REPUBLIC OF TÜRKiYE
ENERGY MARKET
REGULATORY AUTHORITY

CYBER SECURITY MATURITY MODEL IN ENERGY SECTOR

Nuray DEDEOĞLU

Information Security Group Head

Department of ICT/EMRA

ERRA & 21.02.2025

NURAY DEDEOĞLU

- 2006, B.Sc. Computer Engineering (Bilkent University, Ankara, Türkiye, Honor Degree)
- 2006-2010, Assistant Specialist, Prime Ministry of Türkiye
- 2010-2013, Assistant Energy Specialist, EMRA
- 2013-2019, Energy Expert, EMRA
- 2019- ,Information Security Group Head, EMRA

Agenda

- The Duties and Strategies of EMRA in the Cyber Security of the Energy Sector of Türkiye
- Future Projects
- Cyber Threats in the Energy Sector
- Conclusion

Responsibilities of EMRA in Energy Sector Cyber Security

October 2012	• Decision on the Execution, Management and Coordination of National Cyber Security Studies
May 2013	• Establishment of National Computer Emergency Response Team – TR-CERT(Sectoral and Institutional CERTs)
June 2013	• Entry into force of National Cyber Security Strategy and 2013-2014 Action Plan
September 2016	• Introduction of 2016-2019 National Cyber Security Strategy and Action Plan
July 2018	• Establishment of Digital Transformation Office of the Presidency of the Republic of Türkiye
July 2020	• Publication of Information and Communication Security Guide
December 2020	• Entry into force of National Cyber Security Strategy and Action Plan (2020-2023)
September 2024	• Entry into force of National Cyber Security Strategy and Action Plan (2024-2028)
January 2025	• Establishment of Cybersecurity Directorate

Critical Infrastructure Sectors

- Energy
- Telecommunications
- Water Management
- Finance
- Transportation
- Critical Utilities

