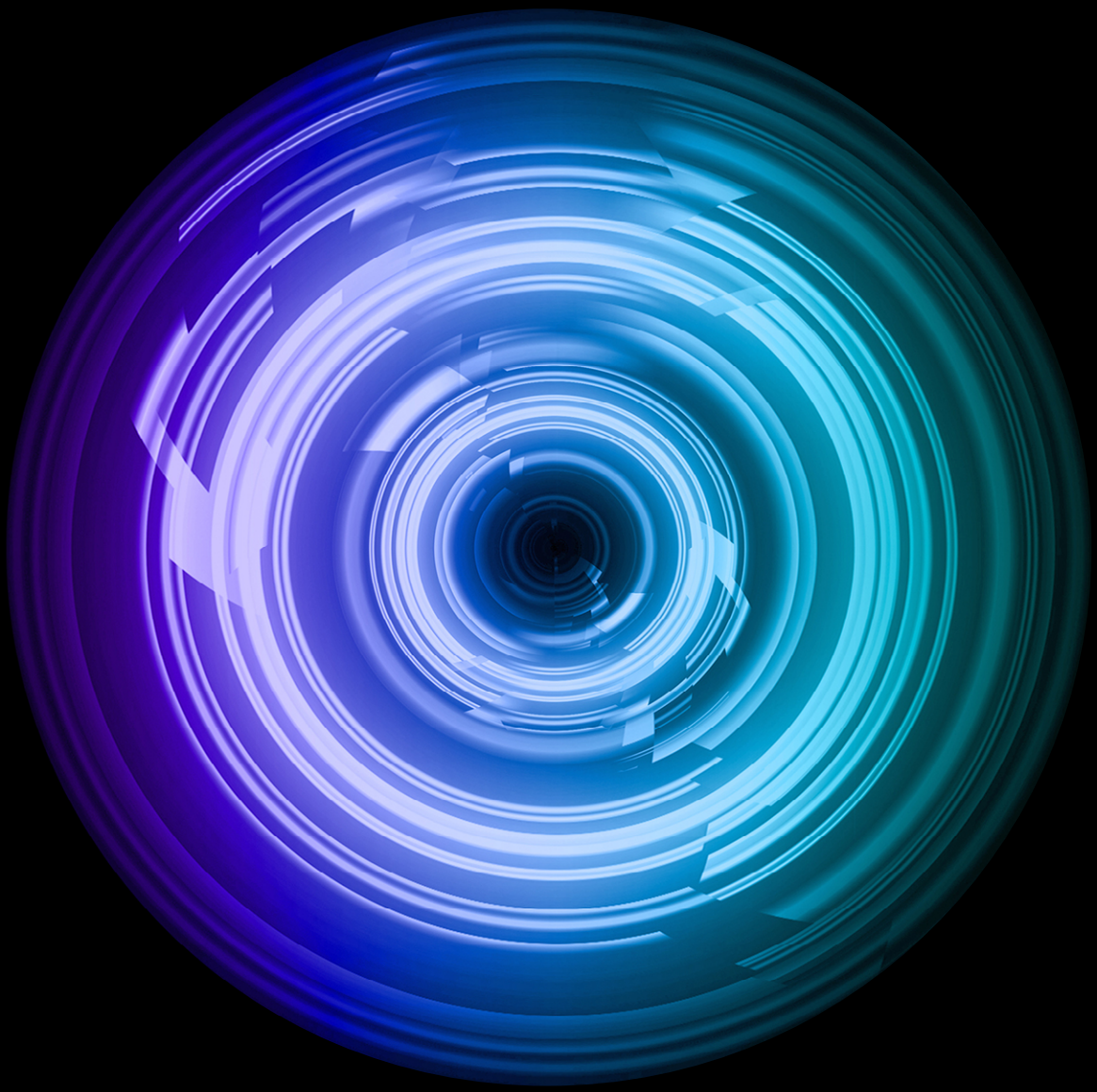
Deloitte.



IT compliance: Integrated? Or disintegrating?

