Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Top Global GRC Risks

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 become the go-to resources for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 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. We provide the world's most comprehensive ethics and compliance ecosystem to manage governance, risk and compliance (GRC), helping protect organisations' people, reputation and bottom line.

Our array of GRC services help capture and respond to business risk, improving the economic and social value of organisations around the world. The company works with clients to manage ethics and compliance programmes through a suite of solutions including case management, whistleblower hotlines, policy management, third-party risk management, online training, risk & program assessments and expert advisory consulting. Our fully integrated offering provides clients with key learnings and actionable data to inform change and protect their organisation. More information can be found at www.navexglobal.com.

Inside this e-Book:

Top 10 Global Compliance Trends to Watch

By Neil Baker

Regulatory and enforcement developments in the European Union, China, South America, the United States, and elsewhere are having a big effect on global companies.

A new European Parliament will be elected in May with a new European Commission appointed in October. Politicians and regulators will be in a rush to see their pet projects finalised before they have to let go of power, including a new data privacy regime that is likely to change the way any company that does business in Europe collects and handles consumer data.

Meanwhile, China is beginning to flex its enforcement muscle, coming down on companies for corruption and antitrust violations. Other countries, including Brazil, Russia, and Canada, have also enacted stricter anti-corruption laws.

Here are 10 developments to watch on the global compliance front.

1. **Data Privacy: Europe decides.** Europe's new data privacy regime has been in the pipeline for a while. The EU will likely end the horse trading and finalise its plans; otherwise the election of a new European Parliament will force it back to square one. In the rush to the finish line, many hope that Europe doesn't over-regulate in this area, but the continued fallout from the Edward Snowden leaks about U.S. government surveillance of European citizens hardly helps their case. Even the future of the bilateral U.S.-European "safe harbor" program, which has traditionally given U.S. companies preferential status when it comes to data privacy rules, is in doubt. By year's end, Europe's data laws are expected to look very different from those in place today and are likely to change how all companies that do business in Europe collect, store, and process customer and employee information.

   As more countries around the globe introduce data privacy rules based on the new European model, the international transfer of personal data has become a real trap for the unwary, warns Nicholas Thomas, a partner in law firm Morgan Lewis. "Many of the world's biggest companies with substantial operations within and outside of the European Union need to re-examine their existing processes and put in place broader and more far-reaching policies to ensure compliance," he says.

2. **Bribery Act enforcement?** When will we see the first significant prosecution under Britain's Bribery Act? We asked the same question last year, and the answer was no. Though the Serious Fraud Office said it had several cases in progress, none came to court. Then at year's end, the SFO was hit by yet another high-profile courtroom humiliation. The trial of a £40 million bribery case against businessman Victor Dahdaleh collapsed after a key witness changed his evidence and two U.S. lawyers refused to testify.

3. **China flexes its enforcement muscle.** Chinese regulators are paying closer attention to pricing practices across several industries, indicating that the government is ramping up antitrust enforcement. From pharmaceuticals to food packaging and consumer products, no industry appears out of the reach of China's evolving antitrust regime. "Multinational companies might have felt that, for a while, they were not really exposed to these kinds of price-related antitrust risks," says Peter Wang, partner-in-charge of Jones Day's antitrust practice in China. "Clearly, that's no longer the case."

   China's anti-bribery enforcement has also grown stronger over the last year and will likely increase going forward, forcing companies that operate there to consider not just compliance with U.K. and U.S. anti-bribery laws, but also with local Chinese anti-bribery laws. "Businesses seem to be recognising, rightly so, a culture of greater enforcement by China on anti-bribery and corruption issues," says Randy Stephens, vice president of Advisory Services at NAVEX Global.

4. **Europe gets tough on anti-trust.** Europe's current competition commissioner, Joaquín Almunia, will be replaced in May. Could we see a flurry of antitrust decisions as he cleans his desk for his successor? Nicole Kar, a partner at law firm Linklaters, thinks so. Hot topics include the long-anticipated settlement of a case against Google, which has been in arbitration for three years. Kar also thinks the European Commission will test the boundaries of antitrust law in the near future with more aggressive enforcement in the legal "grey zone." Firms at risk of action include those that exchange information, signal price changes, and distort market benchmarks. The Commission has also started pushing corporate liability to the minority shareholder level. "These trends will continue to present compliance challenges for in-house legal and compliance teams," says Kar.