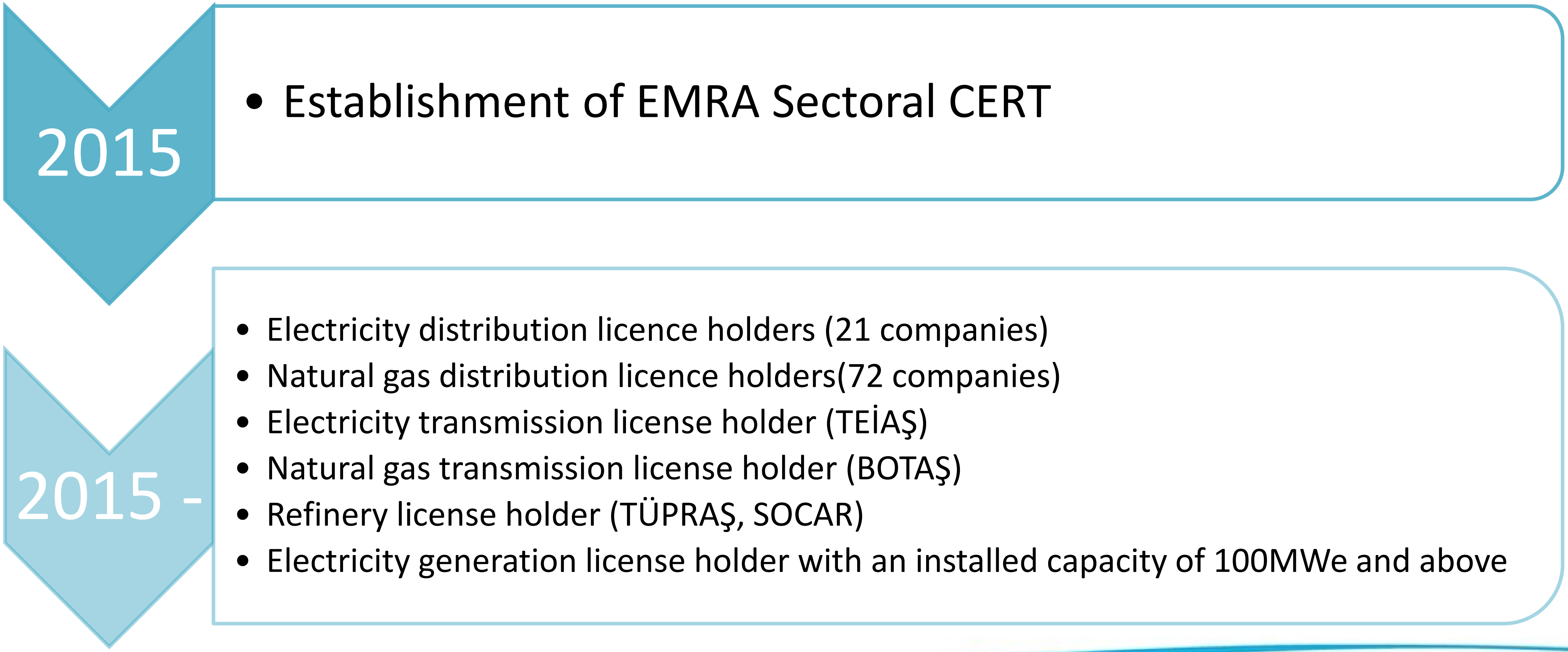
EMRA Actions

- 2013-2014 Action Plan
  - Action No. 1.3: Making ISO/IEC 27001 Information Security Management System(ISMS) standard mandatory for public institutions and private entities in critical infrastructure sectors
- EMRA Action:
  - Introducing the obligation to comply with the ISO/IEC 27001 ISMS standard in EMRA Licensing Regulations (Electricity, Natural Gas, Oil)

EMRA Actions

Sector	# of Entities Obliged to Obtain ISO/IEC 27001 Certificate	# of Entities Received Certificates
Natural Gas Distribution	73	72
Natural Gas Transmission	1	1
Electricity Distribution	21	21
Electricity Transmission	1	1
Electricity Market Operation	1	1
Electricity Generation	150	140
Oil Transmission(by pipeline)	2	2
Refinery	5	5
Total	254	243

EMRA Actions(Establishment of Sectoral CERT and Institutional CERTs)



2015

- Establishment of EMRA Sectoral CERT

2015 -

- Electricity distribution licence holders (21 companies)
- Natural gas distribution licence holders(72 companies)
- Electricity transmission license holder (TEİAŞ)
- Natural gas transmission license holder (BOTAŞ)
- Refinery license holder (TÜPRAŞ, SOCAR)
- Electricity generation license holder with an installed capacity of 100MWe and above

EMRA Actions

- 2016-2019 Action Plan
  - Action No. 1.4: Strengthening Cyber Defense Capacity and Protecting Critical Infrastructures
- EMRA Action:
  - Regulation on Information Security in Industrial Control Systems Used in the Energy Sector (2017)
  - Information security audit and review processes in energy sector

EMRA Actions

- 2016-2019 Action Plan
  - Action No. 1.6: Update of legislation regarding the determination that security testing (penetration testing, APT analysis, etc.) services will be received from natural and legal persons who are document holders.
  - Action No. 1.7: Making penetration tests mandatory in organizations
- EMRA Action:
  - Security Analysis and Testing Procedures and Principles for Industrial Control Systems Used in the Energy Sector (2019)
  - Information security audit and review processes in energy sector

EMRA Actions

- 2016-2019 Action Plan
  - Action No. 2.1: Making a detailed and real situation analysis
    - Monitoring the losses and causes of cyber incidents in public and private sector critical infrastructure operators
    - Determining the damage, including the financial dimension, in the events that occur
- EMRA Action:

🤐 🤐 🤐

EMRA Actions

- 2016-2019 Action Plan
  - Action No. 3.4: Organizing cyber security exercises
    - Organizing cybersecurity exercises on a sectoral scale under the leadership of sector regulatory authorities
- EMRA Action:
  - First Ex4S event (May, 2022)
  - Second Ex4S event (October, 2024)

EMRA Actions

- 2020-2023 Action Plan
  - Action No. 1.3: Preparation of sectoral regulations regarding the minimum cyber security criteria to be followed by legal entities operating in critical infrastructure sectors
  - Action No. 3.2: Preparation of sector-based «IT Products Manufacturer Dependency Analysis Reports»
  - Action No. 10.2: Organization of sectoral cybersecurity exercises
- EMRA Action:
  - Regulation on Information Security in Industrial Control Systems Used in the Energy Sector (2017)
  - Security Analysis and Testing Procedures and Principles for Industrial Control Systems Used in the Energy Sector (2019)
  - First Ex4S event (May, 2022)

