GAN INTEGRITY

Field Guide for Program Improvements

Improving and updating corporate compliance management can be overwhelming. The intricate web of internal processes, stakeholders, workflows, KPIs, and external factors like regulations make these systems, and the programs used to manage them, essential.

These methodical changes often necessitate a comprehensive overhaul of existing workflows, impacting multiple departments and requiring careful coordination. But, despite these challenges, making scalable updates is ultimately beneficial for organizations. These improvements allow compliance programs to scale more efficiently as the organization grows, adapting to new challenges and opportunities.

This field guide acts as a map to compliance management success, exploring do's and don'ts of improving systems, processes, and risk management efforts.

CONTENTS

WHAT'S INSIDE

Click on the section to go directly to that page

Pressure Is Growing

The need to improve compliance and disclosure programs is not an empty one. Regulatory bodies are paying more attention to how programs are run, and how they minimize risks.

The **U.S. Department of Justice's latest update to its Evaluation of Corporate Compliance Programs (ECCP)** guidance emphasizes the need for companies to prioritize modernizing their compliance programs, particularly in light of emerging technologies, complex risks, and data analytics.

Additionally, the DOJ now expects companies to leverage data analytics tools to enhance the efficiency and effectiveness of their compliance operations, ensuring that compliance functions have access to the same resources and technology used for business purposes.

Compliance risks are wide-reaching, as well. Anti-bribery and corruption (ABAC) efforts often fall under this domain, and penalties have teeth. Violations of the Foreign Corrupt Practices Act (FCPA) in the United States can carry both criminal and civil consequences. Organizations implicated in these face a variety of repercussions, including the ejection of any proceeds derived from the illegal activity in question, and substantial fiscal penalties. The largest penalty ever imposed on an entity in the context of a single FCPA-related enforcement action was nearly **$2.9 billion against financial giant Goldman Sachs** in 2020.

With areas of similarity to the FCPA, the United Kingdom's 2010 **UK Bribery Act** is a comprehensive anti-corruption legislation that criminalizes passive and active bribery, bribery of foreign public officials, and failure of commercial organizations to prevent bribery. Penalties for violations can be severe, including unlimited fines for companies and individuals, up to 10 years of imprisonment for individuals, and potential debarment from public contracts throughout the EU.

Penalties for poorly-run compliance programs extend beyond the US and UK, as well as into areas such as corporate due diligence initiatives. The European Union's new **Corporate Sustainability Due Diligence Directive (CSDDD)** is one such example of how these regulations are increasing pressure on organizations. Under the Directive, companies unable to comply with expectations face fines of 5% of yearly turnover.

Many Paths When it Comes to Software

So, with more eyes on programs, compliance teams across all industries are faced with the need to have a robust compliance management program in place. This isn't always an easy, seamless process, however.

The involvement of more internal stakeholders in technology and software purchases has increased significantly in recent years due to the growing complexity and impact of these solutions across organizations. As technology becomes more integrated into various business functions, decisions and input are required from a wider range of stakeholders to ensure the chosen solutions meet diverse needs, align with overall business strategy, and fit within budget and resource constraints.

Software is a significant investment across organizations. **According to Gartner**, by the end of 2024, we are expected to see an 8% growth in software spending compared to the previous year, surpassing $1 trillion USD. And when it comes to compliance management, IT and procurement teams are more involved in strategies and technology decisions.

A major question arises when planning compliance management updates- do you create your own system internally, or purchase one from a vendor?

According to Gartner,

by the end of 2024, we are expected to see an **8% growth in software spending** compared to the previous year, **surpassing $1 trillion USD**.

Why Do Teams Build Their Own Systems?

IT and procurement teams often encourage compliance teams to embrace internal buildouts of compliance management programs for several reasons:

Perceived Cost Savings

One of the primary motivations for building an in-house compliance management program, or certain areas of the program, is the perception of lower costs:

Initial Investment: Teams may believe that developing a custom solution will be cheaper than purchasing and implementing a third-party system. They often focus on the upfront licensing costs of commercial solutions without fully considering the long-term total cost of ownership.

Ongoing Expenses: There's an assumption that maintaining an in-house system will be less expensive than paying recurring subscription fees for a commercial product. However, this often overlooks the hidden costs (financial and otherwise) of internal development and maintenance.

Data Privacy and Control

Another significant factor driving the decision to build in-house compliance programs is the desire for greater data privacy and control:

Data Control: Organizations, especially those in highly regulated industries, may have concerns about storing sensitive compliance data with third-party vendors. It can be an assumption that building an in-house solution allows them to keep all data within their own infrastructure.

Customization: Teams often believe that a custom-built solution will allow for more precise control over data access, retention, and security policies tailored to their specific needs.

