EBOOK

FEAR VS. COST:

Overcoming Compliance's Dual Challenges

RegScale

Executive Summary

Compliance officers across all industries and in large and small organizations are faced with dual challenges.

On the one hand, they are constantly in fear of failing an audit. They worry about the potential for irreparable damage to their own reputation and that of their companies. Officers are all too aware a single bad audit could result in significant fines – even possible termination.

Studies show cost of non-compliance to be **2.71 times higher** than compliance related costs[1]

Simultaneously, they are under pressure from all corners of their organizations to reduce costs. Companies are looking to save as much money as they can, especially in the current economic environment. Executives do not want to see compliance making a dent in their bottom lines, yet they need to keep up with compliance efforts, even as those efforts cut into corporate profits.

It's a double-edge sword – and it keeps compliance managers awake well into the night.

But it's not just compliance managers who are feeling the pressure. CEOs of smaller companies are also feeling the heat from multiple sets of rules and regulations.

As an example, at the U.S. Department of Defense, they worry about the ability of small businesses across their supply chain to meet government cyber security regulations. While DOD work is a great economic opportunity for smaller companies, it comes with a significant compliance burden to meet standards like the DoD's Cybersecurity Maturity Model Certification (CMMC) that calls for defense contractors to implement tighter cybersecurity and risk management protocols.

Unfortunately, many small contractors do not have the resources or skills to both comply with the regulation and track that compliance over time. As such, they are fearful they may lose their government contracts.

Clearly, both compliance officers of large companies and heads of smaller companies need to find a happy medium between doing what needs to be done to meet regulations and standards and managing the resources required to do it. They need to achieve compliance while controlling costs.

In short, they need to break the fear vs. cost cycle.

This ebook will show both groups how to achieve this common objective by employing a strategy that eliminates fear, reduces costs, improves productivity, and minimizes risk.

More Regulations and Complexities Feed Fear and Drive Costs

The fear and pressure being felt by compliance officers and CEOs are being fueled by many factors, all of which are intertwined.

THE GROWING SOPHISTICATION – AND NUMBER – OF CYBERATTACKS

There were more attacks in the first half of 2020 than throughout all of 2019.[2] Those attacks are becoming more sophisticated and hit all three components of the cyber security triad: confidentiality (an attempt to gain access to sensitive information), availability (attacks designed to take down networks, such as DDoS or ransomware attacks) and integrity (where an attacker makes users distrust the accuracy or quality of their data).

MISTRUST OF STORING SENSITIVE INFORMATION IN PUBLIC CLOUDS

Corporations are becoming hesitant to store proprietary information in public clouds. Organizations that do use public cloud providers need to be aware of the fine print included in those providers' shared responsibility models. These models typically assign security and compliance responsibilities over data to the customer as opposed to the cloud provider.

MORE REGULATIONS REQUIRING MORE DILIGENT COMPLIANCE EFFORTS

It's not unusual for a company to be simultaneously maintaining compliance with a bevy of regulations, including Sarbanes-Oxley (SOX), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and more.

By 2023, 65% of the world's population will have its personal data covered under modern privacy regulations.[3]

RISING FINES ASSOCIATED WITH NON-COMPLIANCE

Fines for non-compliance continue to rise across the board. A single Level 4 HIPAA violation, for example, begins at nearly $60,000 and goes up to $1,785,651.[4] This penalty almost tripled[5] over the last year. GDPR fines can reach up to €20 million (just under 24 million US dollars) and represent 4% of an organization's worldwide annual income. While these are two of the more well-known regulations, there are many others that organizations account for daily.

[1] Ponemon Institute and Globalscape True Cost of Compliance with Data Protection Regulations, https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study

[2] CrowdStrike 2020 Threat Hunting Report, https://www.crowdstrike.com/press-releases/crowdstrike-threat-hunting-report-reveals-rise-in-ecrime-during-pandemic/

[3] Gartner https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w

[4] HIPAA Security Suite, https://hipaasecuritysuite.com/hipaa-violation-fines-and-penalties-what-are-they-in-2020/

[5] Federal Register, https://www.govinfo.gov/content/pkg/FR-2020-01-17/pdf/2020-00738.pdf

The Need for a Better Strategy

This is not a winning formula for those who are struggling to maintain compliance and control costs while keeping the lights on. Many managers find themselves simply reacting to requests – and addressing those requests often takes much more time than it should. Implementing a new security measure in response to a regulatory change, for instance, could take months thanks to the backlog that needs to be groomed first.

Meanwhile, many CEOs of smaller companies do not even know where to begin to ensure compliance with regulations such as the CMMC. This standard requires all government contractors to meet basic security controls for data protection, which can be enormously challenging for an independent manufacturer that operates further down the supply chain.

