HOW TO USE THIS TEMPLATE

An Introductory Point

This template is not designed to provide a full project Risk Management Plan (RMP), and it includes a copy of the Risk Register, which is normally not a part of this type of document. If you want to see what a full RMP looks like, you can generally find free copies on the internet. Most major organisations also have their own standards for these, so you would typically use theirs when you need to develop one for that company.

An RMP is normally created during the Planning Phase of the project. The intended audience is typically the Project Sponsor, Project Manager, project team, and stakeholders whose support is needed to carry out the plan.

Using this Template

Firstly, after downloading this template from the LMS, make a copy on your computer using the conventions discussed in the Assignment 2 Information instructions. As the next step, everyone in your team should carefully read the information in this RMP. You will all need to do this to complete the allotted tasks most effectively.

Text that is provided in black Times New Roman font, will remain in your final version of this RMP. The requirements are defined using blue font text shown in square brackets (e.g. [these are the instructions for the information that you need to include]). Read these instructions carefully, before you do your drafting, as they provide important hints and guidelines.

For this part of the assignment what you will need to do is:

1. add the project scope information into Section 2 *(you should use the same version that you used for the QMP and CP)*;
2. complete the Risk Register *(provided in Appendix 1)* as explained in Section 5.1; and
3. complete the EMV calculation and report, based on the scenario information supplied in Section 5.2 and provide the responses in the cells supplied in the associated tables.

When developing your responses, there is not a lot of writing to do for this. However, you will need to put a lot of thought into assessing the issues, so your solutions are sensible and reflect real-world practical issues.

Once you have drafted the required content, you should remove the [blue font instructions] so your material would then be ready to be forwarded to the Project Sponsor for final approval (as simulated by uploading this into the LMS). Additionally, you should remove the information on this page, so your response just starts with the Introduction on the following page.

In practical terms, once you have completed the draft (by taking the preceding steps) and the other required documents, these should be uploaded to the LMS in accordance with the Assignment 2 Information instructions.

Apart from the changes discussed in the preceding elements on this page, you must not change this template. This reflects real-world imperatives. Companies generally want you to conform to the templates that they provide. Therefore, get used to utilising standard templates now.

1 INTRODUCTION

1.1 Purpose of the Project Risk Management Plan

Risk Management (RM) defines the processes required for identification, assessment, mitigation, tracking, control, and management of a project's risks. RM should drive decisions that affect the development of the business capacity and the management of the project.

This Risk Management Plan (RMP) aims to give the EduStream project a consistent method for managing risks, to help ensure success.

1.2 Objectives of this RMP Document

Specific objectives of this RMP include:

- helping to ensure critical risks do not adversely impact on scope, schedule, budget, business performance, and/or Change Management, by proactively identifying, communicating, mitigating, and escalating such matters in a timely manner;
- facilitating the focussing of attention to key risks that are likely to adversely impact on the project and teams;
- ensuring that appropriate stakeholders are informed and, if applicable, engaging them in the mitigation; and
- recording an audit trail of discussions and mitigation processes implemented to manage project risks.

1.3 Guiding Principles

The following guiding principles shall be applied to effectively implement Risk Management:

- the Project Manager is responsible for making an overall risk assessment and reviewing it with the team and stakeholders;
- although Risk Management is the ultimate responsibility of the Project Manager, the administration and control will be supported by the Project Office (PO) and the Quality Group (QG);
- wherever possible, the risks will be addressed in the order of their expected severity;
- high impact, impending risks, will be managed with a rapid decision turnaround;
- realistic due dates will be set and then the team will make best efforts to meet those dates;
- identified risks will be managed and mitigated at the appropriate level *(i.e. project, working group, individual teams, etc.)*;
- stakeholders will be kept consistently informed about the current risk status; and
- planned Risk Management and the mitigation history will be documented, and wherever possible such documentation will include root cause analysis, key learnings and metrics, so similar future risks can be identified and mitigated more effectively.

2 PROJECT SCOPE

[[Instructions for what to include in this section: **Please note that you should use the same Project Scope statement that you developed for the QMP and CP. Therefore, please carefully read and follow the instructions for Section 2 of the QMP.**]

Insert your material here.

