Top 10 Ethics & Compliance Predictions & Recommendations for 2018

Once again it’s time for our annual review of trends and events that will impact your ethics and compliance (E&C) program in the year ahead.

Since our last review twelve months ago, business, societal and political events have transpired at a pace that left many with a fractured view on the industry and its expectations. Too often, however, these divisions and different points of view lead us to conclude that consensus and collaboration are impossible to achieve. While events may seem to be unfolding in unprecedented ways, the end of the year is always a perfect time to take stock of where we’ve been and to look ahead. It’s a time to regain perspective, to reenergize, and to refocus on the future.

It is in that spirit that we offer our Top 10 Predictions and Recommendations for 2018. We’ve garnered input from industry experts, our colleagues at NAVEX Global, and ethics and compliance professionals from our more than 12,500 client organizations. We look forward to hearing your comments and working with you to meet the challenges of the New Year and beyond.

1) THE SHIFT IN POWER OF VOICE IN THE STORY OF HARASSMENT

By Ingrid Fredeen, Vice President, Online Learning Content, NAVEX Global

For decades, victims of harassment have been silenced and blamed for the conduct of harassers, while the perpetrators’ behaviors have been tolerated, and, in the most egregious of cases, enabled.

Traditional methods of recourse available to victims – such as making an internal report or filing a charge of harassment or lawsuit – required effort, courage and risk by the victim, but netted little in the way of true cultural or institutional change. Victims have learned over time that individual action has minimal effect on rebalancing a culture that condones retaliation, improperly assesses the risk of keeping perpetrators on staff, and turns a blind-eye to the true cost of such behaviors.

Today, however, victims of harassment have found a new way to voice their experiences. The internet and social media tools have shifted the balance of power. And organizations in all industries and of all sizes are feeling the tremors. Sexual harassment and sexual assault allegations have surfaced about powerful and influential men, and media coverage of these revelations has dominated news cycles. Bill Cosby, Harvey Weinstein, Charlie Rose, Kevin Spacey, Al Franken, Matt Lauer, and Garrison Keillor are but a few of the names that have been revealed; certainly, there will be more.
VICTIMS HAVE FOUND A NEW OUTLET

What once was quintessentially an individual experience that received little to no public discussion (bringing an individual complaint of harassment against a manager or coworker), is private no longer.

Victims of harassment have the power of choice. They can make an internal report and hope that their organization responds properly, or they can choose to take their story public. The latter has proven to be incredibly powerful in the past 12 months, in what some have called a reckoning.

The “#MeToo” hashtag campaign has given victims a way to speak collectively – share their stories online and create a culture of empathy and activism, effectively shifting the power of voice in the story of harassment. Victims who have joined the #MeToo movement have found solace in numbers, and increased confidence – a defining effect of the events of this transformative time.

DRIVEN BY FRUSTRATION

What is driving this phenomenon? Frustration, cynicism and lack of trust in the process. Employees are tired of feeling like they are not heard, they lack power, and that their issues don’t matter. And when it comes to harassment, they are sick of working in an environment where that conduct is tolerated, or worse yet, condoned. In each of the high-profile events, the story is similar – the victim did speak out or was aware that others had spoken out and nothing had been done. The harasser had power over the victim and objecting was potentially career ending.

With victims of harassment now having increased control over how their own personal stories are told, organizations are placed in a new position. They no longer have dominion over the narrative, or ultimately the actions they must take to redress the wrong. Influential and powerful men are being removed for conduct that their employer had previously brushed off as OK.

WHAT CAN YOU DO ABOUT THE SKELETONS IN YOUR CLOSET?

Employers today are faced with a new challenge. Should they look back in time and reconsider the actions they did or did not take in response to harassment allegations? Every organization has a history with harassment allegations. Now, however, organizations must determine if they addressed those allegations properly at the time or if there are skeletons still in their closet. And what if new allegations emerge that date back to the time of the original incident?

If new allegations emerge, even if they relate to the original incident that was addressed, it is important to look into them and assess them. New information is critical in considering the appropriateness of the original action. Employers must evaluate the cultural impact of harassment, not just legal liability, as they craft appropriate corrective action. Employers should consider the totality of the circumstances as they determine the best next steps. Simply because a matter was closed out at one point, does not mean that an employer cannot revisit it, especially if new allegations emerge.

But the tougher question is: Should the employer start to review old files, even if new facts have not emerged? It is good to be knowledgeable about decisions and actions that have occurred in the past. If for no other reason, knowledge about prior corrective actions can lead to fairness and consistency as you deal with new situations. But on a deeper level, employers can learn much from how situations were handled or mishandled, and how those decisions continued to impact employees after the situation was closed. Employers should be working closely with legal counsel as they evaluate any decisions they have made in the past years, or even decades.
A fresh look at old misconduct may force employers to make difficult decisions about how the matter was originally handled, or make improvements in how they plan to handle future incidents of misconduct. If an employer chooses to go down this path, carefully consider your process, who is involved, and what the purpose of your review is. As you take a look at old events, consider the events in context, and examine them not from a pure legal defensibility angle, but rather from a perspective of culture and a commitment to a respectful environment. Ask yourself:

» Did the original handling of the situation resolve the problem, or has it persisted despite initial actions?
» How proactive are you right now – are you really trying to understand the current state of your culture, including how employees feel about their work environment?
» Was the initial decision to not address the issue at all, and if so, was that the right decision?

It is possible that old wounds have not healed, and that the failure to act properly may be continuing to negatively impact your culture.

**KEY STEPS FOR ORGANIZATIONS TO TAKE**

**Teach Your Employees**
Training, done right, can be effective. Employees need to be reminded about expectations and reassured about your values in our current climate. [High-quality training](#) helps make employees more aware of what is permissible, and what your organization expects of them. Don’t make it overly legal or seem as though you are using training just to build a legal defense. And don’t make promises or statements in your training that aren’t reflective of your true culture.

**Listen Up**
“Speak-up” culture is a great mantra but means nothing if companies do not practice a complementary “listen-up” culture. It doesn’t take long for employees to realize that their concerns, reports and questions are not being heard or taken seriously. Create a corporate culture in which employees feel comfortable raising their voices about anything from sexual harassment to feelings of being insulted. This will allow your compliance program to resolve issues before they turn into scandals, and preserve the integrity of your organization’s culture internally and its reputation externally. And don’t ever tolerate retaliation.

**Make Consequences Real**
Strong cultures are built on actions, not documents. This means you have to enforce your policies by holding people accountable for the things they say and do. If someone is guilty of harassment, they need to be dealt with in a way commensurate with their actions. Similarly, if someone makes an offensive off-the-cuff remark, it needs to be addressed not swept under the rug.

**Fund Your Culture**
You have to fund company culture the same way you would fund product improvements, corporate expansions and R&D. This gives your compliance program the resources it needs to deal with issues when they are small and manageable rather than catastrophic. This requires a long-term view of the ROI of compliance, and it will prove to be more profitable than short term gains accrued by turning a blind eye.
2) THE GLASSDOOR EFFECT: WHEN THE VIRALITY OF SOCIAL MEDIA MIXES WITH THE FRAGILITY OF TRUST

By David Banks, Senior Content Manager, NAVEX Global

Social media does not only provide channels for employees to talk, it also by its very nature encourages and cultivates discussions that may not have happened otherwise. Pair this with a brewing global state of distrust, and we start to see a culture of speaking out, as opposed to a culture of speaking up.

