acunetix

International Standard - ISO 27001:2013

Compliance Report

05 July 2024

Generated by Acunetix

Description

ISO/IEC 27001 is an information security management system (ISMS) standard published in September 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2013 - 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	192.168.0.24
Scan date	05/07/2024, 23:02:26
Duration	7 minutes, 56 seconds
Profile	Full Scan

Compliance at a Glance

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

- Inventory of assets(8.1.1)
No alerts in this category

- Handling of assets(8.2.3)
No alerts in this category

- Access to networks and network services(9.1.2)
No alerts in this category

- Management of privileged access rights(9.2.3)
No alerts in this category

- Management of secret authentication information of users(9.2.4)
No alerts in this category

- Use of secret authentication information(9.3.1)
No alerts in this category

- Information access restriction(9.4.1)
No alerts in this category

- Secure log-on procedures(9.4.2)
No alerts in this category

- Password management system(9.4.3)
No alerts in this category

- Use of privileged utility programs(9.4.4)
No alerts in this category

- Access control to program source code(9.4.5)
No alerts in this category

- Separation of development, testing and operational environments(12.1.4)
No alerts in this category

- Controls against malware(12.2.1)
No alerts in this category

- Protection of log information(12.4.2)
No alerts in this category

- Administrator and operator logs(12.4.3)
No alerts in this category

- Installation of software on operational systems(12.5.1)
No alerts in this category

- Security of network services(13.1.1)
No alerts in this category

- Information transfer policies and procedures(13.2.1)
No alerts in this category

- Electronic messaging(13.2.3)
No alerts in this category

- Securing application services on public networks(14.1.2)
No alerts in this category

- Protecting application services transactions(14.1.3)
No alerts in this category

- Secure development policy(14.2.1)
No alerts in this category

- Protection of test data(14.3.1)
No alerts in this category

- Availability of information processing facilities(17.2.1)
No alerts in this category

- Protection of records(18.1.3)
No alerts in this category

- Privacy and protection of personally identifiable information(18.1.4)
No alerts in this category

- Regulation of cryptographic controls(18.1.5)
No alerts in this category

Compliance According to Categories: A Detailed Report

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

(8.1.1)Inventory of assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

No alerts in this category.

(8.2.3)Handling of assets

Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

No alerts in this category.

(9.1.2)Access to networks and network services

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

No alerts in this category.

(9.2.3)Management of privileged access rights

The allocation and use of privileged access rights shall be restricted and controlled.

No alerts in this category.

(9.2.4)Management of secret authentication information of users

The allocation of secret authentication information shall be controlled through a formal management process.

No alerts in this category.

(9.3.1)Use of secret authentication information

Users shall be required to follow the organization's practices in the use of secret authentication information.

No alerts in this category.

(9.4.1)Information access restriction

Access to information and application system functions shall be restricted in accordance with the access control policy.

No alerts in this category.

(9.4.2)Secure log-on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

No alerts in this category.

(9.4.3)Password management system

Password management systems shall be interactive and shall ensure quality passwords.

No alerts in this category.

(9.4.4)Use of privileged utility programs

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

No alerts in this category.

(9.4.5)Access control to program source code

Access to program source code shall be restricted.

No alerts in this category.

(12.1.4)Separation of development, testing and operational environments

---

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

No alerts in this category.

(12.2.1)Controls against malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

No alerts in this category.

(12.4.2)Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

No alerts in this category.

(12.4.3)Administrator and operator logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

No alerts in this category.

(12.5.1)Installation of software on operational systems

Procedures shall be implemented to control the installation of software on operational systems.

No alerts in this category.

(13.1.1)Security of network services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

No alerts in this category.

(13.2.1)Information transfer policies and procedures

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

No alerts in this category.

(13.2.3)Electronic messaging

Information involved in electronic messaging shall be appropriately protected.

No alerts in this category.

(14.1.2)Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

No alerts in this category.

(14.1.3)Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

No alerts in this category.

(14.2.1)Secure development policy

Rules for the development of software and systems shall be established and applied to developments within the organization.

No alerts in this category.

(14.3.1)Protection of test data

Test data shall be selected carefully, protected and controlled.

No alerts in this category.

(17.2.1)Availability of information processing facilities

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

No alerts in this category.

(18.1.3)Protection of records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

No alerts in this category.

(18.1.4)Privacy and protection of personally identifiable information

---

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

No alerts in this category.

(18.1.5)Regulation of cryptographic controls

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

No alerts in this category.

Affected Items: A Detailed Report

This section provides full details of the types of vulnerabilities found according to individual affected items.

Scanned items (coverage report)

http://192.168.0.24:8000/
http://192.168.0.24:8000/swagger
http://192.168.0.24:8000/swagger/absolute-path.js
http://192.168.0.24:8000/swagger/index.html
http://192.168.0.24:8000/swagger/index.js
http://192.168.0.24:8000/swagger/oauth2-redirect.html
http://192.168.0.24:8000/swagger/swagger-ui-bundle.js
http://192.168.0.24:8000/swagger/swagger-ui-standalone-preset.js
http://192.168.0.24:8000/swagger/swagger-ui.css