Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

The Transformation of Next-Level Compliance

An e-Book publication sponsored by M-Files®

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

M-Files®

M-Files enterprise information management solutions (EIM) improve and simplify how businesses manage documents and other information in order to become more productive, more efficient and stay compliant. M-Files eliminates information silos and provides quick and easy access to the right content from any core business system and device. M-Files achieves higher levels of user adoption resulting in faster ROI with a uniquely intuitive approach based on managing information by “what” it is versus “where” it’s stored. With flexible on-premises, cloud and hybrid deployment options, M-Files reduces demands on IT by enabling those closest to the business need to access and control content based on their requirements. Thousands of organizations in over 100 countries use M-Files as a single platform for managing their critical business information, including companies such as SAS, Elekta and EADS.

Inside this e-Book

The 'Shalt Nots' of GRC Implementations

by Joe Mont

In the current business climate—with unprecedented regulatory risk, complexity, and security threats—companies of all sizes rely heavily on governance, risk, and compliance software. In a perfect world, these solutions help an organization transition from manual processes to state-of-the-art controls, and provide insight into a firm's risk profile and compliance needs.

Alas, it is not a perfect world.

There is no shortage of vendors and products. Choosing the wrong one can be disastrous. Just as problematic, however, is pairing a poor implementation strategy with even the best of solutions.

What's at stake? Missteps can lead to employee revolts, cost overruns, delays, and ineffective controls where you can least afford them should regulators come knocking at your door.

We asked GRC experts to weigh in on what the most common implementation mistakes are.

They "boil the ocean." With an approved budget in hand and a GRC implementation plan garnering top-level support, there may be an understandable urge to act quickly and comprehensively to make every dollar count. An overly ambitious approach, however, can prove counter-productive.

"Once they make the decision to invest in technology, they go overboard. They get funding and decide, 'let's do everything,' from risk to compliance automation and incident response," says Torsten George, global marketing executive for GRC software company Agiliance. Bringing too many functionalities online with too broad a user rollout are common mistakes that lead to an unfocused process and plenty of chaos. "That often backfires," he says. "Do it step by step and don't bite off more than you can chew."

They don't fully appreciate their needs. You may think you know what is needed from the new technology, but are those goals realistic?

"When people try to implement or update risk management within the organization, they often believe that the tool should adjust to their existing procedures and the processes that are already in place," George says. "They are not necessarily seeing an opportunity to review their existing processes, evaluate if they are efficient or not, and tailor [the GRC implementation] toward best practices. Try not to be static and think the tool needs to adjust to your procedures."

They take an "ivory tower" approach. "The people tasked with implementing risk management software often keep that responsibility to themselves and don't want to bring anybody in too early," George says. Unilateral decision making can be a crisis in waiting.

Early on, even in the vendor selection process, as many stakeholders as possible should be part of the process. "You want to get their buy-in early," he says. "We have seen situations where a centralized decision was made, the tool was implemented, and you had end users who spent half their career creating spreadsheets, and implementing special formulas into these spreadsheets, that they had to throw out the window."

Keeping in the loop those who will ultimately use the new tools will help quell internal opposition. "When you are implementing a GRC system, it might be the first time the organization has ever gone down this road," adds Mitch Kraskin, CEO of Compliance Science, a provider of GRC solutions. "You might be asking stakeholders to do certain things they have never done before, such as attestations and certifications. Figure out how to get buy-in before you push it out so they don't have an adverse reaction. You want them to be collaborative, understand why you are doing it, and why it is a benefit to the organization."

Engaged with the process, a small group of early adopters "can become your fan club," Kraskin says, suggesting that those GRC cheerleaders include em-

ployees who are respected by their peers and carry clout. This will "tamp down any adverse reactions to new technology, particularly those things that are part of a cultural shift."

Another reason to have a manageable roll-out and employee buy-in is that problems will emerge and the company must be positioned to deal with them. "You are going to step onto landmines you didn't realize were there and want get them out of the way early," Kraskin says. "Make it manageable. You are going to find things you missed, no matter how good your project management team is."

They reduce workforce. A particular GRC vendor may boast of the many cost savings and efficiencies their wares can create. In fact, that pitch may focus on how the company can reap additional savings once now-unnecessary staff is trimmed from payroll. Think long and hard before pink-slipping all those mid-level clerical employees who grew accustomed to manual or semi-manual processes.

Kraskin suggests that these employees may bring considerable value to the company post-implementation. "You are going to end up saying, 'Gee, I want people on my team who can do that work at a higher level using the system," he says. "You may be able to get those people to go from paper shuffling to providing truly valuable analytical work under the new platform."

A standard mistake is focusing almost exclusively on technology and process and not considering how people fit into the framework.

