MERKEZİ KAYIT KURULUŞU (MKK)

CENTRAL SECURITIES DEPOSITORY &
TRADE REPOSITORY OF TÜRKİYE

RISK MANAGEMENT, INFORMATION SECURITY,
AND NEW CHALLENGES

4 June 2026

BORSA İSTANBUL GRUBU 1873

MERKEZİ KAYIT İSTANBUL
Central Securities Depository
& Trade Repository of Türkiye

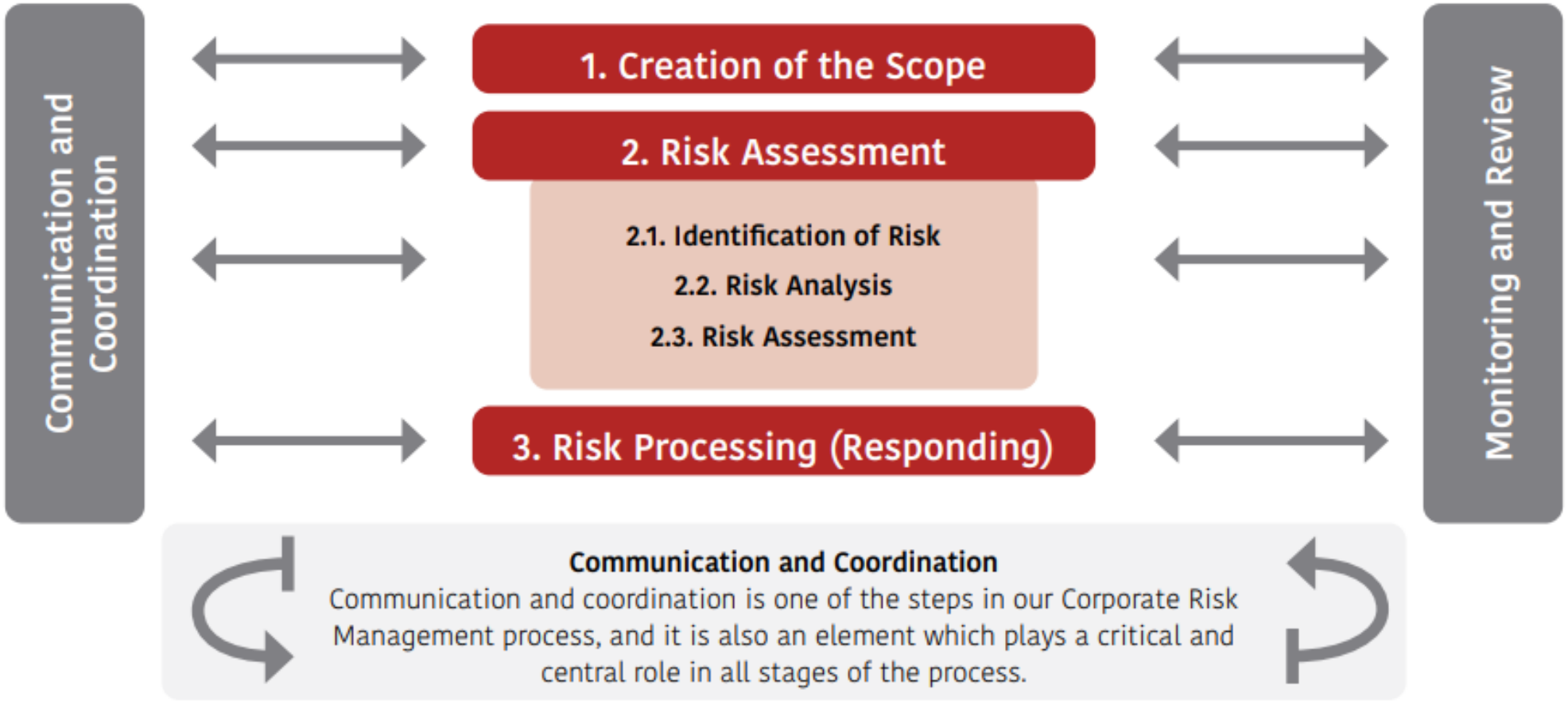
AGENDA

- Standards and Principles
- Enterprise Risk Management
- Business Continuity Structure
- Information Security Strategy and Objectives
- Information Security, Privacy Information, and Business Continuity Management Systems
- Management Systems Organizational Structure
- Cybersecurity Resilience Frameworks
- Cybersecurity: Threat Vectors
- Emerging Challenges and Adaptation Strategies

