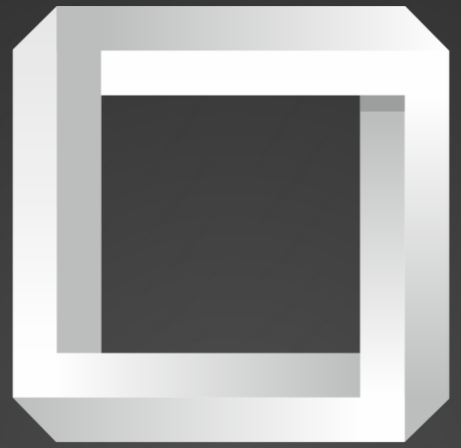


CYBERFLIP

Cybersecurity for Next Generation Enterprises

Cyber Resilience Services - DORA

2026

Contents

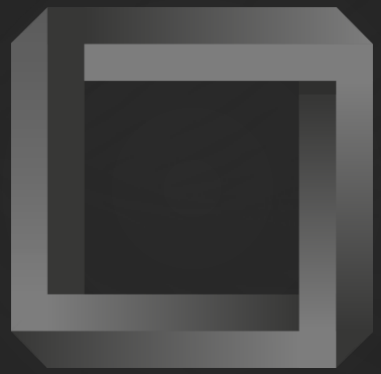
CYBERFLIP

DORA

- Regulation
- Pillars
- Penalties
- Scope

Our Approach

- Addressing DORA Requirements
- Services Bundles
- Your Journey towards DORA Compliance



DORA Regulation

DORA Regulation

CYBERFLIP

- The DORA Regulation refers to the European Union's Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.
- It was introduced in 2020, entered into force on 16 January 2023 and shall apply from 17 January 2025.
- It aims at strengthening the information and communication technology (ICT) security of financial entities in the remit of the 3 European Supervisory Authorities (ESAs) and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational digital disruption.

Pillars

CYBERFLIP

DORA Main Pillars

ICT risk management

A framework setting principles and requirements on ICT risk management

ICT-related incidents

Management of ICT-related incidents, and mandatory reporting of major ones to competent authorities within a defined timeframe

Digital operational resilience testing

Operational resilience testing programme encompassing a range of tests, including advanced testing

ICT third-party risk

Principle-based rules for monitoring third-party risk, key contractual provisions and oversight framework for critical ICT TPPs

Information sharing

Voluntary exchange of information and intelligence on cyber threats

DORA Penalties

CYBERFLIP

- Significant Administrative fines
  Financial Entities: Up to 2% of total annual worldwide turnover or up to €1.000.000 for individuals
  Critical third-party ICT service providers:
  Up to €5.000.000 or €500.000 for individuals
- Remedial measures
  Such as additional reporting requirements, increased scrutiny, restriction of certain business activities.
- Public notices
  Including public statements indicating the identity of the natural or legal person and the nature of the breach.
- Operational restrictions
  Limitations on business activities, forced operational changes, or even the suspension of certain services.
- Criminal penalties
  Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches that are subject to criminal penalties under their national law.

* The administrative penalties and remedial measures may also apply to members of the management body of the entities.

Scope

CYBERFLIP

Entities Covered by the DORA

a. Credit institutions

b. Payment institutions, including payment institutions exempted pursuant to directive (EU) 2015/2366

c. Account information service providers

d. Electronic money institutions, including electronic money institutions exempted pursuant to directive 2009/110/EC

e. Investment firms

f. Crypto-asset service providers as authorised under a regulation of the European parliament and of the council on markets in crypto-assets

g. Central securities depositories

h. Central counterparties

i. Trading venues

j. Trade repositories

Scope

CYBERFLIP

Entities Covered by the DORA

k. Managers of alternative investment funds

l. Management companies

m. Data reporting service providers

n. Insurance and reinsurance undertakings

o. Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries

p. Institutions for occupational retirement provision

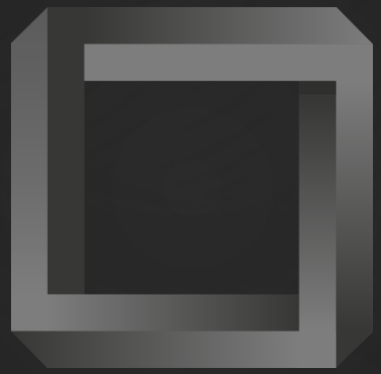
q. Credit rating agencies

r. Administrators of critical benchmarks

s. Crowdfunding service providers

t. Securitisation repositories

u. ICT third-party service providers



Our Approach

Services

CYBERFLIP

End-to-end Security and Compliance

- Tailored solutions from design to implementation ensuring smooth integration of technology and associated policies and procedures.
- Ongoing compliance covering efficiently all requirements.

