Italy’s plans to implement NIS2 Directive

26.01.2022

NIS2 Directive implementation blocks

- National cybersecurity strategy
- National cyber crisis management framework
- CSIRT and technical support
- Risk management measures and reporting obligations
- Supervision
- Coordinated vulnerability disclosure

National cybersecurity strategy – The challenges to face

- NIS2 ready revision adopted in may last year
- Aims to **achieve the national and European strategic autonomy** in the digital domain, given the evolution of the technological and systemic risks

Cyber Risk

- Cyber-attack Risk
- Technological Risk
- Disinformation Risk

- Anticipate the evolution of cyber threats
- Cyber crises management
- National and European digital strategic autonomy
- Tackling online disinformation also in relation to hybrid threats

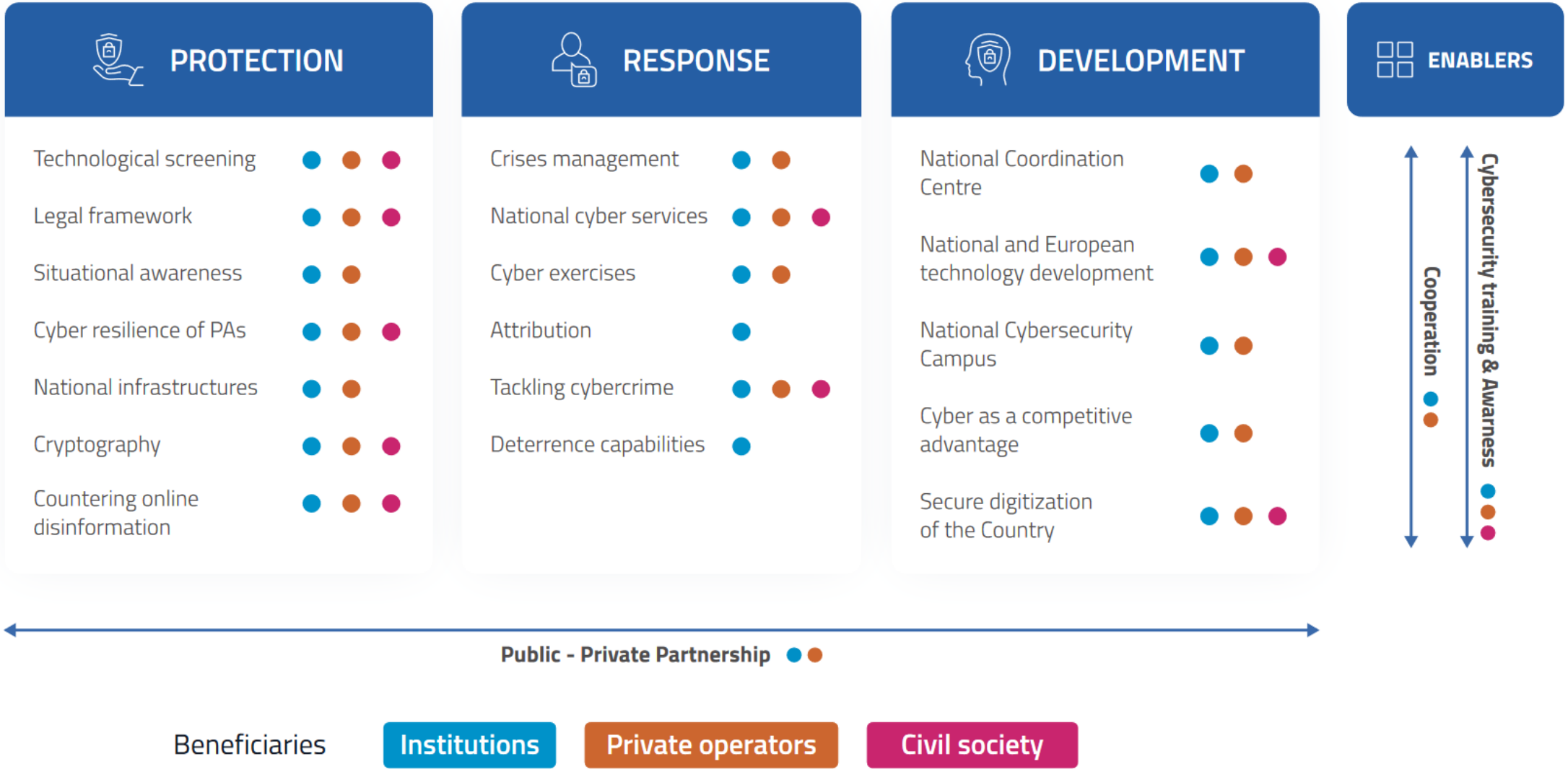
Development

Response

Protection

National cybersecurity strategy – Goals

- The three goals identified have been **grouped by thematic areas** from an organizational, policy and operational point of view
- 82 implementing measure ensure the **effective implementation of the Strategy**



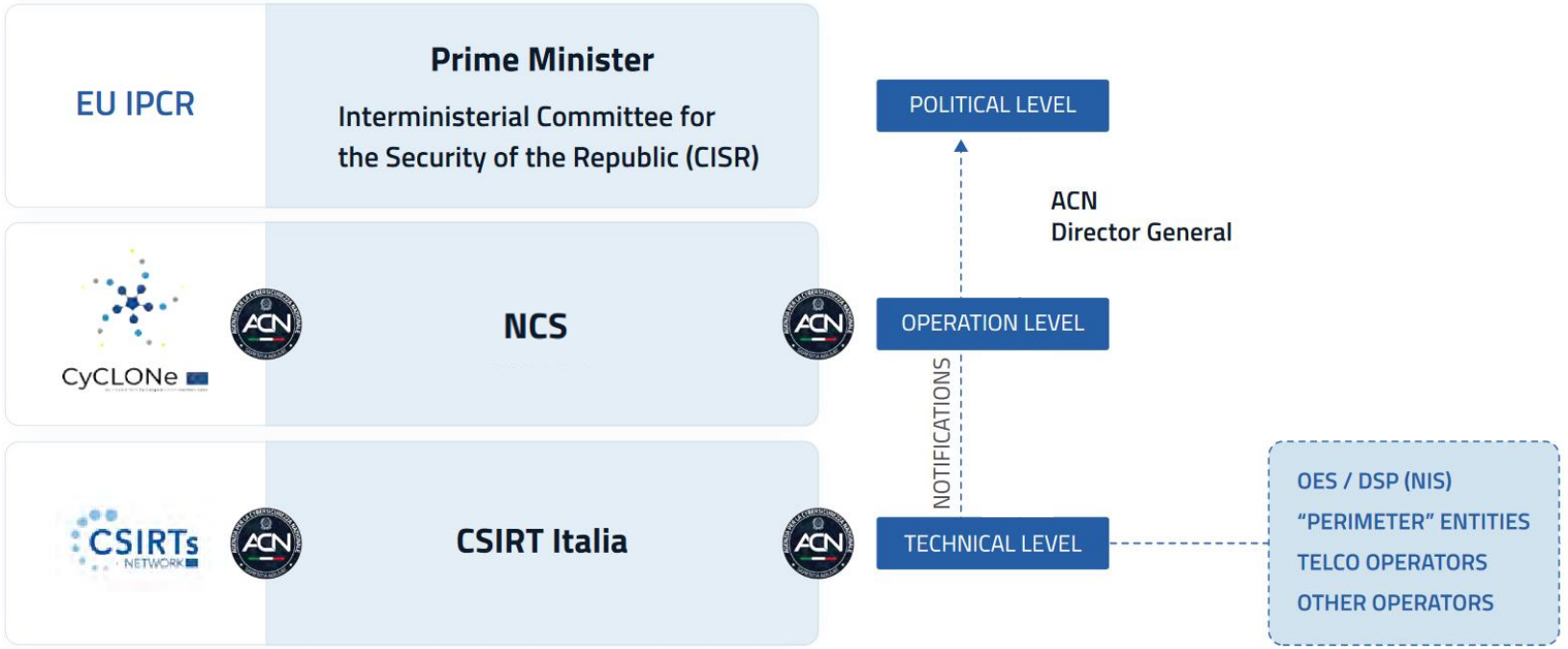
National cyber crisis management framework

5 measure of the national strategy are aimed at improving cyber crises managament.

