

Functional Area: Product & Service Life Cycle (Security)

1. Title	Products / services integrity ensuring	
2. Code	ITCSPL438A	
3. Range	This UoC applies to all considerations and arrangements related to the ensuring of products / services integrity. This is a key step in terms of security protection and goes hand in hand with other security issues such as confidentiality, availability, non-repudiation and authentication.	
4. Level	4	
5. Credit	2	
6. Competency	<p>6.1 Possess the knowledge in the subject area</p> <p>6.2 Products / services integrity ensuring</p>	<p><u>Performance Requirement</u></p> <ul style="list-style-type: none"> ● Fully understand the deemed necessity in incorporating security measures in all CIS products, and own company's products / services are of no exception ● Aware with alertness that ensuring products / services integrity is a fundamental and key element in the context of security protection ● Fully comprehend that products / services integrity basically refers to protecting information from being changed by unauthorised parties, and thus the meanings for "authorised" and "unauthorised" must be clearly defined ● Understand the potential compromises with other security requirements (such as confidentiality, availability) while designing methods and steps to enforce integrity ● Be aware of the different available means and techniques in ensuring products / services availability, each with its own advantages and shortcomings <p>Be able to:</p> <ul style="list-style-type: none"> ● Ensure that all related parties including staff members, customers and even management understand the meaning and nature of integrity in security - protecting information from being changed by unauthorised parties ● Establish agreements with customers or other stakeholders on exact conditions how a user will be regarded as "authorised", and the possibility for multi-levels security integrity setting ● Fully consider related legislations while planning and determining the security integrity issues ● Whenever feasible, formalise the above integrity parameters in the form of guidelines for or agreements with customers, and ensure all involved staff members fully understand the contents and necessity for fulfilling such agreements ● Estimate with accuracy the input resources requirement for enforcing the agreed products / services integrity parameters ● Actually perform or supervise the implementation of the chosen means for integrity availability ● Establish follow up or contingency planning in case the established integrity protection cannot be achieved, with main focus to take remedy actions as soon as possible ● Effectively communicate with customers to ensure they understand both the technical and administrative aspects for integrity protection, and invite their co-operation in adopting and following the related guidelines

	<p>6.3 Exhibit professionalism</p> <ul style="list-style-type: none"> ● Always ensure all related staff members contribute their greatest effort in working towards the ensuring of products / services security integrity ● Always strike a proper balance of interests between customers and the company, and even the society as a whole
7. Assessment Criteria	<p>The integrated outcome requirements of this UoC are the abilities to:</p> <ol style="list-style-type: none"> i. successfully adopt and implement technical and administrative measures to implement agreed products / services security integrity ii. ensure customers fully understand the security integrity features and can make optimal usage of them in case of necessity iii. ensure the implementation of products / services integrity measures result in minimal disturbance to the operation of the company
Remark	