**VILNIUS UNIVERSITY**

**KAUNAS FACULTY**

INSTITUTE OF SOCIAL SCIENCES AND APPLIED INFORMATICS

Study programme Information Systems and Cyber Security

**RISK MANAGEMENT REPORT**

SOFIIA CHEKMENOVA

OLEKSII PARSHYN

**Team №4**

**Participants:**

Sofiia Chekmenova,

Oleksii Parshyn,

Yehor Poliarskyi,

Stepan Kozlov,

Jaykumar Mathukiya

Kaunas 2023

Table of contents

[Possible Risks 4](#_Toc151984177)

[Risk identification 5](#_Toc151984178)

[Risk Analysis and Prioritization 7](#_Toc151984179)

[Risk Planning 8](#_Toc151984180)

[Risk Costing 9](#_Toc151984181)

[Conclusion 10](#_Toc151984182)

**OKR №2** Create Risk Management Document

**Aim:**

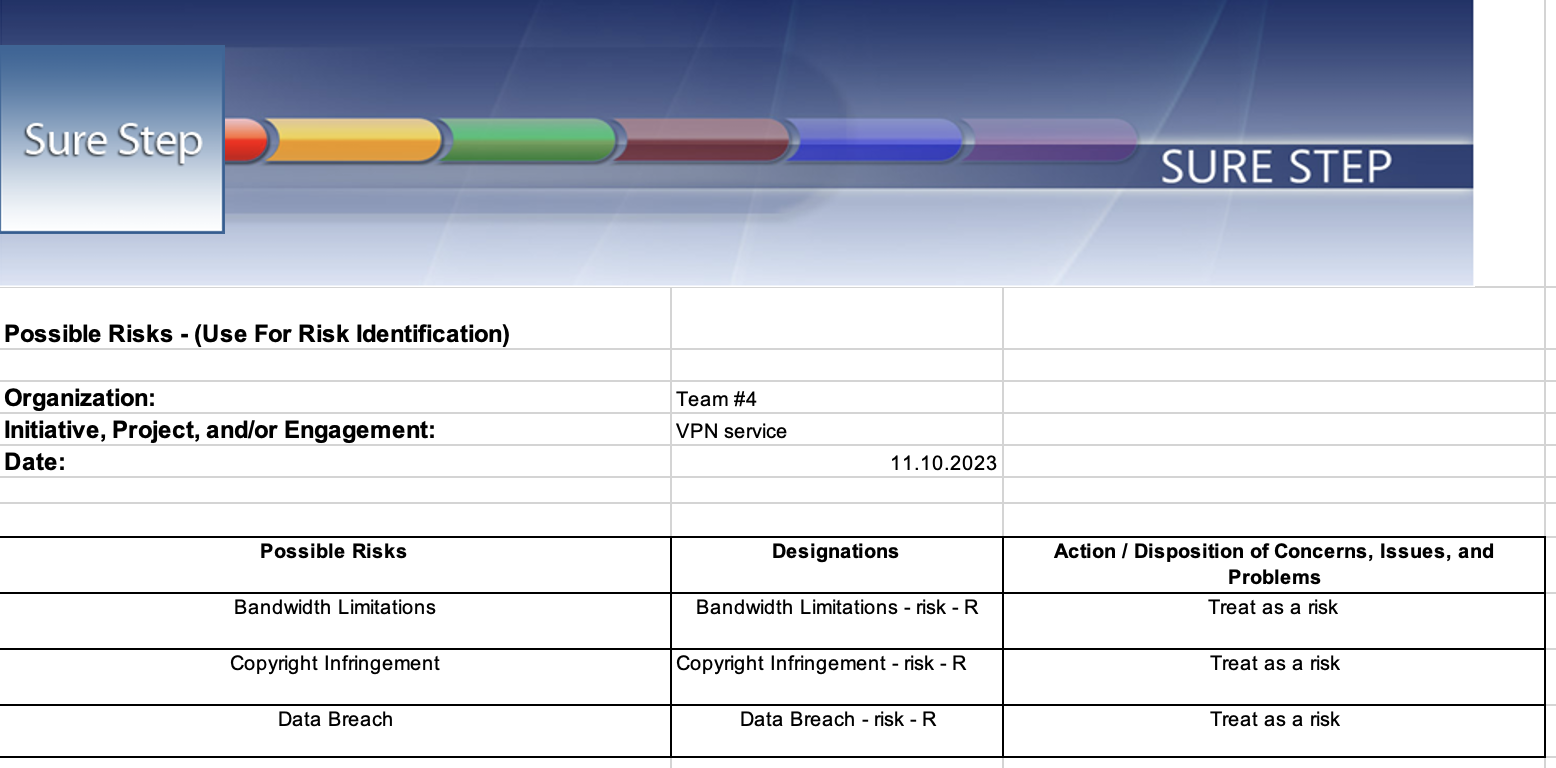
* The aim is to find and describe possible risks of our team project.

