dora360

gieom

Antony Bream

gieom

GTM Advisor – dora360

antony.bream@gieom.com

DORA Regulation :

5 pillars , 64 sections , 79 pages

DORA is in Force from **Jan 16th, 2023**

Technical Standards by **June 2024**

2 Year implementation Period – Jan 17th, 2025

What Needs To Be done :

- Write **Operational** and **Cyber Policies**;
- Create **Processes for CBS** and **Map Resources**;
- **Analyse data** from tools for Risk Management , Cyber , Third-Party Assessment , Incident management etc…
- **Share** incident report with **Regulator**
- Conduct **internal audits** and be **prepared for regulator inspections**
- **Inventorise, monitor and exit plans for 3rd Party Suppliers**

Steep Penalty – Penalty calculation yet to be finalised by authorities (similar to GDPR @ 4% global revenue) + public call outs

ICT providers – 1% of average worldwide turnover

5 PILLARS OF DORA

1 ICT RISK MANAGEMENT

The management body of a financial entity is required to define, approve, oversee, and be accountable for the implementation of all arrangements related to the ICT risk management framework

2 ICT RELATED INCIDENT MANAGEMENT

Financial entities are required to establish and implement an ICT-related incident management process to detect, manage, and notify ICT-related incidents and shall put in place early warning indicators as alerts

3 DIGITAL OPERATIONAL RESILIENCE TESTING

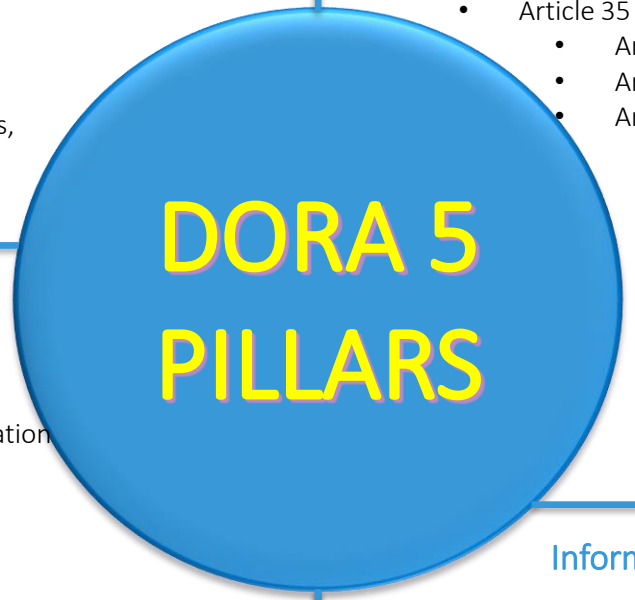
Financial entities are required to establish and implement a testing program that considers a wide variety of tests limited not to IT systems but also to process and people.

4 MANAGING OF ICT THIRD PARTY RISK

Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with key principles for ICT third-party risk management issued by the regulatory authority .

5 INFORMATION SHARING ARRANGEMENT

Financial entities may exchange among themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts, and configuration tools



ICT Risk Management

SECTION I

- Article 5 – Governance & Organisation

SECTION II

- Article 6 – ICT Risk Management Framework
- Article 7 – ICT Systems, Protocols and Tools
- Article 8 – Identification
- Article 9 – Protection and Prevention
- Article 10 – Detection
- Article 11 – Response and Recovery
- Article 12 – Backup Policies and Procedures, Restoration and Recovery Procedures and Methods
- Article 13 – Learning and Evolving
- Article 14 – Communication
- Article 15 – Further Harmonisation of ICT Risk Management Tools, Methods, Processes & Policies
- Article 16 – Simplified ICT Risk Management Framework

ICT Related Incident Management, Classification & Reporting

- Article 17 – ICT Related Incident Management Process
- Article 18 – Classification of ICT Related Incidents and Cyber Threats
- Article 19 – Reporting of Major ICT Related Incidents and Voluntary Notification of Significant Cyber Threats
- Article 20 – Harmonisation of Reporting Content & Templates
- Article 21 – Centralisation of Reporting of Major ICT Related Incidents
- Article 22 – Supervisory Feedback
- Article 23 – Operational or Security Payment Related Incidents Concerning Credit Institutions, Payment Institutions, Account Information Service Providers and Electronic Money Institutions

