NAVEX GLOBAL®
The Ethics and Compliance Experts

WHITEPAPER

What GRC Will Look Like by 2025 and How to Plan for It Now

By Matt Kelly CEO, Radical Compliance

The range of subjects that get bundled into "governance, ethics, and compliance" is huge—so at first glance, trying to identify the major forces that will shape GRC over the next five to 10 years might seem a bit hopeless.

Political dysfunction is on the rise around the world, including here in the United States. The economy continues to wheeze along unimpressively. Investors are more demanding. The "extended enterprise" is growing ever more complicated, and risk events that are difficult to evaluate are becoming more common at the same time. All those dynamics can leave GRC professionals with queasy feelings about the future.

That queasiness may be well-founded. More precisely, you can probably trust your gut feelings that *some* parts of GRC will be more difficult by 2020 or 2025. Yet when you consider the basic direction of where technology, business operations, the economy, and even simple demographics are all going—getting a feel for how GRC will look and feel in the next decade isn't so hard.

For starters, we can put the many trends likely to affect GRC into four broad categories:

- Global political, economic, and demographic forces;
- Regulatory attitudes;
- Technology changes in how individuals work;
- Operational changes in how businesses work.

Some trends will exist in one category (say, technology changes in how people work) and have repercussions in another (operational changes in how businesses work). Some are likely to make compliance overall more difficult, but help compliance officers in their jobs and careers. Above all, specific companies, industries, and compliance officers will all have their own individual experiences in the decade to come: some good, some bad.

So let's consider what those large trends are likely to be, and then spend some time contemplating how companies and compliance officers are likely to confront them.

TREND #1:
THE PRIMARY ECONOMIC CONDITION IS LIKELY TO BE SLOW GROWTH AND LOW INTEREST RATES

The safest assumption to make is that the economy we see today—sluggish growth, low interest rates, tepid demand for products and services—is likely to persist. We may experience a recession or somewhat more energetic growth, but not soaring activity like the 1990s or awful financial crisis like 2009. Most days, most things stay mostly the same.

TREND #2:
CRISES OF *POLITICAL* GOVERNANCE ARE GOING TO CARRY BUSINESS AND ECONOMIC CONSEQUENCES

One prime reason for the economic emphysema around the world today is that nations cannot resolve domestic and international differences to let business flourish. We see political governance failures in Russia, Brazil, the Middle East, China, the European Union, and in the United States. That leaves countries either unable to rid themselves of corruption, or to act decisively to reinvigorate economic growth.

TREND #3:
DEMOGRAPHICS WILL LEAD TO SHORTAGE OF SKILLED LABOR

Within the next 10 years we will see Baby Boomers retire from the labor force, with too few Generation X members to replace them as senior managers and Millennials still in their 20s and 30s. If the labor force participation rate continues its slow decline (from 67 percent in 1997 to 62.5 percent in 2015)[1], that will leave businesses struggling to find skilled labor even with a slow economy that produces a smaller number of new jobs.

TREND #4:
REGULATORS WILL DEMAND BETTER *ENTERPRISE* RISK MANAGEMENT TO HELP THEIR *SYSTEMIC* RISK MANAGEMENT

We've already seen this attitude emerge in the financial sector, as regulators pressure boards to do better at "culture risk" and risks within compensation policies. Their goal of preventing systemic failures (see financial crisis, 2008) means they will hold business to higher standards based on outcomes, rather than what we saw pre-2008: individual firms compliant with specific regulations, while systemic risks accumulated to critical mass.

TREND #5:
THE DEFINITION OF "THE ENTERPRISE" WILL KEEP EXPANDING

This is the logical conclusion of laws such as the UK Modern Slavery Act, the Foreign Corrupt Practices Act, or the Conflict Minerals Rule, which all force companies to assume more responsibility for their supply chain. It is also the implication of broader business trends to outsource business functions, use contingent workers, or otherwise embrace the "gig economy."

