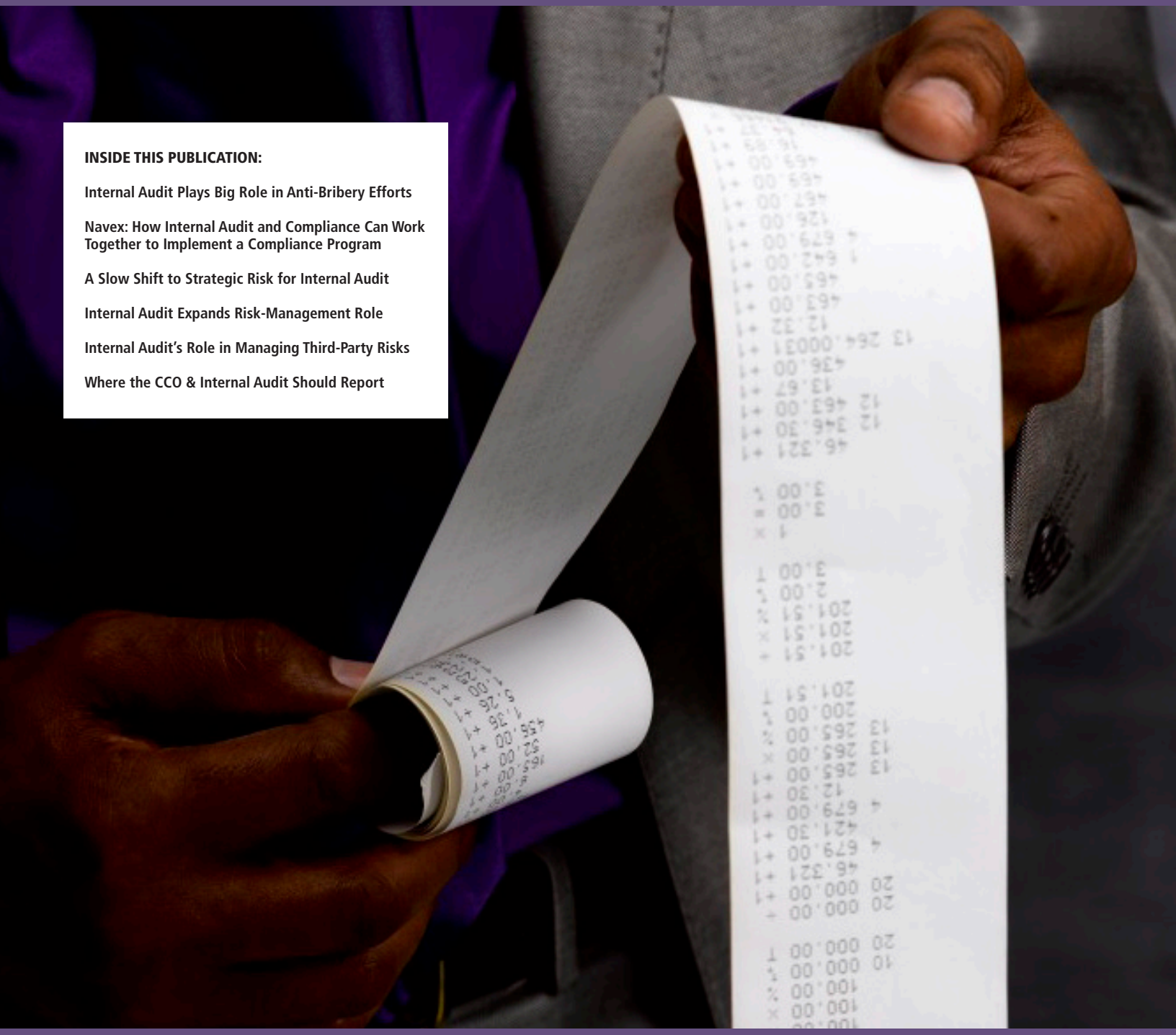
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

The Future of

Effective Internal Audit

An e-Book publication sponsored by NAVEX GLOBAL™ The Ethics and Compliance Experts

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 quickly become one of the most important go-to resources for public companies; Compliance Week now reaches more than 26,000 financial, legal, audit, risk, and compliance executives.

NAVEX GLOBAL™
The Ethics and Compliance Experts

NAVEX Global is the trusted global ethics and compliance expert for more than 8,000 clients in over 200 countries – the largest ethics and compliance community in the world. We provide a comprehensive suite of software and services to manage governance, risk and compliance (GRC), providing critical cross-program insights thorough unmatched expertise and actionable data. More information can be found at www.navexglobal.com.

Learn more about NAVEX Global by following us online: @NAVEXGlobal, YouTube, LinkedIn, Facebook and Google+.

Inside this e-Book:

Internal Audit Plays Big Role in Anti-Bribery Efforts

By Jaclyn Jaeger

As companies continue to push into global markets and regulators intensify scrutiny of risk-management practices, internal auditors are playing a greater role in evaluating and mitigating bribery and corruption risks.

"Bribery and corruption are top risks for many companies," says Princy Jain, a partner in PwC's risk assurance practice. Because of the regulatory focus on anti-corruption and more companies expanding globally, "we've seen greater need over the last couple of years for involving internal audit in the anti-corruption compliance process," he says.

Regulators have noticed that need, too. The Justice Department and the Securities and Exchange Commission have turned up the heat on internal auditors when it comes to their role—or lack thereof—in anti-corruption compliance programs.

In the past, one of the first questions asked by regulators when a fraud was uncovered was, "where were the outside auditors?" says Raymond Sloane, a director at consulting firm Berkeley Research Group. "More frequently that question is now coupled with, 'where were the internal auditors? Why didn't they catch this?'"

Where internal audit can add the most value to anti-corruption compliance programs, say risk-management experts, is on the front-end by helping senior management establish the risk-assessment process at a strategic level.