3 RISK MANAGEMENT ORGANISATION

3.1 Process Responsibility

The Project Risk Manager (PRM) will be the EdMedia International (EdMI) Quality Team Manager (QTM) for this project. In this role, the PRM is directly responsible to the Project Manager for all aspects related to Risk Management.

The PRM has overall responsibility for:

- developing and implementing Risk Mitigation Plans;
- maintaining the Risk Management Plan, in line with the standard configuration management procedures;
- generating risk reports, including trends and metric analysis;
- clarifying, consolidating and documenting risks;
- maintaining and monitoring data in the Risk Register;
- monitoring the status of risk mitigation;
- communicating the status of risks and mitigations to risk owners;
- escalating communication/action, if expected mitigation action deadlines are unlikely to be met; and
- executing the risk closure process.

The PRM may delegate these responsibilities to other team members for implementation, but the accountability to the Project Manager will always rest with the PRM.

The Project Manager will have overall responsibility for ensuring the Risk Management Plan is executed appropriately. Specific Risk Management responsibilities of the Project Manager include:

- approving the mitigation of very high severity level risks;
- supporting mitigation implementation as appropriate; and
- assisting in cross-organisation and controversial risk mitigation, to facilitate involving senior personnel from other organisations and their resources.

3.2 Risk Owners

The Risk Owner (RO) is the person to whom the PRM assigns primary responsibility for managing/mitigating the risk. This assignment of responsibility will be based on the type of risk and will normally be delegated to the team member who can be empowered to assure this risk is managed/mitigated. This will typically be a Team Leader and/or their respective co-lead. Other stakeholders can also be delegated as Risk Co-Owners (RCO), so appropriate skills and authority can be applied to manage and mitigate the risk. However, the RO will always be directly responsible to the PRM for managing/mitigating the assigned risk.

The RO and RCOs (as appropriate) will take the following actions:

- assessing the risk and creating a Risk Response Plan that meets the PRM approval criteria;
- mitigating/controlling risks in accordance with the specified Risk Response Plan;
- recommending risk closure to the PRM once the risk has been mitigated/controlled/ ameliorated appropriately; and
- presenting risk status information at Quality Team meetings, as required.

4 RISK MANAGEMENT PROCESS

Apart from Planning, risk management involves five major phases, which are: Identify Risks, Analyse Risks (Qualitative & Quantitative), Plan Risk Responses, Implement Risk Responses, and Monitor Risks. These are discussed in the following subsections.

4.1 Identify Risks

The ability of our team to identify risks that may affect project outcomes is extremely important. Once a risk has been identified, it must be logged into the Project Risk Register. The Risk Register includes the following information:

1. ***REF ID.*** This is a unique identifier for each risk. Typically, it is a sequential number.
2. ***Description of the Risk.*** A description of each potential risk event is provided in this column of the Risk Register. In many cases, this is supported by more detailed information in separate documentation or notes associated with the Risk Register.
3. ***Potential Impact of the Risk.*** A short explanation of how the risk could affect the project is included in this cell. These are typically defined in terms of aspects such as the impacts on safety, pricing/costs, scheduling, technical, etc. In many cases, this is supported by more detailed information in separate documentation, or notes associated with the Risk Register.
4. ***Risk Level.*** The risk level is typically developed from qualitative analysis. This uses a matrix that includes the probability of occurrence and the impact/seriousness if it does *(see Figure 1)*. The information within this cell should be VH, H, M, L or VL, which equate to Very High, High, Medium, Low, or Very Low. Additionally, a risk score can be added in this section. Risk scores are often developed from Qualitative Analysis (see Section 4.2.2) but may also be defined through different Quantitative Analysis models.
5. ***Risk Owners.*** This column of the Risk Register is used to provide details of the RO and any RCOs who will be responsible for managing the risk. In some cases, this includes contact details, however, this is not required in this version of the Risk Register.
6. ***Date Reported.*** The date on which the risk was reported is included in this column. This allows the age of the risk to be identified effectively, so it becomes clear which risks are slow to be addressed.
7. ***Control/Contingency/Fallback Strategies.*** Include the strategies proposed for dealing with the risk *(preventative, contingency, contingency reserves, fallback, etc.)*. Where necessary, these should be provided as fuller descriptions in separate documents or notes attached to the Risk Register. It is important that this information provides enough content to allow a reader to understand the steps/strategies that will be taken to manage the risk.
8. ***Due Date.*** The due date assigned for completing the risk mitigation/controls defined in the preceding column should be included in this column. When developing this due date,

the team should ensure that the projected resolution duration is appropriate *(e.g. if it is a Very High Risk or High Risk it should be addressed in a very short time frame)*.