Large organizations, when confronted by crisis, will often react by "throwing a whole bunch of technology at the problem and spending a bunch of money to hire outside consultants," says Henry Balani, head of Innovation at Accuity, a financial services consultancy. "They certainly don't focus on the people. You have consultants come in, do their thing, and guess what? Six months later everything falls apart again. In order to have a successful GRC program you need to have people on board who are part of the organization. There is always a resistance to having outsiders coming in to tell you what to do when, after they leave, you are left holding the bag."

They overdo customization. A challenge that goes hand-in-hand with any GRC implementation or upgrade is how much to rely on a vendor's out-of-the-box solution, versus the need for customization to better mesh with business needs.

"If you go with lots of customization, you are creating a very rigid framework. Later on, if your business changes and you want to adjust for them, it will be costly and time consuming," George says, recommending that the focus needs to instead be on configuration, without touching the underlying coding as much as possible.

A careful evaluation of the embedded best practices, templates, and data models included with an out-of-the box product may, in fact, show that your unique challenges aren't that unusual or unheard of after all.

They don't evaluate specific data needs. GRC should never be a one-size-fits-all solution, and specific data needs cannot be an afterthought. Companies cannot underestimate the importance of understanding what is unique about their needs and understand the nature of their data.

"The first step is self-realization. A lot of firms start with a view of an ideal program that doesn't take into account that the hand they are dealt is one of data fragmentation, the complexity of new and legacy systems, and disparate workforces relying on 'bring your own device' and 'bring your own cloud' solutions," says Harald Collet, global head of Bloomberg Vault. "If your GRC program doesn't take into account the status quo and tries to turn the clock back, you end up with an end-user revolt on your hands."

Collet sees merit in piecemeal implementations, rather than attempting too much, too fast. "For smaller firms, an across-the-board approach might be fine because you only deal with hundreds of employees and have integrated business units," he says. "In a firm that has gone through an amalgamation of divestitures and acquisitions, and has a large workforce, the complexity of the business means it may be much wiser to pick a single thing and build on that success over time."

Start with a single policy against a single group of employees, he suggests. This will help the firm avoid the risk of being mired in the process creating taxonomies and overly complicated surveillance review policies. Creating separate "buckets" of employees, regulated and unregulated, allows the roll-out to apply policies in a less granular way initially, adding that specificity over time as false positives and the exceptions needed under a specific policy are better understood.

The worst case scenario that may unfold without such an approach: hundreds of policies, each with a thousand or more exceptions a day. "You will be in a very bad place and may need to dial back your entire

program," Collet says.

They overlook synergies. A lack of central coordination allows opportunities for synergies to be completely missed. With similar regulatory initiatives emerging in various countries, a company benefits from breaking down communication silos.

"In the United States you may have a compliance officer implementing a system for trade reconstruction under the Dodd-Frank Act. Meanwhile, in London, a different compliance team in a different line of business is implementing an identical solution for trade reconstruction under the MiFID 2 law [for Europe's capital markets]," Collet says. "Sometimes, because they are not communicating, it is only through outside parties or a consultancy that they realize they can connect the dots." Until that realization, "cost and operating synergies, and a better risk posture, are lost because you are not communicating internally at the firm." ■

THE HEADACHE PILL OF GRC

What constitutes an effective GRC implementation? What are the common elements of both success stories and worst-case scenarios? Those questions guided recent research ("GRC Vendor Implementation Success Strategies, "Contributors to GRC Implementation Success: Avoiding the Worst-Case Scenario") by David Houlihan, principal analyst at Blue Hill Research.

The studies looked at new GRC projects at large enterprises with a median annual revenue of approximately $3.5 billion and median employee count of approximately 5,700 employees. Typically, "best-case" implementations: took three to four months; cost between $75,000 to $180,000; had high end-user satisfaction; placed an emphasis on business objectives and needs; focused planning on process change required; conducted an assessment of value at the conclusion of each stage; emphasized scalability; balanced both out-of-the-box and configurable capabilities; and restricted the scope to immediate needs.

Worst-case implementations saw organizations give relatively little consideration to future business objectives. They were also reactive, responding to upcoming regulatory change, increased agency enforcement, or high-profile exposures or breaches suffered by peers. "This posture can limit the value provided or the shelf life of the solution as point needs dissipate or change over time," Houlihan wrote.

Sub-par executions also involved attempts to implement most or all of the desired functionality at once, or to roll out the solution to users in one effort. "Big bang approaches are not necessarily harmful, in and of themselves," the study says. "However, when these approaches are also accompanied by lack of attention to underlying business needs or enterprise IT considerations, the consequence will be an unfocused and chaotic process."

Discussing the reports, Houlihan has advice for GRC vendors: "They don't have to sell the world. They can sell a smaller story of implementation."

