# Assessment event 2 of 2: Project – Risk Register

## Criteria

### Unit code and name

Cluster | Workplace Security

BSBXCS404 | Contribute to cyber security risk management

ICTICT443 | Work collaboratively in the ICT industry

ICTICT451 | Comply with IP, ethics and privacy policies in ICT environments

### Qualification/Course code and name

Select your Qualification/Course code and name from the dropdown.

ICT40120 | Certificate IV in Information Technology

## Student details

Student name

Student number

Version: 20231218

Date created: 18 December 2023

© TAFE NSW 2023  
RTO Provider Number 90003 | CRICOS Provider Code: 00591E

This assessment can be found in the TAFE NSW [Learning Bank](https://share.tafensw.edu.au/share/logon.do?.page=searching.do?in%3DC1b145167-45e0-41ec-9f64-92af668e3e54%26q%3D%26type%3Dstandard%26sort%3Drank%26dr%3DAFTER%26page%3D1).

The content in this document is copyright © TAFE NSW 2023 and should not be reproduced without the permission of TAFE NSW. Information contained in this document is correct at time of printing: 19 December 2023. For current information please refer to our website or your teacher or assessor as appropriate.

# Task 1: Risk management approaches

In this Risk Register, use the following risk control options.

Table 1 Risk management approaches

| Approach | Description |
| --- | --- |
| **Avoid** |  |
| **Control** |  |
| **Accept** |  |
| **Transfer** |  |

# Task 2:

## Risk identification

Table 2 Risk analysis

| Incidents and potential incidents | Explain why each is incident is a cyber security risk.  Describe the potential vulnerabilities of assets that could be affected by this risk, such as those related to IP, ethics and privacy. |
| --- | --- |
| **Cyber security incident 1:**  Employees collaborating in MS Teams using a work device from a cafe |  |
| **Cyber security incident 2:**  External contractor able to access and upload files in MS Teams |  |
| **Cyber security incident 3:**  Screen sharing during a team meeting displayed sensitive and confidential information |  |

## Risk analysis

Table 3 Risk analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Risk description | Likelihood | Consequence | Risk rating/Severity | Priority |
| 1 |  | [Choose an item] | [Choose an item] | [Choose an item] | [Choose an item] |
| 2 |  | [Choose an item] | [Choose an item] | [Choose an item] | [Choose an item] |
| 3 |  | [Choose an item] | [Choose an item] | [Choose an item] | [Choose an item] |

## Risk management

Table 4 Risk management strategies

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Risk control option | # | Cyber security response strategy | Personnel responsible | Benchmark |
|  | [Choose an item] | 1 |  |  |  |
|  | [Choose an item] | 2 |  |  |  |
|  | [Choose an item] | 1 |  |  |  |
|  | [Choose an item] | 2 |  |  |  |