Specifically, internal audit can aid executive management in identifying and prioritizing the risk areas that need the most attention, the likelihood and significance of those risks, and how to go about designing an anti-corruption program that is proportionate to the company's risk appetite and business strategy, says Stephen Arietta, vice president of internal audit for United Online.


Arietta

"Internal audit is in a unique position to have visibility into the various operations of a company," Arietta says. "So when you're assessing corruption risks, internal audit can really lead the facilitation process for the conversations being held with senior management."

Still, internal audit will have to make some adjustments to transition to assessing bribery risks. For example, the amount of the bribes may not always be material, a key consideration in traditional auditing, but could still present a potential violation, says Sloane. Thus, the cost of an investigation into potential improper payments could be disproportionate to the amount of the alleged payments, "so what we see are companies enhancing their audits in these areas," he says.

"The more you can do up front and the better a job you can do with your training and communication, the better off you're going to be in the long-run," says Charlie Wright, vice president of internal audit at Devon Energy. "It's all about being proactive and setting up processes and procedures and training and communication—making sure all those things are in place."

Compliance & Internal Audit Teaming Up

Because every company has its own unique structure and culture, the role of the internal audit function differs significantly from company to company. At some companies, for example, internal audit works directly with the risk-management team.

At Ryder System, internal audit co-chairs the enterprise risk-management program with the compliance group, "and we use that as an offshoot for our audit plan for the year," says Cliff Zoller, senior vice president of audit services for Ryder. Compliance and audit also jointly train both employees and third-party agents in their local countries on the company's code of ethics and on acceptable behavior, he says.

At Devon Energy, the compliance group establishes the compliance program and internal audit reviews the operating units to ensure compliance with the company's policies. "We're in a little bit of a unique situation at Devon because we've recently divested most of our international properties to be able to invest more in our North American operations," Wright says.

The internal audit function also adds significant value in helping their companies monitor compliance with anti-corruption compliance programs, whether that involves "performing certain audits in certain countries, or looking at certain data trends on a periodic or continuous basis," Jain says.

At Ryder, for example, internal audit spends roughly 25 percent of its time on continuous auditing of the locations of its largest operations, says Zoller. On a quarterly basis, internal audit requests to see a listing of all accounts payable activities that took place in those countries, which are then closely scrutinized for any potential type of facilitation payment, he says.

"You can't look at every transaction; it has to be a risk-based approach based on areas of the world where the company operates," says Sloane. What the regulators want to see is that the testing of the program by the internal audit function is focusing on those areas most vulnerable to bribery and corruption, he says.

In the event that a violation is discovered, internal audit must alert senior management or "report it directly to the audit committee or board of directors," says Sloane.

> "Internal audit is in a unique position to have visibility into the various operations of a company. So when you're assessing corruption risks, internal audit can really lead the facilitation process for the conversations being held with executive management."
>
> Stephen Arietta, VP of Internal Audit, United Online

In the event of an investigation, internal audit needs to keep in mind that their reports are going to be closely scrutinized, "so it's important that if issues arise they see them through to their logical conclusion," says Sloane. "They need to make sure they're identifying red flags that represent potential corruption areas and are following up."

A robust internal audit function will consistently monitor management's remediation efforts on any weaknesses and follow up on their status. Internal audit should "remain independent from the implementation of any of those remediation efforts, but reviewing it and assessing it from a design perspective is appropriate," says Arietta.

In the event of a government investigation, internal audit can help identify issues, accumulate data for the government, and identify whom to interview. Collaboration is an important component of any investigation related to corruption issues, ensuring that "each subject matter expert play their particular role," says Zoller.

Because allegations of bribery and corruption are particularly sensitive, internal audit has to be objective in their review, says Jain. "They have to take into consideration all facts and circumstances."

In any investigation, issues of attorney-client and work-product privilege must be carefully considered also. "It's important, where internal audit is involved in assisting in the internal investigation, that they do so at the direction of, and report to, general counsel or external counsel," says Sloane.

Zoller

Increasingly, when companies settle a probe, they're tasked with conducting their own reports assessing the compliance program. "If a company has its own self-assessment and reporting requirements, that's going to put additional responsibility on internal audit to prepare those reports," says Sloane, particularly since "one of the things regulators look for are any reports that were issued by the internal audit group on the problem area." ■

ROLE OF INTERNAL AUDIT IN FCPA CASES

Below are examples of FCPA cases where the Justice Department and the SEC have cited alleged internal audit failures and successes.

Examples of FCPA cases where the Justice Department and SEC have cited internal audit failures:

- *SEC v. Biomet* (2012): Biomet's compliance and internal audit functions failed to stop improper payments paid to doctors in Argentina, even after learning about the illegal practices. "Executives and internal auditors at Biomet's Indiana headquarters were aware of the payments as early as 2000, but failed to stop it."
- *SEC v. Oracle* (2012): Oracle "failed to audit and compare" distributor margins against end user prices to "ensure excess margins were not being built into the pricing structure." In addition, Oracle "failed to seek transparency in or audit third-party payments made by distributors on Oracle India's behalf."
- *SEC v. Eli Lilly* (2012): Eli Lilly's audit department had "no procedures specifically designed to assess the FCPA or bribery risks of sales and purchases."

Examples of FCPA cases where the Justice Department and SEC have credited internal audit:

- *U.S. v. BizJet* (2012): "following discovery of the FCPA violations during the course of an internal audit of the implementation of enhanced compliance related to third-party consultants ..."
- *SEC v. Pride International* (2010): "during a routine audit, Pride International discovered an allegation of bribery ..."
- *SEC v. Statoil* (2006): "Statoil's internal audit department reported to Statoil's [CFO] that Statoil had paid $5.2 million under a consulting agreement to an entity that had not been named in the contract ..."
- *SEC v. Chiquita Brands* (2001): "Chiquita's internal audit staff discovered the payment during an audit review ..."