WHAT IS DORA COMPLIANCE ?

Addressing DORA Requirements

CYBERFLIP

ICT Risk Management

DORA Requirements	Services
Governance and organization	Gap analysis & Maturity Assessment
ICT risk management framework	ICT risk management framework (incl. Security Policies)
ICT systems, protocols and tools Identification	ICT risk assessment
Protection and prevention Detection	

Addressing DORA Requirements

CYBERFLIP

ICT Risk Management

DORA Requirements	Services
Response and recovery Backup policies and procedures, restoration and recovery procedures and methods	ICT risk management framework BCMS design Crisis management and simulation Incident response playbooks and simulation
Learning and evolving	ICT risk management framework ICT risk assessment ICT security awareness and digital operational resilience training
Communication	ICT risk management framework Crisis management

Addressing DORA Requirements

CYBERFLIP

ICT Incident Management

DORA Requirements	Services
ICT-related incident management process	ICT risk management framework Crisis management Incident management Incident response playbooks
Classification of ICT-related incidents and cyber threats	
Reporting of major ICT-related incidents and voluntary notification of significant cyber threats	

Addressing DORA Requirements

CYBERFLIP

DOR Testing

DORA Requirements	Services
General requirements of digital operational resilience testing	Digital operational resilience testing programme (Penetration Tests, Vulnerability Assessments, Red/purple teaming, Physical Security reviews, Source Code reviews, BC and DR tests).
Testing of ICT tools and systems	
Advanced testing of ICT tools, systems and processes based on TLPT	
Requirements for testers for the carrying out of TLPT	

Addressing DORA Requirements

CYBERFLIP

ICT Third Party Risk & Information Sharing

DORA Requirements	Services
General principles of managing of ICT third-party risk Preliminary assessment of ICT concentration risk at entity level	ICT risk management framework ICT risk assessment Threat Intelligence Brand Risk Reputation
Information-sharing arrangements on cyber threat information and intelligence	ICT risk management framework Threat Intelligence Brand Risk Reputation

Services Bundles

CYBERFLIP

Choose what you Need & Build your Custom end-to-end Solution

Design	Enhance	Assess	Custom
Gap Analysis & ICT risk assessment	ICT security awareness and DOR Training	Penetration Test and VA	Build your own service bundle based on your needs
ICT risk management framework	Incident Response Playbooks	Red & Purple teaming	
BCMS design	Threat Intelligence & Brand Risk Reputation	Source code review	
Incident Management Framework		Physical Security review & Social Engineering	
Crisis Management Framework		BC and DR Tests	
Maturity Monitoring		Incident and Crisis Simulation	

Design

CYBERFLIP

Objective:

Building a Governance & Risk Management framework tailored to DORA requirements.

- Gap analysis
- ICT risk management framework
- ICT risk assessment
- Business Continuity Management System
- Incident Management Framework
- Crisis Management Framework
- Maturity Monitoring

CYBERFLIP

ICT Risk Assessment and ICT Risk Management Framework

"How to efficiently manage all these requirements?"

Gap Analysis & ICT Risk Assessment

Need

Transform a list of requirements into tailored accurately prioritized actions

Solution

Quantitative approach to transform Risk Assessment into a decision-making tool bridging the gap between technology, regulatory requirements and business objectives.

DORA Requirements:

- ✓ ICT risk management
- ✓ Managing of ICT third-party risk

ICT risk management framework

Need

Efficiently integrate compliance requirements into everyday business

Solution

Design a tailored framework based on DORA requirements and unique operational or additional regulatory needs for each Organization.