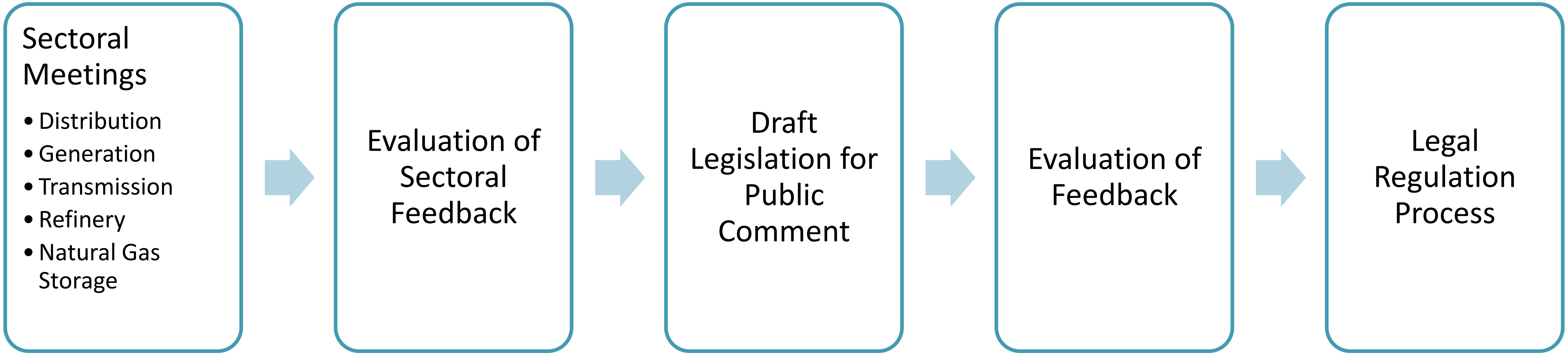
EMRA Actions

- 2020-2023 Action Plan
  - Action No. 7: Measuring and Monitoring Cybersecurity Maturity Levels of CERTs
    - Developing maturity level measurement guide for CERTs
    - Determining maturity levels of CERTs
    - Monitoring the development of maturity levels of CERTs
- EMRA Action:
  - Regulation on Cyber Security Maturity Model in the Energy Sector (2023)

Regulation on Cyber Security Maturity Model in the Energy Sector

Sector	Sub-sector
Distribution	Electricity Distribution Natural Gas Distribution
Transmission	Electricity Transmission Natural Gas Transmission Oil Transmission (by pipeline)
Electricity Generation	Gas-Fired PP Coal-Fired PP HPP WPP GPP SPP NPP
Refinery	Oil Refinery
Natural Gas Storage	Natural Gas Storage (LNG, underground)

Regulation on Cyber Security Maturity Model in the Energy Sector



Sectoral Meetings

- Distribution
- Generation
- Transmission
- Refinery
- Natural Gas Storage

Evaluation of Sectoral Feedback

Draft Legislation for Public Comment

Evaluation of Feedback

Legal Regulation Process

Regulation on Cyber Security Maturity Model in the Energy Sector

- Review of global regulations
- Review of global best practices
- Review of national regulations and guidelines
- Preperation of sectoral checklists and guidelines

Maturity Model, Maturity Levels

Level	Definition	Time Schedule
Level 1	Basic controls	Sector Specific
Level 2	Mid-level controls	Sector Specific
Level 3	Advanced controls	Sector Specific
Extra Control	Controls that are considered to be highly difficult and useful to implement	

Minimum Maturity Level

Electricity Distribution	: Level 2
Natural Gas Distribution	: Level 1
Electricity Transmission	: Level 3
Natural Gas Transmission	: Level 3
Electricity Generation	: Level 1
Oil Transmission	: Level 3
Refinery	: Level 3
Natural Gas Storage	: Level 1

