

Open Information Security Maturity Model

The Open Group information security management maturity model (**O-ISM3**) is [The Open Group](#) framework for managing information security. It aims to ensure that security processes in any organization are implemented so as to operate at a level consistent with that organization's business requirements. O-ISM3 defines a comprehensive but manageable number of information security processes sufficient for the needs of most organizations, with the relevant security control(s) being identified within each process as an essential subset of that process. ^[1]

History

The original motivation behind O-ISM3 development was to narrow the gap between theory and practice for information security management systems, and the trigger was the idea of linking security management and maturity models. O-ISM3 strove to keep clear of a number of pitfalls with previous approaches. ^[2]

The "project" (<https://www.opengroup.org/forum/security/infosecmanagement>) . looked at [Capability Maturity Model Integration](#), [ISO 9000](#), [COBIT](#), [ITIL](#), [ISO/IEC 27001:2013](#), and other

standards, and found some potential for improvement in several fields, such as linking security to business needs, using a process based approach, providing some additional details (who, what, why) for implementation, and suggesting specific metrics, while preserving compatibility with the most popular IT and security management standards.

Availability

The Open Group provides the standard "O-ISM3 v.20" (<https://publications.opengroup.org/c17b>) . free of charge.

References

1. *O-ISM3 v2.0 2018 p6*
2. *Siponen, Mikko (2002-08-24). Designing Secure Information Systems and Software: Critical evaluation of the existing approaches and a new paradigm. OULU 2002, 24 August 2002. Retrieved from <http://jultika.oulu.fi/files/isbn9514267907.pdf> .*

Retrieved from

"https://en.wikipedia.org/w/index.php?title=Open_Information_Security_Maturity_Model&oldid=1060665309"

WIKIPEDIA