5. **A busy time for cartel and patent cases.** 2013 was a mild, if not timid, year for European cartel enforcement, adds Kar, but she expects "a number of significant fines at unprecedented levels" through 2014. "We understand there to be at least 20 cartel investigations ongoing in a wide range of sectors—from sugar to seatbelts and from envelopes to smart card chips. 2014 is likely to see some

progress in those cases and decisions adopted in some of the longer outstanding investigations." Kar also expects Europe's "patent wars" to only intensify. The IT sector will remain a fierce battlefield, with cases involving Apple, Microsoft, Motorola, Google, and Nokia.

6. **Private damages actions.** We could also see a breakthrough in which European legislation is finally adopted to harmonise damages in antitrust actions. If political progress can be reached in the European Parliament and sceptical national governments can be convinced, the "Actions for Damages" directive could be adopted before the European parliamentary elections. The aim is to remove national rules that stop all but the most determined victims of EU competition law infringements from getting compensation. The changes have been eight years in the pipeline.

7. **Global tax transparency: got a strategy?** The G20 governments have promised to make companies in their jurisdictions provide open and clear financial data by the end of 2015, as part of a global clampdown on tax avoidance. Few companies are prepared. A study by Thomson Reuters found that only 35 percent of global companies are planning to be more transparent on tax. "Tax authorities around the world are becoming more aggressive and focused, in turn increasing disclosure and transparency requirements on the business community," says Thomson Reuter's Charlotte Rushton. "Our findings suggest that there is a risk that many could find themselves on the back foot if they do not start planning their transparent tax strategy soon."

8. **Payment card questions.** The global standard that governs how firms should keep payment card information safe changes in 2014. Compliance with the Payment Card Industry Standard (PCI DSS 3.0) is mandatory for companies that store, process, or transmit cardholder data from the start of 2015. "E-commerce merchants will face the biggest changes, since the new standard states that anything that impacts the security of these environments, even if they do not store, process, or transmit cardholder data, will be in scope for PCI DSS 3.0," says Michael Aminzade of Trustwave, an information security company. "This means merchants will have to implement policy and procedural controls as well as security technologies that will help prevent their customers' card-holder data from ending up in the wrong hands."

9. **Energy-sapping regulation.** The EU's slow and faltering rollout of two regimes to regulate the energy sector should finally gain pace. REMIT (Regulation on Energy Market Integrity and Transparency and EMIR (European Market Infrastructure Regulation) create new data collection and reporting requirements for companies involved in Europe's wholesale energy markets. Companies will likely have to invest in new information systems to cope. "Compliance executives need to be seriously concerned," says Steven Ferrigno of Allegro Development, a software company. "If your company trades in energy commodities or operates a hedging strategy to mitigate fuel or energy-related costs, either of these shifting sets of rules could bog you down for the foreseeable future."

10. **Bank audit under fire.** Big audit firms are likely to come under fire when the U.K. Financial Reporting Council looks at their auditing of banks and building societies. In December the regulator said it would investigate how audits in this area are performed so it could identify "why progress in improving their quality has been slow and what needs to be done." The review will start in the second quarter with a formal report due by the end of the year. FRC Chairman Sarah Hogg wants to see "a genuine step change" in the quality of audit work. ■

MAIN OBJECTIVES

Below are the objectives of the EU's REMIT legislation.

REMIT introduces a sector-specific legal framework for the monitoring of wholesale energy markets. The objective is to detect and to deter market manipulation. For the first time, energy trading will be screened at the EU level to uncover abuses. Market integrity and transparency are essential for well-functioning energy markets.

Once REMIT is fully implemented, ACER will be responsible for collecting and analysing wholesale markets and other relevant data to identify possible instances of market abuse. ACER will also notify the concerned National Regulatory Authorities (NRAs). After an initial assessment and when there is grounds to believe that abusive behaviour has actually occurred.

Member States will have to carry out investigations and put in place penalties to help prevent market manipulation.

This is a delicate task because it deals with complex traded products and markets and, because monitoring should be conducted in a vigilant manner without however unduly interfering with the working of energy markets.

Source: ACER.

SHOP TALK

Above, Barry Matthews, director of legal affairs for ITV addresses the group, while CPA Global's Jennifer Aikins-Appiah looks on.

Cooling Off Red-Hot Third-Party Risks

Corruption and bribery risks are expanding rapidly for global firms, with the biggest dangers coming from those at third-party resellers, distributors, and others. During forums in London and Amsterdam, executives discussed their processes for assessing the risks associated with third parties and exchanged ideas on reining them in.

