

SECTORS COVERED BY THE ACT
(based on the adopted amendment to the National Cybersecurity System Act)

I. ESSENTIAL ENTITIES
(Annex 1 to the Act)

SECTOR	SCOPE OF ENTITIES (EXAMPLES)	PRACTICAL COMMENT
1. ENERGY	Generation, transmission, distribution and trading of electricity; gas; oil; hydrogen; electricity system operators	Covers not only “large corporations” but also operators of technical and system infrastructure
2. TRANSPORT	Air, rail, water (maritime and inland), and road transport; infrastructure operators; traffic management	Also applies to entities managing fleets, terminals and logistics centres
3. BANKING AND FINANCIAL MARKET INFRASTRUCTURE	Banks; credit institutions; payment infrastructure; settlement systems	Subject to the precedence of the DORA Regulation with regard to risk management measures and incident reporting
4. HEALTH	Healthcare providers; laboratories; e-health infrastructure; entities processing medical data	Also includes private healthcare entities
5. DRINKING WATER AND WASTEWATER	Water supply companies; wastewater operators; infrastructure operators	Critical from a public health perspective
6. DIGITAL INFRASTRUCTURE	DNS service providers; TLD registries; cloud service providers; data centres; electronic communications network providers; internet exchange points (IXPs)	One of the most heavily regulated sectors
7. PUBLIC ADMINISTRATION	Central government authorities; selected public bodies; local government units (subject to simplified requirements – Annex 4)	Local government units are classified as either essential or important entities depending on their scope of activity

II. IMPORTANT ENTITIES

(Annex 2 to the Act)

This category includes the largest group of companies that were previously outside the scope of the National Cybersecurity System Act.

SECTOR	SCOPE OF ENTITIES (EXAMPLES)	PRACTICAL COMMENT
1. INDUSTRIAL MANUFACTURING	Large-scale food production; industrial processing; chemical manufacturing; pharmaceuticals; machinery; electrical equipment; computer and electronic equipment; vehicle manufacturing	Includes traditional factories, facilities using industrial automation (OT/SCADA), ERP systems
2. LOGISTICS AND WAREHOUSING	Logistics operators; distribution centres; supply chain management entities	A cyber incident may result in operational downtime
3. WASTE MANAGEMENT	Waste processing entities; installation operators	A newly regulated sector
4. WHOLESALE AND DISTRIBUTION	Distributors of products in regulated sectors; commercial infrastructure operators	Particularly relevant in regulated sectors
5. DIGITAL SERVICES	Online platforms; marketplaces; data processing service providers; SaaS providers; managed service providers (MSPs)	Also applies to technology companies servicing other entities
6. BUSINESS PROCESS OUTSOURCING	Shared services centres; payroll outsourcing; HR outsourcing; large-scale data processors	Particularly where services are provided to essential entities