Degree of Criticality

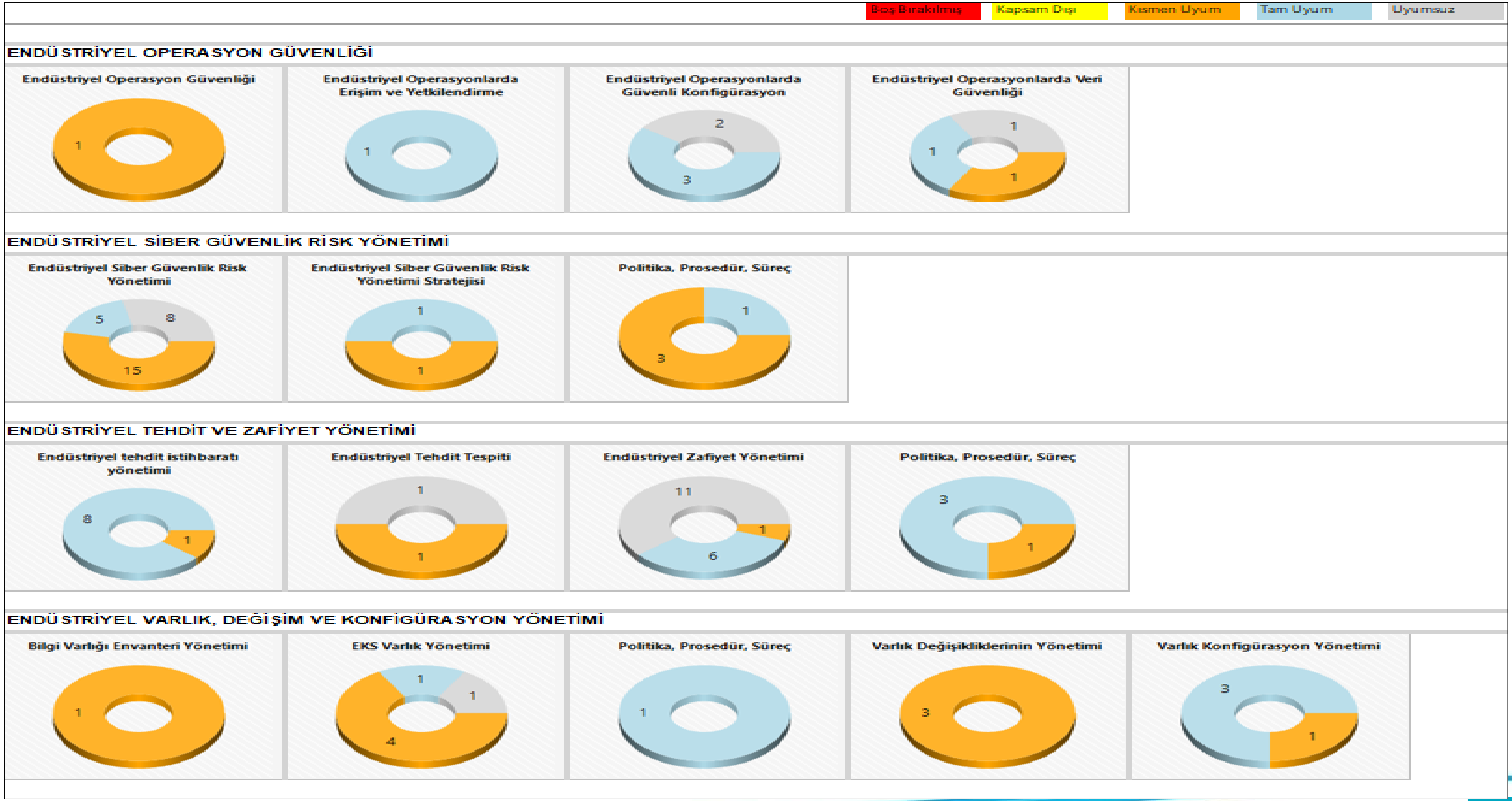
Degree of Criticality	Definition	Min. Level
Level A	Obliged entities with the highest criticality degree in the relevant sector	Level 3
Level B	Obliged entities with the mid-level criticality degree in the relevant sector	Level 2
Level C	Obliged entities whose criticality level is at the expected level in the relevant sector	Level 1

Main Control Group Headings

- Industrial Network Security (INS)
- Industrial Client and Server Security (CSS)
- Industrial Threat and Vulnerability Management (TVM)
- Industrial Cybersecurity Risk Management (CRM)
- Industrial Asset and Configuration Management (ACM)
- Industrial Identity and Access Management (IAM)
- Industrial Event Management and Continuity (IMC)
- Smart Device Security (Smart Meters, IoT) (SDC)
- Industrial Operations Security (IOS)
- Human Resources Security (HRS)
- Physical Security (PS)
- Supplier Management (SM)
- PLC Security (PLC)

