TURKISH COURT OF ACCOUNTS

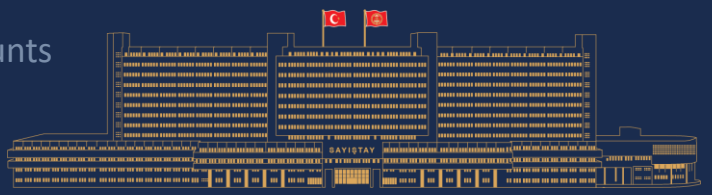
IT Audit of Hospital Information Management Systems

Pınar AVUNDUKLUOĞLU, Principal Auditor

IT Audit Group · Turkish Court of Accounts

Mahmut GÜLER, Principal Auditor

IT Audit Group · Turkish Court of Accounts
mahmutguler@sayistay.gov.tr



Outline

- Introduction
- Information Security and Healthcare Services
- Personnel Structure
- Diversity of Services
- Institutional Structure of Hospitals & Budgetary Choices
- International Standards
- What We Have Learned

Introduction

Key Characteristics of Healthcare IT Audit

- Human life at the centre
- Good practices vs. healthcare realities
- Security–service continuity balance
- uninterrupted operations
- Long working hours of healthcare staff

- Complex and integrated systems
- Limited resources, high expectations
- Wide range of services
- Competing priorities
- Sensitive health data

Security–Service Balance in Hospitals

- Emergency access needs
- Critical health data
- No one-size-fits-all control
- Unit-based risk assessment
- Participatory control design
- Business process alignment
- Periodic review and adjustment

Human Factor in Hospital IT

- Long hours, high stress
- Convenience vs. compliance
- Security as extra workload
- Human behaviour matters
- Senior management support
- No tolerance for system downtime

Complex and Integrated Hospital Systems

- Wide range of services
- Different user groups
- Frequent staff movement
- Continuous updates and support
- High coordination need

- Need for proper needs analysis
- Competing budget priorities
- IT resilience and patient safety
- Health data protection

International Standards

- Information security and privacy, ISO/IEC 27001, ISO 27799 and ISO/IEC 27701
- Access control and authorisation, ISO 22600
- Logging and traceability, ISO 27789
- System integrations, HL7/FHIR, IHE profiles and DICOM
- Clinical data standardisation, ICD-11, SNOMED CT and LOINC
- Electronic health record architecture, ISO 13606 and ISO 12967
- Software development and life cycle processes, IEC 82304-1 and IEC 62304
- Medical device networks and connected systems, IEC 80001-1
- Digital hospital maturity, HIMSS EMRAM and INFRAM
- JCI, or Joint Commission International.

Application controls in hospitals require more than technical review; they require clinical and regulatory understanding.

01

Security controls in hospitals must be balanced, participatory and adapted to the urgency of each unit.

02

Awareness-raising activities should be carried out for staff, primarily in the area of information security, but also covering other IT services.

03

The awareness of senior management regarding IT services should also be increased. Senior management should actively support the implementation of IT policies.

04

The audit team should carefully analyse the working culture and business processes of the hospital.

05

Hospitals should prepare design documents, user manuals and training activities within the scope of system development, system acquisition and IT operations.

06

Hospitals should establish well-designed mechanisms for identifying IT requirements.

What We Learned from Auditing Major Public Hospitals in Türkiye

🔍 What did we observe?

