IT SECURITY & CYBER SECURITY

iAP CYBER SECURITY

iAP – INDEPENDENT CONSULTING + AUDIT PROFESSIONALS offers comprehensive expertise for more than 15 years in the areas of **IT Auditing & Certification, IT Security & Cyber Security, Consulting and Data Protection**.

As auditors and consultants with an extensive industry experience, we offer external IT audits and certifications adding value and advice in a national & international environment.

The degree of digitization is constantly increasing in all institutions leading to an increased risk of cyber attacks. To counteract and optimize your cyber resilience, iAP offers various types of technical cyber security audits.

Examples are:

iAP CYBER SECURITY

- **BASIC CHECK**
- **OSINT ANALYSIS**
- **VULNERABILITIES ASSESSMENT**
- **PENETRATION TEST**

iAP
CYBER SECURITY AUDITS

Don't leave your security to chance.
Get a realistic view of your security level and your partners'. Don't rely on trust only, proof it!

Basic Check

OSINT Analysis

Vulnerability Assessment

Penetration Test

iAP CYBER SECURITY

BASIC CHECK, OSINT ANALYSIS, VULNERABILITIES ASSESSMENT, PENETRATION TEST

The iAP cyber security audits are based on true needs of an institution and can be used individually or combined.

Our proactive security measures are based on the recommendations of the German Federal Office for Information Security (BSI) and the Open Web Application Security Project (OWASP).

The clients' IT systems are examined in various ways, internally, externally or in combination, depending on the respective requirements and purpose, in order to uncover security gaps before they can be exploited by cyber criminals.

The center of auditing are the IT systems relevant to perform critical business processes in order to ensure their availability, confidentiality and integrity.

Every iAP cyber security audit is an evidence-based investment to increase the security level of the corporate IT infrastructure.

iAP CYBER SECURITY BASIC CHECK

- The iAP Basic Check is based on a questionnaire and contains important questions based on the standards of the Federal Office for Information Security (BSI) in order to carry out a basic initial assessment of your information security.
- We focus on data protection, the assignment of authorizations, passwords, the backup concept, the detection and handling of incidents, e-mail security, raising employee awareness, availability requirements, the emergency concept and the online shop security.
- The client answers all questions and then receives an understandable short report from the iAP cyber security experts with a criticality assessment and information on how to treat identified weaknesses.

For whom?

The **iAP Basic Check** is usually used if:

- the aim is to assess which extensive basic cyber security requirements are met
- and to cost-effectively determine safety-related criticalities

iAP CYBER SECURITY OSINT ANALYSIS (**O**PEN **S**OURCE **INT**ELLIGENCE)

- Based on the OSINT framework, iAP collects and evaluates online information about the institution from the point of view of a cybercriminal.
- It is examined whether data is publicly available on the Internet, Deep Web and Darknet, which indicates security gaps and thus possible points of attack. Current threats such as DDoS, phishing, exploits and data breaches are considered.
- OSINT Analysis focuses on the attack surface, infrastructure stability, forwarding of user data from your website visitors, configuration of the DNS infrastructure and more for appropriate encryption of mail servers.
- The client receives a final report with only true positive vulnerabilities.
- In addition, iAP points out criticalities and information on how to treat identified weaknesses.

For whom?

- The iAP OSINT Analysis should be utilized by every institution as it is a very cost-effective service to list the vulnerabilities visible to experienced hackers.

iAP CYBER SECURITY VULNERABILITIES ASSESSMENT

- The iAP Vulnerability Assessment is the most common form of a security audit.
- The clients' IT systems are scanned in detail for known vulnerabilities and threats; existing security gaps can be identified.
- The client receives a final report with only true positive vulnerabilities.
- In addition, iAP points out criticalities and information on how to treat identified weaknesses.

For whom?

The iAP Vulnerabilities Assessment is used if:

- an automated examination and evaluation of the IT infrastructure components and applications regarding commonly known vulnerabilities are desired
- IT systems were reinstalled or massively changed
- the IT systems should be audited regularly using comparable scans in order to identify security-related deficiencies in time.

iAP CYBER SECURITY PENETRATION TEST

iAP Penetration Tests are available in different versions according to the agreed test objectives of the client. In general, the following is tested:

- Determination of existing security measures in terms of existence, appropriateness and effectiveness
- **Networks (internal/external)**, e.g. ports, segmentation, encryption, administrative access, network registration
- **Web applications**, e.g. configuration, authorization, authentication, encryption, session security
- **Cloud,** e.g. API interfaces
- **WLAN,** e.g. access, networks
- **Employees,** e.g. social engineering
- **Physical security facilities,** e.g. access, theft

For whom?

iAP Penetration Tests are is used if:

- An individual and in-depth analysis of the IT systems including a vulnerability scan with manual evaluation is desired
- e.g. "White Tests" with precise system information, "Gray Tests" with limited system information or "Black Tests" without access information.

iAP CYBER SECURITY QUESTIONS AND ANSWERS

Why should you have your security audited by iAP?

The results of the iAP security audits provide a lot of information - for example, whether your security facilities can be bypassed, or how your IT systems deal with exceptionally high loads, such as during a DDoS or a botnet attack.

