COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2021
Compliance by automation or by people? That is the question

By Patrick Wellens, CCEP, CFE, CIA, CRMA

Patrick Wellens (patrickwellens@hotmail.com) is a Global Compliance Business Partner for a division of a multinational pharma company, based in Zürich, Switzerland, and a board member of Ethics and Compliance Switzerland.

Like clockwork, the news is filled with compliance scandals. But why do they continue to occur? Some companies do not have an ethical culture and lack a clear tone at the top, incentive schemes and bonuses add pressure on employees to reach unrealistic targets, or the lack of internal controls allows employees to conduct unauthorized transactions. Another reason for misconduct can be the lack of resources and/or an inadequate structure of the compliance management organization.

Most boards recognize the effects of compliance on the reputation of the company, talent management, employee satisfaction, and—of course—the avoidance of fines; however, compliance budgets are typically not limitless. Chief compliance officers are often asked to do more with less. As a result, many compliance departments have started looking into automation, artificial intelligence, big data analytics, and introducing technology to reduce the human cost of compliance, as salaries and other remuneration benefits are typically the biggest chunk of the compliance budget. Other alternatives being explored are the introduction of shared service centers for compliance operations or doing fewer activities (e.g., rather than doing auditing and monitoring by the compliance department, business functions are asked to self-certify that their processes and controls are working effectively).

The Criminal Division of the U.S. Department of Justice states in its *Evaluation of Corporate Compliance Programs* that every company should take into account "among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations" in defining its risk profile and consequently its compliance resources.[1]

So when a company has completed its risk assessment and understands what risks are managed by the compliance function (e.g., anti-trust, money laundering, sanctions, conflicts of interest, data privacy), how do chief compliance officers determine the amount of resources and the geographical allocation thereof to help mitigate these risks?

In this article, we will focus on the structure and allocation of resources required for an optimal compliance organization with preventive measures to catch misconduct before it occurs. We will take into consideration these factors:

- The breakdown of the organizational structure (i.e., if the company is managed by divisions and/or regions, and where the positions are based);
- The location(s) where most of the business takes place;

- The location(s) where most of the compliance risks take place;
- The strategic decision of whether certain activities (e.g., investigations) will be done in-house or outsourced to law firms;
- The overall compliance budget defines how many positions can be allocated, given that personnel expenses are the largest cost within a compliance department;
- Whether certain resources and/or budgets can be shared with other governance roles (e.g., corporate security, information technology security, data privacy, risk management, human resources); and
- The level of compliance task automation.

Now let's take a closer look.

Automation or local compliance officers?

In order to prevent ethical misconduct and ensure compliance with laws, compliance officers provide compliance training; focus on creating an ethical culture; and develop, implement, and communicate necessary compliance standards, processes, and controls. When developing processes and controls, however, companies can choose to have this done in a decentralized or centralized fashion and have them be manual or automated. The more a process can be standardized globally without any need for regional and/or local level adaptations, the greater the likelihood that a process and the related controls will be centralized. As centralized processes often consist of a high volume of transactions for which the same controls are conducted, it is highly likely that such controls can be automated. On the other hand, the more country-specific (i.e., that have local legal requirements) processes and controls are, the more judgment is needed that considers a variety of different parameters and language requirements. And the higher the risk when deciding on whether a transaction is ethical/compliant, the greater the likelihood that such decisions will be done manually. Therefore, the level of automation in compliance processes and controls will directly affect the organizational structure of the compliance department.

In order to determine which activities can be automated and where the presence of a local compliance officer is needed, it is worthwhile to look at the various activities traditionally done by compliance staff and look at the pros and cons of manual versus automated oversight (Table 1).

	Manual	Automation

Policies and procedures	**Pros**: • Corporate directives/policies typically create high-level principles and thresholds. • For local enactment and the creation of a local implementation and training plan (allowing employees to ask questions), local compliance resources are needed. **Cons**: • Employees have a hard time finding the current version of global and/or local directives or policies.	**Pros**: • Corporate directives and policies can be rolled out to all employees through a central application tool. • An overview exists centrally of all corporate policies and directives that have been enacted in all subsidiaries. • Follow-up can be done on those countries/management teams that did not enact corporate policies. • Employees can easily find a list of active policies in a central location. **Cons**: • The central distribution of a corporate directive and policy does not mean that it is understood by employees. • Typically, a local implementation or training plan, sometimes with local guidelines/policies, is needed.

