## Information and Communications Technology Industry Training Advisory Committee Software Products and Software Services (SW) branch Unit of Competencies

2. Code 3. Range Judge and take appropriate actions after evaluating the information system security audit report [Information Security – Information System Audit] 4. Level 5. Credit 6. Competency 6.1 Understand information system security audit report and security baseline  6.1 Understand information system security audit report and security baseline  6.2 Request and evaluate the detailed proof and its supporting evidence of some important findings and recommendations  6.3 Identify the appropriate level of management and related parties to follow up the finetuned recommendations  6.4 Optimize resources to ensure follow up actions are cost effective  6.5 Evaluate and follow up on the information security audit report and their implied effect and impact over the organisation's business activities  • interpret the findings, recommendations of the information system security leavil the priority of the organisation in business goals in relation to the recommendations and suggestions provided in the audit report  Be able to  • request and clarify further details and proofs from the findings and recommendations of the audit work  • judge and evaluate supporting evidence critically  Be able to  • identify the urgency and priority of the recommendations of the audit work  • judge and evaluate supporting evidence critically  • assign related parties to follow ap actions are cost effective  6.5 Evaluate and follow up on the information security audit report in accordance with the organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable  7. Assessment  Criteria  The integrated outcome requirements of this UoCs are the abilities to evaluate whether appropriate actions have been taken by management in a timely manner.	1. Title	Evaluate and follow up on the recommendations in the information system security audit report	
3. Range   Judge and take appropriate actions after evaluating the information system security audit report [Information Security – Information System Audit]	2. Code		
6. Competency     8.1 Understand information system security audit report and security baseline     8.2 Request and evaluate the detailed proof and its supporting evidence of some important findings and recommendations     8.3 Identify the appropriate level of management and related parties to follow up the fine-tuned recommendations      8.4 Optimize resources to ensure follow up actions are cost effective      8.5 Evaluate and follow up on the information security audit report in a professional manner      7. Assessment Criteria      8.1 Understand information system security audit reports and their implied effect and impact over the information space activities     9. interpret the findings, recommendations of the information space activities     1. interpret the findings, recommendations of the information space activities     1. interpret the findings, recommendations of the information space activities     1. interpret the findings, recommendations of the information business goals in relation to the recommendations and suggestions provided in the audit report in audit work     1. judge and evaluate supporting evidence critically     2. identify the priority of the audit report in assign related parties responsible for the appropriate action in a timely manner  Be able to     1. The integrated outcome requirements of the information security audit report in accordance with the organisation's guidelines as well as any ((scal and international)) laws and regulatory requirements, if applicable     1. Assessment criteria  The integrated outcome requirements of this UoCs are the abilities to evaluate relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely		Judge and take appropriate actions after evaluating the information system security audit report	
6.1 Understand information system security audit report and security baseline  6.2 Request and evaluate the detailed proof and its supporting evidence of some important findings and recommendations  6.3 Identify the appropriate level of management and related parties to follow up the finetuned recommendations  6.4 Optimize resources to ensure follow up actions are cost effective  6.5 Evaluate and follow up on the information security audit report in a professional manner  7. Assessment Criteria  6.1 Understand information system security audit report and their implied effect and impact over the organisation's business goals in relation to the recommendations spaces goals in relation to the recommendations and suggestions provided in the audit report  8. able to  9. request and clarify further details and proofs from the findings and recommendations of the audit report audit work  9. judge and evaluate supporting evidence critically  8. able to  9. identify the urgency and priority of the recommendations of the audit report assign related parties responsible for the appropriate action in a timely manner  8. able to  9. identify further details and proofs from the findings and recommendations of the audit report audit report assign related parties responsible for the appropriate action in a timely manner  8. able to  9. identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and priority of the recommendations of the audit report able to identify the urgency and p			
6.1 Understand information system security audit report and security baseline  8.2 Request and evaluate the detailed proof and its supporting evidence of some important findings and recommendations  6.3 Identify the appropriate level of management and related parties to follow up the finetuned recommendations  6.4 Optimize resources to ensure follow up actions are cost effective  6.5 Evaluate and follow up on the information security audit report in a professional manner  The integrated outcome requirements of this UoCs are the abilities to evaluate report to conclude whether appropriate actions have been taken by management in a timely management in a timely manner.		4	
the detailed proof and its supporting evidence of some important findings and recommendations  6.3 Identify the appropriate level of management and related parties to follow up the fine-tuned recommendations  6.4 Optimize resources to ensure follow up actions are cost effective  6.5 Evaluate and follow up on the information security audit report in a professional manner  Criteria  the detailed proof and its supporting evidence from the findings and recommendations of the audit work  judge and evaluate supporting evidence critically  Be able to  identify the urgency and priority of the recommendations of the audit report assign related parties responsible for the appropriate action in a timely manner  Be able to prioritize the resources for the timely implementation of the information security recommendations bought up in the audit report enformation security audit report in accordance with the organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable  7. Assessment Criteria  The integrated outcome requirements of this UoCs are the abilities to evaluate relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely manner.	6. Competency	information system security audit report	<ul> <li>Be able to</li> <li>interpret the findings, recommendations of the information system security audit reports and their implied effect and impact over the organisation's business activities</li> <li>identify the priority of the organisation business goals in relation to the recommendations and suggestions provided</li> </ul>
level of management and related parties to follow up the fine-tuned recommendations  6.4 Optimize resources to ensure follow up actions are cost effective  6.5 Evaluate and follow up on the information security audit report in a professional manner  6.6 Evaluate and follow up on the information security audit report in a professional manner  7. Assessment Criteria  Criteria  Criteria  Identify the urgency and priority of the recommendations of the audit report assign related parties responsible for the appropriate action in a timely manner  Be able to prioritize the resources for the timely implementation of the information security recommendations bought up in the audit report with the organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable  7. Assessment Criteria  The integrated outcome requirements of this UoCs are the abilities to evaluate relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely manner.		the detailed proof and its supporting evidence of some important findings and	<ul> <li>request and clarify further details and proofs from the findings and recommendations of the audit work</li> <li>judge and evaluate supporting evidence</li> </ul>
ensure follow up actions are cost effective  6.5 Evaluate and follow up on the information security audit report in a professional manner  7. Assessment Criteria  ensure follow up actions are cost effective  Be able to evaluate and follow up on the information security audit report in accordance with the organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable  The integrated outcome requirements of this UoCs are the abilities to evaluate relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely manner.		level of management and related parties to follow up the fine- tuned	<ul> <li>identify the urgency and priority of the recommendations of the audit report</li> <li>assign related parties responsible for the</li> </ul>
on the information security audit report in accordance with the organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable  7. Assessment Criteria  The integrated outcome requirements of this UoCs are the abilities to evaluate relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely manner.		ensure follow up actions are cost	implementation of the information security
Criteria relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely manner.		on the information security audit report in	information security audit report in accordance with the organisation's guidelines as well as any (local and international) laws and regulatory
Pomark		relevant information in the information system security audit report to conclude whether appropriate actions have been taken by management in a timely	
INGINAL IN THE PROPERTY OF THE	Remark		