

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

The EduStream project is an ambitious initiative to develop a comprehensive streaming platform, providing users easy access to various educational content, including videos and interactive games. To successfully achieve this goal, the project will involve the collaboration of eight specialised groups, each contributing their expertise to various aspects of the project.

The Web Development Group, led by James Wasley, Project Manager, will focus on creating the front-end user interface, ensuring a user-friendly experience that allows users to navigate the platform and access content easily. In parallel, the Client Database Group will be managed by Jin Cherng Chong, EdMI Quality Team Manager (QTM), and they will develop a secure and efficient database system to store user information, manage access control, and enable personalised content recommendations.

The Video Streaming Group, led by Nicholas Caruso, Quality Lead StreamTech, will be tasked with implementing the Open Connect Appliances (OCAs) to ensure the efficient streaming and delivery of video content to users while optimising the video format and compression for optimal performance. The Games Development Group, led by Steve Jobs, Quality Lead DemSet, will manage the development and integration of educational games, working to ensure seamless streaming and secure access controls through the implementation of software tokens.

To monitor and optimise system performance, the System Health Management Group, led by Bill Gates, EdMI Test Manager (TM), will develop a monitoring and management solution to track the performance and utilisation of the various components within the CDN nodes, enabling load sharing. Meanwhile, the Client Application Development Group, led by Roy Clark, StreamTech Test Lead, will create the client application, ensuring compatibility across various devices and operating systems, including Android, Apple, and smart TVs, while integrating the necessary codecs and control interfaces for a seamless user experience.

The Network Engineering Group, led by Pardeep Kaur, DemSet Test Lead, will focus on establishing reliable and high-speed network connections between the clients and CDN nodes, ensuring consistent performance and efficient content delivery. Lastly, the Security Group, led by Catherine Dobbs, DCPlus Quality Manager (QM), will be responsible for implementing a comprehensive security strategy, encompassing physical security, secure network connectivity, application security, and database encryption to protect user data and maintain the platform's integrity.

Throughout the project, Rajiv Singh, MBSD Quality Lead (QL), will oversee the overall quality aspects and ensure adherence to quality standards. Angele Smith will serve as the EdMI Document Controller (DC) to manage project documentation, and Dan Hill will be the JP-Media Client Support Manager, responsible for client support and communication.

The project will involve the development of a client application and establishing three Pilot Content Delivery Network (CDN) nodes in Perth, Sydney, and Melbourne. As the project progresses, additional capabilities such as load sharing, batch updates, and database replication will be implemented, ensuring consistent performance across all nodes and accommodating future growth. Once the pilot sites have been tested and refined, the EduStream system will be ready for further expansion through the deployment of additional nodes as needed.

To ensure stakeholder satisfaction, the project will track and evaluate its financial performance using Earned Value Management (EVM). EVM results, including profits and targeted

outcomes for stakeholders, will be regularly analysed and reported to provide insights into the project's financial success and its alignment with stakeholder expectations.

In keeping with the ambitious yet feasible timeline set out for this project, the transition from the project phase to the full operational environment for the EduStream platform is planned for December 15, 2023. This date marks the full market opening and the beginning of the platform's availability to educational institutions and students nationwide. It's important to note that this transition represents the culmination of extensive collaborative efforts, risk management, and adherence to relevant standards and laws, thus facilitating a smooth shift to the operational phase.

In summary, the EduStream project represents a forward-thinking initiative to revolutionise how users' access and engage with educational content. Through the combined efforts of the eight specialised groups and the careful consideration of various technical, network, and security requirements, this project aims to deliver a high-quality, scalable, and secure platform that will bring the world of education to the fingertips of users everywhere.

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.

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.