Compliance training	**Pros**: • Training is not costly. • Interactive, engaging training can increase the retention of training materials. • Employees can ask questions. • Basic and advanced face-to-face training for specific risk groups can be organized. **Cons**: • Training is not practical for a large amount of employee groups.	**Pros**: • Web-based trainings (WBTs) are cost efficient for training a large number of employees. **Cons**: • WBT often contains generic content ("same training for all") but is not suitable to address specific (high-risk) categories for employees. • Training is not interactive; employees cannot ask questions. • There is risk that employees "click through" the WBT without retaining any content. • It is costly to create videos and WBT.
Third-party due diligence	**Pros**: • Due diligence is simple, low cost, and possible if a company has few third parties. **Cons**: • There are no management reports and no holistic overview of third parties. • There can be inconsistent due diligence documentation and document retention. • There is a risk of inconsistent monitoring. • There is no risk-based approach.	**Pros**: • Allows for documentation of the initial due diligence and continuous monitoring of third parties, while considering changes of company ownership and adverse media. • Allows a holistic view of third-party risk across multiple risk domains. **Cons**: • Initial investment in software can be large. • Process design can be complex.

Conflict of interest disclosure	**Pros**: • If a company has few disclosures, the process is simple and low cost. **Cons**: • There is no holistic overview of conflict of interests. • There can be different disclosure documents and standards across subsidiaries. • It's not practical or realistic for a large amount of disclosures.	**Pros**: • Reduces conflict-of-interest risk. • Is managed centrally in a common tool, ensuring consistency. • Increases transparency. • Reduces costs. • Documents mitigation actions. **Cons**: • Initial purchase of a conflict-of-interest software application can be costly.
Culture survey	**Pros**: • For single locations or companies with few employees, it can be simple and low cost. **Cons**: • Comparing results of employee surveys between subsidiaries, across regions/divisions, or for trends over time is difficult without an automated solution. Doing such an analysis manually is very costly.	**Pros**: • Survey questions can be sent to a wide number of employees. • Results can be compared between subsidiaries, across regions/divisions, and over time. **Cons**: • The initial cash outlay for developing the cultural survey questions and management reports can be high.

Auditing	**Pros**: • Audit can be simple and low cost, but it's not adequate for multinational corporations with a multitude of subsidiaries, venture partners, representations, and branch offices. **Cons**: • The lack of a central repository of compliance audit reports hampers insight on high/critical compliance risk areas and trends on repetitive findings or weaknesses in compliance process controls.	**Pros**: • A central repository of compliance audit reports monitoring results will allow you to identify repetitive findings and common weaknesses. These can then be addressed centrally through communication campaigns and/or updated trainings. **Cons**: • The cost of a central repository of audit reports application and the cost of keeping the repository up to date to generate meaningful insights are high.
Compliance (transaction) monitoring	**Pros**: • Compliance monitoring can be simple and low cost if done for a limited number of transactions. **Cons**: • Randomly selecting a limited number of transactions among ten/hundreds of thousands of transactions does not give good assurance of how effectively compliance controls are working.	**Pros**: • Monitoring improves through automated approvals, exception reports, identification of problematic transactions for monitoring/testing, and identification of outliers and fraudulent patterns before they materialize by using predictive analytics. **Cons**: • There is a costly initial investment in technology and designing the compliance approval workflows.

Investigation case management tool	**Pros**: • It can be simple and low cost. • It's possible for a small company with very few investigations. **Cons**: • It is not adequate for a medium/large company with worldwide operations. • The lack of an automated tool hampers the analysis of statistics and/or trends of compliance cases.	**Pros**: • A centralized compliance case management tool allows you to keep track of the status of each and every investigation. • It allows for analyzing trends on the type of compliance violations, regional analysis, root causes of compliance violations, and statistics on sanctions. **Cons**: • Information technology cost of maintaining a compliance case management tool is high.
Investigation function	**Pros**: • Conducting compliance investigations is a complicated process where expertise is needed. The investigator must understand local labor and data privacy laws, be an expert in reviewing documents and conducting electronic evidence reviews of structured and unstructured data (e.g., emails, documents on networks, Skype accounts, social media), and highly skilled in conducting interviews. **Cons**: • Companies might centralize "investigation" activities to a small team of in-house experts or decide to work with specialized law or forensics firms when they are needed. In-house investigators are typically familiar with company processes, applicable policies, and procedures; know where to find evidence; and are usually less expensive than external advisors. The number, the complexity, and the locations where most of the investigations take place will typically drive the decision where to locate investigation teams (if at all needed).	**Pros**: • Technology is typically applied in forensic review of documents and/or mass data queries to identify fraudulent transactions. **Cons**: • A human presence is needed for reviewing documents, conducting email reviews, interviewing suspects, and writing an investigation report.

