Are you ready for compliance with the updated security law?

The better the question.
The better the answer.
The better the world works.

EY
Building a better working world

Amendments to the Law of Georgia on Information Security

The Law of Georgia on Information Security, which sets basic standards for information security has been in force in the country since 2012.

This Law aims to promote the efficient and effective maintenance of information security, define rights and responsibilities for public and private sectors in the field of information security maintenance, and identify the mechanisms for exercising state control over the implementation of information security policy.

On January 1, 2022 significant legislative changes came into force:

- Subjects of the law were increased and categorized.
- Coordinating and supervisory agencies were changed by categories.
- Administrative sanctions for non-compliance with the requirements of the law were defined.

600%

Global cybercrime statistics increased amid ongoing covid pandemic.

Who does the law apply to?

The law applies to the subjects of the critical information system defined by the resolution of the Government of Georgia (Hereinafter referred to as a subject).

The subject of a critical information system is an authority (body)/institution whose continuous functioning of the information system is important for the defense and/or economic security of the country, for the maintenance of state authority and/or public life.

With the new amendment, the critical information system subject is divided into three categories:

Category	Institution		Supervisory Bodies
First Category	Public and Government entities		LEPL Operational-Technical Agency
Second Category	Telecommunication companies		LEPL Operational-Technical Agency
Third Category	Legal entities of private law	Commercial Banks	LEPL Digital Governance Agency National Bank of Georgia
		Insurance and Transportation companies, Energy companies and etc.	LEPL Digital Governance Agency

* The full list of subjects can be found at the link.

What are the legislative key requirements?

Implementation of Information Security Management System

The subject is obliged to develop and implement information security management system within the timeframe defined by the legislation

Information Security Audit

The subject is obliged to conduct primary and periodic audits of information security on compliance with minimum standards

Penetration Testing

The subject is obliged to conduct a penetration test in the information system

Information Security Manager

The subject is obliged to determine the person responsible for the fulfilment of the information security requirements in the organization

What are minimum requirements for Information Security?

The subject is obliged to adopt internal rules for information security and determine the information security policy of the organization, which shall meet the minimum requirements of information security established by the supervisory body.

The first/second category subject is obliged to implement the information security management system within two years after being listed as a critical information system entity. **The third category subject** is obliged to implement the information security management system in accordance with the following requirements determined by the regulator, **within 3 calendar years** after being put on the list approved by a government decree:

Year 1: Planning	Year 2: Implementation	Year 3: Monitoring and Improvement
▸ Leadership and management commitment ▸ Organizational arrangement ▸ Determining the scope of the ISMS ▸ Establish and approve ISMS policy ▸ Asset Management and risk assessment ▸ Preparation of statement of applicability of control mechanisms ▸ Information Security tasks and implementation plans ▸ ISMS documentation management	▸ Implementation of the risk treatment plan ▸ Implementation of control mechanisms in an organization ▸ Defining proper measures for effectiveness of control mechanisms. ▸ Trainings, awareness and competence	▸ Identification and implementation of monitoring and review procedures for ISMS ▸ Perform internal audit on ISMS ▸ Perform management review of ISMS ▸ Corrective actions for discrepancies ▸ Continual improvement and communication of ISMS

Administrative Sanctions

The new amendments established administrative sanctions for violating relevant information security-related requirements. The law defines fines from 5,000 up to 20,000 GEL for various categories of administrative sanctions (**0.01%, 0.05% or 0.1% of the supervisory capital** for third category subjects, **min. 20,000 GEL**), including failure to conduct mandatory information security audits and penetration tests.

How can we help you?

EY has a dedicated team of experienced consultants, who have been helping organizations from various industries protect their information assets, improve technology capabilities, comply with local and international regulations and grow their business with effective information security management. We have developed 6 main areas of interest that will help you comply with new regulatory requirements and ensure high standard of security.

