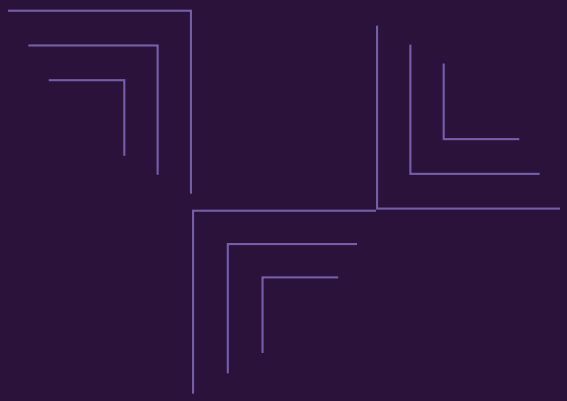
Galvanize
is now Diligent



Better practices for compliance management

How technology can improve your regulatory & policy compliance

Table of contents

Managing the complexities of compliance 3

The main compliance challenges 4

Transform your compliance management 6

Where to start? 7

Case study 10

8 compliance processes in desperate need of technology 12

- 01 Centralize regulations & compliance requirements 13
- 02 Map to risks, policies & controls 14
- 03 Connect to data & use advanced analytics 15
- 04 Monitor incidents & manage issues 16
- 05 Manage investigations 17
- 06 Use surveys, questionnaires & certifications 18
- 07 Manage regulatory changes 19
- 08 Ensure regulatory examination & oversight 20

Technology evaluation checklist 21

Managing the complexities of compliance

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

Non-compliance fines and penalties imposed by regulatory agencies are increasing—and, 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and government agencies struggle to manage compliance requirements because they use inefficient processes and outdated or generic technology.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 the necessary oversight for effective compliance.

We've worked with many organizations to improve their compliance management processes through purpose-built compliance software.

In this eBook, we examine the challenges of compliance management, and explore the 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—and 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 restructuring.

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 to 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 homegrown 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, those systems become more frustrating, inefficient and risky. Compiling hundreds or thousands of spreadsheets to support compliance management and regulatory reporting is a logistical and time-consuming nightmare. Spreadsheets are also prone to error and have significant limitations because they don't provide audit trails or activity logs.

04 Old software that's expensive to upgrade

You may be struggling with older compliance software products that aren't designed to deal with constant change. These are increasingly expensive to upgrade and difficult to maintain, and they aren't user-friendly, resulting in frustrated employees and inefficiencies.

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 whether compliance controls and processes are working, so huge amounts of activity data are never actually checked.

Regulations are increasing: In 2017, Thomson Reuters Regulatory Intelligence captured 56,321 regulatory alerts from 900 regulatory bodies worldwide. That's 216 updates per day, up from 201 in 2016.

» ***Thomson Reuters Regulatory Intelligence,*** Cost of Compliance 2018

Transform your compliance management

Good news! There are 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 organization.

This might not sound simple, but it's what needs to be done. And, in our experience, it can be achieved without becoming time-consuming and expensive.

Compliance management technology has evolved to unite processes and roles across all aspects of the organization.

Look, for example, at how technology like Salesforce (a cloud-based system with big data analytics) has transformed sales, marketing and customer service. Similar technology is now available that brings together different business units around regulatory compliance to improve processes and collaboration.

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.

Step 1: Think about the desired end state.

