



Damien Lachiver

*Senior Manager, Paris
Operational Resilience & Cybersecurity*



Etienne BOUET

*Senior Manager, Paris - Financial Services
Operational Resilience & Cybersecurity*

WAVESTONE







DORA: ROAD TO 2025 AND BEYOND

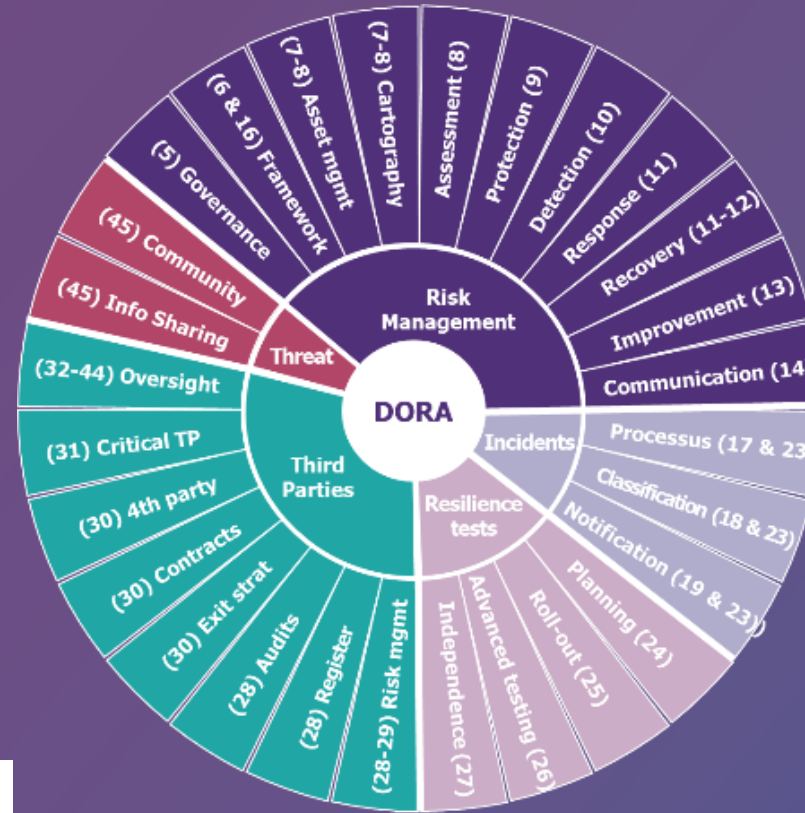
Wavestone Insight Day

23 avril 2024

INTRODUCTION

The Digital Operational Resilience Act (DORA) is a European Union regulation aiming to strengthen the financial sector's resilience to ICT-related major incidents

-  **January 16, 2023**
/ Entry into force of DORA
-  **June 19, 2023**
/ Publication of the first batch of RTS/ITS for consultation until September 2023
-  **December 8, 2023**
/ Publication of the second RTS/ITS batch for consultation until March 2024
-  **January 17, 2024**
/ Publication of the final RTS/ITS draft of lot 1
-  **July 17, 2024**
/ Publication of the final RTS/ITS draft of lot 2
-  **January 17, 2025**
/ Entry into application of the DORA regulation



Chapter II
ICT risk management

Chapter III
ICT-related incidents management, classification and reporting

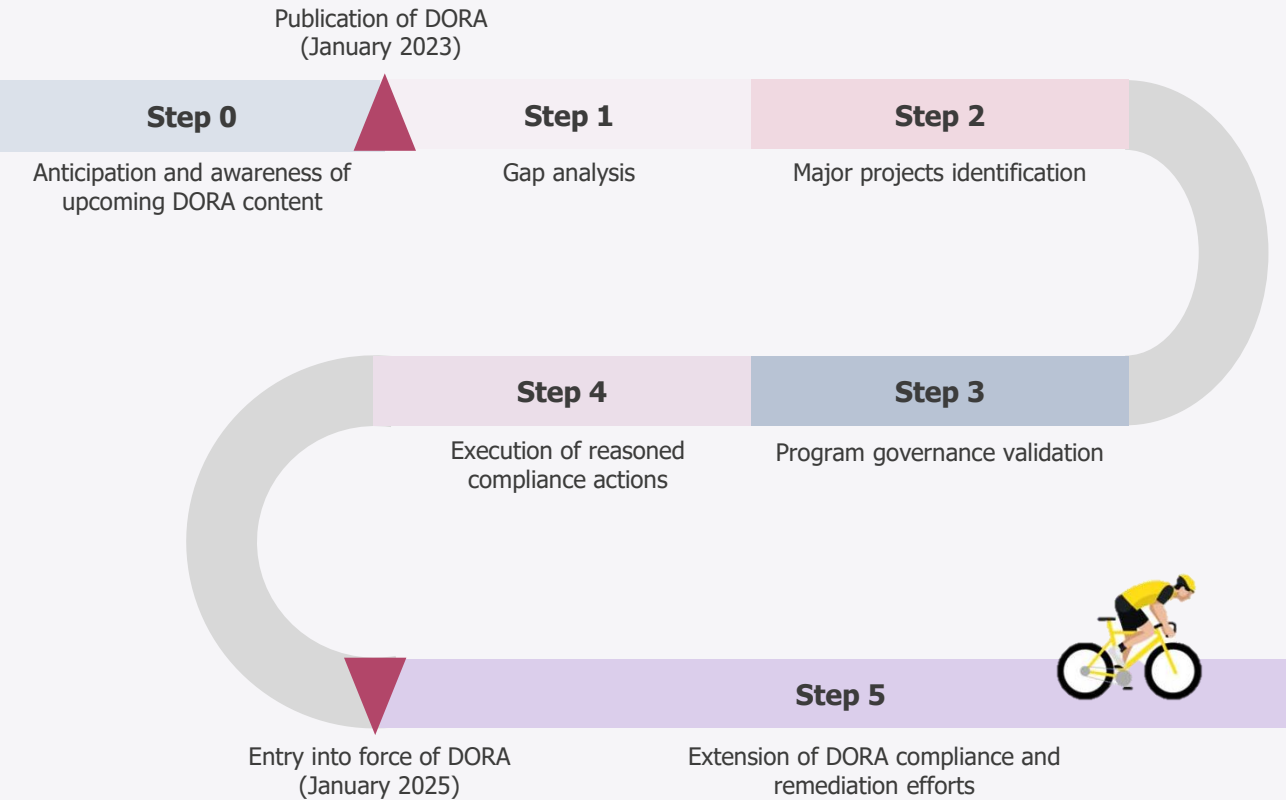
Chapter IV
Digital Operational Resilience testing