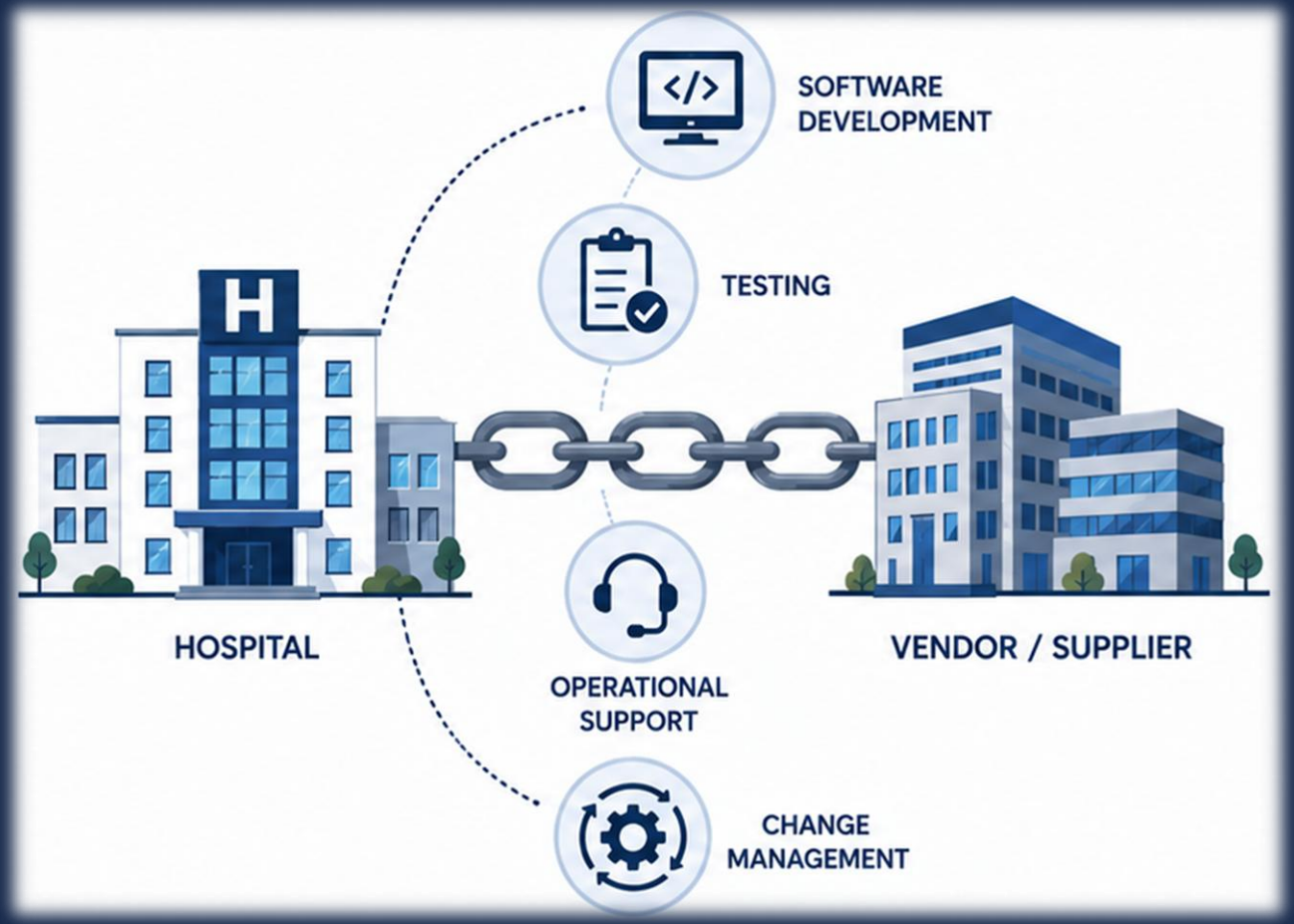
- Governance weaknesses
- Vendor dependency
- Information security gaps
- Test Environment Weaknesses
- Resilience challenges

Governance Weaknesses

Vendor Dependency

- Vendor-operated testing
- Extensive remote access
- Limited institutional ownership
- No exit strategy

