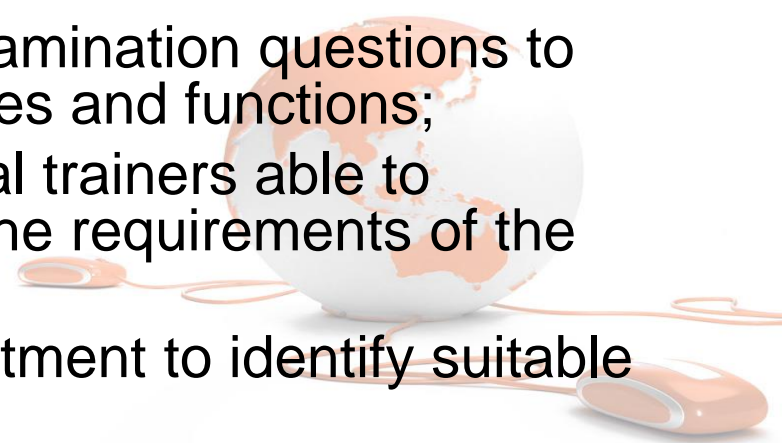




KSA Alignment



Introducing KSA descriptors

- The KSA Descriptor acts as a reference guide, identifying the skills, underpinning knowledge and attitudes required for professionals in the Information Security area
 - The KSA Descriptor should be suitable for use as:
 1. A reference for training providers to facilitate development of suitable training courses relevant to the identified roles and functions;
 2. A reference for the development of examination questions to effectively assess the identified job roles and functions;
 3. A reference for developing professional trainers able to effectively deliver training in line with the requirements of the identified job roles and functions.
 4. A reference for human resource department to identify suitable training to fit specific job role
- 

Transferability

KSA Documentation

There will be other generic skills required for this job role such as report writing, presentation skills, supervisory skills, etc. These are not captured in this template

Johal ACE Information Security KSA Descriptor to Develop Technical Competence	
Job Function	Business Continuity & Disaster Recovery
Level	Intermediate
Code	BP/BCDR/0001
Document Version	1.0
Issue Date	31 October 2016
Industry Segments	Applicable for a range of industry segments including: IT, banking & finance, telecoms, O&G, government, broadcasting, etc.
Synopsis	Personnel with skills in Business Continuity & Disaster Recovery are able to identify threats which can affect the organization operation and plan/prepare for an effective response. Business continuity personnel require extensive understanding of the business model as well as regulatory and compliance requirements. They will also need to plan for implementation of technologies and strategies for continuous monitoring and program improvement and also contingency plans for business recovery purposes.
Recommended Assessment Methods	<input type="checkbox"/> Central assessment (CA) <input type="checkbox"/> Multiple Choice (MC) <input type="checkbox"/> Theory/underpinning knowledge assessment (UK) <input type="checkbox"/> Practical assessment (PA) <input type="checkbox"/> Assignments (AS) <input type="checkbox"/> Case Studies (CS)
Learning Pathway	
Recommended Learning time	40 hours
Training Strategy	>60% practical, Problem based learning, Group work and individual tasks
Experience	
Pre requisite skills	

