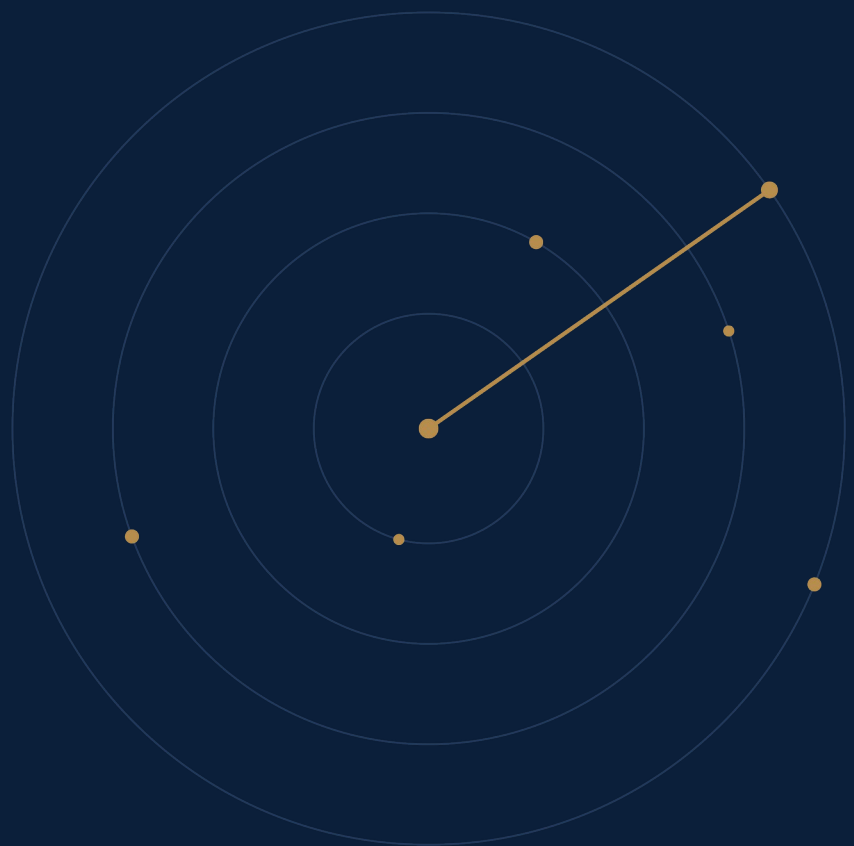

CYBERTECH **AUDIT.**

Beyond Compliance. Towards Resilience.

Integrated audit and risk management services for critical
infrastructure and complex organizations



01

Message

We understand complexity. We support better decisions.

A strategic shift from treating standards as mere checklists to treating them as foundations for proactive adaptability and the creation of sustainable, long-term commercial value.

Clarity · Control · Performance · Resilience · Trust

02

About Us

Who We Are

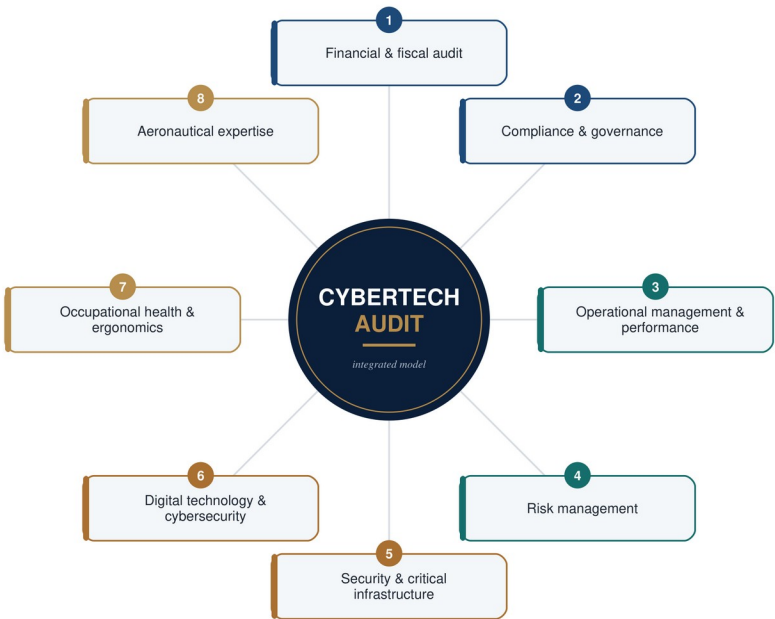
CyberTech Audit is a multidisciplinary team for audit, organizational assessment and risk management, dedicated to organizations operating in complex and regulated environments.