**Task:**

* Figure out possible risks
* Identify the risk: classify the risk, find out which categories may be affected, describe the conditions of occurrence and consequences.
* Сonduct risk analysis and prioritization.
* Conduct risk planning.
* Calculate the cost of each risk.

# Possible Risks

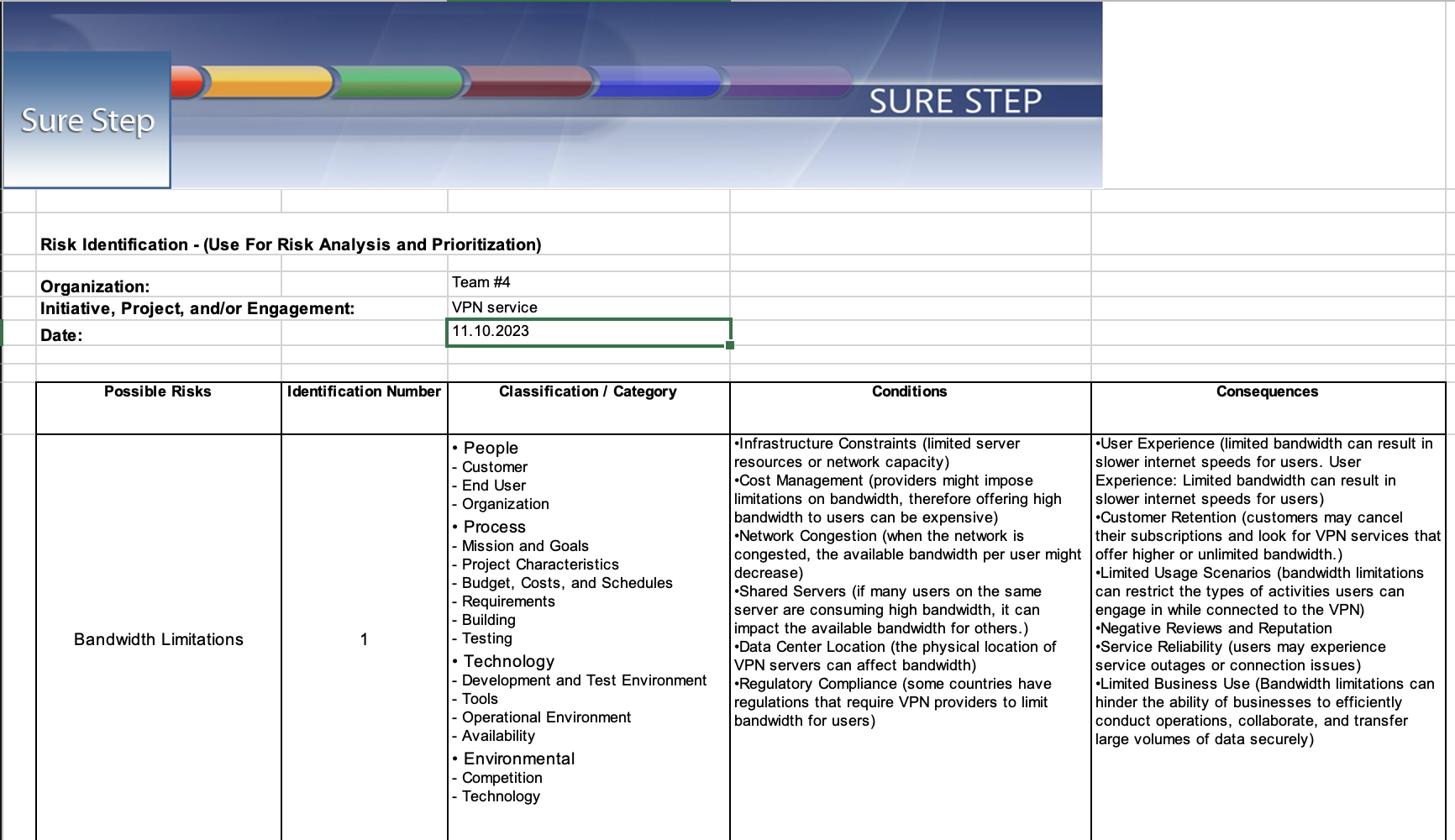
At first, we found out 3 posssible risks that may occure according chosen project – VPN service. There are Bandwidth Limitations, Copyright Infringement and Data Breach. All of them we identifyed as “R” – risk. The screnshot of the table is presented below.