Challenges With Building Independent Compliance Programs

While the intention behind IT and procurement departments wanting to build their own compliance programs may stem from a desire for control and specificity, there are several reasons why this approach can be problematic.

Resource Duplication

Building independent compliance programs can often lead to a duplication of efforts and resources. Departments may invest time, money, and personnel into similar initiatives without leveraging existing frameworks or expertise due to decentralized systems and, oftentimes, lack of clear communication. This redundancy not only wastes valuable resources but also diverts attention from more strategic priorities.

Potential for Increased Cyber and Compliance Risk

Ultimately, the lack of a centralized, automated compliance program can expose organizations to greater operational and governance risks. When internally-built systems are not monitored continuously and rely on manual processes will often lead to non-compliance with policies and circumvention of controls and procedures. Such gaps, like insufficient access controls, can result in data breaches or, in more extreme cases, create unintended opportunities for cybercriminals to exploit system vulnerabilities.

In terms of compliance, disclosure, and third-party risks, decentralized systems often lack the workflows, automated alerts, and data needed to catch incidents well before they occur. Without a unified program that utilizes risk intelligence that updates within your program automatically, vulnerabilities may go unaddressed, leading to potential compliance-related incidents and significant financial and reputational damage.

Lack of Expert Support

While IT teams may build and maintain the programs, they have their own day-to-day priorities which often take precedence over outside requests. Any updates, malfunctions, or scaling up within the built-out system will probably not occur quickly. In addition, without continuous monitoring of these systems, it is more likely that cyber-related vulnerabilities will occur.

The Need for an Advisory Approach

While your internal IT team may implement your compliance process, whether at the outset or during maintenance, they will typically follow a prescriptive approach. In contrast, an external third-party vendor often takes on a more advisory role. Keep in mind that your internal IT team might lack expertise in this specific area, especially if you're their first 'client' for such an implementation. An external vendor, however, brings extensive experience from working with numerous customers with similar needs. This expertise allows them to provide valuable guidance during the initial implementation and help optimize your program during ongoing maintenance.

Lack of Maintenance and Ongoing Updates

Building software in-house requires substantial investment in development, maintenance, and ongoing updates. These expenses can surpass the costs associated with vendor-provided solutions, which benefit from economies of scale and shared development costs across multiple clients.

Additionally, after internal IT teams complete the development of an in-house solution, they are often reassigned to new projects. This can leave compliance teams managing outdated systems without access to the ongoing expert support needed to ensure the solution remains effective and up-to-date with evolving regulatory requirements.

Additionally, an external provider adds incremental value by continuously updating and evolving their platform. As part of their commitment to staying ahead of the competition, you will automatically benefit from system enhancements that your internal IT team may not be able to provide.

Taking the Middle Road

While some organizations risk building their own systems and face scalability issues, others take the middle road and rely on a combination of internal compliance management systems and small, low-priced vendors to supplement capabilities.

This can be risky as patchwork solutions like these often result in an even more decentralized and fragmented compliance infrastructure that struggles to scale as your business grows and regulatory requirements evolve. These disparate systems frequently lack seamless integration, leading to data silos, inconsistent reporting, and increased potential for compliance gaps.

Data Silos

Inconsistent Reporting

Increased Potential for Compliance Gaps

As your organization expands and faces more complex regulatory challenges, these cobbled-together solutions become inadequate and unable to provide the comprehensive risk management and oversight needed to manage complex supply chains, legislation, and stakeholder expectations. Moreover, the initial cost savings from using smaller, cheaper vendors are often outweighed by the long-term expenses of maintaining multiple systems, training staff on various platforms, and eventually having to invest in a more robust, unified compliance solution.

Leveraging multiple compliance systems can also lead to low adoption and limited stakeholder engagement, as users are forced to navigate a variety of platforms or processes with little consistency. This results in more training, more questions, and increased effort to ensure compliance with approval processes. A unified compliance solution, on the other hand, offers long-term advantages by providing employees with a consistent, all-in-one solution for compliance. This consistency makes it easier to adopt and ensures greater efficiency across the organization.

