Grant Thornton

Information Technology Risk and Governance Services

Information Technology Compliance and Audit Services

We provide independent audit services with our expert team to ensure that Information Technology (IT) systems are managed, audited, and reported in compliance with regulations, industry requirements, and international frameworks. Within the scope of the service, control environments compatible with both regulatory authority expectations and global standards are evaluated, reported, and delivered along with institution-specific improvement recommendations.

Legal Compliance Audits

Systemic and managerial controls are assessed for compliance with IT regulations issued by regulatory authorities such as the BDDK, SPK, TCMB, BTK and GİB. The institution's internal control environment, risk management systems, and data security practices are analyzed, and detailed compliance reports are prepared.

Compliance with International Standards

System and process audits are conducted in accordance with internationally recognized frameworks such as COBIT 2019, ISO/IEC 27001, SOX, ITIL, and DORA. Gaps between the institution's current practices and standards are identified, maturity levels are measured, and improvement plans are developed.

Sectoral Compliance and Audits

Special audit approaches are provided for institutions operating in areas such as FinTech, InsurTech, and RegTech. These audits evaluate sector-specific IT controls, compliance with business models, and data processing procedures.

Financial Regulation Compliance

The extent to which information systems comply with financial regulations such as IFRS, Basel II/III, and Solvency II is analyzed. The compliance of IT systems with criteria such as financial accuracy, traceability, and accountability is reported.

International Assurance Reports

We offer both report preparation and process readiness consulting in the preparation of independent assurance reports such as SOC 1, SOC 2, and ISAE 3402. These reports provide internationally recognized assurance regarding the adequacy of IT systems and the reliability of control environments for client institutions.

Risk and Governance

In their digital transformation journeys, organizations must treat IT management as a strategic area to enhance the efficiency of their technological infrastructure, become resilient to cyber threats, and ensure regulatory compliance. In this context, IT Risk and Governance Services cover specialized services to ensure that organizations' IT operations are managed transparently, securely, and in compliance with regulations. Based on national and international standards, our services adopt a risk-based approach and form the foundation for continuity and efficiency in IT structures.

Information Technology Risk and Governance Services

Information Security Consultancy

Information security is a critical area of management under the responsibility of the entire organization, not just the IT departments. This service group aims to protect corporate information assets against unauthorized access, loss, and corruption, while also ensuring compliance with regulatory expectations.

A multi-dimensional approach is adopted, including the implementation of information security management systems (ISMS) in accordance with international standards (especially ISO/IEC 27001), compliance with personal data protection regulations, governance practices, and awareness training. Our services are tailored to the organization's structure and digital risk profile.

ISO/IEC 27001 ISMS Consultancy

Custom information security policies are developed for the organization, risk assessment processes are defined, and preparation for ISO/IEC 27001 certification is carried out. An integrated system approach is adopted, addressing both technical infrastructure and administrative controls.

KVKK and GDPR Compliance Consultancy

A personal data inventory is prepared; consent texts and disclosure obligations are restructured. The organization's data protection measures are evaluated from both administrative and technical perspectives, and a roadmap for legal compliance is created.

ISO/IEC 20000 and ITSM

IT service management processes are aligned with the ISO/IEC 20000 standard. The effectiveness of core processes such as service level management, change management, and problem management are evaluated, and improvement plans are developed.

ISO/IEC 38500 IT Governance

Consultancy is provided based on the ISO 38500 framework, which defines the roles and responsibilities of boards and senior executives for corporate IT governance. The aim is to strengthen the alignment between IT investments and strategic goals.

Awareness and Training Services

Training sessions on social engineering, information security awareness, and data protection are designed and delivered to all employees. Training is conducted using interactive methods aligned with the corporate culture, aiming to reduce behavioral risks.

Corporate Information Security Approach

Information security is a responsibility shared across the organization. This service ensures the protection of corporate information assets and supports legal compliance. Key components include implementing systems compliant with ISO/IEC 27001, adhering to data protection regulations, and delivering awareness training.

All consulting services are delivered considering the organization's structure and risk level. Information security policies, personal data inventories, IT service process compliance, and governance principles are addressed. Additionally, awareness training is provided to employees.

Information Technology Risk and Governance Services

Cybersecurity Services

Our cybersecurity services are based on an approach that adapts to the dynamic nature of the threat environment and protects corporate assets through a multi-layered defense principle. We focus on building structures that help organizations understand their cyber risks, prepare for them, and respond effectively to incidents.

