

Development of a Language Learning Program

Farris Darawsheh & Sandra Mejia Villegas

Risk Management

Fall 2017**FDSMV Consultants**

CONNECTING THE WORLD...ONE LANGUAGE AT THE TIME



Table of Contents

1.	Project Background.....	4
2.	Model Structure	5
a)	Identification of Events	5
b)	Participants and Roles	6
c)	Hierarchy of Threats.....	9
d)	Hierarchy of Objectives.....	10
3.	Measurement Methods.....	11
a)	Measurement Methods for Events – Likelihood of Events	12
b)	Measurement Methods for Threats – Likelihood of Events	13
c)	Measurement Methods for Objectives – Impact of Events.....	17
d)	Measurement Methods for Events – Impact of Events.....	18
e)	Evaluation Results Analysis	18
4.	Synthesis Analysis	19
a)	Likelihood of Events	19
b)	Impact of Events.....	21
5.	Risk without Controls	23
a)	Bow-tie Diagram – Without Controls.....	24
b)	Risk Map – Without Controls.....	24
6.	Risk with Controls	25
a)	Bow-tie Diagram – With Controls.....	28
b)	Risk Map – With Controls.....	29
7.	Optimization	30
8.	Conclusion	33

Table of Figures

Figure 1 – Identification of Events	5
Figure 2 – Participants and Roles	6
Figure 3 – Participant’s Roles for Threats – Likelihood of Events.....	7
Figure 4 – Participant’s Roles for Events – Likelihood of Events.....	7
Figure 5 – Participant’s Roles for Objectives – Impact of Events	8
Figure 6 – Participant’s Roles for Events – Impact of Events	8
Figure 7 – Hierarchy of Threats.....	9
Figure 8 – Contribution of Threats to Events	10
Figure 9 – Hierarchy of Objectives.....	10
Figure 10 – Contribution of Events to Objectives	11
Figure 11 – Measurement Methods for Events – Likelihood of Events	13
Figure 12 – Measurement Methods for Threats – Likelihood of Events	14
Figure 13 – Example of Pairwise Comparisons – verbal.....	14
Figure 14 – Example of Inconsistency Ratio.....	14
Figure 15 – Example of Pairwise with given likelihood – verbal.....	15
Figure 16 – likelihood of two events given source using the pairwise graphical/numerical comparison method	15
Figure 17 – Example of Pairwise of probabilities – two diagonals – all pairs - verbal	16
Figure 18 – Example of Pairwise of probabilities – all pairs – one pair – verbal.....	16
Figure 19 – Individual Expected Value	16
Figure 20 – Rating Scale – direct value	17
Figure 21 – Direct.....	17
Figure 22 – Measurement Methods for Events – Impact of Events.....	18
Figure 23 – Measurement Methods for Objectives – Impact of Events.....	18
Figure 24 – Likelihood Evaluation Progress Summary	18
Figure 25 – Impact Evaluation Progress Summary	19
Figure 26 - Dynamic Sensitivity Showing Sources and Event Likelihoods	20
Figure 27 - Performance Sensitivity Showing Sources and Event Likelihood	20
Figure 28 - Overall Likelihoods of Events with Respect to Sources	20
Figure 29 - Overall Priorities of Objectives – objectives chart.....	21
Figure 30 - Overall Priorities of Objectives – objectives grid	22
Figure 31 - Overall Events Impact – events chart.....	22
Figure 32 - Overall Events Impact – events grid	23
Figure 33 - Overall Likelihood, Impacts, and Risks (Without Controls).....	23
Figure 34 - Bow-Tie Diagram without Controls for Protection of Government Data	24
Figure 35 - Risk Map without Controls (Impact vs. Likelihood)	25
Figure 36 - Control Register with selected controls, associated cost and applications	26
Figure 37 – Example Control for Threats	26
Figure 38 – Example of measurement methods for Control for Threats	27
Figure 39 – Participant Roles for Controls Evaluation	27
Figure 40 – Evaluation Progress Summary for Controls	27
Figure 41 - Overall Likelihood, Impacts, and Risks (With Controls).....	28
Figure 42 - Bow-Tie Diagram with Controls for Protection of Government Data	28
Figure 43 - Risk Map with Controls (Impact vs. Likelihood)	29
Figure 44 - Loss Exceedance Curve - Graph.....	30
Figure 45 - Loss Exceedance Curve - Data	30
Figure 46 - Optimization Results 30% reduction of risk	31
Figure 47 - Efficient Frontier.....	32
Figure 48 - Optimization Results \$1.5MM budget for reduction of risk	32

1. Project Background

Riskion Model: <https://gwcomparison.expertchoice.com/?passcode=8809-9708>

Risk Assessment Time frame: 6 months

Project Budget: \$3M and **Enterprise Value** \$5M

Hybrid Risk Analysis.

The world of defense and national security is a very international, and dynamic environment. As such, we find that the government has developed a number of programs for their employees who work in international areas, or targets, and many of these programs are focused on the development and sustainability of second languages, such as Arabic, Farsi, or Russian. However, in the world of defense contracting we do not see these same programs, or benefits.

Since the tragic events of September 11th 2001, the demand for experienced, professional language enabled analysts has become more and more in demand. In addition, the market for foreign language enabled analysts is set to grow by an estimated 29% by the year 2030. As such, our consulting firm FDSMV entered the market in the year 2010, with the goal of winning contracts and setting bids within the intelligence, and defense community. However, in recent years we have experienced lower retention rates, lower language certification scores, and a much higher demand for not just linguists, but skills experienced linguists not only work without military and federal counterparts, but also mentor, train, and fill experience gaps within their mission's sets.

As such, FDSMV and the board of directors have provided initial funding to research the issues at hand, and find a solution to the problem we face, to better improve the quality of our service, the reputation of our firm, and generate more revenue as a result. Therefore, the firm determined the best course of action would be the development of a foreign language training program, for all language professions within the firm.

The FDSMV Language Learning Program (LLP) is a unique initiative within the world of defense contracting, never has a contracting firm invested in such advanced training for their employees, and in many cases other firms simply release linguists that fail to meet standards over time. However, with an estimated two-year training per linguist, this is unsustainable in the long run. Furthermore, our research has shown that the attrition rate for language fluency is not due to lack of skill, or work ethics, but is simply a fact of second language (2L) learning.

The research conducted on the topic of 2L language attrition rates shows us that 2L linguists, who do not attend annual language refresher training, will show higher level of language loss, due to the linguist not being exposed to certain vocabulary not mentioned during the performance of their duties. However, our research has also shown, that with continues education, and refresher training, linguists develop much higher levels of fluency over time, and

after ten consecutive years of month long annual refresher courses, 2L linguists maintain the language, and do not show levels of decay.

As such, FDSMV has decided to take the initiative, and research the development of a language-learning program, and to take advantage of the resources, and skill force we currently have, and invest on them. However, the firm has also decided to measure the risks involved in such an endeavor, and in doing so, we have turned to the professionals at Expert Choice, and their software Riskion, to better measure our options, and the risks involved. This paper will cover findings made by the firm, using Riskion.

2. Model Structure

We have structured our model having in mind the 7 Basic Risk Elements and Measures learned in class. The basic risk elements are events, threats (or sources), objectives (or consequences) and controls. The basic risk measures are likelihood (or probability), impact and risk.

a) Identification of Events

In order to identify the events, the team had discussions about the definition of a Risk Event. We also want to point out that, as per concepts learned in class, a “Risk” and an “Event” are fundamentally the same. When discussing the events for our model, we define Risk as “an uncertain event that has a loss”.

After a team discussion, events were defined and were listed in figure 1 below.

Unique ID	Events
[01]	Professionals availability resulting from language program design
[02]	Lack of qualified faculty
[03]	Improper planning of language needs
[04]	Low retention rates for language professionals
[05]	Loss of language defense contracts
[06]	Identification of language priorities
[07]	Selection of personnel for each language needs
[08]	Identification of current and future language needs
[09]	System outages
[10]	Obsolete Technology
[11]	Protection of Government Data
[12]	Security of campus defense contractors
[13]	Obtaining clearance to use trademarked teaching materials and software
[14]	Loss of competitive advantage in bidding for contracted due to cost of language program.
[15]	Weather events that might affect client monitoring during winter
[16]	Student failure of course

Figure 1 – Identification of Events

b) Participants and Roles

The team had a meeting to discuss the importance of participants and their roles. We learned in class that participants should be identified and roles assigned based on responsibilities, knowledge, and experience. Participants and their roles are key in any project. Selecting the proper participants is very important in order to have meaningful outcomes.

For this project, we analyzed the critical roles that will contribute to the success of the project as well as the importance of the participants in order to have a holistic view of the project, its events, threats and controls.

Government Liaison Manager, Craig Carter, is responsible for the proper communication as well as the establishment of strategic and operational solutions to the government. Program Manager, Farris Darawsheh oversees the team's entire portfolio lifecycle of projects including front end planning, project execution, and on-going maintenance support. Cyber Security Advisor Eric Peck ensures that government data is well managed. Sandra Mejia Villegas as Project Manager is responsible for project execution and day-to-day project execution. Jane Ramsay as IT Manager is in charge of proper functioning of systems. Marque Pierre ensures that the project stays on schedule and on budget. Pamela Tom is responsible to identify gaps in language validation and communicate them to management. Finally, John Cheng acts as Risk Manager. John is in charge of advising proper identification of risk events and efficiency on managing the controls. John relies heavily on Riskion when communicating with upper management.

Email Address	Participant Name	Permission	Has Data?	Disabled?	Action	Group: Stakeholder	Group: Support Services	Group: Project Success
<input type="checkbox"/> GL_Manager@gwu.edu	Craig Carter_Government Liaison Mar	Evaluator	Yes	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> security_advisor@gwu.edu	Eric Peck_Cyber Security Advisor	Evaluator	Yes	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> farrisdarawsheh@gwu.edu	Farris Darawsheh_Program Manager	Project Manager	Yes	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> IT_Manager@gwu.edu	Jane Ramsay_IT Manager	Evaluator	Yes	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Risk_Manager@gwu.edu	John Cheng_Risk Manager	Evaluator	Yes	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> PS_Manager@gwu.com	Marque Pierre_Project Services Mana	Evaluator	Yes	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> nstavrakakis@gwu.edu	Nicholas Stavrakakis	Project Manager	No	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> l_validation_officer@gwu.edu	Pamela Tom_Language Validation Offi	Evaluator	Yes	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> forman@gwu.edu	Professor Forman	Project Manager	No	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> sandrammv@gwu.edu	Sandra Mejia Villegas_Project Managi	Project Manager	Yes	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 2 – Participants and Roles

Below are figures that reflect examples of participant's roles. We have defined 3 major groups as shown in figure 2. The groups are Stakeholders, Support Services and Project Success. Even though we have defined groups, we also did a manual mapping according to each role and assign specific evaluations.

The role represented by the background color is determined implicitly by groups, the "all Participants" group, as well as any custom defined groups. In addition to the implicit assignment of roles based on groups, an explicit role can be specified for a participant (either allow or restrict). If this is the case, there will also be an interior color for the cell and the background color will appear as a border (Taken from Riskion's help feature).

Figure 3 is an example of a participant's roles for Threats for Likelihood of Events. Figure 4 represents an example of the role for events for Likelihood of Events. Further below, figure 5 shows the example of the participant role to evaluate objectives and finally, figure 6 represents

the participant's roles for events for Impact of Events but in this case we wanted to show that we have restricted all measurements for this participant as we found it to be not applicable, that is why it shows all in red.