[1] U.S. Bureau of Labor Statistics

TREND #6:
BUSINESSES WILL CONTINUE TO SHIFT FROM TANGIBLE ASSETS TO INTANGIBLE ASSETS

From 2010 to 2015, the total value of intangible assets (patents, trademarks, brand value, goodwill) reported by U.S. filers went from $3.73 trillion to $4.87 trillion—or as a portion of all assets, intangibles rose from 7.71 percent to 9.26 percent[2]. Putting more value in data requires better collection and analysis of that data. Likewise, putting more value in employee skill and brand reputation will drive more focus on corporate culture.

TREND #7:
CYBER SECURITY WILL CHANGE

The gurus of IT security know that cyber security based on authentication (passwords, tokens, challenge questions) is reaching its limit. In the modern world of open wi-fi networks, mobile devices, the internet of things, contingent workforces, and endlessly clever hackers, we will need to move to a system of *identity assurance*, where businesses monitor users of their networks to gauge "normal" behavior and investigate abnormal activity.

TREND #8:
RISK ANALYTICS WILL KEEP GETTING BETTER, AND MORE IMPORTANT, AND MORE COMPLICATED

This really is the consequence of all the trends above. By 2025 compliance officers will face persistent economic and regulatory risks, with not enough people skilled enough to manage them well, as more value is placed on the intangible qualities of an enterprise, which itself will be more expansive and ill-defined than ever.

How Compliance Officers Can Prepare Now

So what happens next? The question facing compliance officers today is this: How can you structure your E&C program so you can meet the challenges coming tomorrow? Fundamentally, what you do won't change much; how you do it will need to change enormously.

A big part of the answer is that you will need to be able to leverage technology to "enhance" the GRC function—the people running it, the policies you distribute, the risks you monitor, the investigations you run. You'll need to enhance all of it. (See the breakout box below for specific examples of the need for automation.)

That statement may seem obvious at first glance, but the imperative behind it is more powerful and subtle than that.

It does *not* mean that compliance officers should learn the latest social media app all the Millennials are using, or memorize every feature of every GRC software suite. Rather, you'll need to understand how to make technology augment all your compliance operations.

[2] Analysis from Calcbench, looking at all U.S. filers with financial data tagged in XBRL

In more human terms, this means compliance officers will need to be able to do three things:

- Understand how the macro-scale forces in their world (economic, regulatory, technology) translate into practical challenges at their business;
- Work with internal allies (your CFO, CISO, HR, Legal, operations chiefs) as well as outside experts (consultants, technology providers, and others) to develop cost-efficient answers to those challenges;
- Communicate with the board, CEO, and business operations leaders about how your vision for enhanced GRC protects the company and, whenever possible, gives the business a competitive advantage.

What's At Stake?

Or else what, you might ask? Or else in the very near future, an inability to harness technology for GRC won't simply leave you standing still or falling behind relative to your competitors—*you will fall behind in absolute terms*. Your organization will get worse at what it wants to do, because it will get worse at reaching the right decisions in a more difficult environment.

The same holds true for you, personally: if you cannot master the use of technology to improve GRC operations, your career will falter. That faltering might take the form of unemployment or losing out on plum jobs, or perhaps your job gets more busy and stressful.

Regardless, this is one occasion where the needs of you, your profession, and your company all align in the same direction. The time is now to take a hard look at your program, and begin moving it in the right direction.

Case in Point: Future States of Two Compliance Imperatives

Let's take two examples from opposite ends of the CCO's realm of responsibility: nurturing a strong corporate culture and third-party oversight.

FUTURE STATE: NURTURING CORPORATE CULTURE

A strong corporate culture will confront demographic challenges: a workforce more cosmopolitan among white-collar employees, more burned out among blue-collar. It will face cultural challenges as companies continue to expand—especially those who expand via M&A (low interest rates, sluggish organic growth). Regulators will want to see a stronger commitment to culture from senior executives, to address a wider array of challenges.

