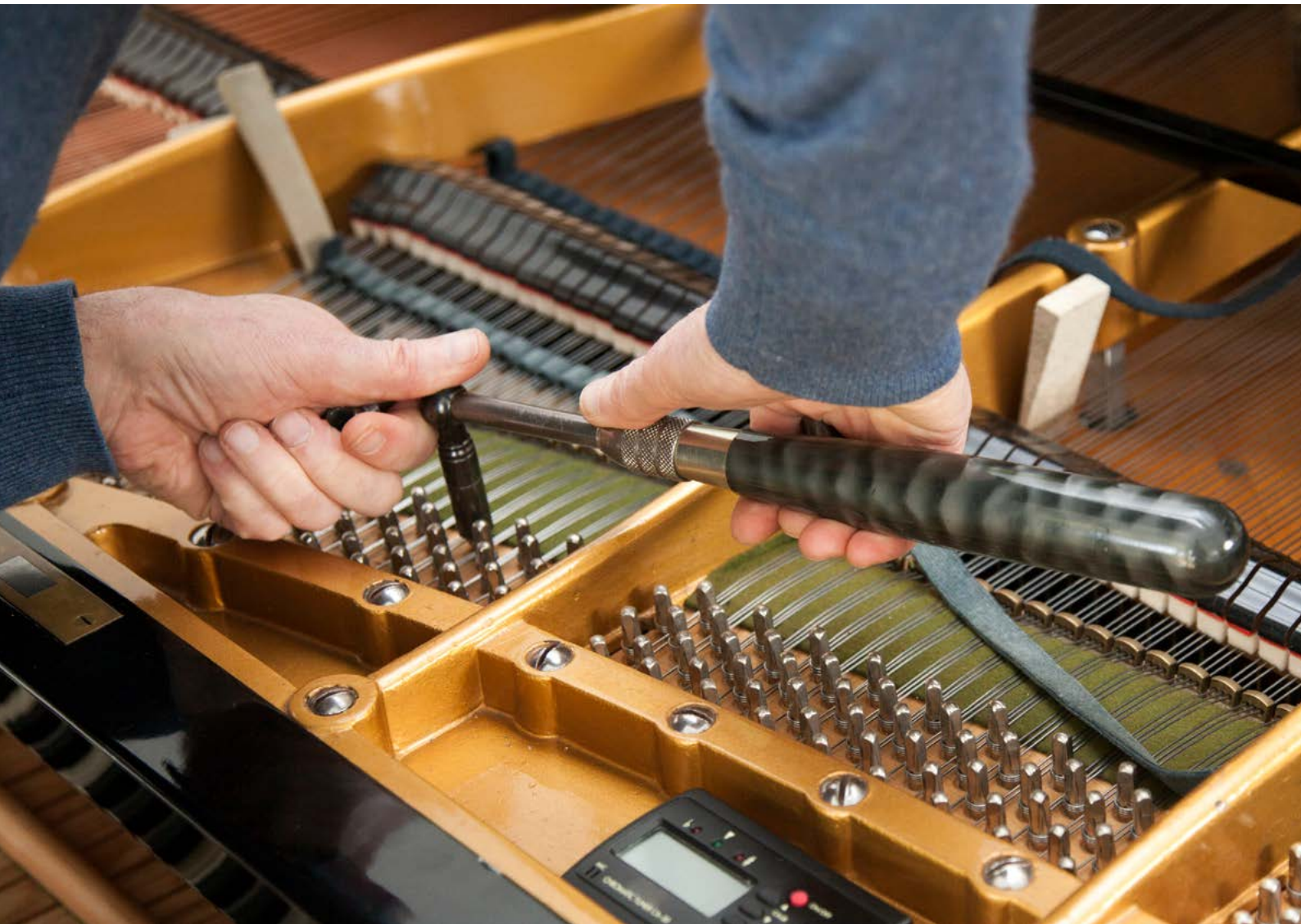
National Cyber Security Centre
Ministry of Justice and Security

Security testing White Paper



The National Cyber Security Centre (NCSC) works with the business community, government bodies and academics to increase the ability of Dutch society to defend itself in the digital domain.

The following parties made a substantial contribution to the quality of this white paper:

- BDO
- Capgemini
- Deloitte
- Directorate-General for Public Works and Water Management
- Employee Insurance Agency
- Fox-IT
- Information Security Service for Dutch Municipalities
- Logius
- Ministry of Economic Affairs and Climate Policy
- Ministry of Foreign Affairs
- Ministry of Justice and Security
- National Audit Service
- National Police
- OWASP
- Port of Amsterdam
- PwC
- Radically Open Security
- Secura
- Securify
- Software Improvement Group
- Sogeti
- Tax and Customs Administration

Table of contents

Introduction

Almost all organisations make use of IT for the vast part of their business processes. It stands to reason, then, that the reliability of information systems is crucial to the smooth operation of organisations. In addition, many organisations process sensitive information belonging to or on behalf of other parties. Organisations have a moral, social and in some cases legal obligation to manage this task in a responsible manner. Adequate security measures contribute to the reliability of services and business operations. Security testing is one of these measures. It contributes to compliance with the multitude of security and privacy regulations. Security testing provides insight into the vulnerabilities, and therefore the risks, of an information system. This is useful information for any organisation. It will allow organisations to become better at applying the right security measures to make themselves more resilient.

This is a manual for parties that commission security testing

Proper terms of reference and adequate management of the performance of a security test will yield results that meet the commissioning party's objectives.

In the best-case scenario, security tests do not lead to major surprises, but confirm the quality of the development process. Checking something only after it is complete to see whether it happens to be secure often results in unpleasant surprises and delays. As a general rule, the sooner a security issue is discovered during development, the easier and cheaper it is to remedy.[1]

In other words, rather than allowing your security test to compensate for the lack of adequate focus on security during development, you should use it as a means to obtain a certain level of certainty, to learn and to improve it further.

You are the commissioning party

This White Paper is intended as a guide for the security testing of information systems that are in use or are about to be deployed. There are a number of situations in which a security test may be called for:

- A security officer wants to gain insight into the vulnerabilities of the IT environment.
- A project manager wants to test the security level of an information system and understand the extent to which security requirements have been met.
- A delivery manager wants to demonstrate that the delivered product or service is capable of withstanding certain threats.
- An application owner wants to prove that an application is free from known vulnerabilities.
- A product manager wants to have the source code of a product tested for vulnerabilities.

You require a security test that is appropriate for your information system.

This White Paper focuses on the process of organising an appropriate security test and how to manage this successfully. This depends on your specific situation and the various ways in which the current security level of an information system can be tested.