By Jaclyn Jaeger

Around every company lie concentric circles of third-party risk. Inside the innermost circle, coloured green, sit the company's core of trusted employees and customers. Then around that is a wider circle of primary third parties used by the company—suppliers, agents, joint venture partners, and others—coloured in yellow.

Then comes the third, final circle: the third parties of *those* third parties—sub-contractors, local agents, and many others, nearly untraceable to corporate headquarters. That final circle is, of course, bright red and for good reason: some multinational companies refer to it as the circle of fear.

Indeed, several compliance and risk executives who attended two separate executive forums conducted by Compliance Week and NAVEX Global in London and Amsterdam said that the outer two circles were where significant compliance danger, along with financial and reputational risk lie due to reliance on third parties in the supply chain and distribution network.

One message that became strikingly clear throughout the forums is that European companies struggle just as much with third-party risk mitigation as U.S. companies. "It was really amazing to hear almost exactly the same set of concerns," said Bob Conlin, chief products officer at NAVEX Global, a corporate compliance solutions and services firm.

Those concerns, Conlin said, go something like this:

- We don't have visibility into all of our third-party relationships, but we know they number into the thousands.
- We can't identify who the primary internal business owner is for each of our third-party relationships.
- We have no way of automating the risk process; we're doing it manually today, and we're not doing a very good job at it.
- We're only assessing the vendors that we think pose the highest risk.
- We have no way to monitor changes in the risk profile for each vendor over time.

For multinational companies, in particular, the risks associated with third parties are rising fast, due to the proliferation of anti-corruption legislation on a global scale, as many attendees attested. Aside from the U.S. Foreign Corrupt Practices Act and U.K. Bribery Act, countries like Canada and Brazil have also enacted their own versions of anti-bribery and corruption legislation or expanded existing laws.

"The biggest risk is corruption by third parties," said Sylvie Bleker-van Eyk, chief compliance and risk officer at construction and engineering company Ballast Nedam, based in the Netherlands.

Due Diligence Done Right

Attendees at both forums agreed that third-party risk mitigation begins with the initial screening process at the start of any relationship and continues with the

ABOUT THE EVENTS

Compliance Week and NAVEX Global presented editorial roundtables at St. Ermin's Hotel in London and at the Grand Hotel Amrath in Amsterdam last year. The focus of the roundtables, which were moderated by Compliance Week Editor Matt Kelly, was on identifying and reducing third-party risks and how to establish compliance programmes to assess and mitigate the risks of corruption by third-party vendors, distributors, resellers, and others.

daily interactions with all the organisations a company touches. "You need to have a consistent on-boarding process for vetting any new third party with whom you're going to do business," Conlin said. "At minimum, that should involve some type of a preliminary background check screening for issues related to sanction and watch lists, politically exposed persons lists, and any relevant adverse media."

A thorough on-boarding process becomes especially important for companies that are going through a shift in their business operations, or are experiencing a merger or acquisition. One executive, whose company is currently undergoing a series of mergers, touted the importance of the on-boarding process as a way to shift from a corporate culture historically used to completing handshake deals to a more formal and structured process.

Barry Matthews, director of legal affairs for U.K. commercial television network ITV, said the company begins the third party Bribery Act due diligence process with a profiling exercise to ascertain the risk category of the "associated person." Third parties that are categorised as "high risk" undergo a much more thorough questionnaire and document production process than those classified as "low." The legal team control the AP database and prompt commercial colleagues to refresh due diligence on an annual basis; this process is complimented by bi-annual spot checks.

Tonnis Poppema, director of compliance at Hasbro International Holdings, a subsidiary of Hasbro International based in Amsterdam, said its office of corporate compliance similarly employs a very thorough inspection process before any employee can do business with a third party. "For us it's non-negotiable not to agree to our standards. If a business partner says 'no' to our compliance standards, we don't work with them," he said. "It's as simple as that."

Then comes the question of who actually owns the risk. "Every third party needs to have a business owner, and that business owner has to have some responsibility for managing the risk associated with that relationship," Conlin said. Who is purchasing from that third party? Who is approving payment to that third party?

If there is a third party out there to whom nobody in the business is claiming ownership, "you have to get rid of them," Conlin said. "You can't afford the risks associated with ambiguous business relationships." Although, that can be a bit of a challenge, he said, because many companies have thousands—if not tens of thousands—of third-party relationships.

At ITV, the commercial operating team and the legal team work together to negotiate contracts with third parties, Matthews said. The legal team's job is to guide the decision-making process during the negotiation, ensuring that the parties to the contract fully understand their obligations to reduce the likelihood of future litigation. The ITV legal team prides itself on a "prevention rather than cure" approach to the delivery of legal services.

