The most common physical and network controls when implementing ISO 27001 in a data center

Neha Yadav | February 26, 2019

Security controls for Data Centers are becoming a huge challenge due to increasing numbers of devices and equipment being added. In this article you will see how to build an **ISO 27001** compliant Data Center by identification and effective implementation of information security controls. The article summarizes **ISO 27001 Data Center requirements** and helps you improve its security.

Security challenges for a Data Center

A Data Center is basically a building or a dedicated space which hosts all critical systems or Information Technology infrastructure of an organization. The number of security attacks, including those affecting Data Centers are increasing day by day. Data Centers contain all the critical information of organizations; therefore, information security is a matter of concern. A Data Center must maintain high standards for assuring the confidentiality, integrity and availability of its hosted IT (Information Technology) environment.

To understand the importance of ISO 27001 certification from the perspective of a CEO of an independent Data Center, read the article **ISO 27001 Case study for data centers: An interview with Goran Djoreski**.

How to select security controls to fulfil ISO 27001 requirements for a secure Data Center?

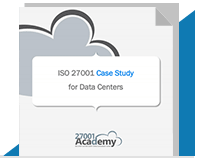
The best approach to select security controls for a Data Center should be to start with a risk assessment. In a risk assessment, you analyze the threats, vulnerabilities and risks that can be present for a Data Center. The risk assessment methodology can be the same as you are using for ISO 27001, if you are certified in it. If not, feel free to define your own methodology for risk assessment.

To learn more about risk assessment, read the article **ISO 27001 risk assessment: How to match assets, threats and vulnerabilities**.

ISO 27001 CASE STUDY FOR DATA CENTERS

Free white paper that explains how the implementation of ISO 27001 can benefit data centers

DOWNLOAD NOW →



Threats

The following are examples of the most common threats to Data Centers:

- Breach of confidential information
- Denial of Service (DoS) Attack
- Unauthorized access and usage of computing resources
- Identity theft
- Data theft or alteration

Vulnerabilities

The most common weaknesses in Data Centers are related to the following areas:

- The flaws in the implementation of things like software and protocols, wrong software design or incomplete testing, etc.
- Configuration flaws such as usage of default credentials, elements not properly configured, known vulnerabilities, out of date systems, etc.
- Ineffective security design
- Ineffective implementation of redundancy for critical systems
- Ineffective physical access control/lack of environmental controls, etc.

Based on the list of risks identified, each risk shall be mapped to security controls, that can be chosen from ISO 27001 (Annex A controls) or security controls from other local/international information security standards.

There are various types of the controls that can be implemented to mitigate identified risks, but this article will focus only on physical controls and virtual/network controls.

Physical security controls

The physical security of a Data Center is the set of protocols that prevent any kind of physical damage to the systems that store the organization's critical data. The selected security controls should be able to handle everything ranging from natural disasters to corporate espionage to terrorist attacks. To understand about the protection of secure areas please read the article **Physical security in ISO 27001: How to protect the secure areas**.

Examples of physical security controls include the following:

- Secure Site selection by considering location factors like networking services, proximity to power grids, telecommunications infrastructure, transportation lines and emergency services, geological risks and climate, etc.
- Natural disaster risk-free locations or Disaster Recovery site

- Physical Access Control with anti-tailgating/anti-pass-back turnstile gate which permits only one person to pass through after authentication
- Single entry point into the facility
- Additional physical access restriction to private racks
- CCTV camera surveillance with video retention as per organization policy
- 24×7 on-site security guards, Network Operations Center (NOC) Services and technical team
- Regular maintenance of hardware in use
- Monitoring access control/activities
- Air conditioning and indirect cooling to control the temperature and humidity
- Monitoring of temperature and humidity
- Uninterruptible Power Supply (UPS)
- Smoke detectors to provide early warning of a fire at its incipient stage
- Fire protection systems, including fire extinguishers. Preferably the fire prevention shall be with zoned dry-pipe sprinkler
- Cabling Security including raised floor cabling, for security reasons and to avoid the addition of cooling systems above the racks

Network security controls

Virtual security or network security are measures put in place to prevent any unauthorized access that will affect the confidentiality, integrity or availability of data stored on servers or computing devices. To understand the access control in ISO 27001, please read the article **How to handle access control according to ISO 27001**.

