GLOBAL CYBER REGULATIONS WHY YOUR ORGANIZATION NEEDS TO CONSIDER THIRD PARTY ASSURANCE REPORTING

Don't let cybersecurity risks catch you off guard - assess your exposure and protect your business today

BDO

NAVIGATING INCREASING THREATS AND REGULATIONS

With the ever-increasing dependence on technology and increased complexity in global supply chains, cyber threats are becoming more sophisticated, frequent and impactful. As cybersecurity incidents have increased sharply across the globe – now more than ever - companies and governments are aware of the need of robust cybersecurity risk management programs.

A recent research report (IBM) has shown that…

USD 4.82 MILLION

Average cost of a critical infrastructure data breach

83%

Percentage of organizations that have had more than one breach

USD 9.44 MILLION

Average cost of a breach in the United States, the highest of any country

Top 5 countries:

- USA: USD 9.44 million
- Middle East: USD 7.46 million
- Canada: USD 5.64 million
- United Kingdom: USD 5.05 million
- Germany: USD 4.85 million

In response to this threat landscape, governments across the globe are enacting cyber regulations to safeguard their citizens and businesses and to increase the overall cybersecurity posture and resilience.

EU

DORA

Focus: Digital Operational Resilience Act

Scope: Financial entities and critical third party providers

Date: Enforcement January 2025

NIS2 Directive

Focus: Network and Information Security

Scope: All organizations > 50 employees or turnover > €10 million

Date: Enforcement October 2025

Cyber Security Act

Focus: Framework for cyber certification for devices and cybersecurity services

Scope: (Smart) device manufacturers and service providers

Date: Enforcement June 2021

European Cyber Resilience Act

Focus: Cybersecurity requirements for products with digital elements

Scope: Manufacturers of digital devices

Date: Enforcement January 2025

BDO

NAVIGATING INCREASING THREATS AND REGULATIONS

US

SEC Cybersecurity disclosure

Focus: Proposed Rules on Cybersecurity Risk Management Disclosures

Scope: Market entities

Date: In effect 2018 - Rules proposed March 2022

NYDFS Cybersecurity Regulation

Focus: Proposed amendments to the Cybersecurity Regulation

Scope: Regulated financial entities

Date: In effect March 2017 – Proposed Amendments November 2022

UK

Cyber Resilience Legislation

Focus: UK building on NIS and NIS2 regulations

Scope: Critical providers of digital services and cybersecurity profession

Date: January 2022

CHINA

Cybersecurity law

Focus: Establishing a uniform regulatory regime for cybersecurity and data protection in China

Scope: Critical Information Infrastructure and Network Operators

Date: Enforcement June 2017

BDO

THE VALUE OF TPA

The cyber threat landscape poses significant risks for organizations today, and the consequences of a breach can be severe. From a good governance perspective and to mitigate these risks, organizations must take proactive steps to protect against these cyber threats by developing a comprehensive cybersecurity strategy and communicate on these efforts to relevant parties. These parties can be any stakeholder internally and externally – Board of Directors, management, investors, business partners, customers, regulators and others – who would benefit from these insights to make informed decisions. This is exactly where Third Party Assurance reports can be uniquely positioned – providing independent assurance on a subject matter such as a cybersecurity risk management program.

With the regulatory landscape evolving continuously, it is essential for organizations to be able to demonstrate compliance with applicable regulations. Not only demonstrating their compliance efforts towards the regulators but more importantly demonstrating - to relevant stakeholders - how protection of the organization's digital assets and integrity of the service provided is ensured.

Depending on the regulation, explicit requirements on the independent assessment of an organization's cybersecurity risk management program may be defined. If not driven by regulation, organizations should make sure they are prepared to provide assurance on their cybersecurity efforts. In the complex ecosystem and interactions between organizations we see today, supply chain attacks through third parties are a real threat.

SOC FOR CYBER

Demonstrating compliance with cybersecurity regulations can be challenging without the right tools and expertise. Organizations need to have an effective cybersecurity program in place that includes regular risk assessments, employee training, incident response plans, security audits, and necessary technical controls with regards to risk mitigation.

Third Party Assurance reports are well-equipped by nature to provide transparency (and independent assurance) on an organization's compliance efforts and make for a solid foundation in a Control and Compliance framework – increasing the organization's Governance Risk & Compliance capabilities.

The SOC (System and Organization Controls)-suit established by the AICPA has recently adopted a SOC for Cyber reporting framework next to other reporting initiatives (SOC 1, SOC 2, SOC 3 and SOC for Supply Chain) for different purposes. The SOC for Cyber framework provides a common and consistent language for organizations to communicate about, and report on, their cybersecurity efforts.

	SOC for Cybersecurity	SOC 1	SOC 2	SOC 3	SOC for Supply Chain
Who is this SOC for?					
Any type of Organization	●				
A Service Organization (One that provides services to user entities)		●	●	●	●
Entities that produce, distribute or manufacture products					
Purpose of the Report	Achieve the cybersecurity objectives	Achieve the service commitments and system requirements	Achieve the service commitments and system requirements	Achieve the service commitments and system requirements	Achieve the principal system objectives

SOC FOR CYBER

A SOC for Cyber report is an independent assessment of an organization's cybersecurity risk management program. It determines how effectively the program monitors, prevents and addresses cybersecurity threats. While not strictly mapping exhaustively into specific requirements of the different regulations – a SOC for Cyber report can provide a very strong baseline to demonstrate compliance with key domains and chapters in the regulations as illustrated by the SOC for Cyber Description Criteria to the right and in the table below.

Description Criteria of a Risk Management Program:

- Nature of Business and Operations
- Nature of Information at Risk
- Cybersecurity Risk Management Program Objectives
- Factors that Have a Significant Effect on Inherent Cybersecurity Risks
- Cybersecurity Risk Governance Structure
- Cybersecurity Risk Assessment Process
- Cybersecurity Communications and Quality of Cybersecurity Information
- Monitoring of the Cybersecurity Risk Management Program
- Cybersecurity Control Processes

This table shows an illustrative mapping between the EU DORA Regulation for the financial services sector including their ICT Third Party Service Providers and the Trust Services Criteria – one of many control frameworks which can be integrated in a SOC for Cyber report.

Pilar	Summary	Trust Services Criteria
1. ICT Risk Management	Risk Management Framework and methodology	CC3 Risk Assessment CC5 Control Activities
2. ICT Incident reporting	Early warning indicators and major incident reporting to the regulator	CC7.3 Security Incident Evaluation CC7.4 Security Incident Response
3. Digital Operational Resilience Testing	Risk based testing including Threat-Led Penetration Testing (TLPT)	CC4 Monitoring Activities CC7 System Operations
4. ICT Third Party Risk Management	Information Security Requirements between financial entities and ICT third-party providers	CC9 Risk Mitigation
5. Information and intelligence sharing	Interaction and sharing within the financial services ecosystem	CC2.3 Communication with external parties

HOW BDO CAN HELP

Assess the organization's current cybersecurity risk management program

Conduct a readiness assessment and gap analysis and recommend remediation strategies

Provide Attestation reporting (e.g., SOC for Cyber) on the organization's cybersecurity risk management program and effectiveness of the related processes and controls in place

Questions? Do not hesitate to contact our experts:

CHRISTOPHE DAEMS
Partner TPA
BDO Belgium
christophe.daems@bdo.be

MICHAEL KRIVAK
Audit Partner SOC
BDO USA
mkrivak@bdo.com

MARTIN HORICKY
Partner
BDO Czech-Republic
martin.horicky@bdo.cz