Chapter V
ICT third-party risk management

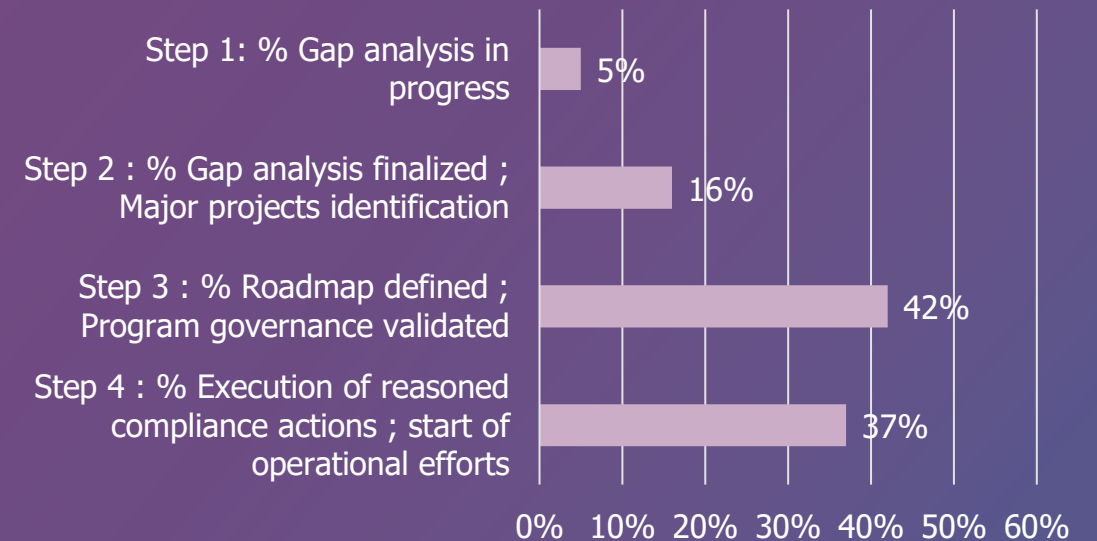
Chapter VI
Information sharing arrangements

THE DORA JOURNEY

The market standard approach to DORA ...



... and where our clients are to date



Benchmark of 19 Banking & Insurance entities supported by Wavestone

PROGRAMS MOBILIZE TRANSVERSALLY ACROSS THE ORGANIZATIONS

**VERY HETEROGENEOUS
STAKEHOLDERS TO COORDINATE**

**STREAM LEAD ROLES DO NOT
OBVIOUSLY FALL UNDER AN EXISTING
FUNCTION**

**SPONSORSHIP NEEDS TO BE AT A
LEVEL THAT ENSURES THE
APPROPRIATE IMPLICATION FROM
ALL STAKEHOLDERS (COO-LEVEL)**



NOW, LET'S BE REALISTIC...

**ALMOST NOBODY WILL BE
FULL COMPLIANT IN JANUARY
2025**

**DORA ROADMAPS EXTEND TO
2026 OR 2027**

**ARBITRATIONS HAVE BEEN
MADE TO FOCUS ON
NORMATIVE ACTIONS IN 2024**

Let's take a closer look chapter by chapter at:



Where you should be

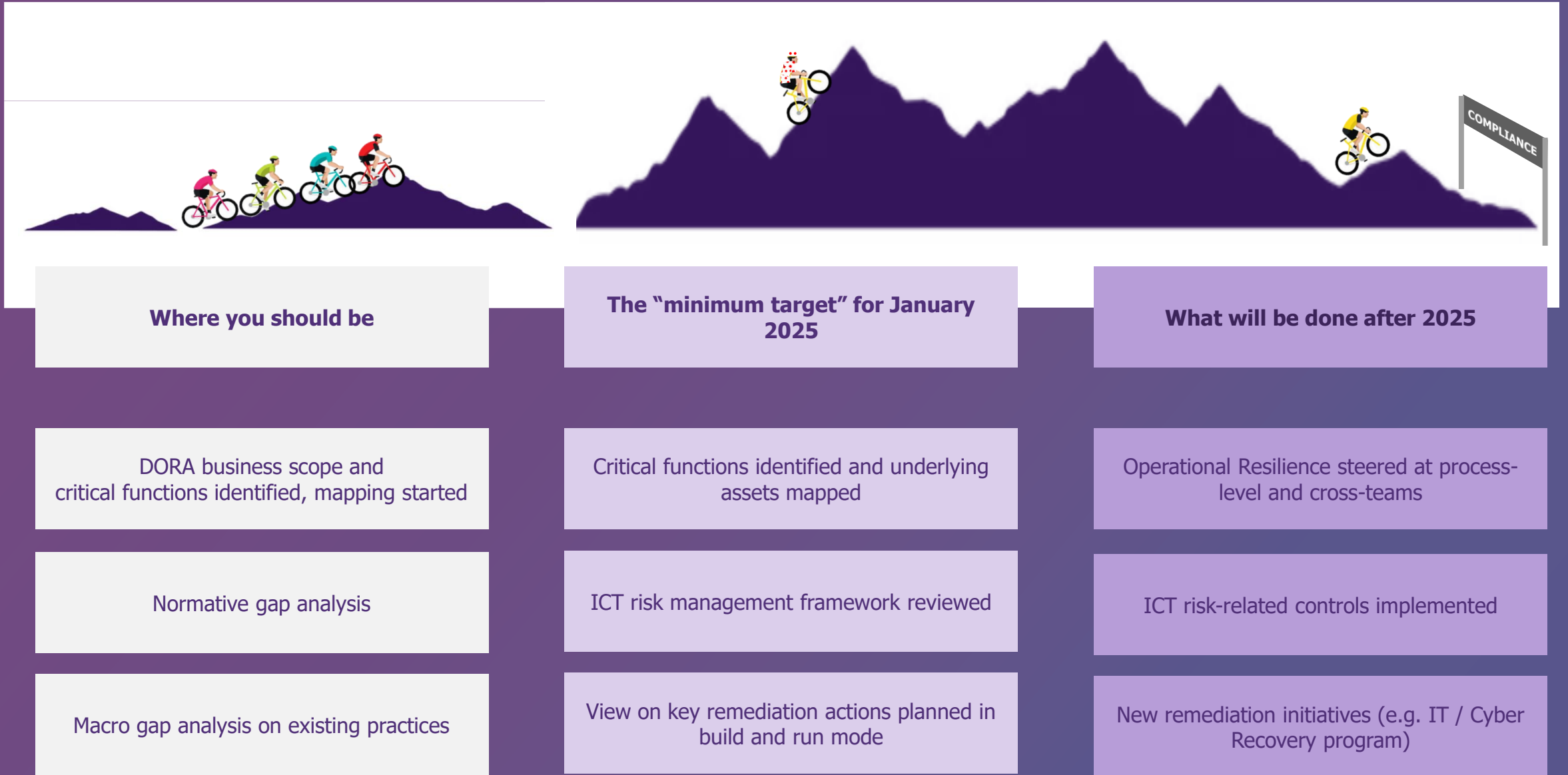
The "minimum target" for
January 2025

What you should do in a
second phase

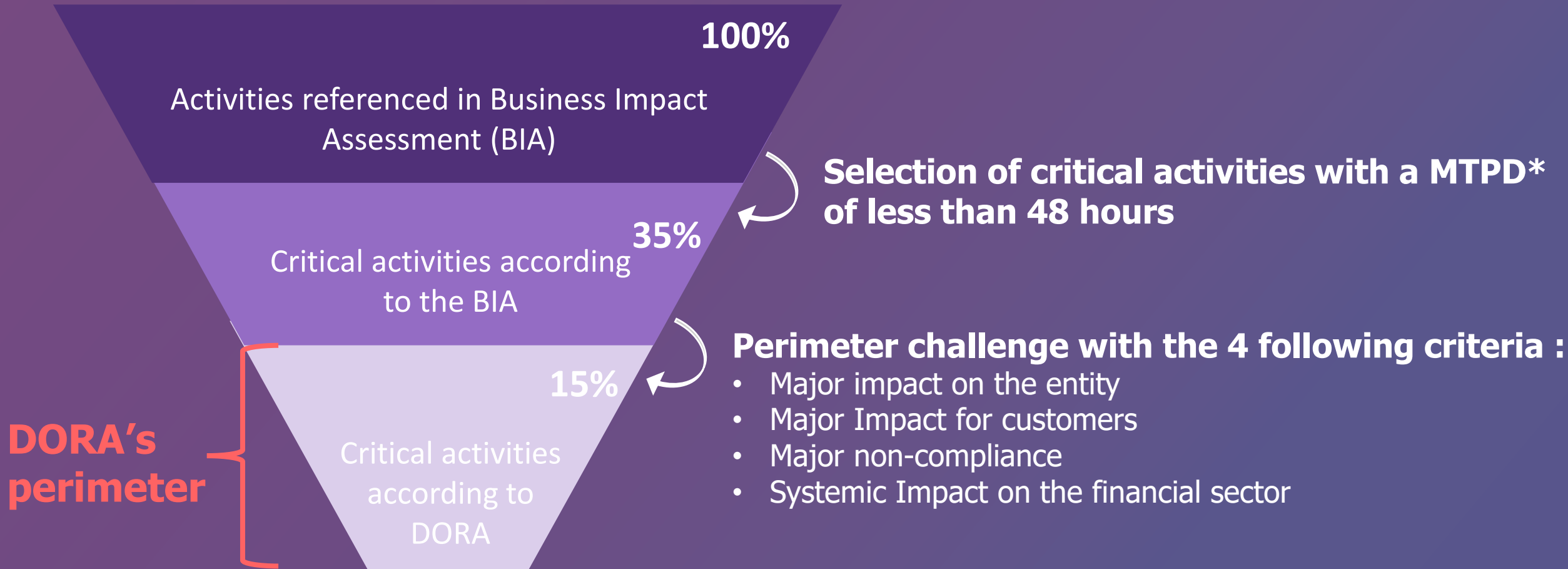
AGENDA

- 1. ICT RISK MANAGEMENT: FROM NORMATIVE EFFORTS TO CONVERGENCE**
- 2. INCIDENT MANAGEMENT: A STRONG CHALLENGE ON NOTIFICATION DELAYS**
- 3. TESTING: A STRATEGIC VISION TO BUILD (NOT ONLY ON TLTP)**
- 4. THIRD-PARTY RISK MANAGEMENT: BUILD, REINFORCE AND INDUSTRIALIZE**

