Galvanize

Better practices for compliance management

How technology can improve your regulatory & policy compliance

Table of contents

Managing the complex web of evolving compliance requirements

Compliance requirements are complex and expensive for organizations to manage. Every business sector faces an ever-growing number of regulations and they're always changing, so how can you keep up?

Non-compliance fines and penalties imposed by regulatory agencies are increasing—in some cases dramatically. It's likely that none of this is news to you. And you're probably well aware of the statistics on the number of regulations—existing, new, and changing—that impact your business. The important question is: How is your organization responding?

The reality is that many businesses and government agencies struggle to manage compliance requirements because they use inefficient processes and outdated or generic technology. This leaves them vulnerable and without necessary oversight for effective compliance. On the other hand, some organizations have responded to the challenge by implementing technologies that are genuinely effective.

We've worked with many organizations to improve their compliance management, and have seen huge benefits when they implement purpose-built compliance software.

In this eBook, we examine the challenges of compliance management, and explore their root causes. We then show you an approach that optimizes the interaction of people, process, and technology to manage compliance requirements and monitor risks and controls.

Let's start untangling this complex web of compliance management.

The main compliance challenges

We know that businesses and government entities alike struggle to manage compliance requirements. Many have put up with challenges for so long—often with limited resources—that they no longer see how problematic the situation has become.

FIVE COMPLIANCE CHALLENGES YOU MIGHT BE DEALING WITH

01 COMPLIANCE SILOS

It's not uncommon that, over time, separate activities, roles, and teams develop to address different compliance requirements. There's often a lack of integration and communication among these teams or individuals. The result is duplicated efforts—and the creation of multiple clumsy and inefficient systems. This is then perpetuated as compliance processes change in response to regulations, mergers and acquisitions, or other internal business re-structuring.

02 NO SINGLE VIEW OF COMPLIANCE ASSURANCE

Siloed compliance systems also make it hard for senior management to get an overview of current compliance activities and perform timely risk assessments. If you can't get a clear view of compliance risks, then chances are good that a damaging risk will slip under the radar, go unaddressed, or simply be ignored.

03 COBBLED TOGETHER, HOME-GROWN SYSTEMS

Using generalized software, like Excel spreadsheets and Word documents, in addition to shared folders and file systems, might have made sense at one point. But, as requirements become more complex, these systems become more frustrating, inefficient, and risky. Compiling hundreds or thousands of spreadsheets to support compliance management and regulatory reporting is a logistical nightmare (not to mention time-consuming). Spreadsheets are also prone to error and limited because they don't provide audit trails or activity logs.

04 OLD SOFTWARE, NOT DESIGNED TO KEEP UP WITH FREQUENT CHANGES

You could be struggling with older compliance software products that aren't designed to deal with constant change. These can be increasingly expensive to upgrade, not the most user-friendly, and difficult to maintain.

05 NOT USING AUTOMATED MONITORING

Many compliance teams are losing out by not using analytics and data automation. Instead, they rely heavily on sample testing to determine if compliance controls and processes are working, so huge amounts of activity data is never actually checked.

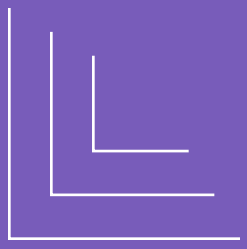
Transform your compliance management process

Good news! There's some practical steps you can take to transform compliance processes and systems so that they become way more efficient and far less expensive and painful.

It's all about optimizing the interactions of people, processes, and technology around regulatory compliance requirements across the entire organization.

It might not sound simple, but it's what needs to be done. And, in our experience, it can be achieved without becoming massively time-consuming and expensive. Technology for regulatory compliance management has evolved to unite processes and roles across all aspects of compliance throughout your organization.

Look, for example, at how technology like Salesforce (a cloud-based system with big data analytics) has transformed sales, marketing, and customer service. Now, there's similar technology which brings together different business units around regulatory compliance to improve processes and collaboration for the better.



The growing pace of regulatory change

In 2017, Thomson Reuters Regulatory Intelligence[1] captured 56,321 regulatory alerts from 900 regulatory bodies worldwide.

