Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002

Proceedings of the 2020 IEEE International Conference on Information Technologies (InfoTech-2020)

September 2020

Veselin Monev,

Information security professional & doctoral student

ORGANISATIONAL INFORMATION SECURITY MATURITY ASSESSMENT BASED ON ISO 27001 AND ISO 27002

Problem:

- Organisations which operate an Information Security Management System (ISMS), based on ISO 27001, are required to measure its effectiveness and continuously improve it.
- There isn't a holistic methodology to systematically and efficiently measure the performance of the ISMS.

Solution:

- A practical methodology for the performance of a maturity assessment of an ISO 27001-based ISMS.

ISMS Maturity Assessment Methodology phases:

- PHASE 1: Assessment initiation
- PHASE 2: Appointing an assessment team
- PHASE 3: Assessment tool creation
- PHASE 4: Document review and interviews
- PHASE 5: Evaluation and recommendations
- PHASE 6: Reporting

ORGANISATIONAL INFORMATION SECURITY MATURITY ASSESSMENT BASED ON ISO 27001 AND ISO 27002

PHASE 1: Assessment initiation

- Competent individual to initiate the assessment.
- Obtaining support from management and other departments.
- Laying down the foundation for an ongoing ISMS Maturity Assessment Programme.

PHASE 2: Appointing an assessment team

- Information security and compliance experts to build the assessment team.
- Formal management mandate is highly recommended.
- External consultants to be involved if required.

PHASE 3: Assessment tool creation

- Manageable through MS Excel.
- ISO 27001 consists of 113 controls in Annex A and 25 subclauses (139 total).
- Used to enter information during the assessment
- Primary source for the final report on the maturity level.

PHASE 4: Document review and interviews

- Review of relevant InfoSec documents and other sources of information.
- Interview of individuals in relation to the established processes. The interviews help for understanding the processes with lower maturity level.
- Describing the current situation of the security controls.

ORGANISATIONAL INFORMATION SECURITY MATURITY ASSESSMENT BASED ON ISO 27001 AND ISO 27002

PHASE 5: Evaluation and recommendations

- Should be performed at the time of Phase 4, as well as afterwards.
- The maturity of every one of the 139 controls is evaluated on a scale 0-5 (see the maturity reference table on this page).
- Recommendations are provided to every control after consulting with ISO 27002, as well as other references with best practices.

Maturity level	Description	Short description
0	The requirement/control is not implemented. As a result, the overall risk is elevated.	*No control*
1	The requirement/control is partially implemented or is ad-hoc. It is not supported by documentation. The employees are not aware of their responsibilities. Deficiencies are not identified.	*Control is partially / ad-hoc implemented, and there is no documentation*
3	The requirement is implemented, and it is supported by adequate documentation. Employees are aware of their responsibilities. However, as periodic reviews of the control are not performed, its effectiveness is not measured.	*Control is implemented + there is documentation*
4	The requirement is implemented, and it is supported by adequate documentation. Employees are aware of their responsibilities. Periodic reviews of the control are performed and documented. However, the requirement and the related process is not actively being improved, and not all issues are being identified.	*Control is implemented + there is documentation + periodic compliance reviews*
5	The requirement is implemented, and it is supported by adequate documentation. Employees are aware of their responsibilities and proactively involved in the improvements. Periodic reviews of the control are performed and documented. Moreover, the requirement and the related process is actively being improved so that all issues can be addressed.	*Control is implemented + there is documentation + periodic compliance reviews + effectiveness reviews and improvements*

ORGANISATIONAL INFORMATION SECURITY MATURITY ASSESSMENT BASED ON ISO 27001 AND ISO 27002

PHASE 6: Reporting

- A maturity assessment report as a final product of the initiative.
- Includes metrics about the performance of the ISMS.
- Can also include a section about the level of compliance with ISO 27001.
- Includes interpretation of the assessment results.
- Includes recommendations for improvement of the ISMS.

Maturity Level	Controls #	Controls %
0	0	0.0%
1	10	7.2%
2	42	30.2%
3	54	38.8%
4	28	20.1%
5	5	3.6%
Total:	139	100.0%

Average maturity level:	**2.8**
Average maturity in %:	**56.6%**

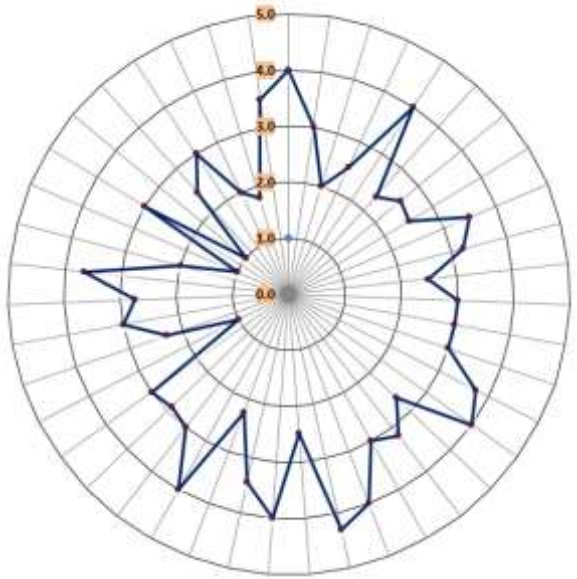
Total number of recommendations for improvement of the ISMS:	284

Number of recommended improvements per clauses and control groups							
Clauses	A5	A6	A7	A8	A9	A10	A11
30	5	15	14	21	19	12	35
	A12	A13	A14	A15	A16	A17	A18
	31	27	17	11	18	8	21

Number of subclauses and controls per maturity score							
Clauses	A5	A6	A7	A8	A9	A10	A11
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
12	0	2	0	2	1	1	1
8	1	3	6	4	6	1	5
3	1	2	0	4	7	0	7
1	0	0	0	0	0	0	2
	A12	A13	A14	A15	A16	A17	A18
	0	0	0	0	0	0	0
	1	0	6	2	1	0	1
	1	2	2	0	2	1	5
	11	4	3	3	4	3	0
	1	1	2	0	0	0	2
	0	0	0	0	0	0	0

Maturity Levels					
0	1	2	3	4	5
Non-existent	*Ad hoc*	*Intuitive*	*Defined process*	*Measurable process*	*Optimising process*

ISO 27001 compliance level achieved (The ISMS is certifiable):	NO



Questions?