Figure 1 provides an overview of the phases of the development process of an information system. Although the total process is more elaborate, it has been roughly divided into three phases for the sake of the interpretation and application of the White Paper: definition, development and deployment. Different forms of security testing apply in each of these phases. In this White Paper, the focus is on the security testing of information systems that are in use or are about to be deployed.

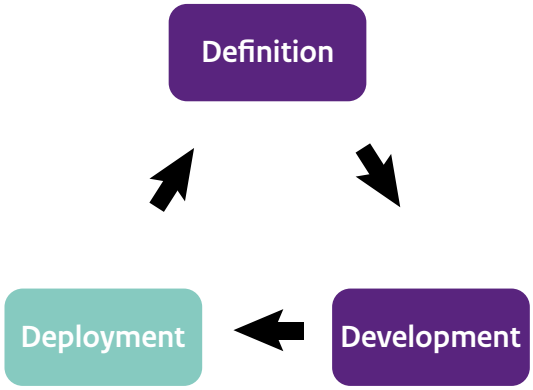
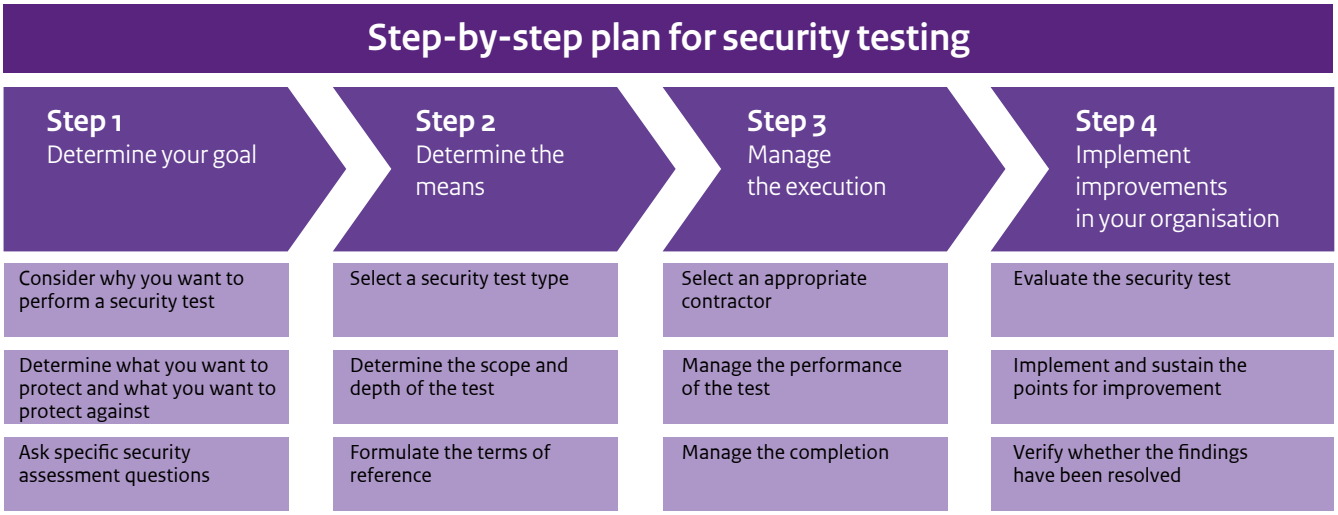


Figure 1. Life cycle of an information system

The security tests described in this White Paper are applicable to information systems. Businesses processes and human actions may also be flawed. Security tests that focus on these aspects of the organisation fall outside of the scope of this White Paper.

[1] See https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beleids--en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software

Proceed as follows



- **Step 1: Determine your goal**
  Determine what you want to protect, what you want to protect against and what insights you want to gain.

- **Step 2: Determine the means**
  Determine the type of security test and options that best suit your situation and objective. Use these as input to formulate the terms of reference for the potential contractor.

- **Step 3: Manage the execution**
  Determine the criteria that are most important for your organisation and security test when selecting a contractor and manage the execution of the test.

- **Step 4: Implement improvements in your organisation**
  Perform an internal evaluation by involving the responsible persons and ensure that the proposed improvements are implemented and sustained.

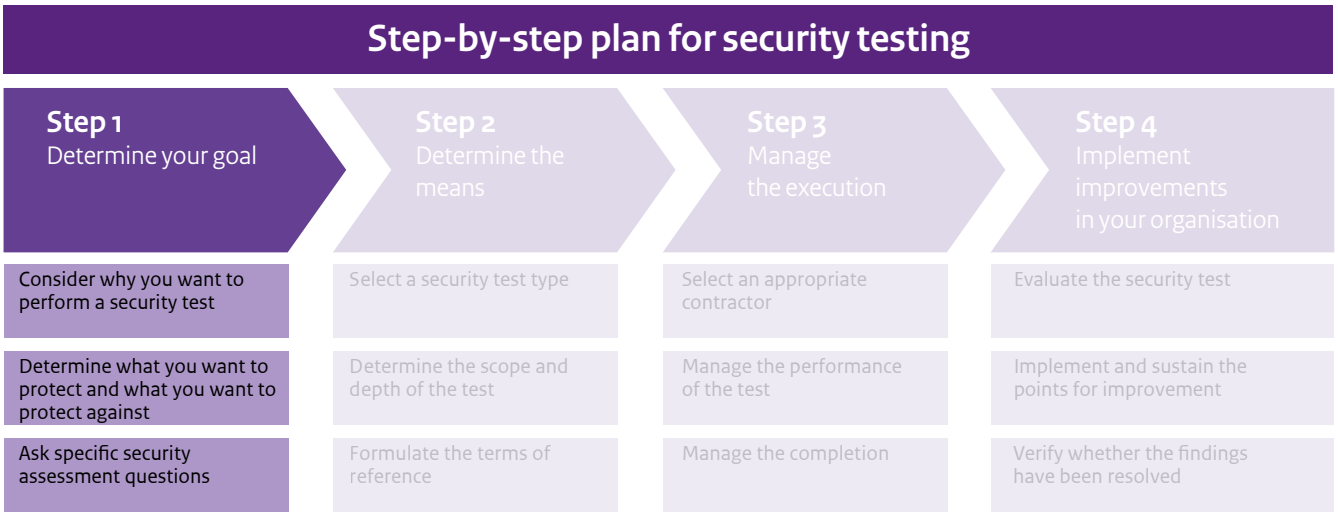
You have to carry out various preparatory activities in order to derive the most added value from a security test. This will prepare you for the subsequent steps, such as inviting tenders, coordinating with a contractor, performing the test and ensuring that the improvements are implemented and sustained in your organisation.

