**Information Security Assessment**

**Information Technology Security Assessment** (IT Security Assessment) is an explicit study to locate [IT security](https://en.wikipedia.org/wiki/IT_security) [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) and risks.  **Security assessments** are periodic exercises that test your organization's **security** preparedness. They include checks for vulnerabilities in your IT systems and business processes, as well as recommending steps to lower the risk of future attacks

**Purpose of Security Assessment**

The goal of a security assessment (also known as a security audit, security review, or network assessment[[1]](https://en.wikipedia.org/wiki/Information_technology_security_assessment#cite_note-1)), is to ensure that necessary security controls are integrated into the design and implementation of a project. A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies. Management can address security gaps in three ways: Management can decide to cancel the project, allocate the necessary resources to correct the security gaps, or accept the risk based on an informed risk / reward analysis.

**What sources threaten information security?**

Threats bypassing the protection of information security can be divided into several categories. The concept of categories is mandatory, since it simplifies and systematizes all factors without exception. The main parameters are

**1.**The degree of intentionality of intervention in the information protection system:

* Threats caused by unwitting employees in the information dimension
* Threats triggered by fraudsters for personal gain.

**2.**Signs of occurrence:

* Artificial information security threat provoked by human hands
* Natural threatening factors beyond the control of information protection systems caused by natural disasters.

**3.**Classification of the immediate cause of the threat. The perpetrator can be:

* A person who disclose confidential information by bribing company employees.
* A natural factor like a catastrophe or local disaster.
* Software with the use of specialized devices or the introduction of malicious code in technical means which disturbs the functioning of the system.
* Accidental deletion of data, authorized software and hardware funds, failure of the operating system.

**4.**Severity of threats on information resources:

* At the moment of data processing in the information space (mailings from virus utilities).
* At the time of receiving new information.
* Regardless of the performance of information storage system (in the case of breaking ciphers or cryptographic protection of information).

**Methodology for security assessment**

The following methodology outline is put forward as the effective means in conducting security assessment.

* Requirement Study and Situation Analysis
* Security policy creation and update
* Document Review
* [Risk Analysis](https://en.wikipedia.org/wiki/Risk_Analysis)
* Vulnerability Scan
* [Data Analysis](https://en.wikipedia.org/wiki/Data_analysis)
* Report & Briefing

**How to Conduct an IT Security Risk Assessment**

1. Identify and catalog your **information** assets
2. Identify **threats**.
3. Identify vulnerabilities.
4. Analyze internal controls.
5. Determine the likelihood that an incident will occur.
6. **Assess** the impact a **threat** would have.
7. Prioritize the **risks** to your **information security**.
8. Design controls.

# Information Security Assessment Types

* **Vulnerability Assessments** are designed to find as many vulnerabilities as possible for the purpose of prioritizing remediation efforts. The output is a list of prioritized issues.
* **Penetration Tests** are designed to determine whether an attacker can achieve specific goals when facing your current security posture, such as stealing sensitive data or other activities that would harm the organization. The output is a report stating whether the goals were achieved or not, and any other observations that might have been made along the way. Penetration Tests do *not* provide a complete list of vulnerabilities or necessarily any prioritization of what was found; it’s mostly a yes or no for achieving the agreed-upon goals.
* **Red Teams** are are designed to continuously and effectively emulate an organization’s real-world attackers for the purpose of improving its defensive capabilties*.* Red Teams operate continuously, with near-full-scope and very limited restrictions, and constantly evolve their approaches to match and/or exceed the capabilities of the organization’s actual attackers.
* **Audits** are are designed to determine how a given organization measures against a given standard. Audits, as a rule, do not test security directly, but rather test compliance with a standard. The standard being tested against might have a strong or weak link to actual security, and should not be confused with a Vulnerability Assessment or Penetration Test. The output of an Audit is a list of areas that must be fixed in order to achieve compliance.
* **White/Grey/Black-box Assessments** are a measure of how much information is being provided to a security testing organization during an assessment. These can be internal, external, application-based, network-based, with or without exploitation, etc. The only consideration for $SHADE-box assessments is the amount of information being shared with the testing party.
* **Risk Assessments** are for determining the most important risks facing a given organization for the purposes of ensuring that they are brought within acceptable levels for the business. They can take many forms, but the output is always a list of prioritized risks followed by recommendations.
* **Threat Assessments** are for determining whether a given threat (often, but not necessarily, physical in nature) is worth spending limited resources on. Output is usually a recommendation of what—if any—amount of effort should be dedicated to the issue.
* **Threat Models** are for determining the various threats, threat scenarios, threat-actors, vulnerabilities, exploits, controls, and impacts that are related to a given system. They are ideally performed early and often during the creation process and can also be repeated after significant changes. Output often includes documentation of each of the above, along with residual risk after controls are considered, combined with recommendations for improvement.
* **Bug Bounties** are projects that leverage crowdsourcing for the discovery of vulnerabilities in a system. They are a tool in the vulnerability assessment toolbox. The techniques used by those participating in a bounty can vary widely, as can the type of system being tested. The important part is that instead of an internal team, or a particular set of contracted employees doing the work, it’s instead a large collection of independent researchers who all bring their own perspectives to the testing.

**A security assessment report should include the following information:**

* Introduction/background information
* Executive and Management summary
* Assessment scope and objectives
* Assumptions and limitations
* Methods and assessment tools used
* Current environment or system description with network diagrams, if any
* Security requirements
* Summary of findings and recommendations
* The general control review result
* The vulnerability test results
* Risk assessment results including identified assets, threats, vulnerabilities, impact and likelihood assessment, and the risk results analysis
* Recommended safeguards

**Five benefits of cyber security risk assessment**

* Identifies vulnerabilities. The risk **assessment** will help you identify risks and threats for your system, whether internal or external. ...
* **Security** requirements.
* Document **security**.
* Educates employees.
* Motivation increases.

**Criticisms and shortcomings**

IT security risk assessments like many risk assessments in IT, are not actually [quantitative](https://en.wikipedia.org/wiki/Numerical_data) and do not represent risk in any actuarially-sound manner. Measuring risk quantitatively can have a significant impact on prioritizing risks and getting investment approval.[[2]](https://en.wikipedia.org/wiki/Information_technology_security_assessment#cite_note-2)

Quantitative risk analysis has been applied to IT security in a major [US government](https://en.wikipedia.org/wiki/US_government) study in 2000. The Federal CIO Council commissioned a study of the $100 million IT security investment for the [Department of Veterans Affairs](https://en.wikipedia.org/wiki/United_States_Department_of_Veterans_Affairs) with results shown quantitatively.[[1]](https://web.archive.org/web/20040202203225/http:/www.cio.gov/documents/aie_report_final.pdf) United States Department of Veterans Affairs

**Professional certifications**

There are common vendor-neutral professional certifications for performing security assessment.

* [CISSP](https://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional)
* CCSP
* CISM
* CISA
* ISO/IEC 27001:2013 Auditor/Lead Auditor
* CRISC
* QSA/ISA

**There are common tools for automatic security assessment for self/third party usage.**

* Wireshark.
* Nessus.
* QualysGuard.
* Core Impact.

* Panorays
* RapidFire Tools
* Beyond Security
* Veracode
* RiskWatch