Integrated Audit Criteria for ISO 27001:2022, ISO 27001:2013 and ISO 9001:2015

eQual assurance

Audit Criteria		ISO 27001:2022 (ER)	ISO 27001:2013 (ER)	ISO 9001:2015 (CQ)
3.1 General		1 Scope 2 Normative references 3 Terms and definitions	1 Scope 2 Normative references 3 Terms and definitions	1 Scope 2 Normative references 3 Terms and definitions
3.2 Context	3.2.1 Organizational context	4.1 Understanding the organization and its context	4.1 Understanding the organization and its context	4.1 Understanding the organization and its context
	3.2.2 Needs and expectations of interested parties	4.2 Understanding the needs and expectations of interested parties	4.2 Understanding the needs and expectations of interested parties	4.2 Understanding the needs and expectations of interested parties
	3.2.3 Management system	4.3 Determining the scope of the information security management system 4.4 Information security management system	4.3 Determining the scope of the information security management system 4.4 Information security management system	4.3 Determining the scope of the quality management system 4.4 Quality management system and its processes
3.3 Leadership	3.3.1 Leadership and commitment	5.1 Leadership and commitment	5.1 Leadership and commitment	5.1 Leadership and commitment
	3.3.2 Policy	5.2 Policy	5.2 Policy	5.2 Policy
	3.3.3 Roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities
3.4 Planning	3.4.1 Risks and opportunities	6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities
	3.4.2 Objectives and related planning	6.2 Information security objectives and planning to achieve them 6.3 Planning of changes	6.2 Information security objectives and planning to achieve them	6.2 Quality objectives and planning to achieve them 6.3 Planning of changes
3.5 Support	3.5.1 Resources	7.1 Resources	7.1 Resources	7.1 Resources
	3.5.2 Competence	7.2 Competence	7.2 Competence	7.2 Competence
	3.5.3 Awareness	7.3 Awareness	7.3 Awareness	7.3 Awareness
	3.5.4 Communication	7.4 Communication	7.4 Communication	7.4 Communication
	3.5.5 Documented information	7.5 Documented information	7.5 Documented information	7.5 Documented information
3.6 Operation	3.6.1 Operational planning and control	8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment	8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment	8.1 Operational planning and control 8.2 Requirements for products and services 8.3 Design and development of products and services 8.4 Control of externally provided processes, products and services 8.5 Production and service provision 8.6 Release of products and services
	3.6.2 Emergency preparedness and response	N/A*	N/A*	8.7 Control of nonconforming outputs
3.7 Performance	3.7.1 Measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation
	3.7.2 Internal audit	9.2 Internal audit	9.2 Internal audit	9.2 Internal audit
	3.7.3 Management review	9.3 Management review	9.3 Management review	9.3 Management review
3.8 Improvement	3.8.1 Nonconformity and corrective action	10.2 Nonconformity and corrective action	10.1 Nonconformity and corrective action	10.1 (Improvement) General 10.2 Nonconformity and corrective action
	3.8.2 Continual improvement	10.1 Continual improvement	10.2 Continual improvement	10.1 (Improvement) General 10.3 Continual improvement

* Some criteria do not have a direct corresponding clause to that Standard (denoted as "N/A"). This does not necessarily imply that such requirements do not exist, but that where and to the extent they do, they have been integrated into other requirements of that Standard.