If compliance officers and CEOs in companies of all sizes, in all industries, want to reduce their fears of non-compliancewhile controlling their compliance management costs, they need a better strategy. They need to simplify the processes they employ to ensure they remain continually in compliance with regulations and minimize vulnerabilities and risk. All the while, they must improve efficiency and reduce unnecessary time and costs.

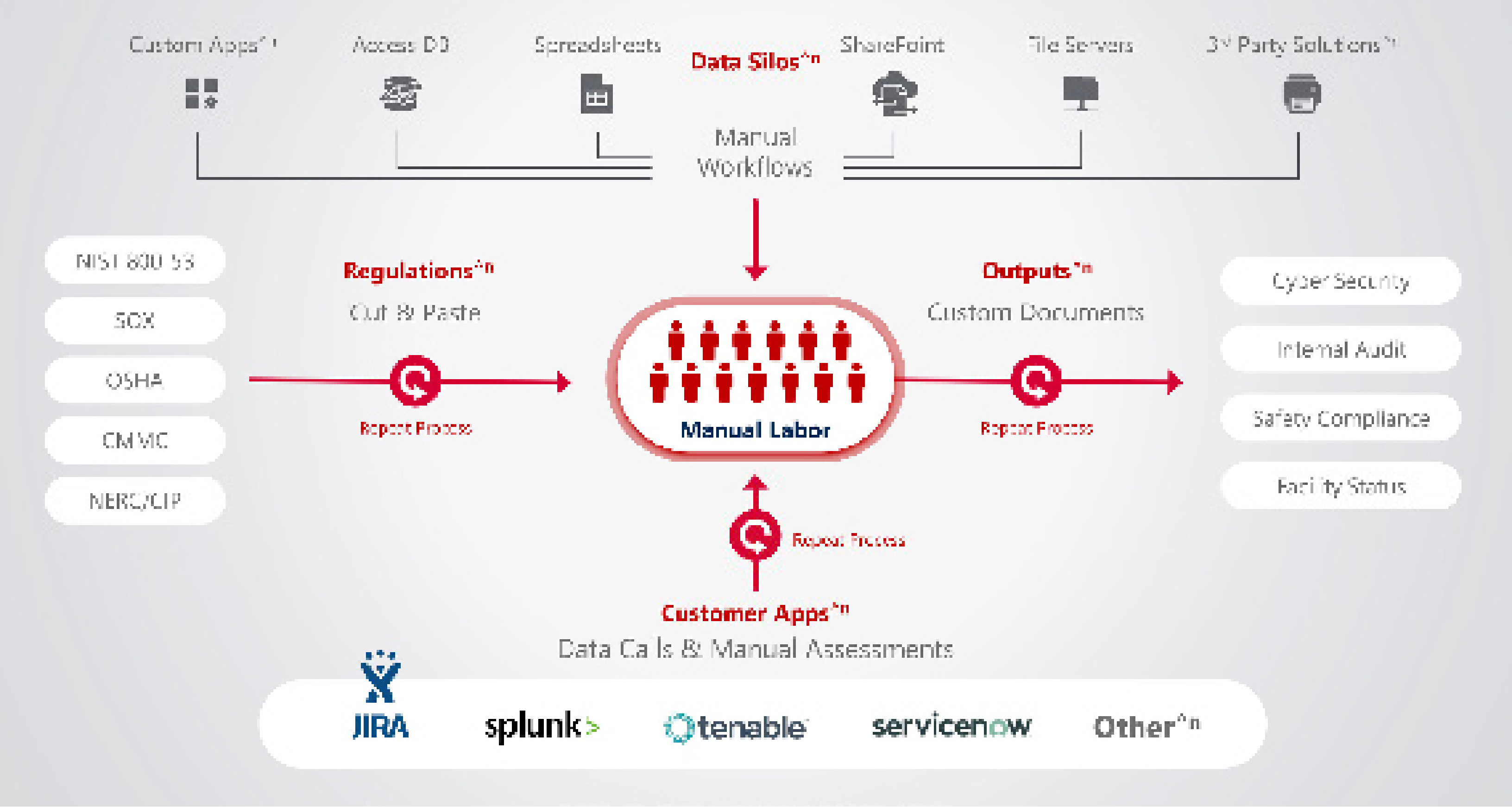
26% of compliance officers' time is spent establishing a liaison with different control functions within their organizations. Only 4% is spent amending policies and procedures.[6]

[6] Thompson Reuters Cost of Compliance Report 2019, http://financial-risk-solutions.thomsonreuters.info/Cost-of-Compliance-2019

Breaking the Compliance Management Complexity Cycle

At first, attempting this may seem overwhelming due to ever increasing demands for compliance and the complexities involved in addressing these demands.

