TECHNICAL AUDITS FOR CERTIFYING EUROPEAN CITIZEN COLLECTION SYSTEMS

Technical audits in accordance with Regulation 211/2011 of the European Union and according to Executional Regulation 1179/2011 of the European Union, in which the technical requirements of article 6 of Regulation 211/2011 are specified, should provide the result of the following checks:

A. Functional Tests.

In web application aimed at collecting support for European citizen initiatives and those affected by Regulations 211/2011 and 1179/2011, functional tests will be performed, aimed at ensuring that the web application functionality is suitable for collecting statements of support via the website.

In order to carry out this task, a checklist is drawn up for dealing with the following issues:

- Analysis of the documentation and functional requirements
- Design and conducting of functional tests. Specifically, it will be checked:
    - Whether the purpose of the application is exclusively collection of support, and that it does not contain other functionalities.
    - The *backend* is separate from the support collection public area.
    - The application detects and prevents and duplicated support.
    - The application prevents automated submission of statements of support.
    - The application generates reports from signatories of statements of support by each Member state.
    - It allows exporting in XML format.
    - Information exported is labelled distribution limited to the member state concerned and as personal data.

- Drafting and Submission of the functional test checklist

B. Dynamic Security tests.

Dynamic security tests will be performed on the web applications aimed at identifying its possible weaknesses and areas of vulnerability. Tests will consist of the following tasks:

- Vulnerability analysis: It involves taking data on areas of vulnerability(inherent, technological or non-technological) of applications involved in the project. This activity will be carried out with the assistance of purpose-designed software tools.
- Intrusion test: Additionally, deep exploitation will be carried out on the existing areas of vulnerability by means of manual "hacking" tests, obtaining data to a greater depth that that obtained in the vulnerability analysis.

  In these intrusion tests, specific testing will be carried out to verify compliance with technical security measures described in regulation 1179/2011. Specifically, testing will be performed to verify the security of:

  - Injection-type attacks: *SQL, XPATH, LDAP*, system commands, etc.
  - XSS (Cross-Site Scripting) attacks.
  - Monitoring of sessions (time-out, randomness and size of identifiers, etc.) and authentication of the application.
  - CSRF (Cross-site Request Forgery) attacks.
  - Upgrading of user permission privileges.
  - Encrypting of communications with the application (correct HTTPS implementation using the most secure configurations).
  - Encryption of communications in remote access to the system or in communications with member states.
  - Invalid use of redirecting.
  - Checking of information leaks by means of information provided by application errors.
  - Attacks defined in the*"OWASP Top 10".*

All these tests will be performed in accordance with the standards and methodologies defined in the security test guides as defined by *OWASP.*

- Drafting of the security test report: with details of areas of vulnerability and weaknesses identified, and a list of recommendations and solutions

C. Static Security tests.

Application security will be tested internally via tests and security assessments, taking their source code, internally identifying possible weaknesses and areas of vulnerability that may be present in the applications' code.

In order to carry out this task, a documentation review will be performed, with applications specifications, and their code will be audited. Auditing of code will be performed with the use of specific tools for that purpose, and by means of assessment of the results by the work team.

According to Regulation 1179/2011, among the tests that will be carried out, this includes the following:

- Verification of the encrypting algorithms used internally in the application, both for storing the information in the database, including user passwords, and for the information authentication and transmission processes.
- Checking the mechanisms for filtering, managing errors and registering the activities carried out (signs in the logs), and especially registering the failed or successful accesses to the data.
- Verification of the algorithms used for generating identification, session control and password management.
- Checking the mechanisms used for labelling information.
- Verification of the validation of entries and exits from the application, as well as references to objects.

All of the tests are in accordance with the standards and methodologies defined by the guidelines for secure development compiled by *OWASP*.

As a result of these tests, a report will be issued that includes the details of the vulnerabilities found in specific cases in which the vulnerabilities occur, as well as recommendations for their correction. This report will also try to show evidence through errors in the code for application of the results obtained in the dynamic tests carried out.

D. Assessments of organisational measures and security requirements.

The IT infrastructure in which the web application is installed and hosted must also fulfil certain physical and logical security policies and measures that are sufficient to guarantee the degree of security of the application.

These security policies and measures will be assessed through a documentary review thereof, and a review of the application in the IT environments hosting the web application, as applicable.

Among the measures to be checked are the following:

- Assessment of compliance with regulation ISO/IEC 27001, and particularly the assessment of risks, the plan for treatment of risks and residual risk, bearing in mind not only the methodology for risk analysis but also the analysis of risks being comprehensive and coherent.
- The security plan and the safeguards applied depending on the category of the information and of the associated risks, especially the ideal nature and coherence with the risk analysis.
- The security policy, and the associated norms and procedures, particularly role assignation, encrypting regulations and the information labelling, information destruction, monitoring and managing signs and events, the policy for updating patches and the policy of backup copies.
- Assessment of controls of physical access to the installations.

- Assessment of patches and applied updates, both in the operating system and in the database and application server.
- Assessment of security controls, whether logical in the systems, or perimetral security in the network (firewalls used, location in the DMZ network segment, etc.) or as the security configuration used in particular measures for hardening, including the execution of the web service by a non-privileged user.
- Regarding backup copies and information encryption, this will assess whether both the backup copies and the auditing registers are adequately protected through the use of encrypting mechanisms.
- Assessment of compliance with legal requirements, and in particular, compliance with the legislation for the protection of personal data and the security document including the measures applied depending on the categorisation of the information.
- Assessments of the different Service Level Agreements (SLA) with providers to guarantee the confidentiality and traceability of the information, as well as to ensure that the physical location of the information is not in a third-party country with legislation that is not comparable to European legislation.

E. Requirements of the team carrying out the audit

The team carrying out the audit in the European Citizen Initiative systems must fulfil the following requirements:

- **The auditors:**
    - All of the auditors must have CISA and CISM certification or the equivalent.
    - The head auditor must have a demonstrable minimum experience of 5 years as a head auditor in audit companies within the cope of the information security management systems. S/he must spend a minimum of 15% of her/his time in auditing.

- The auditors must have a minimum of 3 years' demonstrable professional experienced in auditing in the area of information and communications technologies.
- At least one of the auditors must have a minimum of 3 years' experience in the legal area (LOPD).

- **The technical security personnel:**
  - Those who carry out the ethical penetration/hacking test must have:
    - a minimum of demonstrable experience in the last 3 years
    - demonstrable experience in use attacks of the 10 greatest OWASP vulnerabilities (OWASP top 10).
  - Those who carry out the analysis of the application code (if the software provided by the commission is not used) must have demonstrable experience in the development of applications under OWASP recommendations.