STANDARDS AND PRINCIPLES

- ISO 31000 ERM
- IIA 3 Lines Model
- CPMI-IOSCO Principles for Financial Market Infrastructures
- COSO ERM Framework and Internal Control Framework
- ISO 27001 ISMS, ISO 27701 PIMS
- ISO 22301 BCMS
- ISO 20000-1 ITSMS
- ISO 9001 QMS
- COBIT
- NIST CSF
- KVKK & GDPR

ENTERPRISE RISK MANAGEMENT



Communication and Coordination

Communication and coordination is one of the steps in our Corporate Risk Management process, and it is also an element which plays a critical and central role in all stages of the process.

► RISK CATEGORIES

In MKK, risk categories are classified in accordance with the Principles for Financial Market Infrastructures (CPMI-IOSCO).

- Compliance Risk
- Credit and Liquidity Risk
- Investment and Custody Risk
- General Business Risk
- Operational Risk

RISK ANALYSIS AND REPORTING

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

MKK ENTERPRISE RISK MANAGEMENT

Risks and opportunities are addressed and managed within MKK Enterprise Risk Management Structure.

Risks are identified, analyzed and evaluated in terms of impact and the probability:

- *Financial, reputation, compliance and operational impact criteria for business risks*
- *Confidentiality, availability, and integrity impact criteria for IT risks*

MKK Risk Appetite is determined and approved by BoDs.

Risk mitigating action plans are determined for residual risks that are above MKK's risk appetite.

Quarterly risk reports are submitted to the EDRC and Top Management.
Annual risk assessment reports are submitted to the BoD, Early Detection of Risks Committee (EDRC) and Top Management.

** The EDRC consists of two BoDs.*

▶ RISK ASSESSMENT

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

Risk Assessment Matrix		Severity				
		Very Low	Low	Medium	High	Very High
Probability	Very High	Moderate	High	High	Very High	Very High
	High	Moderate	Moderate	High	High	Very High
	Medium	Low	Moderate	Moderate	High	Very High
	Low	Low	Low	Moderate	High	Very High
	Very Low	Very Low	Very Low	Low	High	High

► KEY RISK INDICATORS

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

Key Risk Indicators

- Acquisition of Information
- Development of Effective KRIs
- Aligning with Risks and Strategic Goals
- Systematic Monitoring and Reporting
- Raising Awareness
- Stakeholder Participation, Communication and Coordination
- Regular Review

- ✓ **Meaningful**
- ✓ **Measurable**
- ✓ **Auditable**
- ✓ **Comparable**
- ✓ **Early Warning Signal**

- Risk Mitigating Action
- Close Monitoring
- Acceptable Risk

▶ RISK RESPONDING STRATEGIES

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

Risk Assessment

Risk Assessment	Determination of Risk Response Strategies	Risk Avoidance	Risk Acceptance	Risk Mitigation	Risk Transfer
		Hedging by avoiding risk related activity	Taking the risk and not taking action	Taking action to mitigate risks	Transfer of risk to third parties through the utilization of insurance mechanisms and the practice of outsourcing

Evaluation of Opportunities

Evaluation of Opportunities	Identifying Strategies for Responding to Opportunities	Exploiting	Maintaining	Enhancing	Sharing
		Leveraging the opportunity	Deliberately refraining from pursuing the opportunity	Implementing strategies to ensure the opportunity is fully leveraged	Sharing the benefits of the opportunity through the distribution of costs.

► ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

Benefits:

- ❑ Minimizes risks.
- ❑ Ensures the confidentiality of information.
- ❑ Ensures compliance with criteria required by legal parties and regulations.
- ❑ Supports business continuity.
- ❑ Protects access to information.
- ❑ Provides a competitive advantage.

