

Functional Area: Product & Service Life Cycle (Security)

1. Title	Carry out functional testing
2. Code	ITCSPL326A
3. Range	This UoC applies to all procedures and activities related to the carrying out of the company's security functional testing. This is a key component of the overall security testing, and actually all subsequent tasks can be considered as subsets or lower level activities of security functional testing.
4. Level	3
5. Credit	3
6. Competency	<p><u>Performance Requirement</u></p> <p>6.1 Possess the knowledge in the subject area</p> <ul style="list-style-type: none"> ● Understand that security functional testing targets for what should be done and test for conformance to security function specifications and underlying security model ● Understand the importance in allocating the appropriate level of resources for carrying out the security functional testing ● Understand that the security functional test needed to be done by qualified personnel with relevant experience and expertise ● Understand the necessity of a security vulnerability testing – identification of flaws in design or implementation that can subvert intended security behaviour ● Be aware of the different available approaches and methodologies to carry out security functional testing, each with its own advantages and shortcomings <p>6.2 Carry out functional testing</p> <p>Be able to:</p> <ul style="list-style-type: none"> ● Well-define in advance the scope and coverage of the security functional testing, and probably consolidate all details into a testing plan ● Fully consider critical factors while preparing the security functional testing plan, including say complexity (representing security functional specification and determining coverage), and costs (non-reusability of previously developed tests) ● Carry out those security functional testing activities, taking into consideration suitability in skills and abilities of responsible employees ● Carry out the execution of tasks listed in the company's security functional testing plan ● Document results and findings about the security functional testing, making use of software such as database management systems (DBMSs) whenever applicable ● Exercise good observation and analysis skills to work with findings from the security functional testing, and propose appropriate follow up actions if necessary ● Effectively communicate with all related staff members in case any follow up / ad hoc activities needed to be performed by them <p>6.3 Exhibit professionalism</p> <ul style="list-style-type: none"> ● Always ensure all related staff members contribute their greatest effort and honesty in activities related to security functional testing ● Always strike a proper balance of interests between customers, employees and the company as a whole
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: <ul style="list-style-type: none"> i. successfully establish a proper security functional testing plan for the company ii. ensure the functional testing will be conducted on time by qualified personnel iii. correctly interpret findings from the testing and propose appropriate follow up actions
Remark	