The Complete Compliance and Ethics Manual 2023
The Relationship between Technology and Compliance

By Heidi Rudolph[1]

Part I

Introduction

In 2004, "Facebook didn't exist, twitter was still a sound, the cloud was still in the sky, 4G was a parking place, LinkedIn was a prison, applications were what you sent to colleges, and Skype was a typo," said *New York Times* columnist Thomas Friedman.[2] Individuals and companies are adopting technology at an increasing speed each year. Technology automates manual processes and workflows, organizes data, stores information, streamlines reporting, and provides an avenue for engaging employees and stakeholders.

Technology Is a Compliance Issue

Compliance professionals must be aware of emerging technologies that apply enterprise-wide as well as to the compliance function. Compliance programs should analyze the potential risk and reward of new and emerging technologies to appropriately guide companies in ethical decision-making. Compliance should have a seat at the table when their company is considering the implementation of transformational technologies. The American Bar Association reflects this view in stating, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all [CLE] requirements to which the lawyer is subject."[3]

In addition to enterprise-wide technologies, compliance should continue to evaluate the technology available to increase its own program's effectiveness and efficiency. The heightened level of legal and regulatory scrutiny facing companies today is a catalyst for exploring new and existing technologies to redesign or streamline existing compliance programs. Technology is one enabler for companies to create and maintain a defensible program. Automation helps companies answer questions from regulators about credibility, measurement, continuous improvement, and accountability. Technology within the compliance space continues to improve and more vendors expanding offerings, resulting in more choices.

In the following section, we will provide an update on the current state and trends of compliance technologies. We will then review why it is important for compliance professionals to stay engaged with what technologies are on the horizon.

Technology's Role in Compliance: Insights and Trends

1. Risk Assessment and Risk Management

Risk assessments are the foundation of compliance programs. The April 2019 *Evaluation of Corporate Compliance Programs*, released by the United States Department of Justice Guidance, mentions risk 49 times.[4] Defensible

compliance programs know their risks. Technology helps streamline the formal risk assessment process by centralizing data, conducting analyses, and facilitating prioritization. Risk assessment technologies are available off-the-shelf with a range of customization, or companies can create their own. Many have an enterprise-wide and compliance-specific risk management perspective. Solutions adding the most value offer the following components: identified legal and regulatory risks, mapped areas of the business affected by the risks, assigned accountability, documented controls, assessed occurrence likelihood and impact severity, identified gaps, and prioritized actions.

Such solutions provide companies with a single, automated source for compliance risks and action plans. Information gathered for analysis and prioritized action plans are stored in a centralized location, ensuring that information exchanges with regulators or other companies during merger and acquisition activity are accessible and accurately communicated.

Reporting dashboards and interactive presentation capability are becoming increasingly important to compliance. Interactive graphs and tables provide a foundation for communication with colleagues and leadership about the company's risk profiles, business areas affected, controls in place, and prioritized actions. Visual representation of the outcomes of legal and regulatory risk assessments and the ongoing risk management activities has become a standard, engaging tool for compliance teams.

2. Reporting, Hotline, and Incident Tracking and Case Management

The reporting process, investigations, and case resolution have well established technology solution providers in the marketplace to streamline this essential compliance process from end to end. Platform integration with other solutions (learning-management solutions, policy-management solutions, conflict-of-interest disclosure registries) is becoming more common to more efficiently review applicable data during internal investigations.[5] As solutions integrate, compliance must ensure that each person who has access to information on the reporting and case management tool has a business need to do so and that such access is appropriately defined.

In 2018, some reporting and case management solutions were required to implement changes based on data privacy regulations (e.g., the General Data Protection Regulation) and additional minor changes in workflows and functionality are expected to develop. For example, clients can customize data intake forms to automatically generate if the reporter is located in or a resident of the European Union.

Other case management trends focus on how the company applies the technology, not the technology functionality itself. The three incident and case management functionalities most companies are refining recently are central data validation, timely communication with the reporter, and robust reporting. These tasks can now be handled through outside vendors that offer functionality to support all three focus areas. The success of the technology (and the program) relies heavily on the resource(s) allotted to manage it.