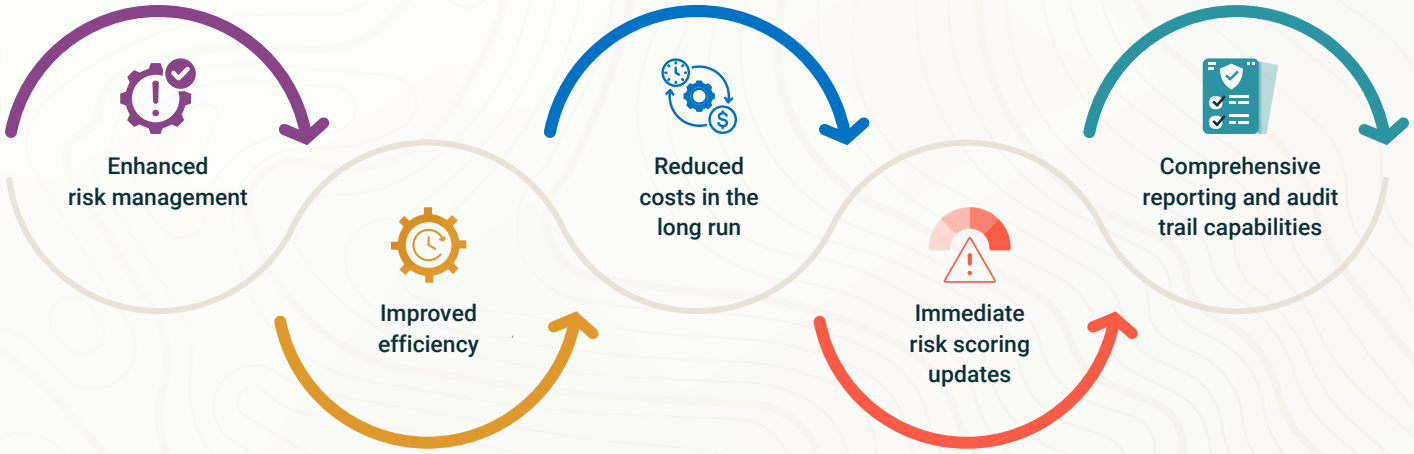
Ultimately, organizations find themselves needing to purchase a new, comprehensive program down the line anyway, making the initial patchwork approach a costly and time-consuming detour.

The Path Forward: Dedicated Compliance Management Software

We've explored challenges around creating your own solution, and taking the middle road of compromise. Now, let's dive into the benefits of investing in a dedicated compliance management system.

Compliance management software, done right, offers automated workflows that streamline processes and reduce human error, AI capabilities that can identify patterns and predict potential risks, and centralized processes that ensure consistency across the organization.

BENEFITS INCLUDE:



By leveraging non-manual tools that feature automation and workflow capabilities, organizations can stay ahead of compliance and disclosure requirements and better protect themselves against potential violations and their associated consequences.

Some key capabilities that set software services apart from manual, internal solutions include:

1. **Customization options that meet hyper-specific needs**
2. **Regular updates to keep pace with changing regulations**
3. **Robust security features to ensure cybersecurity and data privacy**
4. **Integration capabilities with existing systems**
5. **Scalability to grow with the organization**

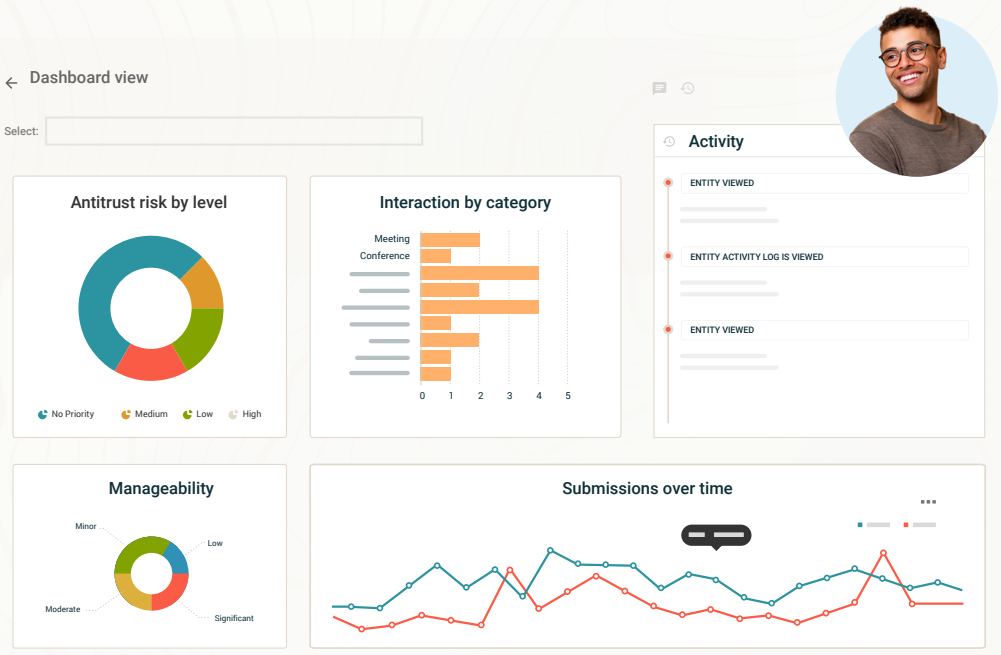
Your Toolkit: GAN Integrity's Solution

GAN Integrity offers comprehensive solutions for organizations that are facing the need to enhance their compliance programs through a combination of automation, streamlined workflows, and expert support.