Business partnering	**Pros**: • Global projects, digital innovations, and new business models for which the business seeks compliance advice often contain a variety of compliance, ethics, and data privacy risks. Compliance officers give such comprehensive advice by taking all risk factors into account. **Cons**: • Business can be slowed down depending on the response time of the compliance officer.	**Pros**: • Decisions are fast. **Cons**: • Automated decisions might not consider all relevant factors for complicated projects affecting many different aspects of law and compliance (e.g., ethics, compliance, data privacy).

Table 1: Activities traditionally carried out by compliance officers, and the pros and cons of these activities under manual vs. automated oversight.

After reviewing these pros and cons, it becomes clear that for some of the traditional compliance activities (e.g., conflict-of-interest disclosure, third-party due diligence, compliance monitoring) companies can generate economies of scale, higher consistency, and greater assurance by standardizing and centralizing processes and controls through increased use of technology, thereby reducing the number of compliance professionals needed for transactional activities. Technology and applications allow compliance officers to analyze trends, remediate root causes, and identify the needle in the haystack among a large number of transactions.

A factor not to be underestimated is that compliance is a *behavioral* science and drives the adoption of "doing the right thing all the time" by company employees. Technology can reduce the cost of compliance operations and should be considered where possible; however, compliance operations are not the everyday average transaction. An incorrect approval or judgment can have serious consequences.

Location of the compliance team

Now that we've looked at which tasks are best handled by the compliance function, let's consider how compliance's own resources should be geographically allocated.

The compliance team is a sparring partner that enables business functions to achieve their strategic goals. It makes sense that various compliance officers are in functions at the headquarters, or in divisional or regional headquarters, in order to be close to the business. Usually the compliance department mirrors the organization in order to understand the business and be part of strategic projects.

A central compliance department with most of the staff in headquarters and few officers acting as local resources can be problematic. This is because the business models and go-to market strategy in various parts of the world are different from headquarters; the one-size-fits-all approach does not work. Large variations in the Corruption Perceptions Index among countries,[2] cultural differences, local requirements (e.g., laws, regulations), the enforcement activity by regulators, and the differences in remuneration of compliance staff in different countries will also play important roles in the overall effectiveness of a compliance department's reach.

In order to participate in local leadership meetings, conduct face-to-face trainings, or develop local policies, the compliance officer must understand the local culture and have the necessary language skills. I have conducted forensic investigations in locations where a global multinational company brought people into a given country that were unfamiliar with the culture and could not read the documents. Not surprisingly, things went south—

quickly.

Like clockwork

The compliance department's organizational structure and geographical allocation depend on the compliance charter (its scope of activities), the locations where most of the business takes place and where the compliance risks are, which resources can be shared with other governance functions, and the level of compliance task automation.

While the drive for efficiency and continuous improvement of the compliance program is normal, the cost reduction in compliance operations when replacing compliance officers with technology/automation should be evaluated against the risks taken. Technology can reduce the cost of compliance operations and should be considered where possible; however, compliance operations are not the everyday average transaction.

It should not be underestimated that compliance is a behavioral science, and driving employees to adopt ethical values and the need to do the right thing all the time requires human interaction (and intervention). Running the compliance department and transactions as clockwork is excellent, but you still need a clocksmith (the compliance officer) to make repairs and improvements.

Takeaways

- A company's risk profile and the ethics and compliance department's scope of work will define a company's compliance resources.
- The geographical allocation of compliance resources will be affected by the location(s) where most of the business and/or most of the compliance risks take place.
- Technology can reduce the cost of compliance operations and should be considered where possible; however, compliance operations are not the everyday average transaction.
- The more a compliance task can be standardized, the higher the likelihood for centralization and automation.
- By using data/predictive analytics, the ethics and compliance department adds value to the business by identifying outliers and predicting fraudulent patterns before they materialize.

1 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), 3, http://bit.ly/2Z2Dp8R.
2 "Corruption Perceptions Index," Transparency International, accessed December 3, 2020, https://bit.ly/3g7qXyg.