Today, social media is much more than just an alternative channel to whistleblower hotlines; it’s a community ready to share in success, commiserate in failure and even amplify when blaming. For instance, Glassdoor allows employees and former employees to review companies anonymously with the intent of helping potential hires make informed decisions about their next career move. There is a personal social responsibility built into the site that encourages people to say something if they see something, even if they weren’t planning to in the first place.

Similarly, “Blind” is another app we were introduced to recently, designed specifically to cultivate employee discussion. It builds on the Glassdoor idea of supporting informed career decisions and adds real-time chat features for employees to talk anonymously with one another about their jobs. This is a forum to talk about salary, benefits and work-life balance, but is also, as Mashable calls it, “The hot app where all the best Silicon Valley gossip is read right now.”

These are no doubt great tools to inform employees and hiring candidates; however, they can prove hazardous for companies who have an ethics failure, or even just the perception of one.

In May of 2017, a company was sued by the Equal Employment Opportunity Commission (EEOC) for retaliation. The alleged retaliation occurred when a disgruntled employee posted an unfavorable comment on Glassdoor and was subsequently fired. The company claims the series of events were unrelated. The EEOC disagreed. But what is more important here is the content of the comment. The employee said that the organization’s managers “do not know what the word ‘discrimination’ means, nor do they think it matters.”

Here’s the thing: whether or not the reporter’s claim is substantiated, this story garnered a lot of media attention, social media traction, and, well, we’re still talking about it here. This is going to influence the way customers, potential customers, employees, and hiring candidates view the company whenever the story comes up in a simple Google search unrelated to the incident.

Maybe for the first time, what we’re seeing is that employees are not reporting outside their organizations just because they fear retaliation, they may now be reporting externally because they receive more immediate affirmation. This is a unique challenge compliance programs will have to navigate.

In today’s typical incident management program, members of the compliance team are the ones diligently processing each report, running it through the proper channels, resolving the case and informing whistleblowers that their reports were heard and taken seriously. But on social media, all that effort is being crowdsourced in the court of public opinion by friends, family and strangers who provide immediate feedback and rally around a cause.
THE STATE OF TRUST

This conversation machine – social media – has now been warmed up and is running at full force in a time of heightened
cynicism and distrust. This has affected the nature of conversations online. According to the 2017 Edelman Trust Barometer,
an annual survey on credibility across industries, organizations, media, regions and individual roles, trust in business is at an
all-time low. This has created a landscape in which companies and their leaders are now operating in a world of
default skepticism.

This shift in trust is unhitching credibility from the wagon of business leaders and brand managers, and hitching it
instead to “a person like you.” This realignment of trust further strengthens social media’s position as a strong choice
for employee reports.

Take for example who we see as trustworthy in 2017 according to the Trust Barometer.

» 37 percent said CEOs were credible
» 48 percent said employees were credible
» 60 percent said “a person like you” was credible
» 60 percent said experts were credible

This shows us that social media is not only a very desirable place for employees to share their workplace reports, but it is also
where external audiences will get their most believable portrayals of a company. That’s to say, it’s not the communication-
department-approved press release that builds your brand reputation, it’s the employee generated tweet, Facebook post,
and Glassdoor comment that reflects the new face of your company.

We find ourselves in a real chicken-and-egg situation – which came first, the opportunity to air out an employer’s dirty laundry,
or the desire to do so. In either case, there is definitely a budding culture of speaking out, which directly competes with the
internal cultures we are trying to cultivate around speaking up.

KEY STEPS FOR ORGANIZATIONS TO TAKE

Focus on the Issue not the Social Channels

There’s not a technical fix to this problem. That’s because this is not a technical problem. This has eloquently been stated
by Bob Corlett, President and Founder of Staffing Advisors and HRExaminer Editorial Advisory Board Member: “Bad online
reviews are not an online problem. They are a real life problem. If you own a restaurant, the solution to your bad restaurant
reviews is not found online – you solve it in the kitchen.”

Similarly, focus on the content of the comment, not where the comment was made. If an employee says that your company
doesn’t know what discrimination means, don’t delete your Glassdoor account, investigate to see if there is any truth to
the statement.

Showcase Your Core Values

This is often an issue of living up to corporate core values, and convincing your employees and the general public of those
values. When a company perceived as “good” is accused of something wrong, the social community may cut them some
slack assuming the issue will be resolved and never happen again. When a company perceived as “bad,” or even neutral, is
accused of something wrong, the social community believes it is its prerogative to administer justice. This is through the
form of reputational damage. Companies can cushion their business with goodwill. This helps protect companies when a
compliance or PR crisis occurs.
Create & Enforce a Strong Anti-Retaliation Policy

Zero tolerance for retaliation needs to be policy, but it also has to be more powerful than just a policy. Employees need to know unequivocally that if they report internally, they will in no way be retaliated against. This definitely includes retaliation by the company, but also more subtle forms of retaliation from coworkers or job duty modifications.

Listen-Up Culture

Lastly – and this is the big one – companies need to create “listen-up” cultures. This is similar to a speak-up culture; however, it puts the onus of internal reporting on organizational leadership rather than employees. It’s the job of the executive team and management to support employees along the path of raising their voices for the betterment of the company. This ensures employees know that their report will be heard, taken seriously, and things will change if necessary.

Furthermore, as mentioned above, social media provides immediate crowdsourced affirmation when people speak out. Organizations and their compliance programs need to find ways to implement similar affirmation points along the incident management process. It can’t be the exact nature of public kudos that social media offers, but individual reporters need to feel like they are contributing to the organization’s mission and are appreciated for it.

The powerful draw of social media is raising the stakes for companies to build robust incident management programs embedded deep within healthy listen-up cultures. This is what will provide the channels on which employees want to report, as well as the trust they need to do so.

3) PITCHING IN WHEN DISASTERS STRIKE

By Matt Kelly, CEO, Radical Compliance & Ed Petry, Vice President, NAVEX Global

When natural or man-made disasters strike, first responders and organizations such as the Red Cross and others are quickly on the scene to assist those in need. Over the years, businesses large and small have also played a role and pitched in to help. For the most part, their efforts received little attention beyond their own employees and the local community. But in recent years, social media has placed a spotlight on these activities, both positive and negative. As a consequence, today’s businesses need to be more deliberate and aware of the impact their response to disasters can have on their public reputation and on employee morale.

For example, in the wake of Hurricane Harvey, the owner of Gallery Furniture, a furniture chain with three stores around Houston, sent out this tweet:

“Our GF N FWRY & GF Grand PKWY stores are open for those in need. If you can safely join us, we invite you for shelter and food. God Bless.”