Using central data validation is a best practice for a variety of reasons. Vendor intake persons receive and record hotline and incident calls. The record is accurate as provided, but some records require minor data clean up, links to other cases, or additional information from a source with internal knowledge. Data validation is essential for accurate reporting. In decentralized companies, duplicate cases emerge from multiple business units because, for instance, the reporter called both hotline numbers by mistake. Prioritizing one central resource with eyes on all cases has the unique ability to spot errors or duplication that an external intake person could not and should not be able to identify and resolve.

The ability to ensure timely communication with the reporter, especially anonymous reporters who want to

remain anonymous, can validate or undermine the integrity of the reporting process. In the world of mobile email access and text messaging, reporters expect timely (within 24-hour) responses and ongoing case updates. Ensuring that reporters feel heard and establishing trust that their concerns are being investigated helps reinforce a culture of speaking up within the organization.

Improvements in robust reporting is a notable off-the-shelf benefit of reporting and case management technologies. Reports can be premade but also customizable. Customizing reports is as easy as selecting a check box of the desired fields. Standard and custom reports can be run weekly and/or monthly to align on case status and assess data validity. Whether running a report for the compliance team to review or to deliver statistics to the board, robust reporting functionality can be made available and effective with appropriate attention and time. Reporting is an essential facet of continuous improvement efforts and demonstrating an effective compliance program.

3. Policy Management

Heightened regulatory scrutiny on policy administration and attestation, especially regarding codes of conduct, generates a greater need for technology in policy management. Policy management tools can automate processes and establish one source of truth for employees. In addition, they easily generate an audit trail of policy revisions and past ownership on the back end for compliance and other key contributors.

Policy management technology has well established workflow management functionality. The software automates an otherwise manual method of tracking versions, collaborating on edits, and requesting approval. No digging for the latest version in an email inbox or SharePoint folder is needed. The software allows assured version control, or "one source of truth," and personalized requests for edits or approval. Once a policy is finalized, it can be quickly posted for employee access. The technology preserves the edits and previous versions on the back end for future reference during an internal investigation, audit, or litigation.

Some policy management solutions track policy-related acknowledgements and attestations in a central location. Creating and recording targeted attestations are simplified for policies that apply to a portion of the organization. Additionally, some software solutions automate surveys designed to test if employees are putting policies into action. Insight into employee knowledge regarding policies allows leadership to address knowledge gaps, remediate, review, and change procedures all within the same system.

As data tagging progresses, policy management solutions are making data tagging available so searches for or within a specific policy can be tracked and reported. Such data helps facilitate conversations amongst compliance leaders about polices that may need a training refresh or clarification based on commonly searched topics (e.g., anti-harassment, gifts and entertainment).

4. Training and Learning Management Systems

Compliance training and learning management are common compliance solutions enabled by technology. High-quality compliance training and learning management system (LMS) vendors exist, which differ significantly in scope and functionality. Companies use LMS providers for a variety of needs: Those with extensive learning management needs may want training content, training delivery, attendance tracking, and reporting, etc. Others may simply want to purchase training content to deliver directly to employees or through another LMS.

Demand for compliance LMS integration with enterprise LMS and human resource information systems (HRIS) continues to increase. In addition to system integration benefits, LMS agility and ease of integration is preferable for many, because companies are trending toward the use of multiple content providers to achieve bespoke

training curricula. Government regulators emphasize that one-size-fits-all training is not considered effective.[6] Targeted training using short videos, additional modules for managers, and applicable case scenarios are some training methodologies that are growing in popularity.

