# Regulatory Revenue? 10 Ways to Turn Compliance into a Competitive Advantage

## Summary

Not complying with regulations like DORA, GDPR, and HIPAA isn’t an option, but compliance doesn’t have to be an obstacle either. By making compliance a top priority and your business’s best friend, you can turn it into a competitive advantage.

[bws_pdfprint display='pdf,print']

The European Union's Digital Operational Resilience Act (DORA) goes into effect this coming January. Also, let's not forget about HIPAA, GDPR, CCPA, and the Telco (Services) Act—all of which also ask companies to change the way they protect their data and come with hefty fines for breaking the rules.

Then there's the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). NIST released an updated version earlier this year—the first major update to the CSF since 2014.

These regulations and frameworks are intended to make everything safer for everyone—companies and customers alike—through better data monitoring and more safeguards around things like data protection and data privacy. But where many companies go wrong is in seeing these new regulations and frameworks as burdens or hurdles as opposed to opportunities and launch pads.

"If we have to do something, let's make it useful," said Rob Glanzman, Global Strategic Alliances Principal Architect, Financial Services, Pure Storage, in a recent webinar: "Compliance as a Catalyst: Transforming Regulatory Challenges into Opportunities."

There's a lot to be said about turning compliance into a competitive advantage. Regulations like DORA, GDPR, and HIPAA are living, breathing documents that evolve to reflect the cyber dangers of the time. As such, they're kind of like the gatekeepers to cyber and data resilience, helping to ensure that only the most resilient companies are let into the cyber resilience realm to survive and thrive.

Read on to learn what it means to make compliance your company's best friend by turning it into resilience and revenue protection.

## The Cost of Non-compliance

First things first: Compliance does not guarantee security. As any CISO will tell you, cybercriminals are not concerned about companies finding a way to be compliant. What many cybercriminals aren't aware of, though, is how much better and easier things would be for them if companies didn't even care about compliance at all and if things like DORA and NIST CSF 2.0 didn't exist.

CSF 2.0, for example, includes several major additions to its first iteration, addressing organizational issues, risk management, and policies; guidelines to help companies measure their compliance level; additional mappings and references to other cybersecurity standards; and a new suite of guidance to help with implementation. It also goes beyond critical infrastructure to promote secure supply chains.

Companies that comply don't just win on the security side, they also win on the revenue side. A McKinsey survey of more than 1,300 business leaders and 3,000 consumers globally found:

- 40% of all respondents no longer worked with a company after a data breach.
- 52% of all business respondents stopped working with a company after a data breach.

- 10% of respondents stopped working with a company that experienced a data breach in the previous 12 months.

The cost of non-compliance?

Lost security, lost revenue, lost reputation, and lost customers.

## How to Be Response-ready

Now that we've established that not complying is not an option, we need to look at the changes you can start making right now to make compliance not just your top priority but also your business's best friend, no matter its size or vertical.

## 1. Data Clean Rooms

We hear more and more talk of "data clean rooms." A data clean room is a secure and controlled environment where multiple parties can share and analyze data sets without directly exposing or sharing sensitive or personally identifiable information (PII). It allows organizations (like advertisers, publishers, or brands) to collaborate and gain insights from combined data sets while maintaining strict privacy and security controls. Clean rooms help organizations comply with data protection laws like GDPR or CCPA, as the data is processed in a way that limits exposure of personal data.

## 2. Data Minimization

Minimizing the data reduces the organization’s risk in the event of a breach and aligns with GDPR’s “data minimization” principle. Collect only the data that is necessary for a specific purpose, and anonymize or pseudonymize personal data to reduce exposure.

## 3. Data Subject Rights Management

GDPR requires that individuals have the ability to exercise these rights and being prepared to respond quickly demonstrates compliance. Develop a process to manage data subject requests such as access, rectification, deletion, and portability of personal data.

## 4. Regular Data Audits and Recordkeeping

Regulations like GDPR mandate clear records of where and how personal data is processed, while the CSF 2.0 directive emphasizes logging and reporting of security incidents. Implement a data inventory or mapping tool to maintain a real-time overview of all data flows within the organization. Perform regular internal audits of data processing activities and maintain detailed records.

## 5. Data Encryption and Multi-factor Authentication (MFA)

The increase in data protection and compliance regulations required by various industries, countries, and regions requires companies to have a high level of built-in security and encryption capability. Encrypt sensitive data both in transit and at rest, and enforce strong access control policies, including MFA. Learn how FlashArray™ helps organizations achieve this high level of built-in security and encryption without making things more complicated. Learn more about why encryption is key to cost-efficient DORA compliance.

## 6. Incident Response and Breach Notification Plans

"I think more and more firms are becoming acutely aware of just how many systems they have, how many of those systems are critical, and in some cases, the horrifying reality of just how much or how little access they have to those systems when things go catastrophically wrong," said Michael Russo, Senior Director Global Strategic Alliances, Financial Services, Pure Storage, in the "Compliance as a Catalyst" webinar.

GDPR requires (and NIST CSF 2.0 recommends) breach notifications to be made within strict timelines (e.g., 72 hours under GDPR), and DORA focuses on operational resilience in the face of incidents. Being ready to respond quickly and mitigate damage is key. Implement a clear incident response plan (IRP) that includes detailed breach reporting timelines and procedures.

## 7. Appointing a Data Protection Officer (DPO)

Appoint a DPO or create a cross-functional data governance team responsible for overseeing compliance with data protection laws. A DPO acts as the point of contact for regulators and ensures that the organization’s data policies align with legal requirements. The team also ensures data is handled properly across departments.

## 8. Employee Training and Awareness

Human error is one of the leading causes of data breaches. Regular training helps employees stay aware of phishing threats, password hygiene, and the importance of following data privacy laws.

## 9. Data Lifecycle Management

GDPR and other regulations require organizations to only retain data for as long as necessary for the purposes it was collected. Proper disposal procedures minimize risk. Establish procedures for managing data across its entire lifecycle, including secure deletion policies for data that is no longer needed.

## 10. Inter-team Collaboration

Communication between departments is key to securing data across the organization. Data comes in from everywhere and the CISO needs to know everything that’s going on. This can only happen with collaboration. Read more about how to build a cyber-resilient future with inter-team collaboration.

## Pure Storage and the Cyber Resilience Advantage

Pure Storage focuses on making enterprises not just compliant but also cyber resilient by enabling them to recover quickly from setbacks and minimize or eliminate damage from cyberattacks.

“If we’re protecting against things like power outages and hurricanes, that’s one thing. But it’s not that simple anymore,” Glanzman said. “Because now we’re getting back to a point in time that there might be parts of that critical chain that have been impacted and others that haven’t, and it’s a waiting game to figure out when to bring them up and when they are designated clean either by the office of a CISO or a regulatory body.”

*Learn more about protecting your data. Get the “Definitive Guide to Data Protection.”*

Cyber Resilience Takes Teamwork

Explore [illegible] essly collaborate to minimize cyber [illegible] urvey results and analyst perspect [illegible] ce.

Learn How

WRITTEN BY:

Roger Boss