That’s an average of 216 regulatory updates per day, up from the 201 per day in 2016.

[1] Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

Where to start?

Let's look at what's involved in establishing a technology-driven compliance management process. One that's driven by data and fully integrated across your organization.

THE BEST PLACE TO START IS THE END

Step 1: Think about the desired end-state.

First, consider the objectives and the most important outcomes of your new process. How will it impact the different stakeholders? Take the time to clearly define the metrics you'll use to measure your progress and success.

A few desired outcomes:

+ Accurately measure and manage the costs of regulatory and policy compliance.
+ Track how risks are trending over time, by regulation, and by region.
+ Understand, at any point in time, the effectiveness of compliance-related controls.
+ Standardize approaches and systems for managing compliance requirements and risks across the organization.
+ Efficiently integrate reporting on compliance activities with those of other risk management functions.
+ Create a quantified view of the risks faced due to regulatory compliance failures for executive management.
+ Increase confidence and response times around changing and new regulations.
+ Reduce duplication of efforts and maximize overall efficiency.

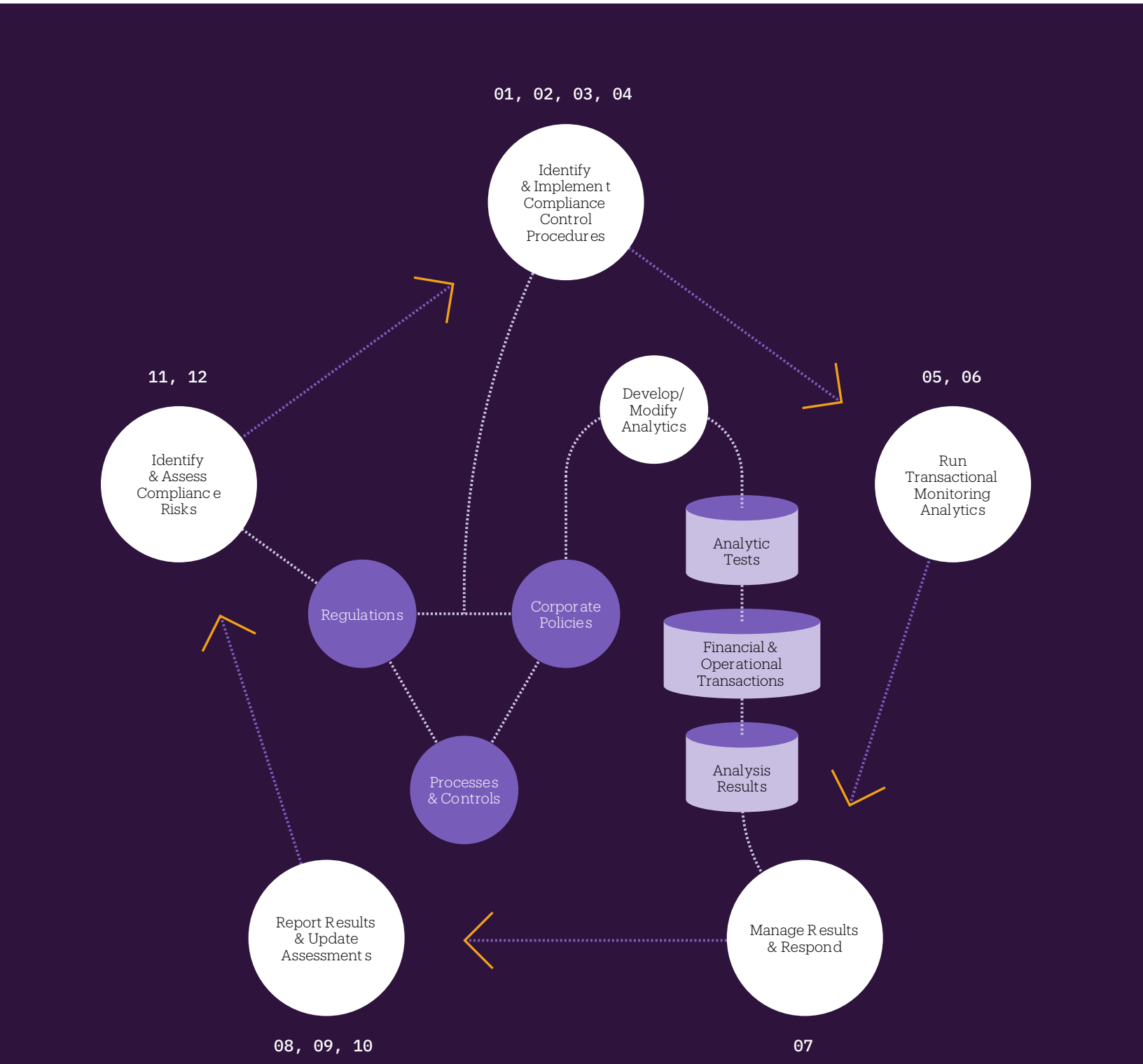
NOW, WHAT DO YOU NEED TO SUPPORT YOUR OBJECTIVES?