The integrated audit model offers expertise across eight complementary domains:

Financial and fiscal audit	Legal compliance and corporate governance
Operational and performance management	Risk management
Security and critical infrastructure	Digital technology and cybersecurity
Occupational health and ergonomics	Aeronautical expertise

INTEGRATED MODEL

Eight domains of expertise



03

Why CyberTech Audit

Beyond Compliance

Traditional audit implementations stop at compliance - they check whether laws, rules and regulations are observed at a given point in time.

CyberTech Audit looks further: we assess whether the organization performs well and is capable enough to continue its activity when disruptions occur.

We assess:

- resilience
- performance
- adaptive capacity
- operational continuity
- organizational vulnerabilities

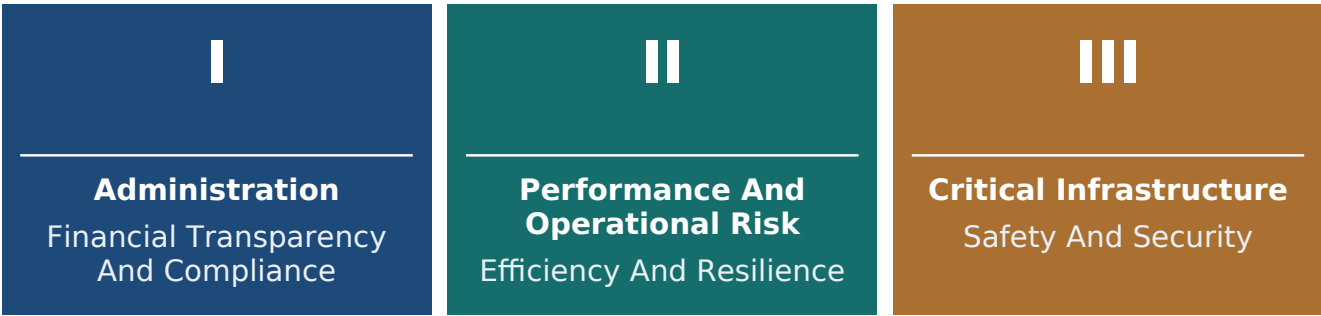
BEYOND COMPLIANCE**From compliance to resilience**

