KPMG

Clarity on Compliance

The future of compliance

June 2016


46


20


40


16


24


6

CONTENT

Clarity on Compliance

EDITORIAL

Keeping up with the future of compliance

Solveig Rufenacht
Head of Compliance, KPMG Switzerland

The challenges facing compliance officers appear to grow year by year: a huge rise in the number and complexity of regulations, more rigorous enforcement by authorities, and societies that are increasingly intolerant of unethical behavior. Compliance officers are expected to more effectively prevent compliance incidents from happening and, in the worst case, detect and deal with them promptly. And to do so while compliance resources are constantly questioned, and often reduced.

The role of compliance is also expanding as it becomes generally better understood, however. Traditionally confined to regulatory and legal compliance, it is moving towards a flexible definition that also covers ethical standards, sustainability and much more. Against this background, compliance functions are transforming their structures and the skills they deploy. Large centralized teams are giving way to decentralized operations that make it easier to embed compliance throughout an organization. As central compliance departments shrink, this once generalist function is being staffed with specialists. Crucially, what in the past was too often seen as a police function is being positioned as a true business partner.

Throughout these changes, technology can play a key role in managing compliance programs. Using data analytics, for example, can enable improvements by providing useful compliance metrics and monitoring tools that allow an organization to measure the effectiveness of its compliance programs and monitor the emergence of compliance issues.

The potential damage from non-compliance is still very high and compliance officers cannot take their eyes off the ball. This publication covers some leading compliance practices and shares insights into building an even more effective compliance function. We trust you find it useful and we would be pleased to discuss with you how your organization is approaching the future of compliance.

Solveig Rufenacht

10.6.2015 Neue Zürcher Zeitung

Misconduct in financial markets: Greater responsibility for individual bankers

4. November 2015 Neue Zürcher Zeitung

Volkswagen scandal: smoke and mirrors in Wolfsburg

24.2.2016 Neue Zürcher Zeitung

Corruption probe: Brazilian arrested in Petrobras scandal

3.2.2016 Neue Zürcher Zeitung

Understanding business culture: soft factors in corporate success

11.1.2016 Tages-Anzeiger

Sensitive data in foreign hands

HANDELSZEITUNG | 19.2.2016

Corruption: Dutch company pays massive fine

HANDELSZEITUNG | 9.3.2016

Hacker attacks: The threat is global

4.11.2015 Neue Zürcher Zeitung

More transparency in the healthcare sector: pharmaceutical companies must reveal their hands

5.3.2016 Neue Zürcher Zeitung

How far does corporate responsibility go? The ethics of profit

13.4.2010 Neue Zürcher Zeitung

Conscious observance of regulations and legitimacy of trade: new dimensions in compliance

16.7.2015 Neue Zürcher Zeitung

Bribery: Fighting corruption is a matter for the bosses

How effective is your compliance function?

With the continuing rise of new regulations, extra-territorial application of national law and progressive enforcement by authorities, organizations have responded by creating compliance management systems (CMS). While a lot of effort goes into sustaining CMS, one key question remains: How can an organization demonstrate to stakeholders that its CMS is effective and efficient in addressing compliance risks?

In the past, the term compliance was usually narrowed down to an adherence to relevant legislation. Today, it has a broader meaning that includes any relevant rules, policies and ethical standards that might be important to both today's legal requirements and societal expectations as well as upcoming ones. This extended understanding of what compliance comprises poses a challenge to the compliance function and its objectives. How can the organization adhere to all relevant requirements? How can it demonstrate effective and efficient compliance as part of its daily business operations? What should be considered 'relevant' for the CMS going forward?

Compliance officers are somewhat challenged by so-called "double-edged circumstances". If compliance within a company proves to be effective – that is, the organization adheres to the law and its internal policies and procedures, including the Code of Conduct and imposed standards – the compliance officer usually faces questions around the necessity of time and resource investments. If, however, adherence to requirements shows signs of ineffectiveness that can ultimately result in serious regulatory breaches, then the firm as a whole might face material financial and reputational losses.

This leads to the question of how to effectively balance investments in a compliance organization – including a set of policies and standards and the need to maintain speed, agility and flexibility towards the markets. In other words: The compliance organization's challenge is to determine if its compliance efforts are appropriate in relation to the risks that the organization is prepared to bear.

The most effective way of determining the optimal level of compliance is to use a consistent methodology in the form of a compliance management system (CMS) that allows for a coherent development and assessment of the compliance measures in terms of design, implementation and operational effectiveness. Such a CMS applies a systematic approach that is comprehensible to all stakeholders involved, focuses on the key compliance risks that matter to the organization, and allows for an efficient and effective implementation as well as sustainability.

1. **Define requirements:**
   Outline the regulatory obligations and assert the responsibilities of the organization regarding these requirements.

2. **Conduct risk assessment and response:**
   Identify and assess the relevant key compliance risks and define mitigating strategies, e.g. defining compliance requirements and designing effective controls.

3. **Company-wide implementation:**
   Ensure that the compliance requirements are incorporated into business processes.

4. **Training and guidance:**
   Provide effective awareness training to employees so that they understand their roles and responsibilities.

5. **Assessment:**
   Conduct recurring reviews within the organization in order to assess the effectiveness of compliance measures and ensure that responsibilities and requirements are met.

6. **Remediation:**
   Take corrective actions and update the compliance management system as deemed necessary.

Choosing the right CMS standard
While certain regulators have provided CMS guidance in relation to established regulatory requirements, they tend to be developed with a single, specific regulatory topic in mind – e.g. the Resource Guide on the Foreign Corrupt Practices Act (FCPA)[1]. It either proves to be overwhelming in terms of volume and complexity, or it focuses too narrowly on one specific regulatory aspect, while not touching on other compliance topics and how these should be incorporated into the CMS.

In order to address this challenge a more holistic approach is needed as to what a compliance framework should consist of. Notably, four suggested compliance frameworks have become known and are common in Switzerland:

- Fundamentals of effective compliance management;
  published by economiesuisse and SwissHoldings[2]; defines general principles as to how good compliance management should be applied by organizations as part of good corporate governance principles.
- ISO standard 19600 – Compliance management systems;
  published by the International Organization for Standardization – ISO; general guidelines on how to implement and maintain a compliance framework.[3]
- COSO Framework;
  published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO); defines a common internal control model against which organizations may assess their control systems in relation to operations, financial reporting and compliance.[4]
- IDW Assurance Standard: Principles for the Proper Performance of Reasonable Assurance Engagements Relating to Compliance Management Systems (IDW AssS 980);
  published by The Institut der Wirtschaftsprüfer in Deutschland e.V. (Institute of Public Auditors in Germany, Incorporated Association) – IDW; standard that was set by the German audit associations to prescribe how an external auditor should assess the CMS of an audit client.[5]

[1] *https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf*
[2] *http://www.economiesuisse.ch/sites/default/files/downloads/compliance_e_web.pdf*
[3] *http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62342*
[4] *http://www.coso.org/guidance.htm*
[5] *https://shop.idw-verlag.de/product.idw;jsessionid=0EF687DF46D4D29654C72186046592A0?product=20205*

Too much choice? The seven essential elements of a good CMS

While these compliance frameworks might vary in terms of methodology, they all have the common objective to embed compliance effectively and efficiently into the organization's business processes. By doing that they allow for a better mitigation of key compliance risks and thus make sure the CMS is an effective part of the organization's corporate governance. Notably, the following seven key elements are usually part of a good compliance framework:[6]

1. Compliance culture: Clear commitment by leadership ('tone-at-the-top'); compliance culture is embedded within the organization (e.g. company values); leadership style on compliance is consistent at all organizational levels ('walk the talk'); design and set-up of the compliance supervisory board and committees is defined.

2. Compliance objectives: Applicable compliance requirements (laws and regulations) are identified and incorporated into the CMS; Compliance framework (e.g. policies and procedures) provide guidance to the organization; Key CMS objectives are aligned with corporate strategy and goals (e.g. growth, development of new business; seeking new or alternative business opportunities etc.).

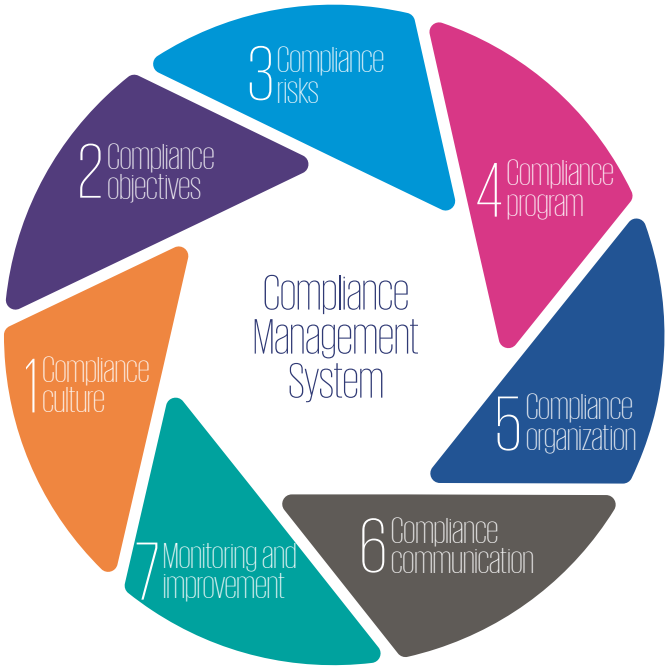
3. Compliance risks: Group risk assessment and risk management is aligned to corporate goals; CMS is developed based on the key compliance risks derived from the risk assessment; identification of compliance risks is done under consideration of compliance objectives; introduction of systematic procedures for risk identification and reporting has an especial focus on emerging risks.

4. Compliance program: Policies designed to mitigate compliance risks are documented and rolled out throughout the organization; training is provided and tailored to the needs of stakeholders; compliance-related documentation is readily available to all relevant stakeholders.

5. Compliance organization: Organizational structure of the CMS is defined and includes formal definition and approval of roles and responsibilities; adequate availability of dedicated compliance resources is ensured in order to make the CMS effective throughout the organization.

6. Compliance communication: Reporting lines to escalate compliance risks including allegations or indications about possible offences are defined; program to ensure adequate and recurring training for target groups is in place; a formal response process to ensure bottom-up feedback is defined.

7. Monitoring and improvement: Process for recurring monitoring of the CMS's effectiveness is established, including reporting channels to address weaknesses; measures in the event of non-compliance are taken promptly and communicated throughout the organization; responsibilities of leadership for maintaining an effective compliance system including remediation of non-compliance issues is clear.