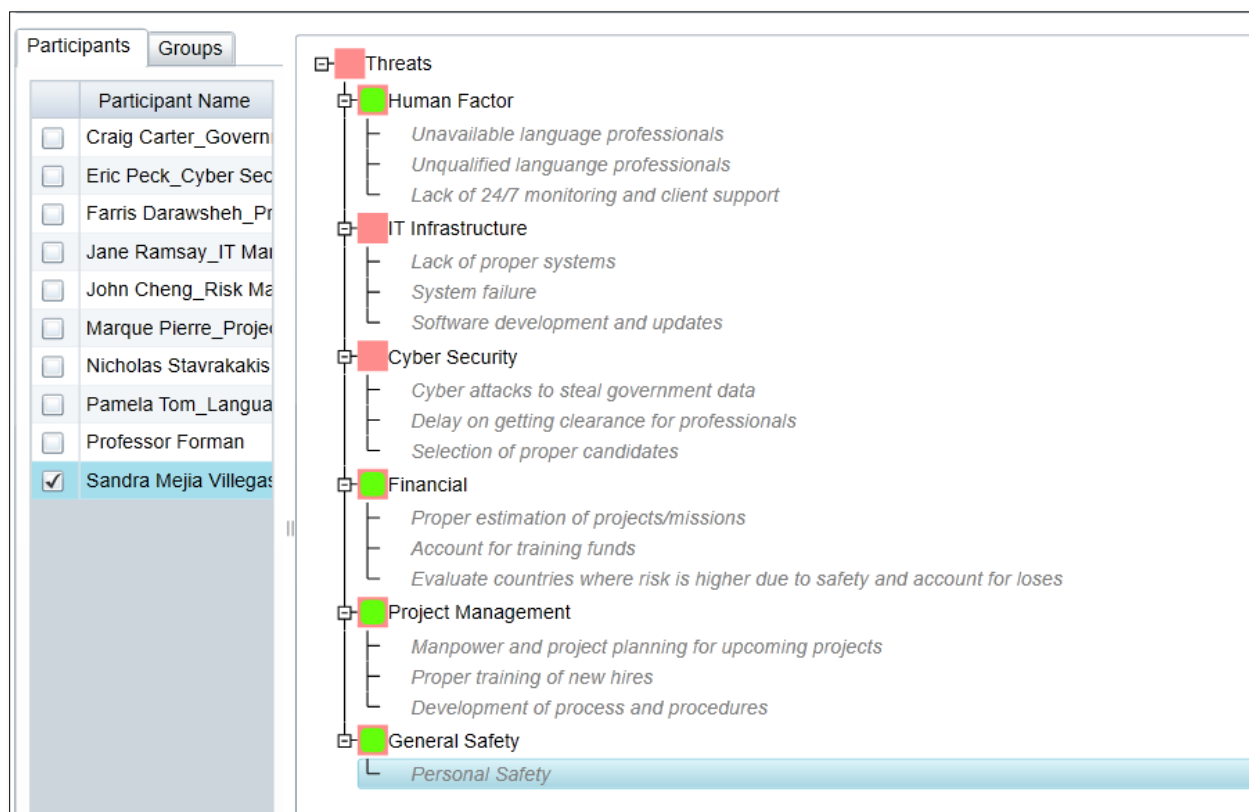


Figure 3 – Participant's Roles for Threats – Likelihood of Events

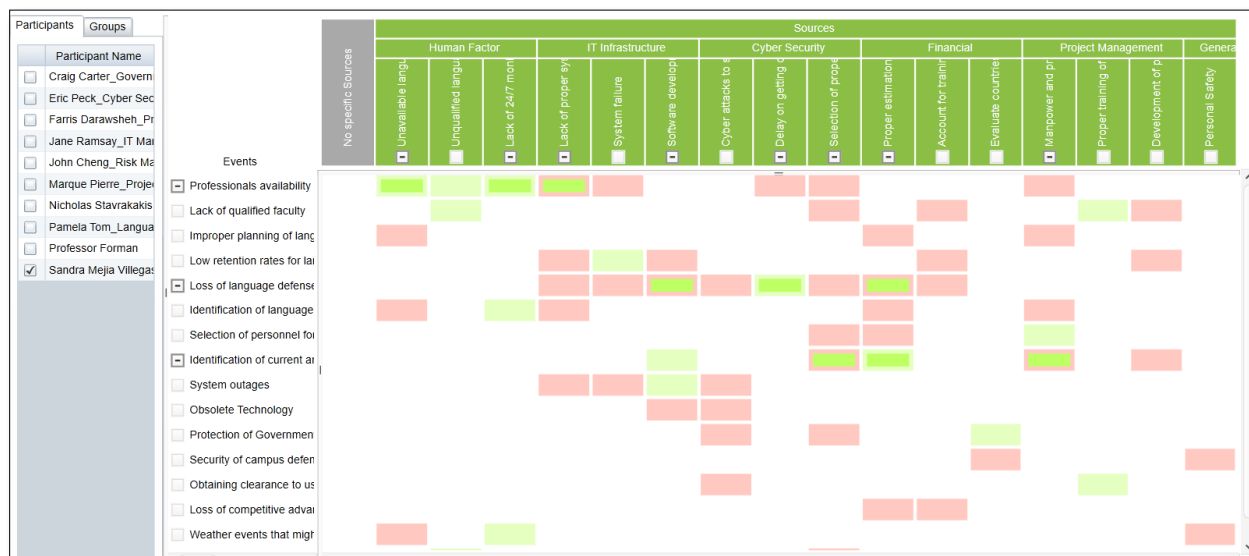


Figure 4 – Participant's Roles for Events – Likelihood of Events

Participants

Groups

	Participant Name
<input type="checkbox"/>	Craig Carter_Govern
<input checked="" type="checkbox"/>	Eric Peck_Cyber Sec
<input type="checkbox"/>	Farris Darawsheh_Pr
<input type="checkbox"/>	Jane Ramsay_IT Ma
<input type="checkbox"/>	John Cheng_Risk Ma
<input type="checkbox"/>	Marque Pierre_Projec
<input type="checkbox"/>	Nicholas Stavrakakis
<input type="checkbox"/>	Pamela Tom_Langua
<input type="checkbox"/>	Professor Forman
<input type="checkbox"/>	Sandra Mejia Villegas

Objectives

- Obtain projects/missions
- Best language professionals
- Efficient usage of manpower needs
- Contractor of choice
- Best Quality of Services
- Most Secure Data

Figure 5 – Participant's Roles for Objectives – Impact of Events

Participants		Objectives/Consequences					
Participant Name		Obtain projects/missions	Best language professional	Efficient usage of money	Contractor of choice	Best Quality of Services	Most Secure Data
<input type="checkbox"/>	Craig Carter_Govern						
<input type="checkbox"/>	Eric Peck_Cyber Sec						
<input type="checkbox"/>	Farris Darawshesh_Pr						
<input type="checkbox"/>	Jane Ramsay_IT Man						
<input type="checkbox"/>	John Cheng_Risk Ma						
<input type="checkbox"/>	Marque Pierre_Proje						
<input type="checkbox"/>	Nicholas Stavrakakis						
<input type="checkbox"/>	Pamela Tom_Langua						
<input checked="" type="checkbox"/>	Professor Forman						
<input type="checkbox"/>	Sandra Mejia Villegas						
Events							
<input type="checkbox"/>	Professionals availability						
<input type="checkbox"/>	Lack of qualified faculty						
<input type="checkbox"/>	Improper planning of language						
<input type="checkbox"/>	Low retention rates for language						
<input type="checkbox"/>	Loss of language defense						
<input type="checkbox"/>	Identification of language						
<input type="checkbox"/>	Selection of personnel for language						
<input type="checkbox"/>	Identification of current language						
<input type="checkbox"/>	System outages						
<input type="checkbox"/>	Obsolete Technology						
<input type="checkbox"/>	Protection of Government						
<input type="checkbox"/>	Security of campus defense						
<input type="checkbox"/>	Obtaining clearance to use language						
<input type="checkbox"/>	Loss of competitive advantage						
<input type="checkbox"/>	Weather events that might impact language						

Figure 6 – Participant's Roles for Events – Impact of Events

c) Hierarchy of Threats

Once the risk events were identified, we moved over to list the threats. Threats (or sources) are one of the Basic Risk Elements. We had discussions on what can be the threats or sources that will eventually turn into a risk event, and then we developed the list shown in figure 7 below.

In Riskion, a threat node can be “Uncertainty” or a “Category”. We have selected them to be categories so we could group them by characteristic.

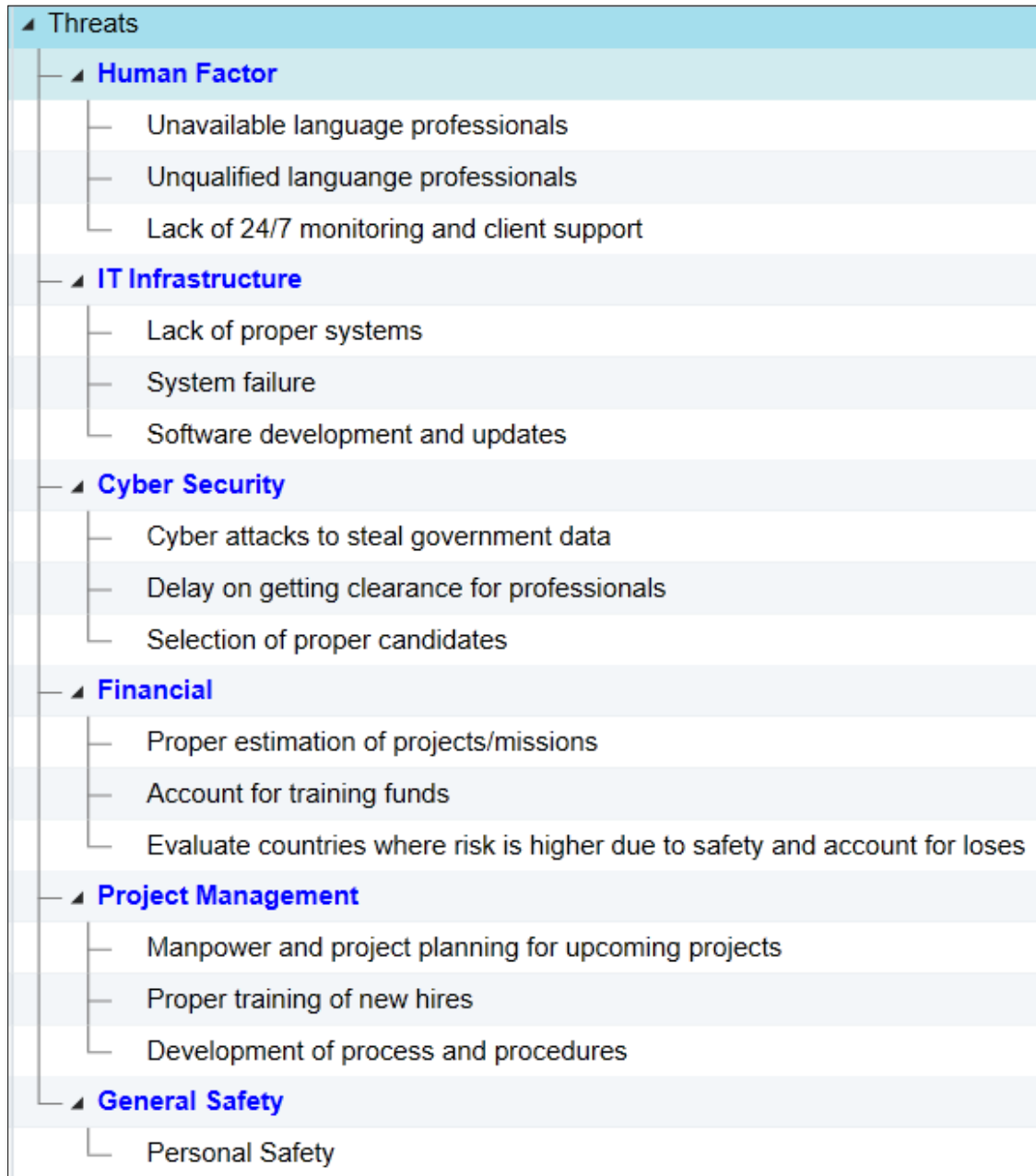


Figure 7 – Hierarchy of Threats

In order to “map” the risk events to threats, it is important to understand how the listed threats contribute to the risk events. Our model’s hierarchy of threats shown in figure 8 below reflects the relationship between threats and risk events. Risk events may be unconditional or it may depend on one or more threats.