Step 2: Identify the activities and capabilities that will get you the desired outcomes.

Consider the different parts of the compliance management process below. Then identify the steps you'll need to take or the changes you'll need to make to your current activity that will help you achieve your objectives. We've put together a cheat sheet to help this along.

In relatively basic terms, the activities and capabilities needed for compliance management typically look like this:

Compliance management process



IDENTIFY & IMPLEMENT COMPLIANCE CONTROL PROCEDURES

01 Maintain a central library of regulatory requirements and internal corporate policies, allocated to owners and managers.

02 Define control processes and procedures that will ensure compliance with regulations and policies.

03 Link control processes to the corresponding regulations and corporate policies.

04 Assess the risk of control weaknesses and failure to comply with regulations and policies.

RUN TRANSACTIONAL MONITORING ANALYTICS

05 Monitor the effectiveness of controls and compliance activities with data analytics.

06 Get up-to-date confirmation of the effectiveness of controls and compliance from owners with automated questionnaires or certification of adherence statements.

MANAGE RESULTS & RESPOND

07 Manage the entire process of exceptions generated from analytic monitoring and from the generation of questionnaires and certifications.

REPORT RESULTS & UPDATE ASSESSMENTS

08 Use the results of monitoring and exception management to produce risk assessments and trends.

09 Identify new and changing regulations as they occur and update repositories and control and compliance procedures.

10 Report on the current status of compliance management activities from high- to low-detail levels.

IMPROVE THE PROCESS

11 Identify duplicate processes and fix procedures to combine and improve controls and compliance tests.

12 Integrate regulatory compliance risk management, monitoring, and reporting with overall risk management activities.

An example approach

Here's an example where an automated, data-driven approach to can evolve traditional compliance management processes.

CASE STUDY: BEFORE & AFTER

The customer:

A US-based multinational conglomerate (primarily a manufacturer and wholesaler).

Compliance requirements:

- Sarbanes-Oxley (SOX)

- Foreign Corrupt Practices Act (FCPA)

- A range of Emergency, Health, and Safety (EH&S) regulations.

Challenges:

+ A risk assessment uncovered certain compliance issues around data privacy in European operations, and the potential for money laundering among certain customers in Asia.
+ Dealing with tons of vendors, some with compliance concerns like conflict minerals, environmental standards, and product component quality.
+ Ensuring compliance with 1,500 regulations. The actual number is hard to say as multiple internal groups own different aspects of compliance.

Process before:

Each group relied on spreadsheets to track requirements, related controls, and evidence of testing and verification. The spreadsheets were maintained independently by each group. This meant it was hard to get a consolidated view of compliance status—let alone finding redundancies or gaps in compliance activities across the organization.

The staff spent thousands of hours emailing all sorts of forms and spreadsheets to those responsible for the countless global regulations and controls. They spent just as much time again chasing people for responses, and then compiling results.

Executive management received a summary report every quarter that highlighted any outstanding compliance concerns. The report was painstakingly amalgamated manually into an overall corporate risk assessment report.