Sources: SEC; Justice Department.

How Internal Audit and Compliance Can Work Together to Implement an Effective Compliance Program

By Randy Stephens, JD, CCEP

As most executives know only too well, many companies are facing increasing scrutiny and expectations from a broader range of stakeholders than at any time in the past.

That intense focus makes enterprise risk management ever more critical. Governments around the globe have become more prescriptive in their ethics and compliance standards, as well as more sophisticated in distinguishing between true compliance initiatives and those that exist primarily to fulfill regulatory obligations— that is, "tick the box" compliance practices.

Consider the recommended approach to deterring bribery and extortion found in the OECD Guidelines for Multinational Enterprises. It advises companies to, "Develop and adopt adequate internal controls, ethics, and compliance programs or measures for preventing and detecting bribery, developed on the basis of a risk assessment addressing the individual circumstances of an enterprise … Such individual circumstances and bribery risks should be regularly monitored and re-assessed ..."

Another example comes from the U.S. Federal Sentencing Guidelines for Organizations, which states that companies need to promote a culture that encourages ethical conduct. It goes on to say that a company's "compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct."

Along with government entities, a wider range of stakeholders—from customers to suppliers to employees to communities— now demand accountability and transparency from the businesses with which they're affiliated.

Compliance and Audit's Natural Partnership

Given these shifts in the business environment, as well as the critical roles both compliance and internal audit play in managing enterprise risk, it increasingly makes sense and improves company compliance for internal audit and compliance to work more closely together. Collaboration between the two functions can help drive a culture of ethical behavior and compliance and also provide management with a more comprehensive, thorough view of the risks a company faces.

Compliance and internal audit share several characteristics that can facilitate a close working relationship.

1. Both disciplines require objectivity and independence and the ability and willingness to report potential misconduct and identify any gaps in the internal control measures.

2. Both must focus on risk and recognize that their performance is critical to the company's ability to achieve its goals.

3. Finally, collaboration between compliance and internal audit can also lead to efficiencies, as the two areas can share expertise and resources.

Compliance sets policy, provides training, and develops controls. After the compliance department identifies critical compliance key performance indicators (KPIs), they partner with internal audit to ensure monitoring for those KPIs. These audits may identify compliance failures which need to be addressed through investigations, policy revisions, or new training.

Third-Party Risk: The Achilles Heel

One area in which a close relationship between compliance and internal audit can pay off occurs when companies engage third parties. In today's global world, it's not unusual for many organizations to engage third parties such as: partners, joint ventures, independent contractors, offshore service providers, and distribution networks, among other entities, many of which span the globe.

What's more, companies risk significant reputational and legal damages from any revelations of compliance failures or abuses within these third-party networks. In fact, fully 90 percent of 2012 enforcement actions by the Department of Justice involved companies' third parties

Compliance professionals can take several steps to mitigate the risks inherent in working with third parties, including supplier codes of conduct, training, and periodic audits of their operations. It is also important to ensure that business representatives within their own organization— that is, the ones actually dealing with the third parties—are ultimately responsible for ensuring that these parties are aware of and comply with the companies' expectations.

Accurate, ongoing monitoring of third

parties can be difficult. The information needed to undertake an effective monitoring effort usually is scattered across different business units. Given other responsibilities, employees may struggle to dedicate great amounts of time to staying abreast of continually evolving third-party information and continually evolving regulations.

To work within these constraints, compliance organizations can use technology, such as NAVEX Global's Third-Party Risk Management solution, to develop central repositories of information on third parties, conduct initial onboarding assessments and ongoing monitoring of third parties, and identify and escalate those considered higher risk. Automating these tasks allows compliance professionals to focus their resources on the third parties that warrant greater analysis.

Internal audit can play an important role here as well. They can examine the process around third-party due diligence, including onboarding and contract execution, checking for any omissions or weaknesses in the processes. They can also selectively audit major transactions to or from third parties, such as payments and reimbursements, ensuring compliance or identifying compliance control failures.

Reputation Damage Control

The rise of social media means that a simple Tweet, video, or Facebook post involving your company can quickly rocket around the globe. If, for instance, a video depicting what appears to be poor working conditions in a manufacturing plant goes viral, or revelations surface in chat rooms or cable news about a senior executive who falsified his or her credentials, a company's reputation and sales likely will almost immediately plummet. This often occurs even if the questionable conditions or behavior is at a third-party supplier, reseller, or other affiliate. Unfortunately, few organizations are prepared for a rapidly moving crisis that requires a coordinated response from various corporate functions.

Containing this risk typically involves several steps. One is putting in place an internal reporting process that requires prompt escalation of allegations involving senior executives or that could cause serious financial or reputational harm to the company. Employees and business partners should be provided with clear instructions on the actions to take, including whom to alert, should they come across such information. Perhaps more importantly, the compliance department can let employees and others know that they shouldn't respond with retaliatory posts or comments of their own.

To test preparedness to react to events which could result in damage to a company's reputation, companies can conduct annual crisis management drills. Along with compliance, participants typically will include board members, senior leadership, investor relations, public affairs, and corporate communications.

This is where internal audit can partner with compliance in developing crisis management protocols and reviewing the drills, employing Business Process Improvement (BPI) analysis to identify ways to improve the response process.

Ethics and Compliance Training

Compliance organizations also need to identify high-risk employees and ensure they receive instruction on such topics as import and export controls, trade restrictions, technology transfers and, of course, bribery and corruption.

Again, the audit area can be of value by working with compliance to identify training KPIs and auditing training completion to ensure that the proper training occurs and is documented.

Some Independence

While the benefits of a close working relationship between audit and compliance are compelling, these two functions still require a measure of independence. Compliance is a management function; as with most other management functions, it needs to undergo regular auditing itself. In most organizations, that job will fall to internal audit.