04

The CyberTech Audit Model

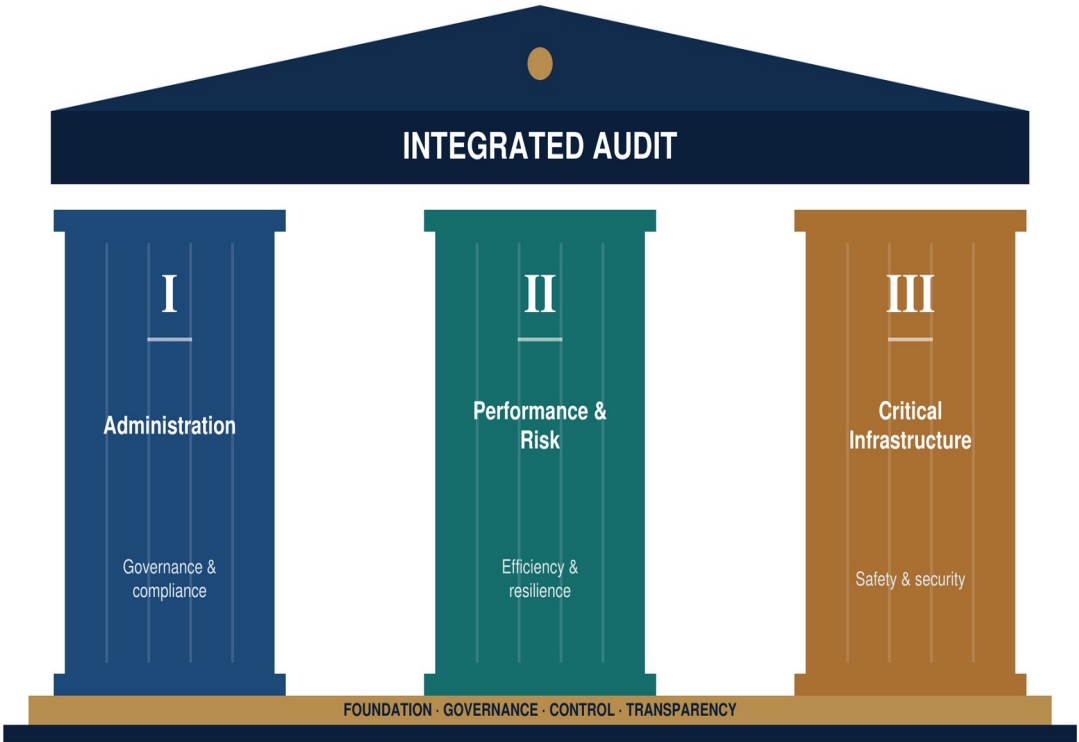
Three pillars, one perspective

The integrated model is structured on three core pillars present in every organization - analyzing from governance and control, to operational performance and further to the safety of critical infrastructure.



THE CYBERTECH MODEL

Three pillars, one integrated audit



05

Pillar I — Administration

Governance, finance, compliance

Covers the financial, fiscal and legal dimension of the organization - the foundation of governance and internal control.

Services:

Financial Audit	Fiscal Audit
Internal Control Audit	Legal and Compliance Audit
Investment Audit	Public Procurement Audit
European Projects Audit	

Main benefit: strengthening governance and organizational control.

06

Pillar II — Performance and operational risk

How the organization operates and endures

Analyzes how the organization carries out its activity and manages operational risks - from processes and logistics, to business continuity and resilience.

Services:

Organizational processes audit	Operational efficiency audit
Logistics audit	Supply chain audit
Business continuity audit	Risk management audit
Organizational resilience audit	

Main benefit: optimizing performance and reducing operational vulnerabilities.

07

Pillar III — Critical infrastructure

Operational safety and security

Specialized services for organizations operating critical infrastructure or systems with major impact on public safety and operational security.

In this pillar, the audit no longer looks only at compliance, but at the ability of systems to operate safely and to withstand incidents - from cyber and physical security, to the health of the people who operate them and the technical integrity of the infrastructure.

Services:

IT and cybersecurity audit	Critical infrastructure security audit
Data protection audit (GDPR)	Access control / physical security audit
Aeronautical technical audit	Aircraft maintenance audit Part-145 / EMAR-145
Operational safety audit	Occupational health audit
Ergonomics and human performance audit	

Main benefit: increasing operational safety and security.

