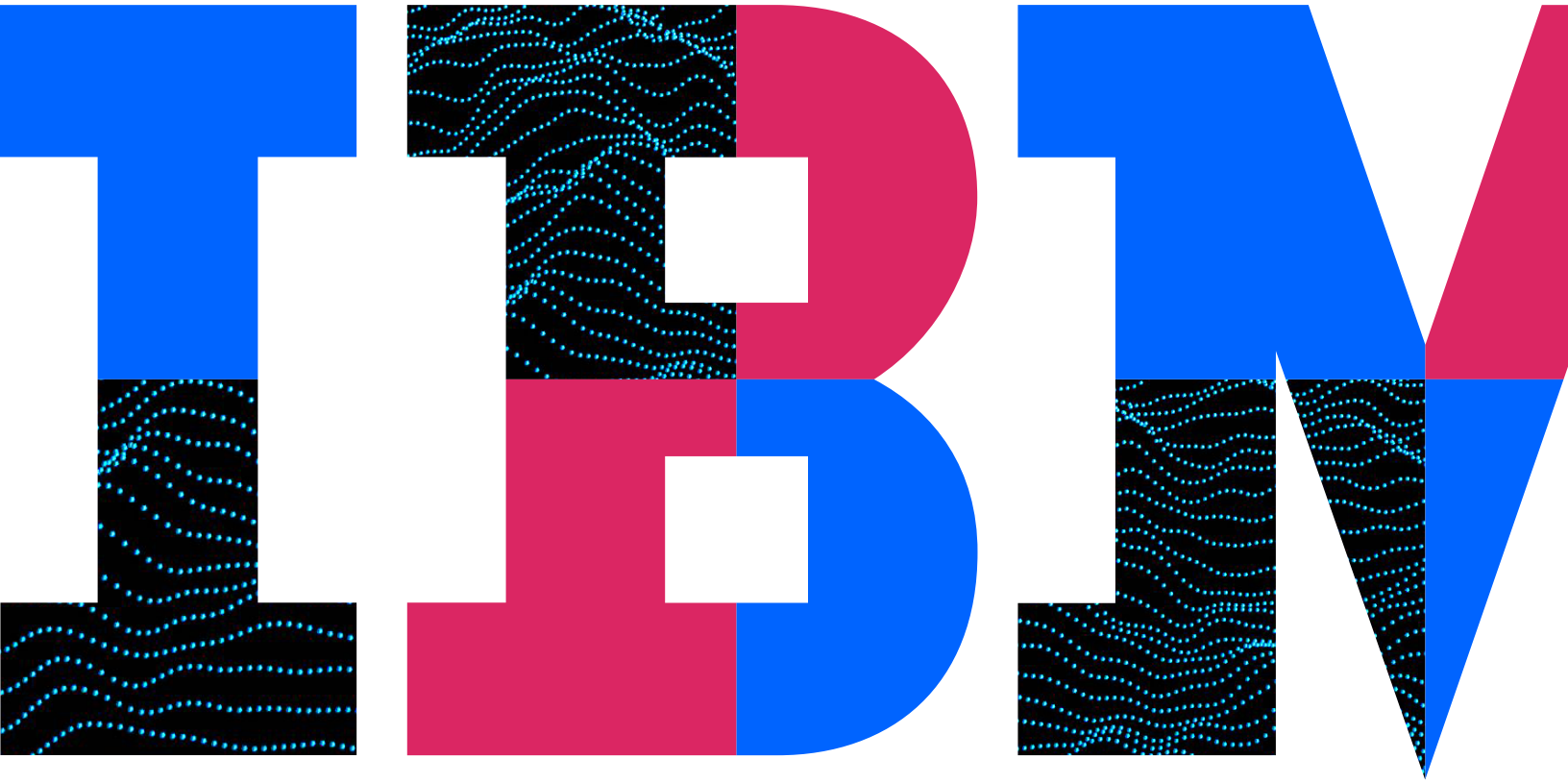
IBM Security
White paper

Get ahead of compliance

Continuous compliance enables you to build trust and protect your world.



