CYBERSECURITY & ISO STANDARD 27701

A project of Swiss Agency for Development and Cooperation SDC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

In partnership with:

MINISTRIA E EKONOMISË, KULTURËS DHE INOVACIONIT

Implemented by:

HELVETAS

PARTNERSALBANIA
FOR CHANGE AND DEVELOPMENT

This document has been produced by RisiAlbania. Risi is a youth employment project of the Swiss Agency for Development and Cooperation SDC, implemented by Helvetas and Partners Albania for Change and Development. The views and conclusions contained here do not necessarily reflect neither those of the Swiss Government nor the Swiss Agency for Development and Cooperataion SDC.

CYBERSECURITY & ISO STANDARD 27701

GUIDANCE

Prepared by:

NIALL CONDON
Independent Consultant

Helvetas and Partners Albania for Change and Development are implementing the RisiAlbania youth employment project, supported by Swiss Agency for Development and Cooperation (SDC).

RisiAlbania supports the creation of quality jobs in the local IT sector. The project has supported the **growth of e-commerce** in Albania by assisting businesses in adopting digital payment solutions and enhancing their online presence. To enhance competitiveness and access to higher-value markets, RisiAlbania has facilitated the **certification** of local companies with international standards such as ISO 27001 (Information Security Management) and ISO 27701 (Privacy Information Management). Recognising the potential of the **business processing outsourcing (BPO) sector**, the project has worked to position Albania as a value-added destination for outsourcing services.

TABLE OF CONTENTS

PART 1 - THE BASICS

What is Cybersecurity?

Cybersecurity is the practice of protecting computers, networks, and data from unauthorized access, theft, damage, and disruption. Cybersecurity measures involve multiple layers of protection (see diagram below) designed to protect digital information from cyber-attacks or other threats such as natural disasters.

In 2024 Albania enacted a new cybersecurity law (Law No. 25/2024 on Cybersecurity) to strengthen its national cybersecurity infrastructure The implementation of the law is overseen by the **National Cyber Security Authority (NCSA).** The law requires compliance from organisations that manage and process significant amounts of digital information, including public and private organisations operating critical infrastructure in the energy, transportation, banking and healthcare sectors.

COMMON TYPES OF CYBERSECURITY THREATS

Phishing

the practice of sending fraudulent emails to steal sensitive data like credit card numbers and login information.

Ransomware

a type of malicious software designed to extort money by blocking access to files or the computer system until a ransom is paid.

Malware

a type of software designed to gain unauthorized access or to cause damage to a computer

What is ISO 27001?

ISO 27001 is an international standard for **managing information security.** The standard provides a framework for setting up and implementing what are called **information security management systems (ISMSs**) to protect against cyberattacks.

ISMS are sets of policies, procedures and controls established by organisations to **protect its information** (e.g. customer information, financial records, intellectual property) from unauthorised access; **identify potential risks** to information security; **build trust** with customers and facilitate **access to new markets** where information security is a key entry requirement; and **ensure compliance** with legal requirements such as the Albania's cybersecurity law and the EU's GDPR legislation (more on this below).

What is ISO 27701 & GDPR?

ISO 27701 is an extension of ISO 27001 focusing on privacy, aiming to ensure the privacy of what's called **personally identifiable information (PII)** - any information connected to a specific individual that can be used to uncover that individual's identity, this includes information such as their social security number, full name, email address or phone number.

Whilst ISO 27001 guides organisations through the process of creating a robust information security system, ISO 27701 takes this a step further by ensuring that strong information privacy measures are incorporated into this system. Organisations already ISO 27001 certified will find it relatively straightforward to meet the requirements of ISO 27701 (see the next page for more details and guidance on the certification process).

ISO 27701 is designed to help organisations meet the requirements of the **EU's General Data Protection Regulation (GDPR)** legislation, which was enacted in 2018 to regulate how organisations handle the personal data of EU citizens. GDPR **protects personal data** by requiring that organisations handle this data responsibly and securely and provides individuals with the **right to access** their data and **limit how their data is used**. ISO 27701 provides a strong foundation for GDPR compliance, addressing many, but not all, of the technical and organizational measures required by GDPR.