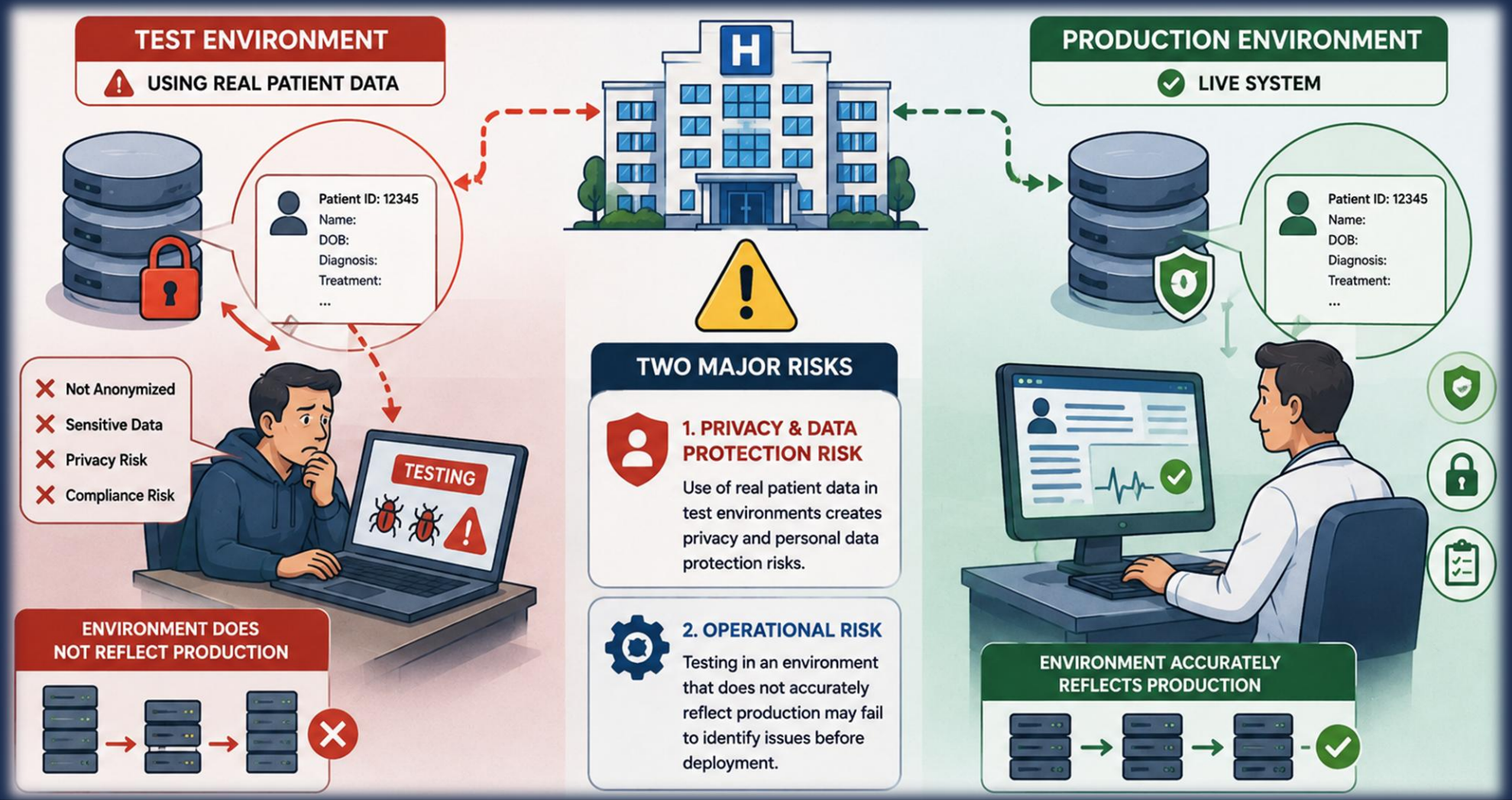
Strong internal capability and knowledge retention are essential to ensure control, continuity and independence over critical systems.



Information Security Findings

- No comprehensive Information Security Management System
- Weak access management
- Excessive remote access privileges
- Delayed patch management
- Limited vulnerability monitoring

Test Environments and Personal Data



Business Continuity and Disaster Recovery

- Incomplete disaster recovery planning
- Undefined RTO and RPO targets
- Outdated crisis scenarios
- Disaster recovery centres located in the same campus
- No disaster recovery centre existed

Key Audit Message

Without effective governance and mature controls:

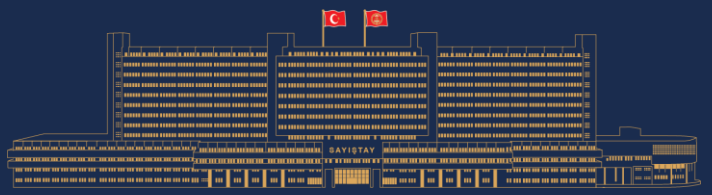
- Cyber risks increase
- Vendor dependency grows
- Operational resilience weakens
- Auditability decreases

Digital transformation alone does not create resilience.

TURKISH COURT OF ACCOUNTS

IT Audit of Hospital Information Management Systems

Thank you

Pınar AVUNDUKLUOĞLU

Mahmut GÜLER
mahmutguler@sayistay.gov.tr