



A need for a holistic approach towards data compliance

In an increasingly complex EU regulatory data landscape



EY

Building a better
working world

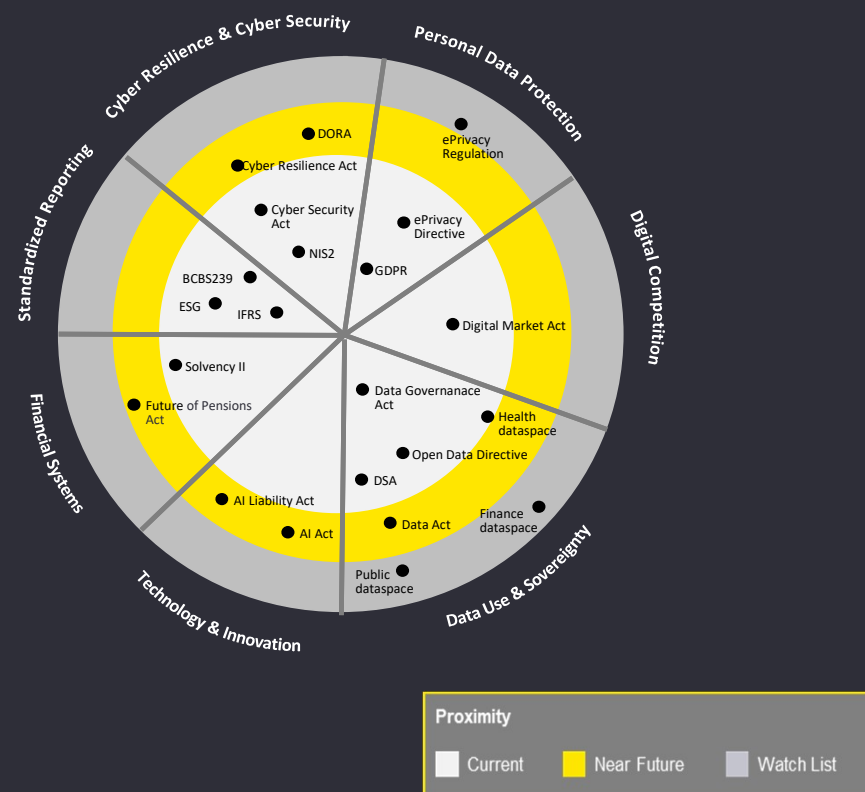
The European Digital Decade seeks to accelerate innovation and establish more trust which has led to new regulations

By 2030, the European Commission seeks to **accelerate the digital transformation** of businesses and public services, **secure sustainable digital infrastructures** and **increase digital capabilities** across the European Union (EU). These established targets are shaping the EU's digital future and sets the stage for Europe's Digital Decade.

Together these objectives and drivers have led to **the need for new regulations and directives** on a wide array of topics relating to technology, digital capabilities and the digital economy.

Considering the diverse goals described, **no single regulation can capture the Digital Decade all at once**. Consequently, a diverse set of regulations, touching upon digital capabilities, are introduced in the EU over the coming decade.

Snapshots of regulations:



One-off project-based efforts to comply with the multitude of regulations have been a trend so far, despite the numerous associated challenges

Organizations face challenges in navigating the complex landscape of various regulations. Often, one-off, project-based efforts are initiated to identify the current state of compliance, which is then followed by an implementation phase. However, organizations frequently fail to embed certain practices into their daily operations, hence missing the opportunity to implement sustainable long-term strategies and practices.

Increased cost of control

Each new regulation requires significant effort to interpret, evaluate, implement, and monitor/maintain, leading to increased costs of control.

Failure to embed practices

One-off, project-based initiatives often fail to incorporate certain practices into daily operations, therefore missing out on creating sustained, long-term value

Limited cross-functional collaboration

Organizational teams often work in silos, which can lead to inefficiencies and missed opportunities to streamline processes.

Lacking knowledge and experience

The variety and complexity of laws and regulations necessitate a broad range of skills and capabilities. The existing shortage of digital talent further complicates the process of achieving compliance with these regulations.