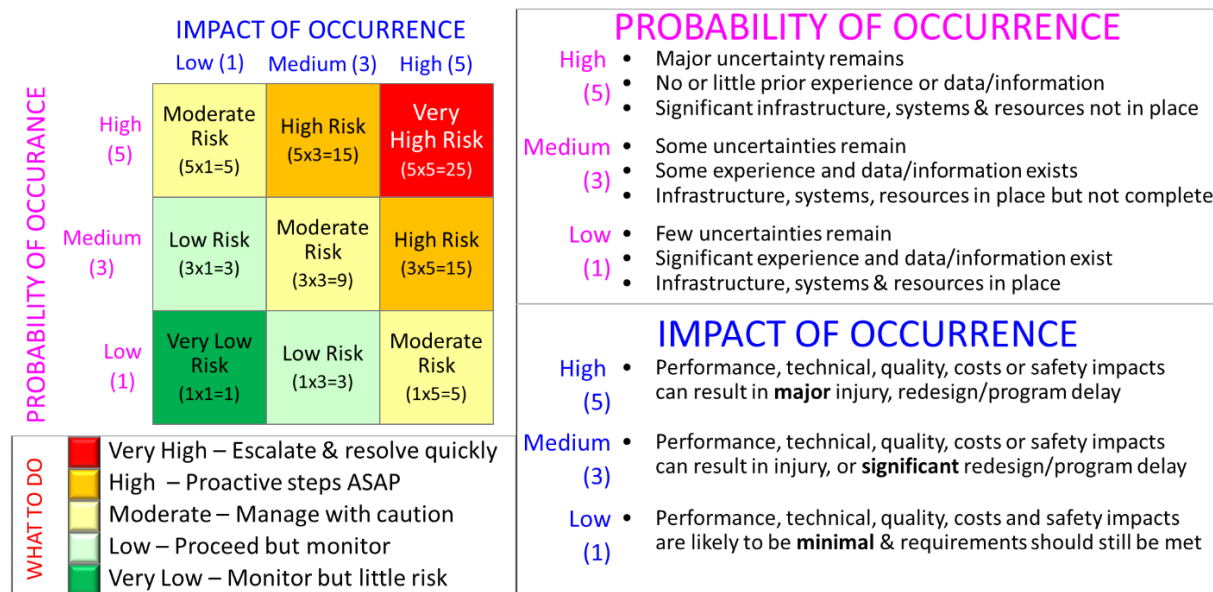


Figure 1: Qualitative Analysis Matrix

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 <i>extreme care</i> 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 Risk Appendix 1

5.1 Task 1

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.	05/04/23 (See Note 4)

						Fallback: Headhunt a person with the appropriate skills from an employment agency.	
4	Artificial intelligence being leveraged as a chatbox providing on demand customer support	EduStream integrates chatbox as the first line of communication for clients. Swiftly and accurately resolving common customer service enquiries. Leading to better customer service MBSD customer service being deployed to other critical areas	M (9)	EdMI FAQ Web Site Lead and EdMI Wiki/Knowledge Base Lead	26/2/2023	Controls: Keep up to date with the latest advanced in AI. Attend AI related conferences and information sessions. In addition, follow the popular major chatbot development companies. Research and investigate integration of chatbot to EduStream service. Contingency: Implement the chatbot and get customer feedback in response to their performance and interactions Fallback: Implement the chatbot in limited areas such as replacing common questions and answer page and implementing the chatbot only when current MBSD support is in high demand and is unable to provide timely support or responses	31/3/2023
5	Contractors specifically DCPlus not meeting the standards and deadlines such as the EduStream rack allocation uptime is not consistent	EduStream having utilising a datacentre which fails to keep the rack online impacts EduStream reputation. It annoys customers and often results in them cancelling their service which means loss of revenue	H (15)	Client Manager	23/6/23	Controls: Contracts should clearly stipulate the EduStream specific demands such as the datacentre needs to have x amount of uptime. And a heavy fee for breaching the contract should be included. Must include ability to export the EduStream existing data to another datacentre upon request or breach. Contingency: Contact the DCPlus and enquire about the lack of uptime and ensure it is resolved and/or the fee must be paid. Fallback: Export the EduStream data and transfer to another viable datacentre	3/4/2023
6	Lack of future educational content exclusivity	With the rise of streaming service content distributors are aware of the leverage that they have in streaming negotiations. The impact of exclusivity being more burdensome to obtain is the operation cost. This may result in less content being available to customers and may cause discontent.	H (15)	EdMI Educational Content Expert EdMI's legal and contractual expert	10/2/2023	Controls: Negotiate with common partners whom offer consistent pricing. Invest in more independent and local films Contingency: Invest only in popular education content and ones which are streamed by subscribers and clients Fallback: Price rices for subscribers	30/8/2023