[6] *This is in line with the structure of the IDW PS 980*

Independent assessment: A useful exercise

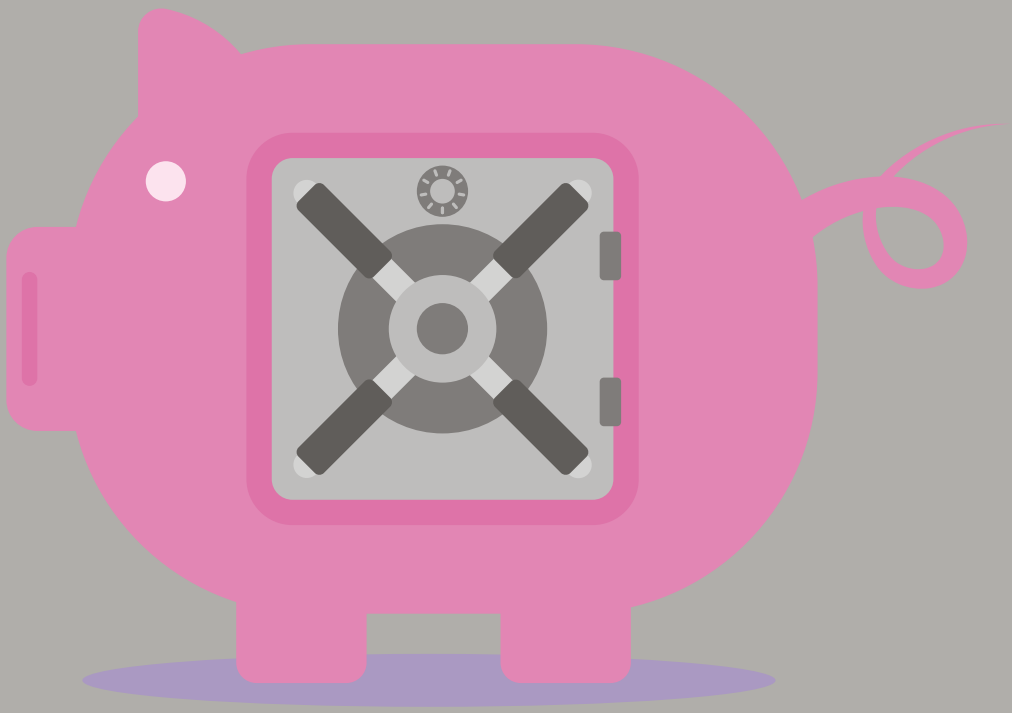
Despite the fact that it is the compliance function's responsibility to design and maintain a CMS, it cannot be emphasized enough that the effective application of the CMS instruments (e.g. controls, guidelines, policies etc.) is the sole duty of the business. To make sure that the business is fully aware of its role and at the same time provides adequate assurance to key stakeholders (e.g. board of directors, executive management) it can be useful for a compliance function to mandate an independent assurance function to provide an 'outside view' – such as the internal audit function or an external service provider. Such a function can give an independent and fresh perspective on how the CMS is adopted within the organization and assurance if it continues to be fit for purpose.

The organization can greatly benefit from such assessments to identify possible gaps, provide an opinion as to how it is implemented and applied or benchmark the CMS against good practice. It can also benefit the compliance officer by demonstrating to stakeholders the compliance function's capabilities in managing an efficient and effective CMS, or if more resources are required to fill identified gaps. Finally, it can serve an organization's leadership to demonstrate that the CMS is appropriate and possible incidents did not arise due to missing policies or because insufficient actions were taken to enforce suitable compliance measures.

In order for an organization to effectively meet the increasing number of internal and external compliance requirements, it is necessary to have a proper CMS in place. Numerous frameworks provide guidance as to how such a CMS should be designed and developed, implemented and sustained. Having a robust CMS in place is only the first step, however. As with the development of new legislations, the CMS should be considered as an evolving framework that needs to be constantly assessed in terms of adequacy of covered key compliance risks, the effective application by the business and the efficient use of resources. Regular reviews and independent assessments can help ensure that what was best practice in the organization yesterday, remains so today and will stand the test of time in the future.

Increasing compliance requirements call for an effective and efficient CMS

Moving beyond (the cost of) compliance



The increasing cost of compliance can feel like an unavoidable fact of business life. The volume of regulations is rising and the regulatory environment is becoming more complex. So much so that the growing internal cost of compliance is considered to be an urgent problem[1] for 69 percent of compliance executives. This gives rise to a recurring question: how to optimize investments in the compliance function to enhance the value it delivers?

Many organizations find themselves spending increasing time on ongoing monitoring and analysis of regulatory changes. The growing internal cost of compliance is considered to be an urgent problem[2] for 69 percent of compliance executives. And 75 percent of Europe-based companies predict compliance costs will increase significantly in 2016.[3] Now is a good time to take a long hard look at your internal compliance model. In particular to ask whether it is efficient in closing the gaps in risk coverage and whether you are leveraging its potential in strategic decision-making. In short, are you turning your compliance activities into a competitive advantage?

With more than 60 percent of compliance direct costs relating to headcount, finding a practical and cost-effective structure is a priority for many corporations. This can be tricky in an area where no single solution fits all. Some small and medium sized organizations raise a valid question: "Do we need a compliance function at all?" A recent publication from economiesuisse Swiss Holding emphasizes how there is no single uniform concept for an efficient compliance organization, giving the example of how small corporations introduce simple but effective compliance measures such as demonstrating appropriate ethical behavior from the leadership, a clear segregation of duties and communication that reinforces the company's fundamental values.

To centralize or decentralize?

Larger organizations meanwhile adopt more formalized structures and functions but must decide whether a centralized, decentralized or hybrid structure is optimal for their needs:

- Centralized: The compliance function retains direct control over all compliance-related activities and execution of controls. A common structure in highly regulated sectors such as financial services, it often involves a large team of dedicated compliance officers.
- Decentralized: Compliance is embedded in existing functions such as finance or human resources. Compliance activities are carried out locally with limited central oversight, resulting in very limited direct compliance headcount cost.
- Hybrid: Responsibilities for some compliance activities are delegated within the organization, but oversight and ultimate responsibility are borne centrally (and regionally, if the corporation is a large multinational). This is increasingly common, as are 'shared' responsibilities where designated employees act in both operational and compliance capacities.

While the fully centralized structure can be perceived as being 'safer', we note it is falling out of favor – perhaps in part because it promotes the view that compliance is the responsibility of a single department rather than the broader organization. By contrast, a decentralized compliance structure ensures that compliance roles are closer to operations, raising awareness of risks and allowing a faster and more efficient response to problems. Moving towards decentralization can help address silo mentality and bring together risk management, business understanding and aspects of legal and compliance expertise. However, limited central compliance involvement can create a lack of monitoring and strategic oversight and may affect the function's independence from the business.

Global, diverse operations are moving to more hybrid compliance structures, which provide the business with a better combination of compliance insight into, and oversight of, local operations. They can also be more effective in embedding a compliance culture across the various parts of the business and achieving greater cost effectiveness due to the creation of dual roles at an operational level. Compliance officers' roles become more strategic / advisory to the business, monitoring regulations and using data analytics to drive the design and execution of compliance programs at an operational level.

Turning compliance into a competitive advantage

It is increasingly important in these resource-constrained times to ensure

[1] *Be Fast and Right in 2016: Key Imperatives for Compliance and Legal Executives, CEB 2015*
[2] *Be Fast and Right in 2016: Key Imperatives for Compliance and Legal Executives, CEB 2015*
[3] *Top 5 Compliance Trends Around the Globe in 2016, Thomson Reuters*
[4] *http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2040*

that the compliance function represents a genuine competitive advantage for the organization. As well as its primary role in protecting the organization there are a number of other ways to drive added value:

Utilizing compliance capabilities for more strategic inputs: Utilizing compliance officers' expertise can support the success of strategic ventures. Involving them in mergers and acquisition activity before a deal is concluded, for example, can help ensure a true understanding of, and preparation for, compliance risks. A pre-acquisition compliance due diligence could look at possible red flags regarding corruption, bribery and anti-competition laws, among other matters. It would consider risks not only within the company to be acquired, but also among its key suppliers, distributors or even charities supported by the company. It would also assess the corporate culture and the formal and informal compliance controls to give a view on behavioral risks, allowing any associated costs to be assessed at an early stage.

Fostering greater loyalty and reducing staff turnover: Training and formal communications from senior and middle management on the topic of compliance and corporate values are essential to raising awareness of compliance issues and expectations. They are, however, insufficient to truly embed the right behaviors in the organization as an isolated effort. To achieve this requires all levels of the organization to demonstrate that they 'walk the talk.' The compliance function has a key role to play here, using a variety of channels to share compliance stories with staff about how the organization has addressed compliance cases or applied ethical standards to business decisions. The effect should be to help create a culture of compliance and set the right tone in terms of ethics and internal justice, directly reinforcing employees' confidence in, and adherence to, appropriate corporate values.

Driving improvements along the value chain: Engaging with external stakeholders about compliance can build and maintain confidence; disseminating information externally can also drive improvements across an industry. The sharing of external assessments and audits of your compliance management system, for example, can provide assurance that you have undertaken all that is reasonably expected to mitigate risks regarding corruption, fraud and export controls – thereby also protecting your clients and other third parties. Several countries have implemented (or are in the process of implementing) an "audit standard" for compliance management systems, and the International Standard Organization (ISO) is due to publish an anti-bribery management system standard (ISO 37001) in late 2016 to "help organizations fight bribery by establishing a culture of integrity, transparency and compliance."[4]

By giving serious thought to how the compliance function is structured and how it engages with both internal and external parties, an organization can help ensure compliance efforts are executed in the right place, resources are utilized properly, unnecessary tasks are avoided, and swift reactions to new developments (changing environment, new regulations) are possible. This can lead overall to a more efficient and cost effective compliance function that can get involved in a broader range of tasks. Altogether, turning the conversation from how expensive the compliance function is, to how much value it delivers.

How cost efficient is your compliance organization?

A review or assessment of your compliance management system should include a cost efficiency analysis that looks at areas such as:

- Benchmark your staffing, spending and program responsibilities against peers
- Proportionality of compliance risks vs regulatory requirements
- Efficiency assessment of the different compliance programs
- Efficiency assessment of the response time to address upcoming / new regulations
- Key Performance Indicators (KPIs) related to existing compliance controls; these KPIs can illustrate how smoothly controls are embedded in the business – being seen as a facilitator, rather than a blockage, in business operations
- Coordinate compliance efforts around the major risks
- Develop and implement a compliance cost efficiency methodology
- Analyze potential risk areas that are not covered
- Develop a flexible compliance program that can react swiftly to changing conditions

Such measures enable the organization to achieve a cost effective yet robust program assessment and to build a strategic plan that is based on its industry needs, the maturity of its compliance organization and upcoming regulatory challenges.

Employees – Managing the risk of unacceptable behavior

Tim Lindon, Chief Compliance Officer at Philip Morris International in Lausanne, Switzerland discusses the importance of understanding human behavior when leading a compliance function, and the role of data analytics to support this task, in an interview with Philippe Fleury and Solveig Rufenacht.