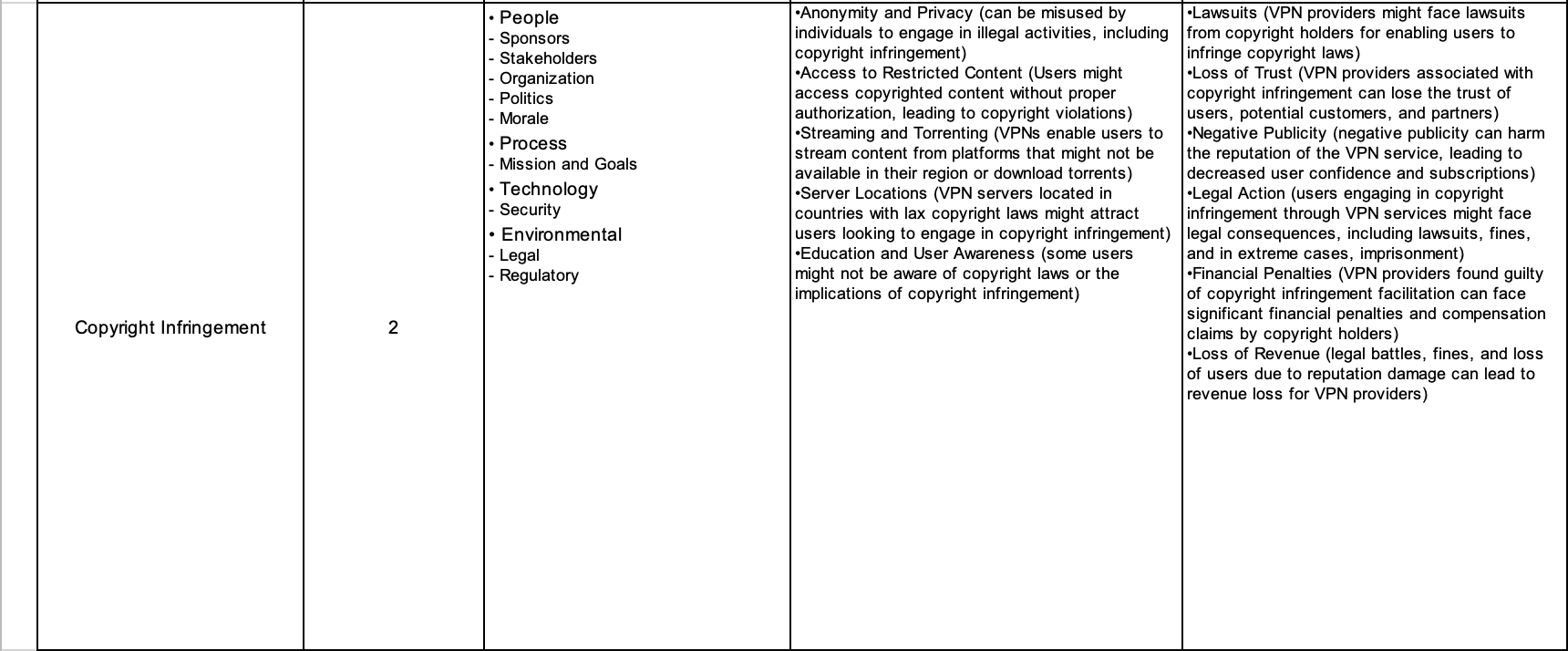
**Figure 1. Possible Risks**

# Risk identification

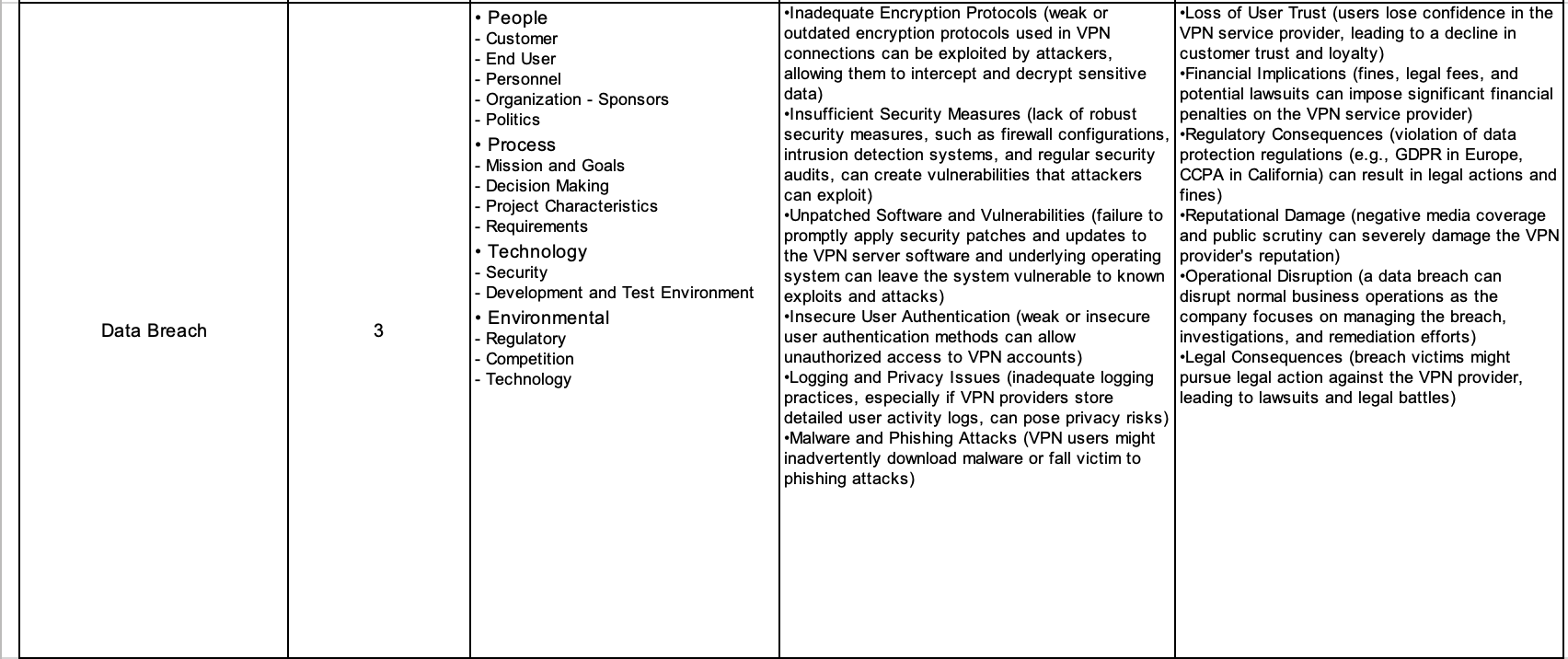
In the tables below you can see the identification of risks. Each risk from the previous table received its own ID number and was assessed according to three parameters. In the first parameter “Classification” we described which people, parts of the project and the environment may be affected by this risk. The next paragraph is “Conditions”. It says under what conditions this risk can occur. On average, we described 4 possible conditions of occurrence. And the last paragraph “Consequences” provides the possible consequences of this risk if it is not eliminated.



