SIGNAVIO

7 Step Guide to Risk & Compliance

Safeguard the future of your organization and make risk and compliance a top priority

Executive **Summary**

In today's volatile business landscape, one thing that remains a constant is the need for robust and proactive risk and compliance management. Whereas in the past, compliance may have been viewed as an unfortunate extra cost, it has become a crucial investment for all organizations to meet the demands created by the pace of global regulatory change, by new market entrants, and consumers themselves.

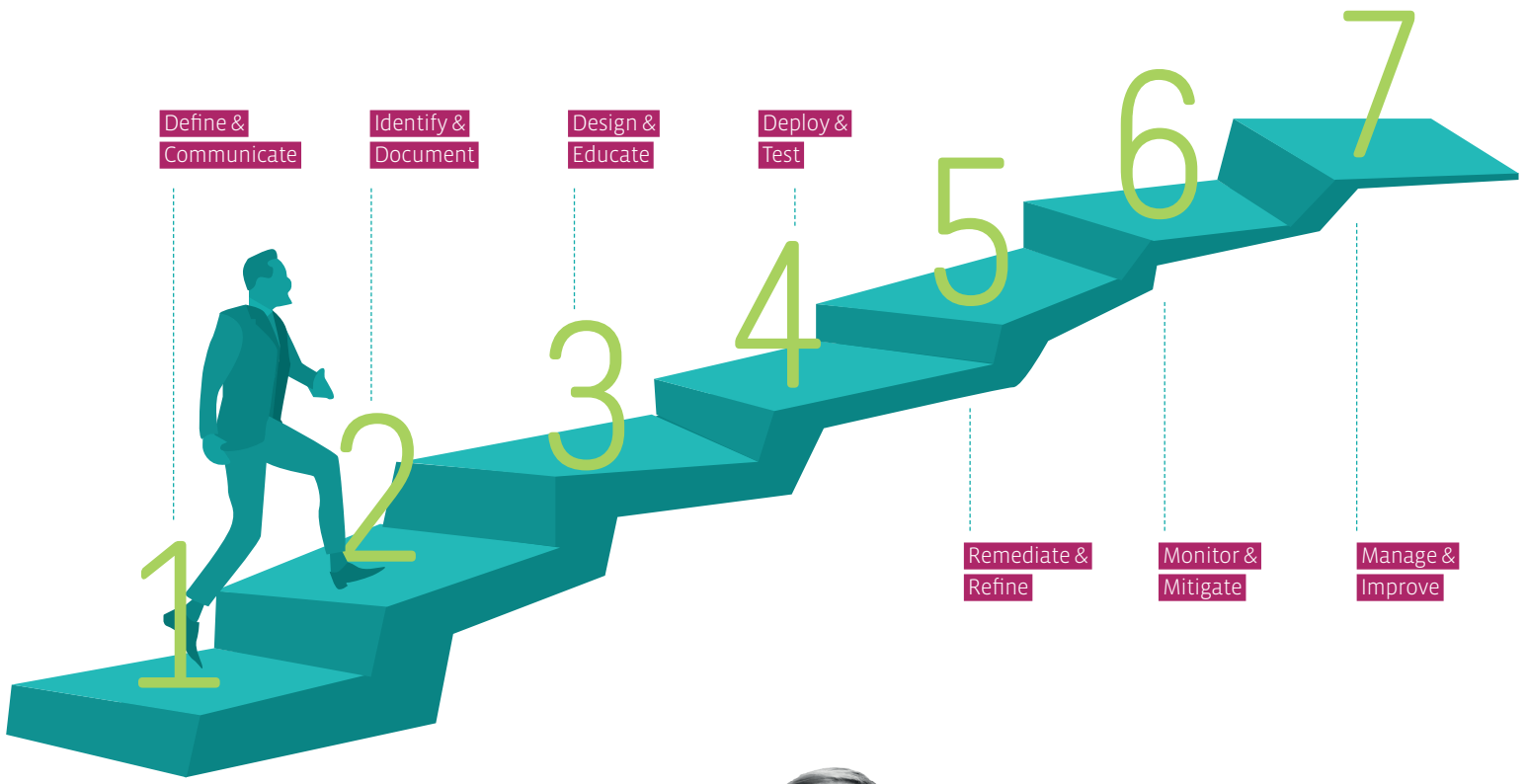
Over a third of organizations spend at least an entire day per week tracking and analyzing regulatory change and two thirds of organizations expect regulators to publish even more regulatory information in the coming year, according to Thomson Reuters. Therefore, an increase in the amount of resources for processing compliance policies and procedures to manage risk is also to be expected. In conjunction with managing internal risks as well as the recent trend in digital disruptors, new technologies and increased global competition, the need for organizations to implement strong risk and compliance frameworks has never been so crucial. Risk management and compliance have always been important, and are now a critical part of operational and strategic decision making, a worthy investment at times of strict budget planning and a trend that will only increase with time.