KPMG: What led you to compliance after a broad career in litigation and corporate law?

Tim Lindon: Becoming a Chief Compliance Officer was not part of my career plan. In fact, when I started at Philip Morris the role didn't even exist. But looking back at my 25 years in the company, it's definitely been the most challenging and rewarding position I've held here. My legal background allowed me to understand the risks facing the company but it was still a significant transition to go from a legal role to running a global function. I hadn't anticipated how different the roles are. In a legal role, no matter how senior you are, you spend most of your time responding to clients' needs and legal developments. Compliance is similar to other functions in that you are developing strategies and managing a function. Law is a good background for it but does not have a monopoly on the necessary characteristics – understanding the business, being respected for trust and integrity, demonstrating leadership skills and knowing how to get things done are the key elements for making a strong Chief Compliance Officer.

How has your role changed over the past five years?

I was lucky. I inherited a compliance program that was very strong and well developed and I work for a company where integrity and compliance is ingrained in the business. So I had to enhance, rather than create, the program. However, I wanted - and in fact we needed - to start doing some things differently to stay contemporary and move forward. The greatest change was in how the compliance program is perceived throughout the business. Changing the perception from it being a function responsible for enforcing rules, to a state where compliance is everyone's responsibility and truly embedded in the business. We made it easier, rather than more complex, for people to comply. We improved transparency, as the more transparent compliance is, the more likely people will comply.

How can you make it easier against a background of increasing regulations?

Through understanding employees' needs first and foremost. What are their questions and concerns? Writing materials and developing trainings that address specific concerns rather than

"...simplifying our Code of Conduct – which we now call our Guidebook for Success – reducing its length by half and highlighting its connection to our business."

"Particularly in compliance, more resources do not guarantee a better program."

trying to cover every eventuality. We started revising and simplifying our Code of Conduct - which we now call our Guidebook for Success – reducing its length by half and highlighting its connection to our business. We made it very specific to what people need to know, and explained why we have certain rules and where they can go to find more information. We put it on an app so it was accessible. Overall, we use a behavioral approach to reducing misconduct, working to understand how employees actually react to ethical dilemmas. More rules are not the route to being more effective. While a strong moral tone is essential, you don't need to preach to people. You try to work peer-to-peer to understand how business proposals might go wrong if people behave certain ways under pressure. Really, you become a psychologist as well as a business advisor.

Which key compliance challenges are you focused on right now?

As at most large companies, the greatest compliance challenges come from increased regulations and globalization. Overall, there is no doubt that in many areas – whether privacy, the environment, anti-corruption or competition – risks are increasing due to a greater number of complex regulations and the rapid globalization of risks. In the area of anti-corruption, for example, it's not about complying only with US law but also with new laws in the UK, Brazil and elsewhere. Regulatory issues are simply too vast to be handled by the compliance department alone, so the keys risks are managed by the functions with the most expertise. For example, the Operations Department is the owner of our Environmental Health and Safety program. The other challenge that is a focus of compliance departments is increased pressure. The pace of change has picked up, competition is more global and employees often face more pressure. This can lead individuals to sometimes forget their ethical obligations in the heat of the moment, so one of the challenges is again not to have more rules but to consider human behavior and how to reinforce a certain conduct. We adjust trainings to avoid giving employees the answers right away but to put them in a pressured situation to see how they adapt. We also look to ensure that trainings are not done remotely but by their supervisors to be more immediate and effective.

What constitutes an effective compliance program and how do you measure its effectiveness at Philip Morris?

Personally I'm very skeptical about many compliance KPIs. The ones I've seen often measure mostly the number of trainings and the number of incidents. A compliance program is not designed to produce numbers but a strong culture; a culture that's going to prevent misconduct. To measure effectiveness, we carry out a comprehensive company-wide ethics and compliance survey every two to three years. Over 28,000 employees responded to the last one. You need to recognize there are pockets of strengths in your program, and different cultures and managers where there might be issues. A broad survey can take the temperature of different functions and countries and then compare them, as well as help to understand trends over time. The most important KPI is the strength of your culture, and it's crucial to have a robust way of measuring this.

What are your views on the use of data analytics in monitoring the effectiveness of compliance programs, and how do you use data in your own role?

Data analytics is both the future of compliance and an important area of concern. Increasingly, big data is showing up everywhere in the company from corporate audit to HR. Compliance has a role in making sure

"A compliance program is not designed to produce numbers but a strong culture; a culture that's going to prevent misconduct."

that the right data are used, and that both privacy laws and employees are respected. Big data and data analytics have enormous potential for compliance but it doesn't require massive investment. It's something that every company can do. At a minimum, companies should be analyzing the number, type and geographic locations of their cases. If this is tied to your human resources system it produces all sorts of interesting analyses that can raise red flags and help prevent incidents in other jurisdictions. The second use of data analytics is to capture the root causes of misconduct and to be able to understand and share them. Last year, we mandated that anyone who carries out a compliance investigation must do an analysis at the end of it. What do they believe were the root causes, the external and internal influences, the behavioral factors, the organizational factors? We then begin to see the links. Data analytics is the future because it is one of the answers to the business need to anticipate compliance issues. But it doesn't have to be a massive undertaking - it just has to involve using your basic data in a way that helps you to understand root causes in order to predict and control misconduct.

What is your advice to mid-sized companies, NGOs and governmental agencies that feel the need to set up a compliance organization but are afraid of the high costs involved?

One size doesn't fit all and particularly in compliance, more resources do not guarantee a better program. My first suggestion is that the more responsibilities that can be assigned to the ongoing business, the better. In a mid-sized organization that's looking to save resources I would seriously consider an approach that focuses on keeping it simple, making the compliance function visible, and understanding the people and the organization. Taking a behavioral approach will save resources because it allows you to understand your organization and to focus on where are the greatest risks and how people might react to changes in the organization. Regulatory authorities in the US Department of Justice and elsewhere don't necessarily expect companies to demonstrate they are making huge financial investments or that they have extensive rules to cover every area comprehensively. Rather that they have an approach that is best tailored to the size and the issues of the organization. This ties with not needing a large central organization. You need to centralize training, communications and risk assessment and this can usually be done with a handful of people; but whether you are a global or a mid-sized organization, the message can get seriously diluted with distance. I would invest in at least one full time person close to each major business unit and in many geographies rather than a larger central staff. It's easier to reinforce your message.

What does the future hold for compliance functions and compliance officers?

I think that compliance in the next five years will increasingly become a distinct profession. The challenge will be, first of all, to enhance the core skills needed for people who want to make their career in compliance, while at the same time finding outstanding talent within the organization that wants to come to the function for two or three years before returning to their areas and becoming life-long ambassadors for compliance.
Data analytics will definitely make compliance easier and help us to anticipate issues.

The future of the compliance role is not necessarily more rules but in doing more to understand employee behavior – working with it, rather than against it.

Don't get bitten by third party risk

With more than one-third of businesses[1] failing to formally identify high-risk third parties, many potential compliance perils go unchecked. To what extent do third parties pose a threat to your business?

Third party compliance risk management is one of the biggest challenges facing companies. More than one-third of businesses do not formally identify high-risk third parties, and many more do not actively use the processes they have in place.[2] Compliance violations by business partners can harm your company, and ignorance of compliance risks is not a valid argument when dealing with law enforcement agencies. Is your business at risk?

In today's international business environment, companies typically deal with a multitude of business partners such as vendors, joint-venture partners and sales agents. Knowing the people with whom you are doing business is critical when assessing your business risks and, increasingly, your compliance risks.

Exposed by association

Authorities and the public at large expect high standards of integrity from businesses. A compliance incident at one of your business partners can have substantial repercussions for your own company. Research shows that third parties are involved in more than 75 percent of corruption cases.[3] A global pharmaceutical manufacturer, for example, recently agreed to pay USD 25 million to settle a U.S. Securities and Exchange Commission (SEC) case that claimed payments had been made through third party event planning and travel companies to Chinese government officials in connection with pharmaceutical sales. According to the SEC: *"Among other things… [the company] failed to conduct proper due diligence in connection with these vendors and failed to ensure sufficient and appropriate support for the selling and marketing expenses submitted by these vendors."*[4]

What you don't know can hurt you

Organizations that fail to evaluate business partners adequately – to know who they are and how they operate — expose themselves to reputational and operational risks, government inquiry, financial penalties and even criminal liability. Two prominent pieces of anti-bribery and corruption (ABC) legislation specifically refer to an organization's accountability for third party involvement in bribes:

- The UK Bribery Act: "A commercial organization will be liable to prosecution if a person associated with it bribes another person intending to obtain or retain business or an advantage in the conduct of business for that organization. A person associated with a commercial organization is defined as a person who 'performs services' for or on behalf of the organization. This person can be an individual or an incorporated or unincorporated body."[5]
- The US Foreign Corrupt Practices Act (FCPA): "the FCPA prohibits corrupt payments made through third parties or intermediaries."[6] It is unlawful to make a payment to a third party, while knowing that all or a portion of the payment will go directly or indirectly to a foreign official. The term 'knowing' includes conscious disregard and deliberate ignorance.

The UK Bribery Act and FCPA both proscribe that organizations should apply risk-based due diligence procedures on third parties who perform or will perform services for or on their behalf. Appropriate processes and policies can reduce the threat posed by third parties and should therefore be high on any board agenda. To achieve the right balance between resources dedicated to due diligence and the level of assurance your organization wants to achieve, a risk-based approach should prioritize resources on the highest risk targets. Four essential steps in any third party risk management (TPRM) system include:

[1] *Anti-Bribery and Corruption: Rising to the challenge in the age of globalization,* KPMG in Switzerland, 2015
[2] *Anti-Bribery and Corruption: Rising to the challenge in the age of globalization,* KPMG in Switzerland, 2015
[3] *OECD Foreign Bribery Report,* OECD, 2014
[4] *https://www.sec.gov/litigation/admin/2016/34-77431.pdf*
[5] The Bribery Act 2010 – Guidance
[6] FCPA U.S. Foreign Corrupt Practices Act By the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission

Four essential steps to mitigate third party risks

1. Identifying relevant third parties: The inventory of third parties with whom you do business might be large and outdated. A good first step is a structured approach to eliminate third parties that are no longer relevant to your business.

2. Managing the onboarding process and risk assessment: Each third party poses a different level of risk. A useful approach is to categorize relevant third parties into high, medium and low risk. This might be determined by country of operation, industry sector or the nature of the business (e.g. commodity risk) conducted together.

3. Conducting an appropriate level of integrity due diligence: You might subject low-risk third parties to desktop due diligence. For high risk, or where there is a lack of publicly available information, a full in-country due diligence may be required.