2 measures dedicated to exercises

Strengthened cyber crises management, with the National CyberSecurity Cell (NCS) and the Agency at its core.

Full integration with the EU, NATO and international relevant mechanisms.



CSIRT and technical support

CSIRT within the Operations Directorat.

Still growing with ongoing recruitments

Tiered approach to the constituency with multiple digital tools being developped to handle the large number of entities

8 measures in the national strategy dedicated to national cyber services, including HyperSOC, HPC and ISACs

(supported by Recovery and Resilience funds)

Risk management measures and reporting obligations

Pending the outcome of NIS Cooperation Group actitivies

Pending the adoption of Commission's delegates Act

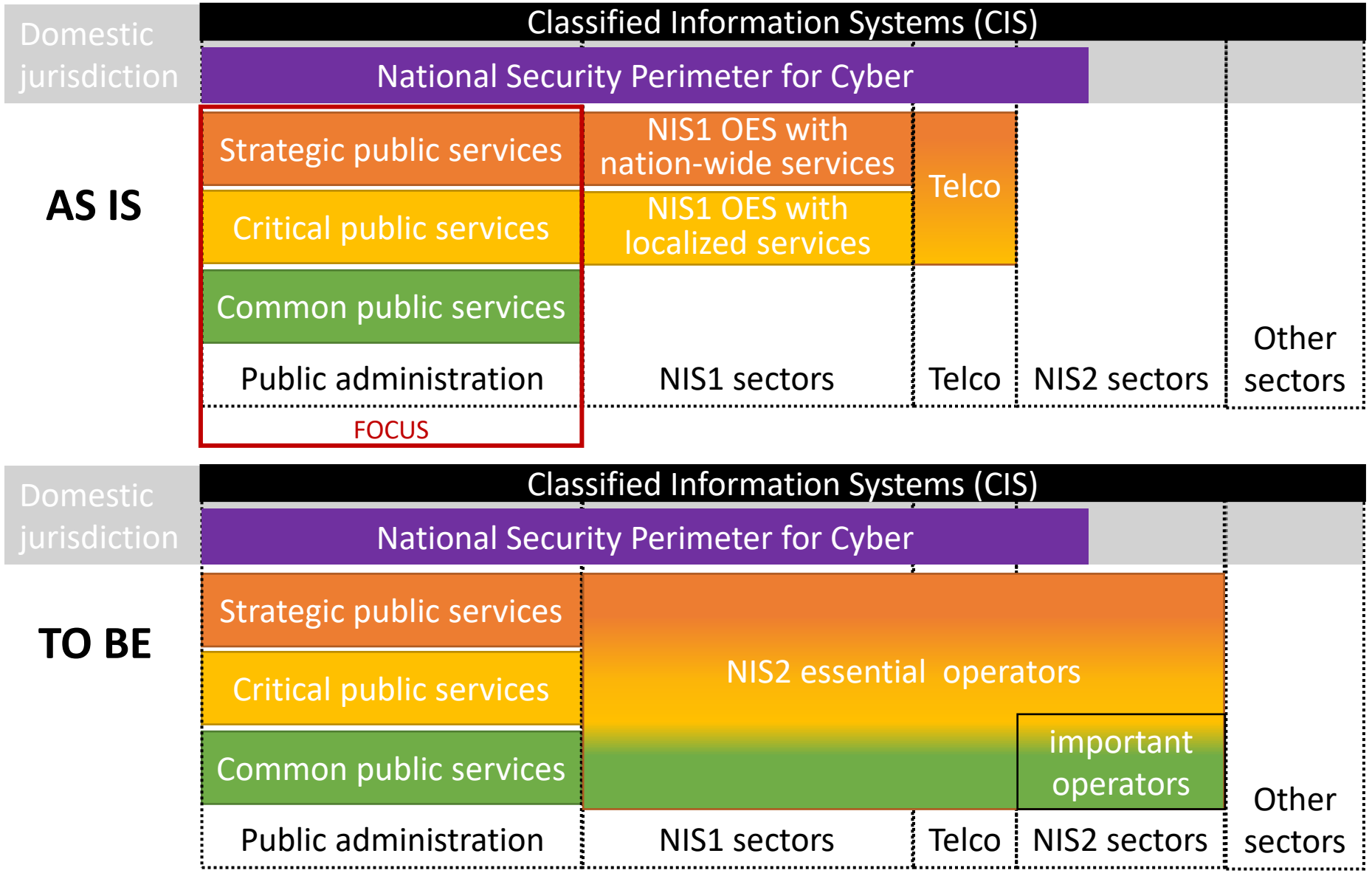
Should be compatible with the current national framework