"This isn't necessarily an organizational transformation story; it is an analgesic. It is headache relief," is how he describes most successful GRC efforts. Accept new capabilities for what they are: a toolset, not necessarily disruptive or life-changing technology.

"Do all the right things with enterprise technology, but lower the expectations and nail it to something that is tangible," Houlihan says. "Talk about the business objectives. Why do we want this? Why do we want compliance to be more efficient? What is our risk tolerance? Where do we see pressure from regulators coming from? GRC should direct those things and the underlying business practices."

—Joe Mont

M-Files®

M-Files QMS

An Out-of-the-Box Solution for Your Daily Quality Management

With M-Files QMS, all quality documents and data are linked together within a single system, enabling organizations to optimize quality processes while streamlining compliance activities and audit requirements. **Learn more at www.M-Files.com.**

ENSURING QUALITY AND COMPLIANCE WITH EFFECTIVE INFORMATION MANAGEMENT

Regulatory Compliance

The Warning Signs of Inadequate Content Management

Companies that operate in highly regulated and frequently audited environments are often challenged with managing an ever-growing mountain of compliance documentation. In the U.S. alone, there are more than 15,000 federal, state and industry laws, standards and regulations that dictate how long to keep paper and electronic records.

The Potential Cost of Non-Compliance is High

With crippling fines and liability issues that can result from non-compliance, the stakes are high for companies to ensure they are managing their compliance-related information in accordance with mandates. However, many companies still maintain manual processes for routing, filing and organizing compliance-critical documentation. These error-prone and time-consuming practices present a major risk and can easily compromise a company's ability to meet FDA, cGMP, ISO 9001 and other regulations and standards.

Given the high priority for regulatory compliance and the amount of documentation required to prove compliance, it is no longer practical to manage the content separately from compliance efforts. If compliance management teams are asking themselves the following questions, chances are their organization is at significant risk for non-compliance due to inadequate content management practices and procedures:

- Where is the gatekeeper? Do compliance management processes slow or stop production when a key person is sick, on vacation or exiting the company?
- Has everyone read the latest compliance-related communication? Is it difficult to get the accurate status about compliance-related tasks, procedures and workflows?
- Are policies being followed and schedules being met? Who has visibility over the completion of the specified processes?
- Where are the required signatures? How easy is it to locate the documents that verify the approval processes?
- Have all of the audit issues been resolved? Are employees and managers barraged with repetitive reminder emails while the status of essential action items remain unclear to key stakeholders?
- Is compliance slowing down the business? Is the organization at a competitive disadvantage because it takes a long time to adjust to the latest regulatory compliance requirements?

ECM Enables Environmental Control

To address these vulnerabilities, organizations should consider aligning compliance management with best-in-class enterprise content management (ECM) solutions and approaches. With a consolidated and unified system for managing compliance-related information, a broad range of structured data and unstructured content can be quickly and easily searched, viewed and managed from any location, which significantly streamlines the regulatory management process while also substantially reducing the risk of non-compliance due to manual errors and lost information.

The introduction of a centralized ECM solution also promotes automated compliance-related workflows. In addition to defining and controlling document access permission levels, compliance teams can establish automated notifications and communications to the individuals who are involved in various compliance-related processes. Organizations can automate the enforcement of policies and procedures that actually save time and boost productivity while also ensuring tasks are completed according to compliance requirements.

By leveraging an ECM system to manage compliance-related content and associated processes, companies can increase information control and visibility while significantly reducing their risk of regulatory compliance violations. ■

M-Files®

ISO 9001 Certification

Is it Worth It?

The ISO 9000/9001 family of standards related to quality management systems help businesses better serve their customers and simultaneously comply with product-related regulatory requirements. More than a million businesses and suppliers have been certified as ISO compliant based on the criteria defined in the ISO 9001 standard.

There are many reasons why businesses continue to join the worldwide ISO 9001 community. The standard has gained acceptance to the degree that many major global corporations and organizations require ISO 9001 certification from their partners and solution providers. The roadmap it provides for quality management has been proven over more than five decades to help lower risks, especially in regulated industries.

Certification Equals Bottom Line Improvement

Often times, certification and compliance initiatives can bring companies to sink-or-swim moments. This is true for the ISO 9001 certification process, which requires the compilation of documentation that can either drown an organization or motivate them to deploy and leverage an enterprise information management (EIM) system in order to effectively manage both their ISO 9001-related content as well as other core information assets. A best-in-class EIM solution can manage and streamline ISO 9001 requirements with many features and capabilities that simultaneously drive up overall productivity and business efficiencies.