7	Possible of revenue through advertisements	EduStream are able to place ads that don't annoy consumer on the web page or hide subtle ad placement during consumption	VH (25)	StreamTech Project Manager and StreamTech Client Software Team	15/2/2023	Controls: Inform organisation of the opportunity to advertise on EduStream streaming platform. Provide low rates and incentives to attract advertisers Contingency: Roll out subtle ads and acquire customer feedback. Offer customers a discounted rate to accept ads Fallback: Offer advertisements during emails and during movie selection or restrict it to movie related advertisements	5/2/2024
8	Less loyal clients	When it comes to streaming services there is a difficulty in customer retention. The lack of loyalty with customers and streaming platforms makes it difficult to forecast and make accurate spending decisions in the future	VH (25)	EdMI Project Sponsor and EdMI Marketing Manager	26/2/2023	Controls: Offer cheaper deal for long term subscribers and offer incentives such as diverse and more content choices Contingency: Offer services to more bigger institutions whom rely on these content types Fallback: Downsize the catalogue offered and only offer targeted content that subscribers enjoy	5/2/2024
9	Educational content being pirated	EdMI will need to be aware of online piracy being problematic understand that all our exclusive content may be pirated and distributed illegally. This could lead to decreased in revenue if more people are lured into piracy	H (15)	EdMI Lawyer and EdMI Educational Content Expert	20/2/2023	Controls: Implement video streaming technology where screen recording is disabled and display notices that indicate the company seeks to prosecute any educational content theft Contingency: Report to authorities and demand websites that host the content to cease and desist hosting the content Fallback: Monitor the number subscribers and judge whether pirated content affects the client retainment	4/12/2023
10	Poorly written End User licenses Agreement (EULA)/ contract	Without a well written EULA or contract, EdMI's rights are not protected in relation to EduStream. It highlights the possibilities of breaches with safety, confidentiality and security with the two entities	H(15)	EdMI's legal and contractual expert, CEO & PM	20/04/2023	Controls: During the process of drafting the EULA or any other contracts, seek extra advice from our lawyers/law firms that specialise in the specific contract/agreement. Contingency: regularly checking any agreements/contracts to see if they need any amending. Fallback: Seek opinions from outside law firms/lawyer or hire a lawyer qualified for the position and needed tasks.	25/05/2023
11		During the testing and release phase, EduStream may experience missing features, which can have negative consequences for technical development	H(15)	EdMI Test Manager & StreamTech	18/06/2023	Control: Collaborate closely with the DemSet team to identify any incomplete features in the webpage and address them accordingly.	25/08/2023

	Incomplete web front-end application	and potentially compromise safety and security measures.		Test Lead , DemSet		Contingency: Create a comprehensive list of upcoming features to be incorporated into the webpage, combining them with the existing features. Fallback: Analyse competitor features to gain insights for potential additions and improvements in Analyse competitor features to gain insights for potential additions and improvements in EduStream's offerings.	
12	Misrepresentation of final product compared to what was originally agreed to in the marketing design	It will disrupt the projects schedule and also cost the project money on remaking/altering designs and purchasing more materials and parts.	M(9)	EdMI PM & JP Media	10/05/2023	Control: Marketing designs team should be well informed and aware of the design needed and have knowledge on the appropriate materials/parts that also go with it. Contingency: As the project reaches the middle stage of completion, marketing team should choose if designs that have been made should stay the same or change, so it doesn't cost time and money, making big changes near the end of the project. Fallback: Continuing and maintain the final design that is given.	07/07/2023
13	The server's slow speed negatively impacting the streaming of videos and games.	Insufficient speed to servers can hinder the support for streaming services, resulting in increased costs and limitations on technical development. It can result in difficulties delivering high-quality video and game content to users, leading to buffering, interruptions, and a subpar user experience.	M(9)	StreamTech PM	21/05/2023	Control: Before the agreement is finalised, negotiate and confirm with server provider of the adequate speed needed for the streaming service Contingency: Research more server providers that can provide faster speed for the server Fallback: Potentially reducing the quality of games and videos so that the lower quality can still provide a faster speed compared to having a high quality that uses more of the server's speed.	29/06/2023
14	Educational videos used by EdMI are old and not up to date	What's being taught at EdMI will not be up to date with the present world, which will make the target audience lose interest quickly resulting in the company losing money	M(5)	EdMI PM & EdMI Educational Content Expert	13/07/2023	Control: Go through all current content and section them in the years they were released, flagging any content that is 2+ years old which will be reviewed Contingency: Frequent checks on all content to see if they are valid within the present world, if they aren't then they are to be delete from the site	07/05/2023

