6.2 IT/Technology Security Management

Discipline Description

This sub-discipline is about the competencies required to ensure the security of all aspects of Information Technology services, systems and assets within an organisation. This includes the data, information, processes, people and other resources needed to ensure that Information Technology can operate.

.

Pre-Entry / Junior Technician Role:

Competence 6.2.J.1 – Carry out specified IT/technology Security Management activities

This competence will be demonstrated by the following **Performance Criteria (6.2.J.1.C.):**

a) Correctly follow the processes, tools and techniques relating to IT/technology security management activities

b) Correctly operate with reference to integrity, confidentiality and professional and ethical standards in IT/technology security management activities,

c) Comply with all relevant and applicable legislation, regulations, strategy, policies, procedures and standards relating to the management of IT/technology security

Competent performance requires **Knowledge (6.2.J.1.K.)** of how to:

a) Apply the processes, tools and techniques relating to IT and other technology security management activities

b) Comply with all relevant and applicable legislation and regulations relating to the management of IT/technology security

c) Comply with all strategy, policies, procedures and standards relating to IT security management within an organisation

d) Operate with reference to organisational strategy, policies and standards in IT and other technology security management activities

e) Operate with reference to professional and ethical standards relating to IT/technology security management activities and their deliverables

f) Operate with integrity and confidentiality in IT and other technology security management activities

Competent performance requires **Understanding (6.2.J.1.U.)** of:

a) what is meant by IT/technology security management

b) the potential implications of IT/technology security failures on an organisation

c) the potential implication of IT/technology security failures on external bodies and individuals

d) the potential implications of IT/technology security management activities being incorrect, incomplete, inadequate and /or inappropriate

e) the rules and regulations relating to IT/technology security within an organisation

f) the fact that many aspects of an organisation's security strategy and functions rely upon IT/technology systems, services and assets and/or information contained within them

Competence 6.2.J.2 – Document specified IT/technology Security Management activities

This competence will be demonstrated by the following **Performance Criteria (6.2.J.2.C.):**

a) Accurately gather, collate and document specified information and data resulting from IT/technology security testing activities

b) Assist others in documenting the processes and procedures to ensure the security of data, knowledge, information and IT/technology systems, services and assets as used both within an organisation and also as it is exchanged between it and external bodies and individuals

c) Assist others in documenting how the levels and structure of security measures are reflected in IT/technology security controls and mechanisms and how these controls and mechanisms mitigate against business threats, risks and vulnerabilities

Competent performance requires **Knowledge (6.2.J.2.K.)** of how to:

a) Collate information and data resulting from IT/technology security testing activities

b) Document, complete and store the results of IT/technology security testing

Competent performance requires **Understanding (6.2.J.2.U.)** of:

a) the processes, tools and techniques that can be used to conduct and document IT and other technology security management activities

b) the importance of documenting the deliverables from IT and other technology security management activities in a clear and understandable manner

c) the importance of providing education, communications and training relating to the effective security of data, knowledge, information and the IT/technology systems, security and assets to sponsors, stakeholders and external bodies and individuals as appropriate

d) the importance of ensuring clear, effective and empathetic communication with external bodies and individuals impacted by IT/technology security breaches

Associate Professional Role:

Competence 6.2.A.1 – Contribute to IT/technology security management activities

This competence will be demonstrated by the following **Performance Criteria (6.2.A.1.C.):**

a) Correctly apply the process, tools and techniques relating to IT/technology security management activities

b) Comply with IT/technology security procedures, controls and mechanisms

Competent performance requires **Knowledge (6.2.A.1.K.)** of how to:

a) complete the processes and procedures to ensure the security of data, knowledge, information and IT/technology systems, services and assets as used both within an organisation and also as it is exchanged between it and external bodies and individuals