Step

1

Step 1 Determine your goal

Step 1 is about determining what you want to achieve via a security test. Here, we will discuss your motivation, what it is you want to protect, what you want to protect against, and the insights you want to gain to this end. In the following steps, we will discuss how you can achieve your objective. The three points for attention shown below can help you finalise the objective of the test.



1.1 Consider why you want to perform a security test

The reason for organising a security test is often related to the security policy, for example, if major changes occur in the IT infrastructure or if there is a need to store and process certain types of sensitive information. Other reasons may be that the organisation is looking for certainty regarding the continuity of services, for something that will help differentiate the organisation positively from competitors, or for confirmation that a purchased product is resistant to misuse. In addition, organisations have adopted numerous security standards[2], which often require some form of periodic security testing.

Legislation and regulations may also be reasons to perform a security test. Examples include the Network and Information Systems Security Directive (NIS Directive)[3] concerning the duty to maintain critical infrastructure and report vulnerabilities; the use of DigiD[4] as an authentication tool by organisations; the GDPR,[5] which requires organisations to obtain a certain level of certainty regarding whether appropriate security measures have been taken; and the Government Information Security Baseline (*Baseline Informatiebeveiliging Overheid*, BIO)[6] for government bodies.

[2] See https://www.wodc.nl/onderzoeksdatabase/2552-inventarisatie-van-standaarden-en-normen-voor-cyber-security.aspx
[3] See https://www.nctv.nl/onderwerpen wet-beveiliging-netwerk--en-informatiesystemen
[4] See https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/
[5] See https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg
[6] See https://www.communicatierijk.nl/vakkennis/r/rijkswebsites/verplichte-richtlijnen/baseline-informatiebeveiliging-rijksdienst

1.2 Determine what you want to protect and what you want to protect against

Make sure you ask the right questions beforehand, as to communicate the terms of reference to the contractor in a clear and concrete manner.

- Which data do you want to protect?
- What level of protection do you need?
- What types of scenarios do you want to protect against and what is the extent of the protection you are looking for?
- Does the emphasis lie on availability, integrity, confidentiality or a combination of these?
- Is it only about infrastructure and application, or is there a need to also include the organisational aspects in the testing?

Risk analysis and threat modelling are two activities that form the basis for understanding what you want to protect, what you want to protect against and why. The quality of the results of the risk analysis and threat modelling is largely determined by the expertise of those who carry out these activities. It is also important to involve the right interested parties. Involving experts from the commissioning party's side helps minimise the know-ledge asymmetry that is often present in such situations, so that a fruitful discussion can be carried out with the contractor. This will ultimately contribute to getting the right answers to the right questions.

When you request a security test, describing this test in overly general terms often leads to confusion. In the case of a penetration test, for instance, an attacker may try to gain access in a variety of ways. You should therefore be specific when it

comes to defining your terms of reference. For example: 'I want to test whether a malicious employee could access data other than their own data.' Since the time available to carry out a test is often limited, it is important to perform the tests that are appropriate for the specific concerns related to the interests that need to be protected.

1.3 Ask specific security assessment questions

Clearly indicate in advance which insights you expect to gain as a result of the test, so that the right resources can be identified for the security test. Sometimes, the security assessment questions are formulated too abstractly, such as 'Can the system be hacked?'. It is worth noting that, given sufficient time and resources, all systems can be hacked. If the assessment question or the scope is too vague or too broad, the test is likely to yield too much information, so that the results that are most relevant get buried underneath the excess of information.

You should therefore be specific when defining the desired results and associated scope. Determine the required results on the basis of the business case and translate them into specific security assessment questions. This will allow for targeted testing.

Examples of required results	Examples of specific security assessment questions
Insight into the effectiveness of IT monitoring measures	How can unauthorised persons gain access to specific company data?
Insight into security awareness levels	To what extent are employees aware of the risks of a phishing attack? To what extent is the organisation vulnerable to this type of attack?
Discovering your low hanging fruit	What kind of information and vulnerabilities of a specific system can be exploited by unauthorised persons?
Learning opportunity for developers	What can the developers learn about how to make certain security improvements based on the findings?
Insight into a system's security level	What is my level of resilience to certain threats? Am I vulnerable to a certain threat, such as a ransomware attack?

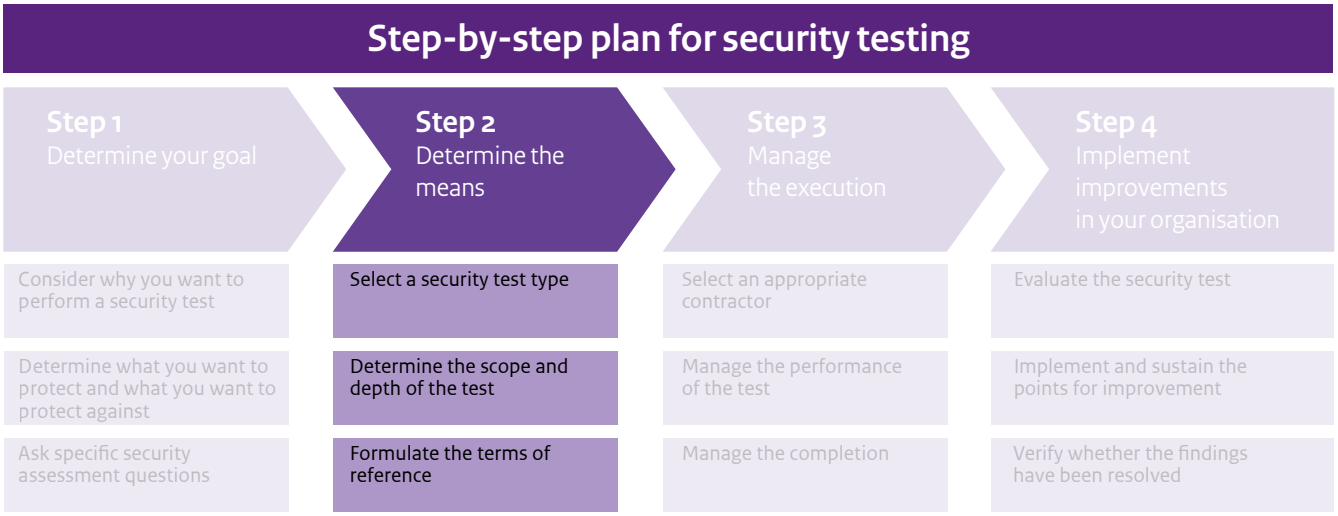
Table 1. Commonly desired insights as results

Step

2

Step 2 Determine the means

Now that you have contextualised your goal, it is important to select an appropriate security test. To this end, you should create a security testing profile based on which you can draw up terms of reference for the contractor.