						Fallback: ONLY upload recent and new learning content	
15	Delays with Content Production	Delay in service launch. Low customer satisfaction	M	Pam Duggins (EdMI Educational Content Expert)	05/05/23	<p>Control Strategy: Develop and adhere to a detailed content production schedule, ensuring enough resources and time are allocated.</p> <p>Contingency Strategy: Hire additional content developers or outsource some content production tasks if delays are anticipated.</p> <p>Fallback Strategy: Prioritize essential content and delay less critical content if significant delays occur.</p>	<p>Control Strategy: Implement immediately and review monthly.</p> <p>Contingency Strategy: Review quarterly or when production deadlines are missed.</p> <p>Fallback Strategy: Implement as soon as significant delays are confirmed</p>
16	Bought Hardware arrives late.	The EduStream project can be delayed if the hardware arrives late. Which can disturb the whole project plan.	H(15)	CIO/ EdMI PM	22/2/2023	<p>Control: Project plan should be planned with a few days of margin of delaying the hardware.</p> <p>Contingency: Check for all possible shipment options and consider the fastest shipment possible.</p> <p>Fallback: Buy hardware as soon as possible.</p>	30/06/2023
17	Staff members can leak confidential data of client.	Company can lose its reputation if any staff member leak customers private information.	H(15)	Security	25/02/2023	<p>Control: Limit staff members access to customer confidential data. Staff members should only be able to see their name and subscription status.</p> <p>Contingency: Staff members should sign an agreement that if they found guilty of breaching customer private information, they will face the consequences.</p>	30/04/2023

18	Hackers can enter our systems through harmful virus.	Hackers can steal our confidential data and customers private information.	H(15)	Security	25/02/2023	Control: Staff access to downloading anything on the systems should be banned. Contingency: Antivirus and firewalls should detect and prevent any incoming threat. Fallback: keep the system clean of virus.	30/08/2023
19	Marketing team unable to promote EduStream project to the target audience	If marketing team did not do their job properly it will result in loss in EduStream project.	H(15)	CEO, EdMI Marketing manager	15/06/2023	Control: Provide training to marketing team early as possible to achieve marketing target. Contingency: Advertisement plan should be ready before marketing. Fallback: Sub-contract a marketing contractor.	6/09/2023
20	EduStream software interface is not user-friendly	EdMI will lose their clients interest which will result in loss.	H(15)	EdMI PM, StreamTech PM	25/06/2023	Control: Keep EduStream software interface user-friendly. Contingency: The software should be tested before to make sure that the software interface is user-friendly. Fallback: Hire another contractor than StreamTech to design a user-friendly software.	30/08/2023
21							
22	Outdated educational content	Loss of interest from the target audience, potential discontent, and reduced revenue.	M (5)	EdMI PM & EdMI Educational Content Expert	13/07/2023	Control: Review and flag outdated content, delete obsolete content from the site.	07/05/2023
23	Marketing team unable to promote to target audience	Loss in the EduStream project due to ineffective marketing.	H (15)	CEO, EdMI Marketing Manager	15/06/2023	Control: Provide training to the marketing team early, establish a marketing plan.	06/09/2023
24	Failure of third-party payment gateway integration	Issues with payment processing, impacting revenue and customer satisfaction.	H (15)	Finance Manager, EdMI	07/07/2023	Control: Thoroughly test and integrate with the payment gateway before going live.	15/07/2023