DORA Requirements:

- ✓ All

Design

CYBERFLIP

ICT Resilience

"How to feel confident that you will survive?"

BCMS Design

Need

Focus on what actually "runs the business"

Solution

Pragmatic approach to fast identify the "crown jewels" and build the BC capability around them.

DORA Requirements:

✓ ICT risk management

IM and Crisis Management Framework

Need

Not only being able to respond but feel confident that Crisis is managed

Solution

Design a specific framework with pre-defined responsibilities of internal and external parties harmonically integrating technical and non-technical roles.

DORA Requirements:

✓ ICT risk management

✓ ICT-related incident management

CYBERFLIP

Monitor and Improve

"Measure your ongoing compliance Journey"

ICT security maturity assessment and monitoring

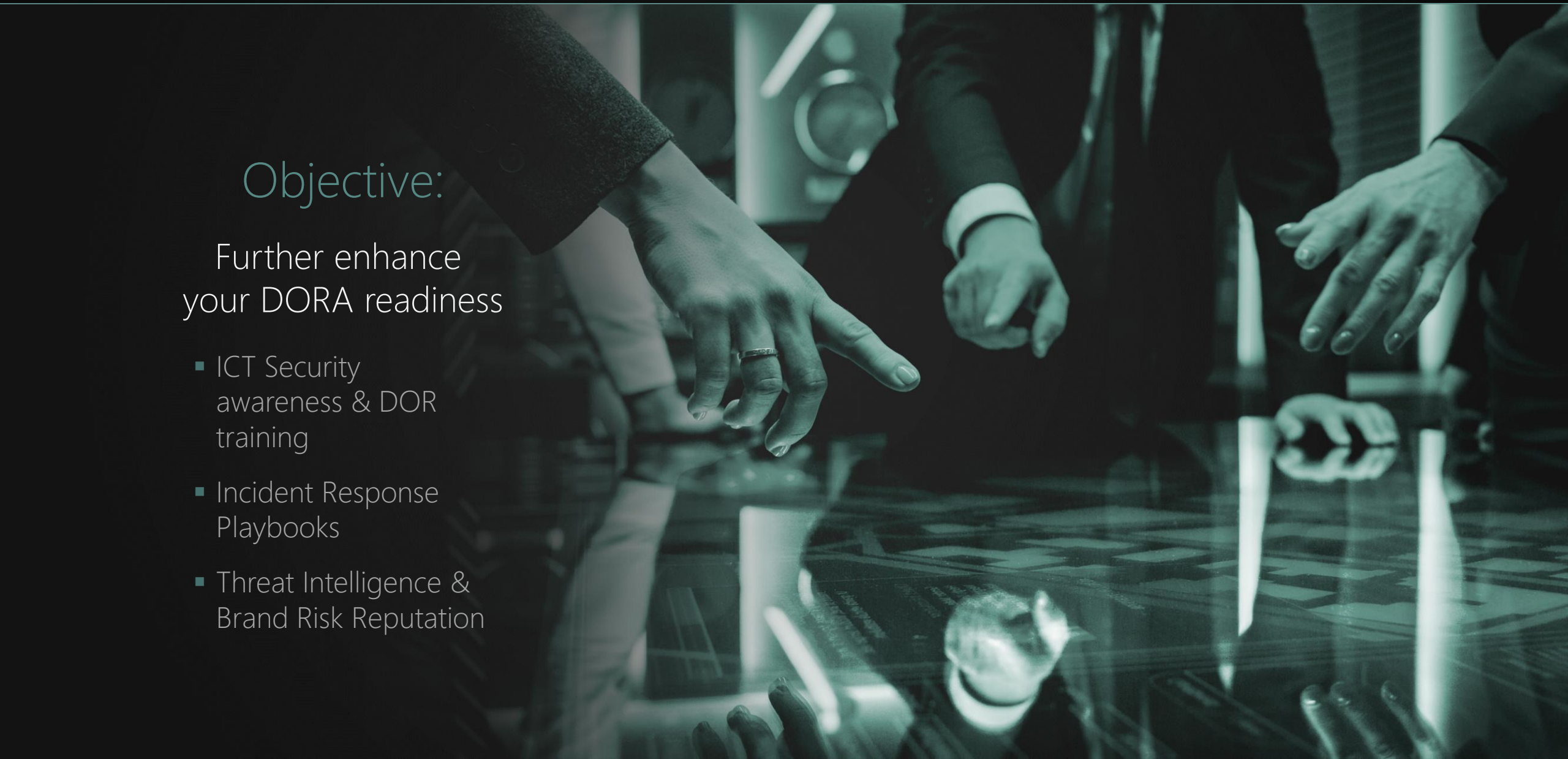
Need	Solution
Define the exact level of readiness	Monitor the level of readiness through a CMMI scale with tailored target points.