After the legal team helps to negotiate the contract, risk ownership moves to an appointed contract manager. "It's not an agreement entered into by the organisation. It's an agreement owned by the individual within the organisation," said Matthews.

The obligations flowing between the parties are summarised for the contract owner, Matthews continued. "We then check in with them from time-to-time to assess how those relationships are going." If that contract manager was to then leave the company, the legal team is there to ensure that knowledge of the workings of the contract does not leave with them. "We provide continuity by ensuring that someone picks up the reins and is properly briefed on that agreement," he said.

> "For us it's non-negotiable not to agree to our standards. If a business partner says 'no' to our compliance standards, we don't work with them. It's as simple as that."
>
> Tonnis Poppema, Director of Compliance, Hasbro International Holdings

From there, it's all about getting third parties to buy into the due diligence process. "Our main challenge is to make sure that our local business partners are up to speed on our compliance standards," Poppema said.

In Asia, where Hasbro produces many of its products, local entities don't have that direct connection to the United States or the United Kingdom, so they aren't too concerned about the FCPA and U.K. Bribery Act, said Poppema. "We constantly have to convince them of the fact that they have

From Left to right: Royal Philips Senior Director of Business Conduct & Ethics Lucianne Verweij; Ahold Europe Legal Counsel Ken van der Wolf; and Ballast Nedam CCO Sylvie Bleker-van Eyk.

Claire Combes, head of risk & internal audit at Intu Properties, joins the discussion.

to adhere to our standards. That's a challenge," he said.

Some attendees said they give their employees' code of conduct to their third parties and have them attest that they have read it. Conlin said this process can be fortified by using a third-party risk-management tool to distribute their policies and then track those attestations on a continual basis.

Remediation Measures

Forum participants also shared ways in which they monitor the level of risk that each third party poses, both from an IT systems standpoint as well as a cultural standpoint.

The most effective way to address third-party due diligence adequately is to have a continuous monitoring process in place, advised Conlin. NAVEX Global launched a third-party risk management solution that automates the assessment and monitoring of all of a company's third parties.

The tool also assists companies in identifying high-risk third parties by cross-referencing information from more than 400 international sanction, watch, and debarment lists, while combing through more than 9,000 global media outlets to identify any adverse activity related to money laundering, terrorism, or fraud.

"The problem is that many companies still depend on manual processes for third-party risk assessments, rather than having fully automated systems in place," Conlin said. Even among companies with automated solutions, they're typically performing risk assessments only on third parties where exposure is thought to be greatest, "which creates a substantial risk through inevitable gaps and lack of consistent evidentiary record," he said.

Don't expect such a scatter-shot approach, however, to hold water with the U.S. Department of Justice or Securities and Exchange Commission in the event one of your perceived lower-risk third parties—such as one in that yellow circle of risk—commits bribery. "They're going to say that's too bad," said Conlin. "You had adequate procedures in place for assessing your third parties; you simply failed to extend those procedures to all of your vendors."

An equally important element of a robust third-party due diligence programme is the training, Poppema said. "It stands or falls with the personal staff managing that."

According to Matthews, all compliance programmes should have a face-to-face component; "You can write policies until they're coming out of your ears, but unless they come to life through face-to-face training, in my experience, they are rarely embraced and followed," he said.

Make sure training is tailor-made to the company by citing real-life examples, said Bleker-van Eyk. "The best way to learn is from mistakes," she said.

She also stressed that educating employees about third-party due diligence is more than just making employees aware of risk. Rather, she said, it's a "state of alertness" that needs to be embedded in the DNA of employees.

When it comes to building a culture of compliance, front-line employees are much more likely to listen to mid-level executives—such as business unit leaders and divisional vice presidents—than they are to the CEO. It's about tone-at-the-top down to the middle, and then tone-at-the-middle down to the bottom, Bleker-van Eyk said.

"The point is if you don't do third-party risk assessment and mitigation right," said Conlin, "you expose your organisation to huge financial and reputational risk." ■

Many EU States Lack Whistleblower Protections

By Roberta Holland

Most European Union nations are doing little to nothing to protect whistleblowers from retaliation, according to a report released by Transparency International.

The report, Whistleblowing in Europe, found that only four of the 27 countries studied had adequate whistleblower protection laws in place. In those four countries—Luxembourg, Romania, Slovenia, and the United Kingdom—a corporate or government employee disclosing serious fraud or wrongdoing would receive sufficient legal protection from dismissal, harassment, or other retaliation.