Albanian businesses, regardless of size or industry, who collect and process personal data of EU citizens as a result of selling goods or services to the EU must comply with the requirements of GDPR. Non-compliance can result in bans or limits on data processing, compulsory audits of data handling or in a worst case scenario fines up of to 4% of turnover. Having ISO 27701 certification goes a long way to ensuring that Albanian businesses meet the requirements of GDPR and are safe to do business in the EU. Compliance with GDPR is also critical to Albania's EU accession process.

EXAMPLES OF LAYERS OF CYBERSECURITY

ENDPOINT SECURITY

Securing individual devices such as computers, smartphones, and tablets; includes antivirus software, anti-malware programs.

DATA SECURITY

Protects data from unauthorized access; includes encryption, data masking, and secure data storage solutions.

NETWORK SECURITY

Protects the integrity, confidentiality, and availability of network and data; includes firewalls, intrusion detection systems, and secure network protocols.

PHYSICAL SECURITY

Securing physical access to computers, servers, and other devices. Measures include locked doors, security guards, and surveillance cameras.

PART 2 - MAKING IT HAPPEN

What do I need to become ISO27701 certified and who can help me to do it?

A key first point to understand is that because ISO 27701 is an extension of ISO 27001, an organisation must first be ISO 27001 certified before it can consider ISO 27701 certification. Organisations typically apply for both standards simultaneously - this is the process set out in the diagram below

1

DECIDE IF CERTIFICATION IS REQUIRED.

WHAT is involved in this?

Answering a couple of simple questions can help your organisation understand whether ISO 27001-27701 certification is needed in the first place:

- Am I required to comply with Albania's 2024 cybersecurity law? In other words, does my organisation operate any critical infrastructure highlighted in this legislation?
- Do I need to comply with the requirements of GDPR? In other words, does my organisation currently, or plan to, collect and process the personal information of EU citizens?

WHO can support me?

Albania's National Cyber Security Authority (NCSA).can provide guidance on who needs to comply with the 2024 cybersecurity law and GDPR.

2

COMPLETE INITIAL ASSESSMENT & PLAN

WHAT is involved in this?

Once it is determined that certification is required, the next step is to conduct a gap analysis to identify and document your organisation's existing information security and privacy controls and highlight gaps against both ISO 27001 and ISO 27701 standards.

The gap analysis will be used to develop a project plan outlining the resources, timelines, and tasks for both ISO 27001 and ISO 27701 implementation.

WHO can support me?

Local security and privacy experts can support your internal IT team to conduct this gap analysis. InfoSecurity https://infosecurity.al is a local service provider with expertise on cybersecurity & conducting ISO 27001/27701 gap analysis and project planning. Fisa Academy https://www.fisa.pro/ offers professional training and international certifications in the fields of cybersecurity, information technology, and ISO standards, tailored for professionals and organizations. Through practical courses, online platforms, and technical consultancy, the academy supports the development of digital skills and compliance with global standards. Additionally, it serves as a bridge between the job market and talent in the ICT sector, fostering employment and professional **growth.**

3 ESTABLISH DATA SECURITY & PRIVACY MANAGEMENT SYSTEMS

WHAT is involved in this?

Develop and put in place the technical and organisational controls[1] required by both standards.

Build employee awareness and understanding of information security and privacy through regular training and education sessions with the ultimate objective of creating a strong culture of information security and privacy within the organisation.

WHO can support me?

Again, a local service provider such as InfoSecurity should be used to support the process of building your organisation's capability to comply with the data security and privacy controls required by both standards.

4 COMPLETE AUDIT & BECOME CERTIFIED

WHAT is involved in this?