Competent performance requires **Understanding (6.2.A.1.U.)** of:

a) What constitutes a breach of IT/technology security

b) What are the other organisational security functions that rely upon IT/technology systems, services and assets or secured information contained within them

c) What are the types of threats and risks that an organisation needs to be protected from by IT/technology security systems, services and assets of information contained within them

d) What are the implications of other organisational security functions relying upon IT technology systems, services and assets or information contained within them

e) What are the risks and threats to IT/technology security

f) The importance of ensuring that external bodies and individuals who exchange information with an organisation are familiar with and comply with IT/technology security procedures, controls and mechanisms

g) The fact that risks and threats to information, data, knowledge IT/technology systems, services and assets can also arise through the actions of individuals who lack security awareness

h) The fact that certain types of risks and threats to the security of information, data, knowledge and IT/technology systems, services and assets are commonly designed, developed and implemented with malicious intent

i) The fact that risks and potential threats to IT/technology systems, services and assets and/or information contained within them are constantly being developed and introduced

j) The fact that IT/technology security needs to be refreshed to keep it current with the range of risks and threats that exist

k) The need for monitoring of compliance with internal rules and regulations relating to organisational security strategy

Competence 6.2.A.2 – Document IT/technology security management processes

This competence will be demonstrated by the following **Performance Criteria (6.2.A.2.C.):**

a) Accurately and comprehensively document the processes and procedures to ensure the security of data, knowledge, information and IT/technology systems services and assets as used both within an organisation and also as it is exchanged between it and external bodies and individuals

b) Correctly document how the levels and structure of security measures are reflected in IT/technology security controls and mechanisms and how these controls and mechanisms mitigate against business threats, risks and vulnerabilities

Competent performance requires **Knowledge (6.2.A.2.K.)** of how to:

a) document the internal and external criteria that IT/technology security management activities need to meet

b) document how the levels and structure of security measures are reflected in IT/technology security controls and mechanisms

c) document how IT/technology security controls and mechanisms mitigate against business threats, risks and vulnerabilities

Competent performance requires **Understanding (6.2.A.2.U.)** of:

a) The importance of verifying the accuracy, currency, completeness and relevance of information collected, produced, used and stored by IT and other technology security management activities

Competence 6.2.A.3 – Assist the management with IT/technology security systems

This competence will be demonstrated by the following **Performance Criteria (6.2.A.3.C.):**

a) Provide timely and complete information relating to IT/technology security controls and mechanisms and how they mitigate against risks, threats and vulnerabilities for inclusion in business risk registers, risk assessments, vulnerability and threat assessments, to a range of internal and external individuals

b) Assist others in identifying any possible breaches of IT/technology security

c) Assist others in identifying and applying a range of appropriate security controls and mechanisms for IT/technology systems, services and assets

Competent performance requires **Knowledge (6.2.A.3.K.)** of how to:

a) Provide information relating to IT/technology security controls and mechanisms and how they mitigate against risks, threats and vulnerabilities for inclusion in business risk registers, risk assessments, vulnerability and threat assessments

Competent performance requires **Understanding (6.2.A.3.U.)** of:

a) The importance of the levels of protection that are appropriate to the needs and activities of the business, the individuals operating within it and the external bodies and individuals exchanging information with an organisation are provided by IT and other technology security controls and mechanisms

b) The importance of taking appropriate action in the event of IT/technology security breaches to contain and mitigate their impact

Professional Role:

Competence 6.2.P.1 – Manage the IT/technology security requirements

This competence will be demonstrated by the following **Performance Criteria (6.2.P.1.C.):**

a) Accurately identify who are the business authorities for IT/technology security management activities and measures

b) Correctly identify and verify the business external criteria and requirements that IT/technology security management activities and measures need to meet

c) Promptly identify any possible breaches of IT/technology security, taking action and escalating where appropriate to superiors

d) Accurately identify the levels and structure of security measures that need to be reflected in IT/technology security controls in order to reflect how the business operates, in line with policies and procedures

Competent performance requires **Knowledge (6.2.P.1.K.)** of how to:

a) Identify:

- and select the business and external criteria and requirements that IT/technology security management activities and the measures need to meet
- and select the levels and structure of security measures that need to be reflected in IT/technology security controls in order to reflect how the business operates
- who are the business authorities for IT/technology security management activities and measures
- a range of appropriate security controls and mechanisms for IT/technology systems, services and assets
- possible breaches of IT/technology security

b) Collate information about external bodies and individuals and/or their access to information that may need to be kept secure

c) Collate information about external bodies and individuals and/or their access to information that may need to be kept secure

d) Source information about the levels of security that need to be implemented in order to reflect the structure of the organisation and /or access to information, data or knowledge within it

e) Gather internal and external intelligence relating to IT/technology security risks and threats that may impact on an organisation

Competent performance requires **Understanding (6.2.P.1.U.)** of:

a) What are:

- the IT/technology systems, services and assets and the information within them that need to be kept secure
- the range of IT and technology considerations such as information, data, knowledge, processes, people and other systems, services and assets that need to be made secure within an organisation

- the legislation, regulations and external standards relating to IY and other technology security management within an organisation
- the potential implications and sensitivities associated with communication with external bodies and individuals in the event of IY and other technology security breaches

b) The fact that:

- effective IT/technology security management is critical to the well being and success of the organisation
- IT and other technology security needs to be refreshed as IT/technology systems, services and assets within an organisation are added, enhanced or decommissioned, as the business use of the changes and/or the individuals using them change
- IT/technology security measures can become quickly outdated
- there are external providers of IT and other technology security management services and the disadvantages and benefits of using them
- IT/technology security management activities must comply with legislation, regulations and external standards

c) Why:

- IT and other technology security within an organisation needs to be monitored
- IT/technology security within an organisation needs to be tested regularly
- the organisation's IT/technology security may need to support privacy requirements

d) Who are the sponsors of and stakeholders for any IT and other technology security management activities

e) The need for monitoring of compliance with legislation, regulations and standards relating to IT/technology security

f) The need for monitoring the effectiveness and quality of IT/technology security management activities

g) The processes, tools and techniques that can be used to monitor IT security within an organisation

Competence 6.2.P.2 – Carry out IT/technology security management activities

This competence will be demonstrated by the following **Performance Criteria (6.2.P.2.C.):**

a) Correctly apply all processes, tools and techniques relating to IT/technology security management activities

b) Correctly identify and apply a range of appropriate security controls and mechanisms for IT/technology systems, services and assets

c) Source and document, clearly and precisely, all relevant and required information about the internal and external individuals and external bodies and/or their access to information that may need to be kept secure

d) Routinely gather internal and external intelligence relating to IT/technology security risks and threats that may impact on an organisation

Competent performance requires **Knowledge (6.2.P.2.K.)** of how to:

a) Select the processes, tools and techniques relevant to the management and monitoring of the security of IT/technology

b) Apply the processes, tools and techniques relating to IT and other technology security management activities

c) Verify the internal and external criteria and requirements that IT/technology security management activities need to meet

d) Use a range of appropriate security controls and mechanisms for IT/technology systems, services and assets

e) Complete, document and store information and data relating to the individuals within the organisation, their information and/or their access to information that may need to be kept secure

f) Complete, document and store information and data relating to the external bodies and individuals their information and/or their access to information that may need to be kept secure

g) Document the deliverables from IT and other technology security management activities in a clear and understandable manner

Competent performance requires **Understanding (6.2.P.2.U.)** of:

a) The importance of :

- testing IT/technology security controls and mechanisms regularly to ensure they remain current, accurate, complete and relevant and provide an appropriate level of protection to an organisation
- maintaining integrity and confidentiality during IT and other technology security management activities
- having business processes and procedures to prevent and respond to security breaches that are effective and well understood by individuals within an organisation, external bodies and individuals
- IT/technology security management aligning with and supporting organisational security strategy, policies, processes, procedures, standards and requirements
- communicating an organisation's IT/technology security approach and standards to external bodies and individuals
- IT/technology security on the full life cycle of information within an organisation
- having an IT/technology security plan
- taking appropriate action to identify, anticipate and mitigate potential security threats