CHAPTER II - ICT RISK MANAGEMENT FRAMEWORK

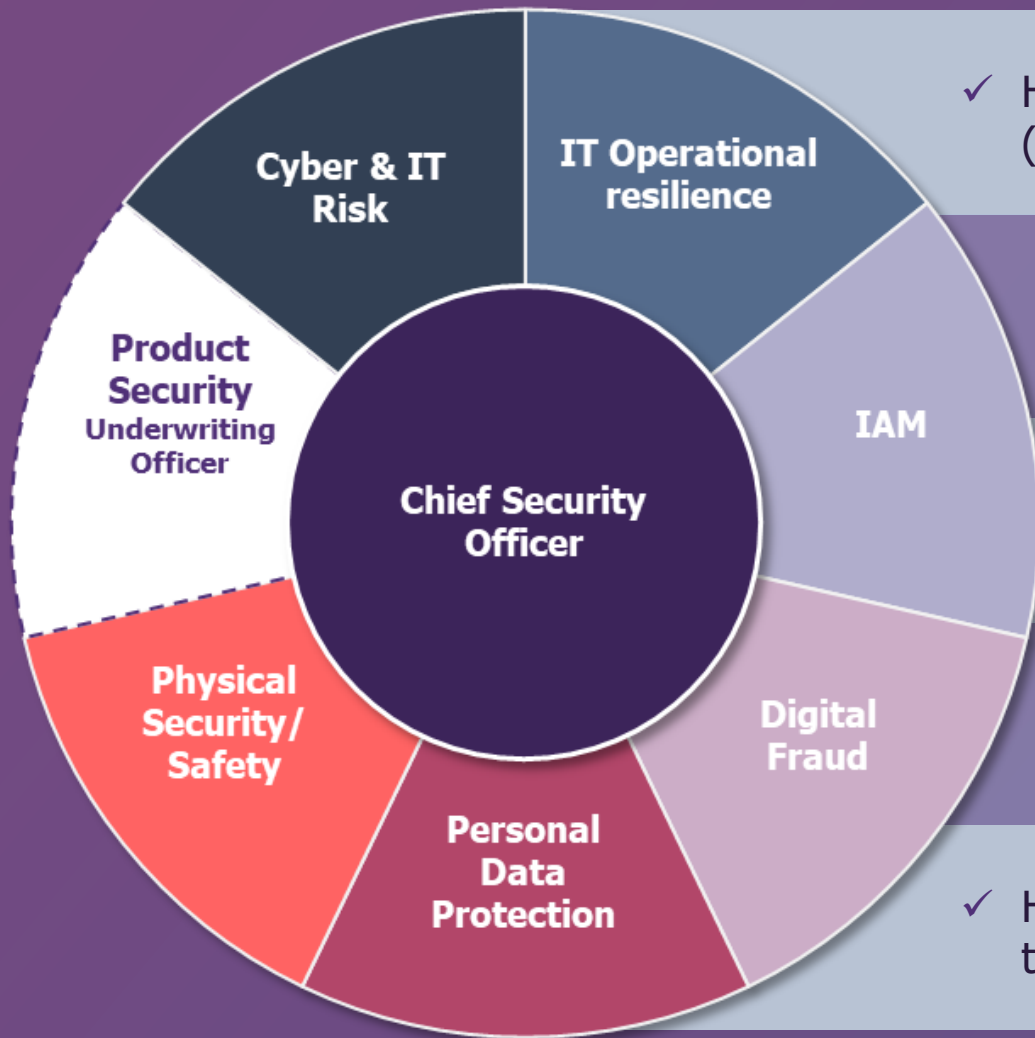


DORA FOCUSES ON CRITICAL BUSINESS ACTIVITIES



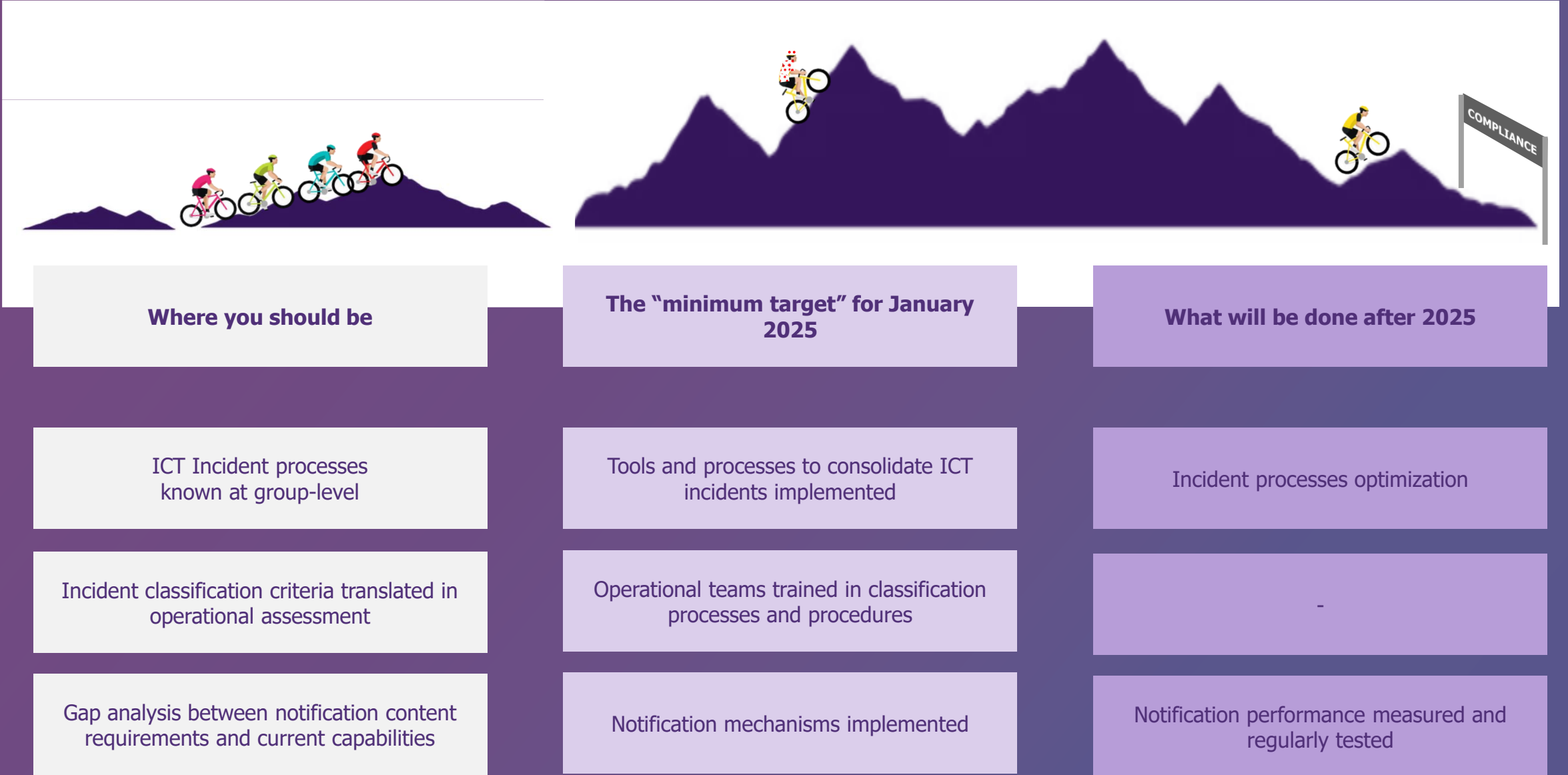
* MTPD : Maximum tolerable period of disruption

