How to Conduct an Audit

Conducting a security audit involves a systematic and comprehensive assessment of an organization's security controls, policies, and procedures.

* **Define Objectives and Scope**: Clearly define the objectives and scope of the security audit. Identify the systems, networks, applications, or processes that will be audited. Determine the specific areas of focus, such as access controls, network security, data protection, or compliance with regulations.
* **Gather Information**: Collect relevant documentation, policies, procedures, and technical specifications related to the audited systems or processes. This includes security policies, network diagrams, system configurations, access control lists, and incident response plans. Gain an understanding of the organization's security goals, regulatory requirements, and industry best practices.
* **Perform Risk Assessment**: Conduct a risk assessment to identify potential vulnerabilities and threats that could impact the audited systems. Assess the likelihood and potential impact of each risk and prioritize them based on their significance to the organization. This assessment helps determine the areas that require more attention during the audit.
* **Develop Audit Plan**: Create a detailed audit plan outlining the methodologies, tools, and techniques that will be used during the audit. Define the audit procedures, such as interviews, document reviews, vulnerability scanning, penetration testing, or configuration analysis. Establish a timeline and allocate resources accordingly.
* **Conduct Fieldwork**: Execute the audit plan by performing the agreed-upon procedures. This may involve interviewing key personnel, reviewing security controls, assessing technical configurations, examining logs and records, and conducting vulnerability assessments or penetration tests. Collect evidence and document observations.
* **Analyze Findings**: Analyze the collected data and evidence to identify security weaknesses, vulnerabilities, or non-compliance with policies and standards. Evaluate the effectiveness of existing security controls and processes. Compare the findings against established benchmarks, industry best practices, and regulatory requirements.
* **Prepare Audit Report**: Prepare a comprehensive audit report summarizing the findings, observations, and recommendations resulting from the audit. Clearly document the identified vulnerabilities, risks, and non-compliance issues. Provide actionable recommendations for improving security controls, policies, or procedures. Prioritize recommendations based on their potential impact and urgency.
* **Communicate Results**: Present the audit report to the relevant stakeholders, including management, IT teams, and other key personnel. Clearly communicate the findings, risks, and recommendations in a concise and understandable manner. Address any questions or concerns and seek feedback or input from stakeholders.
* **Monitor and Follow Up**: Track the implementation of recommended actions and improvements based on the audit findings. Monitor progress and ensure that identified vulnerabilities are remediated and control gaps are addressed. Conduct periodic reviews to assess the effectiveness of implemented measures and monitor changes in the organization's security posture.
* **Continual Improvement**: Use the audit findings as lessons learned to enhance the organization's overall security posture. Continually update and improve security policies, controls, and procedures based on emerging threats, industry trends, and regulatory changes. Regularly schedule security audits to maintain a proactive approach to security.

Red Team Audit

A Red Team audit is meant to simulate a real attack in order to test the global security level of the information system and the [awareness of the employees](https://www.algosecure.fr/conseil/sensibilisation-securite). The objective is to demonstrate the potential consequences of an attack, and to test the reactivity of the defense teams.

It differs from a [penetration test](https://www.algosecure.fr/audit/audit-pentest) because it doesn't limit itself to listing vulnerabilities on a delimited perimeter.

* It targets an entire ecosystem: information system and employees.
* It is less limited in its execution perimeter, just like a real-life attack.

The Red Team audit can be seen as a combination of attack scenarios and objectives to accomplish. They are jointly defined by AlgoSecure and the customer, according to the activity sector and the identified risks. A few examples are:

* Remote intrusion: identifying and exploiting every available public resource, such as websites, message interfaces...
* User Phishing: phishing mails, dropping malicious USB drives near the employees paths...
* Non destructive physical intrusion in the customer's office in order to connect a device to the client's network.

Only a few of the customer's employees are informed of this audit, and it's generally done over a relatively long period, typically a few months, so the customer cannot predict when the different scenarios will be accomplished, and therefore challenge the security in real-life conditions.