Senior Professional Role:

Competence 6.2.S.1 – Control the management of IT/Technology Security activities

This competence will be demonstrated by the following **Performance Criteria (6.2.S.1.C.):**

a) Correctly identify the levels of security that need to be implemented in order to reflect the structure of the organisation and/or access to information, data or knowledge within it

b) Implement and effectively maintain all relevant processes, tools and techniques, relating to IT/technology security management activities

c) Use relevant information contained within risk registers, risk assessments and vulnerability assessments, and internal and external intelligence relating to IT/technology security risks and threats that may impact on an organisation during IT/technology security management activities

d) Accurately document all relevant IT/technology security management plans, responsibilities, controls and mechanisms

e) Develop and deploy effective IT/technology security controls and mechanisms to identify possible and actual security breaches, escalating where appropriate to superiors

Competent performance requires **Knowledge (6.2.S.1.K.)** of how to:

a) Identify and select information about:

- the individuals within the organisation and/or their access to information that may need to be kept secure
- external bodies and individuals and/or their access to information that may need to be kept secure

b) Identify:

- the levels of security that need to be implemented in order to reflect the structure of the organisation and/or access to information, data or knowledge within it
- the sponsors of and stakeholders for any IT and other technology security management activities
- a range of appropriate approaches to undertake IT and other technology security management activities, in a variety of individual business, IT and technology contexts

c) Verify:

- that the levels and structure of security measure in IT/technology security support how the business operates and secures the information contained within its IT/technology systems, services and assets
- the individuals within the organisation, their information and/or their access to information that may need to be kept secure

- the external bodies and individuals, their information and/or their access to information that may need to be kept secure
- the accuracy, currency, completeness and relevance of knowledge, information and data collected, used and produced by IT and other technology security management activities

d) Apply the internal and external criteria that IT/technology security management activities need to meet in order to design security measures

e) use information about the individuals with the organisation and/or their access to information that may need to be kept secure

f) use information about external bodies and individuals and/or their access to information that may need to be kept secure

g) use information about the levels of security that need to be implemented in order to reflect the structure of the organisation and/or access to information, data or knowledge within it

h) apply the most appropriate approaches to undertake IT and other technology security management activities

i) use information contained within risk registers, risk assessments and vulnerability assessments during IT/technology security management activities

j) apply internal and external intelligence relating to IT/technology security risks and threats that may impact on an organisation

k) apply best practice in IT and other technology security management

l) apply learning from other potential and actual IT and other technology security breaches to improve IT/technology security management controls and mechanisms

m) Complete, document and store IT/technology security management plans, responsibilities, controls and mechanisms

n) Take action:

- to assess the effectiveness of IT/technology security measures as mitigation against identified risks, threats and vulnerabilities
- in the event of non-compliance with all strategy, policies, plans processes, procedures and standards relating to IT/technology security
- in the event of external providers not providing the appropriate quality of IT/technology securing services

o) Design/develop IT and other technology security controls and mechanisms, where appropriate

Competent performance requires **Understanding (6.2.S.1.U.)** of:

a) What are the:

- business criteria that need to be met through IT/technology security management activities
- external criteria and requirements, such as those associated with privacy, that need to be supported by IT/technology security management activities

- levels and structure of security controls, policies, processes, procedures and mechanisms that need to be reflected in IT/technology security in order to support and enable business operations
- possible range of IT security controls, policies, processes, procedures and mechanisms, that can be used and their appropriateness in individual business, IT and technology contexts
- possible ranges of issues associated with IT/technology security both within an organisation and also as it exchanges information with external bodies and individuals
- external factors and their implications that may impact on IT and other technology security management activities

b) Who:

- are the business authorities who define the levels of IT/technology security controls that need to be applied
- may access information within the organisation
- may access information from outside the organisation

Competence 6.2.S.2 – Monitor and maintain the effectiveness of IT/Technology Security

