Online Collection Software

Guidelines for system certification

Date:	16/02/2012
Version:	1.00
Authors:	Ivan MARUSICH
	
Revised by:	
Approved by:	Natalia Aristimuño (DIGIT.B1)
	Mario-Paulo Tenreiro (SG.G4)
Public:	
Reference Number:	

RECORD OF ADDITIONS AND VARIANTS

Date	Version	Description	Chapter/Sections changed
XX/XX/YYYY	1.0	First release	

INDEX OF SECTIONS

1. INTRODUCTION

The aim of this document is to propose a security guide in order to assist the Organiser in deploying the OCS which is compliant with security standards, security best practices and with European Commission regulations.

Organisers should, in particular, refer to the, following documents:

- Commission Implementing Regulation No 1179/2011 of 17 November 2011 – Laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative;
- Common Weakness Enumeration (CWE) and in particular "potential mitigations" that are proposed to "contrast" a specific threat-vulnerability;
- FIPS PUB 140-2 - Security requirements for cryptographic modules
- ISO/IEC 17799:2005 - Information technology — Security techniques — Code of practice for information security management
- ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements
- OWASP Application Security Verification Standard – Web Application Standard (for short OWASP ASVS)

1.1. Applicable standards

ISO/IEC 2700k

The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

The standards are the product of ISO/IEC JTC1 (Joint Technical Committee 1) SC27 (Sub Committee 27), an international body that meets in person twice a year.

At present, eleven of the standards in the series are published and available, while several more are still under development. The original ISO/IEC standards are sold directly by ISO, while sales outlets associated with various national standards bodies also sell various versions including local translations.

OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. At OWASP you'll find free and open …

- Application security tools and standards
- Complete books on application security testing, secure code development, and security code review
- Standard security controls and libraries
- Local chapters worldwide
- Cutting edge research
- Extensive conferences worldwide
- Mailing lists
- And more

In particular the OWASP Application Security Verification Standard (ASVS) provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. This standard can be used to establish a level of confidence in the security of Web applications.

2. GLOSSARY

Term	Definition
Captcha	Abbreviation of: "Completely Automated Public Turing-test to tell Computers and Humans Apart" A Captcha is a reaction test used in computing as an attempt to ensure that the response is not generated by a computer. E.g. asking a user to retype a picture that shows a word, which is legible for a human being but not legible for a computer.
Citizen of the Union	A citizen is a person who holds the nationality of one of the 27 EU Member States.
Citizens' committee	A citizens' committee is a group of at least 7 organisers who are residents in at least 7 different EU countries responsible for the preparation of a citizens' initiative and the submission to the Commission.
Citizens' initiative	A citizens' initiative is a proposal for a legal act of the Union by a citizens' committee.
Commodity hardware	Commodity hardware is hardware that is easily and affordably available. A device that is said to use "commodity hardware" is one that uses components that were previously available or designed and are thus not necessarily unique to that device.
Component	Resource or entity forming part of the Perimeter which needs protection as it is potentially exposed to risk of Threats.
Countermeasure	Technical device or organizational procedure that can counter one or more threats and lower the risk level
Data controllers	A data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Term	Definition
Encryption	Encryption is the conversion of data into a form, called a ciphertext, using an algorithm, that cannot be easily understood by unauthorized people.
Exposure	Set of external type conditions which make the occurrence of harm more or less probable
Harm	Negative effect of a threat
Identity stores	An identity store is the location where user identification and authentication information is stored.
Input validation	Input validation is the process of ensuring that a program collects clean, correct and useful data. Validation "rules" check the correctness, meaningfulness, and security of data entered in the system.
Local File Inclusion	Local File Inclusion is the process of including files on a server through the web browser. This vulnerability occurs when a page is not properly sanitized, and allows directory traversal characters to be injected.
MIGRA	Integrated Methodology for the Management of Company Risks.
Online collection system	An online collection system is a web based application designed to collect data over a network.
Open-source software (OSS)	Open-source software (OSS) is computer software that is available in source code form for which the source code and certain other rights normally reserved for copyright holders are provided under a software license that permits users to study, change, and improve the software.
Organisers	Organisers are citizens of the Union forming a citizens' committee responsible for the preparation of a citizens' initiative and the submission to the Commission.
OWASP	Open Web Application Security Project.
OWASP ASVS	OWASP Application Security Verification Standard.
Portal	Front-end site.