After implementing technology to transform their process:

+ Details of all compliance requirements are now maintained in a central library.
+ Details of policies, processes, and controls are clearly linked to the regulations and compliance requirements.
+ An in-depth status is immediately available by selecting, for example, “SOX” or “FCPA” or “PCI” or “SOC.”
+ It’s easy to determine individual ownership for specific sets of compliance requirements.
+ Transactions are automatically monitored across six core financial and operational process areas.
+ Non-compliant activities are identified using advanced data analysis.
+ Identified anomalies and exceptions are automatically flagged for designated individuals for response.
+ Unresolved issues are now escalated for senior management review.

In numbers:

+ 2.5 million payment transactions ($3.9B worth), are all tested for indicators of bribery and corruption.
+ Of these, payments with a total value of $5M are currently being investigated as possible FCPA and UK Bribery Act violations.
+ 22 different analytic tests have been applied to 350K journal entries, looking for indicators of SOX control problems.
+ Based on the results of automated testing for the past six months, 105 journal entries are currently being reviewed by internal and external auditors.

A few more positive outputs:

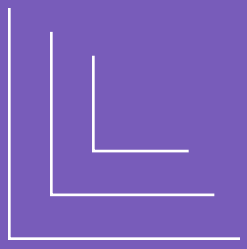
√ Automated attestations are sent to all contractors to confirm they've received training in health and safety regulations and are in compliance with requirements. HR is automatically notified of those who failed to respond or have not received training.

√ Certification requests are automatically sent to specific vendors to confirm they're in compliance with conflict mineral legislation. Vendor status is put on hold in the case of non-compliance or lack of response.

√ Results of transaction monitoring for core processes, and compliance attestation for vendors, employees, and contractors, give an overall assessment of the status of compliance risk. Full drill-down is available to give details of activities and results.

√ The chief compliance officer and the chief risk officer, together with their teams, now have access to a dashboard that shows the current status of compliance by region and by category of regulation.

√ This dashboard is part of a larger overall integrated risk and compliance management dashboard used by the CEO, CFO, board, and audit committee.



Eight compliance processes in desperate need of technology

The unfortunate reality is that many leading compliance management software products were originally built a decade or more ago, and simply aren't capable of dealing with today's global compliance challenges.

Choosing purpose-built governance, risk, and compliance (GRC) management software can help increase efficiencies, reduce risk, and ensure you meet your compliance obligations.

The last part of this eBook looks at eight best practices you can start implementing to improve your compliance management right away.

01

Centralize regulations & compliance requirements

A major part of regulatory compliance management is staying on top of countless regulations and all their details. A solid content repository includes not only the regulations themselves, but also related data. By centralizing your regulations and compliance requirements, you'll be able to start classifying them, so you can eventually search regulations and requirements by type, region of applicability, effective dates, and modification dates.

↳ FOR MORE ON HOW WE CAN HELP, VISIT WEGALVANIZE.COM

02

Map to risks, policies, & controls

Classifying regulatory requirements is no good on its own. They need to be connected to risk management, control and compliance processes, and system functionality. This is the most critical part of a compliance management system.

Typically, in order to do this mapping, you need:

+ An assessment of non-compliant risks for each requirement.
+ Defined processes for how each requirement is met.
+ Defined controls that make sure the compliance process is effective in reducing non-compliance risks.
+ Controls mapped to specific analytics monitoring tests that confirm the effectiveness on an ongoing basis.
+ Assigned owners for each mapped requirement. Specific processes and controls may be assigned to sub-owners.

03

Connect to data & use advanced analytics

Using different automated tests to access and analyze data is foundational to a data-driven compliance management approach.

The range of data sources and data types needed to perform compliance monitoring can be humongous. When it comes to areas like FCPA or other anti-bribery and corruption regulations, you might need to access entire populations of purchase and payment transactions, general ledger entries, payroll, and travel and entertainment expenses. And that's just the internal sources. External sources could include things like the Politically Exposed Persons database or Sanctions Checks.

Extensive suites of tests and analyses can be run against the data to determine whether compliance controls are working effectively and if there are any indications of transactions or activities that fail to comply with regulations. The results of these analyses identify specific anomalies and control exceptions, as well as provide statistical data and trend reports that indicate changes in compliance risk levels.