IBM

Contents

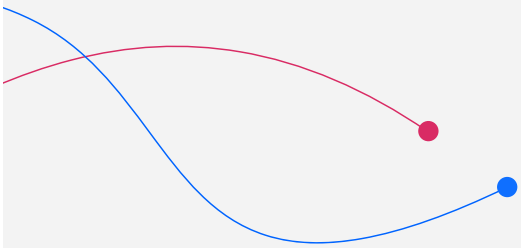
Key points

Get out of reactive mode and get ahead of compliance

Compliance strengthens your total security posture

Automating compliance leads to operational efficiencies

Compliance protects your customers and your data

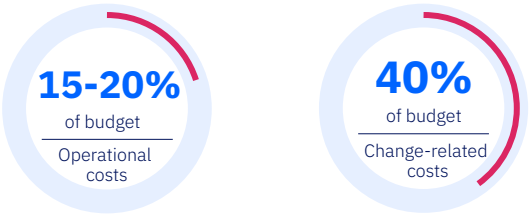


If you're not shipshape, you're shipwrecked

Managing risk and compliance in your business isn't a step, it's a journey. And like all good captains of industry, your goal for the journey is to avoid danger, protect the precious cargo in your business systems and conduct fair and profitable commerce. It will be a perilous journey, fraught with pirates, severe penalties and an unpredictable climate, but with a watertight ship, an experienced crew and a reliable map, success awaits.

While that may be a romanticized picture of compliance, the stakes are no less real. Many businesses have found themselves shipwrecked after straying from the course of compliance and courting risk too closely. With no shortage of cautionary tales to tell, every organization recognizes that industry and regulatory compliance requirements are the rules of engagement. They're not negotiable, they're not flexible and there are no shortcuts.

The cost of compliance can weigh heavily on a business' balance sheet. In the banking industry, governance, risk and compliance (GRC) activities account for an estimated 15 to 20 percent of operational costs and 40 percent of change-related costs.

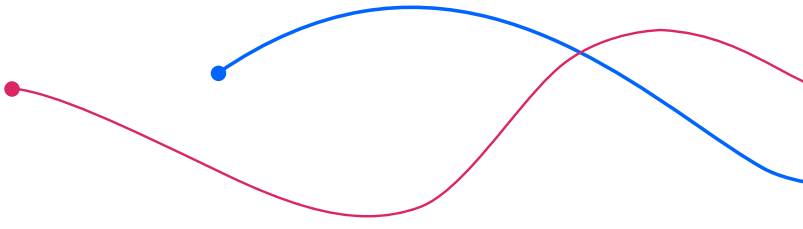


By 2021, banking experts predict that regulatory costs will consume 10 percent of revenue, up from four percent today.[1] Yet the cost of non-compliance can be much higher. New General Data Protection Regulations (GDPR), for example, call for fines of $1,200 for each customer record compromised by non-compliance. Compare that with the $2 per lost record recently levied against one global hotelier for a 2015 data breach, and what was a $700,000 penalty now becomes a $420 million penalty.[2]

Even where regulatory fines are less severe, failure to protect customer privacy can quickly reach millions of dollars, especially when factors such as lost revenue, customer defection and recovery costs are considered. According to the *2018 Cost of a Data Breach Study*, organizations can expect to lose $148 for each lost or stolen record suffered in a data breach, driving the average cost of a data breach to $3.86 million.[3]

All of these factors might seem to place companies between the devil and the deep blue sea where compliance is concerned. But there is a clear upside to compliance as well. Companies that navigate regulatory requirements effectively benefit from a stronger security posture, greater customer trust and higher operational efficiencies.

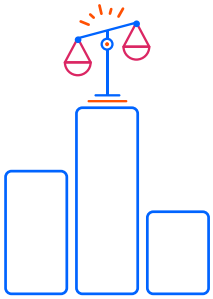
IBM Security Guardium Analyzer Overview. Watch the video.



Smooth sailing starts with security

It's easy to look at compliance as something you *have* to do, but that's only half of the story. Compliance is something your business should *want* to do because of the benefits it brings. Organizations that view compliance as a crown jewel in their security strategy demonstrate respect for both customer and data privacy.