How to conquer the IT compliance conundrum

Depending on your perspective, you may regard the world as woefully divided or as wonderfully diverse. At Deloitte, our inherently optimistic outlook steers us toward the latter, as we view diversity as a source of strength, knowledge, and creativity.
There is, however, one realm where we—and much of the business community—lament global diversity: the area of regulatory and legal compliance. Around the world, the multiplicity of standards, laws, and regulations that establish expectations for how IT systems are secured and controlled present a major challenge to organizations that operate across industries or beyond their home borders.

IT compliance: Compounded complexity

The conundrum becomes especially vexing in the realm of information technology. The ubiquity of and our dependence on IT, overlaid with numerous jurisdictional, industry, and even contractual obligations, can create a daunting labyrinth for organizations to navigate as they pursue profitability and growth. Entering new markets, expanding to new geographies, developing new products or services, and cultivating new clients all compound compliance complexity.

Unfortunately, many organizations take an "everyone for themselves" approach to compliance, dividing responsibility among various divisions, geographies, and job titles. This practice rarely yields good outcomes, as it lacks continuity and focus, dilutes responsibility, drains internal resources, increases costs, and creates a drag on competitiveness and profitability.

As business advisers, we counsel our clients that the situation is unlikely to improve on its own. As the complexity of technology increases, as laws and regulations are enacted at an accelerating pace, and as stakeholder demands and expectations rise, decisive action will be required to effectively manage the IT compliance conundrum. Compliance can no longer be treated as a secondary concern but rather must be prioritized and effectively managed.

To facilitate this, we recommend an "integrated" approach to IT compliance management.

What is IT integrated compliance?

Imagine a business that has operations in both Europe and the United States. Its American division is responsible for meeting the requirements of the California Consumer Privacy Act (CCPA), while the European unit addresses the EU General Data Protection Regulation (GDPR), with no collaboration between the two. This siloed approach, while perhaps making sense from an operational standpoint, fails to recognize the many overlapping requirements of the two laws, nor does it leverage the similar controls and reporting requirements of each.

If our examples were expanded to cover the entire universe of IT-related rules, laws, and regulations that govern the activities of multinational organizations, an abundance of commonalities would emerge, along with the opportunity to leverage them for competitive advantage.

And this, at its essence, is what IT integrated compliance is all about—a holistic approach that embraces the full spectrum of regulatory and legal requirements and exploits the commonalities to create a streamlined and effective system.

When an integrated IT compliance program is functioning effectively, redundancies are eliminated, efficiencies gained, resources optimized, and risks reduced. Consequently, the requirements and obligations arising from and to multiple stakeholders are fulfilled in a more cohesive, comprehensive, cost-efficient, and nonredundant way.

The current landscape

When it comes to IT compliance, no "typical" state exists—organizations are literally and figuratively all over the map. One can't even assume that compliance capabilities improve in tandem with an organization's size and budget, since larger, better-resourced entities tend to operate across multiple geographies and thus must deal with greater complexity and its associated costs.

Similarly, industry profile matters little. Heavily regulated sectors such as finance and health care would seem to have more incentive to get their compliance houses in order, yet the sheer volume and complexity of applicable laws and regulations often overwhelms the best intentions.

If there is any common ground to be found, it's that relatively few organizations have fully optimized their IT compliance programs. A siloed approach predominates, with groups such as HR, legal, compliance, or internal audit often playing a partial role in a patchwork system. Many organizations find that the problem sneaks up on them as they expand into new geographies and markets, subjecting them to new requirements.

We have observed, however, a growing awareness of the need for better coordination and efficiency. Many organizations now have IT compliance on their radar—they are thinking about it, want to address it, and recognize the need for a more proactive approach but are not sure how to get started.

What we've heard: State of maturity

In a recent study, we asked companies across various industries to share information on the state of their IT compliance efforts.

When asked to describe their current status, each of the companies cited numerous challenges they were facing. Only a small percentage described their IT compliance program as "**best in class**." Most organizations gave themselves a middle grade, characterizing their compliance program as "**developing**."

Getting started

Adopting integrated compliance necessitates an ongoing resource commitment. Compliance requirements continually evolve and expand, and keeping up with the changes demands vigilance and diligence.

