



Competency Unit:

**RABQSA-IS –Information Security Management Systems**

Effective date: February 2006

Competency	Performance Criteria	Evidence Guide
<p>1: Understand the application of an Information Security Management System in the context of ISO27001:2005.</p>	<p>1.1 The intent and requirements of each clause of ISO27001:2005 can be described in the context of a given business/industry sector.</p> <p>1.2 The relationship between the OECD (Organization for Economic Co-operation and Development) Guidelines for the Security of Information Systems and Networks ("the Guidelines"), as summarized in Annex B of ISO27001:2005, and the Standard itself is explained within the context of a given business/industry sector.</p> <p>1.3 The documentation required by ISO27001:2005 and the interrelationships between the documented Information Security Management System (ISMS), ISMS planning, risk assessment, policy, objectives and controls are explained within the context of a given business/industry sector.</p> <p>1.4 Evidence needed to demonstrate conformity to the requirements of ISO27001:2005 is identified.</p> <p>1.5 Information Security terminology and sector-specific terminology is correctly used.</p> <p>1.6 The effectiveness of the entire ISMS, including the Plan, Do, Check, Act (PDCA) process approach used to develop, implement and improve the effectiveness of the ISMS, and continual monitoring and improvement is evaluated within the context of a given</p>	<p>The intent and requirements of ISO27001:2005 are defined, without error, giving examples for specific business/industry sectors.</p> <p>The relationship between the OECD Guidelines and the requirements defined in ISO27001:2005 is accurately defined, giving examples for specific business/industry sectors.</p> <p>The documentation required for conformity to ISO27001:2005 is defined, with omission or deviation justified.</p> <p>Interrelationships between documentation required for conformity to ISO27001:2005 such as ISMS planning, risk assessment, controls, policy and objectives are accurately defined, giving examples for specific business/industry sectors.</p> <p>Differing requirements for documentation in a variety of organizational situations are accurately defined.</p> <p>Audit evidence to demonstrate conformity to the clauses of ISO27001:2005 is identified, with omission or deviation justified, giving examples for specific business/industry sectors.</p> <p>The principles and practices of auditing ISO27001:2005 and related standards are accurately described.</p> <p>Correct terminology for ISMS audit reporting is demonstrated.</p> <p>Evidence required to demonstrate operational effectiveness of a documented ISMS is defined, using ISO27001:2005 as the reference, with omission or deviation justified, giving examples for specific business/industry sectors.</p> <p>Information included in an audit report to ensure that it accurately reflects the requirements of ISO27001:2005 is accurately defined, giving examples of specific business/industry sectors.</p> <p>The need to identify sensitive issues and to report these with</p>



Competency Unit:

**RABQSA-IS –Information Security Management Systems**

Effective date: February 2006

Competency	Performance Criteria	Evidence Guide
	<p>business/industry sector.</p> <p>1.7 Audit reference documentation is suitable and appropriate to the requirements of ISO27001:2005 in the context of the auditee business size, industry, environment and sensitivity.</p> <p>1.8 The relationship between legal compliance and ISO27001:2005 is demonstrated in the context of an ISMS audit in a given business/industry sector.</p>	<p>appropriate confidentiality is defined.</p> <p>The difference between legal compliance and conformity with ISO 27001:2005 requirements, in the context of an ISMS audit, is accurately defined.</p>
<p>2: Understand the relationship of the ISMS, including risk assessment and controls, to information assets belonging to the organization, its customers, and partners.</p>	<p>2.1 The relationship of a documented ISMS and information assets belonging to an organization, its customers and partners is explained.</p> <p>2.2 Risk assessment methodologies to identify risks are evaluated to verify the degree of conformity and effectiveness in identifying risks associated with information security.</p> <p>2.3 Controls implemented to manage identified risks are explained in different organizational contexts.</p>	<p>The relationship between a documented ISMS and information assets included under the scope of the ISMS is accurately defined, giving examples for specific business/industry sectors.</p> <p>Risk assessment methodologies appropriate to the evaluation of risk in specific business/industry sectors are accurately described in accordance with ISO27001:2005.</p> <p>Controls appropriate for the management of identified risks are accurately defined, giving examples for specific business/industry sectors.</p>