The message was retweeted 20,000 times within the first 24 hours, adding to the company’s already positive image and building on the goodwill it had cultivated over the years with other similar acts of kindness and good citizenship. On the other hand, Best Buy is an example of how mistakes can be amplified by social media resulting in harm to a company’s reputation. Shortly after the hurricane, a Houston-based store was caught selling bottled water for $42 per case. Though the pricing seems to have been a mistake by unprepared and time-pressed store employees, residents quickly spread images of the price-gouging on Twitter. This quickly came to the attention of Best Buy senior executives, who apologized – but not before the incident captured national attention.

Given what’s at stake, companies need to be proactive about their responses both in terms of how they will act when disasters strike, and how they will respond when mistakes are made.
KEY STEPS FOR ORGANIZATIONS TO TAKE

Don’t Fake Sincerity
The Gallery Furniture example is important because it underscores a key point: you can’t fake sincerity. The CEO’s tweet was widely accepted for what it was – a sincere act of kindness – because of his company’s history. The store chain was well-known locally for donations of furniture to homeless families and schools. Similarly, the grocery chain HEB was praised for their disaster response, not because their leaders were seen working at an emergency operations center, but because the company had a history of being a good neighbor. It had a plan in place that enabled it to quickly raise disaster relief donations at its stores and dispatch “mobile kitchens” to serve meals to flood victims.

This is not just about perception – though that is important. A company’s history and existing commitment is essential if it is to respond correctly when disaster strikes. Ethics and compliance in an organization looks the same in a disaster as it does in non-emergency situations. If a company is doing ethics and compliance by operationalizing it into the fabric of the organization, it will be able to do so in the wake of a disaster. If it has only a paper program, it will have no chance to engage its stakeholders through ethical behavior during a disaster; and if it tries to do so, too often its efforts will be dimly viewed as cynical attempts to exploit the situation.

Plan to Be Prepared
Another key lesson is be prepared. When disasters strike, there’s often little time for planning. Companies that are able to jump immediately into supporting roles demonstrate not only ethical behavior but also show how creative business people can use their resources in ways perhaps different than their commercial focus. Those companies had a plan in place. They prepared and practiced their response. They were ready to react at literally a moment’s notice to respond as soon as they could access the affected areas.

The ethics office can and should play a leading role in disaster preparedness. The role of the ethics office must, however, start long before a catastrophe hits. They must help plan, prepare and practice for an emergency. The ethics office can help play a role to ensure that employees on the front lines are empowered to respond to the emergency as they see fit due to the circumstances on the ground.

Understand the Reputational Risk
As a first step, disaster response should be identified as a reputational risk area and as such should be part of an ethics and compliance risk assessment process and mitigation plan. While identifying the risk and creating a mitigation plan are important first steps, practice is also essential. Mistakes such as the one made by Best Buy, often occur when employees are unaware of how to implement plans or are unsure who has authority when the normal decision-making channels are down.

The single most important lesson for ethics and compliance professionals from 2017’s natural disasters is to practice your preparation plans. Test your emergency hotline. Make sure all contact numbers for the compliance department, C-Suite and board members are current, up to date and working. Test your communications system literally across the globe by practicing an emergency situation. Make sure you have communications and data secured and backed up. And do all you can to ensure that employees are ready and able to react and do their best to pitch in and help when help is needed.
4) AS GROWTH ACCELERATES, SO WILL THE NEED FOR COMPLIANCE & ETHICS

By Matt Kelly, CEO, Radical Compliance

In 2017, economic growth did not just continue, it accelerated in the United States, Europe, Japan and other parts of the world. That’s the good news.

The compliance corollary to that growth is a bit more cautious. As companies continue to grow more quickly and reach more markets, they encounter more ethics and compliance risks, and hit those risks earlier in their corporate lives than ever before. So organizations will need structures in place to govern their ethical culture and compliance practices as they shift into higher gears of activity.

The 2017 example of this challenge was Uber. The year opened with one of its female engineers blowing the whistle on a culture of rampant sexual harassment, and things went downhill from there: investigations into possible FCPA violations; the departure of CEO Travis Kalanick and most other senior executives; and by Thanksgiving, disclosure that Uber’s (now former) top security officer paid $100,000 to hackers to hush up the data breach of 57 million customer records.

We should give Uber the credit it’s due. Few companies see their names turn into a verb (in only eight years!) and spawn legions of startup dreamers saying, “We want to be the Uber of….” But growth without ethics and governance does nobody any favors. Growth with ethics and governance won’t simply be a feel-good mantra in 2018, it will be a business imperative this year and beyond.

KEY STEPS FOR ORGANIZATIONS TO TAKE

Understand the Importance of Governance, Culture, & Support from the Top
Rapid business growth doesn’t leave much time to create a compliance infrastructure on the fly. Can it be done? Sure – but with more cost, and more disruption to business processes already in place. This leaves the compliance function viewed as a drag on business operations, rather than a benefit.

The good news is that startups and high-growth businesses invent new processes all the time; they have the opportunity to embed ethics and compliance into those processes from the start.

For that to happen, however, the senior executives overseeing those processes truly need to value ethics, compliance and good conduct. They need to value an ethical culture.

Appreciate the Difference Between Policy & Procedure
A policy states objectives of the organization: we will never pay bribes; we will always vet third parties; we will investigate allegations of harassment immediately. Those policies can exist even as a company grows rapidly, across multiple markets.

Procedures are the steps you take to fulfill those policies – and sometimes procedures will need to differ from one business unit to the next. For example, worker protection laws in some countries might make investigations more complicated. Vetting of third parties might be done by local managers in one division and by a procurement function in another.

The mechanics of how compliance is achieved is less important than what you want to achieve. A compliance function can often let local managers guide procedures, especially so the procedure respects local law or business practicalities. But policy goals should be as universal as possible, rooted in the corporate ethical culture cited in our first point above.

Is that a tricky balancing act to achieve? Yes. It’s the chief ethics and compliance officer’s job to help everyone achieve it.
Secure the Independence & Authority to Manage Risk
A weak compliance program will never keep pace with the risks a high-growth business faces. But as the organization grows and encounters more jurisdictions with anti-bribery, data security, and other corporate conduct laws – the common thread for all is that the company has a compliance program that’s allowed to work.

With luck, 2018 will continue to be as economically robust as 2017. That means bracing and exciting times for high-growth organizations. Without a strong priority on ethical conduct, however, fast growth can veer into reckless growth.

And as we’ve seen, forcing change at those speeds can cause even the most gleaming and flashy organizations to crash hard.

5) MOVING FROM VICIOUS COMPLIANCE TO A CULTURE OF COMPLIANCE

By Carrie Penman, Chief Compliance Officer and Senior Vice President, NAVEX Global

While we have known for years that culture will always win over compliance, data from across our NAVEX Global benchmark reports and surveys of compliance officers shows a disturbing trend – employee-facing initiatives are becoming more focused on compliance rather than driving a culture of integrity and respect. Our data shows this across various initiatives including:

- Training objectives
- Writing and managing organizational policies
- Managing third parties
- Reporting systems and processes

On one hand, this is not a surprise. Our surveys and benchmark reports indicate that more program elements are under direct scrutiny in legal and regulatory action – most notably organizational policies and third-party risk management. It is understandable that organizations are tightening up processes and documentation in response to the scrutiny.

