DORA: Nuove regole per velocizzare la digitalizzazione e gestire i rischi ICT; Cosa "Re -inventare"?

Nicasio Muscia – Managing Director Accenture Risk & Compliance

June 2023

accenture

DORA: OVERVIEW AND KEY BREAKTHROUGH

DORA KEY PILLARS

ICT RISK MANAGEMENT

- **Set-up and maintain resilient ICT systems** and tools that minimize the impact of ICT risk
- Set up dedicated and comprehensive **BC Policies** and **DR plans**

ICT INCIDENT MANAGEMENT

- **Establish and implement a management process to monitor and log ICT-related incidents**
- **Report "major" ICT-related incidents** to their national regulator.

RESILIENCE TESTING

- **Test capabilities and functions included in the ICT risk management framework** on a regular basis
- Execute a **full range of appropriate tests**, including vulnerability assessments and scans, security assessments,

THIRD PARTY MANAGEMENT

- Enable a **monitoring of ICT third-party risk** throughout the relationship conclusion, performance, termination
- Prescribe **certain content requirements for contracts** between financial entities and ICT third-party service

KEY BREAKTHROUGH INTRODUCED

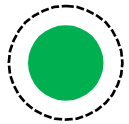
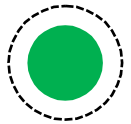
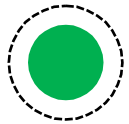
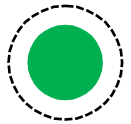
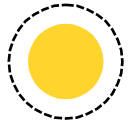
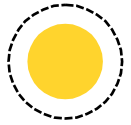
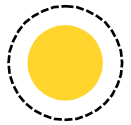
Overcome the **siloed perspective of management of DIGITAL RISK** by asking for a comprehensive assessment

Enhance the **solidity and features of digital risk management** tools and methodologies by moving towards **QUANTITATIVE AND DYNAMIC ANALYSIS**

Enhance testing methodologies by moving from asset perspective to **process one** by asking for alignment with **TIBER – EU REQUIREMENTS**

Extend requirements also to supply chain and vendor management in order to ensure **same level of security features and methodologies**

STATE OF THE ART: FS ITALIAN MARKET MATURITY LEVEL

KEY PILLARS	BANKING PLAYERS STATUS	BANKING PLAYERS DESCRIPTION	INSURANCE PLAYERS STATUS	INSURANCE PLAYERS DESCRIPTION
ICT RISK MANAGEMENT		▪ Overall ICT Risk management framework aligned to DORA ▪ Areas of improvement refer to structured asset inventory to address ICT analysis		▪ Defined ICT risk management framework, although room of improvements impacting (i) policies/procedure and (ii) asset inventory
ICT INCIDENT MANAGEMENT		▪ ICT incident management framework fully aligned with DORA requirements		▪ Solid ICT risk management framework ▪ Area of improvements refers to the need to further enrich incident reporting information (e.g asset impacted)
RESILIENCE TESTING		▪ Performed standard resilience testing at asset level ▪ Need to align framework to TIBER – EU framework		▪ Resilience testing widely performed across players in terms of VA/PT at asset level ▪ Areas of improvement regards the need to enhance current framework and align to TIBER – EU provision
THIRD PARTY MANAGEMENT		▪ Few players have implemented a sound third party management ▪ Remaining players highlight an unstructured management of third parties with missing features like (i) third party register, (ii) monitoring		▪ Third party management framework substantially adopted across players ▪ Room for improvements refer to (i) third party register and (ii) contract clause (e.g termination)

 *Aligned*  *Partially Aligned*  *Not aligned*

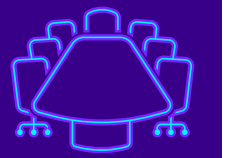
Source: 2023, Accenture Benchmark performed on selected Banking and Insurance Players