The best place to start is the end. 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 for executive management of the risks faced due to regulatory compliance failures
+ Increase confidence and response times around changing and new regulations
+ Reduce duplication of efforts and maximize overall efficiencies

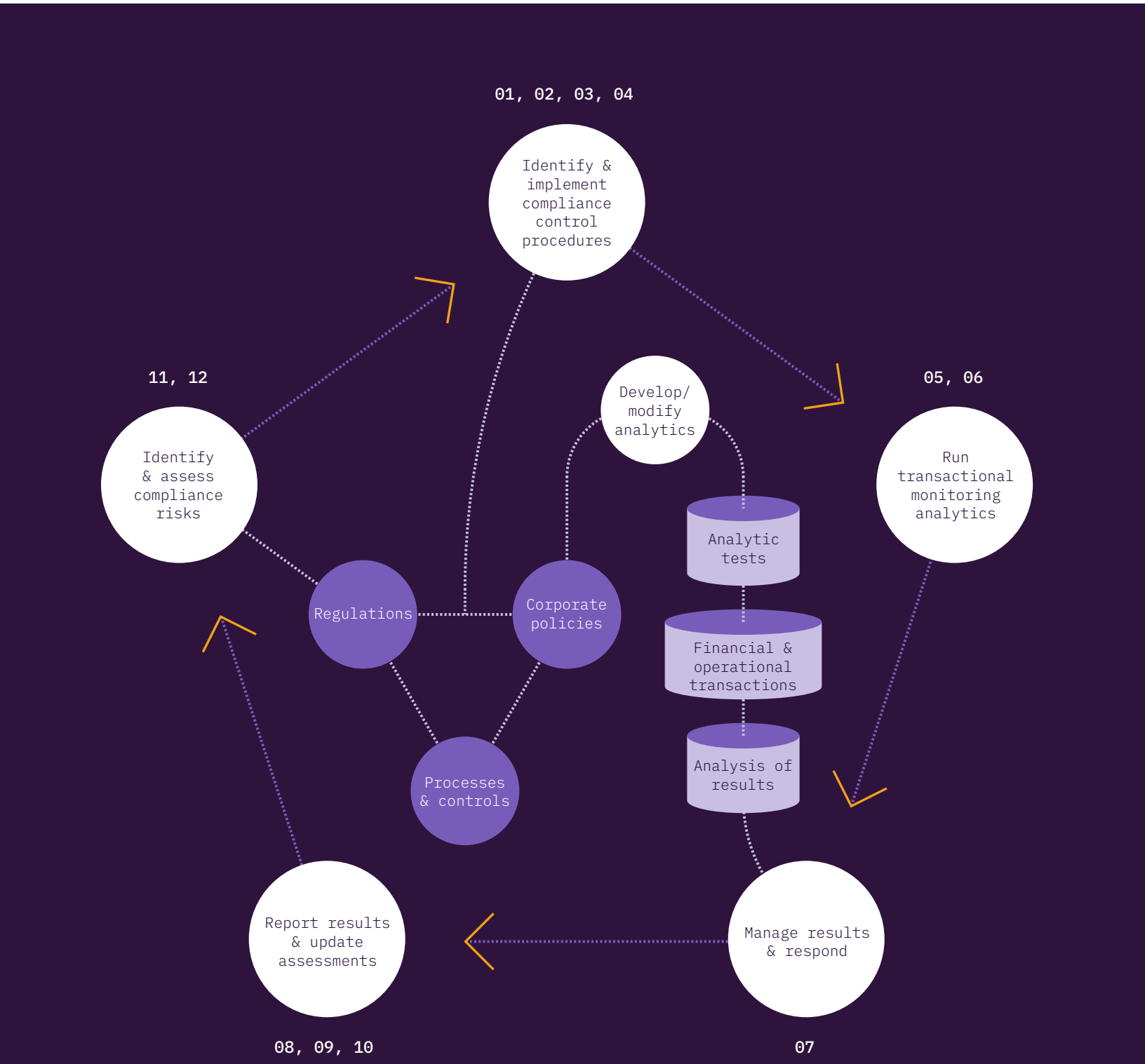
Step 2: Identify the activities and capabilities that will get you the desired outcomes.

What do you need to support your objectives? Consider the different parts of the compliance management process (see page 8).

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 these 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, using 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

Case study

Here's an example of how an automated, data-driven approach can transform traditional compliance management processes.

