Cyber resilience in the European Union, it is time to act!

EY

Building a better working world

Overview

The European Union (EU) has been increasingly addressing the issue of cyber risk and recognizing the need to organize itself on a European scale to adopt a proactive defense by increasing its cyber resilience posture. The strategy mainly focuses on essential or critical sectors by imposing clear and precise requirements for compliance.

Let's talk about cyber resilience

Cyber resilience describes the organization's ability to quickly anticipate, protect, detect, respond to, and recover from a major IT security incident. With the increase in the digitalization of professional activities and the cyber attacks that come with it, cyber resilience has become a major strategic challenge for all companies. The European Union has observed a 26% increase in attacks in 2022. Even more disturbing, according to the Dell Technologies Global Data Protection Index Report, 86% of businesses globally have experienced a cybersecurity incident in 2022. The consequences of a security breach can be disastrous, ranging from loss of sensitive data to loss of customer trust and destruction of the company's reputation. It concerns everyone from very small to large worldwide organizations!

Therefore, adopting an efficient active defense-in-depth approach has become vital when facing the inevitable cybersecurity attack.

A cyber-resilient European Union

Facing these assertions, the European legislation has been revised and has already taken several measures and obligations to strengthen cyber resilience on a European scale. Some noteworthy actions have emerged as a result:

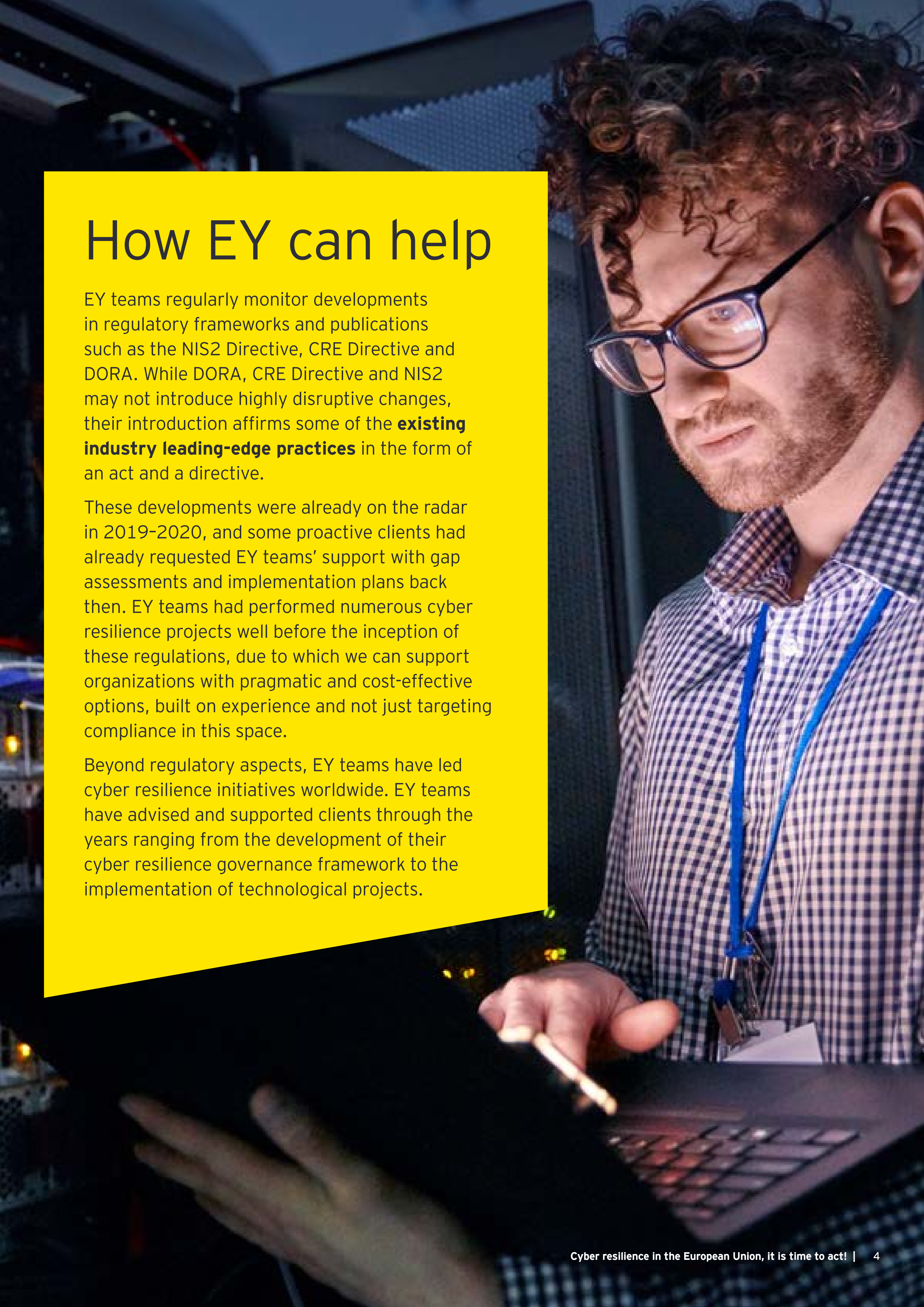
- **NIS2 directive (for Network and Information Systems),** beyond its desire to harmonize cybersecurity requirements at a European scale, aims to strengthen cyber resilience measures for national players deemed essential in a large number of defined critical sectors (energy, transport, health care, public administration, etc.).
- **RCE (Resilience of Critical Entities) directive** is similar to NIS2 and imposes the need for a national strategy to enhance the resilience of critical entities that provide critical state services.
- **DORA (Digital Operational Resilience Act)** exclusively covers the financial sector and tends to create a security framework at a European scale, focusing its requirements on the strong issues of cyber resilience.
- **CRA (Cyber Resilience Act)** is the proposed regulation on cybersecurity requirements for products with digital elements that strengthen cybersecurity rules to ensure greater resilience for hardware and software products.