MID-TERM, CONSIDER GOING FURTHER ON ICT RISK CONVERGENCE

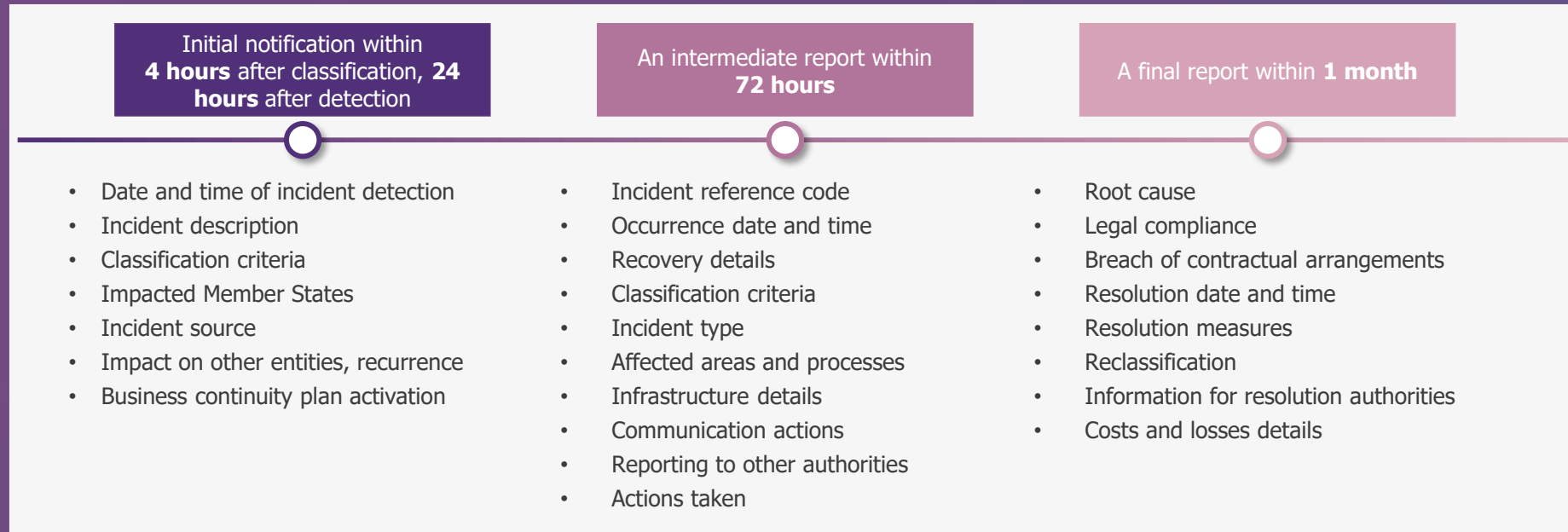


- ✓ Holistic view on ICT risks and reinforced weight on decision-making (especially on historic common pain points such as inventories)
- ✓ Unified and harmonized terminology/taxonomy (inc. critical perimeter scope)
- ✓ Alignment with regulatory approach on audits that does not differentiate between ICT risks
- ✓ Potential efficiency and rationalization gains (Fusion Center, Threat Intelligence, Third-Party Risk Management)
- ✓ HR attractiveness with new career perspectives for the teams on the long term by expanding the risk scope