The report found that 16 countries partially protect whistleblowers while seven countries have either no protections or severely inadequate protections in place. That is despite the fact that all but two of the 27 countries have signed onto the United Nations Convention Against Corruption, which includes a requirement to consider implementing whistleblower protections. Many of the laws that do exist are vaguely written or contain loopholes, the report found. Others lack confidentiality guarantees, protections from defamation claims, or methods for whistleblowers to disclose their claims.

The anti-corruption watchdog also pointed out that in the countries with partial laws, whistleblowers may come forward under the belief they will be protected only to find that not to be the case.

"Whistleblowers are very important to the fight against corruption," Anne Koch, TI's regional director for Europe and Central Asia, said in a statement. "They take on risks that many, if not most, people are unwilling to assume, and they expose crimes that few are interested in or brave enough to report."

According to the report, roughly one third of fraud worldwide is exposed by whistleblowers or other tipsters, which is more than auditors, the police, and security staff combined.

The risk of retaliation is real, the report said, citing examples of whistleblowers in Austria, Estonia, and Portugal who were fired after exposing wrongdoing. In contrast, TI highlighted the 2000 case of Toni Fernandes, the CFO of a telecom company in the U.K. who exposed fraudulent expense claims submitted by the company's managing director. While Fernandes was fired from his job, the whistleblower subsequently received a six-figure compensation award from the U.K. Employment Tribunal and the executive in question left the firm.

The lack of adequate legal protections also can act as a deterrent for would-be whistleblowers to come forward in time to stave off a tragedy or financial scandal, the report said. It pointed to cases like the 2010 flooding of Hungarian villages by aluminum waste, a 1987 ferry accident in Belgium that left 193 people dead, and a 2004 phone-tapping scandal in Greece, as examples of situations in which people knew of problems beforehand but did not come forward in time.

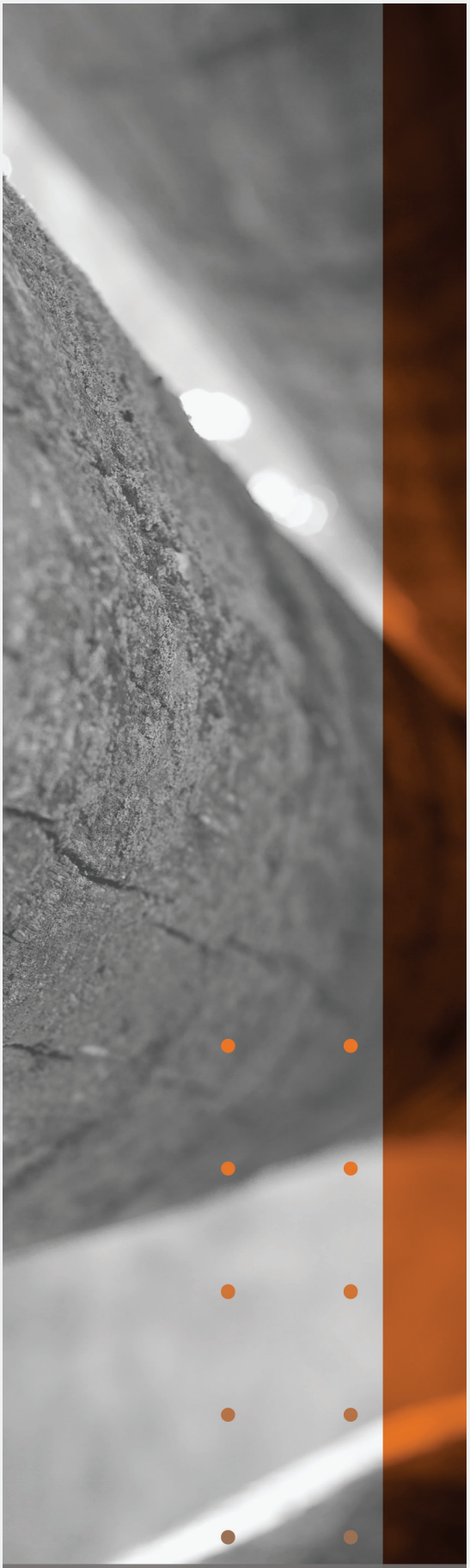
In October 2013, the European Commission signaled it would not move forward at this point with a request by European Parliament to propose legislation for an EU-wide whistleblower protection law.

