



**European Union**  
European Regional  
Development Fund



OPERATIONAL PROGRAMME  
**INNOVATIONS AND  
COMPETITIVENESS**

# PENETRATION TESTS



## What are Penetration Tests?

Penetration tests mimic real attacks to systems, applications, and data that can be triggered by external hackers, malicious employees, cyber-crime organizations and others. This controlled, authorized process is carried out according to the customer's requirements and in no way adversely affects the tested systems. The techniques Lirex uses allow detection of vulnerabilities that could be exploited to harm the organization. Cluster ITOS team performs the penetration tests and after summarizing the results provide you a report containing recommendations for their resolution.

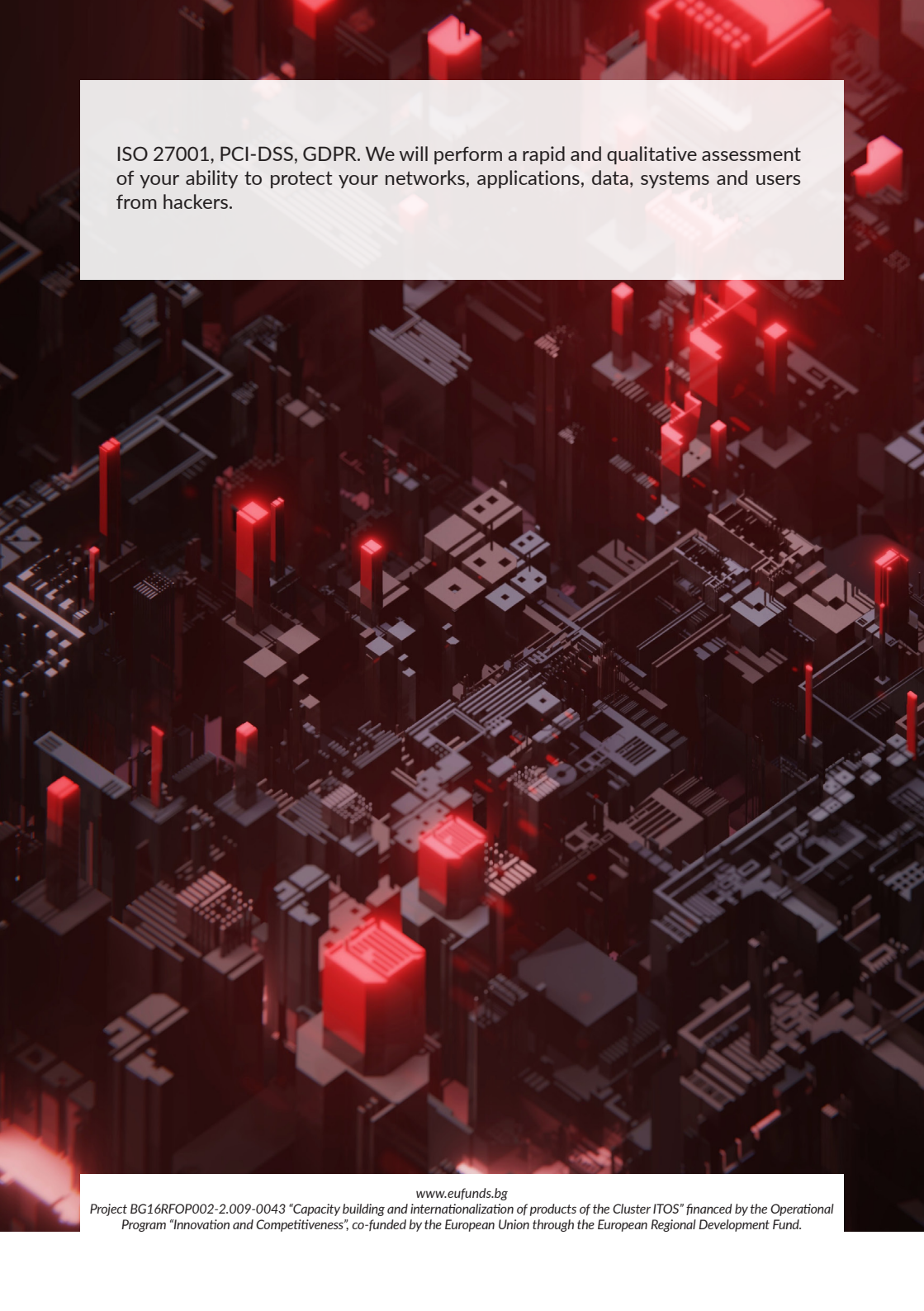
## Information Security Assessment is made by:

- Identification and evaluation of vulnerabilities
- Identification of vulnerabilities that are not detected with automated vulnerability scanning
- Evaluation of the impact in case of a successful attack
- Checking the actual network security performance by performing more frequent and more complex tests, you can predict security risks more effectively and protect the organization from unauthorized access to critical systems and valuable information.

## Why perform such a test?

- To assess the level of protection of your networks, applications, data, systems, and users
- To protect the assets and reputation of the company by avoiding financial losses and negative publicity
- To assess which vulnerabilities are critical to the organization, which are less important, as well as to distinguish "false positives".
- To justify the need for allocating a security budget;
- To detect vulnerabilities and enhance security in order to fit the organization systems' criteria;
- To address basic requirements related to regulations and standards such as ISO 27001, PCI-DSS, GDPR, and prevent the imposition of high sanctions in the event of non-compliance.

Security breakthroughs can negatively affect the reputation of the organization, reduce the credibility of the company and lead to direct financial losses. Companies from Cluster ITOS offers penetration testing services that can be applied as an individual order or as a part of a strategy for regular security testing, in order to meet the requirements of regulations and standards such as



ISO 27001, PCI-DSS, GDPR. We will perform a rapid and qualitative assessment of your ability to protect your networks, applications, data, systems and users from hackers.

[www.eufunds.bg](http://www.eufunds.bg)

Project BG16RFOP002-2.009-0043 "Capacity building and internationalization of products of the Cluster ITOS" financed by the Operational Program "Innovation and Competitiveness", co-funded by the European Union through the European Regional Development Fund.