4. Ongoing monitoring of third parties: As things can change, you should periodically reassess third parties to ensure ongoing compliance, taking into account the risk rating of the third party. Such assessment could include providing compliance training to third parties and on-site audits, among other activities.

It's time to invest in prevention

A weak TPRM system is a significant gap that urgently needs filling. Failure to conduct adequate due diligence blinds you to potential misconduct that could give rise to serious consequences. Even if you conduct business in good faith, you can come under suspicion – or incur a legal liability – through association with a particular entity. Should you be subjected to an investigation, effective and documented measures that show your efforts to comply with legislation may reduce or eliminate sanctions.

In an environment of heightened regulatory scrutiny and increasingly complex global business arrangements, your awareness of people and companies acting on your behalf is critical. Implementing the right sized third party risk management system can deliver substantial benefits to your organization. It can give you a competitive business advantage, lower your risk exposure and reduce the complexity of business relations in high-risk countries or industries.

Environmental regulation violations or human rights abuses in your supply chain are among the wide range of other issues that can also hurt your organization

On 21 April 2015, a broad coalition of Swiss civil society organizations working in human rights, development and environmental protection launched the 'Responsible Business Initiative'. According to the initiative, "Swiss-based firms will be liable for human rights abuses and environmental violations caused abroad by companies under their control. This provision will enable victims of human rights violations and environmental damage to seek redress in Switzerland. Companies who haven't complied with their due diligence obligations will be held accountable in front of Swiss Courts."

The initiative was launched after the Swiss lower chamber of parliament dismissed a motion for increased corporate accountability, after having initially accepted it. If 100,000 signatures have been gathered by 21 October 2016 to support the initiative, it will be submitted to Swiss voters through a referendum.

Commodities trading – Keeping pace with regulatory changes in a fast-moving industry

Brian Lewis, Group Compliance Officer at Gunvor, discusses compliance for commodities traders with Philippe Fleury and Solveig Rufenacht


GUNVOR

KPMG: What led you to work in compliance and how does your current environment differ from where you worked previously?

Brian Lewis: As with most compliance professionals I know, I never set out to have a career in compliance. I was working in banking during a time of great changes, prior to the financial crisis and in 2010, I saw an opportunity to move to a trading house. Not least the culture, the agility in getting things done and the pragmatism in delivering. You are not constrained by having to go through 25 committees, which is important, as commodities trading is a fast-moving market that is in the process of maturing; implementing changes and embedding compliance ownership and responsibility within the operations is key to ensure the industry keeps its agility and response to the market. This is how I see compliance should work, and therefore working for a trading company has been fantastic.

What are the key recent changes that are affecting your industry?

Firstly, the regulatory reforms that have stemmed since 2009 from the financial crisis. They impact what we do, especially as we are commercial users of derivatives. But I think it should be remembered that we did not cause the financial crisis nor will we cause another one. Secondly, there is much greater enforcement by authorities, particularly in the US. Realistically, it is becoming increasingly challenging for corporations to manage the massive increase in regulations.

What do you see as the biggest compliance risks in your industry?

In my view, there are three areas. One is around health and safety and the environment. What happens if one of our vessels or its cargo has a large spill? How to respond to such a disaster? What do we need to do to prevent it from happening in the first place? A second area is paramount – financial crimes. The areas where we trade and from where we source

"Compliance starts to build into a relentless march that is appreciated by, and embedded in, all functions."

commodities are, unfortunately, not always safe. There's a risk of money laundering, terrorist financing, or potentially being inadvertently a facilitator of tax evasion for counterparties; and of course all the risks of being associated with third parties involved in bribery and corruption. The third area is around market conduct or how we trade in our markets. Regulations in this area are continuing to increase but I believe there should be greater market-specific scrutiny by regulatory bodies. Oil is different to metals, which is different to the next commodity. To comply, and importantly demonstrate compliance with regulations, companies are undertaking a significant amount of work to achieve this, whilst maintaining our reactivity, risk management and speed to market, which can be a challenge.
These are the three risks areas I see over the next 12-18 months.

What did you focus on when establishing your global compliance program?

There were two primary things I needed to look at. One was around market conduct - what we do, what are the controls and whether there was any training. Developing our communication towards the trading floor and, by developing our advisory role, becoming a partner to the business. Second was around financial crime – specifically, how did we review our counterparties? How did we make sure we are not associated with illegal practices? At the beginning, the big thing was risk and credit, looking at a new counterparty and credit to question whether they were able to pay us. The necessary data were spread across multiple systems and weren't standardized. So the first thing was to try to find how we could structure that better. We came up with the idea of CMS, the counterparty management system, which we built and have continuously developed. To the questions of credit and risk, we added checks on reputation, trade sanctions etc to come up with a holistic due diligence program that provides us with a high degree of comfort that we are dealing only with reputable parties. This had to be done with buy-in from senior management and trading.

How do you see compliance and sustainability being embedded in your business?

A large multinational corporation is often perceived as being very autocratic and flat. This means the compliance function is viewed as a bureaucratic policeman. But once you start applying commercial logic to a problem, you help to ensure a compliant outcome. When you demonstrate that you are helping the business and the client-facing colleagues, and particularly when you respond quickly rather than being seen as a blockage or a delay, that helps.
Compliance starts to build into a relentless march that is appreciated by, and embedded in, all functions.
Of course, compliance nowadays has an extremely broad role but the compliance function cannot do everything by itself. This is in part why it needs to be embedded throughout the business, but also why we work very closely with our group sustainability function, for instance.
In Europe, we have to submit different sustainability information to different regulators – this is just part of being active in this sector.

Looking forward, how do you see compliance evolving?

It's changing rapidly. If we look at where the authorities and expectations are heading, it's about individual accountability. We've seen enforcement, particularly in the US, against compliance officers who failed to stop incidents. We accept that risk and our responsibilities to the best of our ability. Our role is becoming more advisory driven, but it's also necessary to take a firmer stance in some areas where five years ago a softer approach would have been tolerated. For me, it's about continuing to pay attention to the very small things. Something that can look innocuous to your colleague or to management, but that you can spot is where a problem can start. In five years, we will probably find people becoming more specialized under a broad compliance umbrella. Basel III means we need people to specifically look after capital matters - how the firm calculates and manages its capital. It's traditionally been a blend with finance, but it's again becoming a compliance process.
Compliance itself is becoming blurred in the same way that a few years ago people would think about governance. It's so broad. It's about defining what the boundaries are, and saying for this piece we want zero refinery incidents, zero incidents involving the vessel we've chartered, zero incidents in bribery and corruption. This already broad field looks set to become even wider as regulatory requirements increase.

Applying data analytics to compliance

It is tempting to see thorough data analytics as being too time consuming and complex for the pressured compliance officer. But given the sheer volume of data held by the average organization, can you afford to ignore its potential value for your compliance activities?

Gaining useful insights from the data held throughout your organization can be a mammoth task. Even once you've collected the appropriate data, the challenge is how to create value from them. In an era of tougher regulatory sanctions, however, could data analytics work harder to support your compliance efforts?

Although a large organization typically stores a huge amount of information, it is rare for these data to be systematically utilized for compliance purposes. Yet, as regulators increase their levels of scrutiny and potential sanctions, firms are missing out on a mine of useful information that could feed into their compliance activities – thereby also missing the opportunity to mitigate risks through early detection.

Of course, collecting data is only the beginning. Once the mechanics of how to collect them are addressed, you must make sure you're drawing worthwhile conclusions from them. In short, the challenge is how to turn data into useful insights.

The benefits: Prediction, detection and mitigation

Known compliance risks can be predicted and detected with simple analytical approaches, but what about unknown risks? How should these be tackled when so much information is flowing around the organization? This is where data analytics comes into its own – applying advanced statistical methods based on real-time, continuous monitoring and analysis of both structured and unstructured data. In global finance, for instance, compliance data analytics is often used to meet regulatory requirements by strengthening internal anti-money laundering and counter-terrorist financing. Take the continuous monitoring of electronic payment streams as an example. Payment streams are analyzed overall and by categories such as high-risk countries or individuals. Indicators of potential violations are identified such as unexpected activity peaks and unusual activities that may need further investigation. Similarly, patterns can more readily be identified that suggest hidden relationships between organizations, individuals and/or bank accounts. It's hard to imagine this being even remotely possible with a manual or outdated analytical approach.

Better and more efficient compliance

Data analytics can allow the compliance officer to spend more time on tasks that generate greater value. For instance, in the interpretation of data where the compliance officer can add value by utilizing expertise to set data against the context of regulatory requirements, compliance risks and the organization's unique risk tolerance.

Better use of data also increases the quality of information with which the compliance officer can work. The data gathered through auditing and monitoring activities – as well as information held in silos in the various operating functions – are invaluable sources of possible improvement. They can help deliver better control of compliance risks by enabling insights into the correct application of regulations, as well as judging the riskiest areas where potentially serious issues can arise.

The uses of a compliance dashboard

Compiling this range of compliance-relevant information can be made easier through the use of a single dashboard. The type of information on this dashboard is usually referred to as `non financial risk` to describe the specific character of the dashboard compared to more general business intelligence solutions.

The range of potential compliance benefits is therefore significant, including the provision of:

- **faster** insights and reducing the amount of time-consuming and error-prone manual work by automating data collection and analysis of data
- **greater** number of insights by analyzing all data, not just a sample
- **earlier** insights to counter potentially adverse situations through real-time detection and prediction of trends, patterns and anomalies.

Stage 0

No central system where risk assessments or controls (testing results) are maintained.

Stage 1

Registration of risks, incidents, threats, controls. etc. in IT Governance, Risk Management and Compliance (GRC) Tooling. Optimization of GRC solutions still possible.