In summary, the EU is taking important steps to strengthen cyber resilience and foster closer international cooperation on cybersecurity. All these newly emerging regulations demonstrate a dynamic desire to build a coherent cybersecurity and resilience framework for better coordination between countries, and alignment of security measures and organization against cyber attacks. The European Union Agency for Cybersecurity (ENISA) has been collaborating with European member states to determine the most effective practices in accordance with the regulations set forth in the NIS1 Directive and disseminate them among its stakeholders. The organization is committed to aiding EU member states in adopting the updated regulations outlined in NIS2 and a fresh set of regulations encompassing the Digital Operational Resilience Act (DORA) and those that will be established under the Cyber Resilience Act (CRA), acting at scale and coherently.

Among the many points of agreement between these directives to reinforce cyber resilience in the EU, we highlight the following elements:

1. **Harmonization of cybersecurity measures** — A common security reference basis and framework will be defined in order to attune cyber resilience capabilities and measures.
2. **Definition of a precise and robust risk management framework** — Entities are required to establish and maintain an ICT risk management framework that identifies, assesses and manages risks associated with their ICT systems. The framework should be composed of ICT strategies, policies, procedures, protocols and tools.
3. **Reinforcement of surveillance activities** — Authorities will be definitely more involved in monitoring entities' compliance endeavors.
4. **Obligation of detailed reporting** — Emphasis will be put on the duty to report major cyber incidents to authorities (within undue delay) aiming to increase collaboration between EU states.
5. **Encouraging the exchange of cyber threat intelligence and information** — Collaboration between partners and competitor businesses will be enforced by sharing CTI and information (e.g., IoC, attack mechanisms, threat actors and objectives).
6. **Designation of a single point of contact (SPOC)** — The SPOC will be responsible for fulfilling all reporting requirements outlined in the directive, including incident reporting.
7. **Inclusion of the supply chain (including third-party ICT)** — Regulations include all aspects of the supply chain in the cyber resilience approach, which is increasingly becoming a vector of cyber attacks for malicious actors. One of the aspects of these legislations is that "critical" ICT providers are now fully part of the ecosystem and need to become compliant also.
8. **Power to sanction organizations guilty of noncompliance** — Financial and administrative penalties will be imposed on organizations found to be in code violation. These sanctions can also apply to "critical" third parties' ICT.