Encoding business rules into operations and embedding ethics into every user journey enables companies within the platform to extend compliance practices across all business units efficiently. This approach allows for the automation of operations and the use of data thresholds as triggers, ensuring that tasks are completed and risk prevention audits are queued automatically, thus reducing the manual workload on compliance teams.

When it comes to the topic of costs, the Integrity Platform's focus on user experience and adoption makes it a cost-effective choice for organizations looking to improve their compliance programs without incurring excessive expenses as they grow their programs. The platform's intuitive design guides users through customized journeys with embedded instructions, ensuring that all touchpoints are impactful and easy to navigate.

> ***In terms of cost, it's important to consider the headcount, resources, and managed services which all add additional investment requirements, and costs add up over time. With manual, or pieced-together solutions, these line items add up.***
>
> ***With GAN Integrity, our level of automation delivers significant efficiencies, helping teams minimize the time and resources spent manually inputting data, compiling reports, correcting inconsistent data, sifting through false positive results, monitoring changes in risk data and more. Ultimately, this level of automation and mature features pay for themselves over time and help teams scale up in the future without straining budgets.***



Making the Case to Key Stakeholders: Answering Common Misconceptions

When making the pitch to procurement and IT teams that a dedicated SaaS compliance program is the right choice, there may be questions and resistance. Here is a guide to some questions that may come up, and how to make your case.

Isn't building my own program less expensive?

The total cost of ownership for an in-house solution often exceeds initial estimates. Ongoing maintenance, updates, and security patches require significant resources. Oftentimes, organizations will grow beyond their programs as new risk domains emerge, more users are added, and more processes are created. Eventually, teams will need to invest in additional tools that will add to costs down the road.

If I design my own program, aren't I in more control?

Developing and maintaining a truly comprehensive, effective compliance management system requires specialized knowledge in both compliance regulations and software development. Many organizations underestimate the complexity involved and lack the resources to truly implement the level of complexity needed to proactively manage risks.

With GAN Integrity, you drive your program. Our platform can be tailored to fit your organization, regardless of tech stack, region, or risk appetite. While we provide the tools, you control your program.

I can update in-house programs whenever I want, right?

As compliance requirements evolve and the organization grows, in-house solutions may struggle to scale effectively, leading to increased costs and potential compliance gaps.

There is also the element of time and resources. While compliance may need an immediate change or a new risk domain added, internal IT teams may already be stretched thin with their own priorities. This can leave teams waiting weeks or months for a software update, in the meantime they may fall behind on compliance requirements due to this delay.

GAN Integrity's experts are on hand at all times to assist with needed updates. With GAN Integrity, you will have a dedicated customer service manager who will know you, know your business, and always be ready to pick up the phone and work through any questions or help with program enhancements.

If I build the program myself, I don't have to worry about my vendor experiencing a cyber breach?

Commercial compliance management software typically offers superior cybersecurity compared to manually built, internal programs, due to their ability to provide advanced security measures, regular updates, and specialized expertise.

These solutions often include enterprise-grade features like robust encryption, multi-factor authentication, and compliance with stringent security standards, which are challenging and costly for most organizations to replicate in-house.

Everyone at GAN Integrity understands that data management needs to be handled with the utmost security. Our solutions are designed with security, data privacy, and compliance as a top priority.

Your Way Out of the Woods

Investing in dedicated compliance management solutions is a strategic decision that provides a path forward for your organization's approach to risk and ethics. A comprehensive, centralized platform like GAN Integrity is your map and toolkit needed to grow your compliance programs effectively, adapting to your evolving business needs and regulatory landscape.

By leveraging automation, these solutions help you stay ahead of potential risks, allowing you to proactively identify and address issues before they escalate. For compliance officers, this means less time spent on manual tasks and more focus on strategic initiatives that drive value for the organization and help you reach your destinations.

Moreover, these systems are designed with the future in mind, integrating emerging technologies and accommodating new regulations to help you chart your path and keep you ahead of emerging trends. A robust compliance management solution streamlines your current processes and positions your organization to navigate the complex forest of compliance with confidence and agility, ensuring you're always prepared for what's next.

If you have questions on compliance best practices or would like to speak to our experts to get started, request your personalized demo today.

GAN INTEGRITY
Because good deserves better™