

ISO/IEC 27001:2013 SCOPE DEFINITION

Organization Information					
	Information Security Management System (ISMS) a. Briefly describe the departments of the organisation included in the ISMS.				
No.	Directorate / Department	Region	City	Brief description of business processes	
	ocument the human resou epartment they belong to.	rces that wi	ll be cove	ered by the ISMS according to th	
No.	Directorate / Department		Number	of staff	
c. H	ow many employees work ex	clusively with	information	on security in the Organization?	
d. Is	the organization certified a	ccording to a	nother ISC	standard (for example ISO20000-1	
IS	O9001, ISO22301)?				
e. W	/hen do you aim for the orgai	nization to be	certified?		





т.	Have you recently carried out a security risk assessment? If so, when and for what scope?

g. Have any or all of the following security policies been deployed?

Policies	✓ Yes ✓ No
Acceptable Use of Information Systems Policy	
2. Policy for the Acquisition, Development and	
Operation of Systems and Applications	
3. Internet Security and E-mail Policy	
4. Classification and Protection Policy for	
Information Resources	
5. Liaison Policy with Business Partners	
6. Human Resource Management Policy	
7. Business Continuity Management Policy	
8. Policy for Identifying Weaknesses and	
Conducting Security Audits	
9. Remote Access Policy	
10. Communications and Networks Policy	
11. Encryption Policy	
12. Information Systems Security Monitoring Policy	
13. User Access Policy	
14. Anti-Malware Policy	
15. Mobile Computer Systems and Teleworking	
Policy	
16. Physical and Environmental Safety Policy	
17. Security Incident Management Policy	





h. Have any or all of the following security procedures been developed?

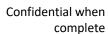
Pro	ocedure	✓ Yes ✓ No
1.	Change Management Process	
2.	Security Incident Management Process	
3.	Capacity Planning	
4.	Security Patch Management	
5.	Backup and Restore Process	
6.	Risk Management	
7.	Interna Audit / Corrective Actions	
8.	Security Monitoring Process	

i. Has an information security briefing been performed on the organization's staff for some or all of the following issues?

Areas	S	✓ Yes ✓ No
1. In	nternet and E-mail Security	
2. Se	ecurity Incident Management	
3. U	sing cryptography	
4. A	cceptable use of information systems	
5. N	Nalware protection	
6. D	ata protection	
7. Pl	hysical security	

j.	Do you maintain a register of information resources (asset register)?	
 k.	Are there any recorded internal information security service agreements between directorates or departments of the organization?	







Information Systems

I. Briefly describe the systems that make up the organization's information environment.

Servers (categories)	Applications
m. Briefly describe the organization's web	environment. If possible, include a network diagram.
n. Briefly describe the basic IT service infrastructure, IDS/IPS, firewalling, Act	e infrastructures (i.e. mail infrastructure, antivirus ive Directory, Wireless , etc).