Digital Operational Resilience Testing

- Article 24 – General Requirements for the Performance of Digital Operational Resilience Testing
- Article 25 – Testing of ICT Tools and Systems
- Article 26 – Advanced Testing of ICT Tools, Systems and Processes based on TLPT
- Article 27 – Requirements for Testers for the Carrying out of TLPT

Managing of ICT Third Party Risk

SECTION I KEY PRINCIPLES FOR A SOUND MANAGEMENT OF ICT THIRD PARTY RISK

- Article 28 – General Principles
- Article 29 – Preliminary Assessment of ICT Concentration Risk at Entry Level
- Article 30 – Key Contractual Provisions

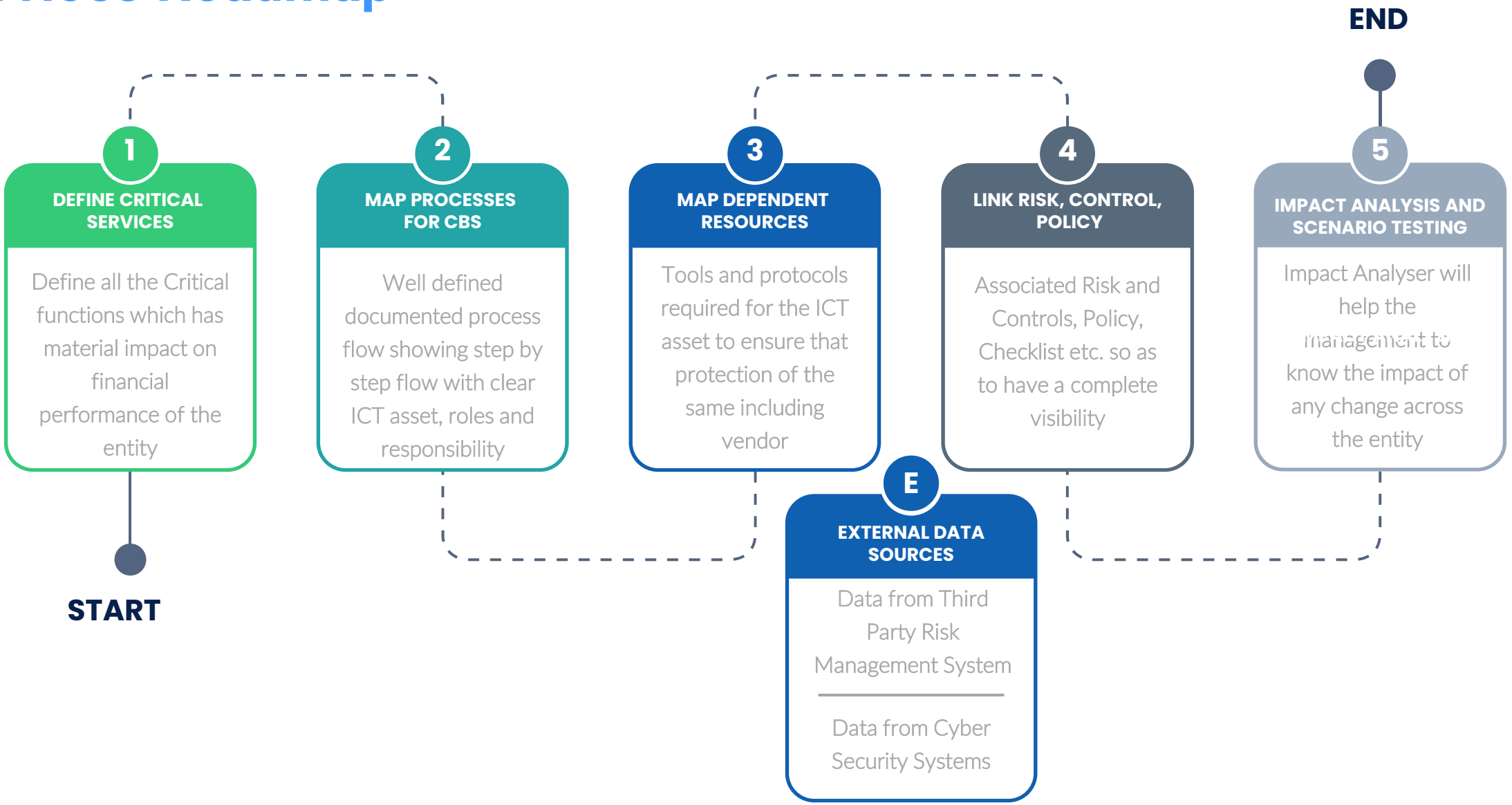
SECTION II OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD PARTY SERVICE PROVIDERS