	Electricity Distribution	Natural Gas Distribution	Electricity Generation	Refinery	Electricity Transmission	Natural Gas & Oil Transmission	Natural Gas Storage
INS	61	61	85	74	50	69	69
CSS	42	42	71	67	48	62	67
TVM	33	33	32	32	33	33	32
CRM	34	34	33	33	38	34	33
ACM	15	15	15	15	15	15	15
IAM	19	19	19	20	19	20	20
IMC	84	84	81	81	96	90	81
SDS	37	38	45	45	37	48	45
IOS	10	18	28	30	17	32	34
HRS	16	16	16	16	18	16	16
PS	97	97	90	91	63	111	91
SM	28	28	30	28	29	28	28
PLC		20	20	20		20	20
Total	476	505	565	552	463	578	551

Regulation on Cyber Security Maturity Model in the Energy Sector - Outputs



🟥 Boş Bırakılmış | 🟨 Kapsam Dışı | 🟧 Kısmen Uyum | 🟦 Tam Uyum | ⬜ Uyumsuz

ENDÜSTRİYEL OPERASYON GÜVENLİĞİ

Endüstriyel Operasyon Güvenliği

Endüstriyel Operasyonlarda Erişim ve Yetkilendirme

Endüstriyel Operasyonlarda Güvenli Konfigürasyon

Endüstriyel Operasyonlarda Veri Güvenliği

ENDÜSTRİYEL SİBER GÜVENLİK RİSK YÖNETİMİ

Endüstriyel Siber Güvenlik Risk Yönetimi

Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi

Politika, Prosedür, Süreç

ENDÜSTRİYEL TEHDİT VE ZAFİYET YÖNETİMİ

Endüstriyel tehdit istihbaratı yönetimi

Endüstriyel Tehdit Tespiti

Endüstriyel Zafiyet Yönetimi

Politika, Prosedür, Süreç

ENDÜSTRİYEL VARLIK, DEĞİŞİM VE KONFİGÜRASYON YÖNETİMİ

Bilgi Varlığı Envanteri Yönetimi

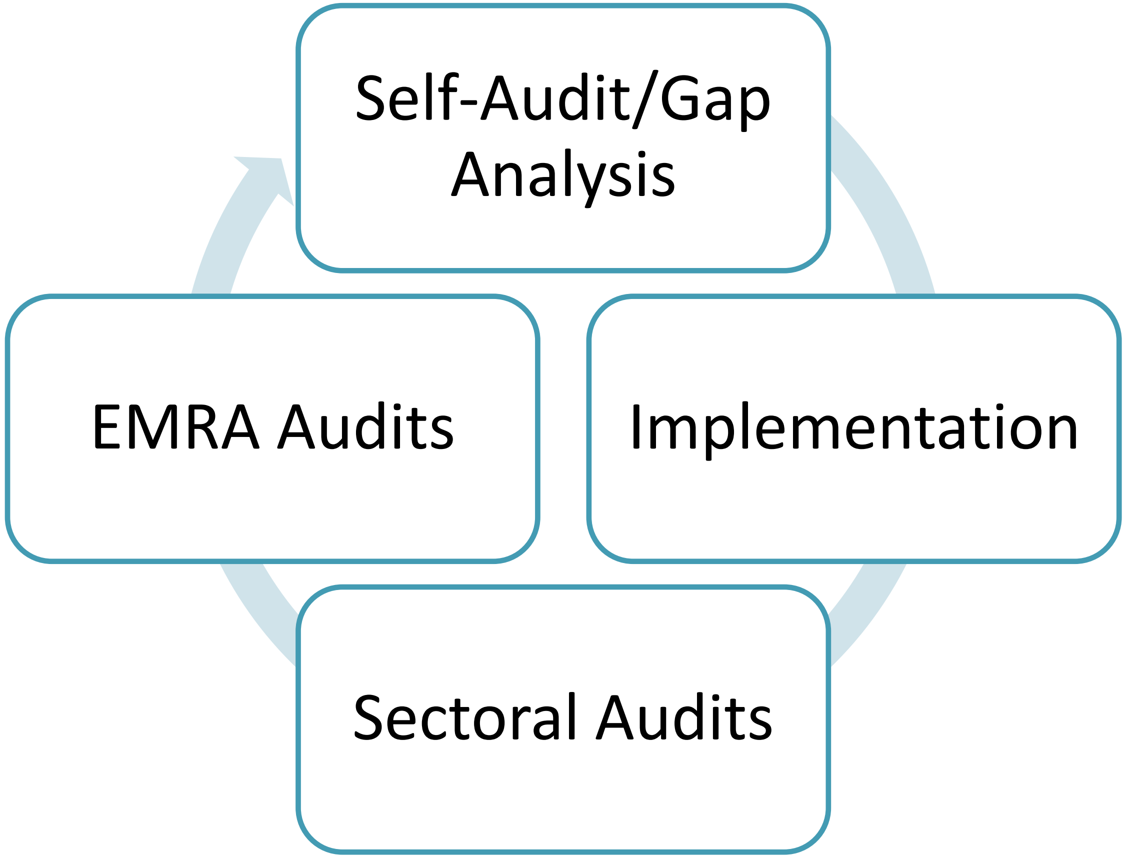
EKS Varlık Yönetimi

Politika, Prosedür, Süreç

Varlık Değişikliklerinin Yönetimi

Varlık Konfigürasyon Yönetimi

Audit and Compliance



Self-Audit/Gap Analysis