9. ***Risk Status.*** The risk status is typically defined as Open or Closed. However, some organisations include other terms such as Escalated or Pending. The information in this cell can then be used to find specific types of risk, such as those ones that are still open.
10. ***Date Closed.*** The column for Date Closed refers to the day on which the risk was officially closed. In some cases, this is an automatic field that updates when the risk status is changed. Including this field allows the team to investigate metrics such as average time for closure of risks *(i.e. the average for Date Closed minus Date Reported)*.
11. ***Lessons Learnt.*** The lessons learnt is an important field, because it allows future projects to proactively identify risks and solutions that worked or did not work. This information is often provided as a link/field for a detailed file, or a note in the Risk Register, which explains issues related to the root cause, and other key factors that could need to be addressed in future projects.

Please note that the last three of these Risk Register elements are not included in the example provided within Appendix 1, as they are not directly pertinent to this assignment.

4.2 Analyse Risks

Risks are analysed using Qualitative and Quantitative methods. Such analysis can be conducted in parallel or in tandem *(e.g. one after the other)*. These types of analysis can be categorised as explained in the following subsections.

4.2.1 Qualitative Analysis

Qualitative Analysis is a method for assessing the level of risk, by entering the probability of occurrence and the impact of an occurrence using a matrix, such as the one provided in Figure 1. This is achieved by defining each issue in terms of the general criteria to the right of this diagram.

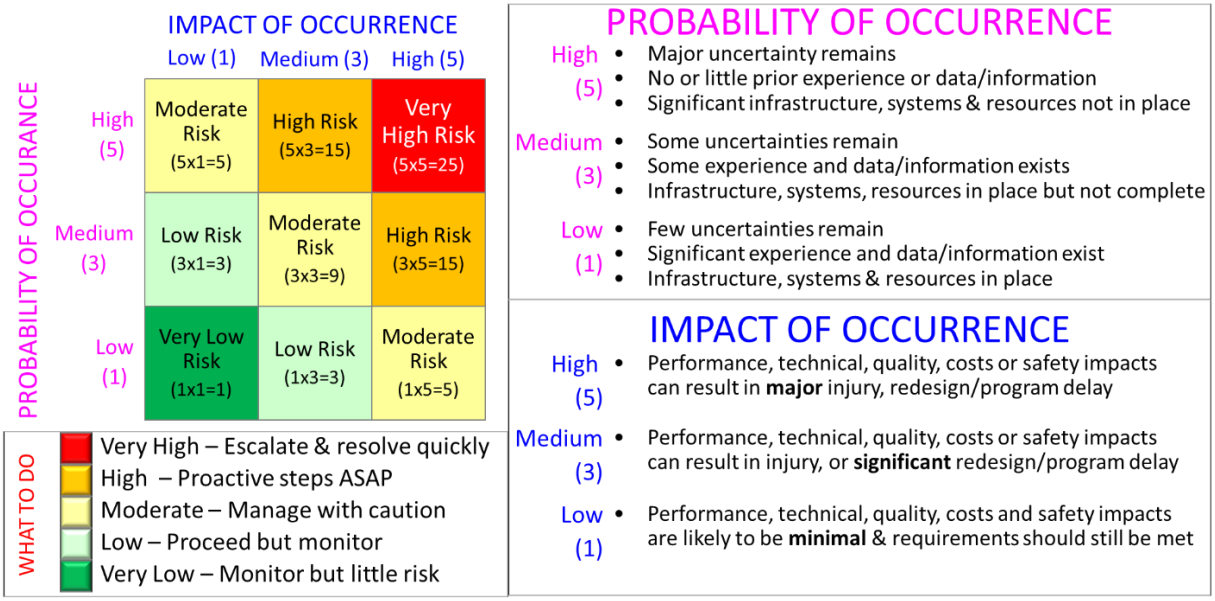

Figure 1: Qualitative Analysis Matrix

Once this qualitative analysis has been completed, take appropriate action as defined in Table 1