Scenario-based learning is not a new philosophy but is becoming the preferred approach in the compliance training space. Learning through facilitated or interactive online scenarios allows companies to collect more useful data. Reviewing trainees' answers to questions can allow trainers to pinpoint potential risk areas that require additional training. Scenario-based training focuses more on learning how to *apply* a policy. Providers are moving policy information and definitions to pop-up bulletins, purposefully recapping the learning created during the interactive scenario. This training philosophy is founded on answering the simple question: What do you want people to do after they complete this training? [7] New online training providers have emerged in recent years that focus on scenario-based learning taught through the lens of real on-the-job scenarios. This approach can be expected to gain popularity in the upcoming years.

5. Communication Management

Compliance should consistently explore new and engaging ways to connect with employees and reinforce an ethical and compliant culture within their organization. There is steady growth in the emergence and adoption of business communication tools, on which compliance can capitalize. Tools available from enterprise licenses (e.g., SharePoint, intranet site, Microsoft Teams), are not all new, but compliance continues to explore the efficacy of using these platforms to engage with employees. Well-frequented intranet sites provide a unique opportunity for compliance to connect with employees in a familiar space. Utilizing company-wide intranets or SharePoint sites allows for the consolidation of compliance content and messaging in one location, creating a central reference for messages, training, reminders, policy links, and contact information for reporting and escalation.

As compliance programs adapt to using intranets and SharePoint sites to deliver messages, some have started to explore new and interactive ways to communicate with employees. Intranet sites can be used to run contests to gain traction on an initiative launch (e.g., speak-up campaign, code of conduct launch or refresh), post short videos or podcasts, poll employees, and recognize individuals for real ethical moments at work.

Companies benefit from posting or distributing short informative videos that remind employees of ethical standards using a common visual medium. Training follow-ups are also an effective use of YouTube-like video communications. Such communications can be targeted to specific audiences or sent company-wide, depending on the message objectives. Senior leadership in some companies are using mobile-captured videos to recognize individuals for their ethical behavior within the company. These videos demonstrate ethical decisions made within the company, focusing on what *to* do, rather than what *not* to do. Similarly, short (2-3 minute) podcast recordings or interviews can be effective means of communication. If the intent of the content is to provide a reminder or a quick engagement, short videos or podcasts are a fruitful and low-cost tool.

6. Third Party Screening and Due Diligence

Patrick Moulette, head of the Organisation for Economic Cooperation and Development (OECD) Anti-Corruption Division states, "The question for us is whether new technologies are a corruption risk or a remedy, and I think they are both. The anti-corruption community is lagging behind the criminals and we need to do more work to look at trends like virtual currencies being used for bribery or money laundering. The trends in criminal activities emerge at first and it usually takes some time before the community of regulators and policymakers becomes fully cognizant and then addresses the issue."[8] As new technology emerges, bad actors and criminals

change their behavior to capitalize on these channels to commit crimes, e.g., pay bribes and launder money. In the final section of this article, we will discuss compliance's duty to keep abreast of new and emerging technologies and the potential risks they bring to the business. It is important to note how new and emerging technologies could increase a company's corruption risk profile if the company does not fully understand the technologies' capabilities and potential uses. For example, individuals can use blockchain or cryptocurrency to pay bribes or launder money.

As Moulette states, leveraging technology is also part of the solution to mitigating corruption risk within an organization. Screening and due diligence tools serve as well-known remedies to mitigate corruption risk. These solutions perform automatic screening of entities (customers, suppliers, other third parties) and automate requests and delivery of due diligence reports with a central repository. Improvements in screening technologies incentivize companies to move from an outsourced managed service model to in-house business process solution. Increasingly, screening and due diligence tools utilize artificial intelligence capabilities to further improve result validity. The artificial intelligence capabilities will undoubtedly improve as companies learn how to harness this technology.

The combination of anti-corruption screening and due diligence technology paired with human judgement and expertise adds value. The technologies generate information, but how the company interprets and evaluates that information against their risk tolerance and thresholds determines what mitigating or remediating actions will or will not be taken. Furthermore, reviewing supplemental external sources of information is helpful when performing more in-depth analysis of screening results. Large companies, especially with a global presence and a high quantity of entities needed to be screened, often decide to add employees or outsource anti-corruption screening analysis.

