Security testing
Because every IT system is important

Security testing

You benefit a secure network and secure applications. We provide a range of services to help optimize your security. SQA delivers a customized solution for your ICT security needs.

1. Penetration testing

A penetration test is an investigation that determines if a system is vulnerable to attacks and assesses the potential impact of such attacks. It is a time-bound examination in which a security specialist, adopting a hacker mindset, uses all possible means and available information to approach the system, infiltrate it, and gather valuable information.

Verify security norms and standards

A penetration test primarily focuses on system infiltration, it is important to determine beforehand if this is the desired objective. If you want a complete understanding of all potential vulnerabilities that can be exploited in your systems, a vulnerability assessment is a more appropriate approach. This helps verify security standards and norms.

2. Vulnerability testing

Vulnerability testing: Applications and networks are vulnerable immediately after updates, as companies may not have the resources to fully test each new release in every project. Until the verification takes place, your system remains vulnerable. You can mitigate this risk by periodically scanning the systems.

Limit the risk of cyber attacks

A periodic automatic scan in addition to manual testing detects vulnerabilities that make your systems susceptible to viruses and other malware. It can also prevent your systems from missing patches and bugs in software from being resolved. A security specialist from SQA manually validates the results of an automatic scan to filter out false positives. If vulnerabilities are found, they are directly reported including advice on mitigating measures.

3. Compliance Audits

Through compliance audits, we assess your applications and infrastructure against a specific set of standards. This includes, for example, Payment Card Industry (PCI) compliance. Another example of a well-known framework is the Open Web Application Security Project (OWASP) for web applications.

Compliance with laws and regulations

We conduct compliance audits in conjunction with Vulnerability Testing and Detailed Security Assessment. This provides you with a comprehensive overview of any vulnerabilities that may result in non-compliance. Of course, we discuss the results with you and can advise you on any necessary repairs for the identified vulnerabilities.

We provide a customized solution for your ICT security needs

4. Infrastructure Testing

Given the importance of your infrastructure, we include it as a standard part of our vulnerability assessments. However, there may be reasons to exclude certain components. We will discuss which systems should be included in the assessment with you beforehand.

Prevent virus attacks

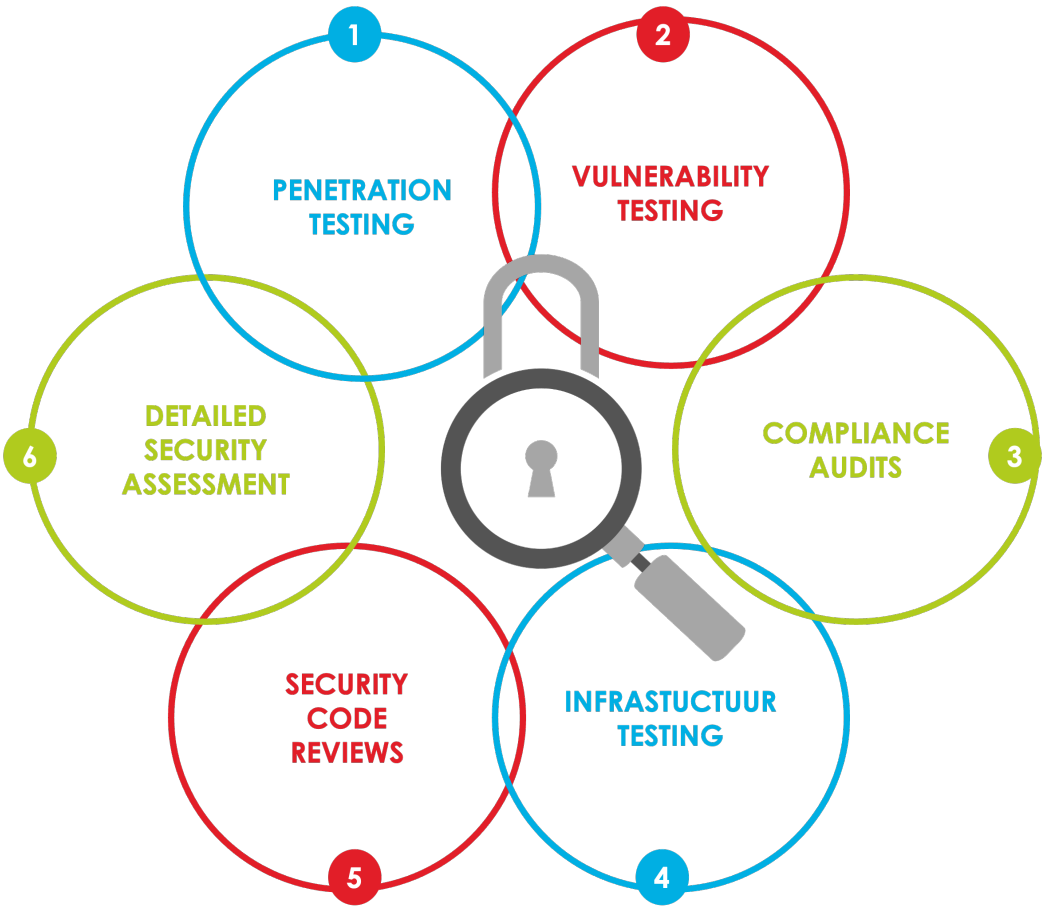
Not only applications, but also all servers and other infrastructure that you use, play a role in the security of an environment. Therefore, we thoroughly investigate these systems for possible vulnerabilities. We do this according to a predefined method so that we can provide a complete picture of the security of the systems within the scope of the test in a structured and reproducible manner. The investigation is carried out in a way that is not (extremely) burdensome for your servers and infrastructure. This means that we identify and verify vulnerabilities while your employees continue to work as usual. Their systems will not be negatively affected in terms of performance. In the event that systems unexpectedly react to our input, the test will be interrupted and we will take the predetermined actions. Additionally, we will advise you on measures you can take to address these vulnerabilities.