Events	Threats													
	Human Factor			IT Infrastructure			Cyber Security			Financial			Project Management	
	Unavailability	Unqualified	Lack of 2	Lack of 1	System s	Software	Cyber att	Delay on	Selection	Proper e	Account	Evaluate	Manpower	Proper tr
Professionals availability resulting from language program design														
Lack of qualified faculty														
Improper planning of language needs														
Low retention rates for language professionals														
Loss of language defense contracts														
Identification of language priorities														
Selection of personnel for each language needs														
Identification of current and future language needs														
System outages														
Obsolete Technology														
Protection of Government Data														
Security of campus defense contractors														
Obtaining clearance to use trademarked teaching materials and software														
Loss of competitive advantage in bidding for contracted due to cost of language program.														
Weather events that might affect client monitoring during winter														
Student failure of course														

Figure 8 – Contribution of Threats to Events

d) Hierarchy of Objectives

In class we learned that a consequence is one of the Basic Risk Elements. The consequence of an event is the loss in the form of failing to achieve one or more objectives and or the loss to one or more assets (statement taken from Riskion).

When the team discussed the objectives hierarchy, we focused on “what will make the project successful” and this not only apply to this specific project but to the strategically growth of our company. Figure 9 below list the identified objectives.

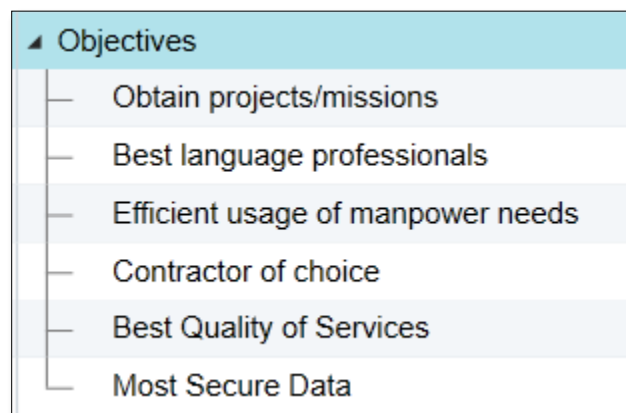


Figure 9 – Hierarchy of Objectives

In order to better analyze the impact of the risk events and to create a valid and clear model structure, the team has mapped which risks events contribute to which objectives (Figure 10). Please note that not all the risk events contribute to all objectives.

Events	Objectives					
	Obtain projects/missions	Best language professionals	Efficient usage of manpower needs	Contractor of choice	Best Quality of Services	Most Secure Data
Professionals availability resulting from language program design	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of qualified faculty	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Improper planning of language needs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Low retention rates for language professionals	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loss of language defense contracts	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identification of language priorities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Selection of personnel for each language needs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Identification of current and future language needs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System outages	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Obsolete Technology	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protection of Government Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Security of campus defense contractors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Obtaining clearance to use trademarked teaching materials and software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Loss of competitive advantage in bidding for contracted due to cost of language program.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Weather events that might affect client monitoring during winter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student failure of course	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 10 – Contribution of Events to Objectives

3. Measurement Methods

After structuring our model by identifying events and threats, participant's roles and a hierarchy of objectives, priorities are derived for relative importance of the objectives as well as the relative preference of the events with respect to the objectives.

All measures derived from Riskion have ratio scale levels of measurement. If priorities do not possess the ratio level property, as often occurs with other methodologies, such as weights and scores in a spreadsheet, the results are likely to be mathematically meaningless (Taken from Riskion's help feature). On the other hand, Riskion supports absolute and relative measures. Absolute represents likelihood of the threat or event occurring and relative represents the likelihood compared to the likelihood of other threats or events.

Whereas relative measurement in AHP (Analytical Hierarchy Process) is performed by comparing two elements, e.g. objectives or events, one to another, absolute measurement is performed on each element, e.g. event, one at a time. There are several ways that this can be done in Riskion. Below we will show some examples.

All measurements were done inviting participants via email as well as sending them a link in order to record their evaluations.

When the participants were working on their evaluation, they used judgment (expertise) as the instrument. In other occasions, if data was available, they used that benchmark to evaluate. But even when data is available, sometimes/often it also needs to incorporate judgment.

The levels of measurements are Nominal, Ordinal, Interval and Ratio. An example of **nominal** level of measurement is the social security numbers. An example of an **ordinal** level of

measurement is the order or rank of finishers in a race. **Interval** numbers add information about the 'intervals' between measures. For example, Horse number 3 finished in first place, 3 lengths or 12 meters ahead of the second place horse. Finally, **Ratio** numbers have the highest level of measure where the ratios of the measures are meaningful in terms of ratios or proportions. For example, the finish time for the winning horse was .973 times that of the second place horse.

What is key to understand when working with mathematically meaningful measurements results is that not all numbers have the same meaning in terms of what operations can legitimately be performed with them. In order for mathematical operations like addition and multiplication with numbers to be mathematically meaningful, the numbers must possess certain properties. (Taken from Riskion's help feature)

a) Measurement Methods for Events – Likelihood of Events

In order to measure likelihood of events, we decided to use the following methods: (Figure 11)

- Pairwise Comparisons – All pairs – Graphical
- Pairwise Comparisons – Two diagonals – Graphical
- Pairwise with given likelihood – All pairs – Graphical
- Rating Scale (Direct)
- Pairwise of probabilities – All pairs – Verbal

Pairwise Comparison's Graphical/numerical judgments represent a judgment about the likelihood of two elements. If there are " n " elements in a cluster of elements being prioritized, and each pairwise comparison was a precise measurement, there would need to be only " $n-1$ " judgments to derive the exact ratio scale priorities. However, since the measurements are judgments and are not precise, making more than the minimum number of judgments will result in more accurate priorities. The maximum number of judgments in a cluster of " n " elements where each element is compared once to every other element is " $(n * (n-1))/2$ " – as shown in figure below. Judgments can be displayed in a two dimensional array, where each entry above the diagonal represents the ratio of the importance of one element to another. The elements on the diagonal correspond to comparing an element to itself and are thus all equal to 1. (Taken from Riskion's help feature and modified)

Ratings scales consist of a set of intensities in the form of words that evaluators can choose from to express the desirability of an event. In our case, we have based our evaluations in the set of intensities but we have entered a direct value that better describes the likelihood between the two elements. (Taken from Riskion's help feature and modified)

Measure Event Likelihoods	Measurement Type Default: Rating Scale	Measurement Scale or Given Likelihood	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: One pair	Pairwise Type Default: Verbal
Threats								
Human Factor								
Unavailable language professionals	Pairwise Com		Copy	4	$4 \times (4-1)/2 = 6$	All pairs (maximum accuracy)	One pair	Graphical
Unqualified language professionals	Pairwise Com		Copy	3	$3 \times (3-1)/2 = 3$	All pairs (maximum accuracy)	One pair	Graphical
Lack of 24/7 monitoring and client support	Pairwise Com		Copy	3	$3 \times (3-1)/2 = 3$	All pairs (maximum accuracy)	One pair	Graphical
IT Infrastructure								
Lack of proper systems	Pairwise Com		Copy	5	$(5-1) \times (5-2) = 7$	Two diagonals	One pair	Graphical
System failure	Pairwise Com		Copy	4	$(4-1) \times (4-2) = 5$	Two diagonals	One pair	Graphical
Software development and updates	Pairwise Com		Copy	5	$(5-1) \times (5-2) = 7$	Two diagonals	One pair	Graphical
Cyber Security								
Cyber attacks to steal government data	Pairwise with	Loss of language defense contr...: 0.5	Copy	5	$5 \times (5-1)/2 = 10$	All pairs (maximum accuracy)	One pair	Graphical
Delay on getting clearance for professional	Pairwise with	Loss of language defense contr...: 1	Copy	2	$2 \times (2-1)/2 = 1$	All pairs (maximum accuracy)	One pair	Graphical
Selection of proper candidates	Pairwise with	Identification of current and ...: 0.3	Copy	7	$7 \times (7-1)/2 = 21$	All pairs (maximum accuracy)	One pair	Graphical
Financial								
Proper estimation of projects/missions	Rating Scale	Scale for Cyber Security	Copy Edit	5	5			
Account for training funds	Rating Scale	Scale for Cyber Security	Copy Edit	4	4			
Evaluate countries where risk is higher or lower	Rating Scale	Scale for Cyber Security	Copy Edit	1	1			
Project Management								
Manpower and project planning for upcoming projects	Pairwise of Prob	Default Pairwise of Probabilities Scale	Copy Edit	5, 7	$7 \times (7-1)/2 \times 5 = 1$	All pairs (maximum accuracy)	One pair	Verbal
Proper training of new hires	Pairwise of Prob	Default Pairwise of Probabilities Scale	Copy Edit	2, 7	$7 \times (7-1)/2 \times 2 = 4$	All pairs (maximum accuracy)	One pair	Verbal
Development of process and procedures	Pairwise of Prob	Default Pairwise of Probabilities Scale	Copy Edit	3, 7	$7 \times (7-1)/2 \times 3 = 6$	All pairs (maximum accuracy)	One pair	Verbal
General Safety								
Personal Safety	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	2	2			

Figure 11 – Measurement Methods for Events – Likelihood of Events

b) Measurement Methods for Threats – Likelihood of Events

We learned in class that the likelihood of an event is the sum product of ratio-scale measures; the likelihood of the threats, times (multiplied by) the likelihood of the event given the threats.

For measurement of threats for likelihood of events, we have selected the following measurement types:

- Pairwise with given likelihood – Two diagonals – Verbal
- Direct
- Rating Scale (Custom scale)
- Pairwise of probabilities – Two diagonals – Verbal
- Pairwise Comparisons – Two diagonals – Graphical

Measure Likelihood	Measurement Type	Measurement Scale or Given Likelihood	Action	# of Elements, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: One pair	Pairwise Type Default: Verbal
Threats								
Human Factor	Pairwise with Give	Unavailable language professionals...	Copy	3	$(3-1)+(3-2) = 3$	Two diagonals	One pair	Verbal
Unavailable language professionals								
Unqualified language professionals								
Lack of 24/7 monitoring and client support								
IT Infrastructure	Direct		Copy	3	3			
Lack of proper systems								
System failure								
Software development and updates								
Cyber Security	Rating Scale	Scale for Cyber Security	Copy Edit	3	3			
Cyber attacks to steal government data								
Delay on getting clearance for professional								
Selection of proper candidates								
Financial	Pairwise of Probab	High Pairwise of Probabilities Scale	Copy Edit	3, 7	$((7-1)+(7-2)) * 3$	Two diagonals	All pairs	Verbal
Proper estimation of projects/missions								
Account for training funds								
Evaluate countries where risk is higher d								
Project Management	Pairwise Compari		Copy	3	$(3-1)+(3-2) = 3$	Two diagonals	One pair	Verbal
Manpower and project planning for upcoming								
Proper training of new hires								
Development of process and procedures								
General Safety	Pairwise Compari		Copy	1		Two diagonals	One pair	Graphic
Personal Safety								

Figure 12 – Measurement Methods for Threats – Likelihood of Events

Below are examples of the measurement methods used for threats – Likelihood of Events and events – Likelihood of Events.



