



International Standard - ISO 27001:2005

~ compliance report ~

International Standard - ISO 27001:2005

compliance report

Description

ISO/IEC 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements.

The objective of this standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.








Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.







Scan

URL	http://agid.internetsoluzioni.it
Scan date	7/28/2015 7:43:51 PM
Duration	8 hours, 30 minutes
Profile	Default

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- [Information handling procedures \(10.7.3\)](#)
Total number of alerts in this category: 32
- [Information exchange policies and procedures \(10.8.1\)](#)
 **No alerts in this category**
- [Electronic messaging \(10.8.4\)](#)
 **No alerts in this category**
- [Electronic commerce \(10.9.1\)](#)
 **No alerts in this category**
- [On-Line Transactions \(10.9.2\)](#)
 **No alerts in this category**
- [Publicly available information \(10.9.3\)](#)
 **No alerts in this category**
- [Protection of log information \(10.10.3\)](#)
Total number of alerts in this category: 32
- [Privilege management \(11.2.2\)](#)
 **No alerts in this category**
- [Password use \(11.3.1\)](#)
 **No alerts in this category**

- User authentication for external connections (11.4.2)
 **No alerts in this category**
- Information access restriction (11.6.1)
 **No alerts in this category**
- Input data validation (12.2.1)
 **No alerts in this category**
- Control of internal processing (12.2.2)
 **No alerts in this category**
- Output data validation (12.2.4)
 **No alerts in this category**
- Control of operational software (12.4.1)
Total number of alerts in this category: 18
- Access control to program source code (12.4.3)
 **No alerts in this category**
- Information leakage (12.5.4)
Total number of alerts in this category: 34

Compliance According to Categories: A Detailed Report

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

(10.7.3) Information handling procedures

Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

Total number of alerts in this category: 32

Alerts in this category

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected item	/editor/ckeditor
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source/plugins/save
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source/tests
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_tests
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/plugins/save
Affected parameter	
Variants	1
Affected item	/editor/fckeditor
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/_source
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/_source/globals
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/filemanager

Affected parameter	
Variants	1
Affected item	/editor/filemanager
Affected parameter	
Variants	1
Affected item	/editor/filemanager/include
Affected parameter	
Variants	1
Affected item	/editor/filemanager/uploader
Affected parameter	
Variants	1
Affected item	/grafica/admin
Affected parameter	
Variants	1
Affected item	/inc
Affected parameter	
Variants	1
Affected item	/temp
Affected parameter	
Variants	1
Affected item	/tmp
Affected parameter	
Variants	1

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	/admin.php
Affected parameter	
Variants	1
Affected item	/personalizzazioni/popover/.gitignore
Affected parameter	
Variants	1

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	/archivio13_strutture-organizzative_0_9861_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9864_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9882_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9892_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9902_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9908_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40509_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40510_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40511_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40512_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40514_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40517_0.html
Affected parameter	
Variants	1

Error page web server version disclosure

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	1

(10.8.1) Information exchange policies and procedures

Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

No alerts in this category.

(10.8.4) Electronic messaging

Information involved in electronic messaging should be appropriately protected.

No alerts in this category.

(10.9.1) Electronic commerce

Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

No alerts in this category.

(10.9.2) On-Line Transactions

Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

No alerts in this category.

(10.9.3) Publicly available information

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

No alerts in this category.

(10.10.3) Protection of log information

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

Total number of alerts in this category: 32

Alerts in this category

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
------	---

CWE	CWE-200
Affected item	/editor/ckeditor
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source/plugins/save
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source/tests
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_tests
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/plugins/save
Affected parameter	
Variants	1
Affected item	/editor/fckeditor
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/_source
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/_source/globals
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/filemanager
Affected parameter	
Variants	1
Affected item	/editor/filemanager
Affected parameter	
Variants	1
Affected item	/editor/filemanager/include
Affected parameter	
Variants	1
Affected item	/editor/filemanager/uploader
Affected parameter	
Variants	1
Affected item	/grafica/admin
Affected parameter	
Variants	1
Affected item	/inc
Affected parameter	
Variants	1
Affected item	/temp

Affected parameter	
Variants	1

Affected item	/tmp
Affected parameter	
Variants	1

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	/admin.php
Affected parameter	
Variants	1