2.1 Select a security test type

Different service providers may use different terminology to distinguish between security test types. This White Paper uses the terminology in the Cyber Security Dictionary.[7]

Due to the limited scope of this White Paper, the test types for physical access, social engineering, coordinated vulnerability disclosure, bug bounty and red teaming are not discussed.[8]

2.1.1 A vulnerability assessment is broad

You use a vulnerability assessment scan to perform a test that is as broad as possible. The scan detects missing patches and known vulnerabilities, weak security configurations such as default passwords or insufficient encryption, unsecured network service parameters, common web application issues or data breaches.

Vulnerability assessments[9] are used to test for known vulnerabilities in a broad-based manner. The security tester indicates that a vulnerability has been detected, but does not actually misuse this security omission and does not attempt to penetrate further into the systems. This is useful when speed is of the essence, or when highly critical objects are being examined and one does not wish to go further than surface testing to avoid any unpredictable and consequential damage resulting from, for example, the use of outdated technology.

2.1.2 A penetration test is deep

A penetration test is an in-depth analysis, rather than a broad assessment. In a penetration test (also known as a 'pen test'), a trained pen tester will look for vulnerabilities and try to exploit them using various tools and manual procedures, depending on the agreed security assessment questions and scope. Based on this, the commissioning party can gain insight into how difficult it is to actually do any harm by exploiting the detected vulnerability.

In some cases, a pen test only adds greater value if the vulnerability assessment and the process for resolving findings have been set up and are being used within the organisation.[10] If an organisation has not yet carried out a vulnerability assessment and resolved the findings, a pen test will be less effective because it will detect many vulnerabilities that could have been detected more easily, i.e. by a vulnerability assessment. As a result, time will be lost that could have been used to search for vulnerabilities that are harder to find.

If a commissioning party wants to gain a better understanding of the way in which these types of tests are carried out, it can look into the various pen test methodologies compiled by, for example, OWASP.[11] Other details and advice on how to get the most out of penetration tests have also been set out by NCSC-UK.[12]

[7] See https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/

[8] The NCSC has published a guideline for coordinated vulnerability disclosure; see https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad. For other test types, see https://en.wikipedia.org/wiki/Social_engineering_(security) and https://www.darkreading.com/threat-intelligence/think-like-an-attacker-how-a-red-team-operates/d/d-id/1332861

[9] See http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Vulnerability-Assessment.aspx

[10] See CIS Control 20: Procedures and Resources: https://www.cisecurity.org/controls/cis-controls-list/

[11] See https://www.owasp.org/index.php/Penetration_testing_methodologies

[12] See https://www.ncsc.gov.uk/guidance/penetration-testing

2.1.3 A source code review is thorough

A source code review is an inspection of the application source code by an expert. The purpose of a source code review is to detect vulnerabilities in the source code. It is a systematic review for programming errors that were possibly overlooked during development. This security test is relevant not only during the development phase, but also during the deployment and management phases, since practical experience shows that the source code is never completely error-free when it is deployed. Errors are always still found afterwards; see for example the items in the OWASP Top 10 of high-risk vulnerabilities in web[13] and mobile applications.[14]

A proper source code review requires specific knowledge and skills in the applied programming languages, frameworks, external components and dependencies. Automated static analyses, composition analyses and manual reviews are often part of a source code review.

2.2 Determine the scope and depth of the test

In addition to the types of security tests that fit a certain maturity level, there are also a number of options for determining the breadth and depth of the test, which help in providing a context for the terms of reference.

2.2.1 Determine the scope of the test

For effective security testing, it is important to clearly establish the scope of the information system to be tested. This is to ensure both the completeness of the expected test results and the avoidance of unnecessary testing activities.

Inputs from the system owner, the architect, the technical specialist and the security specialist are necessary for indicating the dependencies between the components. Also indicate what is not included in the scope of the test, so that the testers do not make any false assumptions.

- **External infrastructure**
  This includes infrastructure (IP ranges, VPN, firewalls) that is available via the internet. Any malicious party can gain access to this.
- **Internal infrastructure**
  This includes infrastructure located behind the protective layer of, for example, a VPN or firewall. This is also relevant for inclusion in the testing scope, in order to apply the defence-in-depth concept. Once a malicious party has succeeded in penetrating the VPN or firewall, how far can the malicious party penetrate into the network and what can the system owner do to prevent this? The same approach applies to a dissatisfied employee with intent to cause damage.
- **Application**
  An application is any source code combination designed to carry out a task, such as a web application, script, mobile application or special programme.
- **Organisation**
  The organisation is the set of people and processes brought together to achieve the organisation's objective. Malicious parties can manipulate people in order to influence their actions or circumvent processes. This is known as social engineering.

2.2.2 Determine the level of penetration

Another variable is how far a security tester is allowed to penetrate, i.e. the level of penetration. This should be agreed clearly in advance. To a certain extent, the level of penetration is inherent to the choice between a vulnerability assessment and a penetration test. In a vulnerability assessment, a tester shows that he or she has been able to detect a vulnerability by using a simple approach; in general, no further attempts are made to penetrate into the systems. In a pen test, in addition to finding vulnerabilities, a tester will also try to exploit them, as an attacker would. Based on this, the commissioning party can find out how difficult it is to actually do any harm by exploiting the detected vulnerability. Nevertheless, you should come to specific agreements with the contractor regardless of the security test type.

2.2.3 Determine how much information to provide to the security testers in advance

The commissioning party may choose to provide the testers with information prior to the test, depending on the perspective from which the test needs to be performed. The following terms are used in this regard:

- **Black box**
  No prior information is provided; the tester knows nothing except, for example, an IP address, domain name or company name. This is often more realistic in terms of the information that a real attacker would have access to, except that, in practice, an attacker has much more time and can therefore gain access to more information. OSINT (Open Source Intelligence, publicly available information via, for example, the internet) is an important source of information for the tester.
- **Grey box**
  The tester is provided with partial information in advance, such as the login data of a user with a certain role within the system, so that it is possible to test what an attacker with certain rights in a system can achieve. Another example is giving a tester access to a building to test how far he can get once the first protective layer, i.e. the physical measures, has been breached.
- **White box**
  The tester receives all the information in advance, such as design documentation, login data, sample messages and source

[13] See https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[14] See https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks

code (even if no source code review is carried out). The terms 'crystal box' and 'white box' are interchangeable. A white box test allows for more efficient testing within the available time. This type of test involves information that is not usually public, such as the source code. However, such tests do not guarantee a thorough code review. It is possible that the code will be mainly used for guiding a pen test. If the aim is to also conduct a code review, it is important that a specialised code reviewer is involved in the test and that the programming relevant for security is assessed in a structured manner. In practice, penetration tests and code reviews are usually performed by different specialists.