A US-based multinational manufacturer and wholesaler transformed its regulatory compliance obligations (including SOX, FCPA and EH&S) through automation, dashboards and reporting, and advanced data analysis.

COMPLIANCE REQUIREMENTS

- *Sarbanes-Oxley Act* (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 a large number of vendors, some with compliance concerns like conflict minerals, environmental standards and product component quality
- Ensuring compliance with 1,500 regulations

PREVIOUS PROCESS

Each group used spreadsheets to track requirements, controls and testing evidence. This made a consolidated view of compliance status impossible.

Staff spent thousands of hours emailing around forms and spreadsheets. They also wasted time chasing individuals for responses and compiling results.

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

AFTER IMPLEMENTING TECHNOLOGY

- Details of all compliance requirements are now maintained in a central library
- Details of policies, processes and controls are clearly linked to relevant regulations and compliance requirements
- In-depth status is immediately available by selecting a category (e.g., SOX, FCPA, PCI, SOC)
- Determining individual ownership for specific sets of compliance requirements is straightforward
- 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
- Unresolved issues are now escalated for senior management review

8 compliance processes in desperate need of technology

The last part of this eBook looks at 8 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.

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 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 huge. 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 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, and provide statistical data and trend reports that indicate changes in compliance risk levels.

The requirements for accessing and analyzing data for compliance are demanding, and truly delivering on this step involves using the right technology. 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 the 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 that 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 issue to the next level.

Some older software systems can't meet the huge range of incident monitoring and issues management requirements. Or it may 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 for 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 on the front lines.

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

For example, if you're required to comply with SOX, you can use automated questionnaires and certifications to collect individual signoff 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 signoff.

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

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

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

07
Manage regulatory changes

Regulations change constantly. 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, which 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 the arrival of software solutions, any regulatory changes meant huge amounts of manual work, 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) even lenient when you can demonstrate that your compliance process is strategic, deliberate and well-designed.

There are big efficiency and cost benefits to using a structured and well-managed regulatory compliance system. But those financial gains pale in comparison to the benefits of avoiding a potentially major financial penalty by replacing an inherently unreliable and complicated legacy system.

Technology evaluation checklist

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 or no IT intervention.

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.

CAN YOU ROLL OUT RAPID CHANGES AND UPDATES?

Your software should let you quickly reconfigure 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.

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 test millions of transactions.

A system that works well and transforms processing and response times can create whole new levels of engagement from users.

ARE YOU GETTING THE FULL STORY FROM YOUR DATA?

Data analysis must support rules-based controls and compliance testing. It should also support various 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 enterprise resource planning (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 the procedures performed.

DO YOU HAVE DASHBOARDS TO SHOW CURRENT COMPLIANCE MANAGEMENT STATUS?

We talked earlier about the importance of reporting for regulatory bodies, often in 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 (ERM) strategy.

Compliance executives and others need specific views into discrete compliance areas, getting not only an overall visual risk assessment for a particular regulatory requirement, but also insight into information such as the percentage and monetary value of anomalies identified, and the results of remediation efforts.

Ready to find out how ComplianceBond can simplify and centralize your compliance management?

For an assessment of how your organization can integrate Galvanize technology to transform your team's value delivery, call 1-888-669-4225, email info@wegalvanize.com or visit **wegalvanize.com**.

Galvanize
is now Diligent

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 a 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, a Diligent brand, is the leading provider of GRC software for security, risk management, compliance and audit professionals. The integrated HighBond platform provides visibility into risk, makes it easy to demonstrate compliance, and helps grow audit, risk and compliance programs without incurring extra costs.

wegalvanize.com

©2021 ACL Services Ltd. ACL, Galvanize, the Galvanize logo, HighBond and the HighBond logo are trademarks or registered trademarks of ACL Services Ltd. dba Galvanize.
© 2021 Diligent Corporation. All other trademarks are the property of their respective owners.