Fläkt Woods is a great example. One of the world's leading manufacturers of air handling units, the company's deployment of an enterprise information management solution has not only enabled effective document handling for ISO certification, but it has also resulted in a significant reduction in design errors due to outdated versions of documents, as explained in this excerpt from Fläkt Woods Creates a Comfortable Environment for Quality Management:

> *"Establishing and enforcing document management and control processes has "improved their manufacturing and production processes, enhanced collaboration internally and with their suppliers, and driven organizational efficiencies that have had a major impact on their bottom-line objectives."*

Other documented EIM deployments highlight examples of potential benefits that can be gained on the path towards ISO certification:

- Less time spent looking for ISO 9001 documents. All ISO 9001-related content can be tagged with metadata attributes that identify them as "ISO 9001 related" as they are created or saved. These metadata attributes allow documents to be retrieved based on context and relevance instead of on which folder they reside in. The added layer of intelligence makes it quick and easy to locate relevant ISO 9001 information, or to retrieve related documents for any other purpose or project.
- Better visibility of ISO assets. Digital content can be managed as part of a single virtual repository, eliminating silos of information that are time consuming to search.
- Automated version control and archiving. Employees can access the most current information, or retrieve historical documents.
- Streamline ISO certification tasks. ISO 9001 certification-related workflows can be automated, with the enterprise information management solution giving managers complete visibility of process status. eSigning capabilities can further automate workflows for certification-related processes.
- Protect sensitive and valuable content. Access management features ensure the security of confidential or mission-critical information.

EIM Engine Propels Quality, Efficiency and Productivity

Take advantage of the ISO 9001 certification process to raise awareness about these types of benefits that can be gained from an enterprise information management solution. Besides driving up efficiency and productivity, every business should consider how improving quality can strengthen the company's reputation and help to avoid risks. Best-in-class EIM solutions can further strengthen a company's position in the market by extracting more value from information and turning it into competitive advantages.

The main advantages of ISO 9001 remain the same 55 years after the original guidelines were drafted – certification gives partners and customers the assurance that the company they're working with has strict processes for ensuring its quality policies are followed throughout the organization and that they've embraced the concept of quality through continual improvement. Today, instead of questioning whether to embark upon ISO certification, it might be better to ask, "Why not?" ■

M-Files®

How Can Manufacturers Keep Their Documents Under Control?

One of the most essential tasks for manufacturers is maintaining compliance with industry standards and regulations, which entails managing large amounts of sensitive information.

This can be a big job and many firms are falling short with the document control requirements associated with quality standards such as ISO 9001, according to an article in Quality Magazine.

The issue is often exacerbated by the fact that quality managers can face difficulties in convincing senior management that implementing a document control solution is a critical component of a manufacturer's ability to adhere to standards and regulations.

In the past, it was often the case that document management consisted of little more than keeping physical copies of confidential files in locked cabinets, to which only certain personnel had access to.

However, manual, paper-based processes often lead to lost data and incorrect versions of documents being utilized, making it difficult to ensure authorized personnel have up-to-date information about the state of quality documentation and processes.

Content in Chaos

When diverse and disconnected filing cabinets, network files, folders and other systems are used to store data, it is almost impossible to get accurate details quickly. Information is also often unnecessarily duplicated, causing an extra layer of work as personnel sort through vast amounts of data to find the correct version.

As a result, quality managers in manufacturing firms are often unsure as to how key processes are being followed and if issues have been resolved.

A document management solution integrated within a quality management framework enables manufacturers to consolidate important operational information into a simple, easy to search platform that allows users to locate and view the most accurate data at the exact moment they need it, without having to hunt down paper documents that can reside in multiple physical locations or are buried within a complex network folder scheme.

Good manufacturing practices require firms to keep tight control over their documents to manage file versions, control employee access and implement changes swiftly. When documents can be searched, viewed and edited across integrated systems, workflow processes are significantly streamlined and operational efficiency is greatly improved. ■

Achieving a Unified View of Financial Crime Risk

by Jaclyn Jaeger

Increased regulatory scrutiny and the sting of billions in fines and penalties resulting from misconduct have prompted many financial firms to pour money into their compliance programs—investments that may be in vain without a unified view of risk.

A recent poll of 90 financial institutions conducted by NICE Actimize, a financial crime solutions provider, underlines the siloed environment many banks still operate in. According to the survey, 53 percent of financial institutions with at least $60 billion in assets have at least 10 different detection systems. Another 31 percent have more than 20.

"Systems and processes that are not linked make it hard to aggregate and consolidate data," says Michael Atkin, managing director for the EDM Council, a non-profit trade association founded by the financial industry to elevate the practice of data management. That means financial institutions don't have a full view of their risk or insight into opportunities, he says.

Increasingly, however, banks recognize the need to achieve a unified view of risk, driven by a confluence of regulatory scrutiny, high-profile fines and penalties, and the need to protect against reputational damage. "We're seeing more and more financial institutions wanting to achieve a unified view of risk," says Chad Hetherington, global vice president at NICE Actimize.