08

Integrated Audit

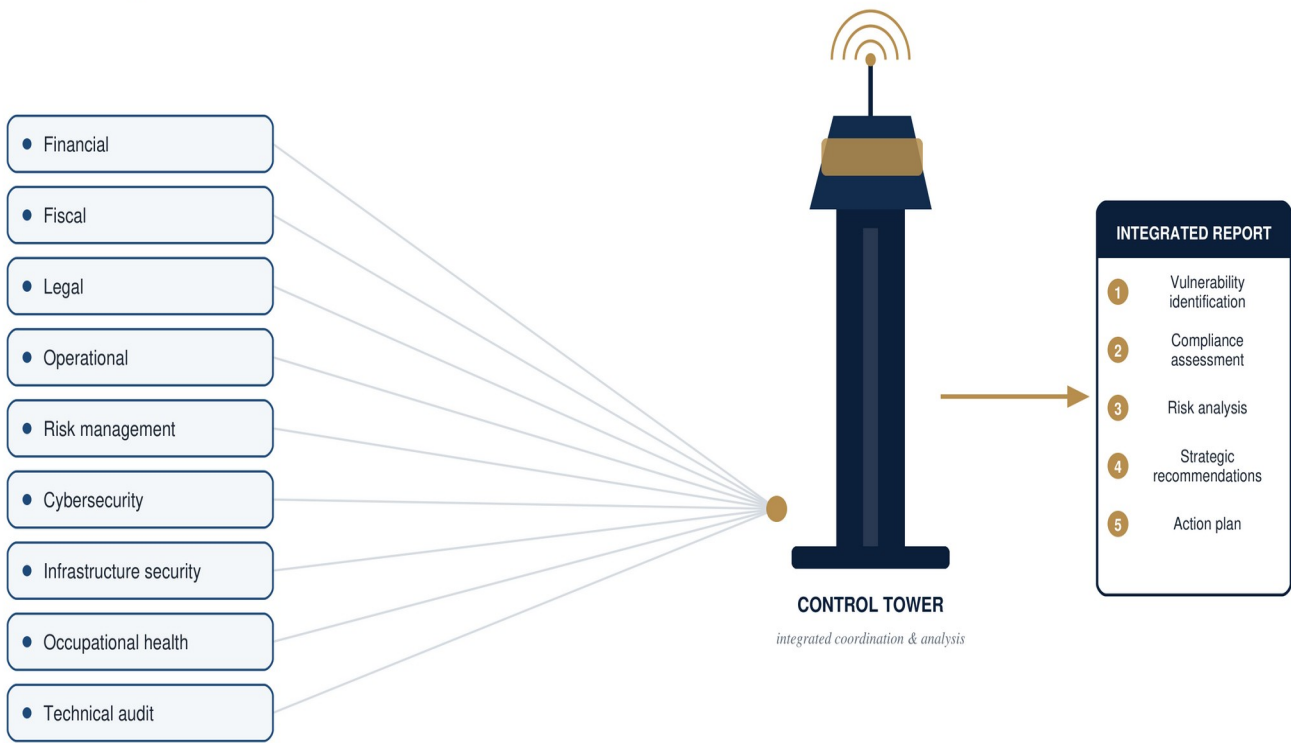
One mission. A complete perspective.

For complex organizations, integrated audit acts as a strategic coordination center - similar to an airport control tower - providing a complete view of risks, vulnerabilities and performance.

The audit can combine: financial · fiscal · legal · operational · risk management · infrastructure cybersecurity · occupational health · technical audit.

INTEGRATED AUDIT

A strategic coordination center



09

Implementations

Fields of application

Integrated audit applies to organizations for which safety, continuity and compliance are not optional, but operating conditions.

Airports - airport infrastructure, operational safety	Aeronautical organizations - maintenance, technical compliance
Transport and logistics - supply chain, continuity	Energy - energy infrastructure, operational security
Critical infrastructure - systems with impact on public safety	Public institutions - budget, public procurement, compliance

10

Risk Performance Resilience

Risk Management

The CyberTech Audit model treats risk not as an isolated event, but as a continuous cycle of identification, assessment and control - turning vulnerabilities into decisions.

The continuous risk cycle:

- risk identification
- impact assessment
- prioritization of vulnerabilities
- development of control measures
- continuous monitoring

RISK & RESILIENCE

A continuous management cycle



11

We do not stop at producing a report

Consulting and implementation

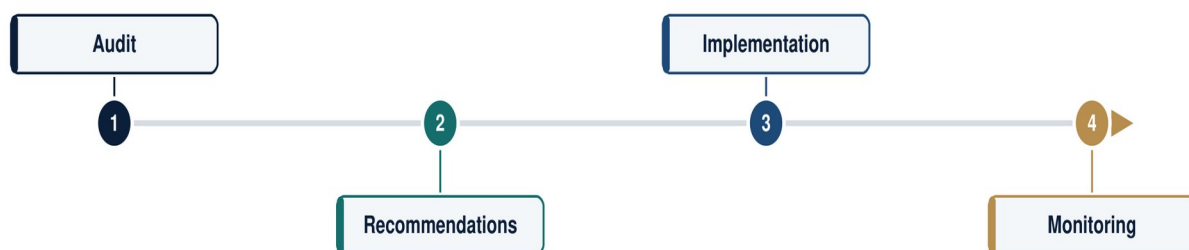
An audit has value only if its recommendations are actually applied. That is why we support organizations and continue the collaboration after the report is delivered, to ensure the correct and effective implementation of the measures.