This competence will be demonstrated by the following **Performance Criteria (6.2.S.2.C.):**

a) Identify and anticipate possible IT/technology security risks, threats and vulnerabilities at the earliest possible time

b) Test IT/technology security controls and mechanisms regularly to ensure they remain effective

c) Routinely monitor the operation of IT/technology security controls and mechanisms to identify possible and actual security breaches

d) Take timely and appropriate action in the event of IT/technology security breaches, to contain and mitigate their impact, reporting their consequences and any actions taken

e) Critically assess the effectiveness of IT/technology security measures as mitigation against identified risks, threats and vulnerabilities, balancing the requirements for security and control mechanisms with the need for the business to operate efficiently and effectively requirements for security and control mechanisms with the need for the business to operate efficiently and effectively

Competent performance requires **Knowledge (6.2.S.2.K.)** of how to:

a) apply the processes, tools and techniques to monitor the alignment of IT and other technology security management activities and their deliverables with all relevant regulation and external standards

b) use information and data resulting from IT/technology security testing activities

c) Implement and maintain:

- the processes, tools and techniques, relating to IT and other technology security management activities
- IT and other technology security controls and mechanisms for use within an organisation
- regular testing of IT/technology security controls and mechanisms
- updated and refreshed IT and other technology security controls and mechanisms to keep them accurate, current, complete and relevant and ensure they provide the most appropriate levels of protection to an organisation
- the processes, tools and techniques to monitor the alignment of IT and other technology security management activities and their deliverables with all relevant legislation regulations and external standards

d) Monitor:

- the emergence and progress of IT/technology threats and risks as they affect other organisations
- the operation of IT and other technology security controls and mechanisms to identify possible and actual security breaches
- compliance with all relevant legislation, regulations and external standards relating to IT/technology security
- compliance with all IT/technology security strategy, policies, plans, processes, procedures and standards within the organisation
- the effectiveness, appropriateness and quality of IT/technology security management activities

e) Report:

- possible IT/technology risks, threats and vulnerabilities to superiors and external bodies, as appropriate
- how IT/technology security controls and mechanisms mitigate against threats, risks and vulnerabilities
- the results of IT/technology security testing to superiors and external bodies, as appropriate
- actual security breaches, their consequences and actions taken, to superiors and external bodies
- the results produced by monitoring IT and other technology security controls, policies, processes, procedures and mechanisms, to superiors and external bodies as appropriate

f) Analyse/interpret:

- the internal and external criteria and requirements that IT/technology security management activities need to meet
- how the levels and structure of IT/technology security controls and mechanisms need to work in order to support the business needs
- information about the individuals within the organisation and/or their access to information that may need to be kept secure

- information data and knowledge about external bodies and individuals and/or their access to information that may need to be kept secure
- internal and external intelligence relating to IT/technology risks and threat that may impact on an organisation
- information relating to the emergence and progress of IT/technology threats and risks as they affect other organisations
- information and data relevant to IT and other technology security management activities
- information produced by IT/technology testing to identify actions required to ensure levels of security meet the business needs
- information produced by IT and other technology security controls and mechanisms to identify possible and actual security breaches
- the results gained from monitoring the alignment of IT and other technology security management activities and their deliverables with all legislation, regulation and external standards
- the results gained from testing IT/technology security within an organisation

g) Recommend how to improve the effectiveness of IT/technology security within an organisation

h) Take action:

- to balance IT/technology security and control mechanisms with the need for the business to operate efficiently and effectively
- to identify possible IT/technology security risks, threats and vulnerabilities at the earliest possible time
- to anticipate the possible impact of IT/technology security risks, threats and vulnerabilities
- to assess and match IT/technology security controls and mechanisms to identified risks, threats and vulnerabilities
- to deploy IT/technology security controls and mechanisms to mitigate against identified risks, threats and vulnerabilities
- to test IT and technology security controls and mechanisms regularly to ensure they remain effective
- in the event of IT/technology security breaches, to contain and mitigate their impact
- in the event of IT and other technology security management activities not supporting the business needs

