WHITEPAPER

Bridging the gap between external regulations and internal guidelines

RegTech's role in managing regulatory change

"Regulatory Change Management" will be a familiar phenomenon for anyone working in financial services or the healthcare sectors. As part of their business as usual compliance activities, firms in these industries have to closely monitor changes to legal regulations and assess their significance for the organization before translating them into internal processes and workflows. At the same time, the topic of regulatory change management has been quietly growing in importance amongst other highly regulated sectors like manufacturing, energy and services as regulators review and enhance regulations in response to new and emerging risks.

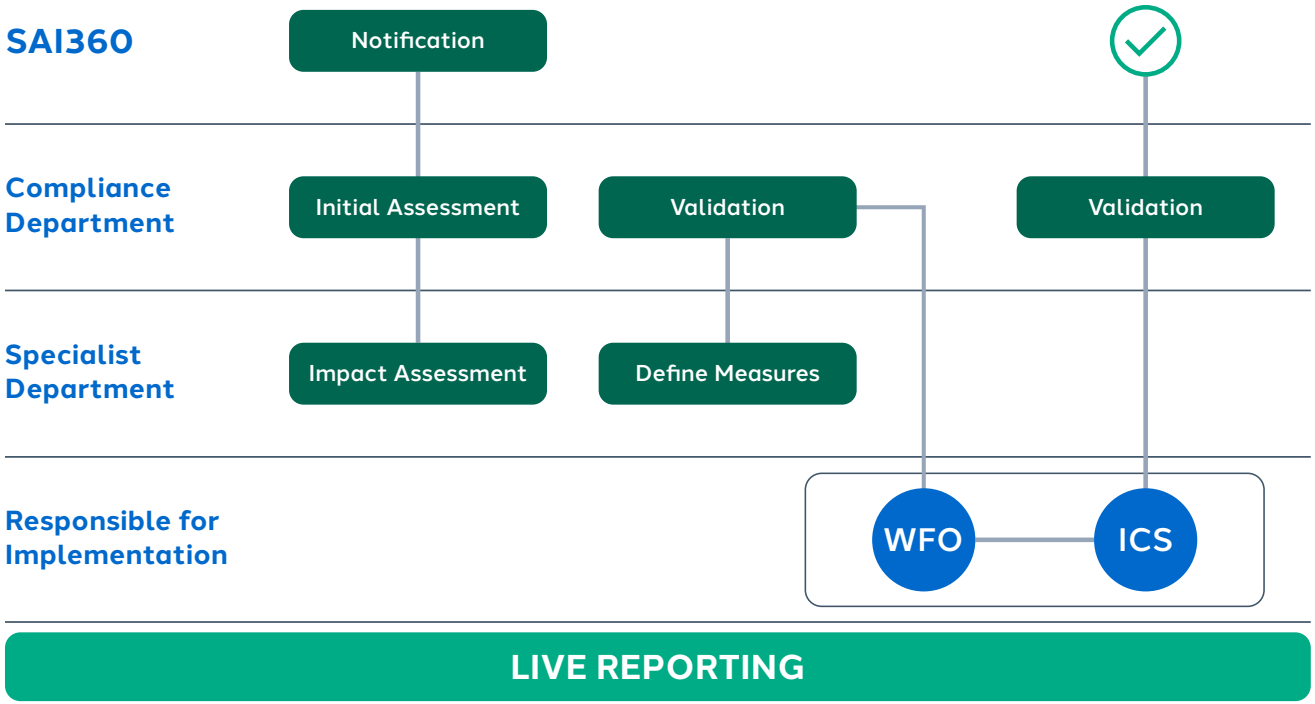
The ultimate challenge for managers is to be able to keep track of myriad regulations and to systematically incorporate these developments into their organization's policy and process frameworks. But it is not only the sheer volume of regulatory requirements that presents a considerable challenge, the scope and complexity of these regulations is also increasing, adding to the difficulty firms have in interpreting rules changes. Given this context, a growing number of executive leaders are acknowledging that effective regulatory change management cannot be achieved without the help of technology. In addition, regulatory and supervisory bodies are becoming less and less tolerant of the use of manual processes for managing regulatory change such as spreadsheets and e-mail.

Firms must ensure they are fully compliant with changing regulations across all business divisions and managers must implement technology-enabled, audit-proof processes to ensure they are best placed to avoid fines and reputational damage resulting from rule violations. So, where should firms start with this seemingly daunting task?

The first step in the process is to ensure that all external regulations relevant to the company are known and recorded in a compliance inventory. Secondly, compliance managers need to assess the implications of changes to these rules and amend existing or create new internal policy guidelines.

SAI360
RISK FROM EVERY ANGLE

And finally, firms must define the workflows required to adhere to these regulations in such a way that their implementation can be monitored and audited throughout. At a high level, this appears relatively straight forward, but there are specific challenges associated with each of these steps.



Step 1

Complete coverage of external regulations

There are tens, if not hundreds of available avenues through which organizations can obtain regulatory information. Whereas direct publications, proposals and press releases from regulators might be the most common sources, newsletters from consultancies, law firms and sometimes even social media can also provide valuable content. It is not just final rules that firms need to be aware of, however. Draft regulations need to be reviewed and understood in advance so their impacts can be assessed ahead of implementation deadlines. In some cases, draft rules may also be included in economic, operational or certification audits.

For organizations with operations across multiple jurisdictions, there is an additional layer of complexity. These firms need to track and understand the laws and regulatory changes in each jurisdiction in which they have a presence which further increases the compliance challenge.