Stage 2

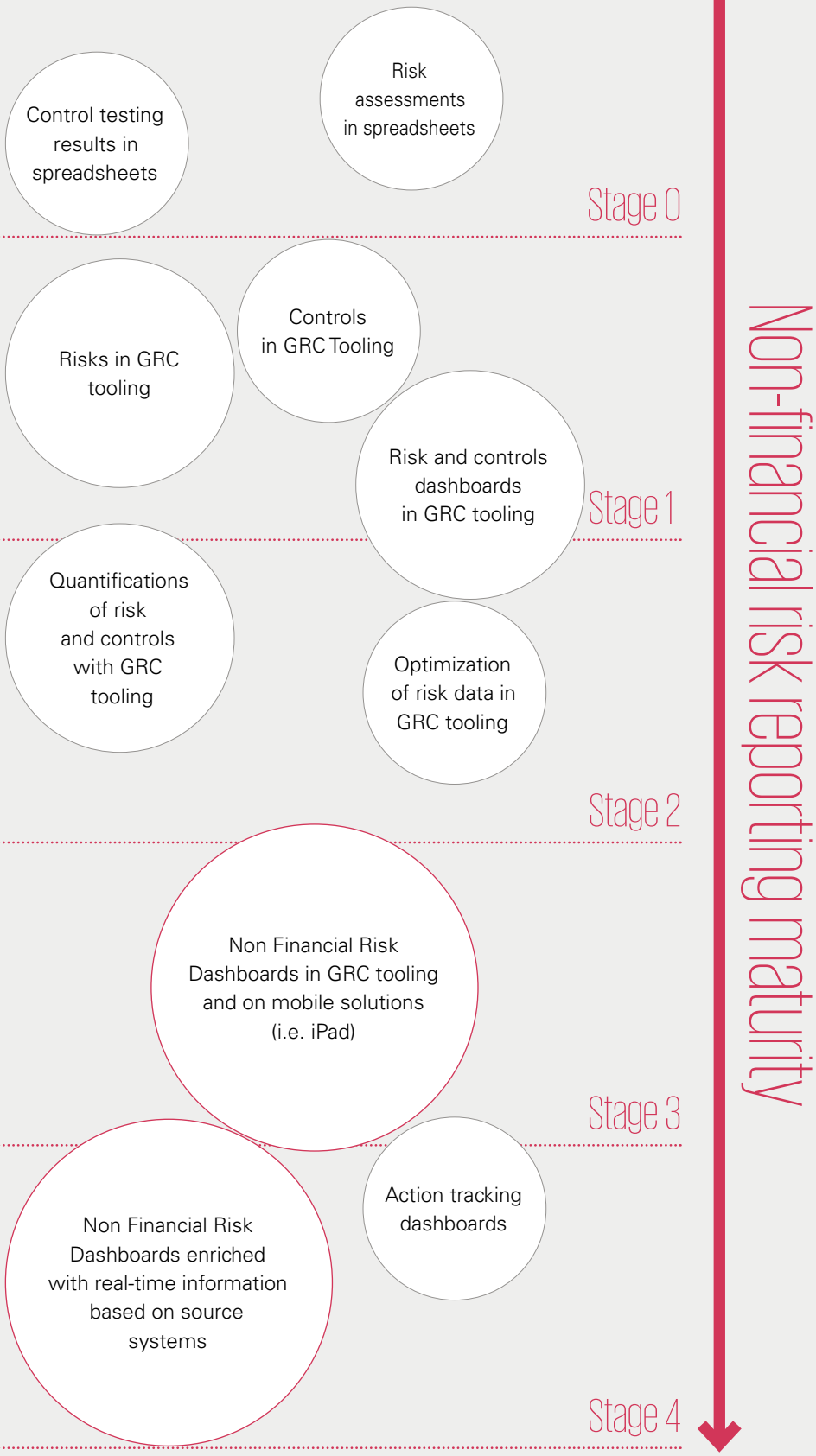
Quantification of non financial risk based on Internal Rating Based (IRB) modeling methods (loss distribution approach).

Stage 3

Design and development of Non Financial Risk Dashboards (tablet compatible).

Stage 4

Development of real time risks dashboards based on source system data.



Source: KPMG Switzerland

A dashboard allows full and real-time compliance and supports strategic purposes. It can generate synergies by integrating into a single interface an organization's compliance with various global legislations, affording the compliance officer a graphical overview of all potential compliance risks and their severity. It also facilitates quicker response times to regulators and a generally more proactive approach that could prevent or minimize any damage caused by possible regulatory investigations.

This ability to respond in real time is hugely important, especially in a collaborative compliance program where you try to correlate different types of risk. The earlier you can get to an issue, the more flexibility you have to deal with employee conduct and prevent issues before they develop. Data analytics can therefore aid the overall compliance effort, feeding useful and timely data back into the organization.

Trade sanctions: supporting the investment case

Complying with trade sanctions is an area where data analytics are increasingly used. And for good reason. With a list of more than 1,000 sanctions worldwide, it is almost impossible for an international business to comply without implementing a solid data analytics solution that continuously monitors all potential matches between that list and a corporation's own set of business partners, suppliers or even employees.

Furthermore, the trend of regulators worldwide to apply heavy economic sanctions looks unlikely to change in the foreseeable future. In 2015, the US levied fines totaling USD 600 million[1] to organizations around the world. In the UK, fines in 2015 amounted to GBP 905 million.[2] Against this background, the investment case for data analytics in the area of export controls – and more specifically trade sanctions – is easier to make, particularly when combined with the possibility of transforming the compliance function to generate more value.

The potential benefits of enhanced data analytics are therefore substantial

It can drive compliance towards greater effectiveness. And its power to help gain the trust of regulators and shareholders should not be underestimated through demonstrating all-important transparency.

[1] *US Department of the Treasury: https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/2015.aspx*
[2] *UK Financial Conduct Authority (FCA): http://www.fca.org.uk/firms/being-regulated/enforcement/fines/2015-fines*

Private matters: Putting data protection on the board agenda

With the General Data Protection Regulation (GDPR) coming into force soon, the bar is being raised for any organization that deals with EU citizens' personal data. As heavier sanctions, notification obligations and other considerations are introduced, is your organization ready for the new data protection reality?

December 2015 marked the European Commission's agreement on the General Data Protection Regulation (GDPR), which will affect all organizations that deal with the personal data of EU citizens. Organizations have some serious compliance homework to do if they are to be fully prepared before enforcement of the GDPR starts in early 2018.

Data protection regulation has been around for decades, but the GDPR makes adequate data protection and corresponding governance systems significantly more important. This new legislation is the most impactful change in privacy and data protection regulation yet and should be treated as a board agenda item at every organization. Here are four very good reasons why.

1. Higher sanctions for non-compliance

Failure to comply with one or more provisions of the GDPR may lead to fines as high as EUR 20 million or 4 percent of global annual turnover. This marks a radical shift from the limited sanctions under the old EU data protection regime, where the financial risks were consequently immaterial to most large organizations. The GDPR brings sanctions more into line with EU competition laws, where fines amounting to tens of millions of dollars are not the exception.

2. Data breach notification obligation

The GDPR introduces to every organization an obligation to report data breach notifications. Organizations must notify the respective supervisory authority within 72 hours after becoming aware of a data breach that requires notification. In the case of a data breach with high privacy risks, affected data subjects must be informed without delay. This obligation means organizations must have appropriate processes and technology in place to monitor, follow up on and ideally prevent data breaches. While many organizations have invested heavily in enhancing information security over recent years, not all have the full set of required safeguards in place. Under the new regulatory requirements, failure to adequately monitor and follow up on data breaches will lead to higher fines and are likely to have negative reputational consequences.

3. Data Protection by Design

Organizations are already required to have implemented appropriate technical and organizational measures to protect personal data. Under the GDPR, they will now need to demonstrate that measures are continuously reviewed and updated. In addition, there is a requirement to be able to demonstrate that appropriate measures are included in the design of processing operations and that by default, personal data are processed only where necessary. In connection with this, organizations must carry out a Data Protection Impact Assessment on the envisaged processing operations where processing is likely to lead to high privacy risks. Simply updating standard policies for data protection compliance will not suffice and it is no longer acceptable

for data protection compliance to be treated as an afterthought. Data protection must be a core consideration when developing new solutions and services. This will lead to situations where the launch of certain products or services is deliberately postponed until data protection risks are resolved and the privacy of consumers can be guaranteed. The Data Protection by Design requirements truly cover a broader sense of data protection.

4. Data lifecycle management

The GDPR enhances the right of the data subject to have all its personal data removed on request. In addition, when processors are used in the chain of personal data processing, liability for correctly deleting all personal data lies in principle with the data controller. This means organizations are generally responsible for finding and erasing relevant personal data related to the data subject concerned – both within the own organization and at any third parties with which the personal data have been shared. For many organizations it demands the introduction of improvements to achieve the highest standards of data governance and personal data lifecycle management.

These are only four reasons why the GDPR should be a main board agenda item

The regulation presents many more. In short, the GDPR moves data protection to the core of business activities. Management's challenge is to not only adapt policy frameworks to the new regulation, but to implement effective data protection controls throughout the organization – and, crucially, at companies with which data are shared.

Sector highlight: As the processing of clinical trial data is considered extremely sensitive and places higher demands on data protection levels, pharmaceuticals is a sector for which the GDPR is especially pertinent.

Given the sheer quantity and sensitivity of personal data processed by the pharmaceutical industry, it can be reasonably expected that regulators will first focus their attention on this sector. With that in mind, organizations should already begin gearing up to comply for when the GDPR is enforced from early 2018. Assessing the organization's current readiness for data protection compliance is an essential first step to understanding where are the gaps and what improvements should be prioritized. With less than two years to go, the new regulation will soon take effect. And with data privacy adopting such a high profile, it will not be easy to keep data breaches private.

The insider threat: Compliance risks from within your organization

History has proved time and again that the most devastating attacks originate from inside an organization. The causes can be a range of intentional or unintentional acts. Is your organization safe from third party risks and your own employees?

Have you considered stress testing your technology or business processes to determine: "What if a malicious insider was to do this or that? Is it possible, and how could I prevent or detect it?"

It is an uncomfortable fact of life that the people we trust may sometimes represent the greatest danger. Employees and third parties have routine access to our most precious information, financial and technical assets. They operate our information systems and know how to manipulate them. They might even be privy to protective security measures, giving them an excellent insight into gaps and loopholes. Together, these factors make the insider threat particularly potent. When addressing human weakness, organizational approaches are generally only responsive. A reaction takes place after the damage has been done, rather than proactively focusing on prevention and detection. While the more security-conscious organizations have rolled out projects around data loss prevention and privileged user monitoring, such solutions excessively emphasize technology.

Understanding the risk

Unlike attacks that originate from outside the company, employees have legitimate reasons to access your premises and systems. Whether intentional (fraud) or unintentional (accident or negligence), insider threats can lead to the loss of intellectual property, negative reputational impact, leakage of vital information, disruption of business operations, and financial loss from any or all of these. Poor economic conditions, inadequate human resource management (absence of a fair appraisal process, no career development planning, lack of clear roles and responsibilities) or personal issues can all heighten the risk.

A credible threat requires all three of the following ingredients to be present. An opportunity must exist in terms of failures in controls or processes. The motivation must be there, perhaps encouraged by headcount reduction, work pressures or financial distress. And there must be an attitude that the organizational culture is negative or employees are treated badly, resulting in a sense of damaged trust. Environments in which costs are being aggressively managed down can contribute to these ingredients. Corporate culture plays a big role, particularly if the culture is that business ethics have no place: "…Enron, where the prevailing corporate culture was to push everything to the limits: business practices, laws and personal behavior."[1]

Insider threats are far more difficult to assess, as they are less technology-based than external threats and are much more people and process-oriented. Detecting and addressing them requires a truly coordinated, multi-disciplinary approach by staff with experience in this field.