				PM, StreamTech PM			
25	Inadequate network infrastructure for high-volume streaming	Buffering, slow loading times, and a poor user experience.	H (15)	IT Infrastructure Manager, StreamTech PM	15/05/2023	Control: Assess and upgrade network infrastructure, implement content delivery networks (CDNs).	31/07/2023
26	Inaccurate content metadata and categorization	Difficulties in search and discovery, impacting user experience and satisfaction.	M (9)	Content Manager, EdMI PM	05/06/2023	Control: Implement quality control processes, establish clear guidelines for content tagging.	31/08/2023
27	Inadequate content moderation and filtering	Presence of inappropriate or offensive content, negatively impacting user experience and brand reputation.	H (15)	EdMI Content Moderation Manager, EdMI PM	20/06/2023	Control: Implement content moderation policies, leverage automated content filtering technologies.	31/08/2023
28	Loss of key personnel during critical project phases	Disruption to project timelines, knowledge transfer, and team dynamics.	H (15)	EdMI HR Manager, EdMI PM	15/06/2023	Control: Implement employee retention strategies, foster cross-training and knowledge sharing.	31/08/2023
29	Inadequate customer support infrastructure	Delays in issue resolution, dissatisfaction among users, and negative word-of-mouth.	M (5)	EdMI Customer Support Manager, EdMI PM	10/06/2023	Control: Establish a dedicated customer support team, implement a ticketing system and knowledge base.	31/08/2023
30	Non-compliance with data privacy regulations	Penalties and reputation damage due to violations of regulations like GDPR, CCPA.	H(15)	Data Compliance Officer, Security	30/06/2023	Control: Regular data compliance audits and trainings, appoint a Data Protection Officer (DPO).	01/08/2023
31	Poorly managed software updates	Bugs, errors, user dissatisfaction due to broken features or usability issues.	M	StreamTech PM, EdMI PM	22/07/2023	Control: Implement a robust testing process for updates, have rollback plans.	01/09/2023
32	Inadequate user analytics and feedback collection	Lack of insight into user behavior, missed opportunities for improvement.	M	EdMI PM, StreamTech PM	28/07/2023	Control: Implement feedback collection systems, analyze user behavior data regularly.	30/11/2023
33	Downtime due to scheduled maintenance	Negative user experience, potential revenue loss.	M	IT Infrastructure Manager, StreamTech PM	08/08/2023	Control: Schedule maintenance during off-peak hours, communicate effectively with users.	01/12/2023
34	Low User/Client adoption	Lower expected revenues. Failure to meet project scope objectives.	H	Dan Hill (JP-Media Client Support Manager),	05/05/23	Control Strategy: Conduct user testing and gather client feedback during	Control Strategy: Implement during development and review after

				EdMI's Marketing Manager & Marketing team		<p>development to ensure the product meets user needs and preferences.</p> <p>Contingency Strategy: Implement extensive training and support for users and clients after launch.</p> <p>Fallback Strategy: If adoption remains low, collect feedback to identify obstacles and address them in product updates or changes in the service model.</p>	<p>user/client feedback sessions.</p> <p>Contingency Strategy: Implement after product launch.</p> <p>Fallback Strategy: Implement after 3-6 months of low adoption rates</p>
	Failure to comply with Regulations/Laws	Legal penalties/fines, Reputation/trust damaged	VH	Bill Sykes (EdMI's legal and contractual expert)	05/05/23	<p>Control Strategy: Regular monitoring of legal and regulatory requirements relevant to the software or service.</p> <p>Contingency Strategy: Engage legal consultants to advise on any changes in regulations or laws.</p> <p>Fallback Strategy: Should non-compliance issues arise, prioritize addressing these issues through updates or changes in operational processes.</p>	<p>Control Strategy: Implement immediately and review quarterly or when laws/regulations change.</p> <p>Contingency Strategy: Review annually or when law/regulation changes are expected.</p> <p>Fallback Strategy: Implement as soon as non-compliance is confirmed</p>
	Over Budget	Lacking funds to complete project. Possible delays, or cancellation.	H	James Wasley (Project Manager)	05/05/23	<p>Control Strategy: Regular budget monitoring and adjustments to keep spending on track.</p> <p>Contingency Strategy: Have an emergency fund set aside to cover unexpected costs.</p>	<p>Control Strategy: Implement immediately and review monthly.</p> <p>Contingency Strategy: Review quarterly or when</p>