Implementation

Sectoral Audits

EMRA Audits

Future Projects

- Expansion of National Industrial Control System Technologies
- Integration of National Technologies in Industrial Control Systems Cybersecurity

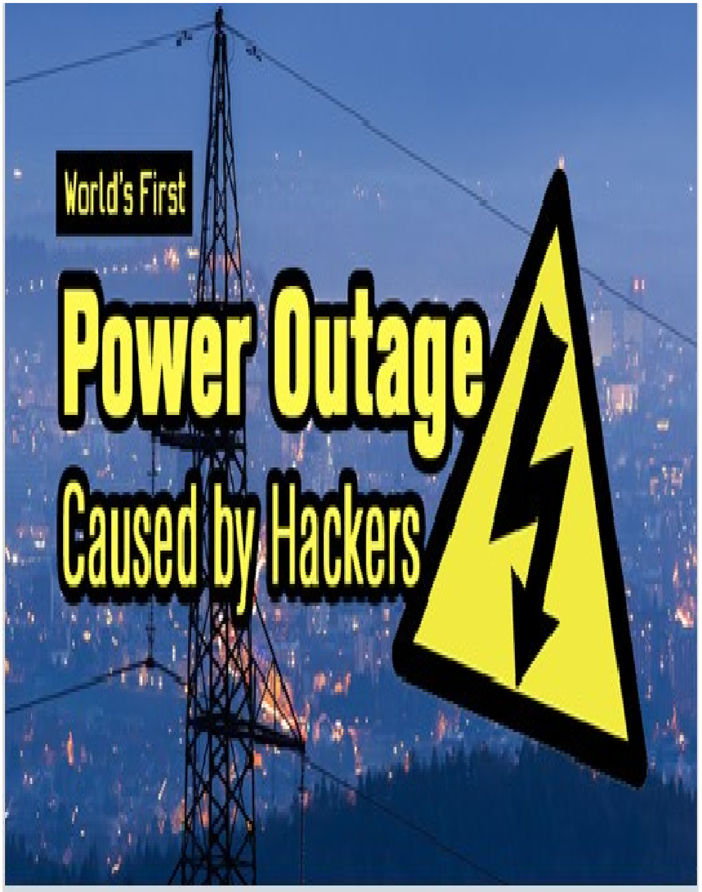
Stuxnet

- **Date:** June 2010 (date detected)
- **Impact:** Iran Nuclear Program
- **Impact source:** USB Memory
- State-sponsored(?) wormware
- Bushehr and Natanz nuclear facilities

Black Energy

- **Date:** December 2015
- **Impact:** Ukraine Electricity Distribution System
- **Impact Source:** Phishing E-mail
- 255,000 people in 3 different distribution areas were left without electricity for 6 hours.

Source: https://ozdenercin.com/2018/12/14/hedef-odakli-zararli-yazilim-blackenergy-tarihcesi-ve-gelisimi/



Colonial Pipeline

- **Date:** May 2021
- **Impact:** US East Coast fuel supply
- **Impact Source:** Theft of authorized account credentials
- The largest US pipeline company, Colonial Pipeline, has had its systems attacked by DarkSide ransomware.

It was reported that the company paid $4.4 million to the ransomware operators.

Source: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Attack on Iranian Gas Stations

- **Date:** December 2023
- **Impact:** Tehran gas stations
- **Impact Source:** Israel(?)
- 60% of Tehran gas stations were affected by the attack

Source: https://www.aa.com.tr/tr/dunya/irandaki-akaryakit-istasyonlarinin-internet-sistemine-siber-saldiri-iddiasi/3085514

Thanks for your attention

ndedeoglu@epdk.gov.tr