ISO 27001 Gap Analysis

Excerpt from sample report

Protect • Comply • Thrive

Please note:

The below excerpts do not represent the entire report, and only provide a small sample of the information provided in the full report.

3.0 Executive summary

This assessment is based upon the scope of the organization operating from offices at a single physical location. The scope is further defined in section 4.

The organization is already certified against ISO 9001:2008 and ISO 14001:2004, and has previously implemented and certified against ISO 27001:2005.

Some aspects of the ISO 9001-based quality management system could be integrated with an information security management system (ISMS) based upon ISO 27001:2013.

In addition, some of the procedures and controls previously implemented for conformance with ISO 27001:2005 could be used with limited work to bring the related processes in line with the Standard's requirements.

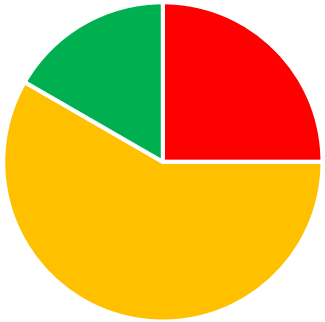
However, there are some fundamental processes that will require more work as follows:

- **Context of the organization** (ISO 27001 clause 4.0): Even though the context and scope of the ISMS are well understood and clear to the entire business, this needs to be documented in line with clauses 4.1 and 4.2, which require the organization to determine external and internal issues that are relevant to its purpose and to understand the needs and expectations of interested parties.
- The organization is implementing a system to provide document control and review notifications and reports in order to help drive continual improvement. It would satisfy clause 4.4 of ISO 27001, which requires the organization to **establish, implement, maintain and continually improve an ISMS.**

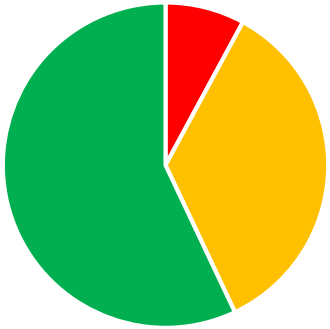
- **Asset management** (ISO 27001, Annex A, control reference A8): a priority for the organization is to identify what information assets it has and to include ownership and classification. An information classification policy exists, which should be reviewed in conjunction with handling of assets, implemented and communicated to meet the controls required in A8.2.
- Actions to address risks and opportunities (ISO 27001, clause 6.1): the organization will need to define a **risk assessment process.**

The following tables indicate the numbers of ISMS processes and information security controls that will require different levels of effort:

Management system:

Description	Color code	No of findings	Possible barriers to certification	Management system
Minimal effort	Green	4	0	
Some effort	Amber	14	12	
Significant effort	Red	6	6	

Information security controls (ISO 27001 Annex A):

Description	Color code	No of findings	Possible barriers to certification	Annex A controls
Minimal effort	Green	65	0	
Some effort	Amber	40	10	
Significant effort	Red	9	9	

None of these shortfalls are insurmountable, but addressing them will require management commitment to establish, implement, maintain and improve a comprehensive ISMS.

(Excerpt continues on next page)

7.0 Appendix A: Management system requirements – findings

Status key:

Green: Areas where minimal effort will be required to achieve compliance.

Amber: Areas where some effort will be required to achieve compliance.

Red: Areas that currently fall significantly short of the requirements of the Standard and where significant effort is required to achieve compliance.

Clause	What's already in place/working well	Areas requiring improvement	Status/level of work required	Possible barrier to certification?
4.1 Understanding the organization and its context	The organization can demonstrate its clear understanding of the organizational context and has determined the external and internal issues that are relevant.	Draft document in progress.		Yes
4.2 Understanding the needs and expectations of interested parties	The organization needs to identify interested parties.	Needs to be documented.		Yes
4.3 Determining the scope of the information security management system	Discussed in recent management review. The scope is defined and already understood.	Needs to be documented.		Yes
4.4 Information security management system	There are a number of documented policies in place but more effort may be required for documentation of processes and procedures.	Need to bring all required documentation together.		Yes
5 Leadership				

5.1 Leadership and commitment	ISO 9001 management review is in place. Strong leadership commitment has been demonstrated and the importance of information security is regularly communicated to all staff.			
5.2 Policy	An information security policy exists with other policies.	Review and update policy.		Yes
5.3 Organizational roles, responsibilities and authorities	A few roles identified; need to document all roles and list responsibilities and competences required.	Needs to be documented.		Yes
6 Planning				
6.1.1 General	Partially exists: context and objectives for the ISMS need to be fully defined.	Needs to be documented.		Yes
6.1.2 Information security risk assessment	Not in place; plan to implement a risk assessment process.	Risk assessment methodology identified in the management review meeting needs to be documented and risk assessment carried out.		Yes
6.1.3 Information security risk treatment	Not in place; plan to implement a risk assessment process.	Risk treatment to be carried out following risk assessment.		Yes
6.2 Information security objectives and planning to achieve them	Need to define objectives.	Need to define measurements and measurement structure. Describe the relationship between the measurements and overall ISMS objectives.		Yes

8.0 Appendix B: ISO 27001 Annex A controls - findings

Control	Title	Control question	Comments	Status/ level of work required	Possible barrier to certification?
6.1.2	**Segregation of duties**	Have conflicting duties and areas of responsibility been segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets?	Examples of controls in place where there is clear segregation of duties. Further documentation required.		No
6.1.3	**Contact with authorities**	Does the organization maintain appropriate contacts with relevant authorities?	The contact details for all relevant authorities are listed and made available to all members of staff.		No
6.1.4	**Contact with special interest groups**	Does the organization maintain appropriate contact with special interest groups or other specialist security forums and professional associations?	Nothing currently in place.		Yes
6.1.5	**Information security in project management**	Does the organization address information security in project management, regardless of the type of project?	Has NDAs, a consultancy procedure with several items that are related to information security but a review and further work is required.		No
6.2.1	**Mobile device policy**	Does the organization have a policy and supporting security measures to manage the risks introduced by the use of mobile devices?	Remote access and mobile computing policy and laptop policy. Check the policies are documented and available to all staff.		Yes