Training Providers



JPK NOSS

IHLs

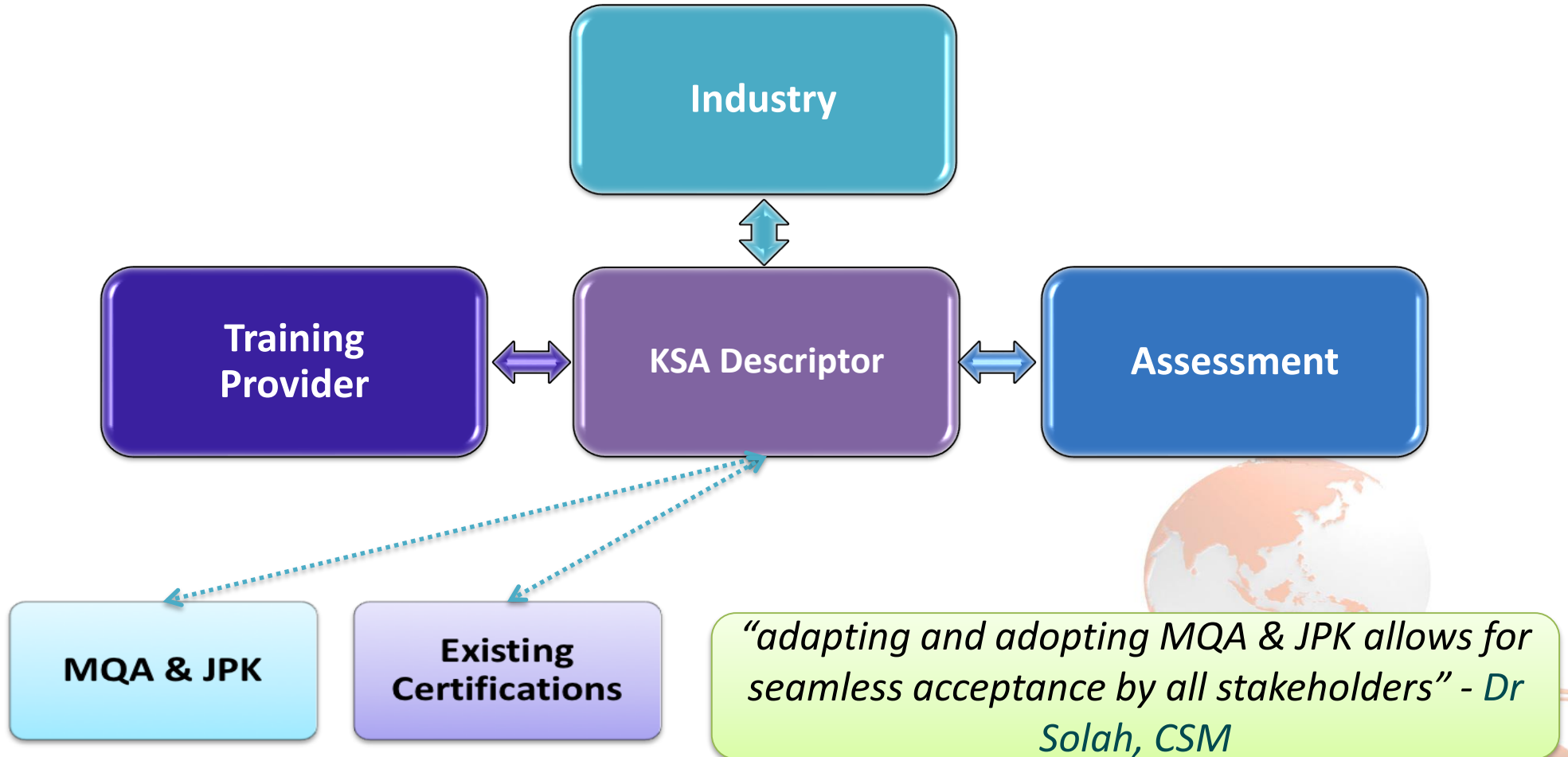


Professional Bodies



Other international certificates & qualifications

Function of KSA Descriptors



Descriptor Structure

Summary

This provides an overall summary of the scope and outcomes of the KSA descriptor including pathway, document ID, version & date and an overview of the recommended training & assessment delivery mechanisms

Knowledge (K)

This provides a set of Knowledge elements for the competency area. This is what one should know

Skills (S)

This provides a set of Skills elements for the competency area. This is what one should be able to do

Assessment Methods

This provides a legend to explain the different possible assessment methods for the K & S elements

Attitudes (A)

This provides a set of Attitude elements for the competency area. This is what traits one should exhibit