All these directives are very challenging for organizations and are stirring up a lot of strategic and operational questions, such as "Can I share such sensitive information with competitors?" Or "How should I interact proactively with my critical ecosystem?" Consequently, organizations (including critical ICP providers) must strengthen their cyber resilience posture to be ready for the imminent major cyber attack, which might be "the one".



How EY can help

EY teams regularly monitor developments in regulatory frameworks and publications such as the NIS2 Directive, CRE Directive and DORA. While DORA, CRE Directive and NIS2 may not introduce highly disruptive changes, their introduction affirms some of the **existing industry leading-edge practices** in the form of an act and a directive.

These developments were already on the radar in 2019–2020, and some proactive clients had already requested EY teams' support with gap assessments and implementation plans back then. EY teams had performed numerous cyber resilience projects well before the inception of these regulations, due to which we can support organizations with pragmatic and cost-effective options, built on experience and not just targeting compliance in this space.

Beyond regulatory aspects, EY teams have led cyber resilience initiatives worldwide. EY teams have advised and supported clients through the years ranging from the development of their cyber resilience governance framework to the implementation of technological projects.

Act now with EY guidance!

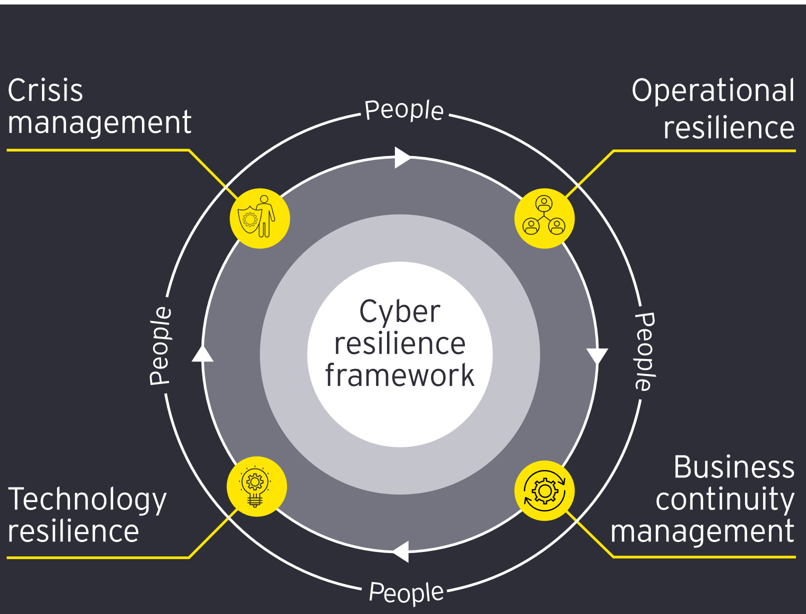
EY Teams have developed a cyber resilience framework that meets worldwide leading practices and recognized standards, an outcome of a global collaboration within the EY cyber resilience professionals' network.

Our global approach is oriented through four major pillars.

External forces are rapidly changing customer needs and expectations, demanding a new resilience model.

Cyber resilience offerings enable the investment in business continuity management (BCM) to be more fully leveraged and optimized, improving the ability to respond to rapid onset, high-impact cyber threats not traditionally covered by BCM.

Offerings are aligned to each respective phase within the Cyber Resilience Cycle.



Cyber operational resilience

Standardize the current Enterprise Cyber Resilience approach against leading practices or established standards to identify existing gaps, key assets, and business roles to support the cyber resilience activities. Cyber resilience is not only about technology capacity but also the preparation and operationalization of processes for helping to manage uncertainty and being able to react from a business perspective without IT systems available.

Cyber business continuity management

The framework helps ensure resilience and robustness in business operations against various threats, incidents and disasters that can have catastrophic effects on business.

Cyber technology resilience

The strategies offer the ability to maintain acceptable service levels through and beyond severe disruptions to critical processes and the IT systems that support them.