DORA Requirements:

✓ ICT risk management

Enhance

CYBERFLIP



Objective:

Further enhance your DORA readiness

- ICT Security awareness & DOR training
- Incident Response Playbooks
- Threat Intelligence & Brand Risk Reputation

CYBERFLIP

Awareness and training

"How to build real awareness?"

ICT security awareness and Digital operational resilience training

Need

Re-gain user interest to achieve real awareness and enhance the most important control – human factor.

Solution

Tailored training program including a blend mix of multimedia, classrooms and social engineering tests, fitted to each Organization's unique profile.

DORA Requirements:

✓ ICT risk management

CYBERFLIP

Incident Response Capability

"Define your threats. Define your response holistically"

Incident Response Playbooks

Need	Solution
Being able to handle specific incidents efficiently.	Specific playbooks, tailored to each industry covering end-to-end response and recovery including technical and non-technical roles on the same frame.

DORA Requirements:

- ✓ ICT risk management
- ✓ ICT-related incident management

Enhance

CYBERFLIP

Digital Risk Monitoring

" Are you one step ahead ? "

Threat Intelligence & Brand Risk Reputation

Need

Get timely notified about new threats and potential breaches related to your firm.

Solution

Threat Intelligence and Brand Risk Reputation as a service through innovative AI driven platform.

DORA Requirements:

- ✓ Managing of ICT third-party risk
- ✓ Information sharing arrangements

Assess

CYBERFLIP

Objective:

Assess your readiness

- Penetration tests
- Vulnerability assessments
- Red & Purple teaming
- Source code review
- Physical security review
- Social Engineering
- BC and DR tests
- Incident response simulation
- Crisis management simulation

CYBERFLIP

Technical Assessments

"How to ensure actual implementation of technical controls?"

Penetration tests and Vulnerability Assessments

Need

Ensure that technical implementations are secure.

Solution

Tailored tests from experienced ethical hackers with clear and defined scope utilizing latest trends.

DORA Requirements:

✓ DOR testing

CYBERFLIP

Be the attacker

"What if a malicious hacker targets your Organization?"

Red & Purple teaming

Need

Investigate how deep a malicious hacker could reach and what the real impact could be

Solution

Run zero-knowledge hacking exercises from experienced ethical hackers and test in practice your security controls

DORA Requirements:

✓ DOR testing

CYBERFLIP

Source code security

"Is your code secure ? "

Source Code Reviews

Need

High quality independent source code review.

Solution

Engaging experts and utilizing technology to identify your code weaknesses and suggest mitigations.

DORA Requirements:

✓ DOR testing

CYBERFLIP

Physical Security

"How difficult is to evade your premises ?"

Physical Security Review & Social Engineering Tests

Need

Assess the mechanisms against physical penetrators.

Solution

A mixed offering of physical security walkthrough and social engineering exercises targeting to gain physical access into critical premises

DORA Requirements:

✓ DOR testing

CYBERFLIP

Simulate

"Are you ready to respond and recover?"

Incident response & Crisis simulations

Need

Experience a real-world scenario and test actual readiness.

Solution

Simulate playbooks utilizing into a combined exercises that involves the participation of all roles.

DORA Requirements:

- ✓ ICT Risk Management
- ✓ Digital operational resilience testing

BC & DR Tests

Need

Feel confidence to manage critical events without jeopardizing your business

Solution

Mutually design a real-world scenario and monitor Organization's performance a disruptive event.