Job Function	Intrusion Detection, Monitoring and Prevention
Level	Intermediate
Code	ISP.IDP.0001
Document Version	1.0
Issue Date	31 October 2016
Synopsis	Personnel with skills in Intrusion Detection, Monitoring and Prevention have the ability to defend an organisation from both internal and external cyber threats. They will have the ability to identify the nature and mechanism of the cyber attack against the organisation. They will be able to configure their cyber defence systems and build strategies to defend their organisation against ongoing attacks and prevent future cyber attacks in line with the policies and procedures of the organisation. They will be able to also monitor and respond to the threat in accordance to the organisation's incident detection and response (IDR) policies. Note: At the Intermediate level there will be overlap between this and the Penetration Testing function since both job functions are looking at the same issues but from different perspectives. Therefore a training program aligned to this KSA may incorporate both attack (red team) and defence (blue team) strategies.
Performance Outcomes	<ol style="list-style-type: none"> Identify & classify the nature and mechanisms of cyber attacks against the organisation Build and implement appropriate strategies to defend an organisation against ongoing attacks Protect an organisation from cyber attacks in line with organisational policies & procedures Maintain and monitor system health in line with organisational policies & procedures Implement Intrusion Detection Systems Prepare Incident Response reports
Learning Pathway	Foundation -> Intermediate -> Specialist
Recommended learning time	24 hours
Training Strategy	At this level it is expected that the program is performance based learning, with practical exercises, group work and individual activities to build performance outcomes
Required Experience/Qualifications	Should possess an understanding of operating systems. This can be gained from courses aligned to the Operating Systems (Security, Foundation) and Computer Networking Security (Security, Foundation) KSA Descriptors

Element	Knowledge	Assessment Method	Indicator	Weightage (40%)
K1	Knowledge of Cyber security standards	MC	Is able to identify at least one security standard relevant to Cyber Security, e.g. ISO/IEC 27001, 27002	5%
K2	Knowledge of Organisational policy & procedures	MC	Is able to identify key elements of an organisational policy related to intrusions	5%
K3	Understanding of current threat landscape and attack mechanisms	MC	Given an attack scenario, able to identify nature and mechanism of the cyber attack against the organisation	10%
K4	Knowledge of cyber defence strategies	CA, MC	Given a set of attacks, is able to correlate with an appropriate, effective defence strategy and propose a suitable defence mechanism	10%
K5	Knowledge of cyber defence tools and technologies	MC	Is able to identify the key tools and technologies available to support a cyber defence strategy (e.g. Firewall, DPI, IDS/IPS, etc.)	10%

Element	Skills	Assessment Method	Indicator	Weightage (60%)
S1	Is able to protect an organisation from cyber attacks	PA, CS	Given a policy and a set of attacks, is able to select and deploy protective measures to protect a target system against a range of security incidents (examples may include DDOS, SQL Injection, Cross-site scripting, virus/trojan, removable media, general system vulnerabilities, etc) in line with organisational policies	10%
S2	Is able to maintain and monitor system health	PA	Given a target system & policy, is able to ensure the system is well maintained, for example, patched and has the latest signatures	5%
S3	Is able to perform a risk and vulnerability analysis	PA, CS	Given a target system, is able to identify critical areas of potential risk and vulnerability	10%
S4	Is able to respond to Intrusion Detection Systems	PA	Given an Intrusion Detection System & a set of potential attacks, is able to configure the system to mitigate these attacks and demonstrate that they have been thwarted	10%

Assessment Methods	<ol style="list-style-type: none"> Continual assessment (CA) Multiple Choice (MC) Theory/underpinning knowledge assessment (UK) Practical assessment (PA) Assignments (AS) Case Studies (CS)
--------------------	--

Element	Attitudes
A1	Work independently to identify, troubleshoot and solve problems related to cyber security incidents
A2	Meticulous in the implementation of defence mechanisms related to cyber security incidents
A3	Demonstrate dedication to continuous learning and professional development
A4	Apply a structured approach to analyse and assess cyber security incidents
A5	Maintain ethical conduct & act as a role model in the execution of duties related to cyber security incidents
A6	Remain up to date with the latest trends, tools and attack/defence methods