Even so, collaboration and coordination between the two areas can enhance both board members' and management's ability to understand all the risks to which a company is exposed, and the actions underway to mitigate their exposure. In addition, working together allows both departments to make the most of their resources.

These benefits are critical, given that the pressure from regulators and other stakeholders wanting to ensure that companies are not just complying with applicable regulations, but also are acting ethically is unlikely to let up any time soon. Indeed, it's more likely to increase.

At the same time, many corporate budgets remain tight. By working together, compliance and internal audit can more cost-effectively meet these demands. ■

A Slow Shift to Strategic Risk for Internal Audit

By Tammy Whitehouse

The latest data on the state of internal audit suggests the profession has heard the news that it is facing new expectations to take a higher-level view of risk and control, but it is still retooling to live up to them.

According to a Thomson Reuters study, internal auditors say they are beginning to shift their attention and resources toward strategic risks but are still heavily bogged down in the basic financial controls and assurance over financial reporting. "This looked globally at the internal audit function, and it confirmed on a global spectrum what we tend to see in the United States," says Warren Stippich, national partner on governance, risk, and compliance for Grant Thornton. "Internal audit departments are generally moving in the same direction, but at different speeds."

Roughly 80 percent of 1,100 internal auditors surveyed said assurance of internal controls consumes the majority of the department's time and resources, with IT security and risk and legal and regulatory risk ranking just below, and those numbers didn't drop significantly from the prior year. Yet internal auditors also say they are placing greater importance on areas like fraud and corruption risk, monitoring activities, and strategic risk management.

Susannah Hammond, senior regulatory intelligence expert at Thomson Reuters, says internal auditors are being asked to carry on with the assurance over financial controls as they have over the past decade or so, but also to pile on some new duties with respect to strategic risks, such as corporate governance, the quality of an organization's culture, and tone at the top. The problem, she says, is internal auditors are still trying to learn to operate in those new areas.

"Those are significantly softer areas," she says. "Where is the rulebook associated with effective corporate governance? It's a judgment call as to whether management is effective or not, and that's a really big change for internal audit."

Jason Pett, leader of U.S. internal audit services for PwC, says the Thomson Reuters findings are consistent with other recent survey findings that suggest internal auditors are working on meeting a new mandate from regulators, boards, and industry leaders—but they're still working on it. "Internal audit functions desire to move into higher-risk, higher-value areas," he says. "What's holding them back is capability. They continue to wrestle with first identifying what those bigger, emerging risks are, and then aligning their skills to meet the organizations where they are."

Carolyn Saint, vice president of internal audit for 7-Eleven, says she sees internal audit functions in many organizations working to define what is strategically relevant for the organization, then trying to determine what will hinder a company's ability to achieve its strategic objectives. At 7-Eleven, for example, some key relevance factors are the fact that the company operates under a franchise model, and it is growing. "So what are the initiatives that support growth and support the franchise model?" she says. That takes the company down the path of identifying the risks that might derail its strategies.

> "Where is the rulebook associated with effective corporate governance? It's a judgment call as to whether management is effective or not, and that's a really big change for internal audit."
>
> Susannah Hammond, Senior Regulatory Intelligence Expert, Thomson Reuters

Bill Watts, partner in charge of internal audit for Crowe Horwath, says he sees internal auditors looking for ways to become more forward looking, even as they continue to focus the majority of their time and resources on "bread-and-butter" areas, such as assurance of compliance, financial controls, information technology, and other similar pursuits. "We know we need to move toward a practice that is focused on continuous monitoring, being more proactive and not reactive," he says. "The question is how do we build on that?"

Tom Harper, executive vice president and general auditor at Federal Home Loan Bank of Chicago, says one of the biggest challenges facing internal auditors is the ambiguity associated with taking that kind of approach. "We are asking internal auditors to look at things where there isn't a framework to follow," he says. "Nobody has set out the controls that have to be in place. Instead, we're trying to look at what might go wrong

or look at regulations that may or may not be implemented. That's much harder for people in the audit profession to deal with. They're used to those very black and white, bright lines."

Making Strides

There's cause for optimism, though, according to many internal audit experts. Pett believes the profession is on the right track. "When you are focused on something you tend to make progress, but it's hard to move quickly," he says.

Saint believes the profession could make great strides if it focused some effort on leveraging resources internally and communicating more closely with other risk and control functions inside the organization. She points to some recent guidance from the Institute of Internal Auditors that tells auditors in the trenches to think about how specific duties are assigned and coordinated within organizations. The model advocated by the IIA would provide a straightforward and effective way to enhance communications on risk management and control by clarifying essential roles and duties. "I really think people will start getting behind that model," she says. "Given that resources are always scarce, how do you better leverage what's happening inside the company?"

To be sure, internal audit has a lot of work to do. The study noted only 9 percent of internal auditors believed their organizations had mature risk-management processes. John McLaughlin, a partner at BDO USA, says companies would be wise to put more emphasis on increasing their capabilities to address risks. "You have to listen to management about what's on their mind and what they're seeing on a day-to-day basis," he says. "Then you have to incorporate that perception of risk into how is it best to monitor that risk. Having a comprehensive monitoring capability extends beyond what the internal audit function may have."

Stippich expects that internal audit will continue a gradual migration toward emerging, bigger-picture risks as they continue addressing the skills issue. In certain skill areas—such as IT, engineering, treasury, commodities, and environmental—it's difficult to entice the right talent to join the internal audit cause. Some companies are coping by rotating their operational professionals into the internal audit area, but that has limitations as well. "It's a struggle if you don't grow up with an audit mindset," he says. "The documentation is pretty intense." ■

RISK MANAGEMENT

Below are some results from the Thomson Reuters survey in regard to companies' risk-management function.

Just [more than] 50 percent of respondents felt that the risk-management function in their organization ranged from implemented (but requires additional work and resources) to robust and embedded; 9 percent of respondents felt that their organization had a robust, mature risk assessment program, with a further 41 percent saying that while a system had been implemented, it needed some work. This left nearly 20 percent of respondents who felt that their organizations had immature risk assessment processes.