Figure 13 – Example of Pairwise Comparisons – verbal

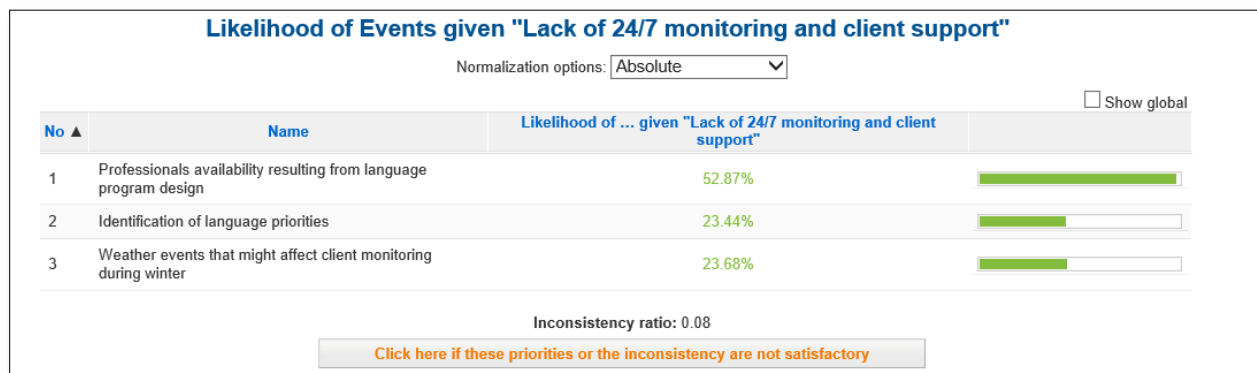


Figure 14 – Example of Inconsistency Ratio

We made sure that the inconsistency ratio was less than 20%. As we learned in class, it is more important to be accurate when deriving priorities than to be consistent.

The theory of AHP does not demand perfect consistency. AHP allows inconsistency, but provides a measure of the inconsistency in each set of judgments. Measuring the inconsistency ratio is an important by-product of the process of deriving priorities based on pairwise comparisons.



Figure 15 – Example of Pairwise with given likelihood – verbal

We used “pairwise with known likelihood or impact” measurement method because we identified a known likelihood or impact. As we learned in class, the unknowns are compared to the known, anchoring the derived likelihoods or impacts to a known, quantitative measure.

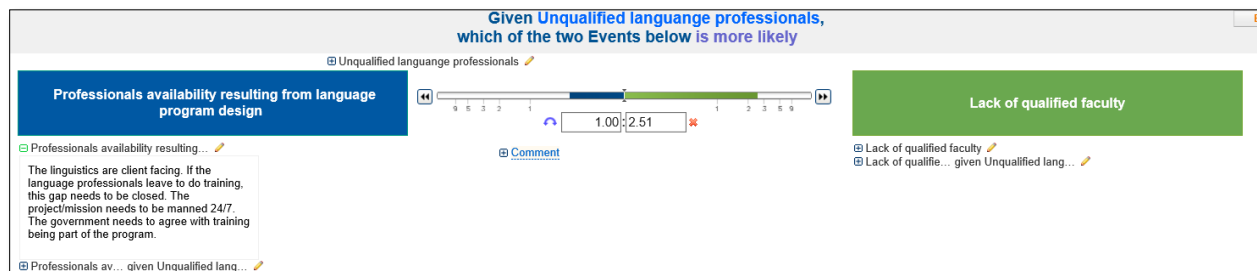


Figure 16 – likelihood of two events given source using the pairwise graphical/numerical comparison method

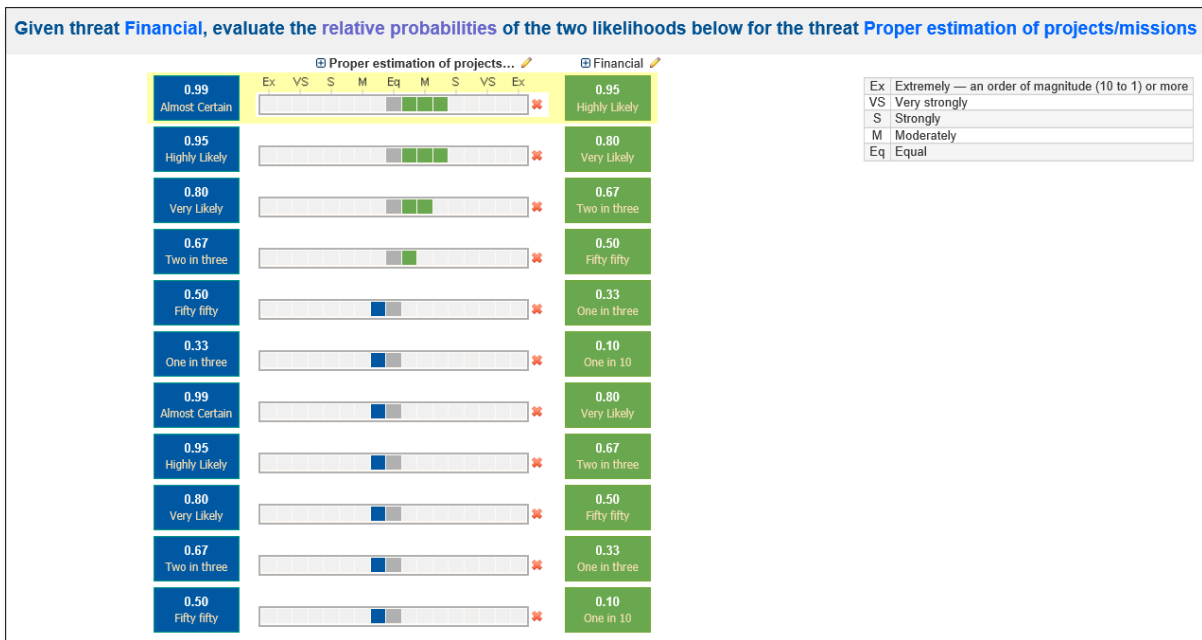


Figure 17 – Example of Pairwise of probabilities – two diagonals – all pairs - verbal



Figure 18 – Example of Pairwise of probabilities – all pairs – one pair – verbal

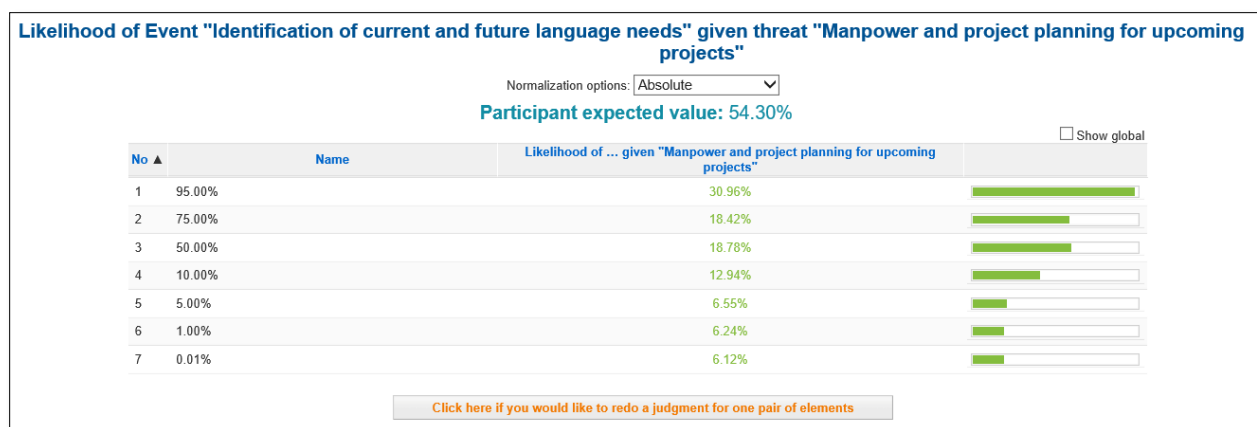


Figure 19 – Individual Expected Value

From the class we learned that pairwise of Probabilities treats risk probabilistically, adding deeper examination and structure to the risk analysis process therefore the outcome. The derived likelihood probability for the event, given that the threat has occurred, is the weighted sum of the assessed likelihoods.

The screenshot shows a software interface for rating the likelihood of events. The title is "Given Proper estimation of projects/missions, rate the likelihood of the following Events". There are four tabs: "Loss of language defense contracts", "Proper estimation of projects/missions", "Loss of language... given Proper estimatio...", and "Scale description". The first tab is active, showing two items: "[05] Loss of language defense contracts" with a value of 0.3 and a progress bar at 30.000%, and "[08] Identification of current and future language needs" with a value of 0.7 and a progress bar at 70.000%. On the right, a detailed view for "Loss of language defense contracts" is shown. It includes a table with "Intensity Name" and "Likelihood". The table has six rows: Negligible, Likely, Moderate, Significantly, Certain, and Not rated, each with a radio button and a likelihood value of 0.000%. The "Direct Value" option is selected, and a value of 0.3 is entered in the adjacent field.

Intensity Name	Likelihood
<input type="radio"/> Negligible	0.000%
<input type="radio"/> Likely	0.000%
<input type="radio"/> Moderate	0.000%
<input type="radio"/> Significantly	0.000%
<input type="radio"/> Certain	0.000%
<input type="radio"/> Not rated	
<input checked="" type="radio"/> Direct Value	0.3

Figure 20 – Rating Scale – direct value

From class we learned that rating scales are useful for subjective judgments when there are a number of elements and to use pairwise comparisons might take more time. Although we use this one in order to practice and learn from it. In figure 20, we can see that a rating scale for likelihood being applied to two events. Direct values are accepted for judgments between intensities and it was used as the custom scale generated an error, but we wanted to show the options and the path that our team took.

The screenshot shows a software interface for estimating the likelihood of each of the sources below. The title is "Given IT Infrastructure, estimate the likelihood of each of the Sources below". There are three items listed: "Lack of proper systems" with a value of 0.4, "System failure" with a value of 0.2, and "Software development and updates" with a value of 0.6. Each item has a progress bar and a red 'X' icon, indicating an error or warning.

Source	Likelihood
Lack of proper systems	0.4
System failure	0.2
Software development and updates	0.6

Figure 21 – Direct

As we stated before, the team wanted to practice with all the different methods of measurements to learn from the inputs and outputs. We learned in class though that direct entry is most useful if we already have ratio scale priorities, possibly from historical data or calculated/derived from a different tool like Montecarlo simulation.

c) Measurement Methods for Objectives – Impact of Events

For measurement of objectives for impact of events, we have selected the following measurement types:

- Pairwise with given likelihood – All pairs – Verbal
- Rating Scale (Default Scale)

Measure Events With Respect To	Measurement Type Default: Rating Scale	Measurement Scale	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: One pair	Pairwise Type Default: Verbal
Objectives								
Obtain projects/missions	Pairwise Comparison		Copy	12	$12*(12-1)/2 = 66$	All pairs (maximum accuracy)	One pair	Verbal
Best language professionals	Pairwise Comparison		Copy	4	$4*(4-1)/2 = 6$	All pairs (maximum accuracy)	One pair	Verbal
Efficient usage of manpower needs	Pairwise Comparison		Copy	4	$4*(4-1)/2 = 6$	All pairs (maximum accuracy)	One pair	Verbal
Contractor of choice	Rating Scale	Default Impact Scale	Copy Edit	7	7			
Best Quality of Services	Rating Scale	Default Impact Scale	Copy Edit	10	10			
Most Secure Data	Rating Scale	Default Impact Scale	Copy Edit	4	4			

Figure 22 – Measurement Methods for Events – Impact of Events

d) Measurement Methods for Events – Impact of Events

For measurement of threats for likelihood of events, we have selected the following measurement types:

- Pairwise Comparisons – All pairs – Verbal

Measure Importance With Respect To	Measurement Type	Measurement Scale	Action	# of Elements, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: One pair	Pairwise Type Default: Verbal
Objectives	Pairwise Comparison		Copy	6	$6*(6-1)/2 = 15$	All pairs (maximum accuracy)	One pair	Verbal
Obtain projects/missions								
Best language professionals								
Efficient usage of manpower needs								
Contractor of choice								
Best Quality of Services								
Most Secure Data								

Figure 23 – Measurement Methods for Objectives – Impact of Events

e) Evaluation Results Analysis

Figures 24 and 25 below shows the results of the evaluations by all participants. The reason of using different methods was to have a good practice and understanding of each measurement type. We also used both graphical and verbal pairwise type in order to make a diversified set of measurements that are valid as well as easy to make. We balanced the number of judgments based on type of measurement and participant role assignment in order to make the evaluation simple but meaningful.