KEY POINTS OF ATTENTION ACROSS DORA REQUIREMENTS

KEY PILLARS	TOPIC	DESCRIPTION
GOVERNANCE	ROLES & RESPONSABILITIES	▪ **Involvement a of a lead function responsible for leading the DORA Programme and underlying streams both at first & second level** (e.g. New Control function ex 285 Bankit)
ICT RISK MANAGEMENT	RESILIENCE METRICS & THRESHOLDS	▪ Organize **different information coming from key sources** in order to define ad hoc indicators to **monitoring group operational resilience** ▪ Set up ad hoc **algorithm** in order to define **tailored thresholds** considering also **risk appetite** and perform **correlation analysis** considering among evidences
	ASSET INVENTORY	▪ Set up a comprehensive **catalog including all organization's assets** (CMDB)
RESILIENCE TESTING	SCENARIO TESTING	▪ **Extend typology of scenario testing** in scope in order to cover all adverse events (e.g Wireless Assessment, Source Code analysis)
	TIBER EU – ALIGNMENT	▪ Enrich **operational resilience framework** in order to **align with TIBER – EU** regulation by **defining annual plan for execution, process** and underlying **actors to be involved**
THIRD PARTY MANAGEMENT	E2E THIRD PARTY FRAMEWORK	▪ Definition of an overall **framework to handle the entire lifecycle of the third party** with main focus on **onboarding** (i.e minimal contractual requirements), **storage of information and post contract management** (i.e exit strategy)

ACCENTURE DORA COMPLIANCE PROGRAMME

WE ARE OUR FIRST CREDENTIAL FOR DORA PROGRAM SET-UP



RELATIONSHIP WITH REGULATORS

Direct connection with regulators as expert matters in formalization and amendment and sharing of the regulation to impacted parties

INTERNAL DORA ASSESSMENT

Internal DORA compliance as directly impacted by the regulation allowing development of assets and best practices to be roll out to clients

SELECT “NO REGREAT ACTIONS”

Ready to use suite of service of DORA assets covering both inception phase and all pillars of the regulation

ESAS REQUEST ON TPRM
INTRODUCTION

During the investigations phase to define what are the **regulatory technical standards, EIOPA/EBA required Accenture** (as a provider of critical services to Financial Institutions) **to answer a questionnaire** on the **methodologies** in place in **third party lifecycle management**

Criticality of Third party
(Questions 1,2 and 3)

Risk Assessment & Mitigation measures
(questions 4 and 5)

Incident Management
(Questions 6 and 7)

Audit Methodologies on Third party
(Questions 8, 9 and 10)

New Oversight Framework
(Question 11)

1. Threat Intelligence-based ethical red teaming, 2. Configuration Management Database, 3. Risk Assessment

OUR DORA IMPLEMENTATION ROADMAP

PROPOSED APPROACH FOR EACH TOPIC

WAVE CONTENT	ICT RISK MANAGEMENT	ICT INCIDENT MANAGEMENT	OPERATIONAL RESILIENCE TESTING	THIRD PARTY RISK MANAGEMENT
WAVE 1 ▪ Deep dive **into activities needed to set up DORA programmed** with **no dependency with RTS**	***Programme** & **Governance Model setup***			
	ICT RM Framework	***Incident Management Framework***	***Operational Resilience Framework***	***Third Party Risk** Management **framework***
	Business Continuity Framework		***Threat & Scenario Modelling***	***Contractual Framework***
	Process/Assets Mapping			
WAVE 2 ▪ Deep dive into **topic and underlying articles** with RTS issuance within **12 months**	***RM Framework** Enhancement (i.e. Art 15)*	***Incident Management** Framework Enhancement - **Classification** (i.e. Art. 16)*		***TPRM framework** Enhancement - **Registry of information** (Art. 28)*
	***BC Framework** Enhancement (i.e. Art 15)*			***TPRM framework** Enhancement - **TP ICT services** Policy (Art. 28)*
WAVE 3 ▪ Deep dive **into topic and underlying articles** with RTS issuance within **18 months**		***Incident Management** Framework Enhancement - **Major Incident** Reporting (i.e. Art. 20)*	*Threat **Led Penetration test** model (i.e. Art 26)*	***Assessment on Sub – contractor** of relevant **ICT services** (Art 30)*
WAVE 4 ▪ Focus on **remaining activities related dashboard formalization & sharing of information** between relevant actors		*Harmonized **ICT incident reporting** to supervisor (i.e. Art 21)*		
	DORA Framework KPIs** & **Dashboarding			

OUR DORA IMPLEMENTATION: "NO REGRET ACTION

- **Perform the assessment in «agile mode»**

- **Invest in the enanchment of existing framework on Cyber /IT Risk & Third Party Risk Management**

TPRM

ICT/Cyber Risk

- **Try to improve efficiency working on target operating model and assets**