However, it is failures in organizational culture that continue to draw the reputation-destroying headlines. So how are organizations responding to these headlines? Our survey results show they are putting even more focus on compliance. This is a downward cycle that leads to what I call “vicious compliance” and ultimately, I believe, even more colossal culture failures.

Let’s look at the most recent data causing this concern. For the first time in the four years of our annual Training Benchmark Report, “create a culture of ethics and respect” dropped to number two behind “comply with laws and regulations” as the top objective for training. And the drop was significant as shown below (note that multiple answers could be selected):

<table>
<thead>
<tr>
<th>Objective</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a culture of ethics and respect</td>
<td>70%</td>
<td>57%</td>
</tr>
<tr>
<td>Comply with laws and regulations</td>
<td>60%</td>
<td>59%</td>
</tr>
</tbody>
</table>

Even more concerning were the results to the question: “How does your organization best define a culture of ethics and respect?” where multiple answers were again permitted. While “encouragement for speaking up, asking questions, and raising concerns” was the top answer (45%), very close behind was “alignment to regulatory requirements and guidelines” (40%). It is hard to understand how alignment with regulatory guidelines is the best way to define a culture of ethics and respect.
Of further concern, the lowest ranking responses included answers we believe would much better define a culture of ethics and respect:

» Retaliation is not tolerated (20%)
» Rules are enforced equally regardless of level (20%)
» Openness to alternative viewpoints and backgrounds (9%)

Finally, from our Hotline Benchmark Report and webinar survey, we continue to find disturbing results relating to issues of retaliation and lack of focus on proactive efforts to prevent or address retaliation. External agencies continue to receive a high rate of complaints of retaliation. Internal complaints remain below 1 percent of all reports received. We surveyed compliance officers about where retaliation prevention falls in their program priorities and were stunned to find that 70 percent of respondents said it was not a priority for 2017. Reducing fear of retaliation is one of the most important ways to improve a “speak-up” culture, yet it is not a priority.

Effective and mature programs must do two things well:

» Selling: This includes the messages and documentation needed to get the necessary programs funded and identified risks addressed. The audience for “selling” is usually the board of directors and senior management.

» Winning: This is what succeeds in changing culture by “winning” the hearts and minds of employees, securing their engagement in the process. Ultimately, the culture has to support compliance with policies, laws and regulations before it can be achieved. The audience here is all employees – including executive management – and often other external stakeholders.

While the messaging and approach may be different for each audience, both are critical to success. Yet what we see now is more organizations that approach “winning” by focusing on even more compliance and box-checking. This will not work.

Further, the “selling” message is missing the mark. For example, when it comes to training, we found the percentage of organizations conducting board training dropped to 44 percent from 58 percent in 2017. Of those who did board training, only 29 percent trained on corporate culture and only 23 percent trained on board oversight obligations. If the rationale for the program’s existence is not understood, and the business value behind a culture of ethics and respect not clear, boards and senior leaders will not see the value of the investment.

This brings me back to the downward cycle and the danger of focusing on compliance without attention to culture (where culture is defined as “the way things really get done around here”). I call it vicious compliance because that’s what it is: requirements to be met for their own sake, but not linked to cultural enhancement. “Vicious” describes the kind of compliance program that’s so prescriptive that all compliance officers (and their employees) do is check the boxes. In such an environment, especially when pressure mounts, employees and leaders too often look for loopholes to simply satisfy the requirement rather than thinking about what is the right thing to do. It inevitably leads to an increase in employee cynicism. Their understanding of what is really important diminishes. In this way, vicious compliance can undermine an organization’s culture and the unintended consequence is that we achieve less compliance not more.
KEY STEPS FOR ORGANIZATIONS TO TAKE

Knowing we need to find the right balance between selling and winning, what is the best approach?

Automate & Keep “Vicious Compliance” Tasks in the Back Office
» Technology and automation help reduce time spent on manual processes, improve reporting and analytics needed to demonstrate ROI of the program, and allow more time to focus on a culture of ethics and respect, but they should not be the entirety of your compliance efforts
» Use compliance and risk management messaging as needed to demonstrate the necessity of various program elements to key stakeholders

Work “Ethical Culture” Messaging & Support into All Aspects of Employee-Facing Program Implementation
» Ensure that training is role and risk based and clearly communicates the “why” of the expectations
» Develop useful, clear and consistent policies that aren’t full of legalese
» Devote considerable attention to creating a speak-up culture without fear of retaliation. Ensure issues are addressed in a timely way. Make retaliation prevention and monitoring a priority, and tell all employees about actions taken against retaliators
» Review business objectives and compensation plans to ensure that these will not put unacceptable pressure on employees to achieve results
» Ensure careful selection of business partners who will not put inappropriate pressure on employees to cross the line
» Finally, and most importantly, leadership accountability is what every employee is watching. In the end, what happens to the top performers who violate the rules will send the loudest message of all to the organization

Let’s make 2018 the year that we break the cycle of trying to “fix” culture with more compliance.

6) CYBER SECURITY IS EVOLVING & SO IS COMPLIANCE’S ROLE IN PREVENTION & MITIGATION

By Pamela Passman, President and CEO, CREATe Compliance

Cyber security has been a priority – 2017 has made it an urgent one. Companies of all sizes and maturity levels are falling victim to cyber attacks. Large enterprises are experiencing breaches that compromise the personal information of millions upon millions of individuals, while small-to medium-sized organizations are being targeted as entry points to infiltrate supply chains and gain access to larger organizations. This has made third parties an increased concern for cyber risk, and rightfully so. According to the NAVEX Global 2017 Benchmark Report, cyber security and data protection have become the top concern for organizations’ third-party risk management programs.

Cyber attacks are not only increasing in frequency and size but also in complexity. New threat types are emerging, and old threats are manifesting in new ways. The now infamous WannaCry attack is a new variation of an old threat and has made “ransomware” a household term. Whereas stealing information has always been a concern, now cyber criminals are holding that information hostage for a ransom at the threat of sharing it publicly, manipulating it or destroying it.

The cyber security environment is expanding as well. Data is proliferating more rapidly than ever and there has been a dramatic increase in the number of digital devices connected to the global IP network. The use of these devices by employees to store and access sensitive information has effectively increased the surface area that cyber security programs are required to protect.
In short, companies are starting to feel the urgency of the risks today. As security experts like to say, “There are two types of companies: those that have been hacked, and those who don’t know they have been hacked.”

**NIST FRAMEWORK IS BECOMING A PREREQUISITE FOR DOING BUSINESS IN THE U.S.**

Governments often use public procurement regulations to influence and advance business practices, and cyber security is a prime example. On that front, the National Institute of Standards and Technology (NIST) Cyber Security Framework is becoming the de facto approach for the private sector to use to advance their cyber risk management practices.

The Department of Defense (DOD), the General Services Administration (GSA), and the Department of Health and Human Services (HHS) have already incorporated some guidelines from the NIST Framework, particularly into their supply chain regulations. The DOD has required the highest level of compliance for contractors among government agencies, instituting mandatory cyber security requirements to all relevant defense contract solicitations and imposing contract terms requiring compliance with several standards highlighted in the NIST Framework. For contractors that deal with its data or IT systems, HHS contracts feature a security clause requiring fulfilment of the standards within the NIST Framework for risk management and security controls in federal information systems.

