AMP-116930-8-2400-FZML.

by def abc

Course Details	
Course Name	

Unit(s) of competency	
Unit Code (s) and Names	**BSBRSK501 Manage Risk**

Assessment Details			
Term and Year		Time allowed	
Assessment No		Assessment Weighting	
Assessment Descriptor			
Due Date		Extension (if approved)	

Re-Assessment Details			
Term and Year		Time allowed	
Assessment No		Re-assessment Fee Paid?	
Assessment Type			
Due Date		No Extension	

Student Details and Declaration			
Student Name			
Student ID		Trainer/Assessor's Name	
Student Declaration: a. I declare that the work submitted is my own and has not been copied or plagiarised from any person or source. b. I have not submitted any part of this assignment previously as part of another unit/course. c. I acknowledge that I understand the requirements to complete the assessment tasks. d. The assessment process including the provisions for re-submitting and academic appeals were explained to me and I understand these processes.		Signature: _____ Date: _____/_____/___	

Assessment Outcome - To be completed by the Assessor			
Assessor's Name			
Results	☐ Satisfactory ☐ Not Satisfactory	Marks:	
Re-assessment eligibility	☐ Yes ☐ No	Due Date:	

This assessment	First Attempt ☐	2nd Attempt ☐	Late ☐ Penalty_____

FEEDBACK TO STUDENT
Progressive feedback to students, identifying gaps in competency and comments on positive improvements:

_____

_____

_____

_____

Student Declaration: I declare that I have been assessed in this unit and I have been advised of my result. I am also aware of my right to appeal and the reassessment procedure.

Signature: _____

Date: _____/_____/_____

Assessor Declaration: I declare that I have conducted a fair, valid, reliable and flexible assessment with this student, and I have provided appropriate feedback

☐ Student did not attend the feedback session. Feedback provided on assessment.

Signature: _____

Date: _____/_____/_____

FEEDBACK TO STUDENT *(FOR REASSESSMENTONLY)*

_____

_____

_____

Student Declaration: I declare that I have been re-assessed in this unit and I have been advised of my result. I am also aware of my right to appeal.

Signature: _____

Date: _____/_____/_____

Assessor Declaration: I declare that I have conducted a fair, valid, reliable and flexible assessment with this student, and I have provided appropriate feedback

☐ Student did not attend the feedback session. Feedback provided on assessment.

Signature: _____

Date: _____/_____/_____

Assessment Task
(Performance)

BSBRSK501

Manage Risk

DOCUMENT CONTROL

VERSION	DATE	COMMENTS
1.0	4th April 2019	▪ Initial

ASSESSOR PRE-ASSESSMENT CHECKLIST

This checklist is to be completed prior to commencing the assessment.

Please discuss this with the learner and circle yes or no for each question.

Is the learner ready for assessment?	☐Yes ☐ No
Have you explained the assessment process and tasks?	☐ Yes ☐No
Does the learner understand which evidence is to be collected and how?	☐ Yes ☐No
Have the learner's rights and the appeal system been fully explained?	☐ Yes ☐No
Have you discussed any special needs or reasonable adjustments to be considered during the assessment?	☐ Yes ☐No
Does the learner have access to all required resources?	☐ Yes ☐No

ASSESSMENT INSTRUCTIONS

PURPOSE OF THE ASSESSMENT TASK		
Assessment Tool	Practical Application (Hazard Identification and Risk Analysis Activities)	
To demonstrate satisfactory completion of this Assessment Task the learner must:	**Satisfactory (S)**	**Not Satisfactory (NS)**
Successful completion of all five (5) Hazard Identification and Risk Analysis Activities	☐	☐
Overall Assessment Task Performance	**Satisfactory (S)**	**Not Satisfactory (NS)**
Practical Application: Hazard Identification and Risk Analysis Activities	☐	☐
Resources required for this Assessment		
Trainers and Assessors are required to ensure all learners have access to:		

- Templates, Legislation, and regulatory process.
- Site or simulated environment for assessment of hazards etc.
- Work Health and Safety Regulations 2011
- Australian Standards 2010
- Building Regulations Act 2006

- Hazard Identification and Risk Analysis Tool
- Risk Matrix Table

Instructions for Trainer and Assessors

This assessment task has to be conducted as per the Assessment Conditions:

| ☒ | In class | ☒ | In an Industry Workplace | ☒ | In a Simulated Industry Environment |

Please read the following instructions carefully

This Assessment tasks covers aspects such as:

- Hazard identification
- Adopting
- Testing
- Selecting
- Reviewing risk control measures
- Employee involvement in the management of risk control measures

Assessment Task Duration

- Week 6

Learner Evidence Submission Requirements

- The completed and signed Assessment Tool
- Completion of each of the five (5) Hazard and Risk Analysis Activities
- Any Supporting materials or documentation

MANAGE RISK

ASSESSMENT TASK: PRACTICAL APPLICATION

ASSESSMENT INSTRUCTIONS

This assessment task is to be conducted as per the following Assessment Conditions:

1. 'The workplace':

The Student can nominate their current place of employment and complete the Assessment Activities referencing their industry workplace.

For authenticity and validity the student is required to complete the following table verifying the venue:

Name of Establishment	
Industry Sector	
Supervisor/Manager's Name	
Location including Address	
Contact Details	

OR

2. 'Scenario':

If the student has no industry experience or currency the following scenario is to be conducted at Academies Australasia Polytechnic (AAPoly).