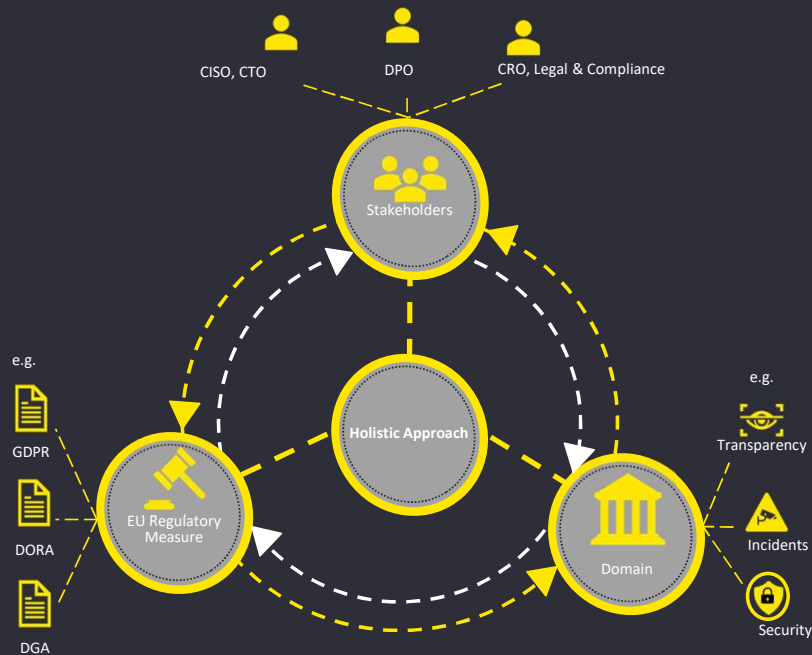
Uncertainty with regards to applicability

Organizations often struggle to understand which regulations apply to them, and to what extent.



Moving from a siloed to a holistic approach to efficiently manage regulatory requirements

The holistic approach, illustrated in the image below, revolves around the idea of engaging multiple stakeholders to collaboratively address a defined set of in-scope regulations. The goal is to identify overlaps and efficiencies across various domains.



Objective:

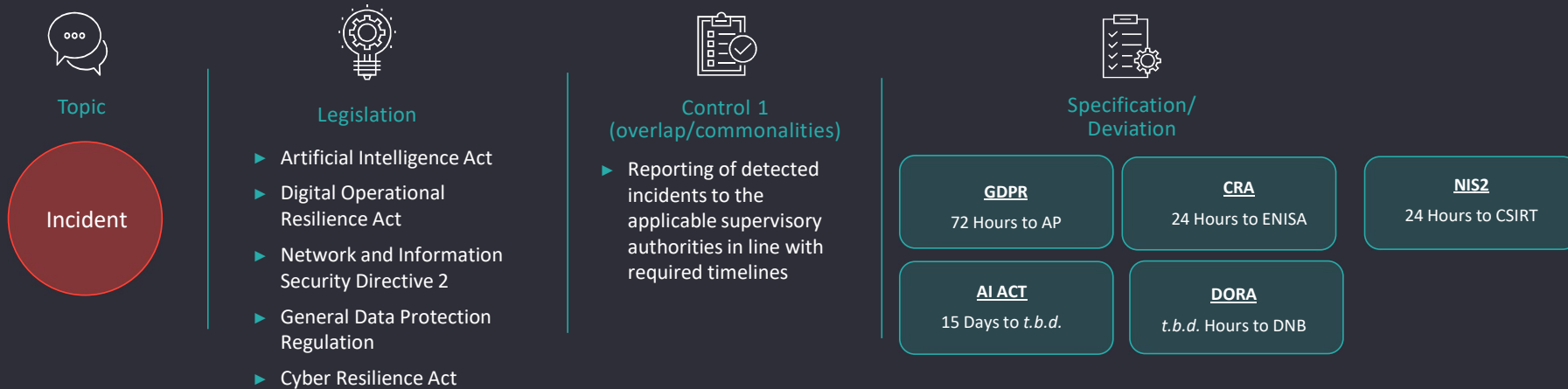
- I. Evaluating Regulations**
Define an overview of Digital regulations (security, privacy, data) relevant for organizations
- II. Defining Themes**
Identify the common themes shared across regulations to simplify and create common language/understanding
- III. Defining Design Principles**
Identify key objectives and requirements for the themes (what are the requirements for your process)
- IV. Defining Key Controls**
Identify best practice controls that can be used to implement design principles (preferably existing controls)

Embedding – the control framework in action

The control framework exists out of different categories in which the overlap between the different regulations is found. First, we apply Control 1 which is a control that is formed by the overlap within the regulations. After this first control is implemented, we implement the deviation controls; that are, the regulation specific controls. Below is an example:

- E.g.
- Transparency
- Accountability
- Legal ground
- Incidents
- Risk Management
- Third Party Risk Management