We support implementation through:

- internal control systems
- operational restructuring
- organizational optimization
- risk management systems
- staff training programs
- development of operational procedures and policies

CONSULTING & IMPLEMENTATION

We don't stop at the report



From audit to monitoring - a continuous journey, not an endpoint.

12

Team Many Competencies

Multidisciplinary expertise

The CyberTech Audit team brings together multifaceted experience, gathered from the private sector, the public sector, critical infrastructure, international organizations and academia. The strength of the model and the way of working does not rely on a single specialization, but on the synergic value of interconnection.

Areas of institutional expertise:

- aeronautical expertise
- financial and fiscal expertise
- critical infrastructure expertise
- security, risk and resilience expertise
- compliance and governance expertise
- occupational health and ergonomics expertise
- operational and project management expertise

13

The Added Value of CyberTech Audit

Why integrated audit matters

Modern audit is a strategic instrument for improving organizational performance and managing risks in a complex operational environment. By integrating financial, legal, operational and technical expertise

CyberTech Audit provides, in an integrated way, complete audit and consulting services for operating in critical infrastructure and highly regulated environments.

CyberTech Audit, a focused partner for the entire perspective on risks and operational performance.

Main benefits:

Improving internal processes	Strengthening organizational resilience
Increasing the level of operational security	Identifying organizational vulnerabilities
Reducing financial, legal and operational risks	

14

Application

Services x sectors

The CyberTech Audit model applies transversally, across all sectors involved, according to each target sector.

Audit domain	Airports	Transport & Logistics	Energy & Critical Infrastructure	Public and Private Organizations	Aeronautical Organizations
Financial audit	✓	✓	✓	✓	✓
Investment audit	✓	✓	✓	✓	✓
European projects audit	✓	✓	✓	✓	✓
Public procurement audit	✓	✓	✓	✓	✓
Fiscal audit	✓	✓	✓	✓	✓
Legal and compliance audit	✓	✓	✓	✓	✓
Operational processes audit	✓	✓	✓	✓	✓
Operational efficiency audit	✓	✓	✓	✓	✓
Procurement / logistics audit	✓	✓	✓	—	✓
Risk management audit	✓	✓	✓	✓	✓
Infrastructure security audit	✓	✓	✓	✓	✓
Business Continuity audit	✓	✓	✓	✓	✓
IT and cybersecurity audit	✓	✓	✓	✓	✓
Data protection audit (GDPR)	✓	✓	✓	✓	✓
Access control / physical security audit	✓	✓	✓	✓	✓
Aeronautical technical audit	✓	—	—	—	✓
Aircraft maintenance audit (Part-145 / EMAR-145)	✓	—	—	—	✓
Operational safety audit	✓	✓	✓	✓	✓
Occupational health audit	✓	✓	✓	✓	✓
Ergonomics and human performance audit	✓	✓	✓	✓	✓

✓ = applicable — = reduced applicability / sector-specific



Contact

Always open to discuss your organization

CYBERTECH **AUDIT.**

Beyond Compliance. Towards Resilience.

Integrated audit and risk management for critical infrastructure and complex organizations.

Website cybertechaudit.com

Email audit@cybertechaudit.com

Phone +0722250904

Address Braşov, str. Mureşsenilo nr.11, Romania



Scan · cybertechaudit.com

We transform organizational complexity into clarity, control and resilience.

With successful solutions for:

I

Administration

Financial transparency
and compliance

II

**Performance and
operational risk**

Efficiency and resilience

III

Critical infrastructure

Safety and security