Note that attitudes will not be assessed separately but rather should be blended into the fabric of the development of knowledge and skills

Descriptor Structure

Summary

This provides an overall synopsis and the tasks expected of someone in the job role. It includes learning pathway, document ID code, version & date and an overview of the recommended training & assessment delivery mechanisms

Role	Digital Forensics First Responder (DFFR)
Level	Foundation
Code	
Document Version	1.0
Issue Date	23 Nov 2017
Synopsis	Personnel with skills in digital forensics first response are responsible for the identification, collection, acquisition and preservation of potential digital evidence. Proper procedures and processes are to be used in this process in accordance with ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence and definitions of terms such as collection and acquisition are as outlined in this ISO document. Definitions of terms such as collection and acquisition are as outlined in this ISO document.
Tasks	<ol style="list-style-type: none"> 1. Carry out a thorough search for items that may contain digital evidence 2. Collect devices that potentially contain digital evidence 3. Conduct acquisition process using suitable acquisition method 4. Initiate and maintain preservation of evidence throughout digital evidence handling 5. Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.
Learning Pathway	Foundation - > Intermediate -> Specialist
Recommended learning time	40 hours
Training Strategy	At this level, it is expected that the program is performance-based learning, with practical exercises, group work and individual to build performance outcomes.
Pre-requisites	The candidate should possess basic computer skills

Descriptor Structure

Knowledge Element
 Each knowledge element breaks down the competency area into the required knowledge at sufficient granularity that it can be assessed. Training providers will use this to ensure the knowledge element is covered sufficiently in training; authors of exam questions will use this to ensure the element is assessed effectively. Both will utilize the Indicator for further clarification of scope.

Element		Assessment Method	Indicator	Weightage (40%)
K1	Understanding of Digital evidence identification	MC CS	<ul style="list-style-type: none"> Given a scenario, is able to identify various type of IT devices and network devices, identify components that contain potential evidence, and assess risks to actions taken in collecting/acquiring potential evidence Is able to determine the state of devices and value of evidentiary information on the devices Is able to understand impact of volatile and non-volatile evidence 	10%
K2	Understanding of		<ul style="list-style-type: none"> Is able to determine best method of collection to preserve maximum information relevant to the incident Is able to formulate a collection process while preserving digital evidence Given a scenario, is able to determine storage 	5%
K3	Unde			6%
K4	Understanding of Digital evidence preservation	MC CS	digital evidence and factors influencing its admissibility	10%

Assessment Methods
 This provides a legend to explain the different possible assessment methods for the K & S elements

Indicator
 The indicator provides further clarification on the scope of the knowledge element. It provides the information to allow both training organisations and examiners to build content & assessments to ensure the topic is addressed

Weightage
 This provides an indication of the amount of coverage there should be in the overall course/examination, e.g. 5% would indicate that in a 40 hour course, 2 hours should be spent on this Knowledge element

Descriptor Structure

Skill Element

Each skill element breaks down the competency area into the required skill at sufficient granularity that it can be assessed. Training providers will use this to ensure the skill element is covered sufficiently in training; authors of exam questions will use this to ensure the element is assessed effectively. Both will utilize the Indicator for further clarification of scope.