Term	Definition
Processing	Processing of data is any process that uses a computer program to enter data and summarise, analyse or otherwise convert data into usable information.
Protection Measure	See countermeasure
EU Register	The register is an online register made available by the Commission to provide the information about the initiative, in particular on the subject-matter and objectives as well as on the sources of funding and support for the proposed citizens' initiative.
Reusable	Software is reusable if a segment of source code can be used again to add new functionalities with slight or no modification.
Risk	Possibility that a negative event will occur intended as the product between the probability of occurrence of the event and the consequent harm
Safety/Security	The condition of being free from harm, or more commonly, the absence of danger
Session	A session is an interactive information exchange between communicating devices.
Signatory	A signatory is a citizen of the European Union, who supports an initiative by completing a statement of support.
Site Visitor	Any site visitor or "end user" of the front-end site/portal.
System	Aggregate of homogenous components in terms of criticality, functionality, and need for protection
Threat	Potential event harmful to the component to protect
Vulnerability	Set of internal type conditions which make the occurrence of any harm more or less probable
Web application	A web application is a software application that can be accessed over a network or internet.

3. GUIDELINES

Firstly, it is important to make the Organiser aware that before deploying the OCS service, it is necessary to perform:

- A specific **Risk Analysis** to the whole system. Risk analysis performed on the OCS is only a part of the entire system. The Organiser's Risk Analysis should also include the following aspects: hardware, environment, operative system, service configuration, back-up system, etc. This is necessary in order to have a complete overview on all security needs.
- A detailed **Compliance Assessment** should be performed to evaluate the system security compliance in respect of EC Regulation No 1179/2011 of 17 November 2011 but also to ensure compliance with the standards applicable in this context: for example ISO27001.
- A detailed **Vulnerability Assessment** should be performed to analyze vulnerabilities in the whole system. The Vulnerability Assessment should be performed, in particular, as a white box and black box to simulate intrusion from internal/external attackers.
- A specific **Penetration Test** is recommended to evaluate how vulnerabilities are exploitable and to indentify possible attack paths. The Penetration test should also propose solutions on how to remedy these vulnerabilities in order to make the system secure.

In addition to these analyzes, the organizers must ensure that all possible solutions are put in place to make sure that the entire IT system is secure.

In order to achieve this, it is suggested that the following guidelines and checks are followed prior to deploying the OCS platform.

Verify that all requirements defined in the technical specification have been implemented. In particular:	
Passwords, session IDs, and other credentials are sent only over Transport Layer Security (TLS).	*TS – point 2.7.3.g*
The system does not have insecure direct object references.	*TS – point 2.7.4*
For direct references to restricted resources, the application verifies that the user is authorized to access the exact resource requested.	*TS – point 2.7.4.a*
If the reference is an indirect reference, the mapping to the direct reference is limited to values authorized for the	*TS – point 2.7.4.b*

current user.	
Proper security configuration is in place, which requires, at least, that: a) All software components are up-to-date, including the OS, web/application server, Data Base Management System (DBMS), applications, and all code libraries. b) OS and web/application server unnecessary services are disabled, removed, or not installed. c) Default account passwords are changed or disabled. d) Error handling is set up to prevent stack traces and other overly informative error messages from leaking. e) Security settings in the development frameworks and libraries are configured in accordance with best practices, such as the guidelines of OWASP.	*TS – point 2.7.6*
The system requires the most current version of the Hypertext Transfer Protocol Secure (HTTPS) to access any sensitive resource using certificates that are valid, not expired, not revoked, and match all domains used by the site.	*TS – point 2.7.9.a*
The system sets the 'secure' flag on all sensitive cookies.	*TS – point 2.7.9.b*
The server configures the TLS provider to only support encryption algorithms in line with best practices. The users are informed that they must enable TLS support in their browser.	*TS – point 2.7.9.c*
The DBMS used is up-to-date and continuously patched for newly discovered exploits	*TS – point 2.15*
A database activity log is in place. The system makes sure that audit logs recording exceptions and other security-relevant events listed below may be produced and kept until the data is destroyed in accordance with Article 12(3) or (5) of Regulation (EU) No 211/2011. Logs are adequately protected, for instance by storage on encrypted media. Organisers/administrators regularly check the logs for suspicious activity. Log contents include at least a) Dates and times for log-on and log-off by organisers/administrators; b) Performed backups; c) All database administrator changes and updates.	*TS – point 2.16*
Physical security Whatever the type of hosting used, the machine hosting the application is properly protected, which provides: a) Hosting area access control and audit log; c) Physical protection of backup data due to theft or incidental misplacement; d) That the server hosting the application is installed in a secured rack.	*TS – point 2.17*