Australasia (62 percent) and Europe (57 percent) felt that their risk-management functions ranged from implemented (but requires further work and resources) to robust and embedded. Africa (39 percent) recorded the weakest responses in this area with Asia (47 percent), South America (47 percent), and North America (50 percent) also recording low scores.

The survey results showed that 9 percent of respondents' time was spent on strategic-level risk management (a decrease of 1 percent from 2012). Process-level risk management registered 30 percent of respondents' time, again a decrease on 2012 results. Whereas 36 percent of respondents felt that strategic-level risk management should be one of the top three internal audit priorities for the next year, with 26 percent highlighting process-level risk management, 36 percent felt that strategic-level risk management should be one of the top three priorities for the board in 2013.

Across the regions the percentage difference between those internal auditors who were already spending time on strategic-level risk management and those who felt they should be spending more time was consistent. The lowest desired increase was in the Middle East, where 25 percent of respondents felt they should be spending more time on strategic-level risk management. This was followed by Europe (26 percent), Asia (27 percent), Australasia (29 percent), North America (30 percent), and South America (31 percent).

Source: Thomson Reuters.

Internal Audit Expands Risk-Management Role

By Tammy Whitehouse

The role of internal audit continues to evolve. New requirements from Nasdaq and the Federal Reserve will put increased demands on internal auditors, as they continue to grow out of their traditional tick-and-tie roots into more risk-focused watchdogs and advisers.

Nasdaq has proposed through the Securities and Exchange Commission to require that its listed companies establish an internal audit function by the end of 2013, whether they staff it internally or outsource it entirely. The idea is to assure that listed companies have a process to review and assess internal controls regularly, identify weaknesses, and remediate as necessary. "The rule is also intended to make sure that the listed company's management and audit committee are provided with ongoing information about risk-management processes and the system of internal control," Nasdaq writes in its proposal.

The proposal came on the heels of a policy statement from the Federal Reserve establishing a new baseline for the internal audit function at any financial institution under its purview with more than $10 billion in assets. The Fed's policy says internal audit departments should go beyond the primary function of auditing internal controls to also provide some "enhanced practices" within their overall processes.

Those enhanced practices include things like analyzing the effectiveness of risk management, looking at a higher level at "thematic macro control" issues that might be missed through traditional audit tactics, challenging management to develop appropriate policies and procedures, scrutinizing infrastructural changes, monitoring the board's and management's compliance with their own stated risk tolerances, and evaluating governance. "What the Fed has articulated here in some ways are leading practices," says Richard Chambers, CEO of the Institute of Internal Auditors. "These are two developments that indicate stakeholders are stepping up their expectations of internal auditors."

The Federal Reserve policy statement also says chief audit executives should report functionally to the audit committee and administratively to the CEO. If a CAE reports to someone other than the CEO, the audit committee should document a rationale and explain its plan for assuring the CAE's independence under that reporting arrangement, the policy says. "That could push even more chief audit executives to report to the CEO even outside of banking," says Chambers. "We've been saying this for some time."

Jonathan Feld, a lawyer with law firm Dykema, says he sees reporting structures rising into higher management ranks. "They need to have the ability to go to these people and address them when the need arises," he says. "What had been something of a staid profession is becoming a more proactive profession."

The IIA and other internal audit groups have been calling on the profession in recent years to equip themselves to meet rising expectations, Chambers says. The most progressive internal auditors have moved on from their focus on financial controls required by the Sarbanes-Oxley Act and faced new expectations and responsibilities for addressing risk in the aftermath of the financial crisis and recession. "Now the regulatory and listing bodies are stepping up as well," he says. In Chambers' view, the requirements in the Federal Reserve policy statement will set a standard for many public companies. "There are several requirements in there that will make their way out of the financial services community," he says.

Still, internal auditors in the trenches see plenty of resistance on the part of management to elevating—and in some cases even having—internal audit functions. Bill Hagerman, a career internal auditor who in 2009 started his own consulting firm, WH Solutions, says companies still widely see internal audit as a "necessary evil." Companies such as those listed on Nasdaq establish internal audit functions only when explicitly required to do so, he says.

John Fraser, senior vice president of internal audit at Hydro One Networks, says improvements in governance are generally not made voluntarily. He puts the Nasdaq and Federal Reserve initiatives in the same category as such mandates contained in the Foreign Corrupt Practices Act, SOX, Dodd-Frank, and others that established minimum requirements. "It will not be perfect at first, but will become the norm for the better of governance," he says. Some firms will "hire token internal audit staff at first," he says. Some of those internal auditors will add value, expand their scope, and eventually their boards and audit committees will see the benefit, he says.

Surveys and studies by several organizations, including the IIA, PwC, Protiviti, and Grant Thornton, have found that the recession-era freeze on resources available to inter-

nal audit departments is finally thawing, and it's just in time to enable internal audit departments to invest in technology and staffing to meet new demands.

The IIA study, for example, says internal audit departments will have more budget and more staffing available to them in 2013 than in any year since the financial crisis. The PwC study concluded that internal audit departments need to stretch themselves to increase their performance and add greater value.

"Internal audit functions are being challenged to elevate their game," says Tom Lawless, a partner in the financial services office at Ernst & Young. Internal audit's use of technology, especially data analytics and data mining, are big areas where internal audit can invest and do more, he says. "I'm not sure anyone has gotten it completely right yet with data analytics," he says. "That's one area that continues to evolve."

The focus on thematic audits is also getting more attention, he says, a point raised in the Federal Reserve policy statement. "Look at thematic control issues across the entire organization," Lawless says. "If you have an issue in New York in the Americas, does it also exist in Asia or in Europe? Is it a thematic problem across the organization?"