CHAPTER III - ICT INCIDENTS MANAGEMENT



NOTIFICATION IS A CHALLENGE FOR CONCERNED ORGANIZATIONS

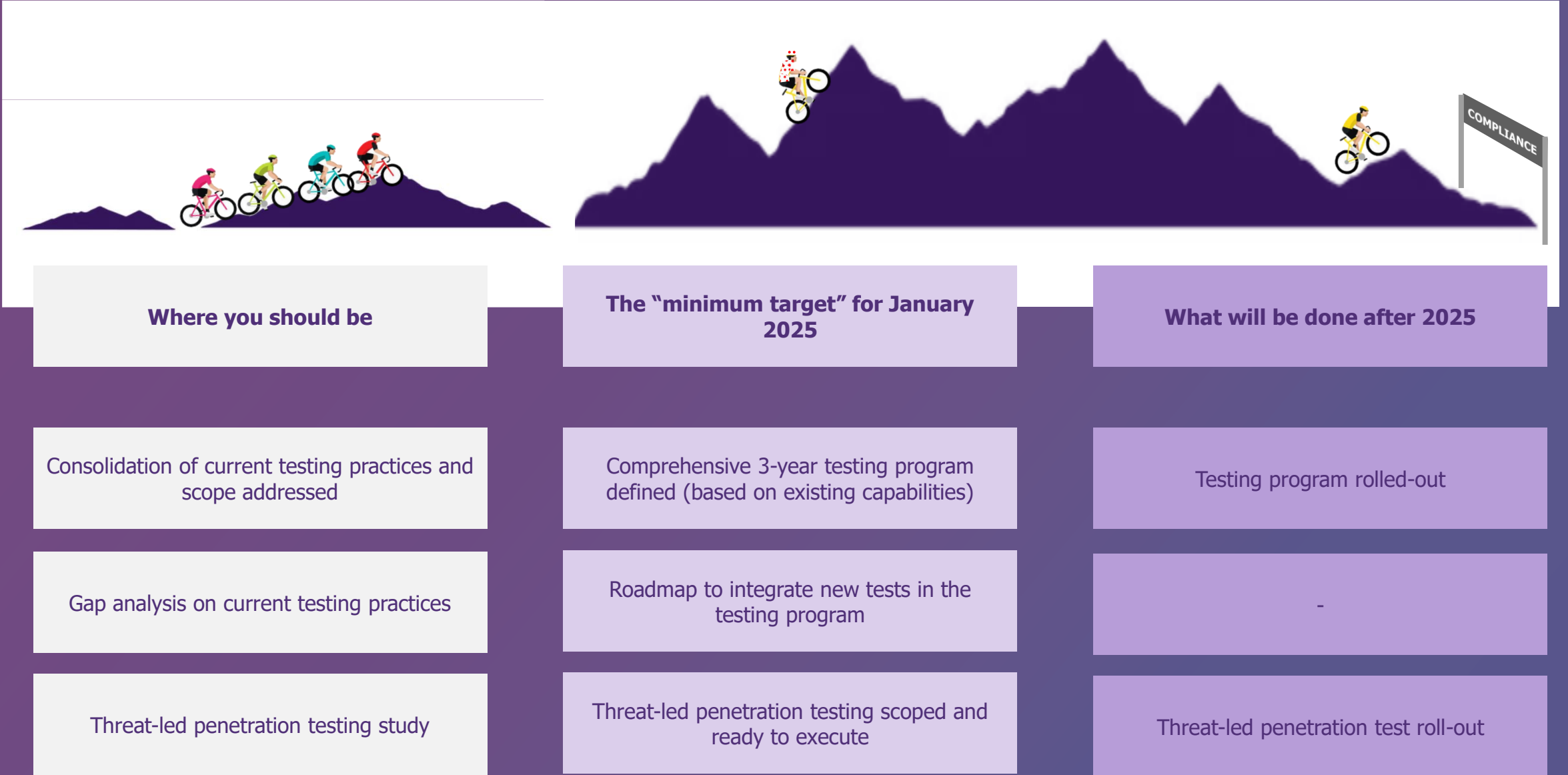


Notification process

Key take-aways

- Fortunately, Cyber teams are used to classify and notify major incidents to authorities
- The first step is to define how to harmonize and converge cyber and IT teams methods (actions and timing)
- Then will come the time to measure and demonstrate the ability to respect delays through KPI and exercises

CHAPTER IV – DIGITAL OPERATIONAL RESILIENCE TESTING



TESTING IS NOT TLPT-ONLY!



Key recommendations

- **Map the tests and identify gaps** with DORA
- For each test **adapt relevant policies and procedures**
- **Build a 3-year program** prioritizing tests with a lower maturity level

Security

- Vulnerability assessments and scans
- Network security assessments
- Physical security reviews
- Questionnaires and scanning software solutions
- Source code reviews where feasible
- Tests on detection mechanisms
- Penetration testing
- **TLPT (Threat-Led Penetration Testing)**

Resilience / Business continuity

- Tests of ICT business continuity plans, ICT response and recovery plans, test of the crisis communication plans
- Tests of the backup procedures and restoration and recovery procedures
- **Tests of exit strategy of ICT third party supporting critical or important functions**

ITSCM / Quality

- Tests of all changes to ICT systems
- Compatibility testing
- Performance testing
- Source code reviews where feasible

Transverse or to be clarified

- Gap analysis
- Open source analyses
- Scenario-based tests
- **End-to-end testing**

Testing to perform

SIGNIFICANT EVOLUTIONS FROM THE CLASSICAL RED TEAMING PHILOSOPHY



Improvable Red Team aspects

Red Team has **too many interpretations**, most often observed as **orthogonal evaluation** of **detection** capabilities as well as **cybersecurity maturity**