The student is nominated as a AAPoly WHS Committee Member and under supervision is required to complete a venue risk assessment and hazard identification of the 628 Bourke Street, Level 8 Campus facilities. Upon completion the evidence gathered can be used to complete the assessment task.

Note: The Trainer is to provide AAPoly's organisational WHS policies and procedures, relevant workplace documents and hazard identification tools.

ACTIVITY 1

Think of one (1) risk or hazard.

This could be a small risk or a larger risk.

Fill in the template provided below, including action items and how you can best manage this risk.

Name the risk	**Financial risk management**

Risk Control Plan template

Action Required	Person Responsible	When is action due	Resources required
Conducting financial due diligence	Financial analyst	10/01/2020	Cash flow statements, financial risk statements
Reviewing final statements for actual audits. **Applying clauses of financial distress.**	Auditors	20/01/2020	Smartsheets, financial software, technology.
Evaluating liabilities and company's ability of paying debts.	Financial analyst	30/01/2020	Cash flow statements, financial risk statements
Need for loans and future funds.	Financial analyst	10/02/2020	Contact register for meeting external stakeholders
Engaging stakeholders through meetings.	Financial manager	30/02/2020	Seminar hall, communication tools such as video conference arrangements.

ACTIVITY 2

Think of any potential hazards you could find and conduct a risk assessment.

Use the template below and fill in the details.

Risk Assessment Template	
Date conducted	20/10/2019
Conducted at	Organization
Conducted by	Risk manager
Signature	John Liam

Potential Hazard	Who could be at risk?	Risk Rating	Current Control Measures	How can risk be prevented?	Who is responsible?
Loss or corruption of data system	Company	1	HSM codes/ cryptology	Identification of anomalies and events. Taking timely action.	It security team
Disruption in business operations	Company	2	Expressing requirements for IT system. Defining purpose of system and documentation.	Limiting access to the unauthorized personnel.	IT manager
Losing sensitive information	Company	2	Applications testing	Software testing is employed for assessing the reliability of software and ensuring it is safe from bugs and does not lead to any failure.	Security manager
Illegal monitoring	Company	3	cryptology/ HTTP	The digital certificates are	Security manager

				used for increasing the security related to software and using the payment gateway server.	
Breaches of cyber security	Company	3	digital wallet/ merchant software	Code tempering is also minimized by incorporation of code safe shield hardware security modes HSMs. The processes are highly secured by the HSM codes and also help the organization to detect the hacking attempts made by hackers	Security manager
Virus, Trojans spyware	Company	3	digital wallet/ merchant software	Network connections are protected via Virtual Private Networks (VPNs) capable of accessing remote locations also. Data- crypto is the backbone of the hardware systems that maximize the level of protection and allowing access only after authentication	IT manager

ACTIVITY 3

Identify risks that exist within your department or organisation as per the table below

Company	**NORD**
Department	Human resource
Function of department	Corporate social responsibility
Risks	
Risks relating to staff	Undermines employees relationship. High-quality and close relationships are affected. Low retention and organizational commitment.
Risks relating to customers	Low customer satisfaction. Loss of potential customers. Loss of loyal customers.
Risks relating to company overall	Low productivity and efficiency. Decline in customers and profits. Difficulty for continuing business. Poor company culture.
Risks relating to reputation of company	Loss of reputation. Negative public response and media attention.
Risks relating to technology and equipment	Threats to privacy. Risks of losing confidential information. Data breaches.
Any others you can think of?	Diminished creativity and engagement from employees.

ACTIVITY 4

Choose three (3) of the Risks you have listed in Activity 2.

Using the Risk Matrix below, determine what rating you would give this risk.

Show to the person next to you and see if they agree with the risk rating you have given each of the risks.

		Consequence				
		How severe could the outcomes be if the risk event occurred?				
		1 Insignificant	2 Minor	3 Significant	4 Major	5 Severe
Likelihood (What's the chance of the risk occurring?)	5 Almost Certain	5 Medium	10 High	15 Very high	20 Extreme	25 Extreme
	4 Likely	4 Medium	8 Medium	12 High	16 Very high	20 Extreme
	3 Moderate	3 Low	6 Medium	9 Medium	12 High	15 Very high
	2 Unlikely	2 Very low	4 Low	6 Medium	8 Medium	10 High
	1 Rare	1 Very low	2 Very low	3 Low	4 Medium	5 Medium

Risk One	Rating Given	Staff Agrees?
Loss or corruption of data system	1	Yes
Disruption in business operations	2	Yes
Breaches of cyber security	3	Yes

ACTIVITY 5

Create a treatment plan for the three (3) risks you have identified in Activity 4.

Complete the Activity using the template provided.

Treatment Plan

Risk	Action required	Who is responsible	Due date	Measure of success	Review date
1	Cryptographic keys and digital credentials further secure the hardware and related information. This establishes a tamper-resistant environment for minimizing the risks of hardware breaches.	Security manager, IT manager, security team	20/03/2020	Risk is preempt at source.	22/03/2020
2	Strengthening critical infrastructure and using leading-edge DNS security capabilities for reducing risks associated with websites, spoofing and service disruption	Security manager, IT manager, security team	15/04/2020	Reduced number of risk events.	16/04/2020
3	Teaching the entire IT team about the identification of potential threats and adopts measures that will minimize the security breach.	Security manager, IT manager, security team	25/04/2020	Adoption of proactive risk management process.	26/04/2020

+++ END OF PAPER +++

AMP-116930-8-2400-FZML.