And yet, solving the problem is as simple as breaking down the compliance management process into its core 4-dimensional pieces:



This legacy process is extraordinarily complicated, manual, costly, and lengthy. It generally involves:

STEP 1

ADDRESSING REGULATIONS

The first step in the process is understanding which framework or regulation an organization must comply with and then assessing the steps necessary for compliance. Most of the time spent in this phase is highly reactive as managers and others address changes in the regulatory environment. It's repetitive, time consuming, and unproductive.

STEP 2

DEALING WITH DATA SILOS

Accessing and managing workflows in spreadsheets, Word documents, SharePoint libraries, and other resources is next. These workflows usually exist in various departments and are siloed throughout the organization. As such, managers and CEOs must call people within these departments for the appropriate information and documentation – another archaic, manual, slow, and ultimately headache inducing process.

STEP 3

ACCESSING CUSTOMER APPLICATIONS

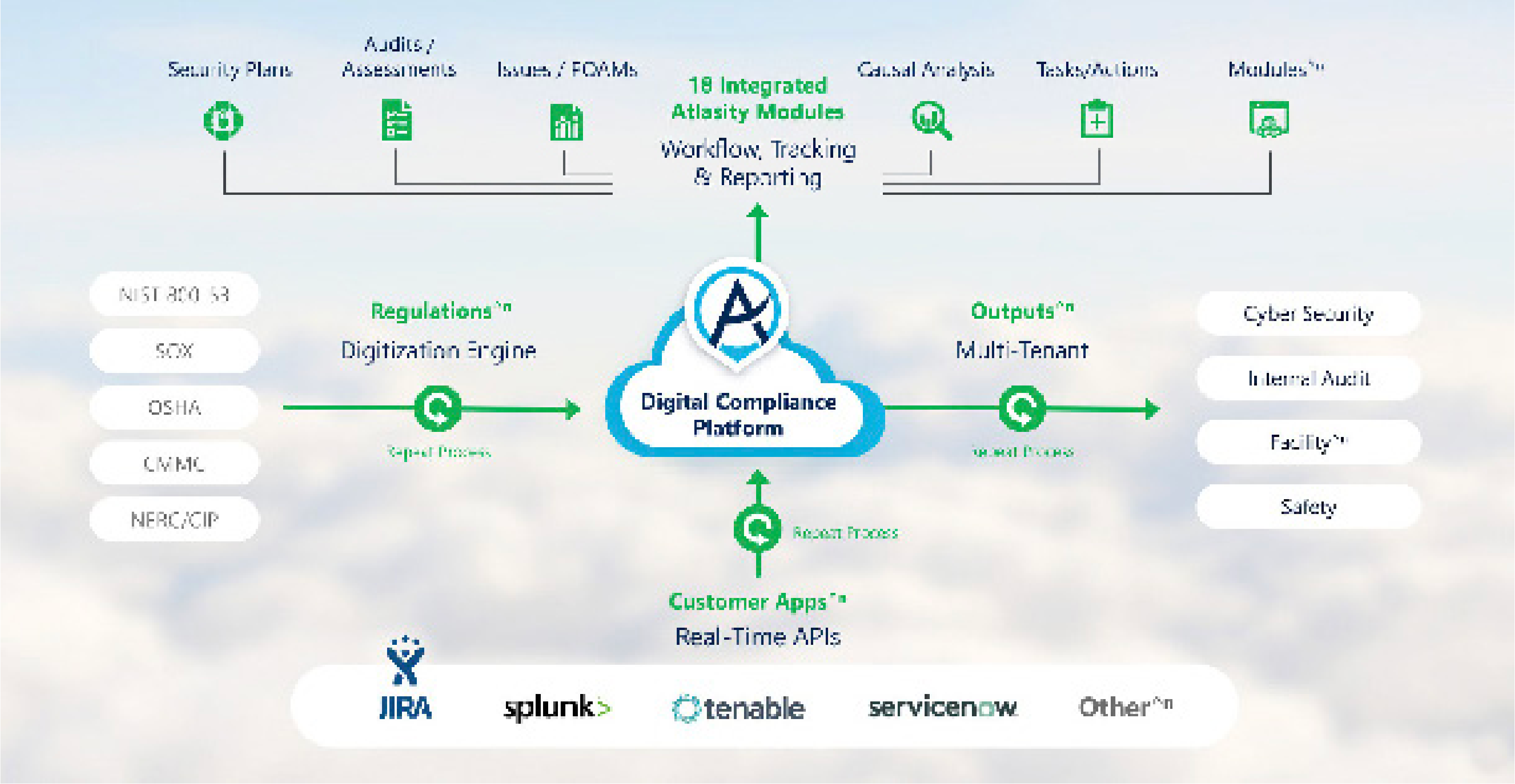
Customer applications are the authoritative sources of data that lives in the workflows. Organizations typically engage in manual audits and data calls to collect this information. This is a slow and expensive process that takes valuable time away from managers who would otherwise be engaged in more productive and value-added tasks.