INFORMATION SECURITY STRATEGY

MKK Information Security Strategy

MKK ensures the confidentiality, integrity, and availability of information related to the services provided to its members, investors, customers, and stakeholders through the support and collaboration of senior management, employees, and all stakeholders.

In this regard, MKK aims to continuously improve its information security processes by maintaining a high level of Information Security awareness and encouraging the active contribution and compliance of all employees and stakeholders.

INFORMATION SECURITY OBJECTIVES

Store and manage member, investor, customer, stakeholder and related party information in secure environments

Fulfill obligations per national and international laws

Protect the reputation of the institution by ensuring the confidentiality, integrity and availability of the information produced, used, transmitted and stored

Keep information security awareness at a high level

Protect the institution, all phyiscal and electronic information assets from internal and external threats

PRACTICES & EXERCISES

- Identify, measure, and monitor potential threats
- Execute penetration tests, vulnerability scans
- Conduct table-top exercises with the participation of Top Management
- Conduct regular phishing and social engineering exercises

► ISO 27701 PRIVACY INFORMATION MANAGEMENT SYSTEM

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

Benefits:

- ❑ Builds trust in the management of personal information.
- ❑ Enables more effective management of business agreements.
- ❑ Supports compliance with privacy regulations.
- ❑ Ensures transparency among stakeholders.
- ❑ Defines roles and responsibilities more clearly.

INFORMATION SECURITY, PRIVACY INFORMATION, AND BUSINESS CONTINUITY MANAGEMENT SYSTEMS

The scope is established within the context of the organization.

MS SCOPE – SERVICES

MKK's all services provided in MKK's facility, Borsa İstanbul Data Center (PDC), Disaster Recovery Center (DRC), Disaster Recovery Operation Center (DROC) are within the scope of the Management System (MS).

- *Central Securities Depository System (MKS)*
- *Electronic Warehouse Receipt Center (e-ÜRÜN)*
- *Public Disclosure Platform (KAP)*
- *Electronic Trade Repository (e-VEDO)*
- *Electronic General Meeting (e-GENEL KURUL)*
- *Companies Information Portal (e-ŞİRKET)*
- *Electronic Board of Directors (e-YKS)*
- *Investor Information Center (e-YATIRIMCI)*
- *Investor Notification Service (YBS)*
- *Investor Risk Monitoring System (YRTS)*
- *Capital Markets Data Bank (e-VERİ)*
- *Data Analysis Platform (VAP)*
- *Crowdfunding Platform (KFS)*
- *Bearer Shares Registry System (HPKS)*
- *MKK Solution Center (MİM)*
- *Real Estate Based And Developing Financial Instruments Information System (GEFAS)*
- *Financial Registration System (FTS)*
- *MİM360 MKK Communication Center (MİM360)*
- *Crypto Asset Central Registry System (KVMKS)*
- *Central Document Management System (MDYS)*
- *PUSULA*
- *MKK API Portal*

All business and information technology processes related to infrastructure and operation support provided to MKK Gayrimenkul Bilgi Merkezi A.Ş. (GABİM), legal regulations and support infrastructure are within the scope of the Management System (MS).