Outside of rare Assume Breach cases, there may be **no assessment** of the **internal** security level when **no intrusion vector** is found. Also, **AD is often targeted first**, failing to provide a **clear vision** on the **security** level of **business processes**

Operations are often **stopped upon detection**, giving **false impressions of security** and the providers goal becomes **stealthiness** rather than evaluation, making it **harder** to define the **Blue team action plan**

Operations are often **constrained** by **low budgets** or **short deadlines**, **increasing** the **risk of detection** or **decreasing** the **depth** of the security **assessment**



With TIBER-EU / TLPT

Operations are **standardized**, offer an **improved approach** to Red Teaming and follow a **clear structure** described in **TIBER-EU framework**

End-to-end testing with advanced **business scenarios** is the main goal, using **leg-ups** to **aid providers** should the target environment be **mature enough**

Detection is an **objective for the Blue team** rather than a **failure** for the Red team, to provide a **clearer picture** of the its **intrinsic capabilities**

Operations are **forced** to happen on a **longer timeframe**, better simulating real-world threat actors with **opportunistic approach** or **advanced tooling**

THE CHALLENGES OF THREAT-LED PENETRATION TESTING



International presence

- / Segmentation of activities in **multiple countries** and **subsidiaries**
- / Selection of **leading TLPT authority** and compliance with **foreign laws**
- / Relying on **joint TLPT** operations to **limit overload** on internal support teams

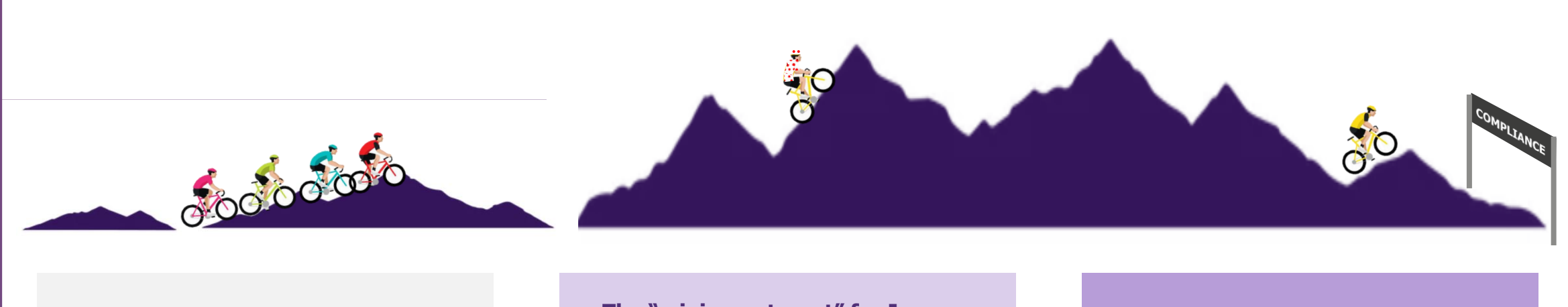
Business lines partitioning

- / **Segment** and **scope Critical Functions** to optimize **costs & workload**
- / Identify **global support teams** and **providers** solicited for **each TLPT**
- / **Validate** the testing **strategy** with **regulators** to forecast organization