Skills (S)

This provides a set of Skills elements for the competency area. This is what one should be able to do

Skills			
Element	Assessment Method	Indicator	Weightage (60%)
S1	PA CS	Is able to systematically disassemble digital devices to extract components that contain potential evidence without compromising the integrity of the media	5%
S2	PA CS	Is able to create a forensically sound duplicate of the evidence (forensic image) from digital devices (e.g. hard drive, RAM, mobile device, camera, etc.)	20%
S3	PA CS	Given a scenario, is able to collect, package, transport and store digital evidence without alteration, loss, physical damage, or destruction of data	20%
S4	PA CS	Is able to record the detailed chain of evidence including maintaining notes, images, videos, etc. with timestamps preserved, and production of relevant reports.	15%

Descriptor Structure

Assessment Methods

This provides a legend to explain the different possible assessment methods for the K & S elements

Assessment Methods

1. Continual assessment (CA)
2. Multiple Choice (MC)
3. Theory/underpinning knowledge assessment (UK)
4. Practical assessment (PA)
5. Assignments (AS)
6. Case Studies (CS)

Assessment Method

For the assessment of this element, the method provides an indicator of the recommended way in which it should be assessed. The letter code is provided in the legend shown. Appropriate learning & assessment techniques and educational best practices should be used in the development of assessments.



Descriptor Structure

Attitudes (A)

This provides a set of Attitude elements for the competency area. This is what traits one should exhibit.

Attitudes

A1	Meticulous in all matters relating to evidence collection, acquisition, preservation and reporting
A2	Display patience and calm in all matters dealing with evidence collection, acquisition, preservation and reporting
A3	Apply a structured approach to identify and assess evidence in line with defined policy and SOPs
A4	Maintain ethical conduct & act as a role model including showing respect in the execution of duties related to Forensic
A5	Use judgement, make decisions and apply solutions with confidence

Note that attitudes will not be assessed separately but rather should be blended into the fabric of the development of knowledge and skills

Attitude Element

Each attitude element breaks down the behaviours that should be developed and exhibited after the training. Training providers will use this to ensure the attitude element is covered sufficiently in training; authors of exam questions do not need to use this as the attitudes will not be assessed separately but rather should be blended into the fabric of the development of knowledge and skills.



Descriptor Structure

Mapping & references

For each *Task* element, indicate the *Knowledge & Skills* elements that are required in order to perform that *Task*

Mapping between Task and Knowledge/Skill Elements

Tasks	Knowledge	Skill
T1	K1, K2	S1, S2
T2	K2, K3	S1, S2
T3	K1, K2, K3	S1, S2, S3
T4	K4, K5	S1, S2, S3
T5	K4, K5	S1, S2, S3

References:

1. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017.
2. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.
3. Common Vulnerability Scoring System (CVSS), (<https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator>).
4. National Cybersecurity and Communication Integration Center (NCCIC) Cyber Incident Scoring System (<https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>).
5. Risk Assessment Principles and Guidelines (https://www.slideshare.net/shaolinint/risk-assessment-principles-and-guidelines?from_action=save).

References

Include the references used to develop the KSA



KSA Example

Job Function	Intrusion Detection, Monitoring and Prevention
Level	Intermediate
Code	ISP.IDP.0001
Document Version	1.0
Issue Date	31 October 2016
Synopsis	<p>Personnel with skills in Intrusion Detection. Monitoring and Prevention have the ability to defend an organisation from both internal and external cyber threats.</p> <p>They will have the ability to identify the nature and mechanism of the cyber attack against the organisation. They will be able to configure their cyber defence systems and build strategies to defend their organisation against ongoing attacks and prevent future cyber attacks in line with the policies and procedures of the organisation. They will be able to also monitor and respond to the threat in accordance to the organisation's incident detection and response (IDR) policies.</p> <p>Note: At the intermediate level there will be overlap between this and the Penetration Testing function since both job functions are looking at the same issues but from different perspectives. Therefore a training program aligned to this KSA may incorporate both attack (red team) and defence (blue team) strategies.</p>
Performance Outcomes	<ol style="list-style-type: none"> 1. Identify & classify the nature and mechanisms of cyber attacks against the organisation 2. Build and implement appropriate strategies to defend an organisation against ongoing attacks 3. Protect an organisation from cyber attacks in line with organisational policies & procedures 4. Maintain and monitor system health in line with organisational policies & procedures 5. Implement Intrusion Detection Systems 6. Prepare Incident Response reports
Learning Pathway	Foundation -> Intermediate -> Specialist
Recommended learning time	24 hours
Training Strategy	At this level it is expected that the program is performance based learning, with practical exercises, group work and individual activities to build performance outcomes
Required Experience/Qualifications	Should possess an understanding of operating systems. This can be gained from courses aligned to the Operating Systems (Security, Foundation) and Computer Networking Security (Security, Foundation) KSA Descriptors