What if your organization began to view compliance, not as a requirement, but as a competitive advantage? Imagine if your CEO saw "time to compliance" in the same light as "time to market." It's not so far-fetched. Consumers have become increasingly educated on their digital privacy rights and the perils of non-compliance, and consistently show a preference for brands that protect their privacy interests.



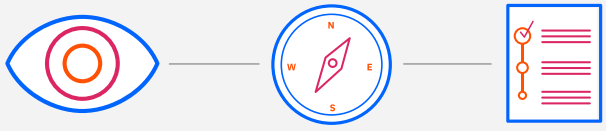
Getting ahead of compliance requirements also leads to heightened operational efficiency. Instead of the all-hands-on-deck model of reactive compliance, organizations that have clear visibility into future regulatory requirements can anticipate and avoid the turbulence of change, even as their competitors are drawn into its vortex. While the competition is rocked by waves of regulatory updates, your business can be enjoying smooth sailing on the other side of the storm.

Steering clear of danger in uncharted territory

Compliance officers need a microscope *and* a telescope to do their jobs: the one to comb through all their data, applications and endpoints for vulnerabilities, the other to predict and prepare for what lies ahead. Improved visibility into your current systems is necessary to establish a solid foundation of compliance. That's because cybercriminals overwhelmingly target known vulnerabilities. In fact, Gartner estimates that 99 percent of exploited vulnerabilities will continue to be those that are already known to security and IT teams.[3]

Once your organization has effectively battened down the hatches, it's time to look at the journey ahead. What are the emerging security trends that impact your industry? Where is the greatest potential for risk and exposure in the next few years? By mapping out future security requirements, organizations can get ahead of compliance rather than letting it control their course.

With improved visibility also comes better reporting. Auditing for compliance is a critical but time-consuming and error-prone process. It's often manually driven and may spread out across hundreds of databases and dozens of different database administrators. The ability to clearly identify and manage at-risk data, applications and systems across your organization leads to faster and more reliable audits, which reduces your operational costs and lowers your risk for non-compliance.



BigFix Compliance – Continuous Endpoint Policy Enforcement.

Watch the video.

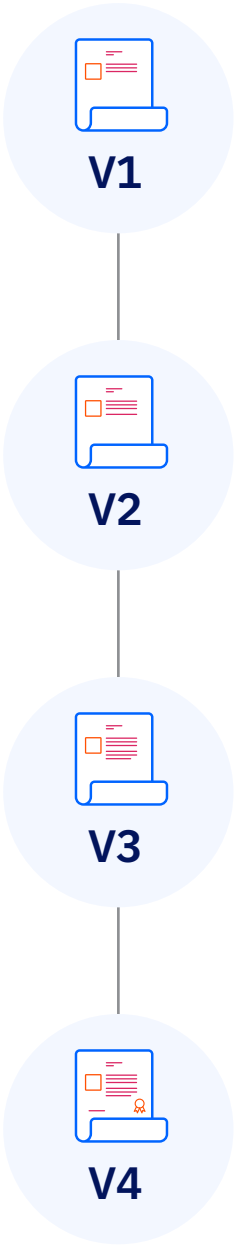
Stemming the tide of cybercrime

You can see compliance as medicine you have to swallow, but you'll miss out on many of its benefits if you do. Instead, look at compliance as exercising healthy security habits that will strengthen your business, your brand and your customer relationships. Better still, view compliance as a compact between you and your customers, a promise to protect them against the pirates, brigands and buccaneers who would steal their data and sell it on the black market.

Many of the security provisions set forth by governments and industries are based on very specific and very real threats aimed to disrupt global financial markets, expose healthcare patient data or undermine national security. It behooves every business to implement these security provisions and, in reality, a majority of these requirements are likely already addressed by internal security policies. Smart organizations recognize that, when compliance and security strategies are aligned, it sends a message to customers *and* fraudsters that security is a priority.

The challenge is that compliance is often a moving target. There are new regulations, with seemingly innocuous names but broad consequences such as GDPR, PSD2 and MiFID II. And existing regulations are constantly evolving, with dozens of new directives arriving each week. In this fast-moving environment, keeping afloat in a sea of change seems an almost impossible feat. How can organizations even think about getting ahead of the compliance curve? They can do it by partnering with compliance experts to help focus on the future, implementing cloud-based solutions to facilitate faster updates and leveraging AI-based technology to predict the course of compliance going forward.