DORA Requirements:

- ✓ DOR testing

Your Journey Towards DORA Compliance

CYBERFLIP

Initial Phase (Steps 1,2)

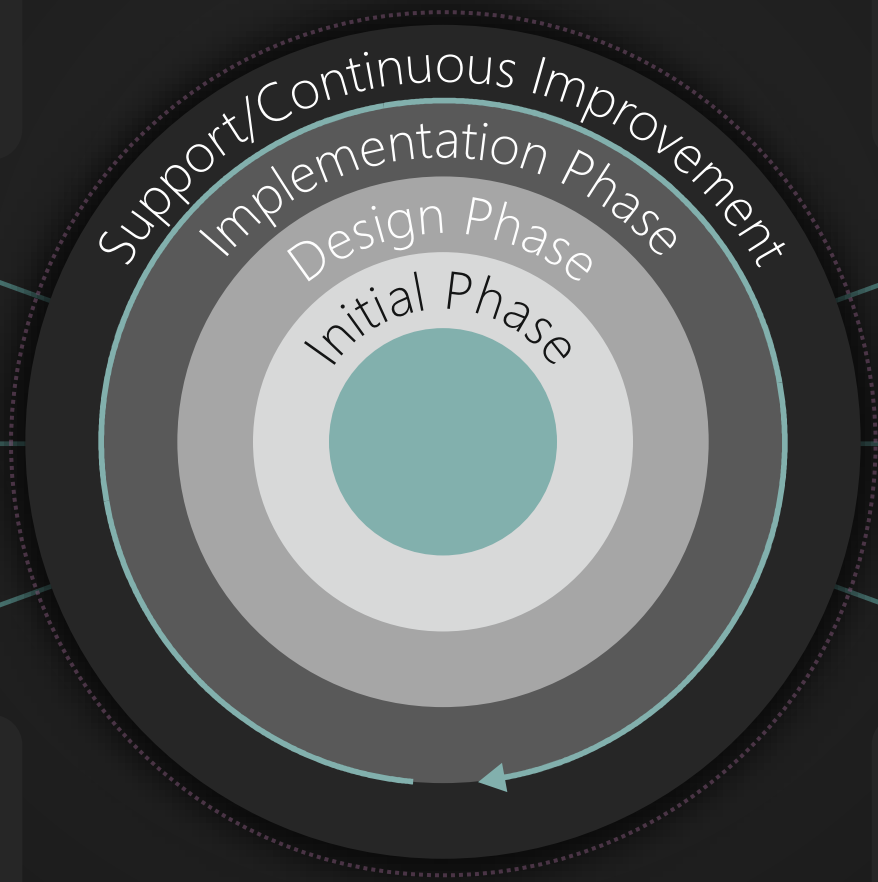
Identifying status (Gap analysis) and prioritize needed actions (Risk Assessment).

Design bundle

Implementation Phase (Step 4)

Guide the Organization into integrating security policies into daily operations.

Design, Enhance bundle



STEP 1 Gap Analysis

STEP 2 Risk Assessment

STEP 3 Design

STEP 4 Implementation

STEP 5 Review

STEP 6 Improvement

Design Phase (Step 3)

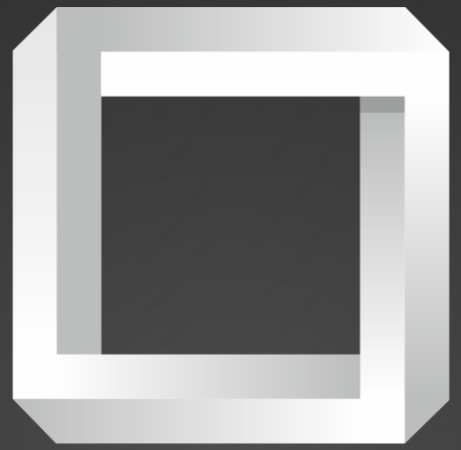
Design of a DORA compliant framework, tailored to Organization's unique needs.

Design, Enhance bundles

Continuous Improvement

Activities that assist Organization into maintaining compliance at the most efficient manner.

Assess bundle



CYBERFLIP

Cybersecurity for Next Generation Enterprises

Thank you!