> "Whistleblowers are very important to the fight against corruption ... They take on risks that many, if not most, people are unwilling to assume, and they expose crimes that few are interested in or brave enough to report."
>
> Anne Koch, TI's regional director for Europe and Central Asia

Transparency International is urging all EU countries to adopt and enforce their own comprehensive whistleblower protections for both government and corporate workers. The watchdog group praised EU countries including Austria, Denmark, France, and Italy for making recent attempts to strengthen whistleblower protections. It also pointed to proposals to strengthen protections in Finland, Greece, Ireland, the Netherlands, and Slovakia.

While detailed analysis of each country can be found in the report, below is a quick summary of how the 27 countries stack up.

- Advanced Protection: Luxembourg, Romania, Slovenia, United Kingdom
- Partial Protection: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Hungary, Ireland, Italy, Latvia, Malta, Netherlands, Poland, Sweden
- None/Very Limited Protection: Bulgaria, Finland, Greece, Lithuania, Portugal, Slovakia, Spain ■



NAVEX GLOBAL™
The Ethics and Compliance Experts

THE ROI OF GRC

MAKING THE BUSINESS CASE FOR AUTOMATED CASE MANAGEMENT

The implementation of a robust Governance, Risk, and Compliance (GRC) programme should be a primary concern for all organisations. Organisations that have a strong commitment to GRC management consistently out-perform those that do not:

- Businesses with superior governance practices on average generate 20% greater profits than other companies (MIT Sloan School of Management)
- Companies who had open communication saw 7.9% shareholder returns over ten years vs. just 2.1% for those who didn't (Corporate Executive Board)
- Non-compliance costs are 2.65 times that of the cost of compliance for companies (Ponemon Institute)
- Companies that had good GRC programmes had 14% lower operating costs than those that didn't (NAVEX Global data)

Key to delivering a strong GRC programme is a centralised case management database containing all of the information for all of the incidents and cases seen within an organisation, accessible by all of the key stakeholders.

Automating the case management process not only provides easy access to a centralised location for all of an organisation's GRC data, it also significantly reduces the time required to manage all of the key steps in the process.

Key GRC Management Challenges

- Minimising the time and costs required to manage all aspects of case management.
- Reducing the duplication of effort encountered in the case management and resolution workflow processes.
- Increasing the awareness of incidents that are occurring within the organisation.
- Increasing overall corporate oversight to avoid fines/penalties, fraud, and other unexpected loss events.

RESULTING VALUE AFTER IMPLEMENTING NAVEX GLOBAL'S SOLUTIONS:

VALUE AREA	SPECIFIC BENEFITS
Improved Operational Efficiencies	• Reduce time spent taking and recording hotline calls • Reduce time spent recording and reporting incidents • Reduce time spent setting up incident cases • Reduce materials, mailing and storage costs • Reduce audit time and costs • Reduce time spent generating reports • Reduce the duplication of effort
Reduction of Corporate Risk	• Increase awareness of small/medium sized incidents • Reduce fines/penalties from regulatory bodies
Elevate Corporate Oversight	• Reduce fraud and other unexpected loss events • Reduce litigation and settlement costs • Protect revenues by pro-actively managing risk

REALISED: ORGANISATION'S CUSTOMER SAVINGS

- **Customer A** receives 60 open door reports a month, which used to take 30 minutes each to complete, and 20,000 conflict of interest forms once a year, taking 5 minutes each to complete. Time required for both forms was reduced by 60% and resulted in $47,400 in annual productivity improvements.
- **Customer B**, with a total of 110 cases a month, was able to reduce the set-up time per case from an average of 2 hours down to 30 minutes and realised $97,100 in annual productivity improvements.
- **Customer C** was able to reduce the duplication of effort previously experienced across cases by an average of 10%, resulting in $108,700 annual productivity improvements.
- **Customer D** saw a 10% increase in cases reported, which were costing them an average of $1,500 in theft and $15K in turnover costs when going unreported, so realised $187,100 in annual cost savings.
- **Customer E**, with annual revenues of $1.0B, noted that 0.01% of better-secured revenues were attributed to the automated solution and realised $125,000 in annual revenue gains.

Your Organisation's Ethics & Compliance ROI

As above, we would love to assist your organisation in gaining the efficiencies NAVEX Global can help provide. We will work with you to discover your organisation's key processes and calculate the time, effort and ROI so you can determine how to best spend your ethics & compliance dollars. To arrive at these calculations, NAVEX Global engaged the ROI analysts of Hobson & Company, a firm that specialises in discovering the key business benefits driving the adoption of new and emerging technologies, to better understand and validate the business opportunities associated with each of these key areas.

