

The Danish Gambling Authority's Certification Programme for betting and online casino



Requirements for penetration testing – SCP.04.00.EN.3.0

Contents

- 1. Objectives of the requirements for penetration testing2**
 - 1.1 Version 3
 - 1.2 Applicability 3

- 2. Frequency and testing organisations4**
 - 2.1 Penetration testing frequency 5
 - 2.1.1 Initial penetration test 5
 - 2.1.2 Renewed penetration test 5
 - 2.2 Testing organisations 5
 - 2.2.1 Requirements for testing organisations 5
 - 2.2.2 Requirements for personnel who performs the penetration test 6
 - 2.2.3 Supervision, assessment and attest of the standard report 6

- 3. Penetration testing framework7**
 - 3.1 Objective of the penetration testing 8
 - 3.2 Protected components 8
 - 3.2.1 Updating software and hardware 8

- 4. Penetration Testing process9**
 - 4.1 Standard report and plan for “not passed” penetration test10

Objectives of the requirements for penetration testing

1

The requirements for penetration testing shall ensure, that the base platform, game platform and business systems are tested to uncover possible vulnerabilities in the systems. Vulnerabilities, which possibly could be exploited to gain unauthorised access to e.g., sensitive information or affecting execution of games.

1.1 Version

Version 1.0 of 2014.07.04

- A new document structure than the previous version 1.3 alongside with a range of updates in different areas. A new version 1.0 is therefore published. It is the intention to follow normal versioning for future changes.

Version 1.1 of 2015.12.21

- Extension of applicability to cover offering of lotteries and betting on horse- and dog races.

Version 1.2 of 2020.01.01

- Spillemyndigheden has removed the requirement saying the ATO's accreditation must refer to a specific version cf. section 2.2.

Version 2.0 of 2023.01.01

- Update of requirements for accredited testing organisations and staff. Clarification of requirements if penetration test is not passed. The section on use of an internal function to perform vulnerability scans and penetration tests has been removed. Furthermore, general adjustments and specifications have been made.

Version 2.1 of 2023.10.01

- Updated visual layout of the document. Minor linguistic corrections. No changes to requirements.

Version 3.0 of 2025.01.01

- Changes are made because of the introduction of supplier licences. CREST accreditation is added as a recognized accreditation for testing organisations.

The Danish Gambling Authority continuously revises the certification programme for betting and online casino. The latest version is accessible at The Danish Gambling Authority's website.

When a new version of the certification programme is released, The Danish Gambling Authority will, if necessary, publish guidelines for a transition period and validity of already completed penetration tests.

It must be emphasised that only the Danish version is legally binding. The English version holds the status of guidance only.

1.2 Applicability

Requirements for penetration testing is applicable for provision of online- and land-based betting (§ 11 in the Danish Gambling act), online casino (§ 18 in the Danish Gambling act) and supply of games (§ 24a in the Danish Gambling act).

Frequency and testing organisations

2

2.1 Penetration testing frequency

The licence holder and game supplier are responsible for having a penetration test completed in accordance with the requirements in this document with an interval of maximum of 12 months.

2.1.1 Initial penetration test

The licence holder and game supplier shall have a penetration test completed before a licence to offer or supply games can be issued unless The Danish Gambling Authority has informed otherwise. See section 2.1.2 and 2.1.3 in the general requirements for further information.

2.1.2 Renewed penetration test

The licence holder and game supplier shall, as a rule, have completed a new penetration test within 12 months of the latest penetration test. The standard report shall reflect when the new penetration test was completed.

The standard report, which documents the renewed penetration test, shall be in the Danish Gambling Authority's possession no later than two months after the penetration test was completed.

2.1.2.1 Postponement of penetration test

The licence holder and game supplier can choose to postpone the penetration test up to 2 months from the time where a new penetration test should have been completed. The new penetration test must be finalised no later than 14 months after the latest penetration test and the standard report must be submitted to The Danish Gambling Authority within the same deadline.

The Danish Gambling Authority must be notified before the penetration test is postponed.

The deadline for renewal of penetration test is shortened with the equally amount of time the former 12-month deadline was postponed. Meaning that if you for instance make use of the maximum two months postponement, then the next penetration test is due 10 months later. The expected time for the next penetration test shall reflect this and be noted in the standard report.

2.2 Testing organisations

To ensure that the necessary qualifications are in place to perform the penetration test, the testing organisation and their staff shall fulfil the requirements in this section.

2.2.1 Requirements for testing organisations

Testing organisations shall attain minimum one of the following accreditations/approvals:

- CREST Accredited Penetration Testing
- ISO/IEC 17025-accreditation with reference to the Danish Gambling Authority's certification programme for betting and online casino SCP.04.00.DK, or
- ISO/IEC 17065-accreditation with reference to the Danish Gambling Authority's certification programme for betting and online casino SCP.04.00.DK, or
- Approved Scanning Vendor (ASV) approval.

The CREST-accreditation is done by the CREST membership body.