The overall goal is to link existing systems and processes to gain a horizontal view of operations, get a consolidated view of risk, and reduce operational costs. "It is not possible or reasonable to rip and replace these systems," Atkin says. "The better approach is to harmonize the data and normalize the messaging processes."

Some banks are trying to achieve that unified view of financial crime risk by establishing financial intelligence units (FIUs). "FIUs are serving as a central body that standardizes processes across lines of business, geographies, and financial crime domains—such as anti-money laundering, fraud, bribery, corruption, sanctions, tax evasion, and cyber-crime—so as to increase efficiency and effectiveness," PwC said in a white paper accompanying the NICE Actimize data. "FIUs use a combination of technology-enabled analytics and coordinated intelligence gathering to determine areas of risk."

The purpose of FIUs at global banking giant HSBC, for example, is "to identify and investigate significant cases, trends, and strategic issues related to financial crime risks and share relevant data and intelligence across the group," HSBC said in a recent post on its website. Other banks that have established FIUs include Royal Bank of Scotland, Standard Chartered, and Barclays.

"Once you establish a data universe, you can begin to see where centralization can reduce duplicative processes and optimize current systems by leveraging data that the organization already has, but may not necessarily have been using in a certain context."

John Sabatini, Advanced Risk and Compliance Solutions Leader, PwC

Even with an FIU in place to centralize processes, gaps in financial crime analysis persist, putting banks at risk. The NICE Actimize survey showed that 75 percent of large financial institutions access at least four systems, and 25 percent access six or more, to obtain the data needed to investigate a typical work item or alert.

"For example, during a standard investigation, the investigator would most likely check the customer relationship management system, a separate sanctions screening system, a separate transaction monitoring system, and a fraud surveillance system that holds additional activity details about an individual," says John Sabatini, advanced risk and compliance solutions leader at PwC.

Centralized Case Management

The solution for many banks is to implement a centralized case management system so investigators can access a single platform that stores information centrally. "Obtaining information from a single source enables investigators to cross-leverage that information more efficiently and effectively, eliminating duplication of effort and accelerating investigations," PwC said in its white paper.

Sabatini says a direct correlation exists between centralizing risk mitigation and centralizing a company's IT and data platforms. "What we've seen in the market is that companies are taking a phased approach to achieve this target operating model," he says. "It begins with an assessment of your current environment and a firm understanding of your key systems and data feeds."

"Once you establish a data universe, you can begin to see where centralization can reduce duplicative processes and optimize current systems by leveraging data that the organization already has, but may not necessarily have been using in a certain context," Sabatini says.

Implementing a centralized case management system typically takes place in three phases:

Core case management. "Core case management capabilities enable financial institutions to more efficiently and effectively manage workflows," PwC said. Automation improves visibility into questionable behavior and makes the triggering, triage, and assignment of alerts by AML or fraud monitoring more streamlined.

Implementing a centralized risk management program is not as daunting as it may seem. "Most companies already have the tools, systems, and data to make advanced risk management a reality," Sabatini says. The goal is to take all that data from transaction-monitoring systems, fraud systems, and customer systems, pour it into a case management system, and make that data easily accessible during an internal investigation.

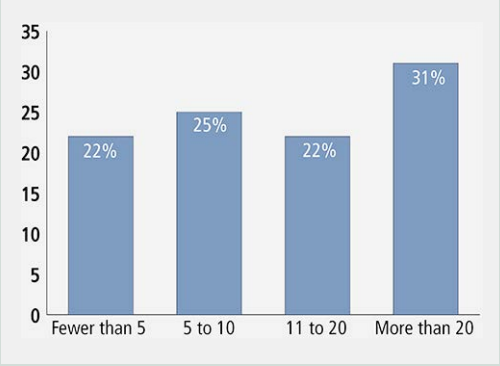
Additionally, Sabatini says, developing consistent procedures across various investigative teams—financial crime, trade surveillance, fraud, corporate security, and more—and making automated recommendations for specific types of investigations can increase overall compliance effectiveness.

Enterprise case management. Once core case management capabilities exist, financial institutions can then focus on culling relevant customer and transaction data sources to "provide a 360-degree view of exposure across AML, fraud, sanctions, advanced due diligence, and so forth," PwC said.

By integrating customer data streams to develop a single customer view, financial institutions can better support risk management and compliance, "so that they can tie all the bits and pieces of data together and they can see all the various relationships that exist," Hetherington says. Sometimes different business

DETECTION SYSTEM STATS

Approximately how many analytic and/or detection systems does your organization have in place to support financial crime and compliance needs?



Source: Nice Actimize.

units share the same customer, "and yet they will treat them differently from a financial crime perspective," he says.