Continuous testing

- / TLPT as the **final evaluation** and **attestation** of **continuous** efforts
- / **Stable maturity level** requires continuation of **audit & testing activities**
- / **Pentests** on global **infrastructure** & standard **Red Team** also contribute

CHAPTER V – ICT THIRD-PARTY RISK MANAGEMENT



Where you should be

Critical TP scope set and registry initiated

TPRM process adapted and reinforced

First exit strategy principles scoped

The “minimum target” for January 2025

% of key contracts reviewed

TPRM staffed and operational (including TP audits and other run risk assessment)

Exit strategy studied for a few critical TP

What will be done after 2025

All contracts reviewed / remediated

Extension of processes to 4th party and beyond

Exit strategy designed and tested for all critical TP

BUILD PROGRESSIVELY ITS TPRM SERVICE CENTER



Baseline of its service center

- Establishment of a **TOM** (Target Operating Models), including a **TPRM framework** (policies, procedures and rules)
- **Setting** of TPRM activities and elaboration of **delivery models**
- Establishment of processes to ensure a **high delivery standard for all group entities**

Bronze Package : Groundwork for contractual remediation

- **Inventory and classification** of third parties
- Creation of a **control library** tailored to each category
- Automation of **contractual reviews**
- **Due diligence** and management of **security topics in negotiations**

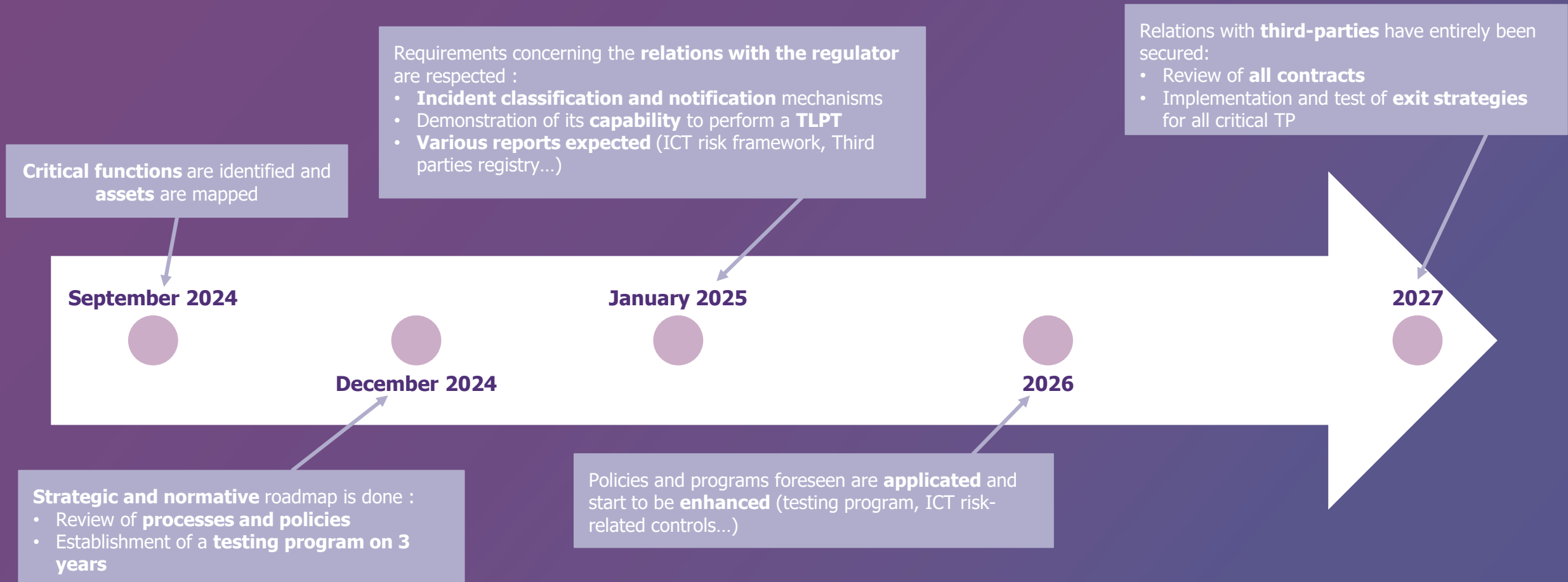
Silver Package : Continuous monitoring of contracts life cycle

- Establishment of **insurance procedures**
- Development of a **testing spectrum**, from automated evidence reviews to comprehensive on-site audits for pivotal providers
- Preparation of procedures to ensure the monitoring and immediate response to **potential vulnerabilities**

Gold Package: Final implementation of all TPRM facets

- Implementation and testing of **exit strategies**
- Performance of **multifaceted crisis exercise**, involving numerous ecosystem stakeholders
- A special focus on **end-to-end testing** that covers **transversally** third-party security, interconnections and exit strategies

CONCLUSION - DORA COMPLIANCE JOURNEY



The Positive Way

WAVESTONE


Etienne BOUET
Senior Manager

Mobile : +33 (0)6 84 51 37 32
etienne.bouet@wavestone.com

Damien LACHIVER
Senior Manager

Mobile : +33 (0)6 68 40 69 82
damien.lachiver@wavestone.com

wavestone.com

 [Wavestone](#)