ABOUT NAVEX GLOBAL

NAVEX Global helps protect your people, reputation and bottom line through a comprehensive suite of ethics and compliance software, content and services. The trusted global expert for more than 8,000 clients in 200+ countries, our solutions are informed by the largest ethics and compliance community in the world.

+44(0)20 8939 1650 | info@navexglobal.com | www.navexglobal.com

ABOUT HOBSON & COMPANY

Hobson & Company helps technology vendors and purchasers uncover, quantify and validate the key sources of value driving the adoption of new and emerging technologies. Our focus on robust validation has helped many technology purchasers more objectively evaluate the underlying business case of a new technology, while better understanding which vendors best deliver against the key value drivers. Our well researched, yet easy-to-use ROI and TCO tools have also helped many technology companies better position and justify their unique value proposition.

For more information, please visit www.hobsonco.com.

 FEBRUARY 2014

Global Policy Management: From Many to One

By Jaclyn Jaeger

Ask any company how many policies it has and where they are located—from the corporate level down to the functional level—and chances are you won't get a straight answer. The policy at headquarters in Europe is likely to differ from the one on any given topic that employees follow at the office in, say, Shanghai or Dubai.

A typical company will have some policies controlled by headquarters, sure; but most tend to be created and managed independently by various business units, facilities, or locations, depending on each company's operations. Absent any sense of where those documents reside, most companies end up with hundreds of conflicting, redundant, or out-of-date policies.

"There are a lot of inefficiencies in such a system, because there is no sharing of knowledge or baseline information across the organisation," says Ingrid Fredeen, vice president of the Ethical Leadership Group, the advisory services division of NAVEX Global. It also creates a lot of compliance and legal risks for the company, she says.

For multinational companies, those challenges are multiplied because policies need to extend across the entire enterprise, including subsidiaries, contractors, and consultants. "That adds a whole other level of complexity of how you deploy policy management," says Gaurav Kapoor, chief operating officer of MetricStream.

Enter the centralised policy management process: an effort to see a company's entire policy landscape, to ensure that each specific policy complies not only with the company's broad approach to policies and procedures, but also all relevant laws and regulations.

The first step is to determine which policies need to be centralised versus those that should remain local, Fredeen says—and no, that's not necessarily the contradiction in terms one might think. For example, unionised workforces often have specific rules that apply to individual facilities. "What is appropriate for local management and what is appropriate for centralising?" she says.

Corporate headquarters, whether in Europe or elsewhere, does want enough oversight that it knows such policies exist, but the idea is not to have so much centralisation that you infringe on local business practices. "You still have to allow people to manage their processes at the local level," Kapoor says. Central command only needs to know "what is being adhered to, and what is being managed and not managed."

What sort of policies *should* be corporate-wide, and obeyed by everybody? Codes of Conduct, anti-corruption policies, anti-competition policies, and harassment policies, to name a few. On the other hand, privacy policies can differ substantially from one nation to the next depending on each country's laws and culture.

Once a company has identified which policies to centralise, the next step is to establish a corporate policy management repository where these policies will reside. "It should be a policy management tool as opposed to a general document management system," says Lisa Hill, president of PolicyScape Consulting and co-chair of OCEG's Policy Management Group.

A policy management tool—assuming it's designed and used correctly—allows companies to create, approve, distribute, and share policies via a single system. That approach also lets the company establish an audit trail, by keeping track of when policies have been accessed or modified and by whom. (And, critically, who grants exceptions to which policies, for what reasons.) Some policy management tools even alert policy owners to changes in the law so they know when a policy needs updating.

> "A policy should not be able to get into the central repository unless it follows the meta policy, so you have that nice circle of control."
>
> Lisa Hill, President, PolicyScape Consulting

While a policy management tool is not mandatory, a document management system like Microsoft SharePoint doesn't allow for the same level of control over policy access and it involves a lot more time and resources, Fredeen says.

Policies on Policies

Companies should also implement a roadmap for managing the policy lifecycle, from drafting and validating to approving and implementing, Hill says. That roadmap should be documented in the company's "meta policy," she says. In many circles, a meta policy is more memorably known as "a policy on policies."

The concept is important, Hill stresses. "Without a meta policy, it's difficult for companies to achieve the consistency and the governance they need for effective policy management." In addition, the meta-policy and policy management lifecycle should be available to employees in case they need to create a new policy.