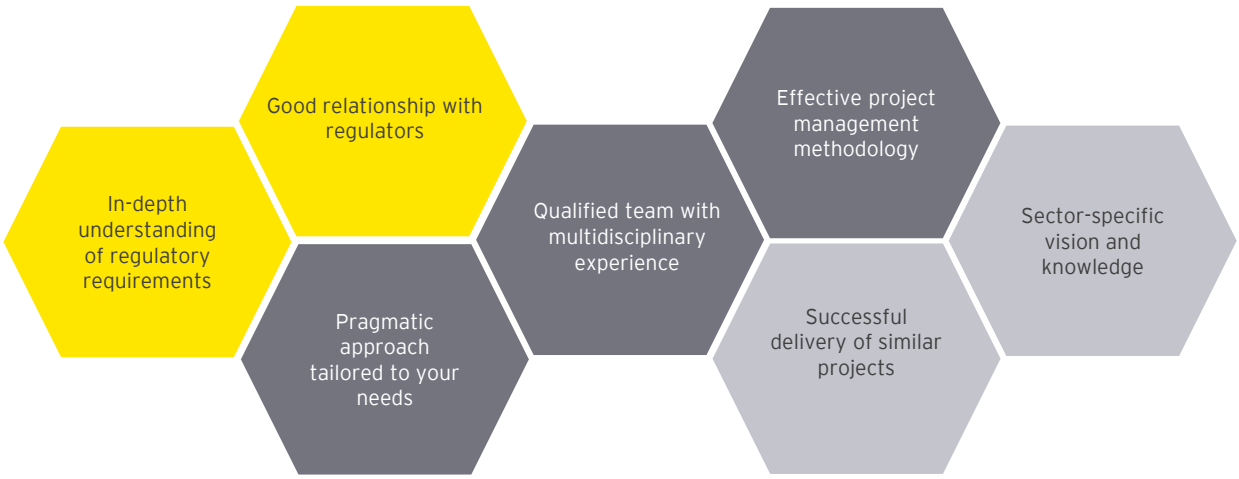
Implementation of Information Security Management System	Development and implementation of the ISMS program, including detection, classification and management of critical information	▸ Current situation assessment (the so-called Gap analysis) ▸ Development of ISMS program tailored to the needs of the organization ▸ Implementation of ISMS program
Implementation of information security systems	Support the organization in the consortium with integrators in the process of the implementing information security systems (e.g. DLP, SIEM, IPS)	▸ Study the needs of the organization and develop tender documents (e.g. technical assignment, qualification requirements and etc.) ▸ Introducing systems in consortium with suppliers and adjusting to organization specifications
Information security audit/ evaluation	Compliance with the minimum requirements established by the supervisory body of the management system	▸ Information security audit/evaluation ▸ Consultation service - preparation of response action plan and guide to the discrepancies identified by the audit
Development of information security incident management program	Develop an incident response framework, methodology and procedures	▸ Development of incident response framework ▸ Define the incident management lifecycle and response methodology ▸ Procedures and instructions for incident detection, containment, elimination and recovery ▸ Testing response plans and developing recommendations ▸ Testing of used system/facilities
Penetration Testing/ Red Teaming	Simulation of techniques and methods used by malicious actors in real life	▸ Identifying weaknesses of the organization's defense mechanisms by simulating attacks, assessing the possibility of their exploitation and developing relevant recommendations. ▸ Consultation service- preparation of legal response plan and guidelines for vulnerability identified as a result of penetration test.
Raising awareness on information security	Raising awareness of the main security threats and relevant protection mechanisms for the employees of the organization	▸ Information security awareness training for different target groups, for example: C- level, privileged users, standard users, physical security specialists, etc. ▸ Social engineering tests (e.g. Self-Phishing) ▸ Implementation and support of the online platform for raising awareness.

Projects conducted in Georgia

EY Georgia team has successfully implemented a number of projects in the field of information security and technologies. The main projects are given as a Table:

#	Name of organization	Project title
1	Operator of Electricity Distribution System	Organization and implementation of Information Security Management System (ISMS) in accordance with ISO/IEC 27001 security standard
2	TOP 3 Georgian Banks	Internal audit of Information Security Management System (ISMS) in accordance with ISO/IEC 27001 security standard
3	TOP 3 Georgian Banks	Compliance assessment against requirements of ISO/IEC 27001 security standard
4	TOP 3 Georgian Banks	7 audit assignments within the framework of IT internal audit co-sourcing, including, cyber, IT and third party risk management audits
5	TOP 10 Georgian Banks	Compliance assessment against Cybersecurity Management Framework of the National Bank of Georgia (NBG)
6	TOP 10 Georgian Banks	Compliance assessment against SWIFT Customer Security Programme (CSP)
7	TOP 10 Georgian Banks	PSD2 Open API Penetration Testing
8	Electricity Distribution Organization	Development of IT and Information Security (IS) processes and policies
9	LEPL Public Service Development Agency	Compliance assessment of trust and qualified trust services (e.g., electronic signature or stamp) against requirements of European Telecommunications Standards Institute (ETSI) standards

Advantages of collaborating with EY



About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

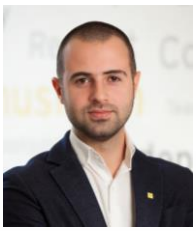
EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

About EY's Advisory Services

EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

Contact person



Giorgi Tsintskiladze
Consulting Service Line Leader,
Technology Risk Group

+995 32 215 88 11

Giorgi.Tsintskiladze@ge.ey.com