Network security is quite difficult to handle as there are multiple ways to compromise the network of an organization. The biggest challenge of network security is that methods of hacking or network attacks evolve year after year. For example, a hacker may decide to use a malware, or malicious software, to bypass the various firewalls and gain access to the organization's critical information. Old systems may put security at risk because they do not contain modern methods of data security. Also, with increasing

popularity of teleworking, there is a risk of virtual attacks. For more about teleworking, please read the article **How to apply information security controls in teleworking according to ISO 27001**.

Virtual attacks can be prevented by using the below techniques:

- Encryption for web applications, files and databases
- Audit Logs of all user activities and monitoring the same
- Best Practices for password security. Usage of strong passwords and secure usernames which are encrypted via 256-bit SSL, and not storing them in plain text, set up of scheduled expirations, prevention of password reuse
- Role Based Access Control
- AD (Active Directory)/LDAP (Lightweight Directory Access Protocol) integration
- Controls based on IP (Internet Protocol) addresses
- Encryption of the session ID cookies in order to identify each unique user
- Dual factor authentication
- Frequent third party VAPT (Vulnerability and Penetration Testing)
- Malware prevention through firewalls and other network devices

Importance of risk assessment

As explained above, it is important to conduct a risk assessment and implement appropriate security controls in order to achieve compliance to ISO 27001, ensuring a secure Data Center. The IT infrastructure of any organization is mainly dependent on the hardware (like servers, storage, etc.) which is in the Data Center. This means that, whenever an organization implements ISO 27001 or other information security standards, the organization needs to consider the above-mentioned risk assessment for the Data Center to fully protect the data.

Read about a real-life implementation in this free **ISO 27001 Case study for data centers**.

About the author:

Neha Yadav is a computer science engineer and has experience in Information Security Management Systems, Information Technology Service Management Systems, Quality Management Systems and Business Continuity Management Systems. She holds an engineering degree in Computer Science. Among her certifications are: ISO 27001 Lead Auditor, ITIL V3 and she has attended multiple information security training courses. She has experience in consultancy, training, implementation and auditing of various national and international standards.

ISO 27001 CASE STUDY FOR DATA CENTERS

Free white paper that explains how the implementation of ISO 27001 can benefit data centers

DOWNLOAD NOW

« Why is ISO 27001 applicable al...

How ISO 27001 and TISAX are re... »

If you enjoyed this article, subscribe for updates

Improve your knowledge with our free resources on ISO 27001/ISO 22301 standards.

Email *

UPDATE ME BY EMAIL

You may unsubscribe at any time.

For more information on what personal data we collect, why we need it, what we do with it, how long we keep it, and what are your rights, see this Privacy Notice.

27001/22301 Expert, Advisera

GET FREE ADVICE

Popular posts | Recent posts

- List of mandatory documents required by ISO 27001 (2013 revision)
- ISO 27001/ISO 27005 risk assessment & treatment – 6 basic steps
- Information classification according to ISO 27001
- ISO 27001 checklist: 16 steps for the implementation
- Catalogue of threats & vulnerabilities

OUR CLIENTS

OUR PARTNERS

Advisera is Exemplar Global Certified TPECS Provider for the IS, QM, EM, TL and AU Competency Units.

DNV GL Business Assurance is one of the leading providers of accredited management systems certification.

EXPLORE ADVISERA

EU GDPR Online Consultation Center

ISO 27001 and ISO 22301 Online Consultation Center

ISO 9001 Online Consultation Center

ISO 14001 Online Consultation Center

ISO 45001 Online Consultation Center

ISO 13485 Online Consultation Center

AS9100 Online Consultation Center

IATF 16949 Online Consultation Center

ISO/IEC 17025 Online Consultation Center

ITIL and ISO 20000 Online Consultation Center

ISO Compliance & Company Management

ISO online courses

Leading books on ISO standards

DOCUMENTATION

Product Tour

EU GDPR & ISO 27001

ISO 27001

ISO 22301

Consultant Toolkit

Free Preview Download

LEARNING CENTER

What is ISO 27001?

What is ISO 22301?

Tools

Free Downloads

ISO 27001 Webinars

Knowledgebase

Security Awareness Training

ABOUT

Product list

About us

Contact us

Newsletter

Privacy and Terms

FAQs

We are hiring

Testimonials

SUPPORT

ISO 27001 Where to start

Free Consultation

Community

BLOG

ISO 27001 & ISO 22301 Blog