Participant Name	Email Address	Evaluation Progress
Sandra Mejia Villegas_Project Manager	sandrammv@gwu.edu	100.0%(135/135)
Farris Darawsheh_Program Manager	farrisdarawsheh@gwu.edu	100.0%(81/81)
Eric Peck_Cyber Security Advisor	security_advisor@gwu.edu	100.0%(37/37)
Pamela Tom_Language Validation Officer	l_validation_officer@gwu.edu	100.0%(13/13)
Jane Ramsay_IT Manager	IT_Manager@gwu.edu	100.0%(108/108)
John Cheng_Risk Manager	Risk_Manager@gwu.edu	100.0%(48/48)
Marque Pierre_Project Services Manager	PS_Manager@gwu.com	100.0%(33/33)
Craig Carter_Government Liaison Manager	GL_Manager@gwu.edu	100.0%(6/6)
Professor Forman	forman@gwu.edu	0.0% (0/0)
Nicholas Stavrakakis	nstavrakakis@gwu.edu	0.0% (0/0)

Figure 24 – Likelihood Evaluation Progress Summary

Participant Name	Email Address	Evaluation Progress
Sandra Mejia Villegas, Project Manager	sandrammv@gwu.edu	<div><div></div></div> 100.0%(114/114)
Farris Darawsheh, Program Manager	farrisdarawsheh@gwu.edu	<div><div></div></div> 100.0%(114/114)
Eric Peck, Cyber Security Advisor	security_advisor@gwu.edu	<div><div></div></div> 100.0%(15/15)
Pamela Tom, Language Validation Officer	I_validation_officer@gwu.edu	<div><div></div></div> 100.0%(15/15)
Jane Ramsay, IT Manager	IT_Manager@gwu.edu	<div><div></div></div> 100.0%(15/15)
John Cheng, Risk Manager	Risk_Manager@gwu.edu	<div><div></div></div> 100.0%(114/114)
Marque Pierre, Project Services Manager	PS_Manager@gwu.com	<div><div></div></div> 100.0%(15/15)
Craig Carter, Government Liaison Manager	GL_Manager@gwu.edu	<div><div></div></div> 100.0%(114/114)
Professor Forman	forman@gwu.edu	<div><div></div></div> 0.0% (0/0)
Nicholas Stavrakakis	nstavrakakis@gwu.edu	<div><div></div></div> 0.0% (0/0)

Figure 25 – Impact Evaluation Progress Summary

4. Synthesis Analysis

Synthesis shows us the results of our risk measurements, and gives us a ratio scale to better measure our choices, and options. Riskion, gives the user the ability to have a much more readable, and more understandable result. Furthermore, synthesizing our analysis in a dynamic, and performance manner, further enables decision makers to examine and evaluate possible outcomes, and make choices based on this. Below, we will consider the likelihood of events, and the impact of events.

a) Likelihood of Events

When looking at the likelihood of events for our project we researched several outcomes, and gave the decision makers the ability to set their judgments, and measures. In addition, we considered how events change, or how a settle change in one event could change the outcome of another, and give those taking the risk a better understanding of impacts that might come as a result, or how to better avoid risks. In doing so, we used the dynamic option within Riskion. The dynamic option, gave us the ability to simply slide bars on our charts from the left or the right, to see how decreasing or increasing one measure, would result in a change throughout the chart. In turn, this would better enable us to determine priorities, with changes that are likely to happen in such an unpredictable market.

Furthermore, we find that “identification of current, and future language needs” showed the greatest effect on the program, and this stems from the fact that in our current day, and global environment, it is hard to predict the next battle, or the language that our adversaries will be using in that battle. In turn, we also notice how settle changes can affect outcomes in Riskion, we were able to simply “increase the proper training of new hires”, and this resulted in a much lower level of event likelihood for the two highest factors, “Selection of personnel for each language need”, and “Identification of current and future language needs.” This is reflected in figure 26.

In addition, while using Riskion, the firm was given a unique ability to make a judgments based on the performance, and with Riskion we are able to also adjust these ricks, and notice how such changes affect other threats, and an example of this is shown in figure 27 where we shifted the “proper estimation of project/missions” and this had a direct outcome on accounting for training funds, and the evaluation of countries that are of risk.

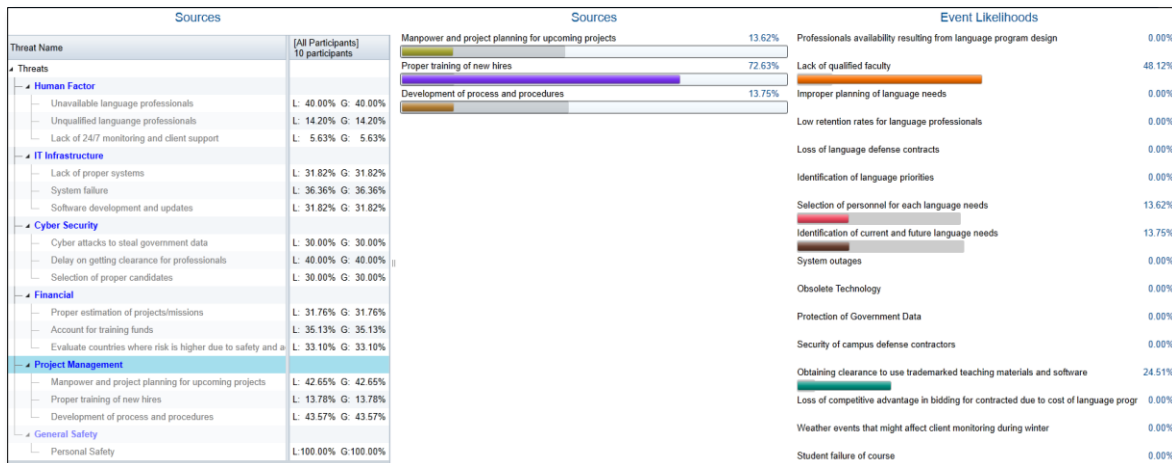


Figure 26 - Dynamic Sensitivity Showing Sources and Event Likelihoods

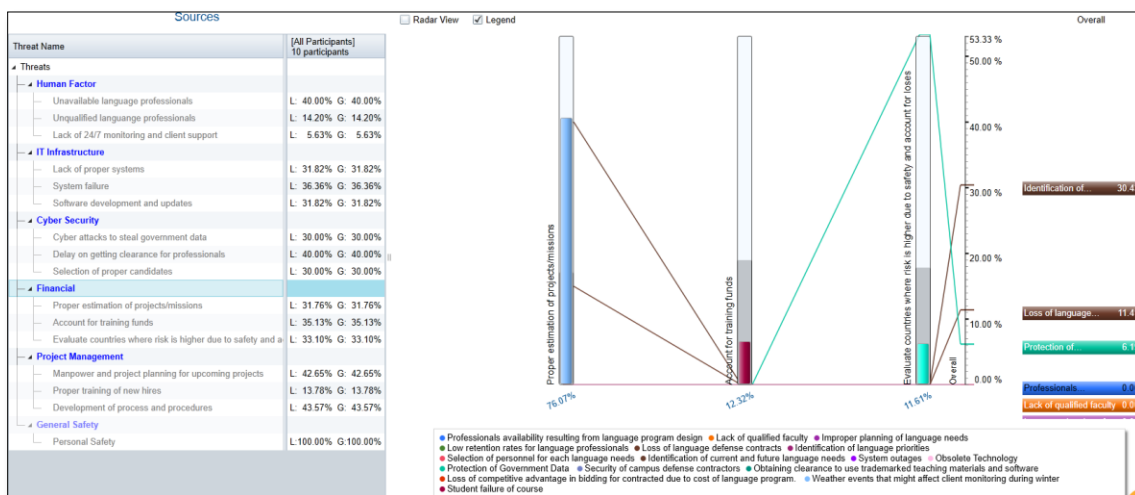


Figure 27 - Performance Sensitivity Showing Sources and Event Likelihood

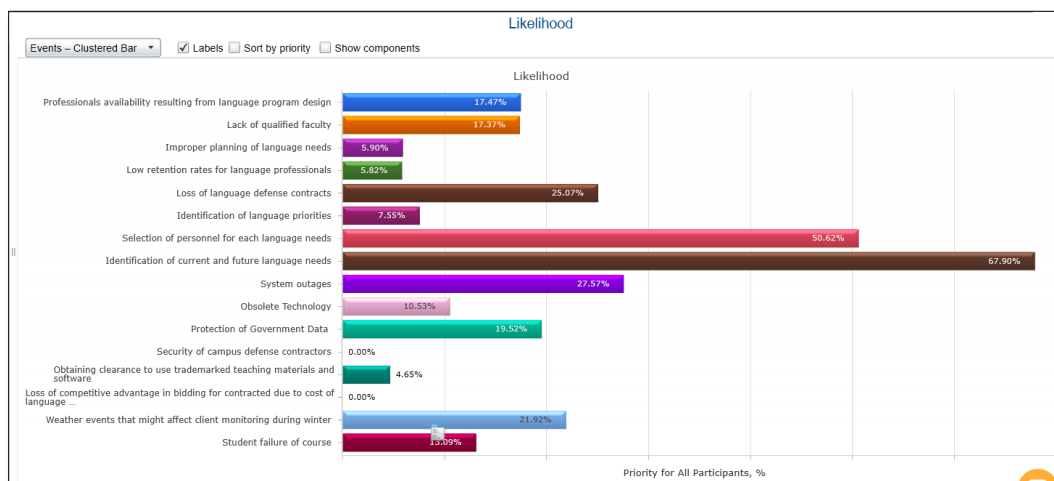


Figure 28 - Overall Likelihoods of Events with Respect to Sources

b) Impact of Events

As mentioned in the preceding section, we have used the Riskion software, to measure the likelihood of events, and the impact of events based on the powerful tools provided by Riskion, which gives the firm a better option for visualizing the dynamic, and priority sensitivity analysis of decisions made regarding risk on this need project.

Given some of the figures we have already provided in the prior section, we have shown you how simple changes in events can lead to lower risk in other aspects. For instance, when describing the performance sensitivity analysis for proper estimation of project and mission's costs, we showed an increase in this would lead to a much lower event likelihood for the other two financial outcomes. As a result, the firm would take this into account, and would hire accountants to increase the success rate of estimations for cost, and thus address the risk. Furthermore, this would enter our list of objects seen in figure 30 Moreover, we have taken an approach to Riskion as being a living document that we can change with the addition of events, priorities, and likelihoods.