The consulting on technologies helps implement and ensure a robust cyber resilience posture.

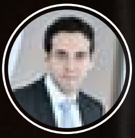
Cyber crisis management

EY teams help prepare for and assist in cyber crisis management and support organizations to better navigate through any stage of a crisis.

When a real cyber crisis happens, EY teams assist the executive management as well as the operational team to take the correct actions.

Meet EY cyber resilience leaders

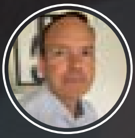
EY teams can assist organizations in Europe and worldwide to implement an efficient and pragmatic cyber resilience program.



Laurent Peliks
Partner,
Cybersecurity,
Ernst & Young
Advisory

Laurent Peliks leads Cyber Resilience in EMEIA (Europe, Middle East, India and Africa). He has more than 20 years of experience in assisting organizations in building and implementing their cyber transformation program and strengthening their cyber resilience capabilities.

Laurent has led several crisis management, business continuity and disaster recovery projects and also managed cyber attack remediation for companies worldwide and public operators.



Paul Robertson
Partner,
Cybersecurity,
Ernst & Young LLP

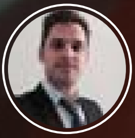
Paul leads Cyber Resilience in UKI with a focus on both preparedness and response. He has spent over 20 years building and delivering resilience capability for some of the largest businesses and agencies.

Having started out in disaster, emergency and incident management, time with the World Health Organization and supporting response to some of the most significant cyber attacks, Paul has been at the heart of major incident resilience for all of his career.

Alessandro Frenza
Director,
Cybersecurity, Ernst
& Young LLP

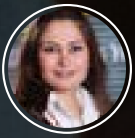
Alessandro is a part of the UK Financial Services Advisory – Cybersecurity team. He has over 20 years of experience in cybersecurity strategy, risk management, security transformation program, cyber resilience, cyber assurance, cyber maturity and controls assessments.

He has experience in supporting C-level executives in the Financial Services sector to define their cyber strategy and execute their cyber transformation programs and has led complex multinational projects leading technically skilled individuals to support the business through security transformation.



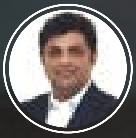
Stéphane Brebion
Manager,
Cybersecurity, Ernst
& Young Advisory

Stéphane Brebion (Cybersecurity Manager) leads Cyber Resilience in Europe West alongside Laurent. He has more than nine years of experience in assisting organizations from different verticals in assessing cyber resilience maturity while designing and implementing cyber resilience transformation programs at a large scale, and strengthening their cyber resilience capabilities. He supports organizations from technology, operational, and business perspectives.



Salam Shouman
Director,
Cybersecurity,
Ernst & Young
Jordan

Salam comes with 18+ years of professional experience in cyber resilience and cyber transformation advisory services. She has a Bachelor's degree in Computer Science and is a Certified Information System Auditor (CISA) and a Certified Information Security Manager (CISM). Salam is a member of the ISACA and has been certified in ISO 22301, ISO 27001, COBIT 5, Microsoft Software Asset Management (2006), NIST Foundation, ITDR implementor and ITIL V 3.0.



Pradeep P Eledath
Partner,
Cybersecurity,
Ernst & Young LLP

Pradeep leads the Resilience Center of Excellence at EY India. He has 28+ years of experience in Information Risk Management, Business Resilience, Technology Resilience and Cyber Resilience. He comes with diverse experience delivering resilience engagements across sectors like Insurance, Defence, ITeS, Aviation, Financial Services, Telecom and Automobile including running a cybersecurity consulting startup. Pradeep uses his experience in cyber defense to provide value to C-suite executives in managing complex cyber and non-cyber incidents.

Reference to articles on cyber resilience at EY

- Cyber resilience: Evidencing a well-thought-out strategy
- Baking cyber resilience into one's digital transformation program
- Decoding DORA and NIS2: how can your organization prepare?
- How to prepare for the Digital Operational Resilience Act?
- Cyber Resilience Through A Risk-Based Approach | World Government Summit

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

EYG no. 009857-23Gbl

BMC Agency
GA 13452425

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com