						<p>Fallback Strategy: In case of severe budget overruns, consider reducing scope or looking for additional funding.</p>	<p>budget is exceeded.</p> <p>Fallback Strategy: Implement as soon as severe budget overruns are confirmed</p>
	Changes in market trends	Reduced demand for our project.	M	JP-Media Client Support Manager and EdMI's Marketing Manager & Marketing team	05/05/23	<p>Control Strategy: Stay informed about market trends and user behavior through continuous market research and analysis.</p> <p>Contingency Strategy: Have a flexible product design that can be updated easily to meet changing user demands.</p> <p>Fallback Strategy: If major market changes occur, consider a product pivot or redesign to stay relevant.</p>	<p>Control Strategy: Implement immediately and review quarterly.</p> <p>Contingency Strategy: Review annually or when significant market changes occur</p> <p>Fallback Strategy: Implement as soon as major market changes that affect the product are confirmed</p>
	Unstable third-party partnerships/contractors	Interruptions in service, increased costs, delays in implementation	M	James Wasley (Project Manager), Ben Dover (EdMI CIO & Project Sponsor)	05/05/23	<p>Control Strategy: Regularly review performance of third-party partners and contractors and maintain open lines of communication.</p> <p>Contingency Strategy: Have backup partners or contractors in place in case of sudden termination of partnership.</p> <p>Fallback Strategy: If a third-party partner drops out unexpectedly, plan to temporarily take over their tasks in-house while seeking new partnerships.</p>	<p>Control Strategy: Implement immediately and review quarterly.</p> <p>Contingency Strategy: Review annually or when signs of instability appear.</p> <p>Fallback Strategy: Implement as soon as a major</p>

							partnership breaks down
	Inability/Slow to scale the platform and services	Poor service during peak usage times, potential loss of users.	H	Nicholas Caruso (Quality Lead StreamTech), Steve Jobs (Quality Lead DemSet), Ben Dover (EdMI CIO & Project Sponsor)	05/05/23	Control Strategy: Design the platform and services with scalability in mind from the start. Contingency Strategy: Plan for staged scaling with corresponding resource allocation. Fallback Strategy: If scaling remains difficult, consider revising the scaling strategy or seeking external help.	Control Strategy: Implement during development and review quarterly. Contingency Strategy: Review after launch and when user base expands significantly. Fallback Strategy: Implement when scaling challenges persist for 6 months
	Technology failure or malfunction	Interruption to service delivery, negatively affecting user experience	VH	Nicholas Caruso (Quality Lead StreamTech), Steve Jobs (Quality Lead DemSet), Bill Gates (EdMI Test Manager)	05/05/23	Control Strategy: Implement robust software testing, regular maintenance, and updates to minimize technology failures. Contingency Strategy: Have a technical support team in place to quickly address any issues that arise. Fallback Strategy: If significant failures occur, have a backup system in place to keep operations running while the primary system is being repaired.	Control Strategy: Implement immediately and review quarterly. Contingency Strategy: Review annually or when technology changes occur. Fallback Strategy: Implement as soon as a major technology failure occurs
	Cybersecurity breach	Potential data loss, compromised user privacy, legal implications, Damaged reputation.	VH	Don Lemon (EdMI Security Expert)	05/05/23	Control Strategy: Invest in strong cybersecurity measures including firewalls, encryption, and secure development practices.	Control Strategy: Implement immediately and review quarterly.

						<p>Contingency Strategy: Have a response team ready to address any breaches, and a plan for communicating about the breach with users and clients.</p> <p>Fallback Strategy: In case of a breach, isolate affected systems, resolve the security issue, and implement measures to prevent future breaches.</p>	<p>Contingency Strategy: Review annually or when new security threats emerge.</p> <p>Fallback Strategy: Implement immediately after a confirmed security breach</p>
	Negative public perception or media coverage	Loss of potential users, reputation damage, decreased trust	M	EdMI's Marketing Manager & Marketing team, Dan Hill (JP-Media Client Support Manager)	05/05/23	<p>Control Strategy: Proactively communicate with the public and media, showcasing the software's benefits and responding to concerns.</p> <p>Contingency Strategy: Have a PR crisis management plan ready in case of negative media coverage.</p> <p>Fallback Strategy: If negative perception persists, consider a rebranding or large-scale PR campaign to rebuild public trust.</p>	<p>Control Strategy: Implement immediately and review quarterly</p> <p>Contingency Strategy: Review annually or after negative media coverage</p> <p>Fallback Strategy: Implement as soon as persistent negative perception is confirmed</p>

NOTES:

- (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.
- (5) The risks should be resolved before the first pilot testing.
- (6) These risks needs to be eliminated before marketing
- (7) All risks needs to be resolved before the Pilot project closure.