BUSINESS CONTINUITY STRUCTURE

Threat and Impact Analysis

Incident Management Procedures

Crisis Management Committee

Alerting and Monitoring Requirements

Business Continuity Strategies

Disruption Scenarios

Incident Evaluation and Escalation

Crisis and Emergency Management

Communication

Recovery / Service Restoration

Return to Normal Operations

Internal Emergency Alert Systems

Business Continuity Organization

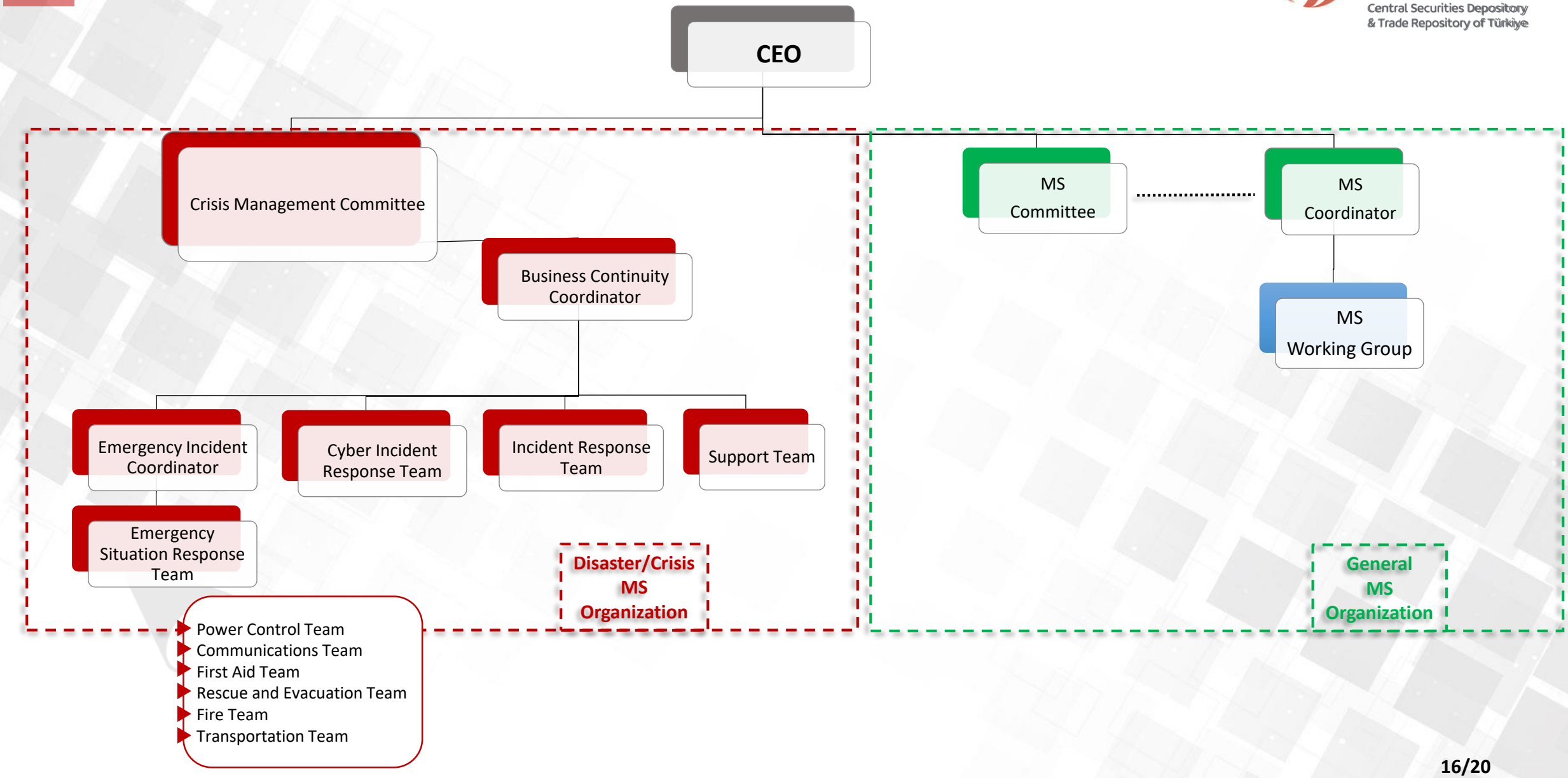
- Crisis Management
- Incident Management
- Emergency Response Teams

Internal and External Communication Plan

Business Continuity Recovery Plans

- IT Disaster Recovery Scenarios
- Business Unit Recovery Scenarios
- Other Scenarios