The magnitude and amorphous nature of the task can seem paralyzing, making many organizations unsure where to start. We recommend beginning with a deep breath—while the task ahead may seem daunting, it's entirely doable. Take heart in the fact that global regulations, regardless of jurisdiction, typically focus on similar threats and require similar mitigating strategies, making the global compliance challenge more manageable than may seem at first blush.

What we've heard: Goals & Objectives

In the aforementioned study, we asked companies what they hoped to accomplish with their IT compliance programs. Their high-level goals included the following:

Achieve efficient and effective compliance, meeting regulatory and other stakeholder obligations without unduly diverting resources or "breaking the bank."

Reduce burdens on the business so that less time is spent testing common and redundant controls.

Combat "audit exhaustion" and counter the negative connotations that often surround audits and compliance initiatives.

Be more risk-focused, reallocating resources and attention to the most strategically important risks.

Increase awareness to help people understand the strategic importance of IT compliance, to get them on board with the program, and to recognize their roles and responsibilities.

Refine and expand training to achieve more consistency across the organization.

Here are a few observations and suggestions to get things rolling:

- **Establish a governance structure:** Involve and educate relevant stakeholders across your organization (e.g., business personnel, CIO/CISO, OGC, acquisition/ supply chain, contracting, cybersecurity). As compliance has complex and far-reaching implications across your organization, it is critical to define a formalized governance structure for your compliance program as early as possible.
- **Understand the magnitude of the effort:** Put some upfront effort into getting a handle on the task ahead. Take inventory of your compliance requirements and understand how they align across the organization—not just within IT but across the entire enterprise.
- **Don't tackle everything at once:** Create a plan that is reasonable and manageable and matches your personnel and budget. Set attainable milestones and closely track progress. Don't overcommit.
- **Be careful with your market-facing representations:** Oftentimes, key personnel—finance, IT, in-house counsel, etc.—don't know what claims are being made to partners, customers, regulators, and other stakeholders. This disconnect can present significant problems if left unaddressed.
- **Identify key stakeholders:** Compliance roles, responsibilities, and impacts extend far and wide, both within and outside the organization. Take a full inventory of all stakeholders.
- **Determine the current cost of compliance:** Roll into your calculation the cost of controls, tools, reporting, personnel, etc. Most organizations are surprised at the tally. If it's larger than you expected or hoped, action may be warranted.
- **Understand your current state of integration:** In some cases, integration activities may have already taken place, which will put you ahead of the game. Use any previous or ongoing integration initiatives as a springboard.

What we've heard: Tips & Tricks

As the companies in the study reflected on their integrated IT compliance journeys, they offered a few tips to make the trek less arduous:

Raise awareness across the organization of the importance and necessity of integrated compliance. Publicize stories, both of replicable successes and instructive failures.

Develop a strategy to get buy-in at the management and senior leadership levels. Your program will go nowhere without it.

Consider automation tools as a means of reducing the burdens on control owners and subject-matter experts (SMEs) for common and repeated evidence requests.

Front-load the initiative by making a vigorous push at the start. Extra effort early on will yield time and budget benefits later.

Key steps

Depending on current state; committed resources; regulatory, industry, and contractual requirements; and other factors, attaining IT integrated compliance can be a complex task. The key to success involves doing things right across multiple dimensions.

As you embark on your integrated IT compliance journey, consider taking these steps:

1. **Document current state:** To develop a clear picture of your present status, inventory existing risks and controls; identify current roles and responsibilities; and compile current reporting requirements.
2. **Risk assess and prioritize:** Examine and document risks across the entire legal, regulatory, and contractual universe, to determine your exposure and to reprioritize consistent with your risk appetite.
3. **Map commonalities:** Find similarities and overlaps across all your documented risks, controls, and reporting requirements.
4. **Rationalize and consolidate:** Take a hard look at your compliance frameworks, tools, policies, procedures, processes, and controls. Identify redundancies and opportunities for consolidation. Keep an eye out for gaps and the need for additional or enhanced controls.
5. **Establish a governance structure**: To drive accountability for the overall program, create a governance structure, including the reallocation of roles and responsibilities, as needed.
6. **Consolidate and enhance monitoring and testing:** Successful compliance programs are built on measurement. Develop an integrated testing framework that includes relevant and useful metrics and KPIs.
7. **Teach and communicate:** Virtually everyone has a role to play in compliance. Develop education and communication plans to support your integrated compliance efforts.
8. **Implement formal incident and escalation programs:** Early warnings and timely interventions can prevent small problems from escalating.
9. **Consolidate and streamline reporting:** Just as you mapped and consolidated controls, do the same for your reporting requirements.