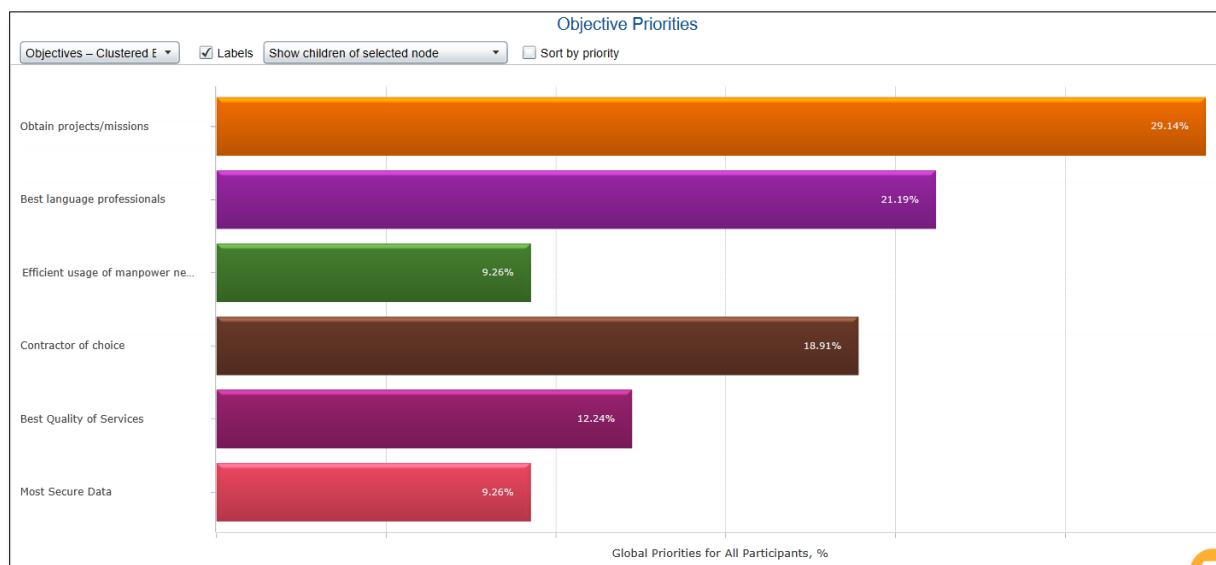


Figure 29 - Overall Priorities of Objectives – objectives chart

Objectives	[All Participants] 8 with judgments
Obtain projects/missions	29.14%
Best language professionals	21.19%
Contractor of choice	18.91%
Best Quality of Services	12.24%
Efficient usage of manpower needs	9.26%
Most Secure Data	9.26%

Figure 30 - Overall Priorities of Objectives – objectives grid

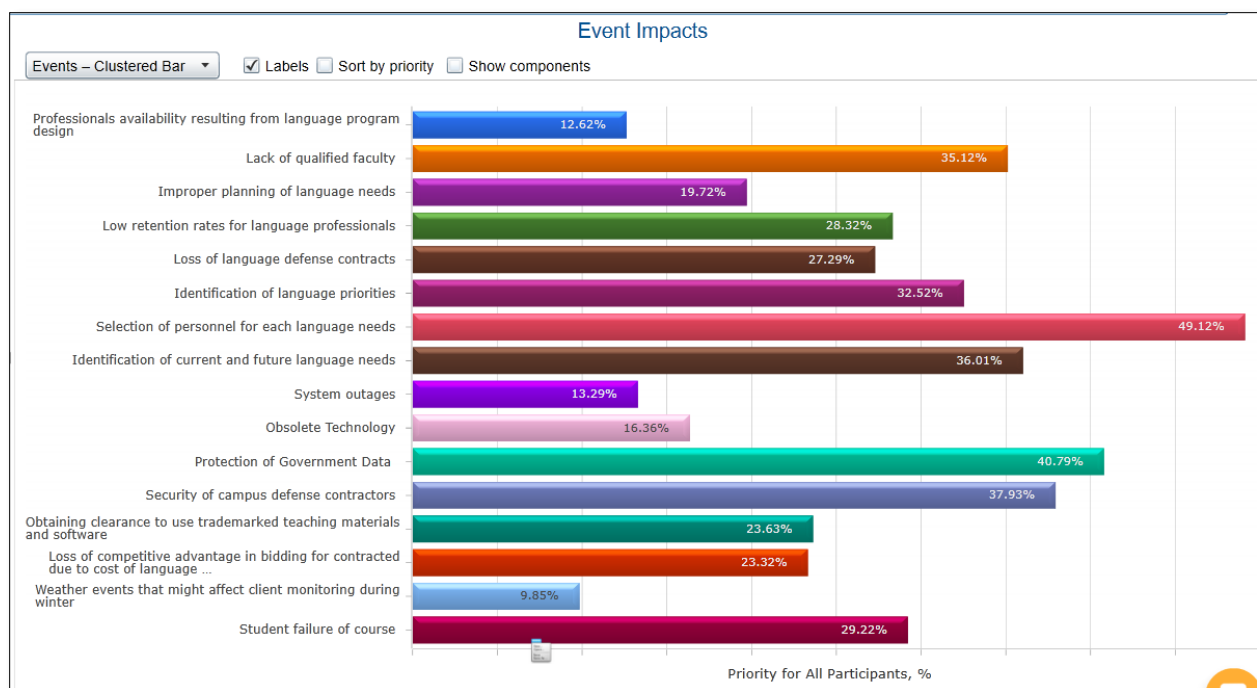


Figure 31 - Overall Events Impact – events chart

	Events	[All Participants] 8 with judgments
[07]	Selection of personnel for each language needs	49.12%
[11]	Protection of Government Data	40.79%
[12]	Security of campus defense contractors	37.93%
[08]	Identification of current and future language needs	36.01%
[02]	Lack of qualified faculty	35.12%
[06]	Identification of language priorities	32.52%
[16]	Student failure of course	29.22%
[04]	Low retention rates for language professionals	28.32%
[05]	Loss of language defense contracts	27.29%
[13]	Obtaining clearance to use trademarked teaching materials and software	23.63%
[14]	Loss of competitive advantage in bidding for contracted due to cost of language program.	23.32%
[03]	Improper planning of language needs	19.72%
[10]	Obsolete Technology	16.36%
[09]	System outages	13.29%
[01]	Professionals availability resulting from language program design	12.62%
[15]	Weather events that might affect client monitoring during winter	9.85%

Figure 32 - Overall Events Impact – events grid

5. Risk without Controls

Risk was identified within the Riskion model, by brainstorming between different aspects within the participant's respectable fields, and also including management. As a result, the firm could judge what possible risks might come to face during the execution of this project. As a result, the firm could determine the risk involved in the project, and was able to better visualize, and present the risk in a more understandable way, as a percentage, or monetary value, such as what we see in figure 33 below.

Overall Likelihoods, Impacts, and Risks for «Project: Development of a Language Learning Program»							
No.	Event	Likelihood		All Participants Impact		Risk	
		Computed	Simulated	Computed	Simulated	Computed ▼	Simulated
[12]	Security of campus defense contractors	59.99%	36.68%	37.93%	29.90%	22.76%	10.94%
[08]	Identification of current and future language needs	56.91%	23.30%	36.01%	30.13%	20.50%	7.02%
[07]	Selection of personnel for each language needs	34.05%	23.70%	49.12%	42.71%	16.72%	10.12%
[11]	Protection of Government Data	28.52%	13.65%	40.79%	31.94%	11.63%	4.36%
[05]	Loss of language defense contracts	29.34%	10.80%	27.29%	18.19%	8.01%	1.96%
[02]	Lack of qualified faculty	16.56%	10.70%	35.12%	26.91%	5.81%	2.88%
[14]	Loss of competitive advantage in bidding for contracted due to cost of language program.	20.20%	15.40%	23.32%	17.87%	4.71%	2.75%
[09]	System outages	30.32%	9.50%	13.29%	11.01%	4.03%	2.15%
[16]	Student failure of course	13.09%	13.10%	29.22%	23.57%	3.82%	3.09%
[06]	Identification of language priorities	7.55%	6.70%	32.52%	26.03%	2.46%	1.74%
[01]	Professionals availability resulting from language program design	17.79%	11.15%	12.62%	9.76%	2.25%	1.09%
[15]	Weather events that might affect client monitoring during winter	21.92%	20.10%	9.85%	8.29%	2.16%	1.67%
[10]	Obsolete Technology	11.59%	11.30%	16.36%	12.99%	1.90%	1.47%
[04]	Low retention rates for language professionals	6.40%	2.70%	28.32%	22.69%	1.81%	0.61%
[03]	Improper planning of language needs	5.90%	5.10%	19.72%	15.37%	1.16%	0.78%
[13]	Obtaining clearance to use trademarked teaching materials and software	4.24%	3.30%	23.63%	15.36%	1.00%	0.51%
		Total Risk: 110.72%					
		Average Loss: 53.15%					

Figure 33 - Overall Likelihood, Impacts, and Risks (Without Controls)

Looking at figure 33, we see that the project was extremely risky at 110.72% with an average loss of 53.15% without controls.

a) Bow-tie Diagram – Without Controls

In addition, another method afforded to us via Riskion, to better visualize our risks comes in the form of bow-tie diagrams such as the one in figure 34. In this figure, we see how threats contribute to the risk of an event. In this case, “Protection of Government Data”. Furthermore, we are also able to see the objectives of the event, and how lowering the risk of said event would in-turn increase the chance that our events are accomplished.

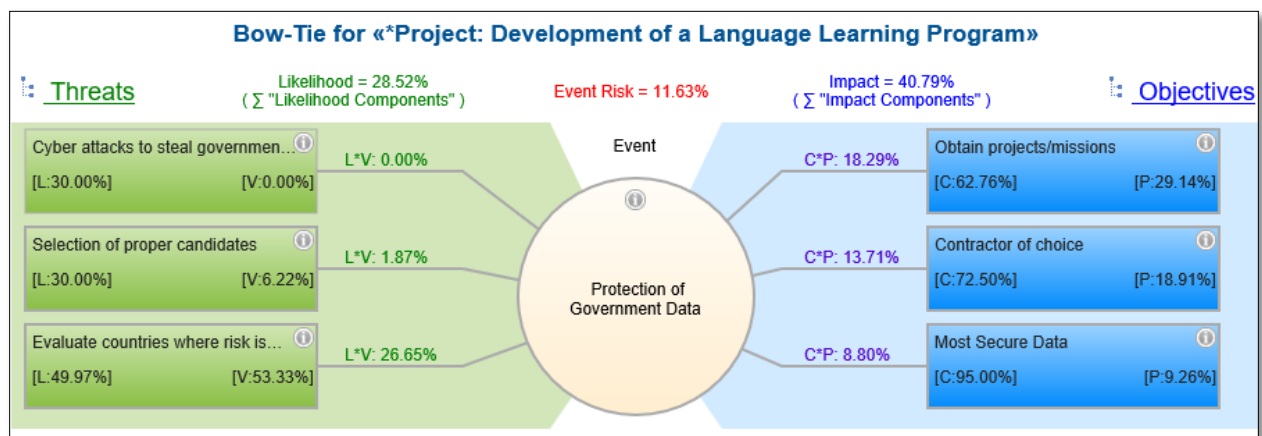


Figure 34 - Bow-Tie Diagram without Controls for Protection of Government Data

b) Risk Map – Without Controls

In addition, we can further visualize the complete picture of the risk involved with this project, by using the “Risk Map” option in Riskion, depicted in figure 35.