The private sector has generally been supportive of making cyber security requirements more consistent across the different government agencies’ contract requirements, and the NIST Framework is often mentioned as a basis for developing more consistency among government procurement practices.

**NEW GLOBAL REQUIREMENTS**

Cyber security standards are being raised throughout Europe and Asia as well, with national governments encouraging tighter security measures when working with the private sector.

- **European Union:** The new Network and Information Security (NIS) Directive calls for additional security protocols specific to government agencies when utilizing digital service providers and considers extending these measures to contractors and suppliers

- **United Kingdom:** In order to qualify for government awards, private sector government contractors must comply with the Cyber Essentials Scheme, involving protection of citizens’ personal information or government data classified at the “Official” level and above

- **Australia:** Government contractors and suppliers must comply with Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) requirements; the Department of Finance requires suppliers to include data protection plans using industry accepted standards with their proposals/contracts and are required to report breaches

- **Japan:** Contractors are required to abide by security policies aligned with government procurement guidelines

**KEY STEPS FOR ORGANIZATIONS TO TAKE**

Cyber security risk usually extends to all business units, operational units, employees and key third parties. That is why the compliance function is playing a critical role. Whenever organizations need to do something on an ongoing and systematic way, where people are to be held accountable, Compliance is front and center. Here are five ways Compliance can play a pivotal role in a cross-functional approach to cyber security.
Own or Implement a Cyber Risk Assessment
Compliance regularly operates in the world of risk assessments and understands how to identify an organization’s greatest risk by developing a comprehensive risk profile. With a full understanding of a company’s risks and threats, Compliance can guide an organization’s approach and control environment to effectively manage and mitigate risks while at the same time deploying scarce resources toward the most significant among them.

Embed Regulatory Requirements into Business Operations
As with other enterprise-wide risks, cyber security is a regulatory compliance challenge for an increasing number of companies. As mentioned above, there is a growing number of fairly nuanced regulations addressing cyber security that apply to private and public sectors, specific industries, and specific data sensitivities. The compliance function has the competence to design and implement policies, procedures and controls that meet these requirements.

Connect the Functional Dots Across the Organization
Cyber security is an enterprise-wide risk and requires a cross-functional approach for management. Compliance is skilled in building a systematic approach across an enterprise. It has the regular contact and seniority to engage effectively with the C-suite, Legal, HR and other functional and operational teams. Compliance can connect the dots across an organization.

Address the “People & Processes” of Cyber Security
Cyber security involves an integrated approach to “people, processes and technology.” The compliance function has deep insights into how to engage broadly with employees and how to collect and analyze data through the monitoring and audit processes needed to manage risks. This proficiency in influencing employee behavior and organizational culture are necessary skills needed to complement the protection efforts deployed by the technology function.

Developing & Tracking Program KPIs
As another aspect of monitoring, Compliance has expertise in developing key performance indicators (KPIs) and specific metrics to track progress and ROI, as well as developing a rhythm for board reporting, and reporting externally, as appropriate. Consistent application of KPIs will help cyber security programs mature over time with a cadence toward continuous improvement. Being on a trajectory of maturing practices not only builds stronger resilience but also demonstrates to customers, partners and regulators, as needed, a commitment to risk management, compliance and best practices.

Now, more than ever, Compliance must play an integral part in any organization’s cross-functional cyber security program to make sure such efforts are enterprise-wide, consistent with regulatory requirements and embedded in how the company operates and its people conduct their work. As with other compliance issues, organizations will need to be in a position to tell their story of continuous improvement through KPIs, metrics and demonstration of using best practices.
7) THE NEW VOICE OF THE WHISTLEBLOWER

By Greg Keating, Partner, Choate, Hall & Stewart

Seven years after the launch of the U.S. Securities and Exchange Commission’s (SEC) whistleblower program, the voice of the whistleblower is starting to sound very different. It's a little stronger, a little bolder, and a little louder.

A review of the SEC whistleblower program’s 2017 Annual Report to Congress gives us a quantifiable look at the monetary force behind this voice. Since the SEC issued its first whistleblower award in 2012, it has proceeded to award approximately $160 million to individuals who have come forth with a report that led to a successful enforcement action. Fiscal year 2017 was a particularly active year with the SEC doling out three of its 10 largest awards of all time. And awarding a total of $50 million (almost a third of all award dollars to date) to 12 individuals.

There is definitely something happening here. More reporters are coming forth with substantiated reports, and the awards for those reports are increasing in number and size.

Going deeper into the annual report, we get a particularly interesting glimpse at the future with a look at the Office of the Whistleblower’s Investor Protection Fund. This is the fund that ensures whistleblower award payments do not subtract from the money to be rightfully returned to investors. Therefore, this is also the fund from which the office will pay out future whistleblower awardees. After the balancing of the 2017 budget, this fund currently has over $320 million dollars in it. That is more than double what the SEC has paid out in all the years it has been in operation. So the SEC is not only poised to maintain its steady growth in annual payouts, but ready to ramp it up as well.

The volume and size of awards are not the only thing on the up. Tips, the submitted reports of whistleblowers, have increased even more drastically. In 2011, the first full year of data from the program, the SEC received 334 whistleblower tips. A modest start. In fiscal year 2017, the program received 4,484 tips.

The type of money the SEC is sitting on is not only incentivizing reluctant whistleblowers, but it is also fueling investment from an ever-expanding cadre of constituents. This is especially true for venture capitalists who are backing whistleblowers to fuel high-stake cases for a portion of the payout. This type of support makes whistleblowers louder than ever, and more capable than ever to survive, and prevail in lengthy court cases.

SILICON VALLEY MIGHT BE BREAKING ITS SILENCE

The majority of whistleblower cases that financially impact corporations have been mostly squared on the finance and healthcare industries; however, there are signs that tech may soon be getting its fair share of litigation and enforcement.

One of the most prominent whistleblower plaintiff attorneys, Jordan Thomas, has recently put Silicon Valley on notice. This is because, while only a minority of tech startups fall into the publicly traded realm, many fall under the SEC rules and regulations because of the nature of their funding and structure. As Thomas states, “The SEC has specifically signaled that it is closely scrutinizing the way in which mutual funds calculate valuations of their holding in these companies.”

Regulatory scrutiny is increasing, and the voice of the whistleblower in the Valley is growing louder as well – mostly by a strength in numbers. The most notable indication of this shift in 2017 was former Uber employee Susan Fowler’s expose, “Reflecting on One Very, Very Strange Year at Uber,” which details a series of compounding instances of sexual harassment she experienced while at the ride-sharing giant. This case, as well as the numerous others coming out of Hollywood, is cultivating an environment of motivation and safety that may effectively shift Silicon Valley’s culture of silence into a culture of silent-no-more.
KEY STEPS FOR COMPANIES TO TAKE

External whistleblower reports can thoroughly shake a company, its reputation externally, and its culture internally. Aside from eliminating wrongdoing, there is no benefit to a company by having its dirty laundry aired, litigated and charged on the mainstage. Companies should do their best to ensure they hear and resolve whistleblowers’ reports internally before they are motivated to go outside. Here are a few best practices to not just hear whistleblowers, but to actually show you’re listening.