**Figure 2. Risk identification.** **Bandwidth Limitations**



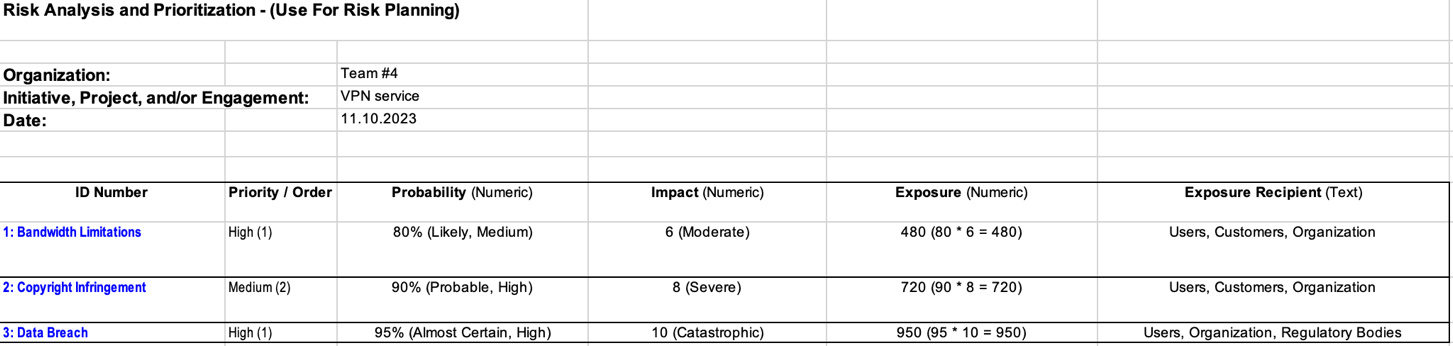
**Figure 3. Risk identification. Copyright Infringement**



**Figure 4. Risk identification. Data Breach**

# Risk Analysis and Prioritization

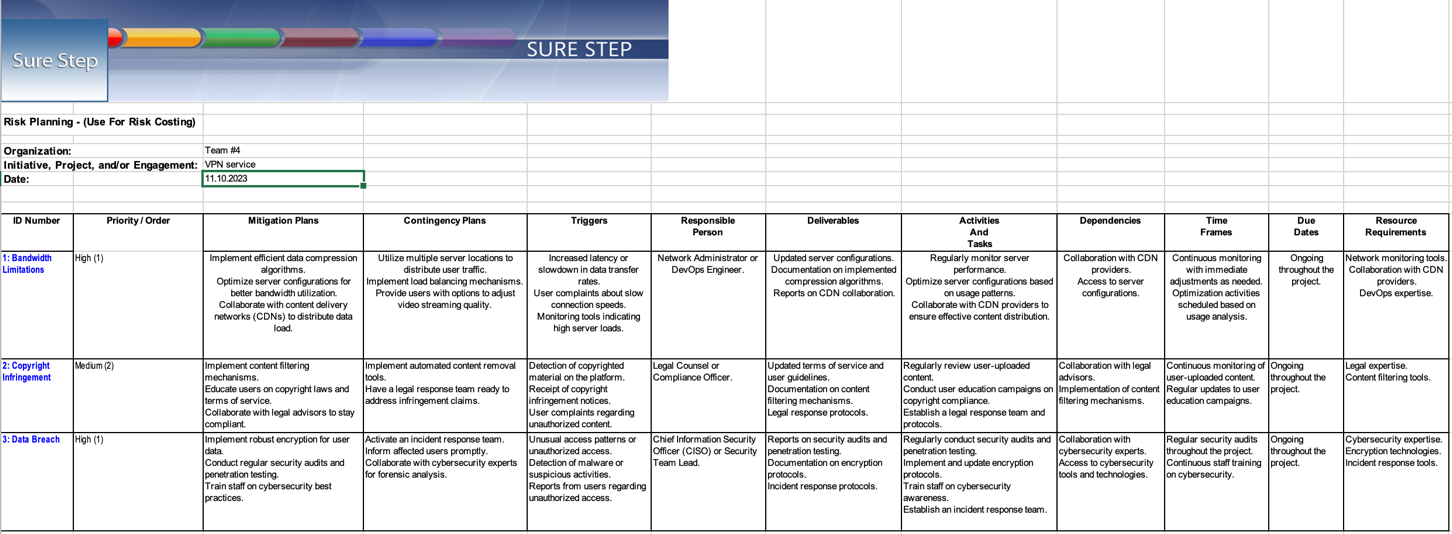
Here are Risk Analysis and Prioritization. You can see 6 columns: ID number, Priority / Order, Probability (Numeric), Impact (Numeric), Exposure (Numeric), Exposure Recipient (Text). The first column contains the ID number of the risk that we assigned to all risks in the previous table. In the second column we indicate the Priority number, that is, which risk should be given more attention. In the “Probability” column, we wrote as a percentage what is the probability of this risk occurring. This column has a big impact on the "Priority / Order" column. In columns 4 and 5 we calculate Impact and Exposure. In the last column we need to write which group will be affected by the risk.