Useful for learning & dev to verify how up to date this is

Useful for non-technical to identify specific program

Useful for management to get program area

Useful for HR to identify program target level & methodology

	Weightage (60%)
1. Identify & classify the nature and mechanisms of cyber attacks against the organisation	10%
2. Build and implement appropriate strategies to defend an organisation against ongoing attacks	5%
3. Protect an organisation from cyber attacks in line with organisational policies & procedures	10%

S1	Is able to protect an organisation from cyber attacks	PA, CS	include DDOS, SQL Injection, Cross-site scripting, virus/trojan, removable media, general system vulnerabilities, etc) in line with organisational policies & procedures	10%
S2	Is able to maintain and monitor system health	PA	Given a target system & policy, is able to ensure the system is well maintained, for example, patched and has the latest signatures	5%
S3	Is able to perform a risk and vulnerability analysis	PA, CS	Given a target system, is able to identify critical areas	10%

Descriptor Details

Job Function	Intrusion D
Level	Intermediat
Code	ISP.IDP.000
Document version	1.0
Issue Date	31 October
Synopsis	Personnel v internal an They will h to configur future cybe to the thre Note: At the functions a rat

Job Function
Identifies the key function of this KSA descriptor. This will not form an entire job role but is rather part of a job role, i.e. a competence area that may be applied to multiple roles. This is since there are many different organisational roles & job titles specific to an organisation that may require this competency area

Level
Identifies the level of this KSA descriptor. Can be foundation, intermediate or specialist

Code
Identifies a unique code assigned to the KSA descriptor. This is a useful reference to identify or reference this document as well as track its version number

Document Version
Identifies the current version for document management and tracking purposes

Issue Date
Identifies the date of the approved publication of the KSA descriptor for tracking purposes

Synopsis
Provides an overview of the scope of the KSA descriptor. This is useful for HR personnel to get a summary of the KSAs and assist with mapping the competency area to relevant job roles in an organisation

Descriptor Details: Knowledge

		Knowledge		
Element		Assessment Method	Indicator	Weightage (40%)
K1	Knowledge of Cyber security standards	MC	Is able to identify at least one security standard relevant to Cyber Security, e.g. ISO/IEC 27001, 27002	5%
K2	Knowledge of Organisational policy & procedures	MC		

Knowledge Element

Each knowledge element breaks down the competency area into the required knowledge at sufficient granularity that it can be assessed. Training providers will use this to ensure the knowledge element is covered sufficiently in training; authors of exam questions will use this to ensure the element is assessed effectively. Both will utilize the Indicator for further clarification of scope.

Indicator

The indicator provides further clarification on the scope of the knowledge element. It provides the information to allow both training organisations and examiners to build content & assessments to ensure the topic is addressed

Weightage

This provides an indication of the amount of coverage there should be in the overall course/examination, e.g. 5% would indicate that in a 40 hour course, 2 hours should be spent on this Knowledge element

Assessment Method

For the assessment of this element, the method provides an indicator of the recommended way in which it should be assessed. The letter code is provided in the legend shown. Appropriate learning & assessment techniques and educational best practices should be used in the development of assessments.

Assessment Methods	
	1. Continual assessment (CA)
	2. Multiple Choice (MC)
	3. Theory/underpinning knowledge (TK)
	4. Practical assessment (PA)
	5. Assignments (AS)
	6. Case Studies (CS)

Descriptor Details: Skills

		Skills		
Element		Assessment Method	Indicator	Weightage (60%)
S1	Is able to protect an organisation from cyber attacks	PA, CS	Given a policy and a set of attacks, is able to select and	

Skill Element

Each skill element breaks down the competency area into the required skill at sufficient granularity that it can be assessed. Training providers will use this to ensure the skill element is covered sufficiently in training; authors of exam questions will use this to ensure the element is assessed effectively. Both will utilize the Indicator for further clarification of scope.