Initial take on the task

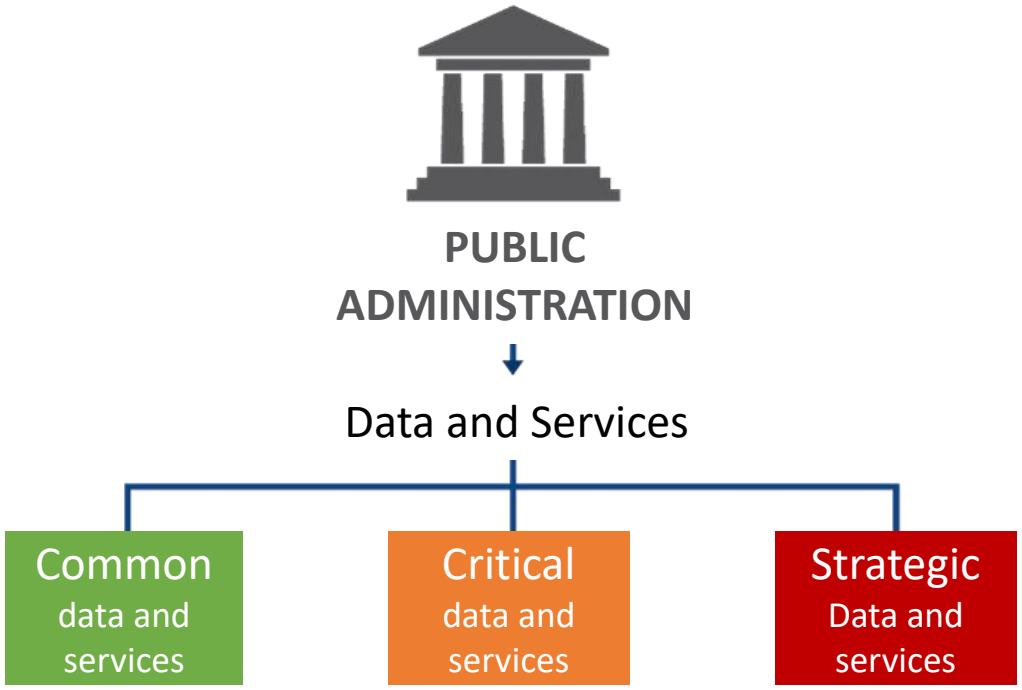
Current national approach

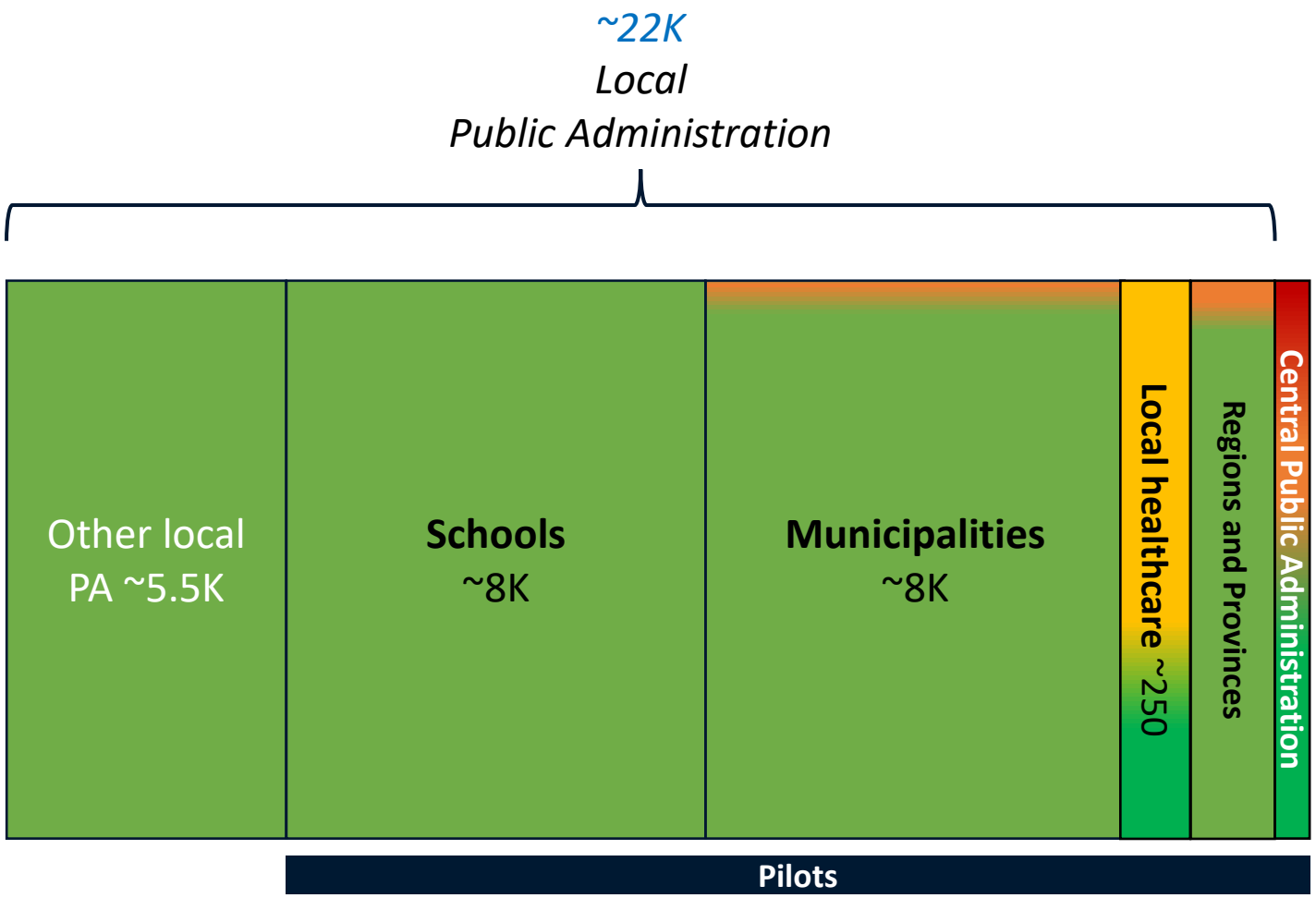
- Tiered set of requirments and obligations ensuring appropriate cost/risk balance
- Measures rooted in the Italian Cybersecurity Framework (NIST) across all regulations
- High-level binding rules on the effects based on risk management with non-binding guidance on the implementation