Truly delivering on this step involves using the right technology since the requirements for accessing and analyzing data for compliance are demanding. Generalized analytic software is seldom able to provide more than basic capabilities, which are far removed from the functionality of specialized risk and control monitoring technologies.

04

Monitor incidents & manage issues

It’s important to quickly and efficiently manage instances once they’re flagged. But systems that create huge amounts of “false positives” or “false negatives” can end up wasting a lot of time and resources. On the other hand, a system that fails to detect high risk activities creates risk of major financial and reputational damage. The monitoring technology you choose should let you fine-tune analytics to flag actual risks and compliance failures and minimize false alarms.

The system should also allow for an issues resolution process that’s timely and maintains the integrity of responses. If the people responsible for resolving a flagged issue don’t do it adequately, an automated workflow should escalate the issues to the next level.

Older software can't meet the huge range of incident monitoring and issues management requirements. Or it can require a lot of effort and expense to modify the procedures when needed.

05

Manage investigations

As exceptions and incidents are identified, some turn into issues that need in-depth investigation. Software helps this investigation process by allowing the user to document and log activities. It should also support easy collaboration of anyone involved in the investigation process.

Effective security must be in place around access to all aspects of a compliance management system. But it’s extra important to have a high level of security and privacy for the investigation management process.

06

Use surveys, questionnaires, & certifications

Going beyond just transactional analysis and monitoring, it's also important to understand what's actually happening right now, by collecting the input of those working in the front-lines.

Software that has built-in automated surveys and questionnaires can gather large amounts of current information directly from these individuals in different compliance roles, then quickly interpret the responses.

For example, if you're required to comply with the Sarbanes-Oxley Act (SOX), you can use automated questionnaires and certifications to collect individual sign-off on SOX control effectiveness questions. That information is consolidated and used to support the SOX certification process far more efficiently than using traditional ways of collecting sign-off.

These automated processes also let you ask managers to confirm they understand an organization's position around regulations and certifications, for example, the US Foreign Corrupt Practices Act (FCPA). This is one of the most important anti-bribery and corruption laws for any organization operating globally. Using surveys and questionnaires, check with your managers to make sure they haven't been involved in any contravening activities.

And finally, automated surveys and questionnaires bring huge value when performing due diligence on third-party or vendor compliance.

It can be very tedious and time-consuming to manually gather confirmation of compliance (e.g., Service Organization Control reports and certifications). Automation makes certain that requests are performed promptly and delays or responses failures are escalated.

07

Manage regulatory changes

Regulations change constantly, and to remain compliant, you need to know—quickly—when those changes happen. This is because changes can often mean modifications to your established procedures or controls, and that could impact your entire compliance management process.

A good compliance software system is built to withstand these revisions. It allows for easy updates to existing definitions of controls, processes, and monitoring activities.

Before software, any regulatory changes would involve huge amounts of manual activities, causing backlogs and delays. Now much (if not most) of the regulatory change process can be automated, freeing your time to manage your part of the overall compliance program.

08

Ensure regulatory examination & oversight

No one likes going through compliance reviews by regulatory bodies. It's even worse if failures or weaknesses surface during the examination.

But if that happens to you, it's good to know that many regulatory authorities have proven to be more accommodating and (dare we say) lenient when your compliance process is strategic, deliberate, and well designed.

There are huge benefits, in terms of efficiency and cost savings, by using a structured and well-managed regulatory compliance system. But the greatest economic benefit happens when you can avoid a potentially major financial penalty as a result of replacing an inherently unreliable and complicated legacy system with one that's purpose-built and data-driven.

↳ FOR MORE ON HOW WE CAN HELP, VISIT WEGALVANIZE.COM

Technology evaluation checklist: Key considerations

Purpose-built compliance management software provides one of the most important overall benefits: ease of use. While simple, this concept is central to how technology can transform an organization—turning inefficient processes into ones that significantly optimize resources and produce greater user satisfaction.

Basically, if no one likes using the software system, you'll never be able to maximize your return on investment.