The Framework – 3. Example of a control



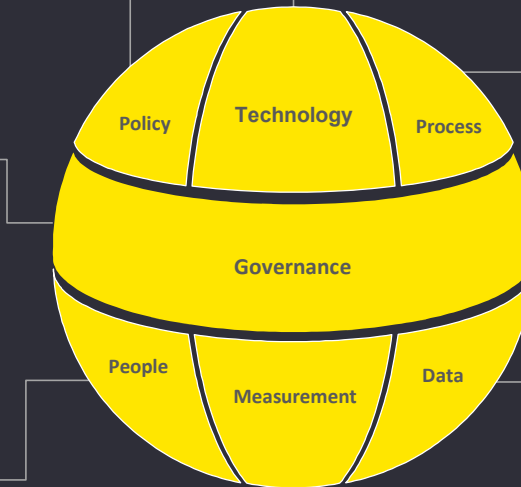
Rethinking Operating Models for integrated and effective regulatory compliance

What: Streamline digital policies; eliminate redundancies and conflicting policy requirements

Factor in: Level of mandate, harmonization of principles and definitions, alignment of policies between local and corporate level (if applicable)

What: re-assess digital roles & responsibilities, reporting lines, decision-making processes, and oversight mechanisms to ensure cross-functional collaboration

What: ensure resources have right skills and capabilities; facilitate appropriate and recurring training and stimulate culture of risk awareness amongst key stakeholders



What: Integration of (GRC) tooling across the data ecosystem

Factor in: consistency in the data and definitions in the different systems used

What: Definition and inventory of end-to-end processes, risks, and controls; continuous enhancement of these processes, risks and controls by 3rd LoD.

What: Embedding data quality and data protection throughout the data lifecycle; inventory and classification of data; integration of controls to ensure data availability and integrity

What: Define KPIs and ensure appropriate dashboarding to allow for maturity comparisons, monitor/integrate KPIs to improve the organization's cyber, privacy and data function

Proposed steps to be taken to facilitate the transition towards the holistic approach

1

Create multi-disciplinary working group

e.g. Cyber, privacy, D&A, IT, Data ethics, Risk, Legal, Compliance, Business etc.

2

(Re)define digital strategic and organizational objectives

Baseline compliance vs best of class.

Align with digital decade and changing imperative

3

Identify existing risk and control frameworks within organization

e.g. risk and control framework for: cybersecurity, privacy, ESG, AI etc.

4

Analyze existing frameworks and identify gaps and possibilities to simplify and streamline






Use design principles to identify gaps in existing risk and control frameworks and possibilities to simplify and streamline

5

Integrate existing frameworks into holistic control framework

Implement a holistic control framework by integrating existing frameworks into a single one that ensures compliance across multiple domains

What are the benefits of a Holistic approach?

Benefit	How
	1. Controlled Compliance Costs / Reduced FTE Requirements
	<ul style="list-style-type: none">➤ Rather than testing controls as part of several control frameworks (privacy, cyber, AI etc.), organizations will now have one uniform control framework which could potentially lead to a <u>reduction in 1st and 2nd line Cyber, Privacy and Data FTEs.</u>➤ <u>Estimate 10-15% reduction</u> in direct costs by lowering the size and number of project-based initiatives to determine applicability, impact and maturity state of the organization with regards to individual regulations.
	2. Decreased risk of non-compliance
	<ul style="list-style-type: none">➤ Decreased risk of financial consequences, such as penalties, by improved oversight and ensuring several digital regulations are considered together.➤ Reducing duplication of compliance efforts and improving efficiency➤ A holistic data framework stimulates organizations to address regulatory compliance as a board level theme by intensifying the collaboration between the CCO and CRO.
	4. Reduced Complexity & Increased Efficiency
	<ul style="list-style-type: none">➤ Merging multiple compliance regulations and requirements into a single framework can simplify processes and enhance efficiency (e.g. change management process, incident management process).
	5. Cross-functional collaboration savings
	<ul style="list-style-type: none">➤ Improved cross-functional collaboration can increase productivity, reduce repetition and lower labor costs: searching for efficiencies and synergies, not reinventing the wheel etc.
	6. More time for higher value activities
	<ul style="list-style-type: none">➤ Centralization and efficient handling of compliance tasks can free up significant time for 1st line teams to work on high value activities.

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 organisation, 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 organisation, please visit ey.com.

© 2024 EYGM Limited.

All Rights Reserved.

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

