المجمـــــع العربـــــي الـــــدولي لتكـنولـوجيـــــا الإدارة
The Arab International Society for Management Technology (AIMICT)
Member of TAG-Foundation عضـو في طلال أبوغزاله فاونديشـن

AIMICT NEWSLETTER

MAY 2019

AIMICT.ORG

IN THIS ISSUE

AIMICT RELEASES PQM EXAM RESULTS

AMMAN - The Arab International Society for Management Technology (AIMICT) released results of PQM exam conducted for a group of participants from different sectors in Amman, Gaza and Ramallah.

AIMICT ORGANIZES ILM'S "HUMAN RESOURCE MANAGER" PROGRAM IN AMMAN

The Arab International Society for Management Technology (AIMICT) will conduct a Human Resource Manager (HRM) session in June 2019, in Amman.

Human Resource Manager Program aims to develop the necessary skills and knowledge of employees in the field of management and Human Resource Planning.

The 40-hour program is accredited by the Institute of Leadership and Management (ILM) – UK and targets trainers, teachers and instructors, co-trainers, and HR staff, and can be given in Arabic and/or English.

Those who wish to register should contact the Society's management and fill the registration application through the following link: *http://www.aimict.com/Certificate_Registration.aspx?title=key_human_resources_manager*

ilm
Recognised Provider

AIMICT ORGANIZES ISO 31000 LEAD RISK MANAGEMENT COURSE IN JORDAN

PECB ISO 31000 Risk Manager

AMMAN - The Arab International Society for Management Technology (AIMICT) will hold new sessions of the accredited ISO 31000 Lead Risk Management course in Jordan.

The ISO 31000 program aims at enabling the participants to acquire the expertise to support and lead an organization and its team to successfully identify, understand and manage a risk process based on ISO 31000, participants will gain comprehensive knowledge of the best practices used to implement a Risk Management framework that provides the foundation for designing, implementing, monitoring, reviewing and continually improving a risk management process in an organization.

The program is accredited by PECB and targets managers and/or professionals responsible for creating and protecting value in organizations through effective management of risks and risk management team members.

Those who are interested in enrolling in the training program are requested to contact the Society's management to proceed with the registration process.

HOW TO INTEGRATE ISO/IEC 27032 CYBERSECURITY ON ISMS?

By PECB

Definition of CyberSecurity

Cybersecurity often is used as a buzzword everybody is talking about these days. Although, a sharp definition of what it is and how it relates to Information Security and an ISMS (Information Security Management System) keeps being unfamiliar and negligent to many people. Additionally, there is already some local legislation which uses this term, so let's first look at the term to get a better understanding.

ISO 27032 defines "Cybersecurity" as the "preservation of confidentiality, integrity and availability of information in the Cyberspace" and "Cyberspace" as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

For those familiar with Information Security, the protection goals "confidentiality, integrity and availability" are already known, thus the specifics of Cybersecurity are closely related to the term Cyber Space. Simply put, Cybersecurity deals with information security wherever the Internet is involved. If you look at Information Security from an organization perspective, cybersecurity appears to be a subset of Information Security where generally all ISO 27001 principles are applied. Please note, that ISO 27032 is a guideline rather than a certification standard.

Why does ISO feel that additional guidance is necessary?

While the general approach of ISO 27001, to establish a PDCA cycle based on risk management, needs to be applied to Cybersecurity, there are some unique aspects to cybersecurity that will be found rarely within the borders of your organization. Let's have a look at them.

Additional Interested Parties and Stakeholders

In compared to an organization where all assets reside within clear defined physical borders, an organization using the Cyberspace deals with a much bigger number of interested parties and stakeholders. Interested parties are all those parties, who are giving input to your existing ISMS or expecting output from your ISMS. Some of the examples of such parties include customers, inter-trade organizations, regulation and legal bodies. Interested parties are usually defined during the planning phase of ISMS. If you are opening your organization to cyberspace, you will have to extend the list of interested parties accordingly. The purpose of this exercise is mainly to clarify who your communication partners are and to specify which kind of information needs to be interchanged, and what the triggers are.

Collaborative Use of Assets with Multiple Owners

The Internet is a shared medium. If you are using a service on the Internet you might not even be aware of all parties involved. Within the physical boundaries of an organization, you usually are. There are services at various layers of the communication stack involved, starting with the carriers up to cloud service providers that rely on each other. Nevertheless, your management responsibilities do not change. The implication is that you have to adjust your context of the organization, interested parties, policies, your "risk assessment process" and various roles. ISO 27001 requires that every asset needs to have one owner. The owner is in the driver seat for assessing risks and caring about remediation. As the borders of the organization dissolve, as a consequence of using the cyberspace, the challenge of mapping the virtual assets to owners in your organization appears.

IoT (Internet of Things)

IoT denotes small devices for specific purposes and limited hardware resources. Usually, they do not have extensive configuration options and are deployed in huge numbers and all communicate over the Internet. A big challenge here is how to patch them if security vulnerabilities are found. Most likely, these devices operate by your customers, who usually can't be forced to install a software update. Additionally, you might not even know the name of the customer using the device. As ownership and responsibilities are cornerstones of an ISMS, you will have to think about which provisions need to be made to your patch management process, incident management, and customer communication, just to name the most prominent areas.

Specific Cybersecurity Threats

There are a plethora of external threats to care about if you start making the cyberspace a part of your business model. Just to name a few, you should be prepared to deal with Denial of Service (DOS), Phishing, Clickjacking, Social Engineering and Backdoors. You should assess, whether you are vulnerable to those kinds of threats and what controls and measures would be appropriate to detect, mitigate and correct any impacts that might arise from the various attack vectors. Awareness and training, as well as incident management, are in the focus of adjustments in order to make your ISMS Cybersecurity ready.

Public Visibility of Incidents

If there is a security breach where many of your customers are involved, chances are high that you will not be able to keep it a secret for very long, due to the huge number of affected parties. Even attempting to keep an incident a secret might be a bad strategy, because you might appear as completely clueless. Additionally, your local legislation might require that you report a major security incident within a short defined timeframe to authorities. Thus, provisions to the incident handling process, business continuity management and communication plans with authorities, the press and customers need to be made.

Putting it all together, if you have an existing ISMS, it would be best to get ready for Cybersecurity by implementing the adjustments necessary through a project, that goes through the full PDCA cycle similar to an initial ISMS implementation project. The difference is that many processes and controls you will identify as necessary are already there, thus only the gap needs to be addressed.

https://pecb.com/article/how-to-integrate-isoiec-27032-cybersecurity-on-isms

For more information
The Arab International Society for Management Technology
Majd Farahat - Executive Director
Tel: (0962-6) 5100900- 1315
Fax: (0962-6) 5100901
info@aimict.org
AIMICT.org

This newsletter is published by:
The Arab International Society for Management Technology