Take a Very Hard Look at Your Internal Complaint Procedure
Your company needs to have a robust whistleblower hotline and incident management system. This ensures employees have multiple channels for reporting. These avenues must also be transparent, and, well, real. As a compliance practitioner responsible for protecting your organization, you should be testing these channels regularly to ensure reports are being properly received, processed, escalated and ultimately resolved efficiently and effectively.

Employ Clearly Thought out Investigative Protocols
Every company should spend time thinking through in advance how it will investigate cases of variant natures and severities. This should include a plan for dealing with the individual who comes forward during the process to ensure they do not feel shunned, ostracized or retaliated against in any way, shape or form.

Train Frontline Managers
Compliance training may be the most important thing companies can do. There needs to be a renewed commitment to training, most significantly for frontline managers. Managers need to understand what a complaint and protected activity look like. And they need to know how to respond to internal reporters. There is no room for responses like, “keep your head down, and I’m sure it will get better.” Finally, managers need to know what they are supposed to do once they get a report, how to escalate it, and what their role is in the investigation.

Whistleblowers, and the internal corporate programs managing them, have always been an integral part of not just improving corporate transparency, but also improving a company’s performance and bottom line. Today, the voice of the whistleblower is getting stronger and louder and companies need to double down on their incident management processes and efforts to develop a healthy speak-up culture that encourages employees to report internally first. This will ensure companies have a chance to resolve issues before they fester and result in significant reputational or financial damage to their brands.

8) MANAGING CULTURE & FREE SPEECH IN POLARIZING TIMES

By Ingrid Fredeen, Vice President, Online Learning Content, NAVEX Global

Today, the chasm that divides us feels deeper than it has felt in the past several decades. Our debates today aren’t just about big government or little government or whether we should fund a new school building; they are about race, gender, sex, sexual orientation, gender identity, national origin, and religion – and people’s right to fair treatment, protection and the rights and benefits enjoyed by others. And often, our conversations fuel and highlight the differences among us rather than bring us closer together.

These conversations are happening everywhere (and yes, this means they are happening in your workplace as well). Individuals are finding ways to express themselves through action such as attending protests and rallies, and showing solidarity through common behaviors like taking a knee. And they are expressing themselves through speech by commenting on social media, posting images and content, joining online groups, and debating at work. This past year has given us a lot to talk about – from religion, terrorism, immigration, race equality, justice, harassment and equal treatment.
Often opinions are fueled by personal beliefs, religious teachings, and experiences. And while discussion is healthy and necessary, it can get heated and disrespectful quickly. Skeptical? Read the comments section of any online post about a controversial topic, and you’ll get a sense about what people are really thinking – the comments and the heated nature of the interactions would easily be considered offensive or inappropriate in any workplace.

In addition, social media has eradicated any line of demarcation between work and personal life. If you have a social media presence, your “private” life is now very public.

This is the new norm. Things are not going to change any time soon. Employees will continue to bring these conversations into their workplaces (virtually and personally). These heated exchanges can damage workplace relationships, and give rise to claims of harassment and discrimination.

Simply put, the workplace is not the best forum for these conversations, and now is the time for employers to address it head-on.

**KEY STEPS FOR COMPANIES TO TAKE**

Employers need to learn how to manage discourse while maintaining their culture, and at the same time help their employees navigate these challenging times. There are a couple of important things to keep in mind as an employer:

» First, consult with a lawyer; there are a lot of laws that can come into play when you are dealing with speech and behavior

» You have a responsibility to foster the culture you want for your employees – elevate the importance of respectful communication

» Don’t take sides – unless you are in the business of taking sides or it’s critical to your business

» Create a workplace that is safe and respectful. Quickly and professionally address any inappropriate discussions

» Train your managers so they know how to handle heated disputes as work

» Train your employees so they understand that unfettered speech at work it not OK and it has consequences. Remind employees about key policies, including your harassment, workplace violence, and business conduct policies

» Be prepared to handle incidents involving employees who engage in offensive conduct off-duty; whether you chose to make it your business or not, you must own your decision

Taking these steps will help organizations ensure that they are demonstrating their commitment to a healthy corporate culture and fostering an environment of ethics and respect in the workplace – no matter what’s going on in the world around us.

---

**9) DATA PRIVACY HAS BECOME A BIGGER BLIP ON THE CCO RADAR**

By Amanda L. Gratchner, Principal, IdeaLegal & Carrie Penman, CCO and SVP, NAVEX Global

Data privacy is by no means a new topic. However, privacy laws and the environments they regulate, have evolved dramatically. Regional and U.S. state-specific laws are developing rapidly and so is enforcement of those laws. This has made the financial and reputational impact of data privacy feel “real” and very new to many legal, IT and compliance teams, not to mention corporate executives and board members.

Data privacy laws are also increasingly more complex and require organizations to make bigger commitments, in both
resources and budget, to stay abreast of new laws and the nuances they embody. Organizations need to adopt a privacy strategy through which they view their data, including all geographic locations in which they do business, store data, or utilize vendors.

Developing and monitoring data management practices is always a key attribute to any privacy compliance program. You will need to have a good idea of how and where you are storing your data, whether it is moving across borders, and if data localization regulations apply. You also have to consider how your privacy management practices will be replicated and managed in all the countries in which you transact business. With new regulations, the protection systems you are building will not always be sufficient across all jurisdictions. If not done properly, this can actually increase data vulnerability.

As we come out of 2017 and move into 2018, these are not the only trends CCOs need to be aware of, but they are a few of the most pressing.

**EU GENERAL DATA PROTECTION REGULATION**

The General Data Protection Regulation (GDPR) definitely rises to the top of virtually any privacy discussion. The GDPR is not just a major concern for privacy officers, but it may also prove to be one of the biggest issues facing the GRC space in 2018. The scope of the regulation is broad, its extraterritorial reach extensive, and penalties for non-compliance are high. There is a lot built into this new regulation and EU regulators expect organizations to be in compliance by its enforcement date of May 25, 2018.

**What You Need to Know**

- **Penalties:** Failure to comply with the GDPR can result in fines of up to 4 percent of your organization’s global annual turnover (revenue), or up to €20 Million, whichever is greater. Penalties for lesser offenses, such as failure to keep accurate records or failure to promptly notify of a breach may result in smaller fines. These fines start at 2 percent of annual turnover or €10 Million, whichever is greater.

- **Extra-Jurisdictional Reach:** Under the new territorial scope of the GDPR, many organizations that were not previously subject to the EU directive will now be subject to GDPR. It cannot be assumed that because you do not have a business operation within the EU that you do not have to abide by the rule. The law will apply to many organizations that sell goods or services within the EU regardless of business presence.

- **Privacy Impact Assessment:** Performing privacy impact assessments is a requirement under the GDPR for controllers. These assessments must be conducted across all areas of the business where personal data is collected, managed and/or used.

- **Privacy by Design:** Data protection is now a legal requirement under the GDPR. This means that data protection and privacy-by-default concepts not only have to be embedded into the development life cycles of products but also across the enterprise to areas like vendor management and selection, human resources and policy and procedures. Privacy needs to be a holistic consideration.