7. Data Privacy

Data privacy regulations continue to develop and strengthen. The European Union's General Data Protection Regulation (GDPR) became a central focus of compliance and privacy departments over the last few years, with other countries following suit and creating a wave of privacy updates and regulations globally. The attention to this area will only continue to increase.

Data privacy regulations require companies to have a comprehensive understanding of where and how their customers' data is stored, what components of personal data are being stored, and how it is being used. Verifying the security of this personal data is also a key objective. New technology has emerged to create a space consisting of all data privacy and management protocols. This offering is noted as the "single pane of glass," which ensures companies are prepared to meet the privacy requirements on an ongoing basis.[9]

Data privacy solutions aid in satisfying the company's objectives of managing all personal data and assigning accountability of that management to the appropriate persons, while still maintaining central oversight. Technologies aiming to automate and support data privacy business processes are being developed and adopted. We expect to see growth in this area as the technology continues to develop and mature. As we have experienced with anti-corruption screening platforms and learning management solutions, we anticipate customization to be at the top of solution providers' list of offerings in upcoming years.

8. Conflict of Interest

Conflict of interest registries automate the disclosure collection workflow, track communication and approvals, offer reporting capability, and provide a central repository for disclosures. The central repository facilitates transparency of potential and existing conflicts and enables leaders to be holistically aware of the existing

relationships.

The registries are available off-the-shelf, while some companies choose to develop a rudimentary homegrown system. The benefit of some off-the-shelf offerings is seamless integration into other systems provided by the same vendor. As previously highlighted, system integration is a fast-growing trend.

Solution integration becomes attractive when different functions own different parts of a business process. For example, integrated solutions enable more efficient workflows with the ability to assign conditional accountability at certain steps, thereby closing the communication loop between legal, compliance, and human resources. Integration helps ensure that the process completes and provides all appropriate parties with secured access to relevant information, especially relevant during internal investigations or audits. Some clients also find benefit in storing disclosures within personnel files, and therefore requiring integration with human resources systems.

Decentralized companies also find benefit in the consistency that a global conflict-of-interest management solution institutes. Automated workflows assure that all locations must go through the same process steps. Uniform communications and specifically guidance and examples can be included in the solution, providing support as the employee discloses or as the manager reviews.

9. Gifts and Entertainment

Gifts-and-entertainment solutions are widely available and sometimes tailored to specific industries. Gifts-and-entertainment registries and approval solutions are often modules that can be purchased as part of a larger governance platform. Solutions can be integrated into other compliance modules and platforms and corporate travel and expense management software. Specific capabilities that companies should capitalize on include but are not limited to: setting financial thresholds that trigger a follow-up action and creating rules for specific purchase categories to trigger an approval process.

Similar trends and contingencies exist for gifts-and-entertainment solutions as those described above for conflict-of-interest management platforms. In addition to the demand for seamless integration, some gifts-and-entertainment providers are emphasizing the capability to utilize the integration to send compliance messages as reminders when the risk is highest. For example, if a company syncs the gifts-and-entertainment module with their travel planning platform, a short reminder is automatically sent to the employee via email if the employee is traveling to a high-risk market, as defined by Transparency International's corruption perception index. The reminder helps the employee distinguish between acceptable behavior and behavior that conflicts with the company's values and policies. A short list of acceptable and unacceptable gift examples also helps the traveler keep the policy standard top of mind.

The Upshot

There are many technology-based options available to support compliance programs with solutions ranging from administrative efficiency to strategic, data-driven, risk mitigation objectives. When evaluating the role for technology within compliance or within the organization, ensure you have clearly defined risks, objectives, and accountabilities. Following good sourcing practices, select three or four vendors to participate in a request for proposal (RFP) process. Include cross-functional or cross-segment teams in RFP discussions and demos to ensure impacted parties have representation during the evaluation process.

Remember, one size does not fit all and the ability to customize is growing. Technology should be selected based on, and implementation tailored to, the needs of the organization and governed by human judgement. Technology is an instrument, but how it is used is determined and governed by each company.