STEP 4

DERIVING OUTPUTS FROM DIFFERENT SOURCES

Once the business units are contacted and customer applications are culled for data, managers and CEOs must review and collate these disparate outputs. Then, they must create artifacts for publishing to regulators, CISOs, internal audit teams and others. This extremely complex and lengthy process is particularly problematic when under pressure to deliver materials to the necessary parties at a specified time.

By automating and digitizing this 4-dimensional process, organizations can **save money, reduce risk, improve productivity,** and ensure they are continuously compliant.



With this approach, each phase of the compliance management process becomes integrated and continuous for greater efficiency and efficacy:

MANUAL REGULATIONS MANAGEMENT → AUTOMATED DIGITIZATION ENGINE

The regulation process becomes completely digitized, eliminating the need for prolonged manual processes. Managers and CEOs immediately understand the requirements they need to meet and the steps they need to take to ensure compliance. Best of all, compliance information moves from unstructured data (Word, PDF, etc.) to digital objects with real-time APIs that can communicate with the outside world.

DATA SILOS → CENTRALIZED INTEGRATED PLATFORM

All data is accessed through an integrated platform with instant access to multiple modules representing different business units and groups within the organization. Compliance managers and CEOs can easily access data and track and report on compliance in an on-demand fashion. All of the modules are tightly integrated to improve workflow and collaboration.

CUSTOMER APPLICATIONS → REAL-TIME APIs

Instead of manually collecting data, compliance managers and CEOs can get information in real-time, from anywhere and with no effort. Documentation will be automatically updated resulting in a continuous understanding of where a company is in the compliance process.

OUTPUTS FROM DIFFERENT SOURCES → MULTI-TENANCY APPROACH

Instead of having to go to different sources for information, compliance managers and CEOs can easily access reports and dashboards for each stakeholder group. They will have the information they need, when they need it, without having to manually ask for it. In addition, each group can have their own workflows, data schemas, and modules, allowing them to optimize for their specific requirements versus forcing themselves to fit a tool; all without the need for developers. The net result: less risk an d greater efficiency, resulting in a reduction of fear and cost.

An automated and digitized approach to compliance management yields several tangible benefits:

- Consolidation and automation = reduced costs and complexity resulting in greater efficiency and savings
- Real-time, on-demand insights = reduced risk and an assurance of accurate compliance data
- Greater transparency = more visibility and greater accountability
- Simplified process = fewer headaches and more time for proactive risk and compliance managementQuick results = no more scrambling and the greatly improved time to value

The net result: less risk and greater efficiency, resulting in a reduction of fear and cost.

The 4-Dimensional Approach in Action

RegScale works with a large state government agency building plans that show the organization is compliant with the Federal Information Security Management Act (FISMA).

The agency has deployed the automated and digitized approach outlined here. As a result, the organization is developing more accurate plans more quickly – in weeks as opposed to months. In addition to saving significant labor hours, the agency is also reducing the amount of cyber insurance it needs to pay, resulting in hundreds of thousands of dollars in savings annually. This customer saw a Return on Investment in under 6 months.

No More Fear

The fear – of failing an audit, of spending too much, of losing one's job, or of the potential for a data breach – is real. Those who are impacted know this all too well.

What they may not know is this fear can be conquered, the costs can be controlled, and the complexity can be managed.

Compliance management does not have to be an onerous and costly endeavor. It can be automated and simplified, allowing compliance managers, CEOs and others to spend less time worrying about compliance and more time growing their business.

Let us show you how to conquer your fears.

Contact us today to schedule a live demo of C2 Labs' Atlasity Integrated Compliance Management solution. We will help you revitalize and reinvent your compliance management processes.

Sometimes, compliance isn't the only problem. Technical debt and legacy systems limit your ability to automate your compliance processes. At C2 Labs, we believe your systems should be simple, consistent and transparent. If you need help modernizing your systems, schedule a no-cost discovery consultation with C2 Labs today. Our experts will partner with you to build and deliver continuously compliant solutions so you can break free from bureaucracy and drive meaningful change in your organization.

RegScale

Contact Us

info@regscale.com

202.991.7881

www.RegScale.com

1775 Tysons Boulevard, Fifth Floor

Tysons, VA 22102 USA