

An underwater photograph of a diver in a dark wetsuit and blue mask, swimming towards the camera. Sunlight rays penetrate the water from the top, creating a dramatic, high-contrast scene. A yellow rectangular frame is overlaid on the left side of the image, containing text.

Are you prepared to dive in the GDPR challenges towards compliance & operationalization ?

June 2019

■ ■ ■ ■
The better the question. The better the answer.
The better the world works.

The EY logo, consisting of the letters 'EY' in a bold, white, sans-serif font. A yellow diagonal bar is positioned above the 'Y'.

Building a better
working world

Introduction



**Ioannis
Fragkoulopoulos**

Senior Manager |
Cybersecurity & Data
Protection Services

Leading Digital Resilience as well as the Data Protection related solutions with special focus on regulatory compliance.

... member of a
high performing team!



>300

Cyber professionals in CESA



50+

Countries the team
has served worldwide



15+

CVEs from top end
Vendors



100+

Certifications collectively

... providing top end
cybersecurity solutions!

Cybersecurity strategy
& management

Digital identity & access

Data and application protection

Privacy

Cyber threat Management

Respond

Cybersecurity Compliance and
Standardization

IoT/ OT Security

Typical approach to compliance



Assess

Gap analysis & remediation/
compliance planning



Implement

Implementing privacy & data
protection **policies and
procedures**



Operationalize

1. Accountability / Data Subjects
2. Data protection
3. Ecosystem

Operationalization meaning...

Minimum documentation required to demonstrate compliance, e.g.:

- RoPAs
- DPIAs
- Policies & Procedures
- Compliance Plan



- IT systems
- 'Knowing where our data is'
- 'Erasure and record retention'

- Procurement Process
- Contracts
- Third Party Risk Assessment
- Third Party Audit

Accountability

Accountability

Data protection

Ecosystem



Capabilities needed
(Technology)

- Basic GDPR documentation
- Consents Management
- Data Subject Rights Management

Data protection

Accountability

Data protection

Ecosystem

It is critical to articulate the business impact of cyber risk at board level down. This can be achieved by defining cyber risk appetite and metrics, and by producing accurate and up-to-date reports that enhance decision making.



Capabilities needed

- Cyber and education awareness
- Board level support
- Cyber risk management
- Cyber quantification

16%

of organisations state that their reporting of information security meets their needs

28%

of organisations say the maturity of their cyber metrics and reporting is poor or non existent

82%

of boards fail to make cyber security a strategic agenda item

Ecosystem

Accountability

Data protection

Ecosystem

Third Party Risk Management (TPRM) is the oversight of key service providers who contribute to operations. This can be achieved by defining cyber risk appetite and metrics, and by producing accurate and up-to-date reports that enhance decision making.

Capabilities needed

- Technology enablement
- Process improvement and redesign
- Third-party Risk as a Managed Service (TPRMS)
- Market utility
- Assessment execution

60% of organisations that identify fourth parties do not maintain an inventory for monitoring and governance purposes

44% of organisations have experienced data breaches that happened at the third party

Ecosystem

Accountability

Data protection

Ecosystem

Classification of Data Handled by Vendor	Examples of Type of Data Handled by Vendor	Example of Vendor Business Relationship
Tier 1 Vendor Highly Confidential	<ul style="list-style-type: none"> Protected health information Medical records Patient /member information Treatment & condition information Credit card information 	<ul style="list-style-type: none"> Member address Phone number Biometric info Email address Date of birth
Tier 2 Vendor Confidential	<ul style="list-style-type: none"> Payroll information Employee performance data HR and personnel records Proprietary and trade secrets Proprietary code & business logic 	<ul style="list-style-type: none"> Investigations Tax information Employee SSNs Highly sensitive reports
Tier 3 Vendor Internal Use Only	<ul style="list-style-type: none"> Reports Assessments Findings and recommendations Strategy and roadmap documents Internal company memoranda Trade secrets 	<ul style="list-style-type: none"> Budgets Financial performance data Projections Departmental memos/reports
Tier 4 Vendor Public Distribution	<ul style="list-style-type: none"> Marketing and promotional materials Mailings and solicitations Public relations Campaigns and outreach 	<ul style="list-style-type: none"> Telemarketing Surveys Advertising material Web and media
		<ul style="list-style-type: none"> Outsourced software development Outsourced software maintenance and support Customer/Member helpdesk Claims processing Mail/Envelope stuffing and fulfillment
		<ul style="list-style-type: none"> Payroll and check printing services Benefits administration services Tax compliance services HR consulting and outsourcing services Mission critical consultants and contractors
		<ul style="list-style-type: none"> Professional services firms Consultants and advisory firms Professional service contractors Law firms (e.g. contract review, regulatory advisory) Business and operational auditors
		<ul style="list-style-type: none"> Advertising agency Event marketing firm Web-design and digital media services Printing and graphics design Marketing and survey companies

We have identified the following priority areas to focus on...



Technologies for demonstrating
GDPR
Accountability



Consents
Management



Data Subject
Rights
Management



Cyber Risk
Management



Third
Party Risk
Management

How can we help?

Digital identity (DI)

- ▶ Access enforcement
- ▶ Identity governance administration
- ▶ Certificate management
- ▶ Cloud Access Security Broker
- ▶ Operation support services
- ▶ Application onboarding service
- ▶ Managed PAM services
- ▶ Manged DI transformation

Data protection (DP)

- ▶ Sensitive data discovery
- ▶ Data minimization
- ▶ Data loss prevention
- ▶ Permissions and activity monitoring
- ▶ DLP policy management and incident response
- ▶ DLP platform
- ▶ Managed DPO services
- ▶ CASB management



Third party risk management (TPRM)

- ▶ Managed TPRM
- ▶ Risk assessment
- ▶ Static and dynamic assessments
- ▶ TPRM automation
- ▶ Cyber risk management
- ▶ Third party lifecycle management

Threat detection and response (TDR)

- ▶ Threat detection
- ▶ Threat response
- ▶ Threat hunting
- ▶ Incident response/Breach response
- ▶ Threat intelligence
- ▶ Technology management
- ▶ Forensic support

Threat exposure management (TEM)

- ▶ Vulnerability discovery and management
- ▶ Configuration scanning
- ▶ Application scanning
- ▶ Penetration testing
- ▶ Remediation orchestration
- ▶ Risk mitigation support
- ▶ Enterprise integration
- ▶ DevSecOps security
- ▶ Threat lifecycle services

Thank you

Q

A

&



About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

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. For more information about our organization, please visit ey.com.

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small and medium-sized enterprises, EY Advisory works with clients — from strategy through execution — to help them design better outcomes and realize long-lasting results. A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with their clients, as well as an ecosystem of internal and external experts, to create innovative answers. Together, EY helps clients' businesses work better.

The better the question. The better the answer. The better the world works.

© 2019 EY
All Rights Reserved.

ey.com