That's problematic, especially where regulators are going into banks today and identifying where different business functions share the same customers. "They're asking them, 'Why did you handle this activity this way, and this activity another way?' When the institution doesn't have a good answer, it's a problem, and it really puts the institution at risk," Hetherington says.

Predictive modeling and intelligence mining. "The next wave in capabilities involves using advanced analytics and technology to enhance case management," PwC said. In this way, data gathered and shared from sources outside the company are used, and screening for adverse media becomes integrated within financial crime operating models.

Some banks today are trying so-called "in-memory computing" technology, like SAP HANA, which helps companies to detect patterns and analyze massive amounts of data "with very little effort in a very short timeframe," says Falk Rieker, global head of banking business at SAP.

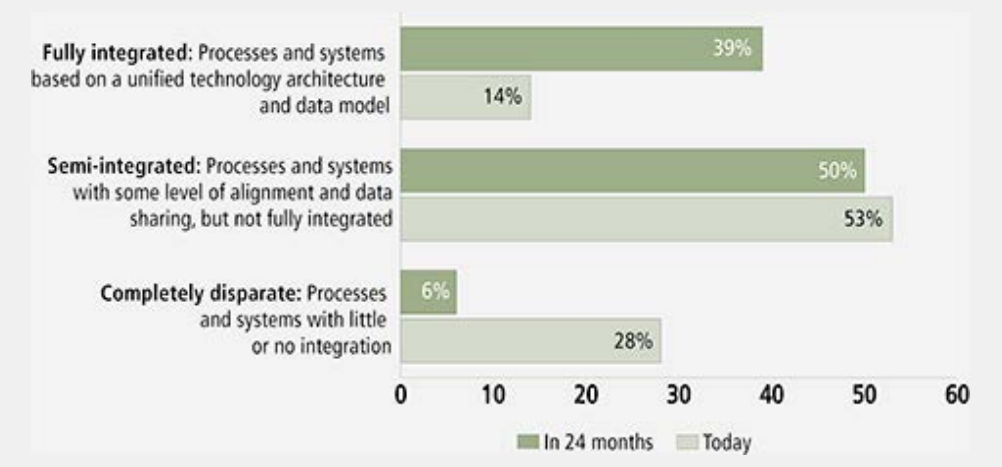
Incorporating intelligence from external sources—such as money-laundering intelligence task forces and financial crime alert services—makes for more effective decision making, "and aggregating both internal and external sources provides investigators with a more comprehensive view of a customer's relationship and makes internal watch lists and high-risk lists more robust and dynamic," PwC said. "With integrated information in hand, financial institutions can also share information more easily with regulatory parties and facilitate information sharing among various authorities."

Data management as an objective does not happen overnight, "because it requires coordination and alignment among organizations that have many, many priorities to manage," Atkin says. He advises approaching data management from a "practical point of view," meaning incremental delivery, having in place well-structured governance mechanisms, and having a clear understanding of business requirements.

Siloed organizational structures, inconsistent processes, and disparate data systems create risks for all financial institutions. Having in place a centralized case management system is one way to reduce financial crime risk and the inevitable aftermath of significant fines and penalties. ■

CRIME RISK MANAGEMENT SYSTEMS

Which of the following most accurately describes your organization's financial crime risk management processes and systems?



Source: Nice Actimize.

Smarter Approaches to Regulatory Change Management

by Joe Mont

The modern compliance officer trying to build a program for so many regulations, changing so often, might feel a lot like the mythical Greek king Sisyphus: sentenced by the gods to push a boulder up a hill, over and over again, for all eternity.

"Compliance officers feel as though they are being punished by the gods," says Steve Taylor, director of product management for Wolters Kluwer's U.S. enterprise risk and compliance business. "Just as they've managed to implement one regulatory development, another 20 come their way. They are continuously rolling the ball up the hill."

In a post-Dodd-Frank Act world where new regulations emerge fast and furious, keeping pace can seem to require inhuman effort. Hence, a push for smarter approaches to regulatory change management to keep compliance and risk managers alerted to new regulations as quickly as possible. "There is a lot of emphasis, at this precise moment in time, on making sure that people know what the rules are and keep up with the developments," says Taylor, whose firm is one of many selling regulatory change management systems.

Once upon a time, firms could do quite well by merely monitoring regulators' websites and, as needed, forming an ad hoc team of lawyers if a new rule was overly complex or risky for a business line. "What's happening now is that tidal wave of information is making it more and more difficult for businesses to keep up with what is going on," he says.

Effective regulatory change managemen (whether you use dedicated software for the task or not) has several parts. Not only must you be aware that a rule change has happened; you must know how the rule affects the company's policies, procedures, and internal controls.