Greater threats in the 21st Century

Current working practices exacerbate the threat. Remote working serves to improve employees' working conditions by promoting a healthy work-life-balance while saving the company costs. From a security perspective, however, it can cause a loss of control over sensitive data and can encourage relaxed behavior. Similarly, BYOD (Bring Your Own Device) – where employees access or store business data on privately owned smartphones, tablets and laptops – is increasingly common, blurring the lines between business and private use as well as causing security concerns.

[1] *The Wall Street Journal, 26 August 2002*

Recognizing the problem: From a responsive to a proactive approach

Tackling the threat requires a collaborative approach across the organization. It also needs strong support from the organization's most senior leaders as well as a willingness to discuss topics that might be taboo, such as people's motivations to cause damage or the real state of an organization's controls. Successfully combating the threat begins with recognizing that problems can exist anywhere and knowing where the weak spots are. Identifying strategic threats, asset and process vulnerabilities and the current effectiveness of security controls helps management to evaluate risks and adopt risk-based organizational, administrative and technical controls.

To achieve this, management must implement a culture that proactively tackles compliance risks. A close dialog between risk managers, executive management and relevant stakeholders can go a long way towards this objective. Together, they can develop, integrate and promote security aspects as part of your strategy and corporate culture. As you work out what you can do and where to start, you might take this a step further by formally assigning responsibility for the management of insider threats with the objective of facilitating such dialog and seeking to balance stakeholders' needs with suitable levels of security.

Mitigating risks through a coordinated approach

Logically, maintaining a single risk operating model across the organization and across locations can be cheaper and less resource-intensive than having five or six. A well-defined and collaborative approach is also more likely to provide management with true oversight and a dashboard. Should any issue or incident occur, they did everything they could have reasonably been expected to. This can be especially helpful in the event of breaches of regulations or legislation and in demonstrating accountability to stakeholders.

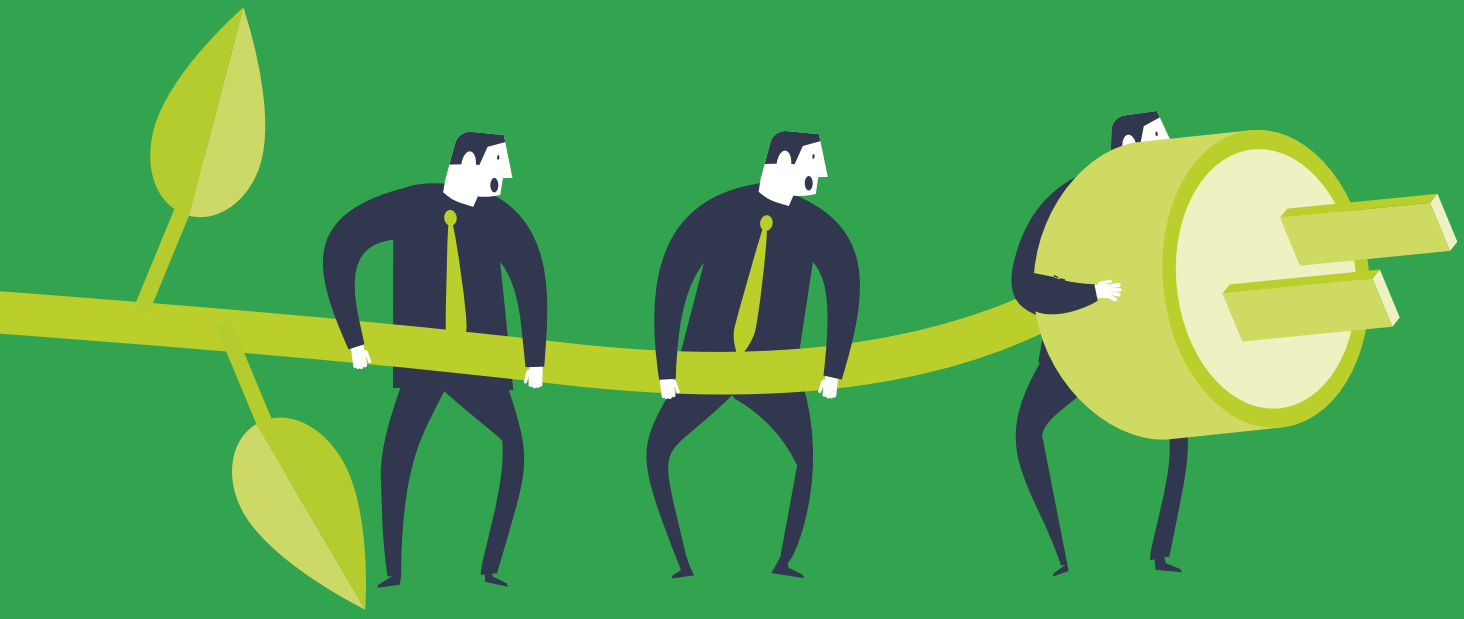
An organized approach to tracking people risks in a way that is understood and supported by management and staff can also improve the organization's culture, deter wrongdoing and discourage inappropriate behavior by potential future employees. It can assure colleagues that the organization takes risks seriously and will do as much to protect 'good' employees as it will to sanction 'bad' ones. Last but not least, a robust approach provides clarity to employees, compliance officers and other staff responsible for the organization's well-being and security. It improves the chance that if something goes wrong, it will be picked up internally rather than being brought to management's attention by an outside party.

Even if your organization has policies and controls in place regarding people, processes and technology, how confident are you that these are being followed and are effective? How many employees fail to comply with them? In a nutshell, policies are good only if they are respected, enforced and measured at regular intervals. They must also seek an equilibrium between strategy, people, process and technology if insider threats are to be reduced. Every department must be coordinated and know how to deal with identified risks. Such an approach can be implemented progressively – it needs to neither be a 'big bang' approach nor appear threatening to employees.

The key is to remember that not every insider threat is malicious

Human beings are capable of carelessness or poor judgment. This is why solutions must be proactive and holistic, ideally to prevent problems from arising in the first case. While external hackers and fraudsters get more attention in the media, the biggest threat is much closer to home.

Sustainability



A new core competence for compliance?

Corporate sustainability has come a long way since it was only a ‘nod’ to green issues. It is now a core element of how we do business. As its importance has grown, so have stakeholders’ expectations. Does your organization treat sustainability as a key compliance issue?

Encompassing a broad range of social, environmental and economic topics, sustainability can mean different things to different people. Yet the rapid pace of change in legislative requirements, reporting standards and stakeholder expectations means one thing for all organizations: Sustainability should be a central topic for the compliance function.

Sustainability impacts almost every aspect of an organization's operations. It has matured from being an isolated topic that concerned 'green' issues such as applying a 'recycle' label to product packaging, to being an area that influences supply chain management, product development, investor relations, the ability to attract and retain talent, and so much more.

A broader compliance role

As the various areas of sustainability management have expanded, there is a need to actively ensure all relevant laws and regulations are adhered to, as well as publicly stated standards and targets. An organization-wide, coordinated approach is necessary to avoid potential gaps caused by silo mentality. The compliance function plays a key role in facilitating this in order to deal with a number of trends:

1. Stakeholder expectations are on the rise

Companies' ethical behaviors are under increasing scrutiny – not only in their own operations but also along the supply chain. Occurrences of serious non-compliance spread in an instant across social media, causing reputational damage that can significantly damage the organization or even an entire industry.

2. Legislation is intensifying

Relevant legislation is becoming both broader and deeper. From the revision of the Swiss Company Law which foresees a quota of 30 percent female board members to the Responsible Business Initiative that would oblige Swiss businesses to conduct environmental and human rights due diligence on entities abroad that are under their control … Although it is not clear if and in which form such laws will be passed in Switzerland, they represent a clear regulatory direction.

3. Voluntary commitments are becoming more popular

Companies are responding to stakeholder expectations by committing to comply with voluntary standards and principles such as the UN Global Compact, sector initiatives such as the Pharmaceutical Supply Chain Initiative, or in the area of consumer products labeling such as that from Fairtrade or the Forest Stewardship Council. Once committed, organizations can find non-compliance expensive in terms of reputation and market position.

A spotlight on pharmaceuticals

The European Federation of Pharmaceutical Industries and Associations (EFPIA) has recognized that interactions between the industry and healthcare professionals can create potential conflicts of interest. It has introduced a 'Code on Disclosure of Transfers of Value from Pharmaceutical Companies to Healthcare Professionals and Healthcare Organizations' that sets out minimum standards to be adhered to by all 33 EFPIA member associations, which are also required to incorporate the disclosure code into their national codes.

For pharmaceutical businesses, key compliance questions nowadays include:

- What payments or transfers of values to healthcare professionals or healthcare organizations is your organization involved in, and how do you capture and report them?
- Are you aware of transparency requirements for each jurisdiction in which you operate?
- How are you raising awareness of policies and procedures within your organization?
- How are you monitoring and anticipating the evolving regulatory landscape?

4. Transparency through publications

Sustainability reports and information in annual reports further enhance commitments and transparency on performance. Reporting on key sustainability topics is now standard in most industries. The KPMG Survey of Corporate Responsibility Reporting 2015 shows that 74 of the 100 largest companies in Switzerland report on sustainability issues. The majority of these apply the Global Reporting Initiative's (GRI) Reporting Guidelines, which include several indicators that relate to compliance. Many companies – including in the pharmaceutical industry, for example – report on the number of non-compliance incidents with regulations and voluntary codes concerning marketing and advertising.

The EU Directive on Non-Financial Reporting is expected to result in around 6,000 of Europe's largest companies reporting on environmental, social, human rights, employee, anti-bribery and anti-corruption matters. Corporate responsibility reporting has become de facto legislated even where it is not yet officially regulated.

Greater transparency leads to greater compliance risks

In a self-perpetuating cycle, companies that claim high sustainability standards will be held to them by stakeholders – especially where products are promoted partly on the basis of sustainable attributes. If the company is found to be failing, the response from investors and customers can be swift and damning.

Those that are required by law to ensure their products comply with environmental standards are especially susceptible to adverse publicity and even investigation by relevant authorities. False sustainability claims can give rise to potentially severe publicity. Witness recent high profile cases of non-compliant emissions testing in the automotive industry.

Integrating sustainability and compliance

As the definition of sustainability continues to widen, it is becoming an increasingly central concern of the compliance function. It is imperative for compliance officers to tackle the subject head on, setting up suitable goals and policies to ensure the organization and its employees act appropriately.

Sustainability practices across the organization and the supply chain are expanding the compliance officer's remit to outside their own organization

This gives rise to a whole new raft of internal and external monitoring requirements. Compliance functions are being drawn further into the world of sustainability. How long before sustainability forms part of a compliance officer's job description?

Sustainability and compliance – A natural match?