Some of the methods that can be done :

Recon:

The recon phase is a lot bigger than in a regular audit. The reason being that we don't just map out the computer resources and information system, but also identify the workers we could compromise later during the audit.

For this, we conduct multiple operations with the goal of:

* identify the company workers based on an organization chart on the company website
* identify the company workers based on informations posted on social networks
* identify the company workers with large permissions and access to the information system, such as administrators, or IT support
* identify the company workers with lesser computer/security skills such as secretaries or entreprise responsible
* identify computer technologies used based on job offers posted on the internet
* and of course, identifying publicly exposed services: webmail, VPN access, extranet, firewall or server administration...

External Resource attack:

This stage amounts to an [external audit](https://www.algosecure.fr/audit/audit-securite-cloud) and a [web application audit](https://www.algosecure.fr/audit/audit-securite-web-mobile).

Social Engineering:

This is one of the main differences between a regular audit and a Red Team audit: we don't solely try to exploit software vulnerabilities, but also make use of the lack of awareness of the employees. Thanks to the informations gathered during the recon stage, we'll try to penetrate your information system using the employees.

A few examples of the methods used:

* Sending phishing emails crafted in order to target one or more employees
* Calling employees claiming to be a technical support agent
* Dropping malicious USB drives close to the office
* Dropping flyers at the reception offering advantages for local shops or restaurants

Penetrating the office:

This stage can have multiple objectives. On one hand, we can test the welcome process for outsiders and see whether it's possible to access restricted areas by using the employees' lack of awareness. On the other hand, we'll try to set up a device on the internal network in order to get a remote access to the network, and initiate the next stage without needing to physically stay in the office.

There are multiples means to this end:

* intrusion using concealed doors such as service doors, garages...
* intrusion using improperly closed windows
* intrusion by mingling with a group of legitimate employees
* intrusion through the main entrance using pretenses such as a delivery, an urgent need...

### [Internal resources attack](https://www.algosecure.fr/en/audit/red-team#attaque-ressources-internes)

If we managed to **connect a device on your network to get remote access**, this stage amounts to a [internal network security audit (LAN)](https://www.algosecure.fr/audit/audit-lan).

Some common security auditing activities performed by a red team:

* **Penetration Testing**: Red teams conduct comprehensive penetration tests to assess the effectiveness of an organization's security controls. They attempt to exploit vulnerabilities in systems, networks, applications, or physical infrastructure to gain unauthorized access or extract sensitive information.
* **Social Engineering**: Red teams employ various social engineering techniques to test the organization's employees' awareness and adherence to security policies. They may attempt to deceive employees through phishing emails, phone calls, or physical interactions to gain access to restricted areas or sensitive information.
* **Wireless Network Testing**: Red teams evaluate the security of wireless networks by attempting to gain unauthorized access to wireless access points, routers, or other wireless infrastructure. They also assess the effectiveness of encryption protocols and authentication mechanisms.
* **Application Security Assessment**: Red teams assess the security of web applications, mobile applications, or other software solutions. They identify vulnerabilities like code injection, insecure authentication, or inadequate access controls that could be exploited by attackers.
* **Physical Security Assessment**: Red teams evaluate the physical security measures in place, such as access controls, CCTV systems, alarm systems, and employee identification systems. They attempt to breach physical security barriers, gain unauthorized entry to restricted areas, or tamper with critical equipment.
* **Threat Modeling**: Red teams analyze an organization's systems, processes, and assets to identify potential threats and prioritize risks. They simulate targeted attacks based on real-world threat scenarios and assess the organization's ability to detect and respond to them effectively.
* **Security Policy Review**: Red teams review an organization's security policies, procedures, and guidelines to identify gaps or inconsistencies. They assess if the policies align with industry best practices and regulatory requirements and provide recommendations for improvements.
* **Incident Response Assessment**: Red teams simulate security incidents to assess the effectiveness of an organization's incident response capabilities. They evaluate the detection, containment, eradication, and recovery processes, and provide feedback to enhance the organization's incident response capabilities.