"You want to codify your controls policies and procedures and make sure you really understand the form of the data—because you can have structured and unstructured data—as well the source of the information," suggests Graham Tasman, business advisory services principal at the accounting firm Grant Thornton. "Where is this critical information going to come from? Integration is crucial because you deal with information flows from many different source systems that all need to come together."

"There is a lot of information out there that organizations could track, some of which is important and some is not," Taylor says. "You don't want to drink from the fire hose. You need customized feeds of information coming into the system that reflect the business activities and the regulators you are tracking."

The challenge is configuring those systems so the business gets the information it needs, delivered to the right people. And, Taylor notes, more than just final rules must be tracked. Firms should also monitor secondary source information from regulators, such as no-action letters and interpretive guidance.

To succeed, a business must identify affected policies, procedures, and controls. "You need to do the initial triage on whether a change is material and, if it is, who has to deal with it," Taylor says. In some firms, a regulatory or legal team does the initial scan of the documents, makes that initial assessment, and passes it onto the business lines.

"Managing regulatory change is less about the data gathering—although that is a critical function—and more about assessing the impact to the business," Taylor stresses. "Organizations need to do some kind of mapping and establish a framework.

Can you identify policies and procedures that are relevant to your business activities and products? Can you identify related supervisory controls and compliance risks that may be tied to them?"

Business operations can be mapped to the regulatory change management technology. "They can understand that 'this part of my business is driven by these rules and regulations and connected to these policies, procedures, and e-learning training activities,' " Taylor says. The data can also be mapped to a specific individual within the organization. "If FINRA Rule 3110 changes, send it to Bob because he deals with those developments." These efforts can help assess the effect of the new or changed rule and what needs to be done, including whether additional training is needed or a new supervisory control must be developed.

Another challenge is to determine how much resources you need for a strong change management system. "What does it look like for an organization to be aware of those operational costs from regulatory change, from the most Pollyanna to the most Chicken Little perspective?" asks David Houlihan, principal analyst for Blue Hill Research, a GRC research firm. "How do they take the situation and develop a strategic understanding rather than a very reactive posture? You need to figure out what the cost components are. You need to know and measure operational cost."

While that assessment, capability may be possible, Houlihan says, although he has yet to find a company or vendor that does it effectively. "Folks that own risk need to do more to understand the rest of the business," he says. "I think they have been comfortable being Chicken Little talking about how the sky is falling, rather than what it costs to build a bomb shelter."

Those relying on a regulatory change management system would do well to take a look at how many large banks approach fraud management, tracking massive amounts of transaction data on a daily basis and still, in real time, maintaining effective lines to risk and compliance and pushing every transaction through those controls, he adds.

As chief compliance officer for Florida-based BankUnited, Marie Blake uses both technology and a hands-on approach to manage regulatory change. Tracking efforts are supplemented with industry newsletters and updates from regulators and law firms. Armed with this information, she produces a regulatory digest for the company. That impact analysis is supplemented with quarterly, in-person meetings with business unit leaders.

"We are tracking things behind the scenes, and working with the business lines to ensure that everything is covered," Blake says. "We know if it is a big change or a small change, whether we need to launch a formal initiative, and whether there are vendors involved."

For her bank, overseen by the Office of the Comptroller of the Currency, adapting to regulatory change is a mandate. Using exams and filings, the OCC directly asks for documentation of how it was engaged throughout regulatory change events and did it assimilate those changes effectively. In addition to rulemaking, guidance and commentary issued by the regulators is "treated as though it is regulation," Blake says. "They expect us to be reading the guidance and incorporating it into our control structure."

BankUnited's approach to regulatory change moves it beyond the compliance function and out into the business lines. "They understand that they are the first line of defense in ensuring that we are managing all risk exposures building these changes into their control environment," Blake says. "It needs to be a very integrated process where they are sitting at the table with us."

Training and education is important for bringing all relevant employees up to speed on a rule change. Training materials at BankUnited are updated at least annually, supplemented by customized programs.

While Blake does use technology to assist regulatory change monitoring, she warns against taking it for granted. "The regulators expect us to be monitoring what vendors do," she says. "We can't contract away regulatory risk exposure." ■

"Tracking regulatory developments is one thing, but you need to develop an impact assessment, and understand where a new rule hits your policies, procedures, and internal supervisory controls."

Steve Taylor, Senior Product Manager, Wolters Kluwer

How Mature Is Your Information Governance Function?

by Jaclyn Jaeger

Most companies still have lots of work to do to turn their information governance into "mature" programs, where they can extract value and insight from their troves of data while minimizing security and privacy risks.

The good news is that progress is being made—albeit slowly.

That's according to the findings of a new report from the Information Governance Initiative (IGI), a think tank dedicated to advancing information governance practices and technology; it polled 100,000 IG professionals on the subject. The report asked companies about the maturity of their IG functions, what IG projects they're currently undertaking, the timeframe and costs involved in achieving those projects, and more.