The system is hosted on an internet facing server installed on a demilitarized zone (DMZ) and protected by a Firewall.	*TS – point 2.18.1*
When relevant updates and patches of the Firewall product become public, then such updates or patches are installed expediently.	*TS – point 2.18.2*
All inbound and outbound traffic to the server (destined to the online collection system) is inspected by the Firewall rules and logged.	*TS – point 2.18.3*
The online collection system must be hosted on an adequately protected production network segment that is separated from segments used to host non-production systems such as development or testing environments.	*TS – point 2.18.4*
Local Area Network (LAN) security measures are in place such as: a) Layer 2 (L2) Access list / Port switch security; b) Unused switch ports are disabled; c) The DMZ is on a dedicated Virtual Local Area Network (VLAN)/LAN; d) No L2 trunking enabled on unnecessary ports.	*TS – point 2.18.5*
Administrator access to the management interface of the online collection system has a short session time-out (maximum 15 minutes).	*TS – point 2.19.3*
When relevant updates and patches of the OS, the application runtimes, applications running on the servers, or anti-malware become public, then such updates or patches are installed expediently.	*TS – point 2.19.4*
Organiser client security For the sake of end-to-end security, the organisers take necessary measures to secure their client application/device that they use to manage and access the online collection system.	*TS – point 2.20*
Users run non-maintenance tasks (such as office automation) with the lowest set of privileges that they require to run	*TS – point 2.20.1*
When relevant updates and patches of the OS, any installed applications, or anti-malware become public, then such updates or patches are installed expediently.	*TS – point 2.20.2*
Verify that at least the security objective proposed by the Standard ISO27001 are implemented.	
Responsibility for asset All assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls	*ISO/IEC 27001:2005* *Objective 7.1*

should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.	
Secure Areas Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.	*ISO/IEC 27001:2005* *Objective 9.1*
Equipment security Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.	*ISO/IEC 27001:2005* *Objective 9.2*
Third party service delivery management The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.	*ISO/IEC 27001:2005* *Objective 10.2*
System planning and acceptance Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.	*ISO/IEC 27001:2005* *Objective 10.3*
Protection against malicious and mobile code Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate,	*ISO/IEC 27001:2005* *Objective 10.4*

introduce controls to prevent, detect, and remove malicious code and control mobile code.	
Backup Routine procedures should be established to implement the agreed back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.	*ISO/IEC 27001:2005* *Objective 10.5*
Network security management The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. Additional controls may also be required to protect sensitive information passing over public networks.	*ISO/IEC 27001:2005* *Objective 10.6*
Media handling Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.	*ISO/IEC 27001:2005* *Objective 10.7*
Exchange of information Exchanges of information and software between organizations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation (see clause 15). Procedures and standards should be established to protect information and physical media containing information in transit.	*ISO/IEC 27001:2005* *Objective 10.8*
Monitoring Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.	*ISO/IEC 27001:2005* *Objective 10.10*
User access management Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special	*ISO/IEC 27001:2005* *Objective 11.2*

attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.	
Network access control Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services by ensuring: a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks; b) appropriate authentication mechanisms are applied for users and equipment; c) control of user access to information services in enforced.	*ISO/IEC 27001:2005* *Objective 11.4*
Operating system access control Security facilities should be used to restrict access to operating systems to authorized users. The facilities should be capable of the following: a) authenticating authorized users, in accordance with a defined access control policy; b) recording successful and failed system authentication attempts; c) recording the use of special system privileges; d) issuing alarms when system security policies are breached; e) providing appropriate means for authentication; f) where appropriate, restricting the connection time of users.	*ISO/IEC 27001:2005* *Objective 11.5*
Application and information access control Security facilities should be used to restrict access to and within application systems. Logical access to application software and information should be restricted to authorized users. Application systems should: a) control user access to information and application system functions, in accordance with a defined access control policy; b) provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls; c) not compromise other systems with which information resources are shared.	*ISO/IEC 27001:2005* *Objective 11.6*
Security requirements of information system Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security.	*ISO/IEC 27001:2005* *Objective 12.1*

Security requirements should be identified and agreed prior to the development and/or implementation of information systems. All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.	
Cryptographic control A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.	*ISO/IEC 27001:2005* *Objective 12.3*
Security of system file Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.	*ISO/IEC 27001:2005* *Objective 12.4*
Technical vulnerability management Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.	*ISO/IEC 27001:2005* *Objective 12.6*
Reporting information security events and weaknesses Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.	*ISO/IEC 27001:2005* *Objective 13.1*
Management of information security incidents and improvements Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements.	*ISO/IEC 27001:2005* *Objective 13.2*
Information security aspects of business continuity management A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be	*ISO/IEC 27001:2005* *Objective 14.1*

the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities. The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization. Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.	
Compliance with legal requirements The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).	*ISO/IEC 27001:2005* *Objective 15.1*
Compliance with security policies and standards, and technical compliance The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.	*ISO/IEC 27001:2005* *Objective 15.2*