Reasons for iAP security audits:

- Identify gaps and weaknesses in your cyber security
- Protect critical business processes and maintain business continuity
- Ensure availability, confidentiality, integrity and authenticity of your information
- Prevent costly impacts of cyber attacks
- Avoid production downtime, loss of reputation, payment of damages and ransom, leak of your knowhow
- Ensure compliance requirements
- Reduce costs of cyber insurance

Don't leave your security to chance. Get a realistic overview of your security level and your partners'.

Don't rely on trust only, proof it!

iAP CYBER SECURITY QUESTIONS AND ANSWERS CONT.

When and how often should iAP security audits be carried out?

The Federal Office for Information Security (BSI) recommends having the IT system landscape verified regularly by professional and independent thirdparty auditors, at least once a year.

Furthermore, the cyber security level should be audited after establishment or massive changes to your IT systems, after cyber attacks and regarding compliance requirements.

How long do iAP security audits take?

The duration of a security audit depends on the agreed objectives, the number and variety of the investigated areas and the audit scope.

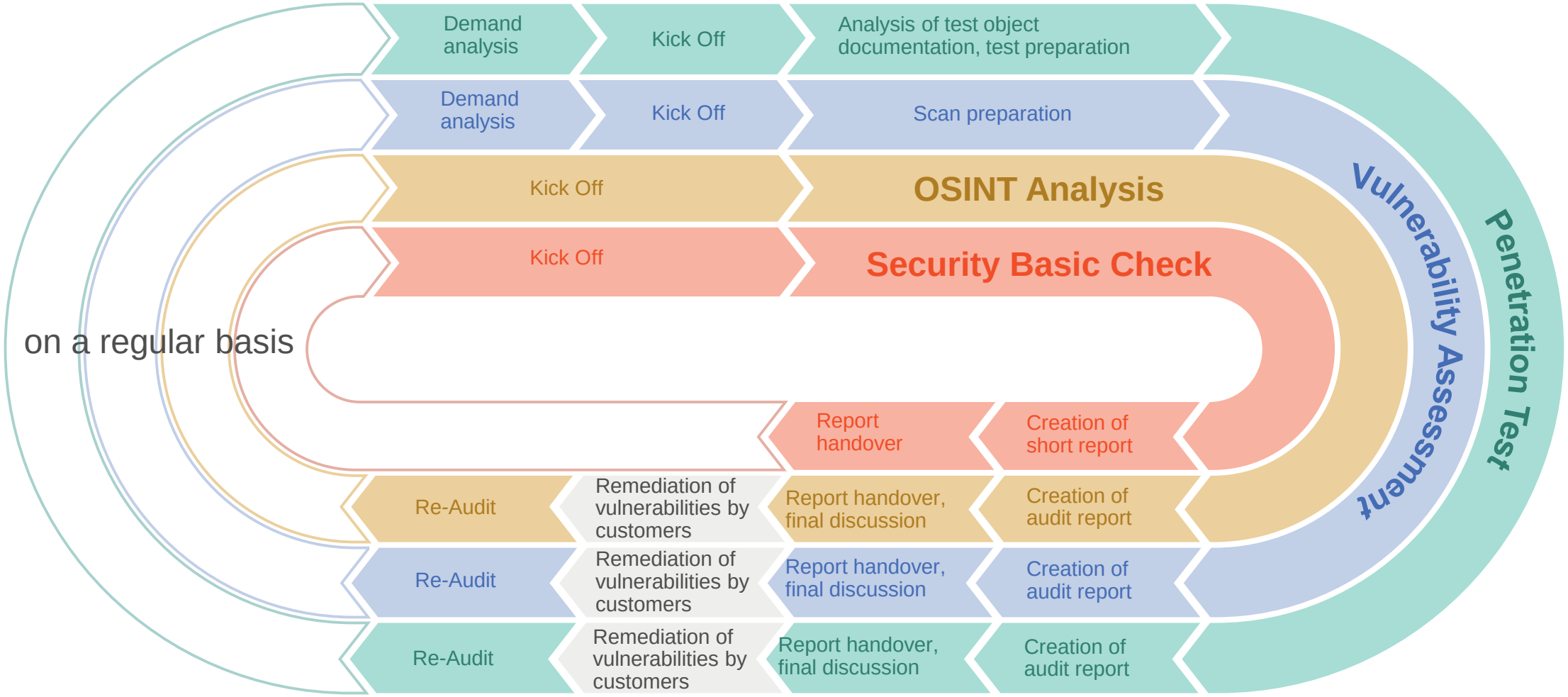
While the Basic Check takes a few hours, the OSINT Analysis, Vulnerability Assessment and Penetration Test can take a few days to several weeks.

How much do iAP security audits cost?

Fixed prices apply for the OSINT Analysis and the Basic Check.

The costs for Vulnerability Assessments and Penetration Tests are calculated individually according to the desired type, scope and goals.

iAP CYBER SECURITY PROJECT EXECUTION



iAP CYBER SECURITY THE AUDIT REPORT

All reports are written and addressed with a confidentiality label to the target group defined by the client.

The reports are available in **German, English and Spanish.**

The **iAP Audit Report** contains

- a description of the audit objects, goals and test conditions
- a management summary
- a detailed list of identified vulnerabilities with criticality assessment
- recommendations for professional risk management.

EXAMPLE: AUDIT REPORT iAP OSINT ANALYSIS

YOU HAVE QUESTIONS? WE HAVE ANSWERS!

iAP - Independent Consulting + Audit Professionals GmbH
Tel. +49 30 4397 16860
kontakt@audit-professionals.de