Understanding ISO 27001 – An Information Security Standard

saki76

August 15, 2016 | Views: 18962

Over the last few months, I have been reading about various IT and InfoSec frameworks such as COBIT, NIST CyberSecurity framework and ISO 27001 as well as CIS Critical Security Controls to find a suitable framework to implement in my organization. ISO 27001 is one of the most important Information Security frameworks. ISO 27000 is a family of standards, which, if implemented properly, helps an organization secure its information assets. In this family, ISO 27000 consists of an overview and vocabulary, ISO 27001 defines the requirements for the program while ISO 27002, defines the operational steps necessary in an information security program.

ISO 27001 is the standard which define requirements for an organization to implement an Information Security Management System (ISMS) and is the main standard in ISO 27000 series. In simple words, it describe how to manage information security in a company. It can be implemented in any organization irrespective of its size or type profit or non profit, private or state owned. An organization can get certified on ISO 27001, but it is not obligatory. One may choose to implement the standard first and get certified later when the organization is compelled by regulations or wants to increase its trust among customers and clients. The standard was first published in 2005 and was recently revised in 2013.

ISO 27001 has eleven short clauses 0 – 10 and an Annex A. Clauses 0 – 3 describe the standard and clauses 4 – 10 set the requirement for information security system, which must be implemented for an organization to be compliant with the standard. Annex A contains 114 security controls or safeguards grouped into 14 sections. The standard takes a risk management approach to protect the information security of company. Risk assessment is done to find out potential risks to information and then risk mitigation is done to address them through security controls. The security controls used to address risk are in form of policies, procedures and technical controls (HW or SW) to secure assets.

ISO 27001 benefits organizations by implementing security in a comprehensive manner. It helps organizations comply with legal requirements, achieve marketing advantage by reassuring customers about security, lower costs by preventing incidents and be better organized by defining processes and procedures for a coordinated approach to information security.

The ISO 27001 standard is not freely available and has to be purchased either online or in paper form for reference and implementation. Advisera a training and consultancy company has number of useful articles on ISO 27001 basics, implementation ideas and checklists. It also has two very useful and surprisingly free courses on the standard. The first ISO 27001:2013 Foundations Course explains the standard and gives an excellent coverage of the standard in 6 modules of total 8 hours. The second, ISO 27001:2013 Internal Auditor Course covers the basics of how an organization can be audited to ensure that the ISO 27001 standard has been implemented properly. Their website has a wealth of information on ISO 27001 and other ISO standards including blog posts, white papers, check lists, presentation, video tutorials and webinars.
I would recommend everyone interested in the standard to go through their website comprehensively before taking any training or implementing the standard. In India, BSI India and SQTC conduct personal trainings on ISO 27001 covering foundations, Lead Implementer and Lead Auditor courses.

I hope I have given a good overview of the ISO 27001 standard. Please do comment and ask questions if you have any queries or suggestions.

References

1. ISO Standard – http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
2. ISO 27001 reference website – http://www.iso27001security.com/

3. What is ISO 27001? – http://advisera.com/27001academy/what-is-iso-27001/
4. ISO 27001 Wikipedia page – https://en.wikipedia.org/wiki/ISO/IEC_27001:2013
5. Advisera – ISO 27001 Academy – http://advisera.com/27001academy/

14 Comments

SLASHBUG

3:45 am on April 30, 2018

Thank you

Log in to Reply

MONCHICHI81

5:43 am on March 23, 2018

Thank you! Very helpful

Log in to Reply

MAGNETO89

11:05 am on February 13, 2018

Needful information for anyone. Thank you.

Log in to Reply

SHASHU1

11:56 pm on November 26, 2017

this is very helpful

Log in to Reply

Comment on This

You must be logged in to post a comment.

OUR REVOLUTION

We believe Cyber Security training should be free, for everyone, FOREVER. Everyone, everywhere, deserves the OPPORTUNITY to learn, begin and grow a career in this fascinating field. Therefore, Cybrary is a free community where people, companies and training come together to give everyone the ability to collaborate in an open source way that is revolutionizing the cyber security educational experience.

Protected by

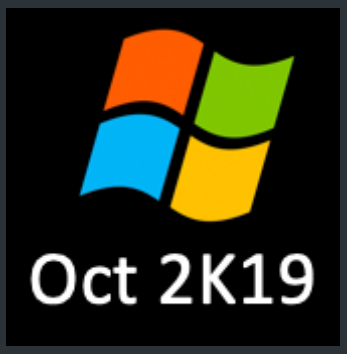
STUDENT SUPPORT

Get Support

OTHER PAGES

- About
- Join Our Team
- Press
- Terms of Service
- Verify Certificate
- Submit Suggestions
- Companies

SUPPORT CYBRARY



Donate Here to Get This Month's Donor Badge

CYBRARY|0P3N

R Marthon

Pass the Cisco CCNA Security 300-209 Exam

Views: 196 / October 26, 2019

solenegabellec

CyberSecurity Quick Guide for Students

Views: 320 / October 25, 2019

gagan1999

Kali Linux: Installing Kali Linux in VirtualBox

Views: 850 / October 24, 2019

slwelty

Our World in Transition and Our Future Demands

Views: 1022 / October 23, 2019

Back to Top