Key takeaways

The regulators made me do it: Compliance and cyber resilience

The ability to recover your data and keep your operations running is no longer optional — it's becoming a regulatory, operational, and competitive necessity. Across industries and geographies, the regulatory landscape is tightening. Organizations are no longer simply encouraged to protect their data — they are now required to prove they can. Consequences will be felt around the globe, with stricter enforcement models affecting especially critical infrastructure and supply chains.

In a recent Keepit webinar, Kim Larsen, CISO at Keepit and Paul Robichaux, Microsoft MVP and Senior Director of Product at Keepit, emphasized that compliance is becoming less about paperwork and more about operational proof: Can you actually recover your systems and data when it matters?

Actionable strategies for building resilience

1. **Know and prioritize your critical data**
   - Conduct a detailed data classification exercise.
   - Identify which data must be backed up, made immutable, and stored offsite.
   - Create a prioritized disaster recovery plan that aligns with internal expectations: Which systems and data must be recovered first to keep your business running?

2. **Modernize backup and recovery practices**

   The classic 3-2-1 rule of backup needs to be adapted to the cloud world – including different media types, off-site copies, and immutability:
   - 3 copies of your data
   - 2 distinct security domains
   - 1 immutable copy

3. **Strengthen security across hybrid environments**
   - Recognize that on-premises and cloud environments are interconnected — a breach in one can compromise the other.
   - Tighten segmentation, enhance security boundaries, and ensure monitoring across both infrastructures.

4. **Build a culture of resilience**
   - Security and resilience are enterprise-wide priorities, not just IT's responsibility.
   - Engage leadership and business units to embed resilience into daily practices — and improve regulatory posture together.

Read more about how we help our customers navigate complex compliance

5. **Prove, don't just plan**

   - Regulators increasingly require evidence of tested recovery, not theoretical policies.
   - Having a backup is no longer enough — you must demonstrate the ability to recover data and resume operations. Test restoration regularly and document outcomes to prove readiness.

"You don't have to wait for a regulator to tell you that resilience matters. Your ability to recover is part of your ability to stay in business — full stop."

Paul Robichaux, Senior Director of Product at Keepit

Prepare now: Here are some key actions	
Prioritize critical data and services.	☐
Update backup practices to include immutable and off-site copies.	☐
Regularly test recovery processes and document the results.	☐
Treat compliance not as a burden but as a business continuity strategy.	☐

Regulators worldwide are shifting focus toward proof of capability. Simply having tools is no longer enough – you need to demonstrate the ability to use these tools effectively. Even if your sector isn't tightly regulated today, that may not hold true tomorrow – with 1,579 new regulations, directives, and decisions adopted by the EU parliament within a year, regulatory changes will affect you soon. And even if you're not affected, your partners and customers likely are — and their compliance needs will extend outward to you.

Regulations aren't just piling up; they're raising the bar. Regulatory pressure is reshaping what "resilience" really means — and what your backup strategy needs to deliver. Organizations that act now will not only meet evolving regulatory demands but also lead the market in resilience, trust, and operational excellence.

Data governance report

Read our data governance report for more insight into how to best classify, protect, and recover your data so you can ensure operational continuity.

Download now

Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on Linkedin