problem," Stephens says. "It is going to be someone that you haven't had a great relationship with, or haven't had a long-term one. That's where you have to apply your risk assessment process."

"You don't have to do the same level of due diligence for each third party," he adds. "If you have a domestic supplier who works for a lot of companies, you might have a lower level of due diligence expectations than a new third party you are adding in a country with a high fraud index rating."

Stephens other advice is that you learn to always trust your gut. "If you get your due diligence back and everything looks great, with green lights all across the board, that itself might send you a red flag," Stephens says. "Don't rely completely on the process; still apply common sense and question things your instincts tell you don't make sense." ■

AVOIDING WEAK LINKS

Below, the Open Compliance & Ethics Group details best practices, and what to avoid, when assessing supply chain risk.

KEYS TO SUCCESS

- » Identify every link in every supply chain, the roles they play, and the risks associated with them.
- » Use a code of conduct, policies, and training to promote awareness of supply chain risk and understanding of required conduct for both employees and parties in the supply chain
- » Select the right technology platform and due diligence partners to build risk intelligence
- » Identify, evaluate and manage risk consistently across and throughout all supply chains, using a standard approach to risk ranking and prioritization.
- » Continually monitor and evaluate the supply chain risk management capability.

COMMON MISTAKES

- » Addressing only a small subset of parties in the supply chain, and then failing to manage even these based on risk ranking.
- » Failing to do business continuity planning.
- » Having inadequate communication between management and personnel involved
- » Allowing activities that reduce supply chain transparency.
- » Not considering consolidated impact.

Source: OCEG.

Cutting Cyber-Threats From the IT Supply Chain

By Jaclyn Jaeger

The longer a global supply chain grows, the less visibility and assurance corporations have into the integrity and security of their products and operations. Now NIST is trying to pierce that fog, and compliance officers in the private sector might want to take notice.

Earlier in April the National Institute of Standards and Technology issued its latest guidance, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"—a 282-page missive on how to better manage the supply chain for technology products, to root out cyber-threats that might leave a piece of IT equipment compromised or simply malfunctioning. NIST's guidance is intended for government agencies acquiring lots of IT and communication technology, but the principles behind it are just as useful elsewhere.

"Every organization relies upon technology, whether it's in their manufacturing processes, their products, or services, or if it's to enable their business activity," says Jon Boyens, a senior adviser for information security at NIST and co-author of the guidance.

In today's globalized world, the components of a laptop or a cellular phone, for example, are routinely manufactured in many different locations, while assembly of the final product may take place in yet another part of the world. Now imagine how much more complex that supply chain becomes for a much larger system, such as the avionics in a commercial airplane or a communications network for the military.

"Each access point into the technology, which ultimately is assembled into one product or service, creates risk," Boyens says. Hackers might try to embed malicious software within those components, or poorly trained workers might just assemble a bad part. Either way, the threats to the supply chain are many, and the final result is the same: an untrustworthy product, that you might not even know exists.

"Cyber-supply chain risk management is still a fairly nascent discipline," Boyens says. "I would say it's where traditional supply chain risk management was about 15 years ago. It's still developing."

> "Cyber-supply chain risk management is still a fairly nascent discipline. I would say it's where traditional supply chain risk management was about 15 years ago; it's still developing."
>
> Jon Boyens, Senior Advisor for Information Security, NIST

Risk Management

One part of the guidance describes three tiers of risk management to help organizations integrate ICT supply chain risk management (yes, there's an acronym for that: ICT SCRM) effectively. They are:

Tier 1: Organization. In this tier, the organization's executive leadership team defines the company's overall ICT SCRM strategy, policies, goals, and objectives. These activities "help to ensure that ICT SCRM mitigation strategies are cost-effective, efficient, and consistent with the strategic goals and objectives of the organization," according to the NIST guidance. This organizational tier is also responsible for establishing a risk tolerance level for ICT supply chain risks.

Senior leadership support is "non-negotiable," says Jennifer Bisceglie, president and CEO of Interos Solutions, a consulting firm that works on supply chain risk management. It must be connected to the business objective, she says, or leadership will not support it.

At the organization tier, another step is to establish a team with roles and responsibilities for leading and supporting ICT SCRM activities. "We advocate a team-based approach," Boyens stresses. The specific functions that may be involved in managing ICT supply chain risks can include compliance, risk, legal, IT, supply chain and logistics, acquisition and procurement, and other relevant functions, he says.