2.2.4 Determine the depth of the security test

The depth of a security test varies from one test type to another. A vulnerability assessment is relatively superficial and simple, and requires less effort and a lower level of expertise than a penetration test and source code review do, but results in numerous, potentially incorrect findings if the results are not verified manually. A penetration test is more in-depth and requires more effort, creativity, perseverance and a higher level of expertise in order to detect less common vulnerabilities and gain access via one or more stepping stones. A source code review goes deepest, because it inspects the basic foundations of an application. When it comes to depth, you can come to specific agreements with the contractor regardless of the security test type.

2.3 Formulate the terms of reference

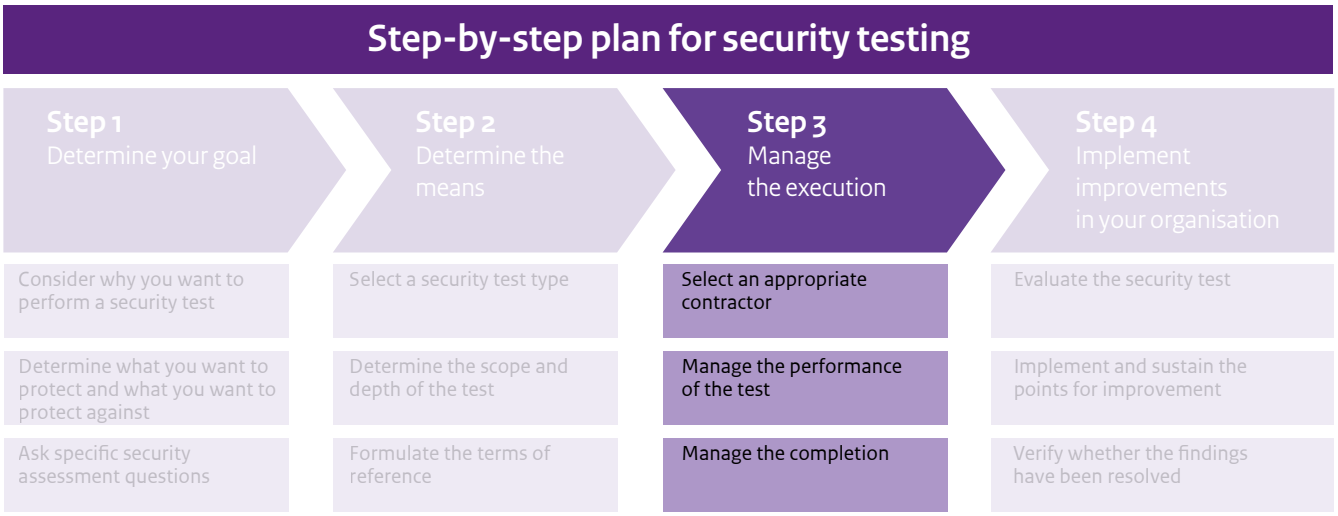
Use the results obtained in Steps 1 and 2 to create a security testing profile. This will serve as input for the terms of reference. Elaborate the previously defined security assessment questions to determine the most suitable security test for obtaining the right answers. Use the security testing profile in Appendix A to compile the terms of reference with which to invite tenders.

Step

3

Step 3 Manage the execution

This step examines the selection of an appropriate contractor for the security test in greater detail. You can steer the process towards a satisfactory completion by ensuring that clear agreements are made. The three points for attention shown below can help you do this.



3.1 Select an appropriate contractor

You have created an initial draft of the terms of reference for the security test. Use this as a basis for finding a match with a contractor. Define criteria regarding the topics that matter to you most in order to ensure that the contractor meets your needs. The internal or external contractor will have to meet most of these criteria, but the fit between you is ultimately most important. You have to make agreements and communicate with one another and trust each other to get the desired results. This works best when the commissioning party and contractor are able to communicate openly and transparently with one another.

3.1.1 Draw up a shortlist

What are the best criteria for comparing parties that carry out security tests? Since it concerns security and therefore sensitive matters, it is important to carefully consider which contractors are eligible. Prepare yourself better for the selection process by considering indicators such as reliability, quality and accessibility, ranked by you in order of priority. This will help you draw up a shortlist.

Reliability
- Relationship of trust
- Protection of test data

Quality
- Solid reputation, history and ethics
- Skilled security testers, references and experience with technologies or measures to be tested
- High quality of service, added value
- Knowledge of your industry or organisation
- Research & development capabilities
- Sample reports

Accessibility
- Availability of testers and flexibility
- Open and transparent form of communication

3.1.2 Remain in contact with potential contractors

Once you have drawn up a shortlist, you should remain in contact with potential contractors throughout the selection process. The initial terms of reference prepared at the end of Step 2 form a solid basis for what you expect from the security test. By keeping in touch with the contractor, you increase the chance of getting what you need. Matters that often require further explanation are the scope, prioritisation, budgeting and whether the parties involved are aware of the testing activities.

3.1.3 Conduct an intake

The main objective of the intake is to collect all the required information, so that the contractor can prepare its proposal (offer or action plan). The intake must be of a high quality and involve the commissioning party and contractor jointly determining which testing activities are required based on the risks and threats.

However, before an intake can take place with a potential contractor, a number of preconditions must be met because of the sensitivity of the information involved in a security test.

- a non-disclosure agreement between the parties as a measure against the leakage of sensitive information;
- an agreement and decision on how findings that are eligible for coordinated vulnerability disclosure (CVD) will be dealt;
- an agreement on protocols for secure communication, storage and deletion of data and dissemination of reports, so that information and discussions regarding the test do not become public.

Once the conditions for exchanging the information for the security test have been agreed, an appointment can be scheduled for the intake. Because of the sensitivity of the information to be shared, this is best conducted face-to-face. In addition, a face-to-face intake helps build a relationship of trust with the contractor and helps prevent erroneous assumptions.

To avoid any surprises, you could consider getting to know the actual testers during the intake or in follow-up discussions. The aim is to prevent a situation where a certain tester is proposed in the offer, but the test is ultimately performed by another tester who does not meet the desired profile.

Ensure that you have sufficient in-house knowledge or obtain this knowledge from outside in order to properly organise a security test. The right knowledge will allow you to conduct a risk analysis, formulate terms of reference, maintain overall control and assess the test report. If this knowledge is lacking, compensatory measures must be taken. Such measures should be taken independently of the contractor to prevent any conflicts of interest. Consider consulting a third party for advice.