Table 1: Actions to be taken for different levels of Qualitative Risk

Score	Definition/Actions to be taken
Very High (25)	Anything classified as **Very High** indicates that this risk is extremely or very likely to occur. Additionally, the occurrence could have a profound impact on the project's safety, technical, cost, and/or schedule, which may cause the project to be terminated or can cause significant cost/schedule changes *(e.g. increases of more than 5 percent)*. The management of this level of risk should be escalated, and that aspect of the project must be implemented with *extreme care* until the risks can be mitigated/controlled effectively.
High Risk (15)	**High Risks** may cause significant safety, technical, cost, and/or schedule increases *(e.g. increases of 2 to 5 percent)* for the project. These risks are to be managed proactively, and a priority must be applied to mitigate/control the risks as soon as practicable. In the meantime, the elements of the project associated with this risk must be managed with due care.
Moderate Risk (5 or 9)	This refers to risks that are **Moderate**, because they may have a relatively small but significant impact on the project's safety, technical, cost, and/or schedule *(e.g. generally less than 2 percent variance)*. Appropriate mitigation/control strategies should be implemented as soon as it is practicable. Obviously, risks with a score of nine (9), should be addressed with higher priority than those with a score of (5). While awaiting mitigation/controls to be implemented, the team should still manage this aspect of the project with care.
Low Risk (3)	A **Low Risk** refers to an event that is relatively unlikely to occur, or the impact would be low if it did occur. In other words, this refers to situations in which the combination of likelihood and impact means that this risk would not be expected to have a significant impact on the project's safety, technical, cost and/or schedule. Typically, consolidated risk management is not applied to these types of risks. However, the team associated with this aspect should keep it in mind while implementing the project and monitor the issue with an appropriate level of caution.
Very Low Risk (1)	A **Very Low Risk** refers to matters where it would be unlikely for the risk to occur and even if it did, the impact is expected to be minimal. In these circumstances, consolidated risk management would not be applied. However, as with all aspects of Risk Management, those involved with the project should continue to monitor evolving levels of risk and take proactive action when considered appropriate.

4.2.2 Quantitative Analysis

Where considered appropriate, Quantitative Analysis should be conducted. This may entail techniques such as statistical analysis (including Expected Monetary Value) and decision trees, simulations, or sensitivity analysis.

4.3 Plan and Implement Risk Responses

Where the risks are identified as being Very High, High, or Moderate, an RO *(and possibly one or more RCO)* will be allocated to manage the risk. They will begin this activity by developing a Risk Response Plan. This plan is used to provide options and action plans, which can help to reduce the threats associated with the identified risk.

To facilitate these activities the RO/RCO will be required to interact with all appropriate stakeholders, to identify suitable solutions/options for mitigation/control. They will then submit their plan to the PRM *(or their delegate for that level of risk)*. Once the plan is approved, the Risk Register is to be updated with specific and suitable details related to the proposed plan. Additionally, appropriate changes are to be implemented through the Change

Management, Configuration Management, Problem Management, and/or Issue Management systems. Where necessary, such changes should also be applied to other documentation, including the Project Management Plan *(and its sub-documents)* and the Work Breakdown Structure/Schedule. Appropriate steps must then be taken to implement the approved risk management steps within an appropriate timeframe.

4.4 Monitor Risk – *to trigger steps to control risks*

Risk Monitoring and Control is the process of identifying, analysing, and planning for newly identified risks, monitoring previously identified risks, and re-evaluating existing risks, to verify the effectiveness of planned risk response strategies.

Activities involved in Risk Monitoring include:

- establishing periodic reviews and scheduling them in the project plan;
- ensuring that all requirements of the Risk Management Plan are being implemented;
- assessing identified risks that are defined in the Risk Register;
- identifying the status of actions to be taken;
- validating previous risk assessments *(in terms of assessed likelihood and impact or the utilisation of qualitative methods)*;
- validating previous assumptions and stating any new assumptions that are defined;
- evaluating the effectiveness of actions taken to mitigate/control risks;
- identifying new risks;
- tracking risk responses; and
- communicating Risk Management status *(and risk response follow-through as appropriate)* to pertinent stakeholders.

