Managing Regulatory Change for **Cybersecurity**

Spurred by digital transformation, cybercrime is a burgeoning issue that can expose financial institutions to massive financial and reputational losses.

Costs associated with managing regulatory change are also escalating. Chief Information Security Officers spend up to 40% of their time managing the compliance requirements of regulatory frameworks related to cybersecurity, rather than tackling cybersecurity itself[1].

Aimed at safeguarding against known risks, regulations change frequently as new threats emerge. One of the most costly and time-consuming challenges for any financial institution is the monitoring of ever-changing regulation. However, tracking all cybersecurity regulations continuously, understanding how they impact your business, and putting robust policies and controls in place are all vital to ensuring business protection and continuity.

Why does cybercrime hit financial services so hard?

Between November 2017 and April 2019 there were 3.5 billion attacks involving previously breached log-in data being used to crack open user accounts[2]. The financial sector was victim to 50% of all phishing attacks, and in the US alone 260 million[3] records have been hacked since 2016, at a cost of $38 billion (assuming average cost per stolen record of $141[4]).

Long-established financial institutions are reliant on interconnected networks and critical infrastructures. Risk is often heightened by legacy systems, which lack resilience and are easy prey for increasingly sophisticated cybercriminals. Digital-only financial services providers are also highly-susceptible to cybercrime, due to their extreme dependency on technology and third parties for service delivery.

[1] 2018 Financial Services Sector Coordinating Council
[2] 2019 State of the Internet/Security Financial Services Attack Economy Report, Akamai
[3] 2019 Cyber Risk for the Financial Sector, International Monetary Fund
[4] 2017 Cost of Data Breach Study, Ponemon Institute

Bolster cybersecurity compliance with CUBE

Cybercrime can cause catastrophic damage, ranging from loss of trust and reputation through to financial losses linked to fraud, litigation costs, customer attrition and lost revenues. Failure to comply with cybersecurity regulation can also result in punishing enforcement fines.

Due to the rapid pace of cyber-related regulatory change, CUBE offers your best defense:

- Have **complete visibility** of all relevant regulations
- Quickly align them with your business to ensure you have **compliant policies and controls** in place, which satisfy current regulatory frameworks
- Maintain a **defensible audit trail** that fully evidences your compliance actions and decision rationale

CUBE is for compliance, IT and cybersecurity teams wanting to take the heavy-lifting out of the regulatory change management process, and gain more time to create and apply effective policies and controls.

CUBE's AI-driven **Digital Regulation Platform (DRP)** replaces manual processes with intelligent automation. CUBE DRP captures global cybersecurity regulation, enriches regulatory content and then maps it to individual policies and controls, providing you with deep insight into the impact of regulatory change across all lines of business and jurisdictions you operate in.

Tackling regulatory change for cybersecurity, with CUBE

Underpinned by Artificial Intelligence (AI), Natural Language Processing (NLP) and Robotic Process Automation (RPA), CUBE delivers exceptional automation of the entire regulatory change lifecycle for cybersecurity compliance.

Key features

- **The world's richest source of global financial services regulatory intelligence**
- **A robust, end-to-end platform** that automates regulatory change across the enterprise, addressing many regulatory topics including cybersecurity, financial crime, AML, information assets, technology risk and more
- **Continuous horizon scanning** to quickly identify new, updated and upcoming regulation
- **Intelligent, automated mapping of all cybersecurity regulation** onto a CUBE-developed best practice cybersecurity taxonomy, or your own taxonomy, which may be based on any one of the many industry-standard frameworks (for example NIST, CSC, ISO and FAIR)
- **Automated regulatory gap analysis,** pinpointing the impact of regulatory change on your policies and controls, near-real time
- **Deep insight into the compliance status** of all cybersecurity policies and controls, enterprise-wide
- **Consistent application of the right compliant action, at the right time**

Why choose CUBE?

- **Vast time and cost savings** through automation and the elimination of repetitive manual processes
- **Continuous monitoring** of your compliance status, 365/24/7
- **Scalable compliance** accommodating exponential growth in information, regulations and business operations
- **Avoidance of enforcement fines** resulting from breaches of cybersecurity regulation and law
- **Reputational risk mitigation** which fosters trust and safeguards revenues
- **Defensible audit trail** enabling you to prove that you are managing cybersecurity in line with all current regulatory obligations
- **Lightweight, versatile infrastructure (SaaS)** that deploys quickly, scales easily and requires no internal IT overheads or maintenance
- **Seamless integration** with pre-existing systems and processes, via CUBE's Open API connectors

You may also like

FACTSHEET
CUBE DIGITAL REGULATION PLATFORM FOR ENTERPRISE REGULATORY CHANGE (DRP)

EBOOK
5 REASONS TO CONSIDER CUBE

VISIT OUR WEBSITE FOR LATEST NEWS, EVENTS, BLOGS, WEBINARS, WHITE PAPERS AND MORE

For a deeper dive
visit www.cube.global
or email connect@cube.global