5. Security Code Reviews

Protecting the confidentiality of data and ensuring the availability of your web applications begins with secure development. It is wise to pay attention to (code) security early in this process. We can help you with this by conducting code reviews at various stages of the project.

Security from the sourcecode

A code review is a comprehensive inspection of the source code in which the security specialist specifically looks for vulnerabilities within the components that may contain potential weak points. We provide direct feedback to the developers on the findings. We also explain how any vulnerabilities can be resolved and suggest improvements. The result of this approach is that the involved developers gain more insight into the security of the systems and can use it throughout the entire project. By integrating security sufficiently from the beginning, you can prevent many problems. The likelihood of finding many vulnerabilities during a manual inspection (often performed at the end of the process) is significantly reduced. Releases also experience less delay. Conducting code reviews not only benefits security but also the progress of the project.



6. Detailed Security Assessment

In order to properly screen your systems, applications, and infrastructure against hackers and other malicious individuals, it is important to thoroughly examine them for vulnerabilities. An efficient method for this is a detailed security assessment based on (predefined) checklists. This allows us to provide a comprehensive view of the security of all utilized systems in a structured and reproducible manner.

This research can take place at different levels, depending on the scope and risk analysis that we determine together with you. You can choose an approach where we primarily check for common vulnerabilities that can be easily exploited and have a significant impact. Or you can opt for a more comprehensive investigation in which we also look for complex vulnerabilities that can only be exploited by a cybercriminal with more motivation and knowledge. An important part of such a comprehensive investigation is the identification of defense-in-depth items. These are measures that you can take to ensure a higher level of security. A detailed security assessment (DSA) is different from a pen-test because the latter is often carried out with the sole purpose of demonstrating that the security can be breached. With our approach, we identify as many vulnerabilities as possible that an attacker could use for a targeted attack. The DSA can be tailored to comply with audit guidelines or meet certain standards, such as OWASP, NCSC, or DigiD.

sqa TEST US

SQA provides a customized solution for your ICT security needs

We provide insights into vulnerabilities and security risks. With the help of our services and solutions, we can detect threats at an early stage before they can cause damage. This makes our clients resilient against digital threats and prepared for the future.

www.sqacaribbean.com