"To date, very few organizations have taken a coordinated approach to how they manage and monetize their data," says Barclay Blair, IGI founder and executive director.

Overall, most companies rate the maturity of their IG programs as "nascent"—that is, they have some elements in place and are building the foundation, but many relevant information-related functions remain missing or underdeveloped. Many others rated their programs as "intermediate," meaning they are building the framework and structure, according to the IGI report.

"Many organizations are beginning to acknowledge the need for proactive IG functions, but most have been slow to develop and implement these functions in a sustainable and consistent fashion," says Eric Robinson, a solution architect for Kroll Ontrack.

In its simplest terms, information governance is a cross-disciplinary approach of governing and managing data across disparate systems and business functions. Historically, companies have struggled to manage risks across several siloed risk management functions: cyber-security, records management, privacy, legal, and more. The goal, in theory, is to have visibility into all those pockets of data at once.

"An information governance function can help those functions to work together to consider information risks holistically and to develop a broader strategy and viewpoint around managing enterprise information risk," says David Remnitz, head of forensic technology and discovery services leader for EY.

Typically, information governance gets kick-started by a risk event—such as litigation or an investigation—when the company suddenly realizes it has no idea what data it has or where that data resides. "Often, no single function possesses the tools and expertise to help the company respond effectively to an event," Remnitz says.

In addition to litigation and an investigation, the surge of cyber-attacks is also driving companies to ask probing questions about their data security and retention policies: What data do we keep? What data do we throw away? What data do we invest time and money managing? "Cyber-security is a huge driver for organizations to get their information house in order," Blair says.

CIGO Function

To put a formal structure around some of the answers to those questions, some companies—Master-

Card, Aon, McKesson, and Autotrader.com, to name a few—have appointed information governance officers, tasked with owning and coordinating the company's information governance program.

In the early stages of an information governance program, many companies said the role of the chief information governance officer (new acronym time: CIGO) is to build a foundation of information governance. That requires someone with sufficient authority and leadership skills to see that the work gets done, according to the IGI report. As a company's information governance improves, CIGO's role is to develop the framework and structure of an information governance program and then maintain and improve on the IG program as it develops and matures.

According to the report, CIGO has three primary tasks:

» **Information leadership.** At most organizations, nobody "owns" the information problem. CIGO fills this leadership gap by taking on accountability for the governance of information in all forms across an organization.
» **Inter-departmental coordination.** Information-related functions often operate in isolation. Information governance needs a leader who can coordinate, call the shots, and drive governance across all information facets in an organization.
» **Balancing risk and value.** Information is a business asset, creating both risks and value. The CIGO must find the right balance between the risk and value.

One way to get started with the coordinating process is to form a steering committee. "That typically is where a lot of organizations are starting with their information governance efforts," says Laurie Fischer, a managing director at Huron Consulting Group.

According to the report, however, most companies (58 percent) said they do not have a steering committee in place. Thirty-seven percent said that they do, and 5 percent were not sure.

Current IG Projects

The IGI report also said many companies have multiple information governance projects underway or planned in the next year. Sixty-nine percent identified updating policies and procedures as one project they are undertaking, followed by scanning paper documents (50 percent), and data consolidation and cleanup (47 percent) as their second- and third- most common projects.

Other common projects include the migration of unstructured information from one system to another (46 percent); defensible deletion (42 percent); and decommissioning an archive or system (40 percent).

"Data mapping is a foundational element in the information governance process," Robinson says. "It is necessary to start with a base understanding of what and where data exists." Only after that happens can you start to leverage all that day, either for regulatory requirements or for business intelligence purposes.

On a practical level, Robinson says, some IG projects might entail:

» Identifying critical assets that require a higher level of protection from cyber-risk;
» Identifying information that may have been compromised in a breach; and
» Identifying redundant, trivial, and obsolete information, and disposing of that data to reduce e-discovery costs, supporting more effective management of information.

"In practice, IG projects can play a role in a wide variety of enterprise risk management initiatives," Remnitz says. "Mature IG organizations are actively managing these risks before a risk event occurs; less mature organizations respond to them only as or after they occur."

Getting an information governance project off the ground can take a significant amount of time. According to the IGI report, the plurality (35 percent) of practitioners said it takes longer than a year to get an information governance project started. Another 22 percent said it takes at least a year, while 16 percent said six months. Only 10 percent said it takes three months or less.

The average number of information governance projects that companies are taking on vary greatly by size. Companies that have 10,000 or more employees are working on an average of seven information governance projects at once, spending an average of $777,000. On the lowest end, companies with up to 1,000 employees are undertaking up to four projects at once, spending an average of $186,000. ■