- **Breach Notification:** The GDPR requires that controllers notify supervisory authorities within 72 hours of becoming aware of a breach of personal data. There are some exceptions such as when the breach is unlikely to result in harm to the individual, but generally organizations will need to abide by the new 72-hour rule or have a very good reason for delay.

The GDPR is a broad and complex regulation. It is key though for CCOs to understand, at least at a high level, the requirement and potential penalties for non-compliance. What is crucial to understand is that the law is intended to protect the owner of personal data – and that’s the individual, not the organization.
DATA BREACHES

Data breaches aren’t just a U.S. phenomenon. Although we have been seeing breaches at a higher volume and scale in the U.S., this is a global concern. The key is to plan, prepare and then plan some more.

What You Need to Know

» Policy & Procedure Resilience: Know how your policies and procedures will perform in a data breach. Are they comprehensive and pervasive enough to combat the complexity of modern attacks and common human errors? Test your policies and employee knowledge.

» Cross-Jurisdictional Breach: Breaches that affect a variety of data sets and/or regions make prevention and containment exceptionally difficult. This requires organizations to understand where their data is, regardless of location around the globe, and the unique regulations that apply to that data so they can respond quickly when something happens.

» Crisis Communications Plan: No one wants to hear that their data has been compromised; however, it is still better for you to inform your employees, the public, and shareholders in a thoughtful and accurate way. It’s good practice to keep in mind that data privacy is about building trust, so having an effective crisis communication plan will help your organization be responsive and transparent in an effort to preserve the trust of your people.

VENDOR MANAGEMENT & DATA PRIVACY

Vendors can often be the Achilles heel of an organization. Today this is a serious concern for data privacy. Vendors present another opportunity for data loss or compromise for which your organization may be responsible. Companies of all sizes are being targeted by cyber and data attacks as a way to infiltrate connected third parties and work their way up the supply chain.

What You Need to Know

» Vendor Privacy: Ensure privacy, where applicable, is part of every vendor agreement. Chances are you already have a vendor management program. You can embed privacy protocols into these existing programs instead of developing and implementing a separate privacy program altogether.

» Audit & Notification Rights: The big privacy issue with vendor management is that you don’t always know when a risk or issue comes up. This significantly reduces your response window for prevention and containment. Vendors should not only be required to notify you in the event of a breach within a reasonable period of time, but also of any suspected breach or any risk associated with the data they have or access. Your organization should also retain the right to audit the data practices of each vendor to ensure they meet your privacy standards.

» Indemnification: In the event of a damaging breach, your vendor agreements should ensure that your third party indemnifies you appropriately for losses.

KEY STEPS FOR COMPANIES TO TAKE

Identify Your Privacy Lead

Even if your organization is not legally required to hire a Data Privacy Officer (DPO), it is still best practice to appoint someone to stay informed and lead your team on data privacy concerns.
Develop a Privacy Committee

Similar to hiring a DPO, you may not be legally required to have a privacy committee, but it will support your organization in embodying a “privacy by design” mentality throughout your business operations. This committee could naturally be woven into a preexisting compliance committee or serve independently.

Understand Your Geographical Footprint

Map out all jurisdictions in which you operate and know exactly which laws apply. This should be a responsibility of your privacy lead, so that someone knows the suite of laws that apply to your operations and how you are addressing your compliance with those laws.

Train Your Employees

Data breaches are still often a result of human error. Ensure your employees are being trained on all the forms of modern cyber attacks like phishing, but also on the larger practice of social engineering.

10) INNOVATION, STAGNATION & THE FUTURE OF THE COMPLIANCE PROFESSIONAL

By Ed Petry, Vice President, NAVEX Global

It’s been more than thirty years since Ronald Reagan created the Packard Commission, “The President’s Blue Ribbon Commission on Defense Management.” The first report of the Commission included what is rightly seen as the marching orders that gave rise to the modern corporate ethics movement:

“To assure that their houses are in order, defense contractors must promulgate and vigilantly enforce codes of ethics that address the unique problems and procedures incident to defense procurement … They must also develop and implement internal controls to monitor these codes of ethics and sensitive aspects of contract compliance.”

Since then, business leaders, academics and others have shared and debated ideas about ethics, compliance, internal controls and governance. The early ethics officers borrowed from one another and often collaborated on innovative approaches to common problems. Over time, the business ethics movement gained momentum and spread worldwide. Within a decade, working professionals in the field settled on best practices for organizational compliance. As new technologies became available and new challenges emerged, innovations continued, especially with respect to training, reporting and data management.

As a group, ethics officers are risk averse by nature – in fact it’s safe to say that avoiding or minimizing risk should be their most essential trait. But when you build a profession out of risk averse people, no one should be surprised when out-of-the-box thinking is rare and even discouraged. Better to be safe than sorry.

In recent years, at conferences and through associations and networks, professional discussions have grown more and more focused and granular. This is to be expected. What was first a movement has become a profession, and much of our time and energy is now devoted to fine tuning ethics and compliance programs, developing efficiencies, and addressing gaps and weaknesses that surface. Thus, as the ethics and compliance field has matured, an unfortunate development has occurred. Our insulated and risk-averse discussions have inadvertently created the conditions that can lead to stagnation. If not corrected, this can eventually undermine our relevance.

In the early days of the movement, innovation and new perspectives often came from academia. However, academic business ethics research is now either dominated by an anti-business bias or it is overly theoretical and impractical. Business ethics centers and think tanks are geared toward the lucrative leadership retreat model. The leadership retreat model features
annual getaways for corporate leaders where they can discuss ethics and values with “thought leaders.” These retreats may inspire some, but have little lasting impact on improving corporate cultures or advancing ethics and compliance initiatives. Associations and conferences, once a key source of new ideas, are now indebted to the status quo, and presentations are mostly old ideas dressed up in new packages.

How can we rekindle innovation, collaborate across the industry and challenge one another to tackle new problems and solve old problems better?

A LOOK TO THE FUTURE

Looking ahead, we do have reason to be optimistic. Our profession is still growing. New ethics officers from diverse backgrounds are joining our ranks. Global and regional organizations are challenging what has for too long been a U.S. and European-centric industry. Hard lines such as those that divided corporate social responsibility and values-based programs from E&C are being blurred. Most importantly, old networking models are giving way to online networks that provide new and unprecedented opportunities to share ideas and collaborate. The only thing standing in the way of innovation is a willingness on our part to be bold, to take some risks, and challenge our assumptions.

We can be sure that new ideas and new approaches will emerge, and they are likely to be novel ideas that those of us who have been around for a while would never think of. While we await these new ideas, and in the interest of priming the pump, we offer a few questions for consideration in the hope of jump starting new debates in 2018. Our questions start with the position of the ethics officer – its function and effectiveness and how we can best approach the challenges we face.