Activities involved in risk control include:

- validating risk mitigation strategies and alternatives;
- taking appropriate corrective action when actual events occur;
- assessing the impact on the project of actions taken *(cost, time, resources)*;
- identifying new risks resulting from risk mitigation actions;
- ensuring that the project plan *(including the Risk Management Plan)* is maintained;
- ensuring that Change Management addresses risks associated with the proposed change;
- revising Risk Management documents, to capture the results of mitigation/control actions;
- updating the Risk Register; and
- communicating Risk Management status *(and risk response follow-through as appropriate)* to pertinent stakeholders.

4.5 Risk Escalation Procedures

Most Risk Management decisions will be made within the Quality Group (QG) led by the EdMI Quality Team Manager (QTM). Escalation to the Project Manager will take place when:

- Very High, or High, risk issues are identified;
- there is a need to coordinate Risk Management across organisations and the level of authority needed to manage the risks is beyond the capabilities/authority of the members of the QG; and
- when the QTM or Project Manager considers it appropriate.

Such escalations are implemented to help ensure that the risks can be mitigated or ameliorated effectively within the appropriate timeframe.

4.6 Risk Closure

Once an identified risk has been appropriately controlled/mitigated, this should be reported to the QTM by the RO as soon as possible. Where a risk has been escalated, the QTM is to advise the Project Manager as soon as it is practicable.

Prior to closure, the QTM *(or the Project Manager if the risk has been escalated)* is to take appropriate steps to ensure that the risk has been appropriately mitigated. Once they are confident that appropriate mitigation has been implemented, they will officially change the status in the Risk Register to closed.

4.7 Risk Management Closeout

At the completion of the project, there will be a transition of any open risks, and the capturing and harvesting of lessons learnt. These are important for future project maintenance and support. Additionally, this activity can assist in the management of future projects. Key activities that are to be undertaken during this phase include the following:

- validating the closure of identified risks *(i.e. ensuring that they have been closed appropriately)*;
- for any open risks, assess whether there are ongoing operational/technical risks that warrant communication of these matters to other stakeholders;
- documenting remaining open risks within an accessible final report;
- producing final Risk Management metrics and evaluating the process effectiveness against established benchmarks; and
- capturing risk factors and Risk Response Plans for inclusion in Risk Reference Models.

5 WHAT YOU NEED TO DO

5.1 Task 1

[Instructions for what to include: The first step will be to identify possible risks associated with the implementation of this project. This exercise is best managed through a workshop discussion involving your entire group.

Your team needs to take the following steps:

(1) Make sure that you have all carefully read and understand the information provided in this RMP before the meeting, so you have key knowledge that you will need to complete this exercise properly.

(2) You may find it easier to do the next steps if you use the template provided for the Risk Breakdown Structure *(see the LMS under Topic 9)*.

(3) Carefully read the Assignment 2 information and other ancillary information/guidance that has been provided. From this, identify any likely risks that could affect the EduStream project (many of these have been outlined in the materials – especially the Topic 9 Workshop).

(4) Additionally, think about any other realistic risks that could adversely affect the project. To achieve this objective, you will need to think about issues that are likely to have been disclosed through previous parts of your work during the semester. Additionally, think about real-world issues that may have an influence *(e.g. political, macro-economic, social, technical, etc.)*.

A USEFUL HINT ON SELECTING WHICH RISKS TO INCLUDE IN YOUR RISK REGISTER – THE RISK IDENTIFICATION PROCESS

Be careful to avoid risks related to imprecise, so-called 'motherhood' statements. For example, risks like 'delay in the project', 'technical faults and errors', 'resource issues', 'financial stability', or 'employee negligence' are not valid (but all were included as risks by members of previous cohorts). Please don't fall into the same trap. These types of statement do not reflect the risks that need to be included.

In your Risk Register you need to ensure that all of the identified risks meet the following key criteria:

- ***The risk must be realistic and there would have to be something that you can do about it.*** There is simply no point including risks where the chance of them occurring are very remote and they would not be manageable anyway. For instance, a risk like 'we could be hit by a meteorite' is not worth including.
- ***Make sure it is specific.*** Ensure that the risks you include are specific enough to be scoped effectively for management. As an example, you would not include 'Human Resources' as a risk in the register. This type of statement simply does not mean anything! Alternately, making a statement like 'Inability to recruit qualified personnel for the Level 2/3 support team' would be valid. In this case, it refers to a Human Resource issue, but it has been scoped so the risk is clear. Just as importantly, there are a number of strategies that you could implement to manage this risk.