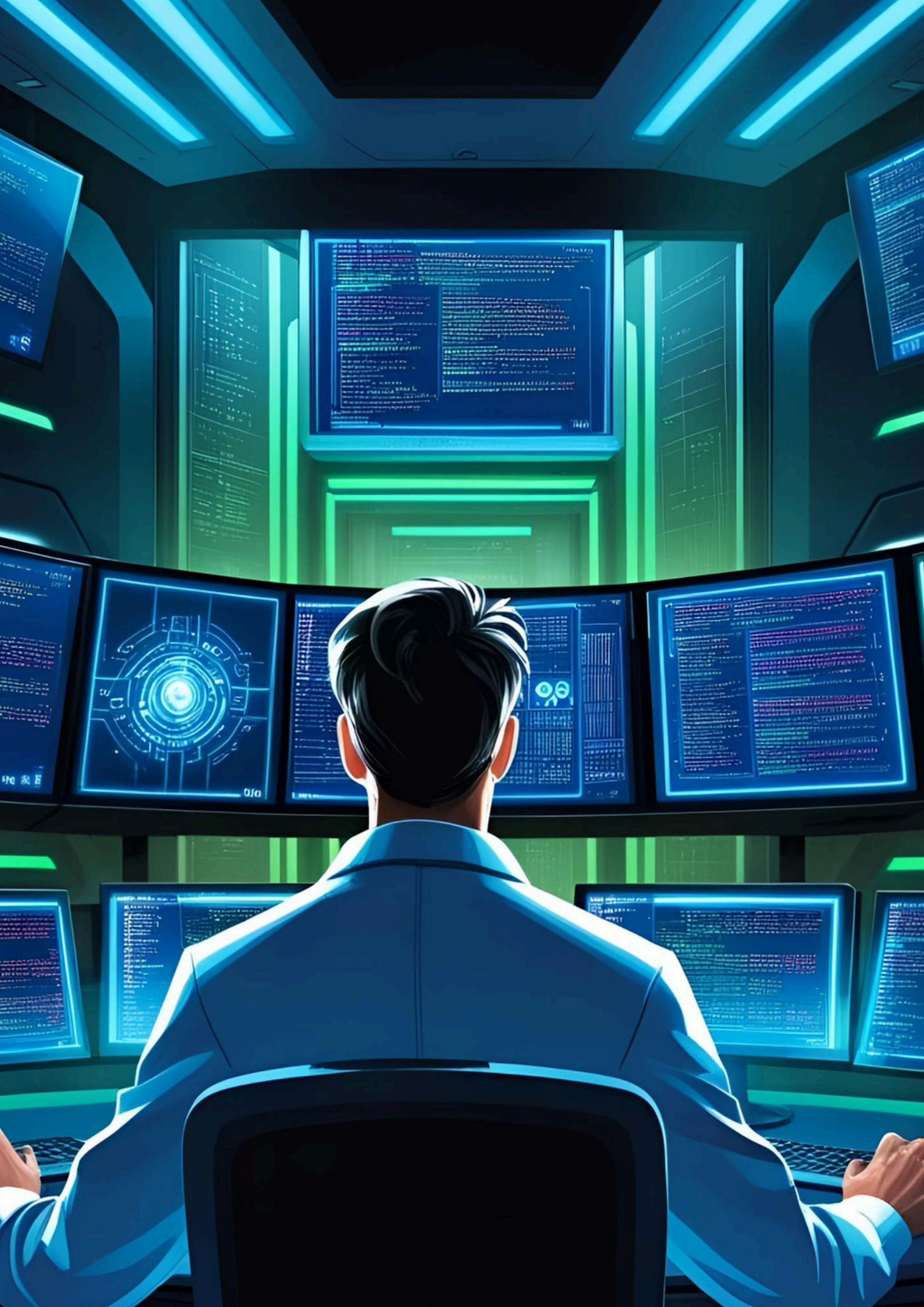
Conduct an internal pre-assessment audit to identify any remaining gaps for both standards.

Complete the formal certification audit by an accredited certification body for both standards. If successful, certification will be awarded.

WHO can support me?

Axe Register https://www.axe-register.com/ is the only local accredited certification body authorised to complete ISO 27001 and 27701 audits and issue certification. International accredited auditors are also an option, albeit more expensive.

[1]Technical controls include access control (user access management, including authentication and authorization mechanisms); encryption to prevent unauthorized access and ensure data privacy; network security (e.g. firewalls) and endpoint security (e.g. anti-virus software on computers). Organisational control include information security and privacy policies and procedures such as data retention and disposal policies; risk and incident management procedures for detecting, reporting, and responding to information security incidents.



Ismail Qemali Str,
P18, H.3, Apt. 15
Tirana, Albania

+355 (0) 422 48 527

info@risialbania.al