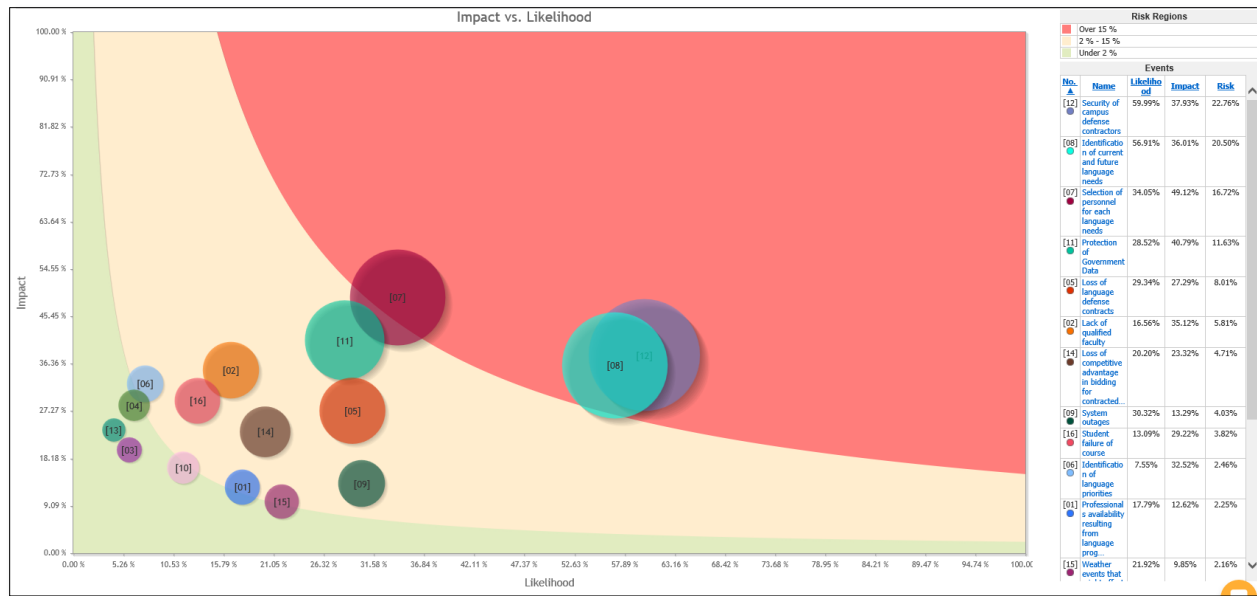


Figure 35 - Risk Map without Controls (Impact vs. Likelihood)

6. Risk with Controls

Much like the prior topic (Risks without Controls) we will now discuss these same risks. However, we will also introduce controls, and explain how these controls have influenced the outcome of the model, and on decision making, regarding the project. Furthermore, these risks are displayed with likelihoods, impacts, and risks much like the proceeding section. However, in this section we have added controls to better mitigate the risk.

Figure 36 below reflects the list of identified controls, the selected controls as well as the cost assigned to each of them. Under column “applications” it reflects where the control is being applied. “S.A Reduction” column stands for Stand Alone Reduction which means that when using that control how much it will reduce the risk.

Effectiveness is the “power” of the control. For exempla “Common Access Card Portal Entry” has no effectiveness as S.A is zero. We left it like that to demonstrate the concept.

For our base scenario, we selected all controls because we wanted to analyze this case. In optimization, we show two alternative scenarios.

Index	Control Name	Control for	Selected	Cost	Applications	Categories	S.A. Reduction	Must	Must Not
01	Cyber Security Professionals	Threat	Yes	250000	4		11.58	<input checked="" type="checkbox"/>	<input type="checkbox"/>
02	Anti-Phishing training	Threat	Yes	50000	3		8.27	<input checked="" type="checkbox"/>	<input type="checkbox"/>
03	Security Gaurd	Threat	Yes	80000	1		16.75	<input checked="" type="checkbox"/>	<input type="checkbox"/>
04	Common Access Card portal enty	Threat	Yes	100000	1		0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
05	Campus Gate/ Security System	Threat	Yes	250000	1		15.89	<input checked="" type="checkbox"/>	<input type="checkbox"/>
06	Hiring Security Specialist (SSO)	Threat	Yes	150000	5		9.58	<input checked="" type="checkbox"/>	<input type="checkbox"/>
07	Increase pay for experience	Vulnerability	Yes	500000	2		2.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>
08	Hire Defense Analyst	Vulnerability	Yes	125000	1		1.46	<input checked="" type="checkbox"/>	<input type="checkbox"/>
09	Retention Contracts	Vulnerability	Yes	350000	2		3.32	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10	Quality Checking	Consequence	Yes	100000	16		19.82	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11	Negotiations with client	Consequence	Yes	15000	17		31.81	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	Hiring additional linguists	Consequence	Yes	600000	15		26.35	<input checked="" type="checkbox"/>	<input type="checkbox"/>
13	Faculty Trial Periods	Consequence	Yes	60000	7		5.57	<input checked="" type="checkbox"/>	<input type="checkbox"/>
14	Language Needs Analyst	Consequence	Yes	170000	13		22.41	<input checked="" type="checkbox"/>	<input type="checkbox"/>
15	Weekly Pre-Tests (Mock Tests)	Consequence	Yes	200000	8		4.83	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 36 - Control Register with selected controls, associated cost and applications

Figure 37 below reflects the “mapping” of the controls with the threats, this means which controls are to be applied to what threats.

Figure 38 represents an example of measurement methods for control for threats. Evaluation summary is further below in figure 40. We used the same method as before where we assigned roles to the participants and send the link for them to make the necessary judgments.

Controls for Threat Likelihoods											
Control Name	Threats										
	Human Factor			IT Infrastructure			Cyber Security			Proper estimation of projects/missions	
	<input type="checkbox"/> Unavailable language professionals	<input type="checkbox"/> Unqualified language professionals	<input type="checkbox"/> Lack of 24/7 monitoring and client support	<input type="checkbox"/> Lack of proper systems	<input checked="" type="checkbox"/> System failure	<input checked="" type="checkbox"/> Software development and updates	<input checked="" type="checkbox"/> Cyber attacks to steal government data	<input checked="" type="checkbox"/> Delay on getting clearance for professionals	<input checked="" type="checkbox"/> Selection of proper candidates		
<input checked="" type="checkbox"/> 1. Cyber Security Professionals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> 2. Anti-Phishing training	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> 3. Security Gaurd	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> 4. Common Access Card portal enty	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> 5. Campus Gate/ Security System	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> 6. Hiring Security Specialist (SSO)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Figure 37 – Example Control for Threats

Measurement Methods for Controls for Threats									
Control Name	Threats								
	Human Factor			IT Infrastructure			Cyber Security		
	Unavailable language professionals	Unqualified language professionals	Lack of 24/7 monitoring and client support	Lack of proper systems	System failure	Software development and updates	Cyber attacks to steal government data	Delay on getting clearance for professionals	Selection of proper candidates
1. Cyber Security Professionals					Direct	Direct	Direct		
2. Anti-Phishing training					Direct		Direct		
3. Security Gaurd									
4. Common Access Card portal enty							Direct		
5. Campus Gate/ Security System									
6. Hiring Security Specialist (SSO)					Direct		Direct	Direct	Direct

Figure 38 – Example of measurement methods for Control for Threats

Participant Roles											
Allow All	Drop All	Show	<input checked="" type="radio"/> All <input type="radio"/> Controls for Threats <input type="radio"/> Controls for Vulnerabilities <input type="radio"/> Controls for Impacts								
Control Name	Farris Darawsheh, Program Manager (farrisdarawsheh@gwu.edu)	Professor Forman (forman@gwu.edu)	Craig Carter, Government Liaison Manager (GL_Manager@gwu.edu)	Jane Ramsay, IT Manager (IT_Manager@gwu.edu)	Pamela Tom, Language Validation Officer (l_validation_officer@gwu.edu)	Nicholas Stavrakakis (nstavrakakis@gwu.edu)	Marque Pierre, Project Services Manager (PS_Manager@gwu.edu)	John Cheng, Risk Manager (Risk_Manager@gwu.edu)	Sandra Mejia Villegas, Project Manager (sandrarmv@gwu.edu)	Eric Peck, Cyber Security Advisor (security_advisor@gwu.edu)	
Controls for Threats											
<input type="checkbox"/> Cyber Security Professionals	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Anti-Phishing training	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Security Gaurd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Common Access Card portal enty	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Campus Gate/ Security System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Hiring Security Specialist (SSO)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Controls for Events											
<input type="checkbox"/> Increase pay for experience	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Hire Defense Analyst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Retention Contracts	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Controls for Consequences											
<input type="checkbox"/> Quality Checking	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Negotiations with client	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Hiring additional linguists	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Faculty Trial Periods	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Language Needs Analyst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> Weekly Pre-Tests (Mock Tests)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Figure 39 – Participant Roles for Controls Evaluation

Participant Name	Email Address	Evaluation Progress	Last Judgment Time	Search:	Actions
Sandra Mejia Villegas, Project Manager	sandrarmv@gwu.edu	100.0% (96/96)	10/9/2017 7:07:31 PM		
Farris Darawsheh, Program Manager	farrisdarawsheh@gwu.edu	100.0% (96/96)	10/16/2017 11:16:32 PM		
Eric Peck, Cyber Security Advisor	security_advisor@gwu.edu	100.0% (18/18)	10/9/2017 6:15:46 PM		
Pamela Tom, Language Validation Officer	l_validation_officer@gwu.edu	100.0% (17/17)	10/9/2017 6:21:59 PM		
Jane Ramsay, IT Manager	IT_Manager@gwu.edu	100.0% (5/5)	10/9/2017 6:27:50 PM		
John Cheng, Risk Manager	Risk_Manager@gwu.edu	100.0% (8/8)	10/9/2017 6:30:20 PM		
Marque Pierre, Project Services Manager	PS_Manager@gwu.com	100.0% (16/16)	10/16/2017 11:10:22 PM		
Craig Carter, Government Liaison Manager	GL_Manager@gwu.edu	100.0% (6/6)	10/16/2017 11:31:40 PM		
Professor Forman	forman@gwu.edu	0.0% (0/0)			
Nicholas Stavrakakis	nstavrakakis@gwu.edu	0.0% (0/0)			

Figure 40 – Evaluation Progress Summary for Controls

The Riskion software enables the user to apply controls to many events which have been populated into the project model. In the following figure 41, we see an example of the

overall project with all the controls added. As a result, we see in the figure that the risk had been reduced by 82.06% or \$2,461,771.64 which is rather significant for the health of the project.

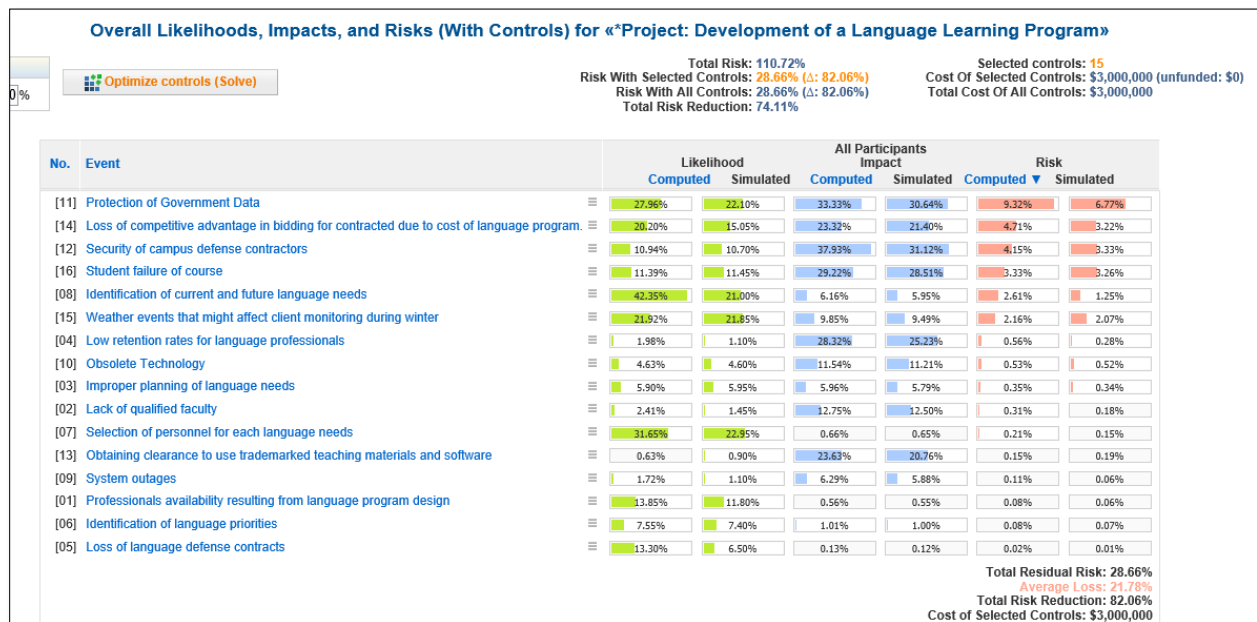


Figure 41 - Overall Likelihood, Impacts, and Risks (With Controls)

a) Bow-tie Diagram – With Controls

Much like the bow-tie diagram in the prior section without controls, the following figure is simply an example of a bow-tie diagram for “Protection of Government Data” with controls added, as seen in figure 42.