Organizations spend considerable time and effort attempting to stay on top of the tracking and reporting required to achieve regulatory compliance. Traditionally focused on financial service and utility companies, regulations are now applicable to all market sectors. Take as an example the fines being levied for noncompliance related to data protection and the use of personal data.

However not all risk is based on regulatory stipulations; many of the risks faced by organizations go far beyond these requirements. In a highly competitive marketplace, safeguarding against reputational risk is an essential element of success. And every organization is faced with operational risks such as appropriate staffing and resource distribution. Not to mention financial risks, which include any number of issues from not processing orders correctly to delays in invoicing to employee reimbursements. Operational, financial, and reputational risks will have far reaching consequences and potentially an even broader scope than noncompliance.

In order to meet and address these challenges, organizations need to find a better way. Not just to deal with discrete regulations and to control risk, but to also to manage the interdepencies between them. Managing risk and compliance is not simply about managing the regulations and risks themselves, but also ensuring that all employees are operating in accordance with your risk framework, and that work is being completed in a compliant way. Achieving this means ensuring employees have access to accurate, up-to-date procedural information. The translation of regulations into work practices has another major organizational benefit – it provides the audit and documentation trail needed to demonstrate compliance with regulations.

Introducing **the 7 Steps**



The following 7 step model suggests ways in which organizations can maximize their business returns from investing in compliance, and about the ways in which technology can empower compliance professionals with the correct tools to assess impacts of regulations on the business and operating model, and to communicate information effectively.

To ensure that compliance becomes a company-wide endeavour, safeguarding your organization from potential reputational damage and other unwanted risks, harnessing the potential and capacity of your whole team is imperative to success. The following steps will guide you in these efforts. We recommend that for each step you consider the suggested outcomes, review the suggested actions, and then ask what mechanisms you already have which could be repurposed or reinvigorated to undertake this.

Dr. Gero Decker,
Co-Founder
& CEO

The pace, complexity, and impact of change is affecting every vertical and company, especially when it comes to new regulatory requirements. Incorporating these new regulations directly into your processes will safeguard the future of your organization and make risk and compliance a top priority.

Define & Communicate

This first step is about creating a structure to allow for agile and effective management of regulations. Setting your organization up with "good bones" in the form of a well designed regulatory system is key. This system must meet the requirements of the particular industry of operation, as well as allow for flexibility, transparency, and scalability to future proof your organization, and ensure it is able to adapt to changing regulatory and audit requirements as they happen. In other words, your compliance system must be set up to be and remain compliant itself.

When designing/defining this type of framework, it is essential to anticipate and cater for the audit requirements of the current environment, as well as those in the future. Many industries are required to keep detailed documentation showing exactly how industry regulations are translated into the company's day-to-day operational workings, i.e. the business processes. They may also be required to demonstrate and prove exactly how, and when, communications to staff regarding how to work compliantly were done, and may even require formal acknowledgement and record of this. The volume and frequency of changes makes the task of assessing the required impact of a regulation on business operations a time consuming task. Fortunately, compliance managers are no longer forced to rely on manual workflows and untraceable email communication in order to communicate and keep track of changes. Organizations can work to build single sources of knowledge within their intranets that allow tham to update workers about changes quickly and easily, reducing the risk of non-compliant activities.