(5) Insert a short description for each of the risks that you identify through steps (3) and (4) into the Risk Register provided in Appendix 1. Where you need to provide more detail, include a very short description in the appropriate cell for that risk, and refer the reader to a specific Note number (see below). You can then write a Note into the appropriate section below the Risk Register Table.

(6) Next, for each risk, insert potential impacts of the risk. You need to think about these in terms of issues such as safety, pricing, cost, schedule, technical, security, etc. If you can effectively describe these elements in the table cell for each risk, do so. If you cannot fully describe the risk impacts, you can add a short descriptive note into the cell and then direct the reader to an appropriate Note provided below the Risk Register table.

(7) Carefully assess the risk level for each of the risks that you have identified. Mark these as VH, H, M, L or VL in line with the qualitative assessment that you make (see Sections 4.1 and 4.2.1). Additionally, you can optionally include the risk score as well. **This aspect is really important**. Your team need to think carefully about this, so the assessment is realistic.

(8) Assign a Risk Owner (RO) *(and Risk Co-Owners (RCO) where appropriate)*. Do not insert names but include the appropriate role identification/s from the Stakeholder Engagement Matrix *(Provided in Topic 7)*. It is important that you assign the right people to address each risk. Remember, they will need the expertise/authority/capability to manage that risk.

SOME USEFUL HINTS ON ALLOCATING RISK OWNERS

- Firstly, do not just insert RO/RCO in the Risk Owner's column. You need to include appropriate role titles as specified in the preceding point.
- Do not just allocate the Project Manager as the RO for everything. Trust me, you will have plenty of other things to do as the Project Manager, so you will need to delegate the RO/RCO responsibilities to other people. Put some thought into this. The key is to ensure that the RO/RCO is appropriate for that risk. As an example, if the risk is defined as: 'Client Software tokens may not stop unauthorised usage of the system', you would allocate the RO/RCO roles as follows:
  - ***RO:*** The PM StreamTech (because his team is responsible for developing the Client Software, so this role would take the primary responsibility).
  - ***RCOs:*** The DemSet Web Team Leader, DemSet DB Team Leader, DemSet Security Manager (because these people will be responsible for managing elements of the system that will handle the token to protect against unauthorised access).

(9) For the Date Reported, just insert the date for the day on which you held the workshop to identify the risks.

(10) For each risk, you need to include sensible and practical control/contingency/fallback strategies. You can provide a synopsis in the cell, and if necessary, expand on this within an associated Note. It is very important that you think about this carefully because this aspect will have the highest weighting in the scores allocated to this part of the assignment.

WHAT IS REQUIRED FOR CONTROL CONTINGENCY & FEEDBACK STRATEGIES?

- The strategies that you define must be practical and assist you to manage the risk appropriately. This approach is discussed in the Topic 9 Lecture and Workshop in more detail. In essence the three levels can be defined as follows:
  - ***Controls:*** Controls are approaches that are implemented to help avoid negative risks or induce positive risks. In other words, they are the things that you will implement from the outset, even before the risk event occurs.
  - ***Contingencies:*** A contingency strategy refers to primary actions that you will take if the risk occurs. Obviously, if it is a negative risk, the contingency should be designed to mitigate, or reduce the impact of, the risk. Alternately, if it is a positive risk, the contingency should be designed to optimise the outcomes from that event.
  - ***Fallbacks.*** Whereas Contingencies are effectively 'Plan A' in the event of a risk occurring, Fallbacks are implemented when the Contingency approach does not provide the required result or outcome. You can, therefore, consider these 'Plan B'. In some cases, you will have more than one Fallback. However, for this assignment, just think about defining the one that is likely to provide the best outcome if the Contingency plan does not work.

(11) The Due Date for each risk should be entered. **Make sure that this aligns to the level of risk that you identified**. For example, Very High risks should be addressed as soon as possible. You can get guidance on this within Table 1 (above). Additionally, **take**

into account the project schedule, as this will also help to drive your decision making on this aspect.

(12) You must **provide a minimum of 30 *additional* realistic Moderate to Very High risks** in your Risk Register *(Note - that you can include Positive/Negative risks)*. The more realistic your risks are, the higher your assessment score will be. At the moment, 33 rows have been included in the Risk Register. This is because three examples have been provided in the table, so you can see what is required. If you need more rows because you have identified more risks, just add them and make sure that they are sequentially numbered.