Pothole avoidance

Misconceptions and missteps abound when it comes to integrated compliance. Here are a few potholes to steer around:

- **This is not a "one and done" exercise:** Your compliance requirements are never-ending and ever-evolving, so a means of staying up to date must be built in.
- **Pace yourself:** Sustainability needs to be a key consideration. Don't make a frenetic hard push early, which will likely only lead to burnout. Rather, plan for the long haul.
- **There's no silver bullet:** It's a common misconception that acquiring a GRC tool will "solve" your compliance issues. Technology can help in myriad ways, but it alone cannot solve the problem. And even the best tools require constant upkeep, including processing new and revised regulations, software upgrades, security patches, and the like.
- **In-house talent may be scarce:** In our experience, few organizations have the resources in-house to, for example, distill 20 different regulatory requirements into a single framework. Outside expertise may be needed.

What we've heard: Challenges

Integrated IT compliance challenges faced by surveyed companies in recent years included the following:

- **The pandemic**, which contributed to significant employee turnover, loss of institutional knowledge, and the need for additional onboarding and training.
- **Pace of change**, with regulations and requirements being enacted and revised at a rate that was hard to monitor and adapt to.
- **Organizational culture**, where some departments were hesitant to change their ways and accept new roles and responsibilities.
- **Leadership support**, where compliance was not perceived as a priority, making it difficult to bring the rest of the organization on board.
- **Complexity**, with organizations forced to digest a virtual alphabet soup of regulations based on geography, industry, and other factors.
- **Automated tools**, which were sometimes wrongly perceived as a "silver bullet," when in fact the best they can do is incrementally improve the situation, not entirely solve the problem.

Final thoughts

The world at large may be increasingly polarized, but in the business realm there are several generally agreed-upon concepts. Few executives, for example, would dispute the notions that (1) the "business of business" is becoming increasingly complex; (2) organizations face ever-growing demands from multiple stakeholders; and (3) devoting ever-increasing resources to regulatory compliance is unsustainable over the long haul.

In terms of countering these trends, an integrated IT compliance program offers the potential for relief. While regulatory requirements may seem disparate and convoluted from afar, upon closer scrutiny, many commonalities may be identified that can be leveraged to advantage. A thoughtful analysis that maps and correlates IT-related requirements across a company's geographies and frameworks can be eye-opening, revealing untapped potential for efficiencies and effectiveness.

Yet gains don't come without pains. Leaders need to recalibrate their thinking around IT compliance, devoting upfront time and resources to develop a well-thought-out plan. Roles must be clearly defined; accountability for the day-to-day program and its progress must be established. Typically, responsibility has fallen squarely on the IT department, but given the many tentacles of regulation, a successful initiative requires shared responsibility across business units and job titles. Buy-in and visible support from the executive and managerial teams represent a prerequisite for realizing the full benefits.

Larger organizations in particular may find that a dedicated team is needed to meet IT compliance needs. A number of companies have reported pushback from operational employees who are finding their growing compliance burdens untenable, with a common refrain of, "You want me to do my regular job and handle this too?!"

Many organizations have found that the use of consultants can provide needed expertise and specialized skills to help ensure the program rests on solid footing and that the long-term outlook is positive. An impartial, yet authoritative, perspective can be especially useful in the initial stages of an IT integrated compliance program, and in instances where significant change management is required around acceptance, expectations, and responsibilities.

As with most projects, upfront investment yields backend dividends. In the case of integrated IT compliance, those benefits will notably include the ultimate freeing up of both personnel and budget resources for other strategic imperatives.

Comply, then fly.

Contacts

Brandon Brown
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
brandonbrown@deloitte.com
+1 801 366 2659

Chad Phillips
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
chadphillips@deloitte.com
+1 313 396 5938

Dasha Seleznyov
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
dseleznyov@deloitte.com
+1 703 251 1486

Deloitte.