ISO-accreditation shall be done by DANAK (the Danish Accreditation Fund) or a similar accreditation body, who is co-signer of EA's (European co-operation for Accreditation) multilateral agreement on reciprocal recognition regarding testing, or for labs outside EA's jurisdiction, by an accreditation body, who is co-signer of ILAC's (the International Laboratory Accreditation Cooperation) multilateral agreement on reciprocal recognition regarding testing.

The ASV-approval is done by Payment Card Industry (PCI) Security Standards Council (SSC).

Documentation for the testing organisation's CREST-accreditation, ISO-accreditation or ASV-approval shall be enclosed with the standard report. Alternatively, a link to the accreditation or approval can be provided in the standard report.

2.2.2 Requirements for personnel who performs the penetration test

The penetration test shall be performed by staff with sufficient qualifications, which means the testing organisation shall hire and educate sufficiently qualified, competent, and experienced personnel. It is expected that the personnel who performs the penetration test, has at least 5 years of practical experience with penetration testing and has a personal certification, which demonstrates competence with penetration testing. This can e.g., be one of the following:

- Offensive Security Certified Professional (OSCP)
- EC-Council: Certified Ethical Hacker (CEH), Licensed Penetration Tester Master (LPT Master),
- Global Information Assurance Certification (GIAC): GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),
- CREST Penetration Testing Certifications,
- Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification,
- Tiger Scheme: Senior Security Tester, Qualified Security Tester.

2.2.3 Supervision, assessment and attest of the standard report

Performing the penetration test shall be supervised cf. the requirements for supervision in section 2.3 in the general requirements. Furthermore, the result of the penetration test and the need for possible remediation of vulnerabilities shall be assessed. It is the supervisor's responsibility to sign the standard report, and thereby warrant that the penetration test has been completed in an appropriate professional manner.

Guidance: A person who supervise, assess and signs, can also perform the penetration test cf. the requirements for supervision in section 2.3 in SCP.00.00 General requirements.

Penetration testing framework

3

The Danish Gambling Authority's requirements for penetration testing is based on gained experience with regulatory supervision in the area, recommendations from and dialogue with the industry.

3.1 Objective of the penetration testing

The purpose of penetration testing is to identify and seek to exploit any vulnerabilities in the base platform, game platform and business systems.

3.2 Protected components

The platforms and business systems in the licence holder's and game supplier's production environment shall be protected against any attacks from unauthorised persons. Particularly components containing sensitive information concerning customers shall be protected. The definition of components and their relevance shall be seen in context with The Danish Gambling Authority's Change Management Programme SCP.06.00.EN, section 3.3.3.

The licence holder and game supplier can minimise the risk of unauthorised access by segmenting the internal networks including which sub-systems communicates sensitive information by public networks.

3.2.1 Updating software and hardware

It is the licence holder's and game supplier's responsibility, that system components are updated to a degree that ensures the highest level of security possible and does not compromise the integrity of the systems, so the risk of unauthorised access is minimised.

Penetration Testing process

4

With no more than 12 months interval the licence holder shall have a penetration test completed of their base platform and business systems.

With no more than 12 months interval the game supplier shall have a penetration test completed of their game platform and business systems.

Guidance: 'Base platform', 'game platform' and 'business system' are defined in the general requirements and cover both frontend, backend, datawarehouse and games.

The penetration test shall cover, but not be limited to, any weaknesses uncovered during the vulnerability scanning, cf. The Danish Gambling Authority's requirements for vulnerability scanning SCP.05.00.DK.

The testing organisation shall furthermore seek to gain unauthorised access to the base platform, game platform and business systems. The unauthorised access shall be attempted escalated to the highest access level possible and completed with and without access credentials available (whitebox/blackbox). Through this access the following list of scenarios shall as a minimum be tested:

- Manipulation of result generation
- Affecting the execution of games
- Fraud with customer funds
- Theft of customer funds
- Manipulation of audit logs
- Access to sensitive information
- Manipulation of sensitive information
- Manipulation of data transfer to SAFE

4.1 Standard report and plan for "not passed" penetration test

In the standard report it must be stated whether the penetration test is passed, passed with remediation, or not passed.

'Passed' shall be used, when the penetration test is completed without finding any vulnerabilities.

'Passed after remediation' shall be used, when the penetration test has uncovered vulnerabilities, which have been remediated and a following test has shown, that the vulnerabilities are no longer present.

'Not passed' shall be used, if there are vulnerabilities, which cannot be remediated before the deadline for submitting the report to the Danish Gambling Authority. In this situation an annex containing a plan for remediating the identified vulnerabilities and a description of compensating control measures, shall be submitted along with the standard report. The licence holder or game supplier shall afterwards as soon as possible remediate the vulnerabilities and within 3 months have completed a new penetration test.

After the new penetration test, documentation showing that vulnerabilities have been remediated, shall be submitted to the Danish Gambling Authority.

In practise a 'not passed' report cannot be accepted by the Danish Gambling Authority, without the annex containing a plan for remediation and a description of compensating controls.

If a complete penetration test is performed of the licence holder's base platform and business systems or the game supplier's game platform and business systems after remediation of any vulnerabilities, the date of completion of this penetration will be the point of reference for determining the deadline for the next penetration test.