Ineffective company cultures are a major source of risk for organizations . Organizational culture will affect risk taking behavior, both negatively and positively. It is the ultimate responsibility of the Chief Compliance and Risk Officers to ensure the rhetoric from the top filters down to promote desirable behaviour in terms of policy compliance, risk prevention, whistleblowing and accountability – and the risk and compliance structure must support this. This is why integrating a framework based on legal/standardized requirements into a workflow tool is crucial as a means of keeping everyone involved in your risk-prone processes up-to-date, and of communicating to stakeholders what the necessary defence controls are.

Identify & Document

Risk identification is the foundation of risk management, as you cannot manage a risk you don't know about. To ensure this process is thorough and effective, it is essential to involve a range of both Subject Matter Experts, and stakeholders – these are the people actually carrying out the work. These people hold the keys to both identifying opportunities to improve the business process overall, as well as the ability to offer insights into why work may be completed incorrectly or non-compliantly. For example, if certain steps required for compliance conflict with activities related to KPIs and bonuses, you might find higher instances of non-compliant behavior. You might find higher instances of non-compliant behavior.

On a broader level, strategic, operational, financial and reputational risks must also all be defined and documented (with clear linkages between strategic, tactical, and operational processes and associated risks). This means identifying, prioritizing and assigning accountability for managing any risk significantly impacting the organization's ability to achieve its strategic objectives. On a more specific compliance level, it means identifying, prioritizing and assigning accountability for managing compliance in regard to particular laws and regulations. Ensuring the right people are involved, consulted, and their feedback factored into the compliance system is essential. Doing this means setting up the basis for communication and collaboration across the whole system – from meeting the needs of Execs, to those of the employees executing on transactional tasks for customers.

As both of these broader and more specific risks are constantly open to change, it is important that you define a compliance framework that is capable of protecting your organization from risk. This should include not only simply staying informed about the latest regulatory updates, a huge job in itself, but also incorporating them into business processes and activities, and training and educating your team accordingly to ensure a strong compliance culture.

Identification, documentation, and prioritization of risks in collaboration with Subject Matter Experts and stakeholders.

Design & Educate

Once the initial work to identify, prioritize, and get input on risks in your organization has been completed, the next step is to define how the organization will assess and control each risk, and create the supporting process and test structure to accompany this. Again, this step should make good use of iterative design of the control system, and the deep knowledge your people already have regarding the reality of how work gets done. This means that the structure of controls created to manage the risks identified during the identification stage must be tightly bound to the ways in which your real employees complete real work. It is also a rallying cry ensuring collaboration is designed into the system.

Designing collaboration into your compliance system is indispensable. Rules, although necessary and important to define, can also in some cases have the opposite effect of that desired, by inhibiting independent thought and discussion, leading many organizations to overlook or misread ambiguous threats. According to Harvard Business Review, rather than mitigating risk, firms actually incubate risk as they learn to tolerate apparently minor failures and defects and treat early warning signals as false alarms rather than alerts to imminent danger. Creating and nurturing a culture of transparency, questioning, and open communication across the org chart is essential not just for productivity and performance, but also compliance and risk mitigation.

Deploy & Test

Once the design of exactly how risk and compliance will be measured has been completed, it is time to automate the actual workings of the system as much as possible. This has obvious benefits, with many areas of the globe enduring a serious shortage of compliance professionals. Automation allows you to do more with less.

Being able to respond in a timely way to incidents is imperative to mitigating risks and compliance breaches. Ensuring effective, reactive action and defining responsibilities, thresholds and deadlines is crucial to resolving risk issues before they blow up, costing far more money (and potentially far more reputational damage) to fix. Potential risk incidents within an organization are often quite similar, or follow a similar structure and response pattern, defining incident models will ensure a standardized and comprehensive response process. To ensure that your framework is fire proof, it is recommendable that you implement workflow processes to manage risks as well as implementing controls and test against a variety of scenarios.