ORGANIZATIONAL STRUCTURE



► CYBERSECURITY RESILIENCE FRAMEWORK

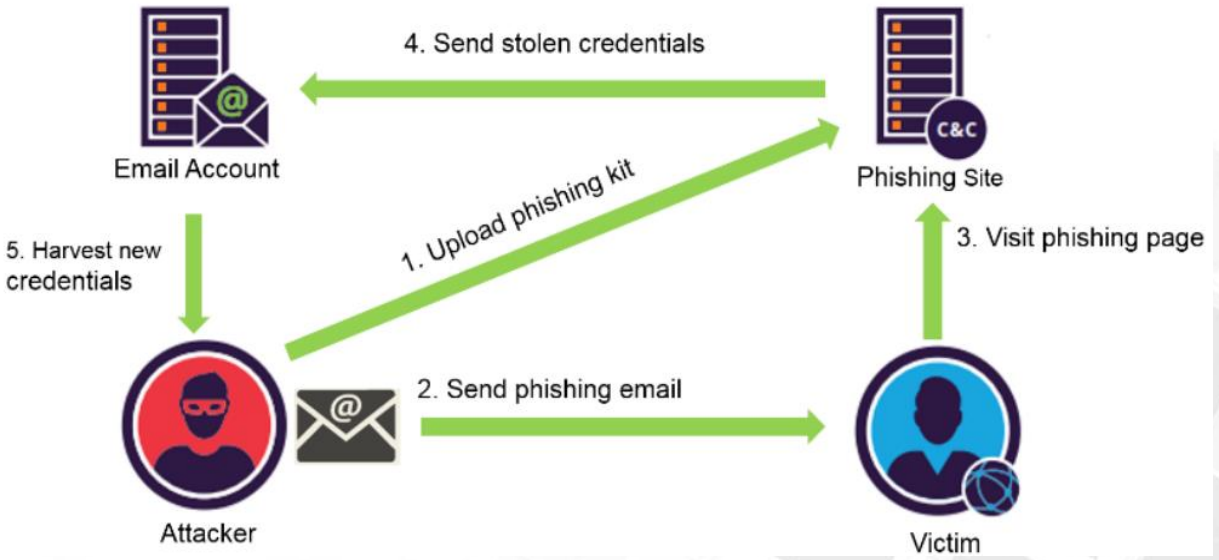
MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

- **Technical Controls**
  - Log Management through SIEM Technologies
  - Security Monitoring and Response – SOAR Technologies
  - Advanced Persistent Threat (APT) Protection Mechanisms
  - Endpoint Detection and Response (EDR) Solutions
  - Network Detection and Response (NDR) Solutions
  - Intrusion Detection and Intrusion Prevention Systems (IDS/IPS)
  - Vulnerability Scans/Penetration Tests
  - Virtual Private Network (VPN)
  - Internet Protocol (IP) Restriction
  - Firewall, Web Application Firewalls (WAF)
  - Secure Sockets Layer and Transport Layer Security (SSL/TLS)
  - Mobile Device Management and Mobile Application Management Solutions (MDM/MAM)
  - Data Leakage Prevention (DLP)
  - Identity and Access Management (IAM)
- **Administrative Controls**
  - Enterprise Risk Management
  - Management Systems Policies and Procedures:
    - Password Policy
    - Cyber Awareness and Exercises
    - Data Classification
    - Supplier Management
    - Clean Desk Policy
    - Cyber Incident Response and Communication Plan
    - Business Continuity Plan
    - Back up and Restore Procedures
  - Control Objectives for Information and Related Technology (COBIT)
  - The COSO Internal Control Framework
  - Three Lines of Defense Model

►CYBERSECURITY: THREAT VECTORS

Cybersecurity threat vectors are rapidly expanding…

- ❑ Ransomware
- ❑ Malware
- ❑ DoS and DDoS
- ❑ Phishing
- ❑ Social Engineering
- ❑ Man in the Middle
- ❑ Zero-Day
- ❑ SQL Injections



EMERGING CHALLENGES AND ADAPTATION STRATEGIES

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye

Emerging Challenges

- *•AI-Powered Cyber Attacks*
- *•Technological Advancements*
- *Third-Party Risk and Supply Chain*
- *Regulatory and Compliance Issues*
- *Geopolitical Concerns*
- *Global Economic Concerns*
- *Natural Disasters*

Adaptation Strategies

- New Technology Utilization
- Collaboration with Regulators
- Focus on Safety and ESG (Environmental, Social, Governance) Human-based
- Capability and Competency
- Artificial Intelligence

Thank you.

erva.kan@mkk.com.tr

taner.uluturk@mkk.com.tr

MERKEZİ KAYIT İSTANBUL
Central Securities Depository & Trade Repository of Türkiye