Warren Stippich, a partner at Grant Thornton, sees increasing interest around streamlining audit testing. There's a great deal of planning required and obstacles to navigate, but the potential payoff is turning heads, he says. When companies look at the various requirements to which they must comply, "you're going to have overlap of upwards of 80 percent," he says. "Instead of going in four or five times and testing for different requirements, you go in once and knock out that 80 percent."

PwC's study suggested internal auditors have more work to do to better align themselves with management and the board. They're not always on the same page in some areas, such as their view of the critical risks facing the company, or the role of internal audit in risk management, compliance, or other functional areas.

"The biggest thing internal auditors can do is really drive that dialogue," says Jason Pett, internal audit leader for PwC. "Audit committees need to have the loudest voice in ensuring internal audit has a clear focus on what the key risks are, and management tends to be closer to those risks, so they all have a role to play. Internal audit needs to make sure that dialogue happens and on a regular basis." ■

STAFF SIZE

Below, results from the Institute of Internal Auditors' study of internal auditors show how staff size has fluctuated since 2007 for respondents, with 23 percent noting an increase in 2013.

Year	Increased	Same	Decreased
2012-2013	23%	70%	7%
2011-2012	21%	65%	14%
2010-2011	19%	73%	7%
2009-2010	18%	73%	9%
2008-2009	20%	61%	19%
2007-2008	22%	70%	8%

Source: Institute of Internal Auditors.

BUDGET SIZE

Below, results from the Institute of Internal Auditors' study of internal auditors shows how budget size has fluctuated since 2007 for respondents, with 37 percent noting an increase in 2013.

Year	Increased	Same	Decreased
2012-2013	37%	52%	—
2011-2012	37%	46%	—
2010-2011	26%	48%	16%
2009-2010	30%	45%	25%
2008-2009	27%	44%	29%
2007-2008	36%	50%	14%

Source: Institute of Internal Auditors.

Internal Audit's Role in Managing Third-Party Risks

By Jose Tabuena
Compliance Week Columnist

As companies continue to get in trouble for the actions of their business partners, some may be wondering, "Am I my brother's keeper?" The answer, at least in the eyes of regulators, is yes.

The types of risks from third parties continue to proliferate: corruption, product defects, supply chain disruption, data security breaches, theft of intellectual property, and others—with any occurrence potentially resulting in negative publicity and prosecution. Additionally, companies should recognize that vendors, distributors, and licensees can fail to meet their full contract obligations given the complexity of the environment.


Jose Tabuena
Columnist

So how well should a company know its third parties? And to what extent can regulators reasonably expect companies to control the actions of others? Keep in mind that a substantial portion of charges of Foreign Corrupt Practices Act violations arise from the actions of third parties acting on another company's behalf. According to a 2012 Ernst & Young Global Fraud Survey, more than 90 percent of reported Foreign Corrupt Practices Act cases involve third parties, such as sales affiliates and resellers, acting on the company's behalf.

It has become clear that regulators are increasing their focus on potential third-party risks. They want to see that organizations are: identifying potential risks, verifying that business partners and their employees are compliant, monitoring for changes that might create new risks, and managing the investigation and remediation of incidents.

Moreover, increased outsourcing of business processes has been driven by the need to cut costs and improve organizational efficiencies. Many outsourcing activities take place offshore or in the cloud and in some cases companies may be unaware if a business activity has been further subcontracted.

Third parties can work under highly complex contracts and regulatory confusion, where requirements may not be clearly identified or important responsibilities overlooked. A critical consideration is when a third party's practices are passed along to your company. The new adage is that you can outsource everything—except your liability—you still own and need to manage the risk.

As a result, companies have focused their efforts developing third-party risk-management programs comprised of due diligence, onboarding, and ongoing monitoring. Internal audit can play a vital role in developing and supporting such a program.

Where Are the Risks?

There are numerous categories of third-party risks companies should consider including: regulatory compliance, financial stability, operational, security, geo-political, and others. While the risk categories may differ, the guidance and practices for managing them is similar across industries.

Below is a rough framework of the types of third-party areas that can assist in keeping risk categories distinct. The suggested classifications are not always mutually exclusive but can be useful in the development of a third-party risk-management program:

- **Demand chain:** This category comprises marketing, sales, and services activities which collectively drive and sustain demand for a company's products or services.
- **Supply chain:** Generally the activities involved in moving a product or service from supplier to customer such as purchasing, manufacturing, and distribution.
- **Outsourcing:** When certain tasks or functions related to a business, including those core to their operations, are outsourced to a service organization.

Not all third-party risks are created equal. Business partners often have different legal exposures that can affect the level of due diligence and monitoring that a company should conduct on a specific organization.

With third-party corruption risks, for example, the biggest concern comes from resellers, distributors, agents, or joint-venture partners. Often companies group third-party risks from agents, resellers, and distributors under the same umbrella. But distributors often pose greater risks than resellers or agents because companies have less control over them. Where resellers and agents sell products and services on a company's behalf, distributors are independent parties who buy and assume title of a company's products to resell into other markets, potentially including high-risk foreign markets.

Companies concerned about third-party risk typically focus on the start of relationships (on-boarding) but often fail to proactively account for issues that can occur throughout the relationship cycle. Because there are many different types of third parties, each managed by a distinct department with its own set of objectives, internal audit with its understanding of company operations is in an excellent position to consolidate the process into a single third-party risk program.

Companies often complain that they have too many third-party relationships to keep track and monitor all of them. Taking a risk-based approach to third-party due diligence helps the organization allocate resources more effectively. A full due-diligence profile is not always necessary. Internal audit's expertise can assist in examining and developing re-

lationship criteria in order to judge the level of compliance measures and oversight that is required.

The breadth of vendor risk factors can appear daunting, but the areas for internal audit structural support can be broken down into the following areas.