In order to effectively respond to incidents and to ensure that reported breaches are escalated correctly, an incident model that streamlines the process and reduces risk should be defined. Incident handling routines and escalation routing should include defining the sequence of steps, the individuals responsible, the precautions to be taken prior to resolving the incident, timescales for resolution, escalation procedures, and evidence preservation.

Completing this work manually is possible, but consumes a huge amount of resources and time - and with the constant deluge of new regulations requiring assessment, can be tricky to provide for. Many organizations are now beginning to use workflow solutions to take the heavy lifting out of risk system deployment and management, leaving those responsible more time to dedicate to higher value work.

Remediate & Refine

Detecting compliance deviations based on your previously defined and documented framework will allow you to compare “as-required” processes with “as-implemented” processes more easily. At this point your current state will still require some testing in order for you to recognize gaps and see where certain processes are failing to adequately address and mitigate risks. This is where identifying compliance issues across your implemented compliance framework, processes and procedures comes in. As with the last step, this can be made much more efficient with technology which allows you to use the data your business systems are already generating, in order to alert risk managers to breaches and issues before they become a huge and expensive issue.

An efficient deviation handling system should also implement a mechanism to discriminate incidents of compliance deviation based on their relevance and to objectively categorize them. Figuring out whether or not a compliance deviation will result in damage to your company, your product, or your reputation, and whether or not it will result in financial or legal repercussions is an important part of the detection process, allowing you to then manage and correctly escalate incidents and to ultimately identify any potential for “process hardening.” In this case you may want to consider adding extra steps to existing processes, making compliance deviation less likely and adding an extra fire-wall to ensure that end users do not accidentally act in a non-compliant way due to lack of documentation or discrepancies in your compliance framework.

Monitor & Mitigate

Once you have set the wheels in motion and your framework is in place, it is of equal strategic importance that you continue to monitor and report on compliance related behaviour, while mitigating non-compliance and identified risks. Responding to incidents consistently and in a timely fashion, whilst implementing & enforcing routing logic should go hand-in-hand with the continuous reassessment of risks.

The benefit in having your compliance framework mapped out and documented in workflows and processes is that you can collect data over time to ensure that nothing goes undocumented, and ensure evidence related to any incident is kept on record. This is not only often a legal requirement when it comes to auditing and external checks, but also useful to ensure that your compliance and risk related processes are operating at an optimum level and that ultimately, you stay well ahead of the competition.

Monitor and report continual compliance, while mitigating non-compliance and identified risks.

Continuously monitor and measure performance, identify and act on areas for improvement.

Manage & Improve

Within a holistic and ongoing risk and compliance management system is a consistent focus on seeking and acting upon ideas to improve. Monitoring and reporting continual compliance allows you to have an overview of where your organization currently stands in terms of desirable behaviour and what the current state of compliance is, meaning you can start working on the gap between your current and future state. It also allows you to reward and promote compliant behaviour and improvements. Mitigating non-compliance and identified risks is also a continual task, as the regulatory landscape is constantly in flux.

As part of this holistic approach, ensuring that HR policies avoid mutual accountability and promote open communication, appropriate escalation and whistleblowing reporting is a crucial foundation. Personal accountability as well as the involvement of suppliers, investors, clients and regulators in creating and developing action plans will aid in the promotion of a transparent compliance culture.

Conclusion

These steps are of course not the definitive or final word on how to undertake an organizational transformation. They are however based on expert experience and lessons learned over the course of decades of compliance system design. They are intended to provide you with the mindset and insights to steer your organization through the complex, often messy, but ultimately rewarding process of transformation. We encourage you to adapt and augment the steps to match your organizational context, while taking note of the underlying themes of communication, inclusion, collaboration, and smart monitoring.

Effectively translating strategy into action is the cornerstone of transformation, we hope this guide will support you in creating positive behaviors and mitigating threats you will encounter as your organization embarks on this journey by providing insights from others who have gone before.

If you want to learn more about how Signavio can assist you with compliance, sign up for one of our free webinars or come meet us at a Lunch and Learn event in a city near you. Or, if you're ready, take our products for a test drive with a free personalized demo.

www.signavio.com