Indicator

The indicator provides further clarification on the scope of the skill element. It provides the information to allow both training organisations and examiners to build content & assessments to ensure the topic is addressed

Weightage

This provides an indication of the amount of coverage there should be in the overall course/examination, e.g. 10% would indicate that in a 40 hour course, 4 hours should be spent on this skill element, i.e. practical activities

Assessment Method

For the assessment of this element, the method provides an indicator of the recommended way in which it should be assessed. The letter code is provided in the legend shown. Appropriate learning & assessment techniques and educational best practices should be used in the development of assessments.

Assessment Methods
<ol style="list-style-type: none"> 1. Continual assessment (CA) 2. Multiple Choice (MC) 3. Theory/underpinning knowledge assessment (UK) 4. Practical assessment (PA) 5. Assignments (AS) 6. Case Studies (CS)



Descriptor Details: Attitudes

Attitudes	
A1	Work independently to identify, troubleshoot and solve problems related to cyber security incidents
A2	Meticulous in the implementation of defence mechanisms related to cyber security incidents
A3	Demonstrate dedication to continuous learning and professional development
A4	

Attitude Element

Each attitude element breaks down the behaviours that should be developed and exhibited after the training. Training providers will use this to ensure the attitude element is covered sufficiently in training; authors of exam questions do not need to use this as the attitudes will not be assessed separately but rather should be blended into the fabric of the development of knowledge and skills.



KSA Levels

Specialist Level:

- Specialist KSAs for a given discipline
- Defines skills and underpinning knowledge required to achieve mastery in a defined set of performance outcomes in specific areas under a given discipline

Intermediate Level:

- Discipline specific KSAs
- Defines core skills and underpinning knowledge required to be able to perform a defined set of performance outcomes in a given discipline

Foundation Level:

- Common core KSAs
- Defines foundational, transferable skills and underpinning knowledge required for one or more disciplines at practitioner level

**Global ACE
Professional
Membership
Requirements**

PROFESSIONAL

Foundation

At the foundation level, the candidates are just starting out to learn core pre- requisites and foundational knowledge that will be required to understand the intermediate level topics.

Intermediate

At the intermediate level, the candidates must have several years of experience in the related work role. They can execute the tasks with supervision. They are expected to be able to execute the tasks, using existing tools, techniques and method.

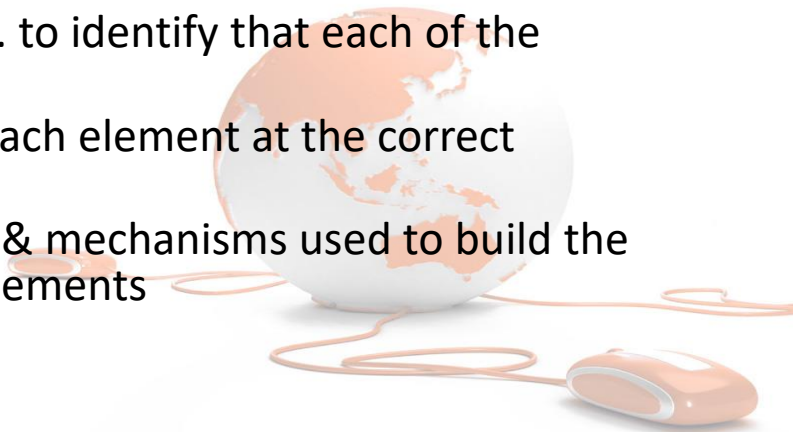
Specialist

At the specialist level, the candidates must already have 5 years or more experience in the related work role and can execute the tasks with minimal supervision. They have a deep understanding of the domain and may develop their own tools, techniques or methods.