During the intake, clarify and record the following points for attention:
- Discussion regarding the prepared security testing profile and initial terms of reference by the commissioning party
- Discussion regarding the assignment and explanation of how the contractor works
- Clear explanation of what is and is not included in the scope
- Prioritisation of focus areas during testing
- Confirmation of the parties involved and the required approvals in case any components fall outside the responsibility of the commissioning party
- Explanation of the risk analysis and development of the threat modelling with further input from the contractor
- Clarification of the reason, objective, intended results and specific security assessment questions
- The contractor's action plan
- Scheduling, budget and method of delivery
- Possible follow-up and scheduling of a retest

The intake also gives contractors the opportunity to discuss in greater detail the commissioning party's expectations, as well as the scope of the information system to be tested. This will help in preparing the final offer for the test. Asking further questions often brings additional information to the fore. Otherwise, there may be confusion afterwards regarding issues such as ownership, scope and dependencies. If the intake is satisfactory and an agreement is reached, it is important that these agreements are clearly included in the contract.

3.1.4 Prepare a healthy contract

A healthy contract is one that sets out all the essential elements that, if omitted, could lead to confusion. This allows the commissioning party to properly manage the performance of the test. The following contract ingredients help define clear rules to be followed before, during and after the test:
- The agreed terms of reference
- Contact persons and how they can be reached (in case of emergency)
- Involvement of third parties and the process of coordination with these parties
- The method of reporting and the persons to whom the report will be provided
- Conditions, agreements and responsibilities
- Permitted resources and when they may be used
- How the permitted resources can be recognised
- As indicated by the contractor, in advance and in sufficient detail, the tests that it will perform, along with a detailed report of the results and the factors taken into consideration for the report
- A log in which the contractor keeps track of the activities carried out and the time they were carried out, so that any unforeseen effects can be traced
- Adequate processes demonstrably set up by the contractor, such as the encryption, archiving and deletion of data, to prevent unauthorised parties from accessing the test results
- Assessment of the equipment that the contractor brings into contact with the commissioning party's systems with regard to any risks for the commissioning party, such as equipment that is used in insecure third-party environments
- A clear distinction between the tasks and responsibilities of the contractor and the commissioning party, where the considerations from the business perspective must be managed by the commissioning party
- Quality criteria for reports, including:
  - report on findings;
  - explanation of applied test methodology;
  - description of how findings were made;
  - reproducibility of findings;
  - technical findings;
  - procedural findings;
  - business impact of findings;
  - risk descriptions;
  - recommendations;
  - conclusion;
  - executive summary.

Appendix B contains a checklist for elements to be included in the contracts.

3.2 Manage the execution of the test

A thorough preparation ensures that tests do not have to be postponed and that the expected results are achieved. Facilitating testers in the right manner creates the preconditions for a proper execution of the test.

3.2.1 Prepare for the execution of the test

If the commissioning party pays attention to a number of points during preparation, this could have a major positive impact on the test.

- Method of validation and classification of findings
- Testing of authorisations (with and without test accounts, black box, grey box or white box)
- Login details
- Monitoring of attack attempts
- Permission for:
  - brute force attacks (or, for example, only offline);
  - tests that can lead to denial of service (service disruption);
  - tests performed in the production or acceptance environment.
- Whitelisting of testers, i.e. allowing certain traffic flows initiated by the testers[15]
- How to deal with scope changes during the test: if changes are made in scope during the test based on new insights, it may appear afterwards that the test no longer fully covers the previously agreed scope
- Clarity regarding the need for a retest (this should take place within a foreseeable period of time after agreement on findings
- Signing of an indemnity agreement with the parties involved
- Rules of Engagement (rules for the test)
- Intake form
- Agreements on how to deal with the findings regarding:
  - closed-source code;
  - open-source code.
- Agreements on how to deal with the obtained documents and, for example, the source code
- Documentation to be provided (for example, whether or not to include the raw output of tools)
- Preliminary test/sanity check to verify that everything is actually ready for testing (for example, whether the test environment is externally accessible)

3.2.2 Facilitate the execution of the test

If the commissioning party pays attention to a number of points during facilitation, this could have a major positive impact on the test.

- Appoint a security test supervisor, for example to assist the testers on location.
- Make agreements on communication:
  - prior to the security test;
  - during the security test;
  - after the security test.
- Inform the system and network administrators involved.
- Make sure that the right environments are available during the test and that other activities, such as major modifications, backup and restore actions or other tests that may influence the results, do not take place at the same time as the security test.
- Ensure that suitable workspaces with network connections are set up for the contractor.

3.2.3 Ensure direct and prompt communication with the contractor

By communicating directly and promptly with the contractor during the test, you ensure that issues can be clarified quickly. For example, this will help reduce the need for workarounds due to unforeseen circumstances and prevent unnecessary delays.

- Provide frequent updates on findings and progress via, for example, a brief daily stand-up meeting.
- Make direct contact in case of findings that require urgent action.
- Coordinate priorities if more time is being spent on a particular priority at the expense of the others.
- Agree on any scope changes during testing in a timely manner.
- Allow administrators or developers to participate in the performance of the security test, so that they can learn from it.

3.3 Manage the completion

Engage the correct parties involved in a timely manner, not only at the start of the security test, but also when the moment of completion approaches. To establish a clear overview of the internal or external responsibilities assigned for specific findings, it is helpful to agree on an appropriate form of completion (for example, a face-to-face meeting to discuss the findings) so that questions can be answered and other uncertainties clarified before the test is definitively completed.

[15] In case of vulnerability assessments and penetration tests, testers are often unaware of the location of defence layers, such as a firewall or IDS, that block attacks. If it was agreed in Step 2 that these defence layers fall outside of the scope of the test, it would be unnecessarily time-consuming to circumvent or shut these off during the test.