**Figure 5. Risk Analysis and Prioritization**

# Risk Planning

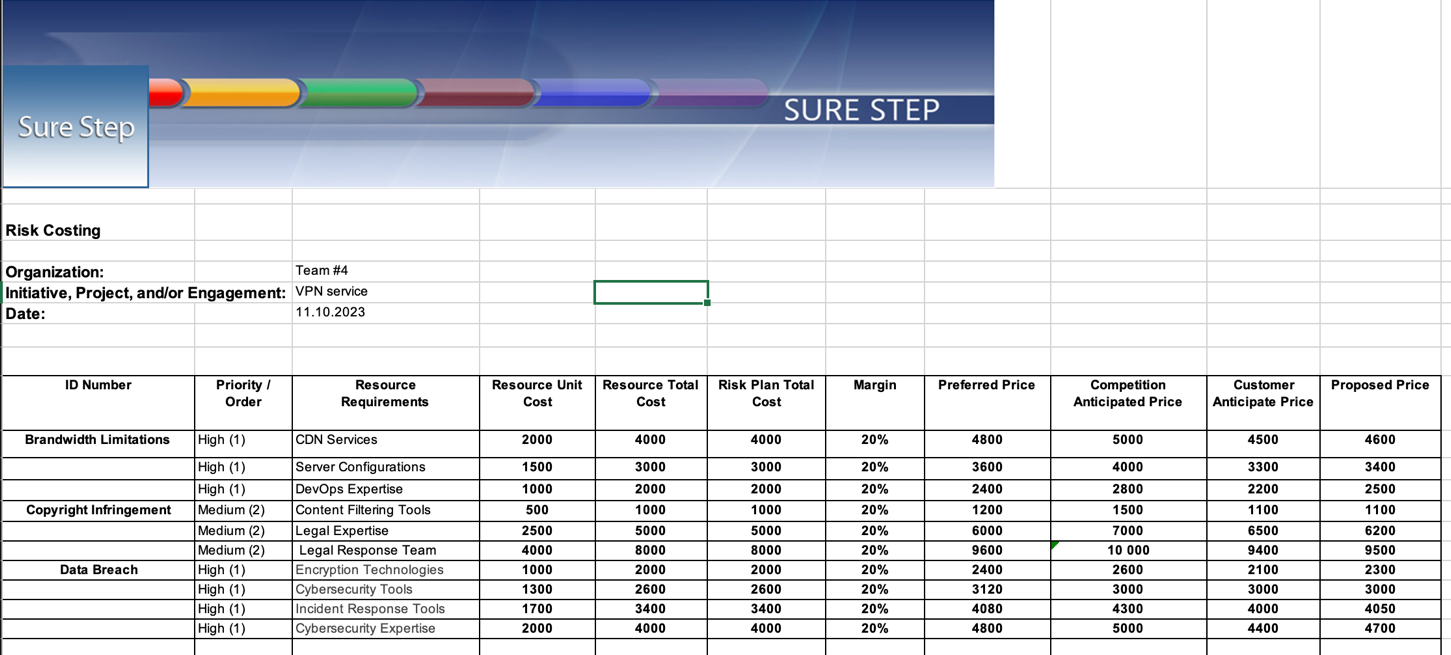
This table is responsible for risk planning. there are such parameters as: Mitigation Plans, Contingency Plans, Triggers, Responsible Person, Deliverables, Activities And Tasks, Dependencies, Time Frames, Due Dates and Resource Requirements. Each risk must be described according to these parameters. You can see the table in more detail in the screenshot below.



**Figure 6. Risk Planning**

# Risk Costing

The last table „Risk Costing” we provide aproximate numbers of costing of each risk. You can see that risk “Copyright Infringement” is the most expensive one. “Data Breach” is located on the second place and the less expencive among them is Brandwidth Limitations.



**Figure 7. Risk Costing**

# Conclusion

In wrapping up, our mission was to uncover and explain the potential challenges in our team project. We began by identifying risks, sorting them into categories, and understanding how they might affect different aspects. We looked at the conditions that might lead to these risks and what consequences they could bring. Then, we analyzed and ranked these risks based on priority. This helped us focus on the most crucial ones. Moving forward, we made a plan to handle these risks wisely. We also calculated the potential cost of each risk In short, we've taken proactive steps to understand, prioritize, and plan for potential bumps of VPN service.