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	\$1,600,000	\$1,600,000 x 0.20 = \$320,000
		1B: Moderate Demand	30%	\$2,600,000	\$500,000	\$500,000 x 0.30 = \$150,000
		1C: Weak Demand	50%	\$1,700,000	\$-400,000	\$-400,000 x 0.50 = \$-200,000
Option 2: Adelaide Node	\$ 2,400,000	2A: Strong Demand	35%	\$3,500,000	\$1,100,000	\$1,100,000 x 0.35 = \$385,000
		2B: Moderate Demand	40%	\$2,800,000	\$400,000	\$400,000 x 0.40 = \$160,000
		2C: Weak Demand	25%	\$1,500,000	\$-900,000	\$-900,000 x 0.25 = \$-225,000
Option 3: Darwin Node	\$ 1,800,000	3A: Strong Demand	30%	\$3,100,000	\$1,300,000	\$1,300,000 x 0.30 = \$390,000
		3B: Moderate Demand	30%	\$2,200,000	\$400,000	\$400,000 x 0.30 = \$120,000
		3C: Weak Demand	40%	\$1,400,000	\$-400,000	\$-400,000 x 0.40 = \$-160,000

EMV Option 1 (Brisbane)	EMV Option 2 (Adelaide)	EMV Option 3 (Darwin)
--------------------------------	--------------------------------	------------------------------

$\$320,000 + \$150,000 - \$200,000 = \$270,000$	$\$385,000 + \$160,000 - \$225,000 = \$320,000$	$\$390,000 + \$120,000 - \$160,000 = \$350,000$
---	---	---

Recommendation on which Project to Implement

There are several factors which influence the selection of a particular state for the fourth pilot site-

- The National Indigenous Australians Agency has requested the deployment of a pilot project to remote Indigenous communities, including those in the Northern Territory (NT). Although Darwin is located in NT, it does not encompass remote Indigenous communities in NT. However, the nodes in Darwin are the closest to these communities, ensuring a smooth experience for the participants using the EduStream education streaming solution. Given that the National Indigenous Australians Agency is a government agency and has requested the project, it is reasonable to assume that funding will be provided. Hence, guaranteed funding is expected, regardless of the pilot project's success. The funding should be interpreted as short-term to medium-term because it may disappear when there is a change in government. Therefore, a pilot node in Brisbane or Adelaide would not be eligible to receive this funding
- Brisbane has a distinct advantage in that EdMI has existing sales personnel operating there. This means that the sales personnel already have direct contact and knowledge about appropriate stakeholders and potential adopters for the project. The downside, however, is that the estimated probability of weak demand is at its highest, standing at 50%. The quantitative data from Brisbane sales personnel is included in this statistical analysis, which provides a solid foundation for estimating the likelihood of weak demand.
- In the EMV analysis, Adelaide has a moderate risk profile. While it does not offer the highest expected monetary value, it doesn't have the highest probability of weak demand either.
- Adelaide has a decent population, which could provide a substantial market for EduStream services. While it's not as large as Brisbane, the risk of weak demand is lower, making it a more stable market. Furthermore, future population growth could lead to increased demand over time.
- Located in Queensland, Brisbane provides a unique advantage for EduStream as it is home to a considerable population of Indigenous Australians, estimated to be approximately 252,700 individuals. This demographic presence offers EduStream an opportunity to actively engage with the National Indigenous Australians Agency and foster collaborations with Indigenous communities. By leveraging this connection, EduStream can work towards providing tailored educational content and resources that cater to the specific needs and interests of Indigenous Australians.
- Despite having lower profitability compared to the other two cities, Brisbane is still the most recommended option for the launch of EduStream. It has a population of approximately 2.5 million, the highest among the three cities considered.

