Zámbó Gergely
1986.02.17
zgergely0217@gmail.com
+3630-2671225

Dear Recruitment Team!

My current workplace is at Hungarian Defense Forces, Air Operation Command and Control Centre as an Information Security officer since 2017. My duties are mainly divided in three major tasks: Information Security (Infosec) of unclassified systems, Infosec of classified systems and crypto management of classified systems.

Considering the unclassified systems my role is to develop the units ISMS to be in compliance with the state new information security laws, and to prepare the unit for the authority's audit. The new ISMS documentation was based mainly on the ISO 27001:2013 standard. The process included developing a new risk management procedure, – based on ISO 27005 and MIL-STD 882 - and performing the risk analysis of all unclassified systems and deployment sites. With the new ISMS, a new structure was implemented, where all subunits were connected to the information security center. As the infosec officer, I was in charge of control, implementation and the audit of the system, leading the subunit's selected personal for the role.

In 2020, our regiment merged with another unit, and in this new organization I took role as deputy of the Unclassified systems information security manager. In this role I am representing the unit in authority audits, managing implementation of new software and hardware, improving controls and methods, and collecting materials for security incident investigation. My duties also include leading of the infosec awareness trainings, preparing materials, carry out courses and most importantly, as a reaction to security incidents, execute awareness checks and occasional courses. My focus in cybersecurity trainings is the user behavior, which has to include not just unit/company related information, but has to be relevant to the events of the personal usage of "electronic information systems", smart devices and recognizing risks, while suggesting easier and safer methods.

Management of Classified systems as part of my work duties has similar subtasks. My unit is using more than 30 classified systems, and after understanding the processes and state laws, I prepared a similar system documentation as with the unclassified systems, to be able to have same controls at all sites, within different systems. It included standardized document management, centralized authorization processes, new directive of reporting routes. This approach let us act as one in the eyes of the government authorities. Same standards were used to develop risk management procedures, the difference was in the methods, with unclassified systems every deployment site had separate risk analysis, while with classified systems, I took different approach, focusing on each single system, identifying hazards by this rule.

Crypto management includes cryptographic key management, crypto network installation in permanent and mobile sites, testing and installing new IP networks, and as deputy commander of the Information security center directing the daily tasks of 15 specialists.

According to standards, I am familiar with the ISO 27000 standard family and the military variants of it, including specialized ones, like TEMPEST standards and procedures. I have limited practice experience of other standards and guidelines like COBIT, ITIL, NIST and ITSEC, but I'm eager to extend it. I have CCNA R&S certification, however army has specialized units for these duties.

Many thanks for your time please don't hesitate to contact me in case more details or specified information is required.

Kind regards

Gergely Zámbó