To give some idea of the sheer volume of regulatory data that needs to be processed, in 2020 there was an average of 217 regulatory updates posted per day across the globe, which equates to circa 300,000,000 pages of regulatory documents.[1]

Firms also need to be aware of all the sources that may contain information on the external regulations which are relevant to them, which may include:

- National laws
- National regulations
- National standards
- Other publications of national states
- EU Regulations
- EU Directives
- EU Guidelines
- International standards
- Publications from international organizations
- General product specifications
- Implementation guidelines
- Industry-specific documents and guidelines from foreign authorities, e.g. FDA

The greatest challenge for managers therefore is to collate all of the relevant regulatory sources in one easily accessible place, ensure that nothing had been missed and that the information is up to date so that it can then be incorporated into internal guidelines. This is an extremely laborious process which often requires input from multiple employees or external service providers.

There are a growing number of software solutions emerging in the market which can automate this complex, time-consuming and cost- intensive process. These solutions enable regulated firms to manage changes to regulation across the life cycle, from horizon scanning through to impact assessment, implementation and evidencing of compliance with new rules.

Step 2

Assessment of relevance and adapting internal policies

Once a relevant change in an external piece of regulation has been identified, relevant people in the organization need to be notified so they can perform an initial assessment. Typically, this is the job of the compliance officer or in-house counsel. If the change is relevant for the company, an impact assessment is carried out by the departments and/ or regions that are affected by the regulatory change. Depending on the scope and extent of this change, several areas of the company may be involved. These impacted departments are also usually responsible for defining the internal processes and workflows that need to be implemented to remain compliant.

1 "Cost of Compliance Report 2020 and Covid-19 ... - Thomson Reuters." https://corporate.thomsonreuters.com/Cost-of-Compliance-2020

Workflow: Changing a policy

The compliance department validates all the impact assessments, proposed changes and controls from specialist departments and derives an overall assessment with necessary recommendations for action. In some cases, due to their broader perspective on the whole company, the compliance department may disagree with elements of the impact assessments completed by specialist departments which may in turn alter the significance of a particular regulatory change and the subsequent actions.

Once the recommendations for action from the individual departments have been aggregated and validated, they are incorporated into internal guidelines.

Firms should ensure they have a quality assurance or four-eyes check in place prior to the formal approval process and publication. Once approved, the proposed changes to internal guidelines need to be cascaded down to all impacted employees to make them aware of the updates.

To summarize, the workflow involved in changing an internal policy is as follows:

1. Policy Creation (based off of the regulatory changes identified)
2. Four-eyes check or QA process
3. Internal Approval
4. Final Publication

Step 3

Adapting internal processes and implementing new controls

By this point, although external requirements have been incorporated into internal policies, firms still need to carry out the operational steps to ensure that the new requirements are implemented company-wide.

The requirements of the external regulations and the concrete implementation of compliance measures are linked together through a firm's internal control system (ICS). Corporate governance legislation in a number of jurisdictions mandates that companies should have an ICS in place and even without a firm regulatory requirement, internal controls are still a vital part of enterprise risk management. The ICS comprises the whole network of systems and processes that, when implemented, provide reasonable assurance that organizational objectives can be achieved and risks can be effectively managed. The ICS is therefore an integral component of a company-wide risk management system and ensures that corporate risks are mapped, monitored and reduced where necessary in line with the firm's risk appetite.

The ICS is deeply embedded within the company, with controls being directly linked to risks, processes and IT systems. The control measures within the ICS form the basis of controls testing, which is carried out periodically to ensure controls remain effective in managing and mitigating all the types of risk to which the firm is exposed.

The measures and controls agreed in Step 2 are implemented and documented by the responsible people in each department as part of the standard ICS process. This ensures regulatory requirements are implemented in day-to-day operations and can be monitored as a regular part of the ICS reporting process, allocating individual responsibilities and deadlines to the relevant departments.

The integration of measures and controls into the corporate ICS therefore ensures that new or amended regulatory requirements are consistently and systematically incorporated into internal processes, ensuring the organization is compliant at all times.

How software supports the regulatory change management process

Using software to automate the workflows associated with regulatory change management can greatly reduce the amount of administrative work required to remain compliant. The capabilities of these solutions are extremely comprehensive, supporting each step of the process from regulatory change monitoring through to implementation tracking and impact assessments.

Horizon scanning is performed to identify relevant regulatory changes and the system will then automatically notify the relevant personnel via email that they need to review a regulatory alert. These solutions also automate the creation of new policies or the modification of existing documents, storing updated documents centrally so they are accessible to all stakeholders. These documents can be viewed or edited by employees, as long as they have the required access permissions. Policy approvals can also be automated, using rule- based workflows or they can be reviewed manually, in real-time by compliance managers. These solutions also have the ability to integrate with the ICS to enable a holistic view of the implementation of regulatory changes.

Translating external regulations into internal policies and workflows affects a number of distinct organizational processes, such as policy management, risk management and the ICS. It therefore makes sense for these systems to share a common data source which will improve the effectiveness and efficiency of each process. For users, it is also far simpler to only have to sign on to one software tool to perform all their tasks, and this is made easier if all the data is structured according to the same schema.

Regulatory change management solutions also create a full audit trail of the end-to-end process. Each step, from horizon scanning, defining the changes through to implementation of controls is automatically recorded and stored within the system, allowing firms to evidence their activities and provide assurance they have taken all the appropriate actions. Some more sophisticated software solutions also provide data visualizations and dashboards, allowing users a complete picture of the current status of all regulatory changes. By providing a fully automated process, those involved in regulatory change management can ensure they are focusing on the implementation tasks that really matter, rather than organizing multiple spreadsheets and emails to keep track of what is happening.

Interested in learning more about SAI360's Regulatory Change Management solutions?

[Request a demo.]

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360 RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

157650 0424