One part of that commitment to culture will be your whistleblower hotline. That's not news today, much less in 2025. The real question will be whether your whistleblower hotline operations amplifies the other parts of your compliance program, and vice-versa?

For example, workers who are more cynical or more prone to job-hopping in the future will want to know more quickly that their concerns are heard. That means you will need to align your whistleblower operation more closely to investigations (so you can know what's happening) and communications (so you can reply properly to the whistleblower and others).

Let's not stop there. You'll also need to configure the program to give you more actionable intelligence: metrics on complaints about retaliation, or on specific executives. You'll need to digest how patterns in whistleblower complaints might diverge from your risk assessment, and how they dictate which employee groups need what training about ethics and compliance.

FUTURE STATE: THIRD PARTY RISK MANAGEMENT

Third-party oversight, meanwhile, is a more prosaic challenge. You are likely to have more third parties in your extended enterprise by 2025, performing more mission-critical tasks (data protection, product assembly, overseas sales, and so forth).

You'll also have more demands from more regulators, who will want you to certify more exacting standards of business conduct. (Call it the evolution from anti-bribery laws specifically to good conduct laws generally, for everything from conflict minerals to human trafficking to pay equity.) If your company flubs the oversight of some unsavory third party, you're likely to be flayed on social media more quickly.

For this challenge, the CCO's real question is: How do you run your compliance risk assessment and third-party oversight as a single, constant operation? After all, failure could result in swift and severe consequences (regulatory probes, reputation damage, supply chain disruptions). Neither the risk assessment nor third-party oversight will be exercises you can do sporadically; they will be as routine to a compliance program as breathing is to a compliance officer.

How might a system like that actually run? You'll need to monitor regulatory changes—probably from multiple sources, inside and outside your company—that updates your company's risk profile. That, in turn, might trigger alerts to operating units to change their suppliers, or to impose additional audits, or take other remediation steps. The bottom line is that you will have more points along the way where you will need to assess, monitor, and mitigate risks; all that will need to be automated.

In both examples, the goal is really the same thing: to stitch together various components of a compliance program more tightly. They clearly are a huge Big Data undertaking, since that's what "stitching together" different types of information is.

Books have already been written on the technical challenges of integration. Compliance officers will need to understand the conceptual challenges. That is, you will need to know what stakeholders want a compliance program to deliver, and how to reverse-engineer those demands back into smart IT and workflow patterns.

You won't have the time, personnel, or ability to deliver an effective compliance program otherwise.

NAVEX GLOBAL®
The Ethics and Compliance Experts

GET IN TOUCH

Let NAVEX Global's Solutions Experts help you get your program where you need it to go. We help you manage an increasingly complex ethical and regulatory environment with integrated, scalable solutions—and work with you to build the E&C program of the future. Get in touch today at info@navexglobal.com, or give us a call:
Americas +1 (866) 297 0224 or EMEA + APAC +44 (0) 20 8939 1650.

ABOUT THE AUTHOR

Matt Kelly, *CEO, Radical Compliance*

Matt Kelly was editor of Compliance Week from 2006-2015. Prior to his role at Compliance Week, he was a reporter and contributor on corporate compliance and technology issues for magazines such as Time, Boston Business Journal, eWeek, and numerous other publications. Matt now maintains his own blog, Radical Compliance, and writes & speaks frequently on all things GRC. Follow him at @compliancememe or email him at mkelly@radicalcompliance.com.

ABOUT NAVEX GLOBAL

NAVEX Global's comprehensive suite of ethics and compliance software, content and services helps organizations protect their people, reputation and bottom line. Trusted by 95 of the FORTUNE 100 and more than 12,500 clients, our solutions are informed by the largest ethics and compliance community in the world.

+1 866 297 0224   INFO@NAVEXGLOBAL.COM   WWW.NAVEXGLOBAL.COM