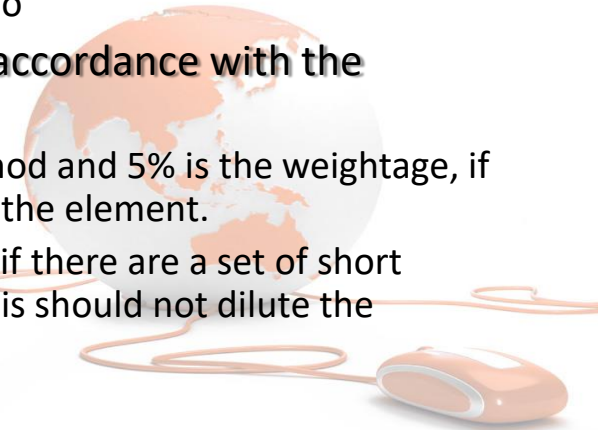
How does a training organisation use these?

- In course development
 - The course developer must ensure that in development of the training materials:
 - Each Knowledge element is covered in the training materials, e.g. slides and notes
 - Each Skills element is covered in the practical exercises
 - For each, the indicators are used to clarify the scope of coverage
 - The correct weightage is achieved for each element
 - There is a strategy to develop and reinforce the Attitude elements throughout the training
- Upon submission of course materials to the evaluation panel, the training organisation must adhere to the evaluation requirements. This will include marking up all training materials to validate that the KSA elements are all covered, for example:
 - Provision of highlighted slides, workbook, notes, etc. to identify that each of the Knowledge & Skills elements are addressed;
 - Provision of a schedule to indicate the coverage of each element at the correct weightage
 - Provision of a description of the training philosophy & mechanisms used to build the Attitude elements through the Knowledge & Skills elements



How does an examiner use these?

- In question bank development
 - The course developer must ensure that in development of the training materials:
 - Each element is covered in line with the indicator and using the defined assessment method
 - The correct weightage is achieved for each element
 - There should be a pool of questions for each element which are randomly assigned to an exam paper while maintaining the weightage
- In exam delivery, the exam system must ensure that:
 - The appropriate assessment technique is used to assess each Knowledge & Skill element
 - E.g. if the descriptor indicates that “PA” practical assessment should be used, then the exam system must assess this in a practical context.
 - Note that does not preclude the use of a computer based examination system, however it must demonstrate how the system can emulate a live environment/scenario
 - there is sufficient coverage of each Knowledge & Skill element in accordance with the weightage guidelines provided in the descriptor
 - E.g. If the Knowledge element indicates “MC” is the assessment method and 5% is the weightage, if the exam has 40 multiple choice questions, at least two should cover the element.
 - Note that the overall weightage in the exam must be maintained, i.e. if there are a set of short answer/written questions in addition to multiple choice questions, this should not dilute the weightage of the topic.



GLOBAL ACCREDITED CYBERSECURITY EDUCATION (ACE) SCHEME

GOAL & OUTCOME

GOAL

To create world class competent work-force in cyber security and promote the development of cyber security professional programmes within the region



Professional Certification

EXPECTED OUTCOME

To provide cyber security professionals with the right Knowledge, Skills, Attitudes (KSA) and experience

OBJECTIVES

1 To establish a professional certification programme that is recognized globally

2 **To create world class competent work-force in cyber security**

3 To provide cyber security professionals with the right knowledge, skills, abilities, attitude (KSA) and experience

4 **To be a global cyber security training programme providers**

5 To promote the development of cyber security professional programmes globally

6 **To ensure accredited personnel has been independently assessed and committed to a consistent and high quality service level**



Thank you

Corporate Office
CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888
F : +603 8992 6841
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

 www.facebook.com/CyberSecurityMalaysia
 twitter.com/cybersecuritymy
 www.youtube.com/cybersecuritymy

