

# Digital Operations Resilience Act

Minimizing Cyber Risks for  
Financial Services

# 1 Security regulatory landscape



# Security regulatory landscape

**The European regulatory context widens and becomes more complex every day thus calling for transformation projects and remediation initiatives**



## Regulatory Challenges



**+5000 regulatory changes** only in the last year across various sector and multiple subject matters



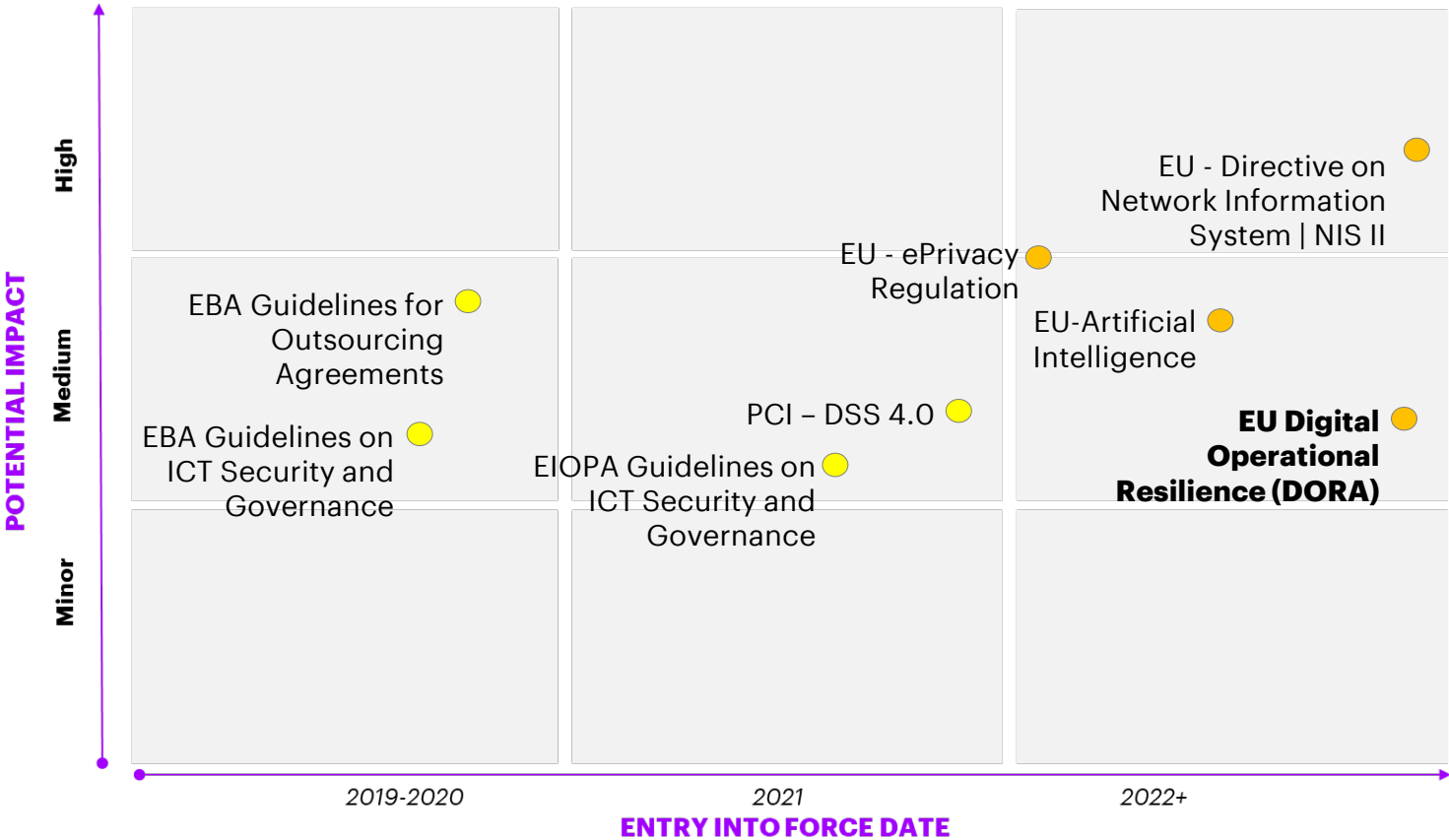
**160 regulatory publications** generated in the last months by COVID-19, with main impacts on risk management