Tier 2: Mission/business process. This tier is responsible for developing actionable policies and procedures, guidance, and constraints. In this tier, program requirements are defined and managed, and they might include cost, schedule, performance, and a variety of critical non-functional requirements—such as reliability, dependability, safety, security, and quality. "Many threats to and through the supply chain are addressed at this level, in the management of trust relationships with system integrators suppliers, and external service providers of ICT products and services," the guidance states.

SUPPLY CHAIN GOALS

Below are several key strategies recommended by NIST when implementing a supply chain risk management program.

As a starting point, NIST recommended four goals to keep in mind while developing an SCRM plan:

- Manage, rather than eliminate risk;
- Ensure that operations are able to adapt to constantly evolving threats;
- Be responsive to changes within your own organization, programs, and the supporting information systems; and
- Adjust to the rapidly evolving practices of the private sector's global ICT supply chain.

Source: NIST.

Tier 3: Information system. This tier is where ICT SCRM activities are integrated into the system development lifecycle of information technology systems and system components. "Many threats through the supply chain are addressed at this level, with the use of ICT SCRM-related information security requirements," the guidance explains.

Reducing ICT supply chain risks should be an enterprise-wide effort. "Generally, senior leaders provide the strategic direction, mid-level leaders plan and manage projects, and individuals on the front lines develop, implement, and operate the ICT supply chain infrastructure," the guidance states.

After these three tiers have been established, ICT SCRM should be integrated into enterprise-wide risk management processes by implementing the following steps:

» **Frame:** Establish the context for risk-based decisions and the current state of the information system or ICT supply chain infrastructure.

» **Assess:** Review and interpret severity, threat, vulnerability, likelihood, impact, and related information.

» **Respond:** Select, tailor, and implement mitigation controls once a risk has been identified.

» **Monitor:** Monitor risk on an ongoing basis, including changes to an information system or ICT supply chain infrastructure, using effective communications and a feedback loop for continuous improvement.

Any company that's trying to implement supply chain risk management best practices can use the NIST guidance as a framework, although the exercise will always involve lots of effort and attention. "This does not negate the need for each organization to take the time to review their internal policies and processes to see where they might be introducing vulnerabilities into their operations, or accepting risk from their supplier base and partners," Bisceglie says.

Furthermore, Boyens says that the guidance is meant to complement, rather than replace, existing standards and guidelines, such as CoBIT 5.0 or ISO 27000. "Our risk management processes are consistent with other risk management processes in terms of identifying, assessing, and managing that risk," he says.

Because technology supply chains differ across and within organizations, those risk management plans "should be tailored to individual organizational, program, and operational contexts," the guidance stresses. Tailored plans will "help organizations to focus appropriate resources on the most critical functions and components based on organizational mission/business requirements and their risk environment."

"We need to change the workflow from reactive to proactive," Bisceglie says; supply chain risk management should be a process, rather than a compliance checklist activity. ■

MULTI-TIERED RISK MANAGEMENT

Below is an excerpt from the National Institute of Standards and Technology's guidance, describing the three organizational tiers that make up information and communication technology supply chain risk management (ICT SCRM).

To integrate risk management throughout an organization, [NIST SP 800-39] describes three organizational tiers ... that address risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. ICT SCRM requires the involvement of all three tiers.

Tier 1: Organizational level. In general, Tier 1 is engaged in the development of the overall ICT SCRM strategy, determination of organization-level ICT SCRM risks, and setting of theorganization-wide ICT SCRM policies to guide the organization's activities in establishing and maintaining organization-wide ICT SCRM capability.

Tier 2: Mission/business process level. Tier 2 is engaged in prioritizing the organization's mission and business functions, conducting mission/business-level risk assessment, implementing Tier 1 strategy and guidance to establish an overarching organizational capability to manage ICT supply chain risks, and guiding organization-wide ICT acquisitions and their corresponding SDLCs.

Tier 3: Information system level. Tier 3 is involved in specific ICT SCRM activities to be applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' [development life cycles].

The ICT SCRM activities can be performed by a variety of individuals or groups within an organization, ranging from a single individual to committees, divisions, programs, or any other organizational structures. ICT SCRM activities will be distinct for different organizations depending on their organization's structure, culture, mission, and many other factors.

It should be noted that this publication gives organizations the flexibility to either develop stand-alone documentation (e.g., policies, assessment and authorization plan and ICT SCRM plan) for ICT SCRM, or to integrate it into existing agency documentation.

The ICT SCRM process should be carried out across the three risk management tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication, thus integrating both strategic and tactical activities among all stakeholders with a shared interest in the mission/business success of the organization. Whether addressing a component, a system, a process, a mission function, or a policy, it is important to engage the relevant ICT SCRM stakeholders at each tier to ensure that risk management activities are as informed as possible.

Source: NIST.