ISO 27001:2013 Quick Reference

ISO 27001:2013 Clauses	Summary of Requirements
4. Context of the organization	
4.1 Understanding the organization and its context	Internal issues; external issues; intended outcomes of ISMS
4.2 Understanding the needs and expectations of interested parties	Interested parties relevant to ISMS; Requirements relevant to information security
4.3 Determining the scope of the ISMS	Boundaries and applicability of ISMS; consider 4.1 and 4.2;
	Interfaces and dependencies; documented scope
4.4 Information security management system	Establish, implement, maintain, continually improve ISMS
5. Leadership	
5.1 Leadership and commitment	Policy and objectives compatible with strategic direction;
	Integration; resources; importance; outcomes; direct; support;
	Promote improvement; demonstrate leadership
5.2 Policy	Appropriate, framework; objectives; information security;
	Documented policy; communicated; available
5.3 Organizational roles, responsibilities, and authorities	Assigned; communicated; performance reporting
6. Planning	
6.1 Actions to address risks and opportunities	
6.1.1 General	Issues (4.1); requirements (4.2); determine risks;
	Prevent or reduce undesired effects; achieve improvement;
	Plan actions; address risks; integrate actions; evaluate actions
6.1.2 Information security risk assessment	Risk criteria; risk identification; risk owners; risk levels;
	Possible consequences; realistic likelihood; risk prioritization
6.1.3 Information security risk treatment	Treatment options; risk controls; use of Annex A;
	Statement of Applicability; treatment plan; risk owner approval
6.2 Information security objectives & planning to achieve them	Objectives; functions and levels; consistent with policy;
	Measureable; considers risk assessment and treatment;
	Communicated; updated; planning of what, who, when, how
7. Support	
7.1 Resources	Resources to establish, implement, maintain, improve ISMS
7.2 Competence	Education; training; experience; action; competency evidence
7.3 Awareness	Policy; objectives; contributions; implications of nonconformity
7.4 Communication	What; when; with whom; how; who communicates; process
7.5 Documented information	
7.5.1 General	Required by ISO 27001; determined by organization
7.5.2 Creating and updating	Identification; description; format; media; approvals
7.5.3 Control of documented information	Available; suitable; protected from loss or improper use;
	Access; use; storage; version control; retention; disposition;
	Documents of external origin; identified; controlled

ISO 27001:2013 Quick Reference

ISO 27001:2013 Clauses	Summary of Requirements
8. Operation	
8.1 Operational planning and control	Plan, implement, control processes; implement risk actions;
	Documented information; control changes; outsourcing
8.2 Information security risk assessment	Perform risk assessments; retain records of results
8.3 Information security risk treatment	Implement risk treatment plan; retain records of results

9. Performance evaluation	
9.1 Monitoring, measurement, analysis, and evaluation	Information security performance; effectiveness of ISMS
	What monitored and measured; methods for valid results;
	When done; who does; when results analyzed and evaluated;
	Records retained as evidence of results
9.2 Internal audit	Planned intervals; conformity to requirements; effectiveness;
	Audit program; frequency; methods; responsibilities; reporting;
	Audit criteria; scope; impartial, objective auditors and audits;
	Results to management; records of program and audit results
9.3 Management review	Planned intervals; action status; issue changes; performance;
	Trends: NCs, CAs, measurements; audit results; objectives;
	Interested parties; risk assessments; risk treatments;
	Decisions; changes; improvements; records of review results

10. Improvement	
10.1 Nonconformity and corrective action	React; correct; deal with consequences; eliminate causes;
	Similar NCs; take action; review effectiveness; change ISMS;
	Records of nonconformities; actions taken; results of actions
10.2 Continual improvement	Improve suitability, adequacy, and effectiveness of ISMS

This reference is a quick clause-by-clause summary of the ISO 27001:2013 requirements. See the actual ISO 27001:2013 standard for a complete description of the requirements.

Contact Whittington & Associates, LLC at 770-862-1766, or by e-mail at <Larry@WhittingtonAssociates.com>.