71% of firms expect the amount of **regulatory information published** by regulators to **increase over the next 12 months**



# Regulatory Trends & Impacts



## Colors for Regulations

- Major impacts
- Medium/ high impacts
- Medium/ low impacts
- Minor impacts

# 2 Overview



# Overview

**Digital Operations Resilience Act (DORA) aims to consistently target digital risks for all financial entities**



## OBJECTIVE

Establish **harmonized regulations** at European Level to ensure **operational resilience** against cyber-attacks



## CONTENT

### Harmonization of:

- ICT-risk management rules
- ICT-related incident management
- Digital operational resilience testing
- Management of ICT-third-party risk



## AFFECTED PARTIES

- **All operators** in the financial sector
- Respective **third-party service providers** (such as providers of cloud computing services, software, data analytics and data centers)





## VALIDITY

The European Commission has received public feedback on the proposals on the 12<sup>th</sup> of April 2021.

DORA is expected to be taken into effect during mid of 2022 and therefore must be enforced **by mid of 2023**.



## IMPACT

Compliance will be ensured by the entity's competent authority.

EU Member states will have the right to **impose criminal penalties** for breach of the obligations.



## OBJECTIVE

Establish **harmonized regulations** at European Level to ensure **operational resilience** against cyber-attacks

# 3

## Background and Objectives



# **DORA set new regulations for the financial sector with the goal to minimize ICT risks on an European level**

## **What is DORA?**

**DORA** (“Digital Operational Resilience Act”) is expected to be taken into effect during the first half of 2022.

The aim of this regulation is the harmonization of existing rules on managing ICT (“Information and Communication Technology”) governance, ICT risks and incident reporting for all financial institutions to ensure operational resilience against ICT risks.

**DORA** will come into force as new regulation at European level and must be applied in an equal manner in all EU countries.

## Enactment details

### Entry into force

The regulation shall enter into force on the 20<sup>th</sup> day following its publication.

### Deadline for transposition

It shall apply 12 month after the date of its publication.

### Exception

Articles 23 and 24 (threat-based penetration tests) apply 36 month after the due date of entry into force.



## Essential content



### ICT Governance

Update existing rules on ICT governance to align respective business strategies



### ICT Risk Management

Key requirements and principles on ICT risk management



### ICT Incident Reporting

Monitoring and reporting of ICT-related incidents



### Digital Operational Resilience Testing

Regular performance of enhanced operational resilience tests



### ICT Third-Party Management

Active management of ICT third-party risk and the contract design



### Reporting to Authorities

Compliance with the regulation will be ensured by respective authorities

4

# **DORA Financial Services implications**





## GOVERNANCE

### REQUIREMENTS

The management body will be required to maintain an active and crucial role in the management of security risks and shall pursue the respect of a strong cyber hygiene.

The following must also be ensured with regard to security: (i) clear definition of roles and responsibilities for all ICT-related functions, (ii) continuous engagement to risk control and monitoring through defined processes, (iii) appropriate allocating of ICT investments and trainings.

### IMPLICATIONS

- Directly involve the management body in the ICT risk assessment process and foreseen the the explicit assessment and control of residual risks
- Plan specific security investments
- Implement and record the execution of security awareness programs



## **ICT RISKS MANAGEMENT**

### **REQUIREMENTS**

Financial Entities are required to set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk, implementing appropriate protection and prevention measures and continuously define solutions that cover all relevant scenarios.