Almost all major compliance violations stem from human behavior. As stakeholder scrutiny of businesses conduct intensifies, are you confident that you can adequately identify, manage, mitigate and report on conduct risks? Peter Herrmann, Group Compliance Officer at Actelion, shares his insights into the alignment between compliance and sustainability.

Peter Herrmann
Group Compliance Officer
at Actelion Pharmaceuticals Ltd

KPMG: Sustainability falls within your remit as Actelion's compliance officer. What is the reasoning behind it being a responsibility of the compliance function?
Peter Herrmann: There was no question about it, as compliance and sustainability are a natural match for us. It is clear to us that if we are not compliant, we are not sustainable. Working in the highly regulated pharmaceutical environment, compliance is a material topic for us. This was also confirmed by the materiality analysis we performed for our first corporate sustainability report.

Where do you see the greatest overlap between sustainability and compliance?
Stakeholder expectations for both topics have increased substantially in recent years. This is partially due to much higher levels of transparency resulting from a dramatic increase in the speed of, and access to, information. Local issues can become global issues within moments.

Stakeholder expectations have also changed - the younger generation in particular is much more sensitive to these topics and has growing expectations. We therefore need to develop a company culture where employees understand there is zero tolerance and they abide by all relevant codes and policies. Such a culture can of course only develop with the right 'tone at the top'. This holds true for sustainability as well as other compliance topics.

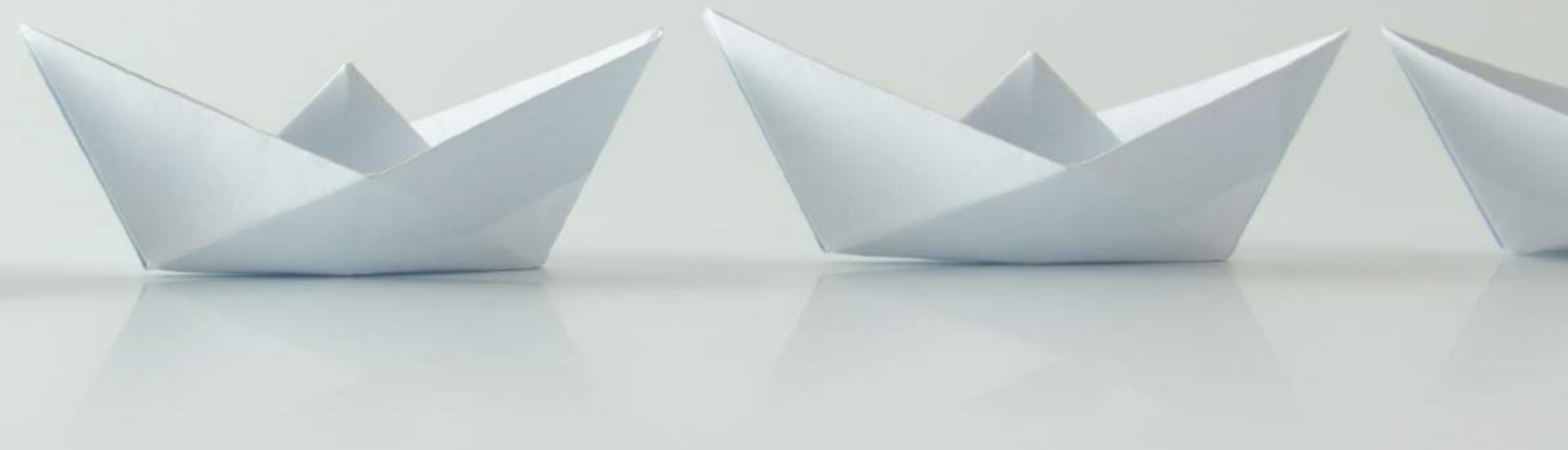
Which sustainability topics are on your radar in general and for Actelion in particular?
For Actelion in particular, we have recently seen an increase in requests from stakeholders with regard to sustainability governance, requiring board-level oversight of related topics. In addition to increased transparency requirements across our business from research to sales, we see the issue of human rights becoming more prominent, as well of course as environmental issues such as CO2 emissions.

Which sustainability-related developments have particularly challenged you as a compliance officer and how have you responded?
It is the transparency initiatives that have had a substantial impact on my and my team's workload. An example of this is the disclosure of payments to physicians, disclosure of clinical trial data and sustainability reporting as a whole. There has been a clear cultural change in the direction of increased transparency, meaning that while for younger generations transparency is 'the new normal', for older generations it can be a struggle to make all this information public. We at Actelion use various means to meet these growing expectations and requirements for transparency. We have introduced a new code of conduct, specific employee training and, last but not least, published our first sustainability report in accordance with the Global Reporting Initiative's reporting standards.

Looking ahead, what do you see to be the biggest challenges?
Values vary across cultures and geographies. I believe that ensuring ethical business standards are respected and applied globally, thereby leveling the playing field, is a major challenge. This needs to be a collaborative effort between industry, politicians and regulators worldwide.

Unacceptable conduct: Assessing and managing the risks

Almost all major compliance violations stem from human behavior. As stakeholder scrutiny of businesses conduct intensifies, are you confident that you can adequately identify, manage, mitigate and report on conduct risks?



Human behavior is such a significant source of compliance risk that financial regulators have declared conduct risk one of the highest regulatory priorities. As enforcement activity is stepped up and stakeholders express growing intolerance of poor corporate attitudes, firms are paying dearly for employees' misconduct. But what precisely is conduct risk and how can it be managed effectively?

The lack of a universal definition of conduct risk can cause confusion; for example, 81 percent of financial services firms globally are unclear about what it is and how to deal with it.[1] Yet, conduct risk can be generally described as closely relating to the corporate culture, whereby individuals' poor attitudes and behaviors cause designed systems and controls to fail.

Taking up the challenge: Assessing and managing the risks

The complexity of human nature makes conduct and associated risks difficult to influence through standard measures or a framework of procedures and policies. However, the following steps can guide your conduct risk management efforts:

[1] *Thomson Reuters, ACCELUS; CONDUCT RISK REPORT 2014/15, p. 3.*

Step 1 - Understand conduct risk

Determine a definition of conduct risk that is unique to your organization, taking into account its business model, organizational structure and existing systems and controls. Put simply: "We know there is a risk of people doing the wrong things but what does this mean for our company?"

Step 2 - Assign ownership and develop governance structures

The regulatory focus on conduct risk will increase senior management's personal liability. Organizations where the board does not – or is perceived not to – own conduct risk are likely to be vulnerable to additional regulatory scrutiny. It is therefore critical to determine who is accountable for conduct risk oversight, implementation and monitoring; how conduct risks interact with other risks; and how the organization ensures the effective operation and integration of risk management frameworks. Most cases will involve the compliance function taking on this task for, and reporting to, top management.

Step 3 - Undertake an effective risk assessment

Adequate assessment of potential conduct risks is vital. The challenge is to decide against which criteria conduct risk is being assessed and what is the risk appetite for qualitative, human behavior-based risks. The effectiveness of systems and controls may be jeopardized if behavioral elements are not properly addressed and if risks are not reviewed on a regular basis. Understanding the potential behavioral risks and implications enables a strategy to be developed and accountability to be assigned in line with the organization's risk appetite.

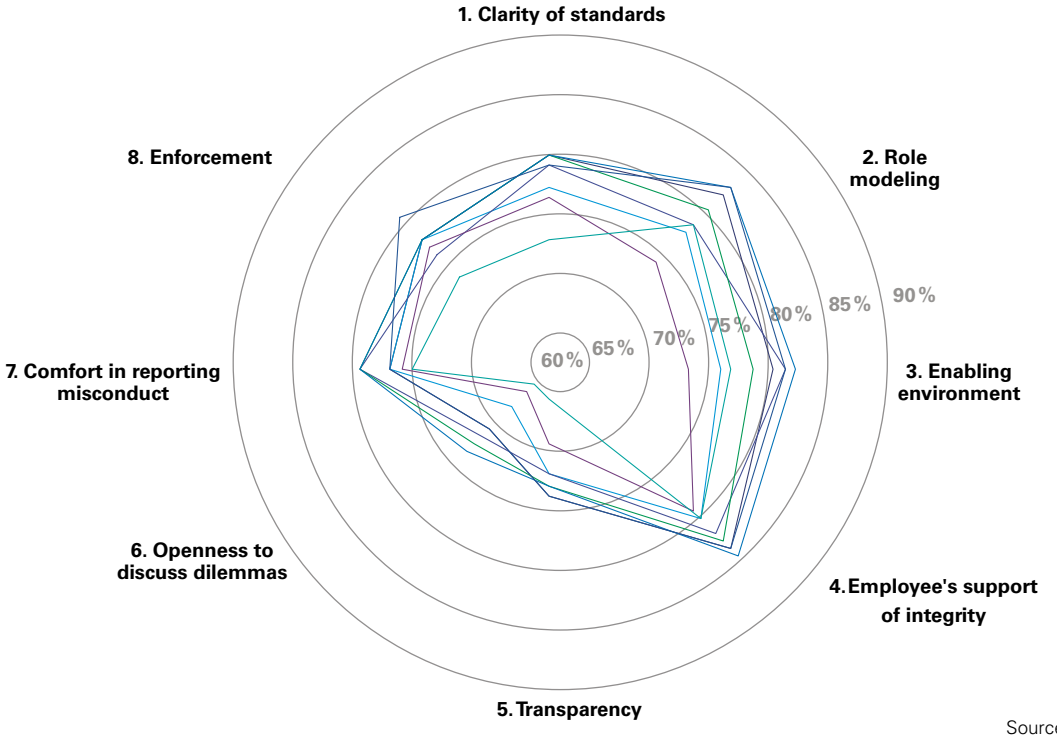
Step 4 - Define appropriate management information and reporting

Robust metrics are necessary to measure conduct risks and the effectiveness of actions taken to mitigate them. Management information should therefore include quantitative metrics, with results fed into key decisions for the approval of improvements. Defining quantitative metrics to measure culture remains a challenge, however, as does defining forward-looking management information indicators to identify conduct risks at an early stage.

Moving forward: Defining quantitative data for conduct and culture

Culture is not a one-dimensional concept. Eight elements form the basis of an organization's culture and are helpful for developing the quantitative management information indicators needed for conduct risk management.

Quantitative data on organizational culture for internal and external benchmarking



Source: KPMG Switzerland

1. **Clarity of standards:** The degree to which policies and procedures are accurate, specific to the organization and complete, so employees understand what is expected in terms of ethical conduct.
   Regulators have highlighted the need to document how conduct risk is managed. This includes the definition of what the desired behavior entails. The result should be clarity over policies, procedures, systems and controls, including clarity among employees regarding what the organization stands for and what is considered (in)appropriate behavior.

   Example of management information: Survey or audit data on employees' awareness of specific compliance rules.