Hill advises corporations to establish a rule (oh, let's just say it: establish a policy) that says if a policy is *not* stored in that central repository, it isn't an official corporate policy. That reduces the company's possible legal liability should an employee refer to an out-of-date policy not stored in the central repository, "and a policy should not be able to get

into the central repository unless it follows the meta policy, so you have that nice circle of control," Hill says.

How a policy is approved will vary from company to company. Some companies might prefer to establish a policy steering committee with representatives from all business units; others assign each new policy to an existing committee that has purview over the policy subject, says Hill.

Policy Owners

Because policy owners typically are dispersed across siloed functions without a corporate-wide view—that is, no single executive "owns" all policies—there is also a huge need for a corporate policy manager, Hill says. "It's not enough just to say, 'We have policy owners, and they're accountable,'" she says.

Freeden agrees. "Someone has to be given responsibility for managing the centralised process," she says. "It can't be an untended garden; it's a labour of love to do a great job managing policies."

The centralised policy manager should also have responsibility to guide managers through the policy creation process, Hill says: reviewing and editing policies before final approval, ensuring they conform to the company's style guide, confirming they don't violate governance principles.

Another strongly recommended idea: close, and regular, oversight of policies by a legal adviser, since laws and regulation change rapidly. Some legal expert (outside counsel, in-house legal officers with the necessary knowledge) should review policies to ensure they reflect current law and regulation rather than fall out of date.

Along similar lines, policy owners themselves should review policies too, to be sure the policies stay current with the business and still solve the problems they were meant to address. Freeden recommends such reviews at least once a year.

Kapoor stresses that centralised policy management is "not a product; it's a process." Companies that have clearly defined policies in a central repository, with effective implementation procedures and proper oversight, are well on their way to having a well-run centralised policy management program. ■

POLICY MANAGEMENT CHECKLIST

Below is a checklist regarding how to determine if your policy management system enables effective policy implementation and enforcement across the policy lifecycle:

- Provide a consistent policy management framework for the entire enterprise.
- Manage the policy lifecycle of creation, communication, implementation, monitoring, maintenance, revision, and archiving.
- Deliver a system to document, approve, monitor, and review exceptions to policies.
- Consistent format for policy assessments and surveys to gauge compliance and understanding.
- Integrated eLearning and training quizzing and attestation.
- Provide easy access to policies in the right language and format for the audience.
- Gather and track comments to policies.
- Map policies to obligations, risks, controls, and investigations so there is a holistic view of policies and metrics.
- Provide a robust system of records to track who accessed a policy as well as dates of attestation, training, and read-and-understood acknowledgments.
- Provide a user-friendly portal for policies with workflow, content management, and integration to other systems.
- Provide a calendar view to see policies being communicated to various areas of the business, and ensure policy communications do not burden employees with too many tasks in any given time..
- Provide links to hotlines for reporting policy violations.
- Publish access to additional resources such as helplines, FAQs, and forms.
- Enable cross-referencing and linking of related and supporting policies and procedures so users can quickly navigate to what is needed.
- Create categories of metadata to store within policies, and display documents by category so policies are easily catalogued and accessed.
- Restrict access to policy documents so readers cannot change them, and sensitive documents are not accessible to those who do not need them.
- Keep a record of the versions and interactions of each policy so the organisation can refer to them when there is an incident or issue to defend the organization or provide evidence for.
- Maintain accountable workflows to allow certain people to approve policy documents, and move tasks to others with full audit trails.
- Deliver comprehensive metrics and reporting on the status, implementation, understanding, and enforcement of policies.

Source: Michael Rasmussen, GRC 20/20 Research.

Meet NAVEX Global

NAVEX Global provides an array of GRC products and services that help our **8000+ customers worldwide** capture and respond to risk.

Our **Hotline and Case Management** clients have documented **better employee relations, improved brand equity and higher share value.**

Our **Third Party Risk Management** solution enables companies to **identify, assess, mitigate and monitor** the third party risk.

Our **Policy Management** software **simplifies** the process of **writing,** sharing, distributing and **attesting** to policies and procedures.

Our **interactive Online Training** supports **learning and retention** across all critical ethics and compliance topics.

Our expert ethics and compliance consultants have more direct ethics & compliance experience than **ANYONE** in the industry.

Learn more at www.navexglobal.com.

NAVEX GLOBAL™
The Ethics and Compliance Experts

+44(0)20 8939 1650 | info@navexglobal.com | www.navexglobal.com