### **IMPLICATIONS**

- Update the ICT Risk management framework, envisaging its integration with the Business Continuity and Disaster Recovery plan
- Evolve the Business Continuity and Disaster Recovery plan towards an Operational Resilience plan considering cyber attack scenarios and related countermeasures



## **INCIDENT REPORTING**

### **REQUIREMENTS**

Financial Entities are required to establish and implement a process for monitoring and managing ICT related incidents, classifying them based on criteria to be developed by a joint committee of European Supervisory Authorities (ESAs).

### **IMPLICATIONS**

- Provide constantly updated incident reports, informing customers of any potential impacts
- Define or modify the incident reporting processes currently implemented, in accordance with the new guidelines



## **DIGITAL OPERATIONAL RESILIENCE TESTING**

### **REQUIREMENTS**

In accordance with the principle of proportionality and thus depending on the size, business and risk profile, Financial Entities are required to conduct advanced threat-lead penetration tests of ICT tools and systems.

The regulation sets out requirements for testers and the recognition of threat-lead penetration tests results across the Union for financial entities operating in several Member States.

### **IMPLICATIONS**

- Involve qualified Third Parties in the conduction of red-teaming activities in accordance with the TIBER-EU framework
- Involve qualified personnel to perform the testing activities



## ICT THIRD-PARTY

### REQUIREMENTS

Enable comprehensive risk monitoring of ICT Third Parties during the preliminary, execution, and post-contractual phases of the relationship. Maintain a Register of Third Parties for which specific requirements/contractual clauses should be defined.

### IMPLICATIONS

- Design and implement processes for defining and continuously reviewing contractual and technical security measures relating to Third Parties, based on related service levels agreed



## REPORTING TO AUTHORITIES

### REQUIREMENTS

Financial entities are required to set-up arrangements to exchange amongst themselves cyber threat information and intelligence, to reduce its propagation and supporting defence capabilities.