2. **Role modeling ("tone from the top"):** The degree to which the board and management set a good example for the organization and its employees.
   Regulators expect boards to lead by example, including communicating and demonstrating proper behavior. Senior management must send the right message in terms of culture and governance.

   Example of management information: Approval scores of the board and top management in employee satisfaction surveys compared to the benchmark.

3. **Enabling environment:** The degree to which an organization's business targets correspond to predetermined values and principles.
   Do employees have the appropriate time and resources to reach their business targets while also fulfilling their compliance responsibilities?

   Example of management information: Review of compliance incidents to see if the root causes can be linked to time or budget constraints.

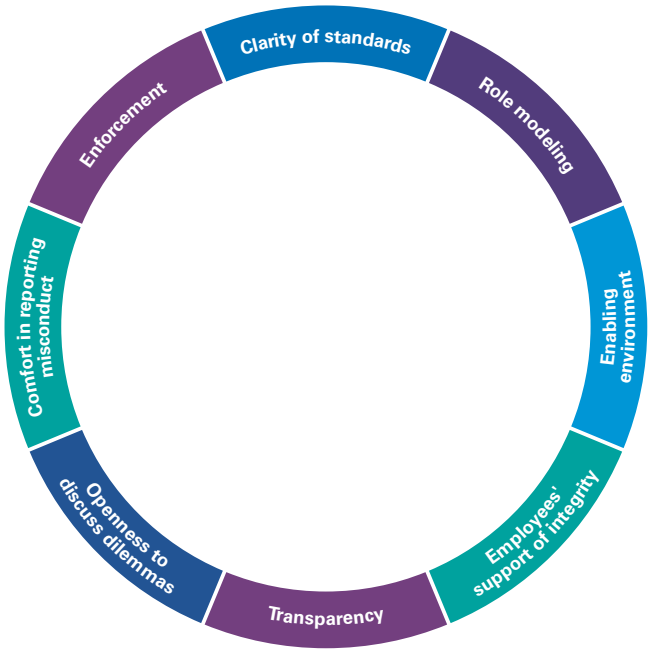
4. **Employees' support of integrity:** The degree to which employees personally endorse integrity and desired behavior within the organization.
   Measuring employees' motivation for doing the right thing and upholding compliance standards is essential to be able to make any claim about the organization's culture.

   Example of management information: Employee satisfaction survey, or a dedicated 'integrity culture' survey could provide further insights.

5. **Transparency:** The degree to which conduct and its implications are visible within the organization.
   If bad or good conduct is visible in the organization it might spark copycat behavior. A high level of transparency makes it more likely to change undesirable behavior.

As regulators set clear expectations, they will continue to scrutinize corporate cultures, conduct risk management and individuals' accountability and liability – ultimately following this up with enforcement actions.

The eight elements of organizational culture



Source: KPMG Switzerland

Example of management information: Employee survey asking about compliance violations, which could be simultaneously used as a conduct risk assessment.

6. **Openness to discuss dilemmas:** The degree to which employees feel they can openly discuss ethical dilemmas within the organization.
Employees should feel confident to raise questions and seek support in difficult situations. Any fear of talking openly about ethical dilemmas will adversely affect culture.

   Example of management information: Specific questions in an employee survey.

7. **Comfort in reporting misconduct:** The degree to which employees feel comfortable raising concerns over potential misconduct without fear of retaliation.
An organization should provide dedicated reporting channels that allow confidential or even anonymous communication outside of the traditional hierarchy with supervisors or specific functions. Most organizations have a formal reporting structure, but it is a question of how low is the threshold for employees to actually report a concern. Encouraging them to speak up requires more than the mere existence of a reporting mechanism.

   Example of management information: Compare the number of reports per 1,000 employees with a country or industry benchmark. Also use the employee survey to assess trust in the existing reporting procedures.

8. **Enforcement:** The degree to which irresponsible, unethical or illegal conduct is sanctioned and positive behavior rewarded.
Employees need to assume responsibility for their behavior and must consistently be held accountable for their actions. This includes a fair enforcement process at all levels, including adequate corrective actions in case of misconduct.
The cultural element of enforcement relates to how much initiative is taken to apply this.

   Example of management information: Review data on enforcement actions and compare these with the number of reported compliance violations.

Compliance – A priority for life sciences

As the level of fines and settlements increases, and as authorities show a growing willingness to pursue both corporations and their senior executives, does every member of your senior management team treat the avoidance of compliance failures as a top agenda item?

Not a week goes by without a drug or medical device company hitting the headlines for alleged infringement of the law. Only recently, the public learned that a US biopharmaceutical company faced a USD 4 million fine for fraud. In addition, the US SEC sought to ban three of its former executives from leadership positions in any company going forward after they allegedly misled investors regarding the safety of a key cancer drug. Compliance is becoming an increasingly personal matter.

Cases such as this demonstrate clearly how authorities – particularly in the US – are actively enforcing laws to the extent that they do not hesitate to punish individuals as well as issuing severe penalties to the company. This is true not only in fraud cases but also for bribery or where potential infringements of anti-trust or data protection provisions are identified.

It comes as no surprise that the life sciences sector is under particular scrutiny. Pharmaceuticals is a multi-billion dollar industry where product safety and pricing profoundly affect the end user. Its businesses operate in a highly regulated market dealing with patients and patient health, handling highly sensitive patient information that is governed by data protection legislation in all major jurisdictions. Scrutiny is enhanced by the fact that government health programs are the main buyers of pharmaceuticals and medical devices.

Risks at home and abroad

We often hear about companies being prosecuted by the US and UK authorities, yet penalties in Switzerland can also be severe. Art. 102 Swiss Criminal Code (SCC) states that if a felony is committed in a corporation and if it is not possible to attribute this act to any specific natural person due to an inadequate organization, then the felony is attributed to the corporation – in which case such corporation is liable to a fine not exceeding CHF 5 million. This is what happened to Alstom some years ago. The company was handed a fine of CHF 2.5 million and had to pay compensation of CHF 36.4 million for violating these provisions in a bribery case. The prosecutor stated in his reasoning that said company had failed to take necessary and reasonable organizational measures to prevent bribery of foreign public officials.

The impact on life sciences

Prosecution can result in damage to both profits and reputations. In a nutshell, shortcomings in a compliance organization can heavily impact a company's financials. In addition to hefty fines and settlements (which have increased considerably in recent years), costs incurred in connection with the defense of such allegations have reached an unprecedented scale. And this does not even include potential liability claims by users of defective products, which may arise from a failure of internal compliance organizations to oversee the integrity of research, marketing and manufacturing. On top of the severe financial penalties, the reputation of both the company and senior managers can suffer when patients and shareholders become aware of alleged corporate wrongdoing.

The duty of the board of directors is broad

It includes responsibility for ensuring that compliance operates effectively in the organization, and that any breaches of laws or standards are identified and dealt with swiftly. Failure to do so can have severe repercussions, and not only for the business itself. Senior management take note: in assessing where responsibility lies, enforcement authorities are increasingly dissatisfied with holding only the corporate entity to account.

A question of responsibility

All this makes it imperative for any life sciences corporation and its senior executives to take compliance and ethics seriously. Management must demonstrate genuine efforts to establish an effective compliance program to mitigate risks related to bribery, anti-trust and data protection. Senior managers bear the ultimate responsibility for this task in Switzerland as in other parts of the world. Determining a corporation's organization is a non-transferable and inalienable duty of the board of directors. This includes implementing a compliance program that is in accordance with legislation as well as recognized industry standards. Further, the compliance program must be appropriate to the size, complexity and risk profile of the corporation.

The board of directors must implement the respective regulations – such as a code of conduct or a code of ethics – enforcing these throughout the group and even along the supply chain. There is a further obligation to review the compliance organization regularly, applying established processes and putting in place regular controls and severe consequences if infringements are detected. In this regard, ensuring the timely reporting of major incidents taking place in lower management functions is central.

“Clarity on” publications

The “Clarity on” series from KPMG Switzerland offers a wide range of studies, analysis and technical articles. All publications are available in print and online. For more information, please email **kpmgpublications@kpmg.com**

Latest issues

Clarity on
Cyber Security

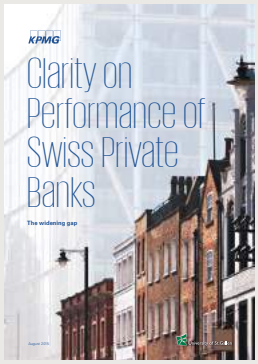
Clarity on
Entrepreneurs

Clarity on
Swiss Taxes

Clarity on
Commodities Trading

Clarity on
Mergers & Acquisitions

Clarity on
Tax Function Transformation



Clarity on
Performance of Swiss Private Banks

Clarity on
Data & Analytics

Clarity on
kpmg.ch/clarity-on

KPMG Knowledge App

Get instant access to the expertise of KPMG’s specialists with the “Knowledge app” for iPad – now even more compact and customizable to your specific requirements.

Download on the App Store

Google play

KPMG Apps
kpmg.ch/apps

IMPRINT AND CONTACTS

For further information on
Clarity on Compliance
please contact:

Anne van Heerden
Partner, Head of Advisory
+41 58 249 28 61
annevanheerden@kpmg.com

Philippe Fleury
Head of Forensic Switzerland
+41 58 249 37 53
pfleury@kpmg.com

Solveig Rufenacht
Director, Head of Compliance
+41 58 249 36 54
srufenacht@kpmg.com

Jörg Kilchmann
Partner, Attorney-at-law, Legal
+41 58 249 35 73
jkilchmann@kpmg.com

Kathleen Tench
Director, Head of Life Sciences Compliance
+41 58 249 35 96
kathleentench@kpmg.com

Isabelle Hirs-Schaller
Manager, Head Climate Change & Sustainability
+41 58 249 54 74
ihirs@kpmg.com

Gerben Schreurs
Partner, Forensic
+41 58 249 48 29
gschreurs1@kpmg.com

Jeffrey Bholasing
Manager, Head of Data Protection & Governance
+41 58 249 42 88
jeffreybholasing@kpmg.com

Marc Bieri
Director, Head of Insider Threat Management
+41 58 249 64 05
marcbieri@kpmg.com

Luka Zupan
Partner, Head of Internal Audit, Risk & Compliance
+41 58 249 36 61
lzupan@kpmg.com

Publisher
KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich
+41 58 249 31 31
kpmgpublications@kpmg.ch

KPMG editorial team support
Cédric Biedermann
Martijn de Kiewit
Aleksandra Goes
Theresa Mayer
Felix Schraner
Marvin Schilling
Fabienne Sonderegger

External writer
Stuart Garforth, outhouse communication

Concept and design
Konkret, Martin Bühlmann
KPMG, Stephan Erdmann
KPMG, Irene Hug

Print
GfK PrintCenter, Hergiswil

Pictures
Shutterstock

Clarity on Compliance
kpmg.ch/compliance