From strategic planning to operational testing, incident response scenarios to third-party risk assessments, our services ensure both regulatory compliance and operational resilience. Each service is customized according to the organization's specific security architecture and threat model.

Cybersecurity Strategy and Roadmap

The organization's current cybersecurity maturity is analyzed in detail. Based on identified weaknesses, strengths, and industry-specific threats, a tailored strategic roadmap is created. This roadmap includes technical, administrative, and cultural security steps in a holistic framework.

Vulnerability Scanning and Penetration Testing

Comprehensive security tests are performed on the organization's IT infrastructure, networks, applications, and cloud systems. Both automated vulnerability scans and manual penetration tests are conducted to identify vulnerabilities. Detailed reports and improvement plans are then provided.

Identity and Access Management (IAM)

IAM systems are designed and implemented ensuring that access to critical systems is limited to authorized individuals and granted only as needed. Security is enhanced through role-based access controls and multi-factor authentication processes.

Incident Response and Crisis Simulations

Incident response plans are developed to prepare internal teams for cyber incidents. Role-specific scenarios are designed, and crisis simulations (cyber wargames) are conducted. These exercises assess the institution's technical reflexes and management decision-making speed.

SIEM and Threat Intelligence

Advanced SIEM systems are implemented to improve internal threat monitoring capabilities. Log collection, anomaly detection, and automation-assisted incident response infrastructure are established to enable real-time defense mechanisms.

Third-Party and Supplier Risk Management

The security levels of external service providers working with the organization are evaluated. Compliance with contracts and SLAs is audited to ensure supply chain security. Special tracking and control recommendations are provided for high-risk third parties.

Cybersecurity Management and Implementation Areas

Cybersecurity services aim to protect organizations' digital assets with a multi-layered defense approach and create adaptable structures to respond to the evolving threat environment. Institution-specific strategies are developed through assessments of current maturity, vulnerability scans, penetration tests, and identity and access management practices.

Incident response plans, crisis scenarios, threat intelligence systems, and third-party risk assessments are designed to support operational and administrative resilience.

Business Continuity and Crisis Management Services

Business continuity management ensures the sustainability of corporate operations and tests resilience during crises. We develop strategic solutions to help organizations prepare for service disruptions, natural disasters, cyberattacks, and operational failures.

Our services go beyond documentation and are based on a comprehensive system that is integrated across the organization, tested, and continuously improved. We provide holistic business continuity solutions by integrating IT systems with organizational planning.

ISO 22301 Consultancy

Critical processes and resources are analyzed to conduct a Business Impact Analysis (BIA). Based on this analysis, business continuity strategies are developed, and a management system in compliance with ISO 22301 is implemented.

Exercises and Gap Analysis

Prepared business continuity plans are tested through tabletop and field-based exercises. These exercises measure the applicability of the plans, personnel awareness, and the organization's crisis reflexes, and gap analyses are conducted based on the results.

IT Continuity and Recovery Plans

Disaster recovery (DR) plans are prepared for data centers, network infrastructures, and application systems. Backup strategies, alternative operation methods, and emergency transition scenarios are developed to ensure continuity of IT infrastructure.

Preparation for IT Disaster Scenarios

To ensure uninterrupted continuity of corporate activities, critical processes are identified, and Business Impact Analysis (BIA) is conducted. Based on the results, business continuity strategies are developed, and an ISO 22301-compliant management system is established. Plan applicability is tested through tabletop and field exercises, and gap analyses are performed based on results.

As part of IT continuity, disaster recovery plans are prepared for systems such as data centers and network infrastructure. Backup scenarios, transition procedures, and emergency response plans are developed to enhance technological resilience.

Can Taylan

Senior Manager
T +90 212 373 00 00
E can.taylan@tr.gt.com

Enis Seven

Manager
T +90 212 373 00 00
E enis.seven@tr.gt.com

About us

Grant Thornton is one of the world's leading organizations providing independent audit, tax, and advisory services. Its member firms support dynamic organizations in unlocking their growth potential by delivering meaningful and forward-looking guidance. With over 76,000 professionals in more than 150 countries, we work to create value for our clients, our colleagues, and the communities in which we live and work.

Grant Thornton

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.