Regulation and Compliance.
Watch the video.



Check yourself before you shipwreck yourself

Organizations understand that time, tide and compliance wait for no one, so they create internal processes to support continuous compliance. It may be monthly or seasonal, get pushed back or given priority depending on resource availability or urgency, but it gets done. Afterwards, the compliance teams can breathe a collective sigh of relief … until the next time.

By automating compliance audits and updates, organizations can simplify and streamline this process. Automation quickly checks existing data, applications and systems against the latest compliance guidelines and recommends or may even initiate steps for remediation. This not only accelerates the auditing/compliance process but also reduces the cost of compliance. Think of it as running your taxes through a trusted computer system before handing them off to your accountant.

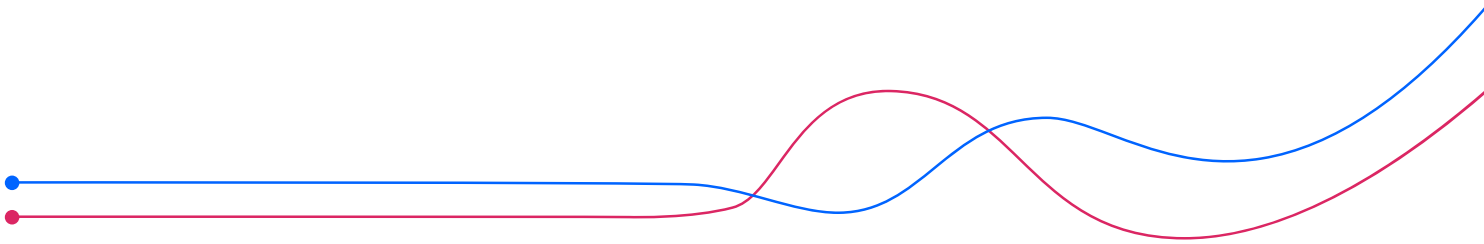
Automation is a valuable tool for internal auditing teams, as it allows them to quickly and reliably validate compliance prior to external audits. Automatically generated reports provide further validation that can be shared with external auditors, avoiding the disruption of a lengthy manual audit. When looking at compliance processes, remember this simple rule: If it needs to be regulated, ask yourself if it could benefit from being automated as well.

Create a safe harbor for your customers

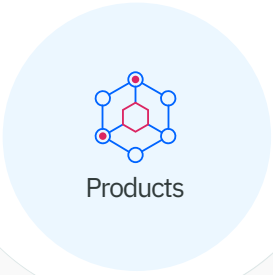
Successful organizations view compliance as an ally, not an enemy. Compliance provides a powerful band of protection around your data wherever it is — at rest, in transit, on mobile devices or stored in the cloud. By keeping data in a continuously compliant state, organizations establish themselves as a safe harbor for e-commerce and digital omnichannel interactions.

With IBM Security solutions, companies can get ahead of compliance with:

- AI-based software to predict regulatory trends
- Real-time monitoring tools to track compliance risk across your organizations
- Automation software to streamline auditing and reporting
- Cloud-based services to deliver invaluable expertise and insight



Get ahead of compliance with IBM Security products and services

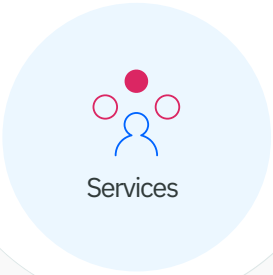


IBM Guardium

IBM BigFix

IBM QRadar

IBM Security Identity Governance and Intelligence



IBM Security Strategy and Planning Services

IBM Security Strategy Risk and Compliance Services

IBM Data Security Services

IBM Identity and Access Management Services

IBM Managed Data Protection Services for Guardium

Sources

1. Taming the High Cost of Compliance with Tech

2. The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.

3. 2018 Cost of a Data Breach Study: Global Overview

4. Focus on the Biggest Security Threats, Not the Most Publicized

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2018

Please Recycle

110-21811-USEN