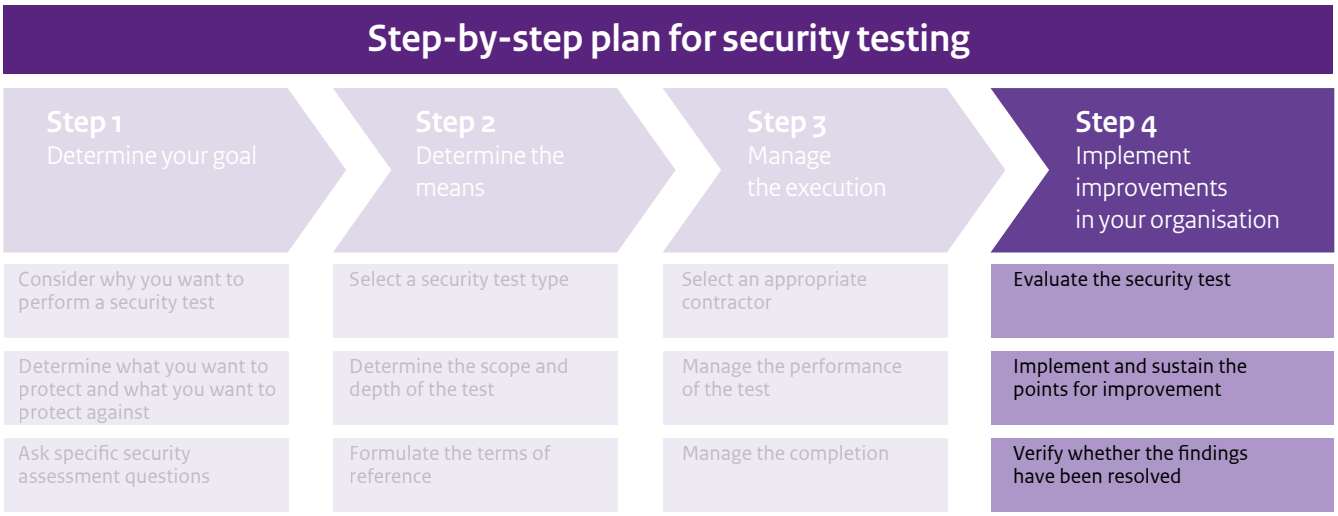
Step

4


TU/e
Technische Universiteit
Eindhoven
University of Technology
WIND TUNNEL

Step 4 Implement improvements in your organisation

Once the security test has been completed and the results have been handed over, it is important to implement and sustain the proposed improvements in your organisation, so that the same mistakes are not repeated in other parts of the organisation and the same improvements can potentially be applied elsewhere. The three points for attention shown below can help you do this.



4.1 Evaluate the security test

Schedule an evaluation with the parties involved within a short period of receiving the results, so that the momentum created by the security test can be optimally exploited. If too long a period elapses before an evaluation, there is a risk that nothing will be done with the results because this will be overshadowed by other priorities in the daily activities of the persons involved. The internal evaluation should include the following elements, so that the organisation can learn from the evaluation.

4.1.1 Evaluate the results

Once the results have been handed over, the persons involved should be clearly aware of the impact of the technical findings on the business, the estimated effort required to resolve the findings and the possible underlying causes of the findings. The following points should be included in the evaluation:

- Do the results conform to agreements regarding quality (depth, argumentation, proof)?
- Are the results a surprise for the organisation? Which conclusions can be drawn from the findings and underlying causes?
- Book a session with the internal party involved and the contractor to discuss the security test, so that all the findings are completely clear to those involved and any issues that may arise can be clarified. Moreover, this will encourage those involved in the internal organisation to read through the report properly in advance.

4.1.2 Evaluate the process of organising the security test

The process of organising the security test that has just taken place should also be evaluated. What are the aspects that went well? What aspects could be improved? Should the project plan be adjusted ahead of the next test?

4.1.3 Evaluate the contractor

Carry out an internal evaluation with the parties involved regarding the performance of the contractor. By discussing the completed evaluation with the contractor, both organisations can improve their processes.

4.2 Implement and sustain the points for improvement

It is beneficial for the organisation to define clear points for improvement for the different areas of responsibility within the organisation. These points for improvement could apply to infrastructure, applications or the organisation itself, but also to outsourced components. Therefore, clearly indicate the components of the information system to which the findings apply and the parties responsible for this. If other parties are accountable for findings that apply to components, it must be ensured that these findings are properly communicated and assigned to these parties and that the handling of the findings is monitored. This can only be effective if a protocol is established for processing the findings and improvements emerging from the security tests.

The organisation must be prepared to take action and responsibility on the basis of the findings. Do the organisation's employees have the right skills to address these?

Record the findings from security test reports in, for example, service management packages already in use by the organisation. This can also be done to ensure that the action points are implemented and that the same test does not produce the same findings next time.

4.2.1 Implement short-term points of improvement straight away

Depending on the applied classifications and assigned priorities, you should implement short-term points for improvement without delay. Determine which findings require immediate action and whether they require internal communication or escalation. Monitor the progress of the implementation of solutions.

4.2.2 Schedule long-term points for improvement

To avoid losing sight of long-term points for improvement, you can set deadlines for action items. Inform the parties involved when a deadline for implementing a solution is about to expire.

4.2.3 Seek synergies with the overarching risk management process

Improvements can be optimally implemented and sustained within the organisation by linking them to an overarching risk management process and a risk register. This will also allow you record how the organisation deals with any residual risk if a recommendation is not followed or only implemented partially.

4.3 Verify whether the findings have been resolved

You can schedule a retest to verify that a proposed improvement has actually been implemented.