Risk management measures and reporting obligations

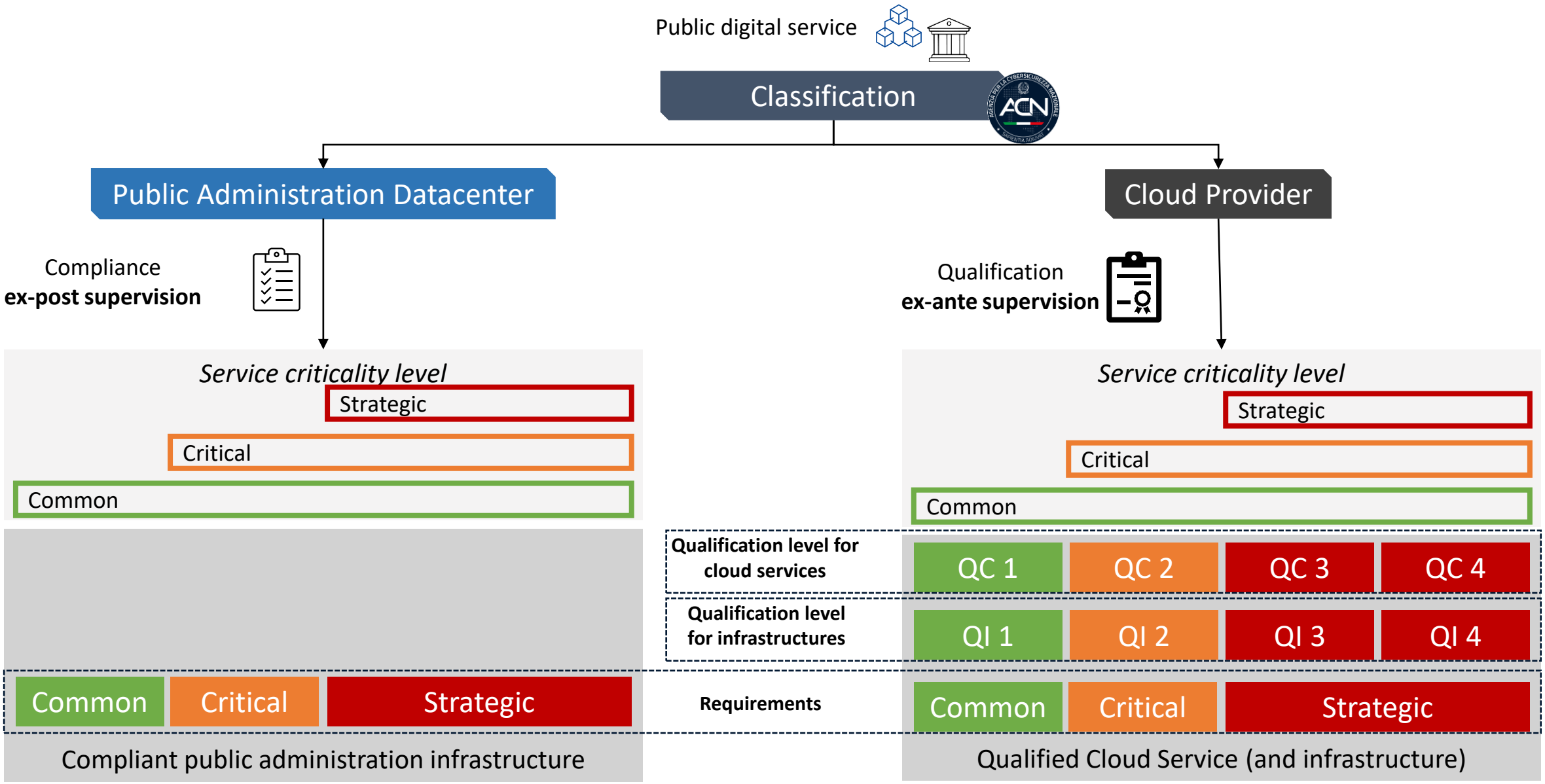


Case case: Public service and data classification





Use case: Tiered risk management measures and reporting obligations in PA



Supervision

Measure #3 of the national cybersecurity strategy mandates the activation of a central inspection team

(supported by Recovery and Resilience funds)

Recent establishment of

Authority & Sanction Directorate

and

Certification & Supervision Directorate

Provided the number of entities to be supervised, the approach will most likley be tiered

No specific approach has been developed yet

Coordinated vulnerability disclosure

Measure #9 of the national strategy mandates the adoption of a national policy

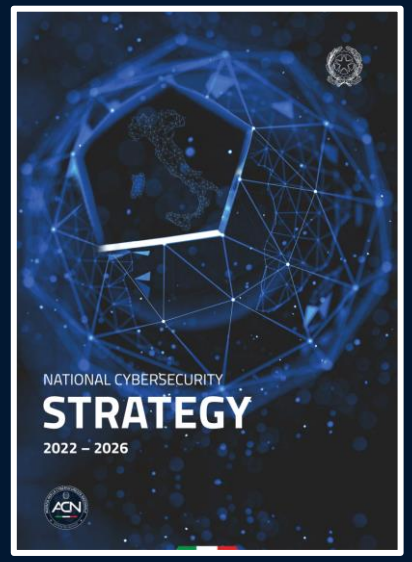
Complex interplay with national criminal law

Interministerial activity

Agency, Ministry of Interior and Ministry of Justice

European activity

Dedicated strand of NIS Cooperation Work Stream



- D.L. 82/2021 – Establishment of the National Cybersecurity Agency and renewal of the national cybersecurity architecture
- D.L. 105/2019 – National Security Perimeter for Cyber
- Determinazioni 625/2021, 306/2022, 307/2022 – Cloud Regulation