



## Knowledge Based Assessment Task

Form no: XXXXX  
Issue date: 1/12/2017  
Review date:  
1/12/2018

Qualification details			
Training Package	ICT - Information and Communications Technology		
Qualification National Code & Title	ICT40120 Certificate IV in Information Technology	State code:	
Unit National Code & Title	BSBXCS404 Contribute to cyber security risk management	State code:	



Student's name:	Richard Pountney	Student ID:	30007736
Assessor's name:		Assessment Date:	
Time allocated:	2 weeks		
Resources allowed:	Internet, Blackboard, PowerPoint Presentations		
Assessment Task Instructions:	<p><b>Scenario:</b> <i>You are a member of the CITE MS security team. The management team of one of your clients wants to expand their understanding of risk management in relation to cyber security. As such, they have sent a series of questions, the answers of which are aimed to help guide their decision-making for training material in the future.</i></p> <p>Fully answer all questions in detail and submit to the lecturer via Blackboard as an electronic copy. Any and all external sources used (images, websites, articles, or otherwise) need to be referenced.</p>		

Questions to be answered by the student:		Satisfactory Response	
		Yes ✓	No ✗
Q1	Name and describe the Australian legislation that pertains to data protection and privacy. In your answer, specifically include how this legislation relates to cyber security.		
Response: Privacy Act 1988 This legislation sets out rules for businesses to follow. It outlines the requirements on how to collect, use, store & disclose personal information. This is meant to protect your personal information privacy & not your physical privacy. This contains the 13 Australian Privacy Principles (APP). These principles provide guidance on how personal information should be handled.			
Q2	Explain how the Notifiable Data Breach legislation affects organisations and how it links to other Australian legislation.		



<p>Response:</p> <p>Under the Notifiable Data Breaches (NDB) scheme any organisation or agency the Privacy Act 1988 covers must notify affected individuals &amp; the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.</p>			
Q3	Describe the General Data Protection Regulations (GDPR), its major provisions, and how it relates to Australian entities. In your response, describe at least two differences it has to Australian privacy legislation.		
<p>Response:</p> <p>The GDPR is the toughest privacy &amp; security law in the world. Even though it was made &amp; passed by the European Union (EU), it imposes obligations onto organisations anywhere, as long as they target or collect data related to people in the EU.</p> <p>The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy &amp; security standards, with penalties reaching into the tens of millions of euros. Ten million euros ≈ 14805452.20 AUD</p>			
Q4	Describe the objective and purpose of regular organizational training in relation to risk management.		
<p>Response:</p> <p>Education, Training, &amp; Awareness (ETA) is a means to help address one of the most major issues within organisation security, users.</p> <p>People are ultimately the weakest link in security. They are often gullible, fallible, &amp; have access to the systems.</p> <p>Roughly 85% of all 'attacks' are initiated from a user-triggered action. These aren't necessarily malicious &amp; are often accidental. Have you ever accidentally deleted your work?</p>			
Q5	Describe the objective and purpose of regular threat assessment in relation to risk management.		
<p>Response:</p> <p>To check if there are any gaps in the risk management &amp; to improve that area. It provides a way to update &amp; review assessments as new developments occur &amp; then to take steps to protect the organisation, people, &amp; assets.</p>			
Q6	Describe the objective and purpose of a cyber security incident response plan in relation to risk management.		



<p>Response:</p> <p>It aims to minimize the negative impact on the business.</p> <p>To prepare businesses for unexpected disruptions.</p> <p>Resumes an ICT service to normal as quickly as possible after a disruption.</p> <p>It demonstrates IT's value to the business by aligning IT activities to business priorities.</p> <p>To reduce the impact on the business &amp; user with improved monitoring.</p> <p>To meet legal &amp; regulatory compliance.</p>		
<p>Q7 Describe the objective and purpose of clear escalation routes in relation to risk management.</p>		
<p>Response:</p> <p>Incident escalation is what happens when an employee can't resolve an incident themselves &amp; needs to hand off the task to a more experienced or specialized employee. This usually happens when the existing knowledge base does not consist information for the reported incident.</p> <p>By having a well-planned incident escalation process, organisations can ensure that all incidents are managed at an appropriate level by the appropriate personnel.</p>		
<p>Q8 Describe the procedures involved in analysing and reviewing risk management methodologies.</p>		
<p>Response:</p> <p>Risk management is best understood as a cyclical process in which new &amp; ongoing risks are continually identified, assessed, managed, &amp; monitored.</p> <p>This is a structured approach to addressing risks &amp; can be used in companies of all sizes &amp; across any industry.</p>		
<p>Q9 Describe the procedures involved in developing communication plans.</p>		
<p>Response:</p> <p>Encourages stakeholder engagement &amp; accountability.</p> <p>Maximizes the information obtained to reduce uncertainty.</p> <p>Meet the report &amp; assurance needs of the stakeholder.</p> <p>Ensures that relevant expertise is drawn upon to inform each step of the process.</p> <p>Inform other entity processes such as corporate planning &amp; resource allocation.</p>		X
<p>Q10 Describe the procedures involved in evaluating effectiveness of risk management strategies.</p>		
<p>Response:</p> <p>You match the outcomes of a risk management plan with its objectives.</p> <p>Check if the risks are avoided, transferred, mitigated, or accepted according to the plan.</p> <p>Evaluate if all the activities that are in the plan would be effective.</p> <p>The strategy is only as strong as the weakest link.</p> <p>Evaluate the business environment.</p>		