(13) Where you have complex information to include in the Risk Register cells, make a synopsis statement about this in the table and refer to a specific Note. These notes are auto-numbered, so just point the reader to the right number by inserting the text 'See Note # for more information' – where # is the Note number.]

5.2 Task 2

Your team has been contacted by the Project Sponsor because the Board is thinking about adding a fourth Pilot site into the project. The options for this are Brisbane, Adelaide and Darwin. Your team has been asked to implement an Expected Monetary Value (EMV) analysis based on the following information. This data was developed by the EdMI Marketing Department based on:

- the expected additional costs associated with implementing that node in Year 0;
- the probabilities for different levels of demand for the EduStream services, based on a statistical analysis of various prospective clients *(defined as probabilities of Strong, Moderate or Weak demand)*;
- costs are based on establishment and operation of the additional node for ***Year 0 and Year 1***; and
- the expected revenue that is ***likely to be generated within the first year if the demand*** is Strong, Moderate or Weak *(please note that these figures have already been adjusted for Net Present Value)*.

Decision Node	Cost	Chance Node	Chance Probability	Expected Revenue for Demand Type	Differential (Profit/Loss)	Profit/Loss x Probability
Option 1: Brisbane Node	$ 2,100,000	1A: Strong Demand	20%	$3,700,000		
		1B: Moderate Demand	30%	$2,600,000		
		1C: Weak Demand	50%	$1,700,000		
Option 2: Adelaide Node	$ 2,400,000	2A: Strong Demand	35%	$3,500,000		
		2B: Moderate Demand	40%	$2,800,000		
		2C: Weak Demand	25%	$1,500,000		

Decision Node	Cost	Chance Node	Chance Probability	Expected Revenue for Demand Type	Differential (Profit/Loss)	Profit/Loss x Probability
Option 3: Darwin Node	$ 1,800,000	3A: Strong Demand	30%	$3,100,000		
		3B: Moderate Demand	30%	$2,200,000		
		3C: Weak Demand	40%	$1,400,000		

EMV Option 1 (Brisbane)	**EMV Option 2 (Adelaide)**	**EMV Option 3 (Darwin)**
Recommendation on which Project to Implement		
Insert your answer here		

[Instructions for what to include in this section: Using the information provided in the first table above:

(1) Work out the expected Differential (Profit/Loss) and Profit/Loss x Probability and insert these into the columns provided in the upper table.

(2) Using the processes discussed in the Topic 9 workshop, work out the EMV for each project, and insert the results into the allocated cells within the lower table provided above.

(3) Finally, in the bottom cell of the answer table, write a statement that explains your recommendation for project selection. When developing this part of the response, begin by discussing the direct outcome of to the EMV calculation. However, please note that EMV is typically not just assessed on its own. Other real-world factors would also be assessed. For example, in this case you would need to think about the following:

a. The risk profile of the various options should be assessed. For example, are there options where the risk of low demand is higher than the others. If so, think about why this might be the case and whether this should influence the decision.

b. Think about the population size for the three options and therefore the likely size of the market in each city. Additionally, assess a range of other aspects such as future population growth, as this might change the outcome noting that the revenues in this case are only covering the first year of operation.

c. Assess the implications related to selecting different cities. For instance, establishing the node in which of these three cities would help us to engage with the National Indigenous Australians Agency. Noting that this would be a large client that could provide guaranteed cashflow, should this change the decision?

d. What are the macroeconomic conditions likely to be during the period and is there likely to be differences in their impact on these different cities? As a hint, it is typically best to select cities for nodes where their economic power and growth are likely to be less affected by the expected economic situation.

e. Think about the availability of technical infrastructure in the various cities (e.g. the presence of Tier 3 datacentres or network connections such as cheap high bandwidth backhauls) as these will influence the feasibility, risks and costs related to the project.

f. Think about the fact that the costs for Year 0 and Year 1 are included, but the revenues only cover the first year of operation. If we were to take into account costs and revenues over five years, is this likely to make a difference in the outcome? You don't need to work out the longer projections, just think about the implications in terms of the preceding points.

When you get out into the industry always look at these bigger picture issues and put them into the context of risks.]