4.3.1 Schedule the retest

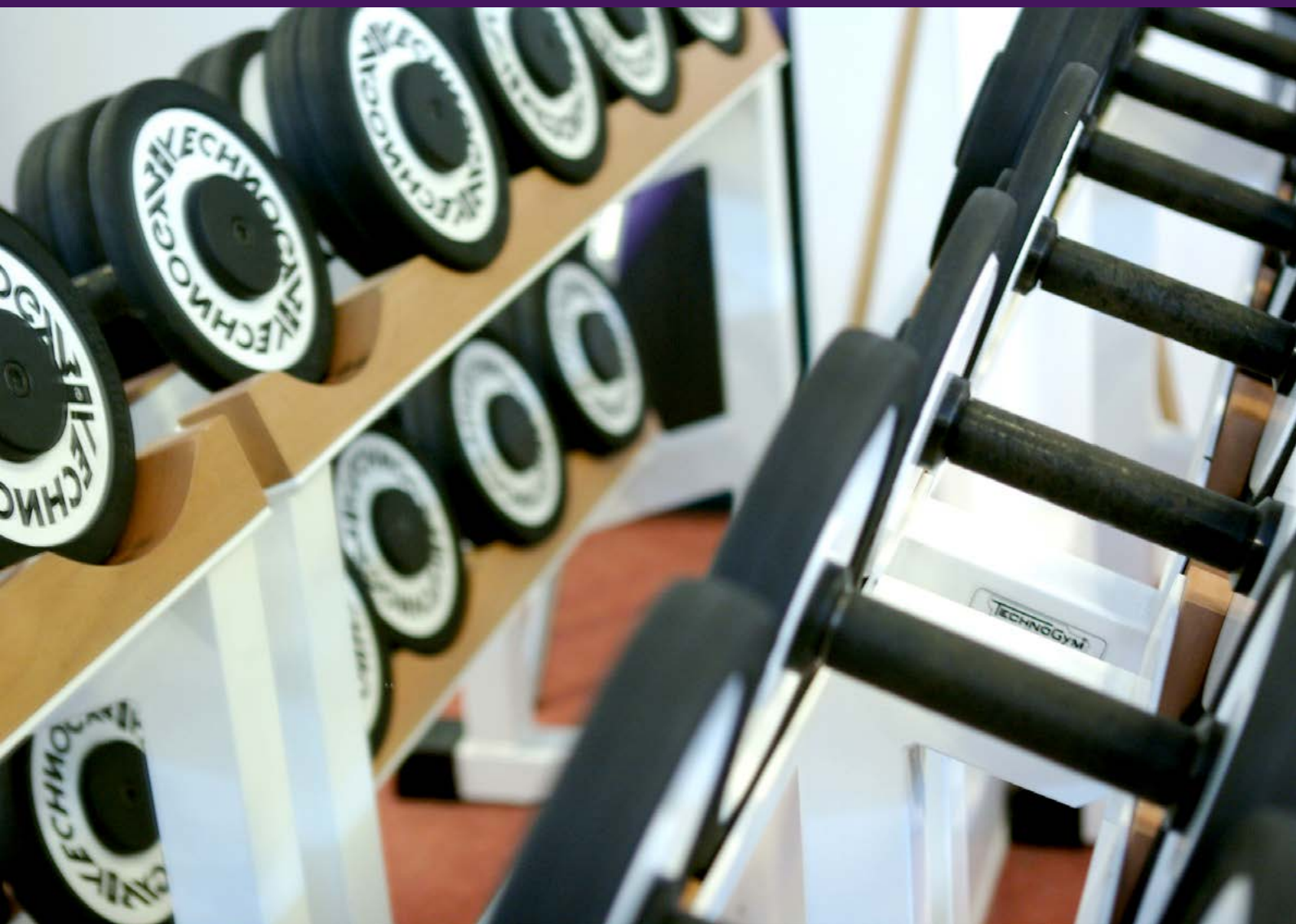
To avoid leaving a detected vulnerability in the infrastructure, application or organisation unresolved for too long, it is in the interest of the organisation to ensure that a retest with regard to the relevant findings is carried out quickly. You can already schedule one at the start of the original test. The security level can be restored or improved in a timely manner by embedding the retest in an improvement process, taking into account the overarching risk management process.

4.3.2 Include security tests in the security programme

Include the organisation of security testing and the points for evaluation and improvement in an overarching security programme. Ensure that this is in line with your organisation's security strategy. Adopting a systematic approach also ensures that all considerations, such as contractual issues, the selection of a suitable contractor and risk management for the organisation as a whole, become embedded within the organisation. CREST has published a practical guide with an extensive elaboration of such a programme, using penetration testing as an example.[16]

[16] See https://www.crest-approved.org/2018/07/20/penetration-testing-a-guide-for-running-an-effective-programme/index.html

Appendix



Appendix A Security testing profile

Security testing profile		
Step-by-step plan		Input for terms of reference – details
Step 1: Determine your goal		
Consider why you want to perform a security test		
Determine what you want to protect and what you want to protect against	Infrastructure	
	Application	
	Organisation	
Ask specific security assessment questions		
Step 2: Determine the means		
Select a security test type		Vulnerability assessment, penetration test, source code review
Determine the scope and depth of the test	Scope	External infrastructure, internal infrastructure, application, organisation
	Level of penetration	
	Prior information	Black box, grey box, white box
	Depth	
Components for testing		
Component A		Number of lines of code, programming languages, frameworks, protocols, IP addresses, architecture diagram, traffic flows
Component B		
Component C		

Appendix B Checklist for standard elements of security testing contracts

		Vulnerability assessment	Penetration test	Source code review
A.	Offer			
B.	Action plan			
C.	Intake form			
D.	Confidentiality statement			
E.	Indemnity statement			
F.	Reports			

A Offer

1. Action plan
2. Sample report
3. Overview of costs and activities
4. Time schedule
5. People who will perform the test

B Action plan

1. Terms of reference based on the security testing profile
2. Test methodology and scenarios
3. Attack strategies
4. Risk classification methodology
5. Method of delivery
6. Phasing
7. Agreements regarding deletion of data
8. Location

C Intake form

1. Commissioning party's contact information
2. Testers' contact information
3. Hosting parties' contact information
4. Notification of third parties that host systems or applications that fall within the scope
5. Communication plan
6. Reporting language
7. Method of delivery
8. Proposed schedule
9. Proposed testing times
10. Proposed scope
    a. Specific scope of the expected test (components included in the chain)
        I Infrastructure information
        II Application information
        III Organisation information
    b. Tests that fall outside the scope (absolutely forbidden actions)
    c. Components that fall outside the scope
    d. Which attack vectors are included in the scope, determined based on a risk assessment

e. Which testing elements are included in the scope, determined based on a risk assessment
f. Defined assumptions
g. Agreements on resources made available to the contractor for the tests, such as login details and digital or physical access points

11. Schematic representation of the scope

D Confidentiality statement

1. Acknowledgement of receipt for information received
2. Access to measures taken
3. Return/deletion of information received
4. Obligations relating to the confidentiality of information
5. Avoidance of unauthorised disclosures
6. Agreements on actions to be taken for a finding that qualifies for a coordinated vulnerability disclosure and the related roles and responsibilities
7. Legal consequences
8. Signature

E Indemnity statement

1. Agreements on actions to be taken in case of issues that cause a schedule overrun
2. Agreements regarding the contractor's liability
3. Agreements on confidentiality and deletion of information and results
4. Agreements on what to do if any personally identifiable information are encountered
5. Agreements to ensure that no information remains in the tested systems after completion of testing
6. Agreements on actions to be taken if any test evidence remains in the log files of the tested systems after completion of testing
7. Agreements regarding configuration files, any temporary changes made to these during the test and the restoration of the original configuration settings
8. Agreements regarding the authorisation of any penetration attempts within the agreed scope, using tools that have been tested beforehand and are free of malicious code
9. Agreements on denial-of-service tests that may disrupt the continuity of the commissioning party's services
10. Agreements on communication about the relevant testing activities on a need-to-know basis, if necessary, in connection with possible detection of and response to the tests
11. Agreements concerning the minimal potential impact on the continuity of services provided by the commissioning party
12. Signature on the indemnity agreement

F Reports

1. Report with findings
2. Management summary
3. Findings
   a. Description of how a finding was made
   b. Reproducibility of the finding
   c. Impact of the finding
   d. Risk description
   e. Recommendations
4. Explanation of the applied test methodology
5. Conclusion

Publication:

National Cyber Security Centre
Postbus 117 | 2501 cc Den Haag
070-751 55 55
info@ncsc.nl
@ncsc_nl

March 2020