Security Assessment

Why to perform a Security Assessment?

A security assessment is performed to identify the current security posture of an information system or organization. The assessment provides recommendations for improvement, which allows the organization to a reach a security goal that mitigates risk and enables the organization to havesafe business processes implemented.

What is Security Assessment?

Security assessment projects have a beginning and an end. They produce a unique value to the organization. Information security assessment is a measurement of the security posture of a system or organization. Security posture is the way the information security is implemented. Security assessments are risk-based assessments, due to their focus on vulnerabilities and impact. Security assessments rely on three main assessment methods that are interrelated. Combined, the three methods can accurately assess the Technology, People and Process elements of security.

How will we help you with our security assessment approach ?

Our approach to security assessment will provide you answers to the following questions:

- What is critical information?
- What controls are in place for information systems?
- What is the current security posture of information systems?
- Should more or less stringent countermeasures be instituted?
- What is the prioritized security roadmap to follow?
- What high-priority issues should be fixed first?
- Is my company in compliance with adopted policies?

Security assessment services from Ibis instruments can help you to:

- Understand your current risk posture as compared to the leading practices and compliance requirements
- Reconcile current controls with your appetite for risk
- Document existing controls and security efforts
- Identify and quantify risks to your information assets
- Understand the strengths and weaknesses of your current defences
- Examine weaknesses from the perspective of the attacker
- Align organization IT risk management programs with your security and business goals
- Identify areas of operation where the risk to your organization may be too high
- Implement cost-effective security measures in order to protect your information assets

How do we perform security assessment?

In order to obtain adequate results, Ibis-Instruments uses the "big picture" activities approach which can be divided into the following steps:

Reviewing Method

The reviewing method includes passive review techniques and interviews, which are generally conducted manually. They help evaluate systems, applications, networks, policies and procedures to discover vulnerabilities. They include the review of documentation, architecture, rule sets and system configurations. The reviewing method enables the understanding of critical information & systems and how the organization wants to focus on security.

Examination Method

Examination is a hands-on technical process that looks at the organization specifically from the aspect of system/network level to identify security vulnerabilities that exist in those systems. This includes doing technical analysis of the firewalls, intrusion detection systems and routers, as well as used processes. It also includes vulnerability scans of the customer's networks. The reviewing assessment method provides excellent information that leads to future examinations.

Testing Method

Testing, often called security stress testing, is a process whereby someone imitates an adversary looking for security vulnerabilities within your infrastructure, regardless of whether they are on the IT side or on the side of implemented processes, which allow them to break into the system or network or jeopardize some of your resources.

Ibis Instruments
Measurement & Telecommunication Systems

What benefits can I reach by using Ibis-Instruments security assessment?

There are various benefits from implementing a security assessment approach because they provide support to an organization's business activities, namely:

- Security assessment programs help ensure that the greatest risks to the organization are identified and addressed on a continuous basis. Such programs help ensure that the expertise and best judgments of the personnel, both in IT and the wider organization, are tapped to develop reasonable steps for preventing or mitigating situations that could interfere with accomplishing the organization's mission.
- Security assessments help the personnel throughout the organization to better understand risks to business operations. They also teach them how to avoid risky practices, such as disclosing passwords or other sensitive information, and recognize suspicious events. This understanding grows, in part, from improved communication among business managers, system support staff and security specialists.
- Security assessments provide a mechanism for reaching a consensus as to which risks are the greatest and what steps are appropriate for mitigating them. The processes used encourage discussion and generally require the resolution of disagreements. This, in turn, makes it more likely that business managers will understand the need for agreed-upon controls, feel that the controls are aligned with the organization's business goals and support their effective implementation. Executives have found that controls selected in this manner are more likely to be effectively adopted than controls that are imposed by personnel outside the organization.
- A formal security assessment program provides an efficient means for communicating assessment findings and recommending actions to business unit managers as well as to senior corporate officials. Standard report formats and the periodic nature of assessments provide organizations a means to readily understand reported information and compare results between units over time.

Ibis Instruments Belgrade
Tošin bunar 272, 11070 Belgrade, Serbia
Office: +381 11 7152 200, Fax: +381 11 7152 201
e-mail: info@ibis-instruments.com
www.ibis-instruments.com

Ibis Instruments DOOE import-export Skopje
Veljko Vlahović 1-2/2, 1000 Skopje, Macedonia
Office: +389 2 321 5700, Fax: +389 2 321 5700
e-mail: info@ibis-instruments.mk
www.ibis-instruments.com/mk

Ibis Instruments Banja Luka (branch office)
Jovana Dučića 37, 78000 Banja Luka
Office: 387 51 223 840, Fax: 387 51 223 841
e-mail: office-bl@ibis-instruments.com
www.ibis-instruments.com