A USEFUL HINT FOR MANAGING THE EMV RESPONSE

If you get the EMV calculation correct, this is worth a maximum of 60% of the total marks for this question. The remaining 40% of the marks will be allocated in terms of how well you look at the bigger picture issues. This is an important point to remember. Real success in the industry comes to those people who can not only assess the specifics (such as an EMV calculation) but can also make informed and well-reasoned decisions based on much broader issues. This is the type of skill that is widely in demand in the ICT industry. Consequently, the last part of this question is designed to help you build this skill.

REF ID	Description of the Risk *(Insert a short description of the risk)*	Potential Impact of the Risk *(Explain the impact of the risk in terms of safety, pricing/costs, schedule, technical, security, etc.)*	Risk Level (VH/H/M/L/VL)	Risk Owner/s (RO/RCO)	Date Reported	Control/Contingency/Fallback Strategies *(Provide a synopsis of the approaches that you are proposing to manage this risk. Remember that this approach must conform to the RMP framework.)*	Due Date (For Plan/Action)
1	Netflix not providing rights to utilise OCA Equipment (see Note # 1 for more information)	EduStream will not have a video streaming server. As this is a core element of the system, this lack would have significant cost, schedule and technical impacts	H (15)	CIO/ EdMI PM, StreamTech PM	2/03/23	***Control:*** Continue negotiations and secure the utilisation of the OCAs. Offer resource sharing. ***Contingency:*** Deploy through Netflix and become a content provider (this has significant business & technical implications). ***Fallback:*** Utilise another video streaming engine (develop or reuse another COTS solution). This fallback could have a significant business/technical impact.	16/03/23 (See Note 2)
2	Planned client software tokens may not stop unauthorised usage of the system	Unless the token system can be made foolproof there is a high probability that security protocols can be breached, and unauthorised users will gain access to content. This will have significant cashflow, technical and security ramifications.	VH (25)	DemSet PM/ StreamTech PM, EdMI Security Advisor	31/05/23	***Control:*** Investigate and implement 128b token solution including storage of tokens in the Client DB. Do extensive white hat hacker security testing. ***Contingency:*** Option up to a 256b token. Do extensive hacker security testing. ***Fallback:*** Option up to a 512b token and implement more rigorous multi-level security measures.	09/07/23 (See Note 3)
3	Inability to recruit appropriately skilled personnel to provide Level 2/3 Support	This means that we would only be able to deliver Level 1 support through the MBSD. Lack of this Level 2/3 service may make it difficult to resolve technical risks quickly. A shortfall of this nature could adversely impact on our ability to deploy a stable system and encourage corporate groups to engage. This will have significant cashflow and technical development implications	M (5)	CIO/ EdMI HR Manager	2/03/23	***Control:*** Start the recruitment process early and engage the recruited staff member during project and document development, so they have time to understand the system intimately prior to deployment. To help ensure the right people are engaged, ensure that the monetary offering and conditions are competitive. ***Contingency:*** Engage StreamTech and DemSet on long term support contracts to provide the support. This would have to be a tight contract to control cost blowouts. ***Fallback:*** Headhunt a person with the appropriate skills from an employment agency.	05/04/23 (See Note 4)
4							
5							
6							
7							
8							
9							
10							
11							

REF ID	Description of the Risk *(Insert a short description of the risk)*	Potential Impact of the Risk *(Explain the impact of the risk in terms of safety, pricing/costs, schedule, technical, security, etc.)*	Risk Level (VH/H/M/L/VL)	Risk Owner/s (RO/RCO)	Date Reported	Control/Contingency/Fallback Strategies *(Provide a synopsis of the approaches that you are proposing to manage this risk. Remember that this approach must conform to the RMP framework.)*	Due Date (For Plan/Action)
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							

NOTES: [Add your notes below. Autonumbering is used, so to add a new note, just press enter at the end of the note.]

(1) At this stage, our team has assumed that EduStream can utilise OCAs, which may be provided for free or at low cost. However, negotiations with Netflix are ongoing and the use of this technology has not been finalised.

(2) This needs to be done before we go out to tender, which is why the early date has been selected.

(3) This date is late in the design and prototype phase, so we would test this carefully before making a decision, but also leave scope in the design to change it out if necessary, without making fundamental changes to the architecture.

(4) This should kick off early engagement through recruitment.