1. The program should have a means of adding and organizing data that already exists about the vendor. The function of this information is to allow the company to manage the vendor based on how critical they are and what function they perform. Much of this information may be available in other systems of which internal audit has intimate familiarity.
2. When considering financial risk (the viability of the third party as a going concern), a mechanism is needed to gather data and track the relevant data. Internal audit has familiarity with data that is available from a range of third-party service providers, often as a Web services feed which can allow for integration.
3. Heavily regulated organizations should have a means of assessing the third party's compliance with the relevant regulatory requirements. Most companies now have third parties complete self-assessments that include the appropriate attestations. Much of that information overlaps with what internal audit already collects as part of a formal examination. By cross referencing questions and requiring supporting documentation, they can monitor compliance.
4. By taking all of the data sources, internal audit can assist in aggregating risk factors that might not be apparent from looking at each vendor individually. Aggregate risk would only be apparent with the necessary data and analytics.
5. Finally, audit of the third-party risk-management process itself can prove valuable. If individuals and company units are not abiding by the program and following due diligence requirements, then the risk-management program itself is unlikely to succeed.

The practical way to minimize third-party risk associated with a large, global network and managing resources of time and money toward compliance efforts is to conduct a risk analysis to determine which third parties pose the highest risks.

Monitoring Third-Party Risks

Generally the vendor risk process will start with due diligence before contracts are executed and will include provisions for regular assessment of risks as an ongoing part of the vendor review process. Ultimately organizations need to move beyond the initial risk assessment to proactively address the bigger challenge of monitoring and assessing third-party risks on an ongoing basis.

As a general principle, how effective are requests for a third party to agree to follow a company code of conduct? Such a practice has some value to demonstrate due diligence but may be more form over substance.

Monitoring of third-party risks, like most compliance initiatives, requires a sustained effort. The questionnaires third parties complete should be updated quarterly, since the parties' risk profile can change quickly. Effort should be made to exercise the right-to-audit when the company develops a reasonable belief that some improper behavior took place.

Contracts with third parties often include right-to-audit clauses; but realistically how often are they actually exercised? A successful risk and compliance strategy will have clear policies and processes defining when and how audits of business partners are conducted and when internal auditors or external auditors should be engaged. Elements of the audit process include:

- Management and prioritization of the audit staff time and resources, and calendar activities to schedule and conduct audits, often driven by the risk assessments
- Ongoing monitoring of watch and sanctioned contractor lists to assure the company only does business with lawful entities
- Periodic attestation to and validation of third-party adherence to the company code of conduct, policies, and procedures
- Audit validation to assess the validity of risk and performance assessments of specific business partners

Service Organization Control Reporting

Companies that outsource to a service organization certain critical tasks or functions should consider the value of undergoing a Service Organization Control engagement. Historically, audit firms reporting on controls over financial reporting at a service organization relied on Statement of Auditing Standards 70 reports. As organizations became concerned with risks beyond financial reporting, the use of SAS 70 reporting was seen as misused to obtain assurance regarding controls over compliance and operations.

SAS 70 has been replaced with Statement on Standards for Attestation Engagements 16, *Reporting on Controls at a Service Engagement*. There are now versions of SOC engagements and reports that can address controls at a third-party service organization and better address the effectiveness of controls over compliance and operations.

Managing third-party risk is becoming a critical success factor for all enterprises. Internal audit should be looked to as a resource to help build a vendor risk-management program. ■

Where the CCO & Internal Audit Should Report

By Jose Tabuena
Compliance Week Columnist

On parallel yet similar tracks, the roles and reporting relationships of the chief audit executive and the chief compliance officer continue to be heated, contested, and ultimately muddled topics.

Although the view that CAEs and CCOs need a high degree of independence and clout to accomplish their responsibilities has gained momentum, there are still naysayers and skeptics who believe they should remain where they have historically resided and reported—the CAE within finance and to the chief financial officer, and the CCO under the purview of legal and to the general counsel.

Jose Tabuena
Columnist

Both titles face the controversy of too many chiefs (officers that is), with many CEOs questioning whether yet another executive is needed in the crowded C-suite. Or is there indeed value, they wonder, to empower these positions with sufficient independence and authority so they can play a gate-keeping role that seems to be sorely lacking, especially at large complex organizations?

Richard Chambers, president and CEO of the Institute of Internal Auditors, recently wrote that it's time for internal audit to move out from under the CFO's shadow. He observes that the majority of CAEs report functionally to an audit committee and that there is agreement that such reporting enhances internal audit independence. But he also questions whether internal audit executives are truly as independent as they like to think they are, and if administrative reporting lines, particularly to CFOs, are problematic?

For compliance professionals, the U.S. government has increasingly made clear the expectation that the CCO is not to be subordinate to the general counsel. The government's position was recently expressed in a deferred prosecution agreement with HSBC, which requires the bank to elevate the status of its anti-money laundering unit by "separating the legal and compliance departments

As pointed out by Donna Boehme, principal of Compliance Strategists and frequent commentator in the field of organizational compliance and ethics, "[the] HSBC case is further indication that U.S. regulators and prosecutors are closely scrutinizing the independence, empowerment, and resources of corporate compliance functions—and even further, are re-thinking the relative seniority and positioning of the chief compliance officer vis-a-vis other senior managers." The HSBC case tracks the expectations of the Federal Sentencing Guidelines which makes clear the preference for CCO independence and unfiltered access to the governing authority.

Independence Is Not Always Independence

Audit and compliance professionals should recognize that all assertions of independence are not created equal. First, true independence ideally involves professionals from outside the company. As classically defined, a gatekeeper is a *third party* who supplements efforts to deter wrongdoers by disrupting the conduct of their client representatives. Historically for the capital markets, a gatekeeper is an agent who acts as a reputational intermediary to assure investors as to the quality of information sent by a corporate issuer (and so would include investment banking, accounting firms, and lawyers in their activities related to securities issues). The ideal gatekeeper was viewed as an outsider with a career and assets beyond the firm and thus having less to lose than an inside manager.