- Article 31 – Designation of Critical ICT Third Party Service Providers
- Article 32 – Structure of the Oversight Framework
- Article 33 – Tasks of the Lead Overseer
- Article 34 – Operational Coordination Between Lead Overseers
- Article 35 – Powers of the Lead Overseer
  - Article 36 – Exercise of the Powers of the Lead Overseer Outside the Union
  - Article 37 – Request for Information
  - Article 38 – General Investigations
    - Article 39 – Inspections
    - Article 40 – Ongoing Oversight
    - Article 41 – Harmonisation of Conditions Enabling the Conduct of the Oversight Activities
    - Article 42 – Follow-up by Competent Authorities
    - Article 43 – Oversight Fees
    - Article 44 – International Cooperation

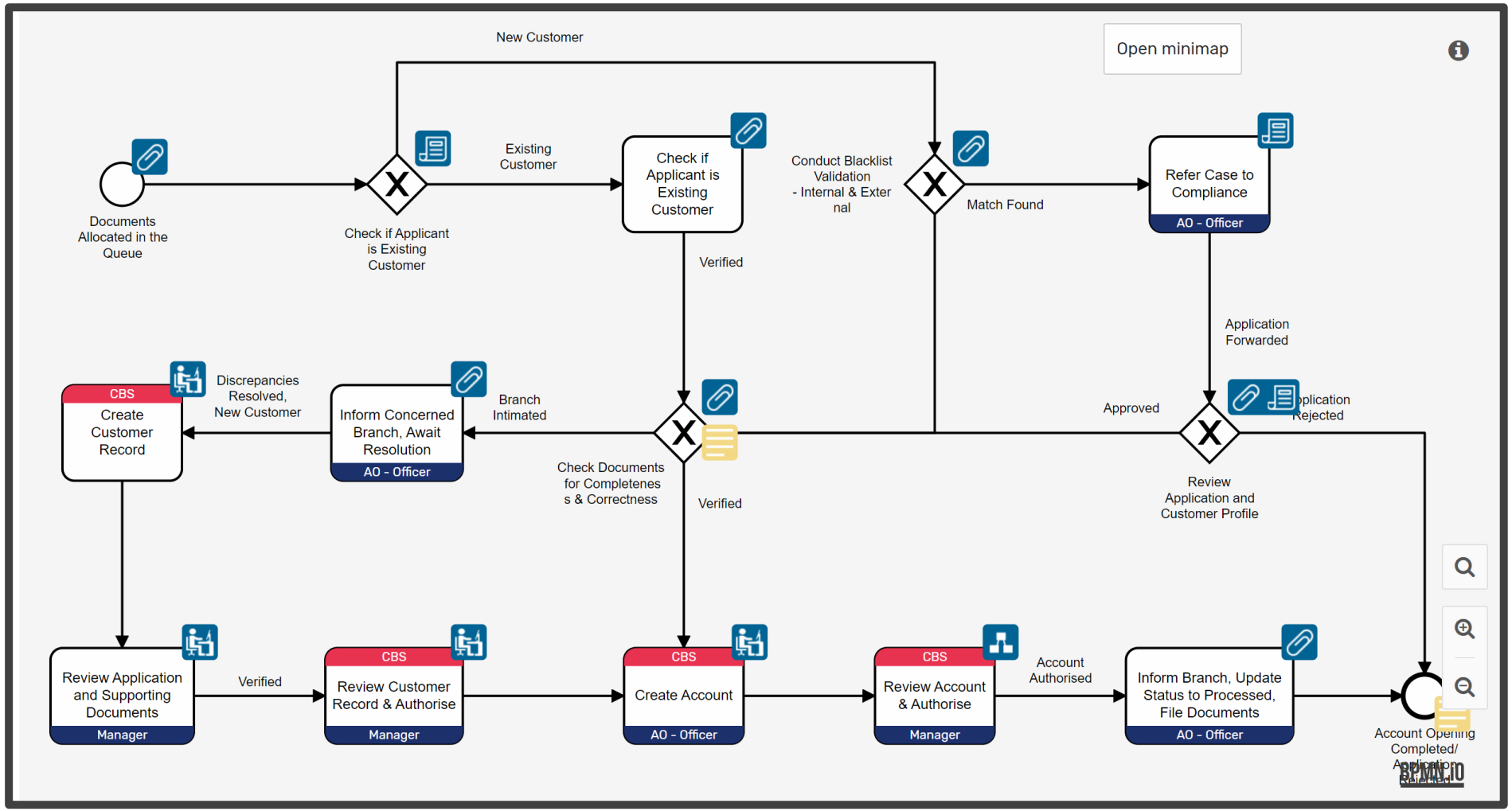
Information Sharing Arrangements

- Article 45 – Information Sharing Arrangements on Cyber Threat Information and Intelligence

Dora360 Continuous Monitoring of Critical Business Services Roadmap



Visualise Critical Business Services and Map Resources

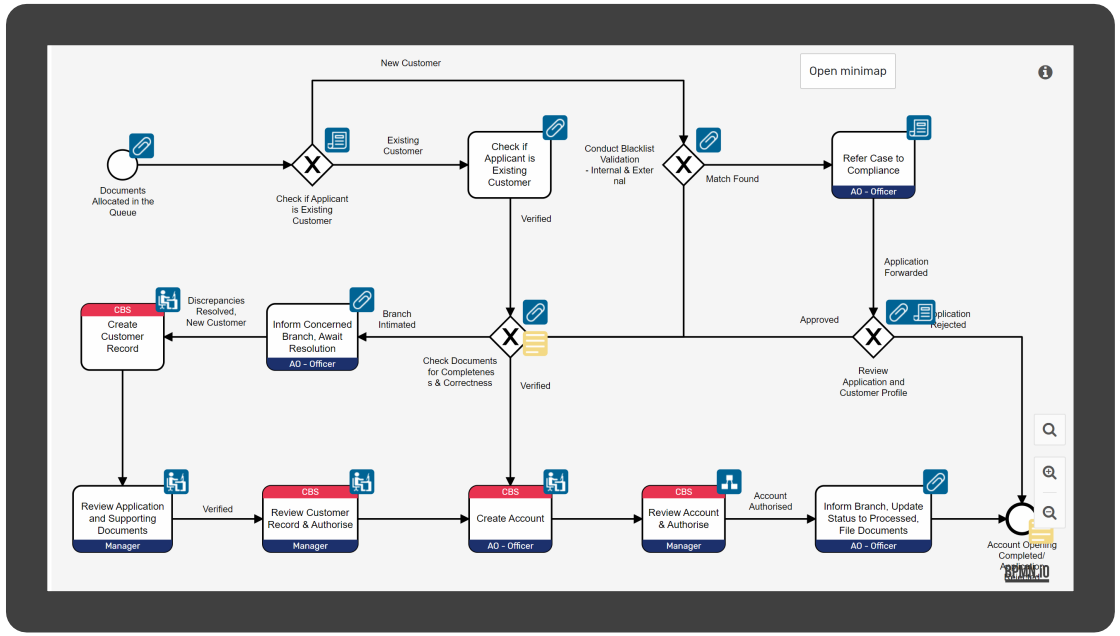


Attach All DORA Assets To The Critical Business Process Map

Repository of DORA Regulations
(UCF interface)

