



Competency Unit:

RABQSA-SCY – Security Management Systems Auditing

Effective date: January 2007

Competency	Performance Criteria	Evidence Guide
1. Understand requirements of management systems.	1.1 The documentation required for an effective management system is described.	Management system documentation requirements are defined in accordance with ISO/PAS 28000:2005 clauses 4.1 (general requirements) and 4.4.4 (documentation)
	1.2 The interrelationships between the management system manual, procedures, planning, policy, and objectives are explained within the context of a given business/industry sector.	Interrelationships between the various levels of documentation are described in accordance with ISO/PAS 28000:2005 clauses 4.1 (general), 4.2 (policy), and 4.3 (security risk assessment planning)
	1.3 The benefits of using the process approach to develop, implement and improve the effectiveness of a management system, customer focus and continual improvement are described, within the context of a given business/industry sector.	The process approach to development of management systems is described in accordance with ISO/PAS 28000:2005 Introduction
	1.4 The importance of planning and resourcing a management system is described.	Requirements for planning and resourcing a management system are described in accordance with ISO/PAS 28000:2005 clauses 4.3.1 d) (risk assessment) and 4.4.1 d) (structure authority & responsibilities for security management)
2. Understand how to determine the adequacy and effectiveness of a management system.	2.1 Methods to evaluate the effectiveness of an entire management system are described, within the context of a given business/industry sector.	Requirements for Management Review are described in accordance with ISO/PAS 28000:2005 clause 4.6 (management review and continual improvement)
	2.2 Appropriate verification procedures to establish the currency, relevance, and effectiveness of a management system are described.	Requirements for Internal Audit are described in accordance with ISO/PAS 28000:2005 clauses 4.5.2 (systems evaluation) and 4.6 (management review and continual improvement)



Competency Unit:

RABQSA-SCY – Security Management Systems Auditing

Effective date: January 2007

Competency	Performance Criteria	Evidence Guide
	2.3 Omissions in a management system that could affect security are identified.	Critical omissions are defined in accordance with ISO/PAS 28000:2005 clauses 4.3 (security risk assessments) and 4.5.2 (systems evaluation)
	2.4 The adequacy of a management system in preventing, reducing, or eliminating security hazards is described.	System adequacy is defined in accordance with ISO/PAS 28000:2005 clauses 4.5.1 (security performance measurement and monitoring) and 4.5.2 (systems evaluation)
3. Understand requirements and methods for ensuring continuous improvement.	3.1 The impact of continuous improvement processes on management systems is described.	Continuous improvement processes are described in accordance with ISO/PAS 28000:2005 clause 4.6 (management review and continual improvement)
	3.2 The role of continuous improvement in identification of preventive actions is described.	Methods for identification of preventive actions are described in accordance with ISO/PAS 28000:2005 clause 4.6 (management review and continual improvement)
4. Understand legislative requirements, industry codes and regulations that are applicable to security management.	4. The appropriateness and effectiveness of controls based on legislative requirements, industry codes, and other technical information relevant to security management are defined.	Methods to identify legal and other requirements applicable to security management are described in accordance with ISO/PAS 28000:2005 clause 4.3.2 (legal, statutory and other security regulatory requirements)
5. Understand the elements of risk management as defined in AS4360:1999.	5.1 The main elements of risk management are defined.	The elements of risk management are described in accordance with AS4360:1999 clause 3.2 a) to g) and ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment)
6. Understand the processes of risk management.	6.1 Requirements for establishing the contexts of risk management processes are described.	The range of contexts of risk management and methods used to establish these contexts are described in accordance with AS4360:1999 clauses 4.1.1 to 4.1.4 and ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment)

Competency	Performance Criteria	Evidence Guide
	6.2 Requirements for developing risk evaluation criteria of risk management processes are described.	Methods used to develop risk evaluation criteria are described in accordance with AS43601999 clause 4.1 and ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment)
	6.3 The structure and interrelationships of risk management processes is defined.	Structure of risk management is described in accordance with AS43601999 clause 4.1.6 Interrelationships of risk management processes are described in accordance with AS4360:1999 Figure 4.1
7. Understand the processes of risk identification.	7.1 Requirements to identify risks to be managed are described.	Methods used to identify risks to be managed are described in accordance with AS4360:1999 clause 4.2 and ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment)
8. Understand the processes of risk analysis.	8.1 Requirements used to analyse risks are described.	Methods used to analyse risks are described in accordance with AS43601999 clause 4.3 and ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment). Examples of risk definition and classification methods, such as described in AS4360:1999 Appendices E & F, are demonstrated.
9. Understand the processes of risk evaluation.	9.1 Requirements for evaluation of risks are described.	Methods used to evaluate risks are described in accordance with AS4360 clause 4.4 and ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment)
10. Understand the processes of risk treatment.	10.1 Requirements for treatment of risks are described.	Methods used to treat risks are described in accordance with AS4360 clause 4.5 and ISO/PAS 28000:2005 clauses 4.3. (security risk assessment planning); 4.5 (checking and corrective action)
11. Understand the processes of monitoring	11.1 Requirements for monitoring and reviewing risks are described.	Methods used to monitor and review risks are described in accordance with AS4360 clause 4.6 and ISO/PAS 28000:2005