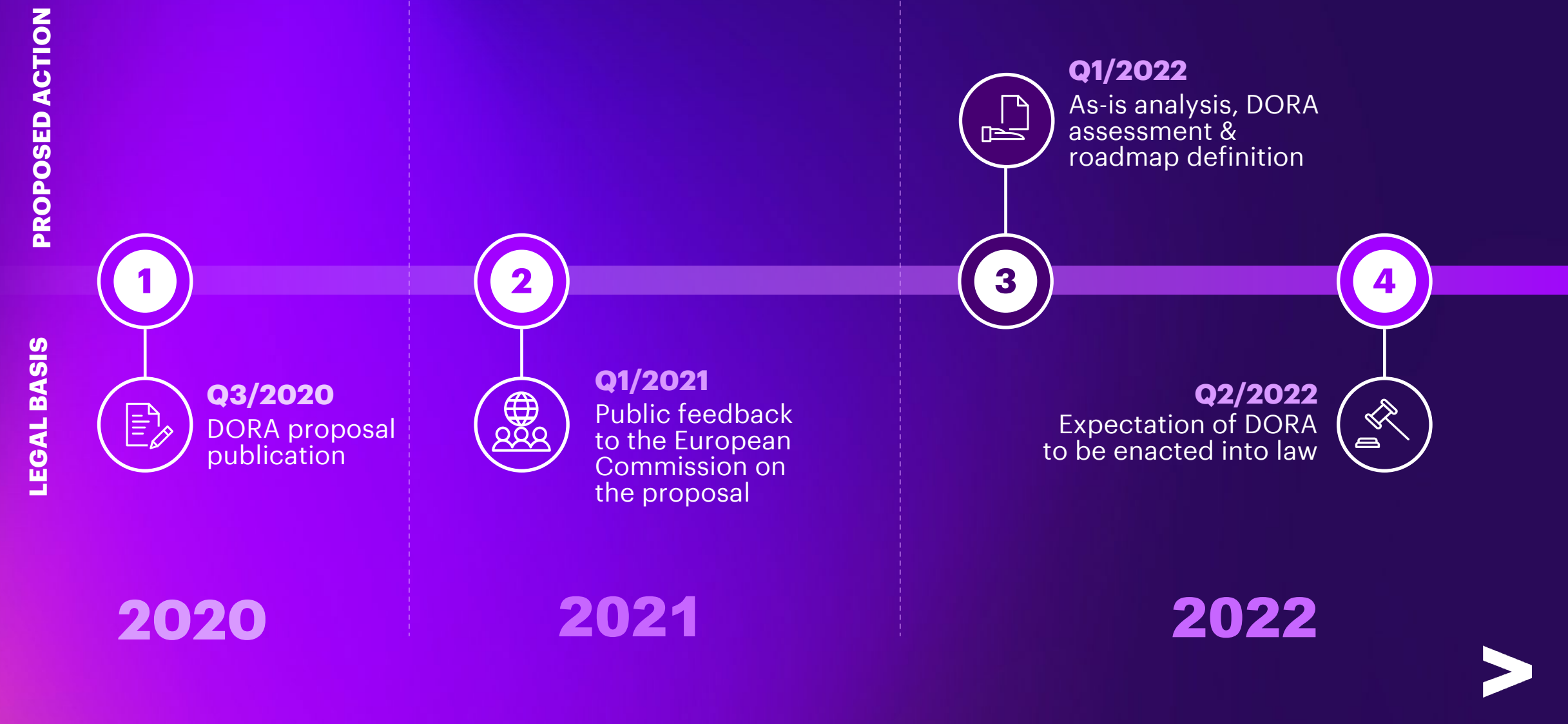
### IMPLICATIONS

- Define protocols for exchanging and sharing information with other financial entities on security threats and events, also relying on the support of system/national structures.

5

# Next steps





6

# Our Assets

**Accenture will support clients on the organizational as well as the technical implementation of DORA**





**Main  
Improvements  
required**

## GOVERNANCE

## ICT RISKS MANAGEMENT

## INCIDENT REPORTING


## DIGITAL OPERATIONAL RESILIENCE TESTING


## ICT THIRD-PARTY

## SECURITY INFO SHARING

1


Set up / improve ICT risk and security management regulation according to standard, best practices and experiences from other countries


 Provide our benchmark services in order to set security investment aligned to comparable players

 Provide security awareness as a service leveraging on our platforms

2

 Apply new Operational Resilience framework developed for integrate cyber attack


 Implement versioning / back-up solutions for manage «cold copies» against ransomware attack


 Specific ICT risk evaluation for cloud services with our Cloud Security express service

3


Set up / improve incident management and reporting processes according to standard, best practices and experiences from other countries

4

 Provide red teaming exercise by our Global team in order to identify customer threat exposure according to TIBER-EU framework

 Accenture is leader in the execution of red teaming exercise thank to the support delivered to several Authorities and is CREST/CBEST certified

5

 Provide Third Party Risk Management as a service supported by automation and tools for reducing operating costs of control

6

Set up / improve security data exchange process according to standard, best practices and experiences from other countries



# Contacts

## **Fabio Colombo**

Accenture Security Managing Director

✉ [fabio.colombo@accenture.com](mailto:fabio.colombo@accenture.com)

☎ +39 335-1252820

---

## **Marco Valsecchi**

Accenture Security Managing Director

✉ [marco.valsecchi@accenture.com](mailto:marco.valsecchi@accenture.com)

☎ +39 324-5983808

---

## **Luca Ticchiati**

Accenture Security Manager

✉ [luca.ticchiati@accenture.com](mailto:luca.ticchiati@accenture.com)

☎ +39 349-9377999

---

## **About Accenture**

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.

Visit us at [www.accenture.com](http://www.accenture.com)

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.