SOME QUESTIONS TO CONSIDER

The position of full-time ethics officer was considered an experiment when it was introduced in the late 1980s. It was one of many possible ways of ensuring ethics and compliance accountability while spearheading the development of ethics and compliance initiatives that would take root throughout the organization. Is it time to assess the results of the experiment? Are there alternative options for the ethics office or different ways to better meet our goals? For instance:

» Have regulatory and other pressures distorted the current role of the ethics office to such an extent that there is simply not enough time to perform all of its essential functions? How much time does today’s ethics officer spend on managing their program, crunching data and providing status reports versus time spent interacting with employees? Is it time for an objective reevaluation of priorities?

» Can leadership assume even greater assigned responsibilities for ethics and compliance? As a start, should all rising leaders in your organization have an assigned ethics function for a period of time as part of their grooming for senior positions? Not only would this approach add resources, but it would also expand the diversity of talent and perspectives available to your office. And in the long-run, it would build a cadre of leaders who have firsthand experience with the ethics function.

» Instead of a central, corporate ethics officer overseeing all ethics initiatives, is it better for some program elements – risk assessment, for example – to be handled by other functions such as Audit?

» Should a portion of your ethics and compliance training budget be set aside to train managers so that they are comfortable doing more to support ethics and compliance?

» Especially in wide-ranging/diverse organizations, can a matrix of part-time local ethics officers who are coordinated by a corporate ethics officer be created? Local ethics officers can often better understand and influence cultures and sub-cultures, and are more flexible to address local matters.
Conclusion

At NAVEX Global, we rely on the insights we gain from research and ongoing discussions with our 12,500 clients – the largest ethics and compliance community in the world. Throughout the year, we will continue to provide thought leadership, facilitate open dialog and encourage the sharing of best practices to grow and strengthen the ethics and compliance function. Our experience demonstrates that the best insight and the most valuable advice comes from working with clients to solve their day-to-day challenges.

In the year ahead, we encourage you to join the NAVEX Global conversation. Give us your feedback to this article. Subscribe to our blog, Ethics & Compliance Matters. Participate in our webinars. Visit with us at conferences. Join our newsletter lists. And let us know what you see as emerging trends and challenges – and how we can help.

ABOUT THE AUTHORS

Ingrid Fredeen, Vice President, Online Learning Content, NAVEX Global

Ingrid Fredeen, J.D., Vice President, Online Learning Content, has been specializing in ethics and legal compliance training for more than 10 years. She has been the principal design and content developer for NAVEX Global’s online training course initiatives utilizing her more than 20 years of specialization in employment law and legal compliance. Prior to joining NAVEX Global, Ingrid worked both as a litigator with Littler Mendelson, the world’s largest employment law firm, and as in-house corporate counsel for General Mills, Inc. a premier Fortune 500 food manufacturing company.

Amanda Gratchner, Principal, IdeaLegal

Amanda is a principal at IdeaLegal and former Global Privacy Officer & Senior Counsel for NAVEX Global. Amanda is a Certified Information Privacy Professional (holding both CIPP-US and CIPP-EU certifications), Certified Ethics and Compliance Professional and is licensed to practice in both Oregon and Washington. She is a member of the International Association of Privacy Professionals, the Society of Corporate Compliance Executives, and the Association of Corporate Counsel.

Greg Keating, Partner, Choate, Hall & Stewart

Gregory Keating is a partner in Choate’s Labor Employment & Benefits Group. He is recognized as a national authority in the area of whistleblowing and retaliation. Greg litigates a wide range of whistleblower cases and has extensive experience handling matters arising under the Sarbanes-Oxley Act, the Dodd-Frank Act, the False Claims Act and the Foreign Corrupt Practices Act. Greg is the principal author of the national treatise on Whistleblowing and Retaliation: A Guide for Human Resources Professionals and Counsel, now in its 5th edition. He was appointed to serve as a management representative on the Whistleblower Protection Advisory Committee in 2012 and 2014. In addition, Greg has been named America’s Leading Lawyers for Business by Chambers USA, The Best Lawyers in America and Super Lawyers.
Matt Kelly, CEO, Radical Compliance

Matt Kelly is a consultant who studies corporate compliance, governance and risk management issues. He is the founder of Radical Compliance, which provides consulting and commentary on compliance, audit, governance and risk management. Previously, Matt was the editor-in-chief of Compliance Week, a corporate compliance newsletter, from 2006 through 2015. Matt continues to be a source of industry thought leadership through the RadicalCompliance.com blog, where he shares his thoughts on business issues and speaks on compliance, governance and risk topics frequently. He was named “Rising Star of Corporate Governance” by Millstein Center for Corporate Governance in its inaugural class of 2008 and was named to Ethisphere’s “Most Influential in Business Ethics” list in 2011 (no. 91) and 2013 (no. 77).

Pamela Passman, President and CEO, CREATe Compliance

Pamela Passman is president and CEO of the Center for Responsible Enterprise And Trade (CREATe.org), and its wholly-owned subsidiary, CREATe Compliance Inc., two entities with a common mission to promote leading practices in cyber security, intellectual property (IP) and trade secret protection, and anti-corruption. Prior to founding CREATe in 2011, Passman was corporate vice president and deputy general counsel, Global Corporate and Regulatory Affairs, Microsoft Corporation. From 2002 to 2011, Passman led Microsoft’s global public policy work and regulatory compliance across a range of issues, including privacy, security and cloud computing issues. She worked closely with business leaders and research and development teams to advance Microsoft’s businesses in China and other emerging markets.

Carrie Penman, Chief Compliance Officer & Senior Vice President, NAVEX Global

Carrie is the Chief Compliance Officer of NAVEX Global and Senior Vice President, Advisory Services. Carrie has been with NAVEX Global since 2003 after serving four years as deputy director of the Ethics and Compliance Officer Association (ECOA). Carrie was one of the earliest ethics officers in America. She is a scientist who developed and directed the first corporate-wide global ethics program at Westinghouse Electric Corporation.

Since joining NAVEX Global, she has conducted numerous program, risk and culture assessment projects globally for its clients and regularly works with and trains boards of directors and executive teams. She also serves as a corporate monitor and independent consultant for companies with government agreements. As Chief Compliance Officer, she oversees NAVEX Global’s internal ethics and compliance activities employing many of the best practices that we recommend to our clients. In 2017, Carrie received the Ethics & Compliance Initiative (ECI) Carol R. Marshall Award for Innovation in Corporate Ethics for an extensive career contributing to the advancement of the ethics and compliance field worldwide.
Ed Petry, Vice President, NAVEX Global

Ed Petry, Ph.D., vice president at NAVEX Global, joined the organization in 2004 after almost 10 years as executive director of the Ethics and Compliance Officer Association (ECOA). Ed served on the Advisory Panel to the U.S. Sentencing Commission, which was responsible for the 2004 revisions. Earlier in his career, he was a tenured professor of ethics and a prolific author and researcher. Ed's work with the ECOA and the Sentencing Commission helped establish the best practices and standards by which the industry is measured today. Ed applies his over 25 years of experience to help companies assess their ethics and compliance programs. He has also written many of the most admired codes of conduct for companies worldwide across nearly every industry.

David Banks, Senior Content Manager, NAVEX Global

David is the editor of NAVEX Global's Ethics & Compliance Matters Blog. He works with thought leaders in the ethics and compliance industry to source, create and distribute content that educates, informs and inspires the daily work of compliance professionals.