Competent performance requires **Understanding (6.2.S.2.U.)** of:

a) What actions may be taken in the event of IT and other technology security management activities not supporting the business needs and/or compliance requirements

b) The importance of effective IT/technology security management to an organisation's brand, reputation and its organisational effectiveness

c) The need for monitoring the effectiveness and quality of external providers of IT/technology security services

Competence 6.2.S.3 – Communicate with others on IT/Technology system security

This competence will be demonstrated by the following **Performance Criteria (6.2.S.3.C.):**

a) Provide appropriate education, communications and training relating to the effective security of IT/technology systems, services and assets and/or information within them to sponsors, stakeholders and external bodies and individuals as appropriate

b) Clearly communicate business professes and procedures to ensure the security of IT/technology systems, services and assets and the information data and knowledge contained within them, to a wide range of internal and external individuals and bodies, as appropriate

c) Promptly and clearly communicate with business authorities on matters relating to actions taken during or required by IT/technology security management activities

Competent performance requires **Knowledge (6.2.S.3.K.)** of how to:

a) Provide education, communications and training relating to the effective security of IT/technology systems, services and assets and/or information within them to sponsors, stakeholders and external bodies and individuals as appropriate

b) Provide information and data relating to the security of IT/technology systems, services and assets and/or information within them to internal sponsors and stakeholders and external bodies and individuals

c) Communicate effectively with stakeholders and external bodies on IT and other technology security management within an organisation

d) Liaise with business authorities on matters relating to actions taken during or required by IT/technology security management activities

e) Communicate business processes and procedures to ensure the security of IT/technology systems, services and assets and the information data and knowledge contained within them

f) Liaise with external bodies offering a range of IT/technology security services appropriate to the organisation

g) Manage:

- external factors that may impact on IT and other technology security management activities
- relationships with sponsors, stakeholders and external bodies on matters relating to IT and other technology security management activities
- relationships with external providers offering IT and other technology security management services
- relationships with external bodies and individuals with whom an organisation exchanges information data and knowledge relating to IT/technology security

Competent performance requires **Understanding (6.2.S.3.U.)** of:

a) The importance of managing relationships with sponsors, stakeholders and external bodies in all aspects of IT and other technology security management activities

b) The importance of clear, unambiguous and consistent communications with sponsors, stakeholders and external bodies in all aspects of knowledge, information and data management activities

Lead Professional Role:

Competence 6.2.L.1 – Implement the strategy for IT/technology Security

This competence will be demonstrated by the following **Performance Criteria (6.2.L.1.C.):**

a) Design, implement and maintain effective and appropriate standards relating to IT/technology security management activities

b) Develop, implement and maintain effective business processes to ensure the security of data, knowledge, information and IT/technology systems, services and assets both with an organisation and also as it is exchanged between it and external bodies and individuals

c) Manage the effective implementation and operation of IT/technology security controls and mechanisms for the organisation

Competent performance requires **Knowledge (6.2.L.1.K.)** of how to:

a) Identify/select:

- the actions that may be taken to mitigate against potential security threats
- the actions that may be taken in the event of IT/technology breaches
- the actions that may be taken in the event of IT/technology security activities not meeting the business needs
- when and how to use external providers of IT/technology security services
- which external providers of IT/technology security services to use
- opportunities to improve the effectiveness of IT/technology security within an organisation

b) Verify IT and other technology security controls and mechanisms for accuracy, currency, completeness, effectiveness and relevance

c) Implement and maintain:

- standards relating to IT and other technology security management activities
- strategy and policies to ensure the alignment of IT and other technology security management activities and their deliverables with all relevant regulation and external standards
- business processes and procedures to ensure the security of information data, knowledge and IT/technology systems, services and assets both within an organisation and also as it is exchanged between it and external bodies and individuals

d) Manage the effective implementation:

- and operation of IT and other technology security controls and mechanisms
- of processes and procedures to ensure the security of data, knowledge, information and IT/technology systems, services and assets as used both within an

organisation and also as it is exchanged between it and external bodies and individuals

e) Design and develop:

- standards relating to IT and other technology security management activities
- strategy and policies to ensure the alignment of IT/technology security management activities and their deliverables with all relevant legislation, regulations and external standards
- the processes, tools and techniques to monitor the alignment of IT/technology security management activities and their deliverables with all relevant legislation, regulations and external standards
- the implementation and use of IT and other technology security controls, mechanisms and procedures to meet business needs
- business processes and procedures to ensure the security of data, knowledge, information and IT/technology systems, services and assets both within an organisation and also as it is exchanged between it and external bodies and individuals

f) Negotiate with external providers of IT/technology security services

g) Authorise and/or agree:

- actions
- approaches
- proposals
- strategy, policies, plans, procedures, standards, methods, tools and techniques

h) Authorise contractual arrangements with external providers of IT/technology security services

Competent performance requires **Understanding (6.2.L.1.U.)** of:

a) What are the ranges of approaches that can be taken to IT and other technology security management and their appropriateness in a range of business, IT and technology contexts

Competence 6.2.L.2 – Direct the management of IT/technology security

This competence will be demonstrated by the following **Performance Criteria (6.2.L.2.C.):**

a) Identify and manage all necessary actions required to mitigate against potential security threats and in the event of IT/technology breaches

b) Verify IT/technology security controls and mechanisms for accuracy, currency, completeness, effectiveness and relevance

c) Make timely decisions in the event of IT/technology security breaches, on actions to be taken to mitigate and contain their impact

d) Make decisions as to the most effective IT/technology security controls and mechanisms to use in order to contain and mitigate against risks, threats and vulnerabilities, applying own judgement and experience

e) Manage the planning and scheduling of regular testing of IT/technology security controls and mechanisms within the organisation

f) Routinely identify opportunities to improve the effectiveness of IT/technology security within an organisation

Competent performance requires **Knowledge (6.2.L.2.K.)** of how to:

a) Manage:

- the planning and scheduling of regular testing of IT/technology security controls and mechanisms
- issues arising as a result of IT and other technology security management activities
- issues arising in the event of a breach of IT/technology security controls and mechanisms

b) Review:

- the effectiveness and quality of IT and other technology security management activities and their deliverables in supporting the business needs
- the effectiveness of business processes, tools and techniques relevant to the management of the security of IT/technology
- compliance with all IT/technology security strategy, policies, plans, procedures and standards within the organisation

c) Recommend proposals for IT/technology security that balance the need for security with the need for the business to operate efficiently and effectively

d) Review how to improve the effectiveness of IT/technology security within an organisation

e) Monitor the effectiveness and quality of external providers of IT/technology security services

f) Make decisions:

- in the event of IT/technology security breaches, on actions to be taken to mitigate and contain their impact
- on when and how to use external providers of IT and other technology security management services
- on the external providers of IT/technology security management services to use
- on how to apply internal and external criteria, business requirements and other information in order to design, develop and implement IT/technology security
- as to the most effective IT/technology security controls and mechanisms to use in order to contain and mitigate against risks, threats and vulnerabilities

Competence (6.2.L.3): Provide direction to improve IT/technology security

a) Develop suitable and comprehensive communications, education and training for the organisation relating to the effective security of IT/technology systems, services and assets and/or information within them

b) Advise and guide others internally and externally as appropriate, on the security of IT/technology services, systems and assets and the information with them

Competent performance requires **Knowledge (6.2.L.3.K.)** of how to:

a) Design/develop communications, education and training to the organisation relating to the effective security of IT/technology systems, services and assets and /or information within them

b) Communicate/liaise with sponsors, stakeholders and external bodies and individuals in the event of a suspected or actual breach of IT/technology security both within an organisation and also as it is communicated to and from an organisation

c) Advise and guide others:

- on all aspects of IT and other technology security management activities and their deliverables
- on internally and externally as appropriate, on the security of IT/technology services, systems and assets and the information within them
- on best practice in IT/technology security
- on the appropriateness of the use of external providers of IT/technology security services

d) Advise on actions to be taken in the event of IT/technology security breaches