<p>Check if the strategies have affected the business environment. Identify areas of improvement. After all, evaluations try to make possible changes in the action plan to get the desired results.</p>			
Q11	Describe the procedures involved in monitoring cyber risk.		
<p>Response:</p> <p>Detecting changes in the internal &amp; external environment.</p> <p>Identifying new or emerging risks.</p> <p>Ensuring the effectiveness &amp; relevance of controls &amp; implementation of treatment programs.</p> <p>Obtaining further information to improve the understanding &amp; management of already identified risks.</p> <p>Analyse &amp; learn lessons from past events, including near-misses, successes, &amp; failures.</p> <p>Document the results and observations from the monitoring &amp; reviews.</p>			
Q12	Describe the procedures involved in reviewing currency of risk register.		
<p>Response:</p> <p>Monitor &amp; review changes periodically to ensure that the controls in place are still suitable for the current landscape.</p> <p>New IT asset addition to the infrastructure.</p> <p>The introduction of new assets into the infrastructure will create new risks.</p> <p>The organisation must identify the additions in order to manage the threats &amp; risks associated.</p> <p>Technology advancement.</p> <p>As technology advances, new systems will be created &amp;or changes will be made to existing systems. This will inevitably introduce new threats &amp; risks.</p> <p>Changes in the work procedures.</p> <p>When there are changes in work procedures, the organisation should review their risk landscape. Changes in the work procedures may increase or decrease existing risk exposure to cyber threats.</p> <p>This can include a role change or new employees.</p> <p>New threats in the wild.</p> <p>Sometimes even if the risk management strategies are current &amp; valid, new threats may still arise. These threats are often referred to as zero-day exploits.</p> <p>Zero-day exploits are threats where no existing resolutions are available.</p> <p>Interim solutions may be applied to avoid or mitigate these exploits.</p>			
Q13	You have been tasked to review the risk management strategies for a client in the <b>healthcare industry</b> . What kind of industry-specific considerations should you keep in mind when implementing the risk management procedures?		



<p><b>Response:</b> You should keep in mind the goals of the industry risk management. For the healthcare industry, their overall goal is the safety of clients &amp; financial stability. Some of the goals are decreasing malpractice claims, using skin protocols to prevent skin ulcers, &amp; improving communication with insurance companies to earn points &amp; reduce overall costs.</p> <p>Reference for my answer: <a href="#">The Importance of Health Care Risk Management</a></p>		X
<p>Q14 List and describe the steps involved in updating technology based on an industry-accepted guideline.</p>		
<p><b>Response:</b> Make sure that the industry guideline accepts the technology that is being updated or added. Use the SWOT analysis to evaluate what the update will do &amp; what changes need to be made. Use a fishbone diagram to guess possible risks for updating.</p>		
<p>Q15 Describe 2 business process design principles in relation to risk management.</p>		
<p><b>Response:</b> SWOT analysis: it helps identify Strengths, Weaknesses, Threats &amp; Opportunities associated with risks that may occur. Fishbone Diagram: the cause &amp; effect diagram is used to break down a problem to identify the root causes behind it. This diagram can also work backward because it can help identify the causes of an effect. This can be useful for presenting multiple options.</p>		
<p>Q16 Explain what and how reporting mechanisms are used for tracking organisational cyber security maturity.</p>		
<p><b>Response:</b> The reporting mechanisms are the report documents that are made when you make risk management strategies. How they are used to track the cyber security maturity is by having all the documents filed away so you can see how much has been done &amp; how the organisation has matured.</p>		

Assessor Feedback			
Assessment Decision	<input type="checkbox"/> Satisfactory	<input type="checkbox"/> Not Yet Satisfactory	
Is student eligible for reassessment (Re-sit)?	<input type="checkbox"/> No	<input type="checkbox"/> Yes	Reassessment Date:



### Feedback to student

### Feedback from student

**Student's signature:**

*(Once feedback has been provided)*

**Date:**

**Assessor's signature:**

*(Once feedback has been provided)*

**Date:**