Comparison between ISO27001 and IASME

ISO 27001:2013	IASME Governance Standard 2016
1. Scope	0.1. General
	0.2. IASME's objectives
2. Normative references	3. Normative references
3. Terms and definitions	2. Glossary
4. Context of the organization — 4.1 Understanding the organization and its context	4.1. Understanding your risk profile - and defending it
	4.5. Businesses in more than one location
	6.1. Planning
	6.2. Organisation
4.2 Understanding the needs and expectations of interested parties	4.1. Understanding your risk profile - and defending it
	4.3. Showing customers, suppliers and yourself
	6.4. Assessing risks
4.3 Determining the scope of the information security management system	4.1. Understanding your risk profile - and defending it
4.4 Information security management system	0.3. Compatibility with other cyber and information security standards
	4.2. Implementation, orchestration, and adjustment
	7.1. Policy realisation
5. Leadership — 5.1 Leadership and commitment	6.2. Organisation
5.2 Policy	7.1. Policy realisation
5.3 Organizational roles, responsibilities and authorities	6.2. Organisation
6. Planning — 6.1 Actions to address risks	7.1. Policy realisation and opportunities
6.2 Information security objectives and planning to achieve them	6.1. Planning

7. Support	7.1 Resources	→	6.3. Assets
			6.6. People
	7.2 Competence	→	6.6. People
	7.3 Awareness	→	6.6. People
	7.4 Communication	→	4.3. Showing customers, suppliers and yourself
			6.6. People
	7.5 Documented information	→	5. Investing in cyber and information security with IASME

8. Operation	8.1 Operational planning and control	→	5. Investing in cyber and information security with IASME
			6.1. Planning
	8.2 Information security risk assessment	→	4.1. Understanding your risk profile - and defending it
			6.4. Assessing risks
	8.3 Information security risk treatment	→	7.1. Policy realisation
			7.2. Physical and environmental protection
			7.3. Secure business operations
			7.4. Access control
			8.1. Malware and technical intrusion
			9.1. Backup and restore
			9.2. Incident management
			9.3. Business continuity, disaster recovery, and resilience

9. Performance evaluation	9.1 Monitoring, measurement, analysis and evaluation	→	4.3. Showing customers, suppliers and yourself
			8.2. Monitoring - for healthy systems and unauthorized activity
	9.2 Internal audit	→	6.5. Legal and regulatory landscape
			7.1. Policy realisation
	9.3 Management review	→	6.2. Organisation
			7.1. Policy realisation

10. Improvement	10.1 Nonconformity and corrective action	→	6.5. Legal and regulatory landscape
			9.2. Incident management
	10.2 Continual improvement	→	4.2. Implementation, orchestration, and adjustment
			4.4. Who watches the watchmen