Article to Article Linkage
(Pre-created control repository linking tech standards to multiple articles)

Policy Repository
(link policies to procedures)



TPRM – identify third parties from critical processes, categorise and market scan

MAGPIE (Gen AI) - compare existing documents with regulatory clauses to generate coverage report

Incident Reporting- Report incidents on critical services and create mitigation plan. Report to central bank as per rule

dora360 Compliance Dashboard – Single Pane of Glass

gieom

RISK CENTRAL

DORA - COMPLIANCE MANAGEMENT

derek

System Preferences
Home
Dashboards
Action Center
Templates Hub
Applications

FRAMEWORK DRILLDOWN

- (All)
- DORA Regulation 2022
  - Article 6 - ICT Risk Manag...
  - Article 8 -Identification
    - Article 8.1

STATUS

- (All)
- Completed
- Not Completed

PUBLISHED DATE

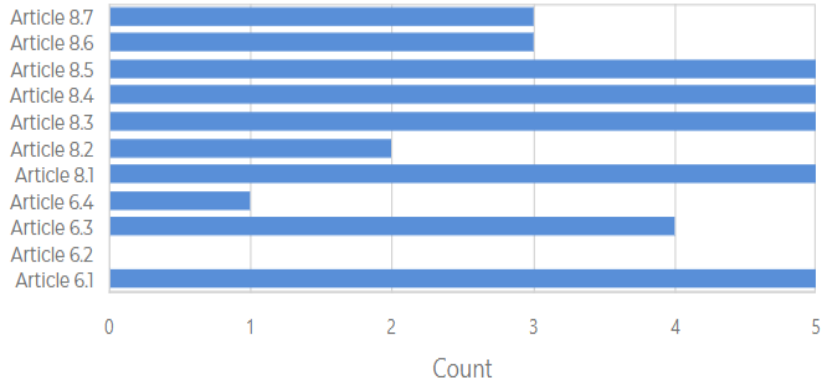
- (All)
- 2023

TARGET DATE

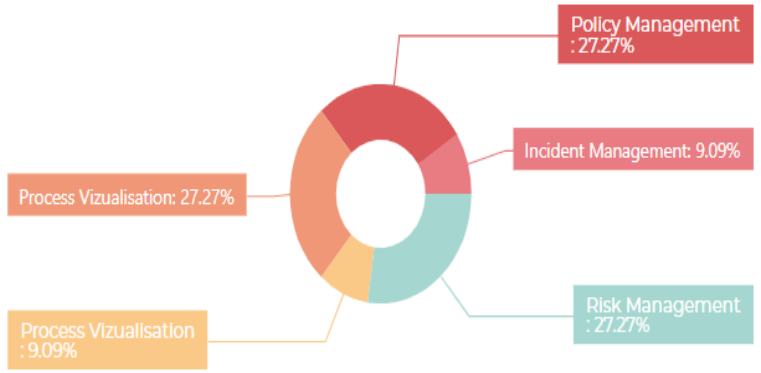
- (All)
- 2023

TOTAL	COMPLETED	NOT COMPLETED	DUE	OVERDUE	UPCOMING
11	5	6	1	3	2

BASED ON ASSESSMENT RATING



BASED ON MODULE



DETAILS

Clause	Clause Description	Assessment Rating	Target Rating	Target Date	Published Date	Completion Date	Status	Policy Category	Policy Type	Module	Actioner
Article 6.1	Financial entities shall have a sound, comprehensive and	5	0	8/18/2023	4/12/2023	8/18/2023	Completed	Circular	New Regulation	Policy Management	Felix

dora360 Vendor Risk Management

- Organisational
- Financial
- Operational Resilience
- Cyber (including dark web)
- Social Media
- Real-time controversy alerting
- Regulatory Compliance (e.g. FCA Register)
- Proactive Vulnerability
- Individual Data Analysis (e.g. Companies House)