Recent events, however, have led to some inconvenient truths. Since the Private Securities Litigation Reform Act of 1995, external auditors have been obligated to report to the Securities and Exchange Commission any unrectified material illegalities encountered in the course of their work. Yet evidence suggests that they are reluctant to do so. The failures of big accounting firms and outside counsel in the Enron and WorldCom collapses have raised the issue as to whether outsiders actually make reliable gatekeepers.

Although all internal employees have a vested interest in the company's ongoing success—and thus cannot be viewed as wholly independent—commentators have increasingly noted that internal functions are better suited to serve as effective gatekeepers. As stated by Ben Heineman, former general counsel with General Electric:

"If we want companies to fuse high performance with high integrity, the place to begin—and to be the most effective—is inside the company itself. Outside regulators and gatekeepers can never be as potent and preventative as internal governance on the front lines from the CEO on down."

Inside the organization, internal audit and compliance have served in this gatekeeping function. Their roles require the capacity and willingness to prevent misconduct. Their formal and informal communication channels means they are well-positioned to access critical information that may reveal company misconduct. I would argue that internal audit and compliance are more independent than the legal and finance functions and therefore better suited to be internal gatekeepers, especially when they are unhinged from those functions.

Originally viewed as a financial gatekeeper, the role of the CFO has expanded and evolved to a strategic partner and adviser to the CEO. Auditor independence was thus strengthened to fill the void and the important role that internal audit plays in their companies' systems of risk man-

agement and internal controls became recognized.

Likewise, the role of the GC has evolved to that of strategic partner and company advocate more so than that of an internal monitor. Otherwise, why has the legal bar vigorously opposed efforts to impose gatekeeping obligations on lawyers, such as when Congress formally recognized such a role when enacting Sarbanes-Oxley Section 307? At the core of the bar's opposition (especially to the SEC's noisy withdrawal proposals) is hostility to the notion that attorneys should have any obligations that could put them at odds with their client representatives. The in-house bar can't have it both ways; if legal wants oversight over compliance it must also accept the full accountability of a gatekeeping role.

Internal Audit Reporting Lines

The internal audit profession has developed recommended reporting lines that provide a useful model for internal gatekeeping. In its guidance the IIA refers to functional and administrative reporting relationships (sometimes confusingly mixed with the terms direct and indirect reporting).

The IIA states that the CAE should report functionally to the audit committee or its equivalent. It also says that the CAE should report administratively to the chief executive officer of the organization. Finally, the guidance says, "the chief financial officer, controller, or other similar officer should ideally be excluded from overseeing the internal audit activities even in a dual role (with the CAE reporting functionally to the audit committee)."

A functional reporting relationship establishes a connection between positions or organizational units at different management levels based on the specialized nature of the function for which a mutual responsibility is shared. Though it is not always clear, generally the functional reporting relationship is stronger than the administrative one , because the functional body controls the individual's compensation and evaluations.

According to the IIA's Practice Advisory 1110-2, reporting functionally means that the governing authority would:

- Approve the overall charter of the internal audit function, the risk assessment, and the related audit plan;
- Receive communications from the results of internal audit activities or other matters that the CAE determines are necessary, including private meetings (executive sessions) without management present;
- Approve all decisions regarding the appointment or removal of the CAE including approving the annual compensation and salary adjustment of the CAE; and
- Make appropriate inquiries of management and the CAE to determine whether there are scope or budgetary limitations that impede the ability of the internal audit function to execute its responsibilities

In contrast, administrative reporting is the reporting relationship within the organization's management structure that facilitates the day-to-day operations of the internal audit function. Administrative reporting typically includes:

- Budgeting and management accounting;
- Human resource administration, including personnel evaluations and compensation of department staff;
- Internal communications and information flows; and
- Administration of the organization's internal policies and procedures.

According to some estimates, more than 50 percent of chief audit executives still report administratively to their companies' CFO. While safeguards such as functional reporting relationships to audit committees may mitigate the risk of interference with internal audit, reporting to the CFO is still fraught with risks and challenges for the CAE.

If the CAE knows that he or she will be dependent on the CFO for his or her next career assignment, how objective can they really be in assessing the CFO's areas of responsibility? While a strong working relationship with the CFO is needed, internal audit also needs the independence and flexibility to evaluate financial information and to establish audit plans without undue influence or even the perception of influence.

Replace CAE with CCO and GC for CFO, and the foregoing principles still apply. Legal has a separate and distinct mandate from compliance. Companies that have placed the CCO under the thumb of the GC, and have viewed compliance purely through a legal prism, have paid a steep price. Compelling reasons are increasingly made to bolster the CCO role with independence from the GC, usually as a direct report to the CEO with unfiltered access to the board of directors.

A point often made is that the working relationship the CAE or CCO develops within the executive ranks and is more critical than any formal reporting relationship. I've heard from CAEs and CCOs who report respectively to the CFO and GC that the reporting structure was not an issue because their supervisor understood the value of their function. But such a relationship is not static and doesn't guarantee that a new CFO or GC will "get it" and similarly understand the distinctive roles. The position needs to be institutionally positioned for success. Too many chiefs do not necessarily spoil the broth. ■

NAVEX GLOBAL™

The Ethics and Compliance Experts

Are you getting the full ROI of automated third party due diligence software?

ACCESSIBLE ANYWHERE

Time & Cost Savings GAIN AUTOMATION EFFICIENCIES

COMBAT CORRUPTION & BRIBERY

Create a defensible program

Focus on the Highest Risk Partners MITIGATE REGULATORY RISK

CONDUCT CONTINUOUS MONITORING

Avoid Reputational Embarrassment **Improve Internal Processes & Control**

Integration with Training, Policy & Case Management

COMPLETE VIEW OF ALL THIRD PARTY RISKS

Contact Us to Learn How

www.navexglobal.com | +1 (866) 297 0224 | insight@ navexglobal.com