

Why?

To protect your company's information, **Rempart international** offers you a complete training audit, with regard to your expectations and needs.

The cyber audit reviews objectively the situation in terms of security of your digital intangible assets.

How?

A three-step process:

- Pre-audit
- Operational auditing
- Implementation of recommendations

Conducted by specialists:

- In cryptography
- In network security
- In application vulnerability

Several possible strategies :

Participative or White box

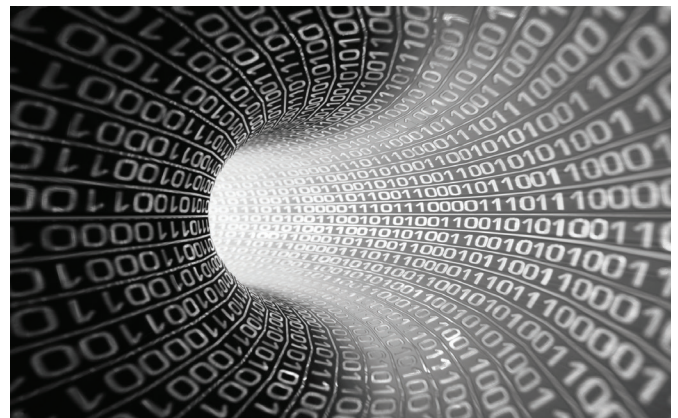
Auditors have a total access to the infrastructures, with the participation of the employees/users.

Cooperative or Grey box

Auditors have a total access to the infrastructures without employee participation.

Blind test or Black box

Auditors don't have any access and establish their own information database.



Deliverable on request :

- An audit report : at each stage, delivery of a confidential record to the client, with the findings report.
- Fault correction guide : at the end of the audit, delivery of a file to the client, with the methods and good practices to correct detected vulnerabilities.
- The application guidelines for corrective measures : at the end of the audit, intervention of a team to correct all or a part of the detected vulnerabilities.

In addition to this audit, we recommend you to follow an adapted training to optimize your protections.

Contact us for more information



Rempart-International

26, rue de Louvigny – L1946 Luxembourg

T : +352 288 557 - contact@rempart-international.com

RCS Luxembourg B196245- Autorisation ME N°10058858/0 - 10058858/1 - 10058858/2 - Autorisation MJ N° 22-2-800-458