Competency Unit:

RABQSA-SCY – Security Management Systems Auditing

Effective date: January 2007

Competency	Performance Criteria	Evidence Guide
and reviewing risks.		clause 4.5 (checking and corrective action)
12. Understand the process of communication and consultation.	12.1 Requirements for communication and consultation at each step of the risk management process are described.	Methods used for communication and consultation in relation to risks are described in accordance with AS4360:1999 clause 4.7
13. Understand the reasons for documentation in the risk management process as defined in AS4360:1999.	13.1 Reasons for documentation related to risk management are described.	Documentation requirements are described in accordance with AS4360:1999 clauses 5.1 and 5.2
14. Understand general requirements for operational security.	14.1 Functional understanding of major operational security elements that will be encountered while undertaking security management system audits is demonstrated. This includes awareness of key assessment criteria and appropriate control applications associated with each element type.	<p>Typical risks associated with the following areas are identified and assessed with appropriate security controls described:</p> <p>Asset protection Industrial Commercial Domestic Crisis management</p> <p>Loss prevention Fraud Theft IP protection</p> <p>IT and electronic systems Systems design and access Storage and handling of data Analysis of data</p> <p>Personnel protection VIP protection Employee protection</p>



Competency Unit:

RABQSA-SCY – Security Management Systems Auditing

Effective date: January 2007

Competency	Performance Criteria	Evidence Guide
		General public protection Transport and logistics Maritime Aircraft Land transport Terminals Handling facilities
15. Understand roles and responsibilities for security management.	15.1 The roles and responsibilities of personnel responsible for security are clearly identified.	Typical roles and responsibilities for security are described in accordance with ISO 27001:2005 clause 5.1c) and ISO/PAS 28000:2005 clause 4.4.1 (structure, authority, roles and responsibilities of security management)
	15.2 The inter-relationship between the security hierarchy and the corporate organizational structure is defined.	Appropriate organizational structures to ensure effective inter-relationships between the security hierarchy and corporate organisation are described with reference to ISO 27001:2005 clause 4.2.1 a) and b) and ISO/PAS 28000:2005 clause 4.4.1 (structure, authority, roles and responsibilities of security management)
	15.3 Barriers to the effective implementation of a security management system are identified and methods to eliminate these barriers are described.	Limitations to effective implementation of a security management system are described as detailed in ISO/PAS 28000:2005 clause 4.3.1 (security risk assessment)

ISO/PAS 28000:2005 references for evidence guide

<i>Clause</i>	<i>Name</i>	<i>Coverage</i>
4.1	General requirements	Establishment of system structure, continual improvement,
4.2	Security policy	Developed / acknowledged by top management
4.3	Risk Assessment and Planning	
4.3.1	Security Risk Assessment	Physical, operational, environmental threats and risks
4.3.2	Legal, statutory and other security regulatory requirements	Identify legal and other requirements related to organization
4.3.3	Security management objectives	Establish and document management objectives
4.3.4	Security management targets	Establish measurable, relevant targets communicated to the organization
4.3.5	Security management programs	Establishment, documented programs
4.4	Implementation	
4.4.1	Structure, authority & responsibilities for security management	Establish / appoint, organization roles, responsibilities authorities
4.4.2	Competence, training and awareness	System to ensure qualified competent personnel
4.4.3	Communication	System to communicate information to the organization
4.4.4	Documentation	Policy objectives, scopes, references, records,
4.4.5	Document and data control	Location and access, review, currency, archival
4.4.6	Operational control	Documented procedures, threat evaluation,
4.4.7	Emergency preparedness, response and security recovery	Identify potential threats, develop plans, responses,
4.5	Checking and Corrective action	
4.5.1	Security performance measurement and monitoring	Qualitative, quantitative, monitoring objectives & targets, non conformances
4.5.2	System evaluation	Review plans, procedures, incidents reports, performance evaluations
4.5.3	Security related failures, incidents, non-conformances and corrective and preventative actions	Evaluating system failures, incidents, near misses, false alarms, near misses
4.5.4	Control of records	Identification, storage, protection, retrieval, retention disposal of records
4.5.5	Audit	Develop an audit program
4.6	Management review and continual improvement	Review of system by top management.