Affected item	/personalizzazioni/popover/.gitignore
Affected parameter	
Variants	1

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	/archivio13_strutture-organizzative_0_9861_0.html
Affected parameter	
Variants	1

Affected item	/archivio13_strutture-organizzative_0_9864_0.html
Affected parameter	
Variants	1

Affected item	/archivio13_strutture-organizzative_0_9882_0.html
Affected parameter	
Variants	1

Affected item	/archivio13_strutture-organizzative_0_9892_0.html
Affected parameter	
Variants	1

Affected item	/archivio13_strutture-organizzative_0_9902_0.html
---------------	--

Affected parameter	
Variants	1

Affected item	/archivio13_strutture-organizzative_0_9908_0.html
Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40509_0.html
Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40510_0.html
Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40511_0.html
Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40512_0.html
Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40514_0.html
Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40517_0.html
Affected parameter	
Variants	1

Error page web server version disclosure

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	Web Server
Affected parameter	
Variants	1

(11.2.2) Privilege management

The allocation and use of privileges should be restricted and controlled.

No alerts in this category.

(11.3.1) Password use

Users should be required to follow good security practices in the selection and use of passwords.

No alerts in this category.

(11.4.2) User authentication for external connections

Appropriate authentication methods should be used to control access by remote users.

No alerts in this category.

(11.6.1) Information access restriction

Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

No alerts in this category.

(12.2.1) Input data validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

No alerts in this category.

(12.2.2) Control of internal processing

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

No alerts in this category.

(12.2.4) Output data validation

Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

No alerts in this category.

(12.4.1) Control of operational software

There should be procedures in place to control the installation of software on operational systems.

Total number of alerts in this category: 18

Alerts in this category

Apache httpd remote denial of service

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

<http://seclists.org/fulldisclosure/2011/Aug/175>

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

CVSS	Base Score: 7.9 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: Complete
CWE	CWE-399
CVE	CVE-2011-3192
Affected item	Web Server
Affected parameter	
Variants	1

Cookie without HttpOnly flag set

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CWE	CWE-16
Affected item	/
Affected parameter	
Variants	4

Cookie without Secure flag set

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CWE	CWE-16
Affected item	/
Affected parameter	
Variants	10

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CWE	CWE-16
Affected item	/media/_
Affected parameter	
Variants	2

Error page web server version disclosure

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	1

(12.4.3) Access control to program source code

Access to program source code should be restricted.

No alerts in this category.

(12.5.4) Information leakage

Opportunities for information leakage should be prevented.

Total number of alerts in this category: 34

Alerts in this category

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	/editor/ckeditor
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source/plugins/save
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_source/tests
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/_tests
Affected parameter	
Variants	1
Affected item	/editor/ckeditor/plugins/save
Affected parameter	

Variants	1
Affected item	/editor/fckeditor
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/_source
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/_source/globals
Affected parameter	
Variants	1
Affected item	/editor/fckeditor/editor/filemanager
Affected parameter	
Variants	1
Affected item	/editor/filemanager
Affected parameter	
Variants	1
Affected item	/editor/filemanager/include
Affected parameter	
Variants	1
Affected item	/editor/filemanager/uploader
Affected parameter	
Variants	1
Affected item	/grafica/admin
Affected parameter	
Variants	1
Affected item	/inc
Affected parameter	
Variants	1
Affected item	/temp
Affected parameter	
Variants	1
Affected item	/tmp
Affected parameter	
Variants	1

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	/admin.php
Affected parameter	

Variants	2
Affected item	/personalizzazioni/popopover/.gitignore
Affected parameter	
Variants	2

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200
Affected item	/archivio13_strutture-organizzative_0_9861_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9864_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9882_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9892_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9902_0.html
Affected parameter	
Variants	1
Affected item	/archivio13_strutture-organizzative_0_9908_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40509_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40510_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40511_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40512_0.html
Affected parameter	
Variants	1
Affected item	/archivio3_personale-ente_0_40514_0.html

Affected parameter	
Variants	1

Affected item	/archivio3_personale-ente_0_40517_0.html
Affected parameter	
Variants	1

Error page web server version disclosure

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	Web Server
Affected parameter	
Variants	1