

Does the Possession of ISO/IEC 27001 Certificate guarantee the Information Security, and why not?

Miran Novak, M. Sc., Informatika d.d., Vetrinjska ulica 2, 2000 Maribor, SLOVENIA

An organization must, in order to obtain the ISO/IEC 27001 certificate, fulfil plenty of security, organizational, human resources, common business, and other demands, which are thoroughly verified by certification authority, before certificate is granted. At that point, the process of certificate maintenance is starting, with annual audits, where organization must prove, that achieved level was successfully kept, and even improved. At a glance, the idea might appear, that fulfilling the standard's demands and running the certificate maintenance activities, shall guarantee a privilege of "peaceful sleeping". The paper is showing, that obtaining the ISO/IEC 27001 certificate represents a solid ground for keeping appropriate level of information security, but is far from assuring it by itself.