Whether you're looking to get a new compliance management system or update your current system, we've shared the following key points for you to consider.

- **Are you embracing the cloud?**
  Cloud-based systems have been proven to be highly secure and hold a lot of advantages over legacy on-site applications. One primary advantage is the continuous deployment of enhancements. You no longer need to deal with new version implementation. The software capabilities are constantly improving with minimal impact, and updates are made with little to no intervention from IT.

- **Is the technology portable?**
  It's no longer realistic to run important applications strictly on desktop or laptop computers. Executives, managers, and specialists involved in compliance management need to be able to access and update systems using a number of devices, while working in any environment, from any location.
  Your compliance software needs to be optimized to operate on those devices.

- **How does system performance rate?**
  System performance plays a major part in user satisfaction. When an application is inefficient or slow, people become frustrated and stop using it.
  This applies to everything from screen input and response times, to the time it takes to consolidate thousands of reports and survey responses, and testing millions of transactions.
  A system that works well and transforms processing and response times can create whole new levels of engagement from users.

- **Can you roll-out rapid changes and updates?**
  Your software should let you quickly re-configure and modify the system, both to take advantage of new capabilities and to implement new processes when needed. The better and more purpose-built the software, the easier these types of tasks will be.

- **Are you getting the full story from your data?**

  Data analysis needs to be able to support rules-based controls and compliance testing. It should also support a range of forms of visual and statistical analysis to provide insight into overall risks and trends. It should be able to support rapid access to, and analysis of, multiple different data types and sources, including ERP, corporate databases, and emails/formal communications.

  Additionally, logging of all analytic processes is an important capability seldom found in generic analytic technologies. Compliance requirements often mean that an activity log of everything that took place is necessary for adequate documentation and verification of procedures performed.

- **Do you have dashboards to show current compliance management status?**

  We talked earlier about the importance of reporting for regulatory bodies, which is often a prescribed format. Another important aspect of reporting is the ability to provide management with an overview of the current status of the entire compliance management process. In fact, this ultimately may need to be closely integrated into an overall corporate risk management dashboard as part of the organization's enterprise risk management strategy. Compliance executives and others will need to have specific views into discrete compliance areas, getting not only an overall visual risk assessment for a particular regulatory requirement, but insight into information such as the percentage and monetary value of anomalies identified, and the results of remediation efforts.

What can you do now?

We've covered a lot. Hopefully we've provided you with some useful takeaways to improve the performance of your compliance management activities.

Next steps to help you get going right away

1) Jot down some notes to describe your organization's current approach or challenges with regulatory and corporate policy compliance management.

- ❑ For example: Separate teams have independent processes to manage main categories of compliance requirements.
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____

2) Assess how well your approach works overall and identify any shortcomings. Go back to step 1 and score each item on a scale of 1 (desperately needs improvement) to 5 (couldn't be better!). Circle everything that scores 3 or below.

3) Estimate (doesn't need to be exact) what it costs your organization annually to run your compliance management processes. In your calculations, include: people resources + software licenses + IT support + training + external consultants, including for corporate integration and reporting.

4) Ask yourself (and your colleagues) what could be better?

- ❑ _____
- ❑ _____

5) Consider and list what steps or tips from this eBook would help your organization.

- ❑ _____
- ❑ _____
- ❑ _____

How can you improve your compliance process and protect your organization?

↳

Get in touch and let us show you how you can transform your organization's compliance program with technology, call 1-888-669-4225, email info@wegalvanize.com, or visit **wegalvanize.com**.

About the Author

John Verver

CPA CA, CMC, CISA

John Verver is a former vice president of Galvanize. His overall responsibility was for product and services strategy, as well as leadership and growth of professional services.

An expert and thought leader on the use of enterprise governance technology, particularly data analytics and data automation, John speaks regularly at global conferences and is a frequent contributor of articles in professional and business publications.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000; 72% of the S&P 500; and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

©2019 ACL Services Ltd. ACL, Galvanize, the Galvanize logo, HighBond, and the HighBond logo are trademarks or registered trademarks of ACL Services Ltd. dba Galvanize. All other trademarks are the property of their respective owners.