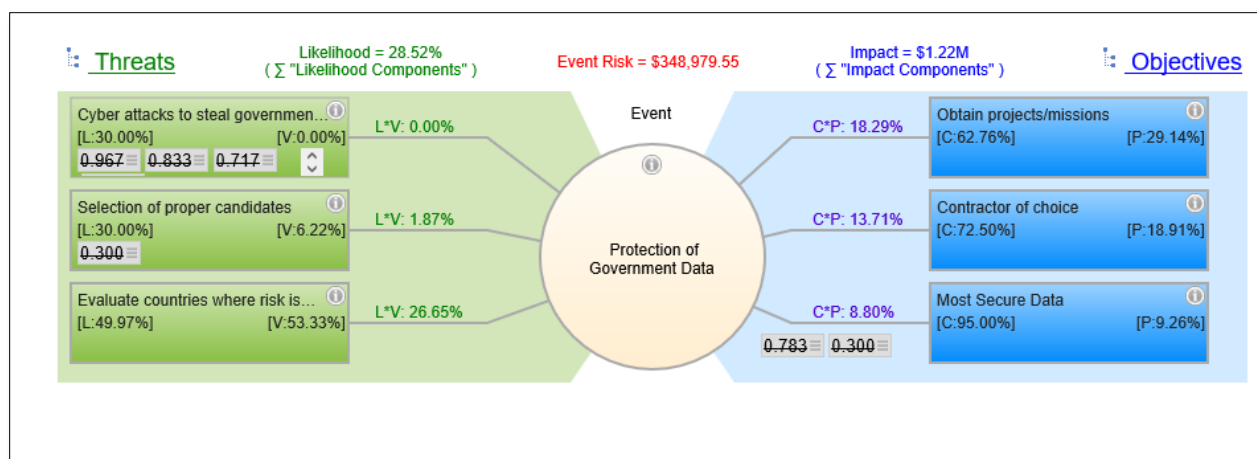


Figure 42 - Bow-Tie Diagram with Controls for Protection of Government Data

b) Risk Map – With Controls

In addition, we can use other methods to display the risk we might experience within a project, and one of these ways comes in the form of risk maps. Risk maps give us the ability to see impacts vs. likelihoods on an easier to understand format, such as what we see in figure 43.

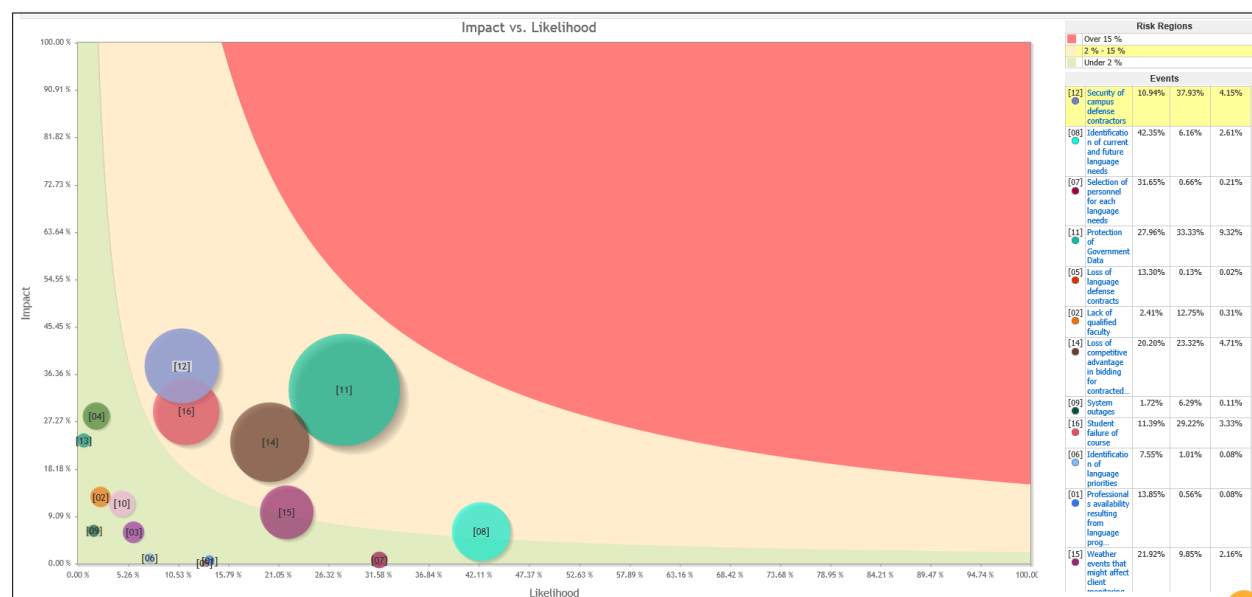


Figure 43 - Risk Map with Controls (Impact vs. Likelihood)

Figure 44 below shows the loss exceedance curve, the frequency chart and the cumulative frequency chart.

In the frequency chart, each dot represents a possible outcome of a trial (or simulation). If we analyze figure 45 further below, we can see an example of one trial. Highlighted in yellow are the threats that fired, this means that the random number generator has values less than the likelihood of that event.

In figure 44 in the top part, we can see a cell named “step”, this represents the different simulations or trials. The difference between simulations and calculated averages are that in the simulation each fired threat fires only once.

In organizations, decision makers analyze risk as having too much loss therefore they tend to use more the loss exceedance curve instead of the cumulative frequency chart. If you look closely you will notice that one is the complement of the other one.

In the loss exceedance curve, the “y” axis is the probability of losing that much or more. The “x” axis is the percent loss. One important point to use when communicating to upper management when using this curve is the “value at risk”. The value at risk is typically a convention of 95%.

For example, in our case, in the table below, we can see that we are 95% sure that we won't lose more than 57.7% or \$1.83MM.

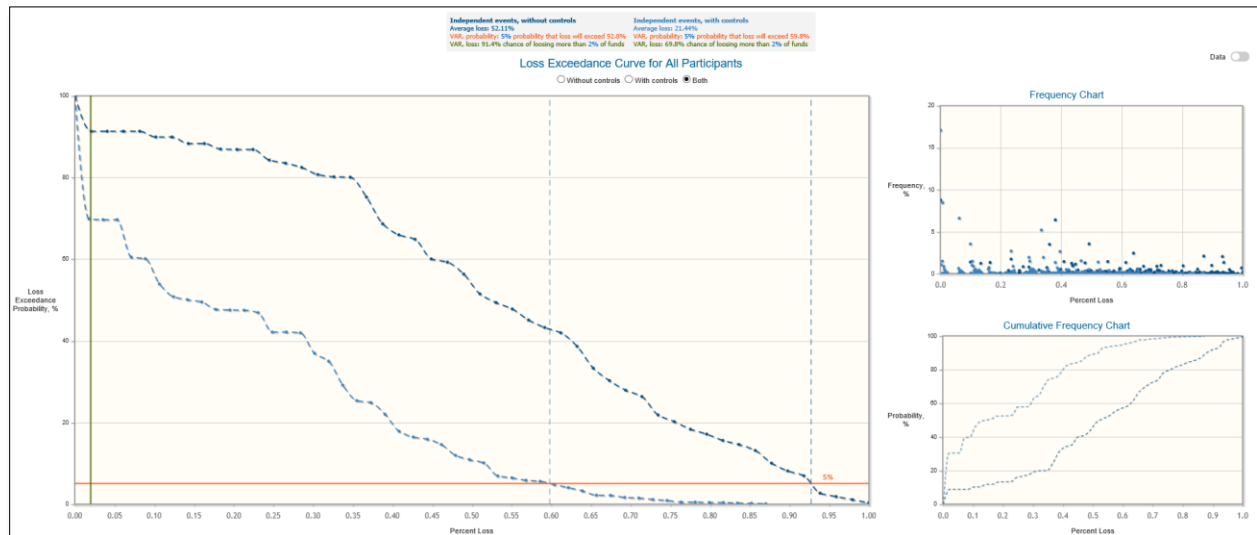


Figure 44 - Loss Exceedance Curve - Graph

Threats (without controls)				Threats (with controls)				Total loss of simulation: 0.674601				Total loss of simulation: 0.333301					
Number of threats that fired: 7				Number of threats that fired: 4				Number of Events that fired: 2				Number of Events that fired: 1					
Threat Name	Threat Random()	Priority		Threat Random()	Priority			Event Name	Random()	Vulnerability	Impact	Risk	Random()	Vulnerability	Impact	Risk	
[2] Unavailable language professionals	0.85668726	0.40000001		0.85668726	0.40000001			Professionals availability resulting from lan... T ₀ =[1]	0.85264204		0	0.12621182	0.02245575	0.85264204	0	0.12621182	0.02245575
[3] Unqualified language professionals	0.33010182	0.14198147		0.33010182	0.14198147			Low retention rates for language professional... T ₀ =[5]	0.13467804		0	0.28323904	0.01812263	0.13467804	0	0.28323904	0.01812263
[6] Lack of 24/7 monitoring and client support	0.96265205	0.05634538		0.96265205	0.05634538			Loss of language defense contracts T ₀ =[5]	0.54524043		0	0.27288106	0.08006019	0.54524043	0	0.27288106	0.08006019
[5] Lack of proper systems	0.322788381	0.35000002		0.322788381	0.35000002			Identification of language priorities T ₀ =[5]	0.19639483		0	0.32523946	0.02455943	0.19639483	0	0.32523946	0.02455943
[9] System failure	0.89159377	0.40000001		0.89159377	0.40000001			System outages T ₀ =[5]	0.42767305		0	0.1329022	0.04030147	0.42767305	0	0.1329022	0.04030147
[16] Software development and updates	0.66565605	0.35000002		0.66565605	0.35000002			Obsolete Technology T ₀ =[8]	0.84772998		0	0.16364373	0.0189585	0.84772998	0	0.16364373	0.0189585
[8] Cyber attacks to steal government data	0.20154529	0.30000001		0.20154529	0.30000001			Protection of Government Data T ₀ =[8]	0.78839439		0	0.40791854	0.11632652	0.78839439	0	0.40791854	0.11632652
[11] Delay on getting clearance for professionals	0.11620664	0.40000001		0.11620664	0.40000001			Obtaining clearance to use trademarked teach... T ₀ =[8]	0.52670309		0	0.01001118	0.00000000	0.52670309	0	0.01001118	0.00000000
[14] Selection of proper candidates	0.20808994	0.30000001		0.20808994	0.30000001			Lack of qualified faculty T ₀ =[14]	0.00992428	0.12996405	0.3630829	0.35117656	0.00992428	0.00992428	0.12996405	0.3630829	0.35117656
[18] Proper estimation of projects/missions	0.29321951	0.47949961		0.29321951	0.47949961			Selection of personnel for each language need... T ₀ =[14]	0.26568866	0.76877	0.49117389	0.16722303	0.26568866	0.18902931	0.720734	0.29221374	0.03824113
[19] Account for training funds	0.79308426	0.53035313		0.79308426	0.53035313			Identification of current and future language... T ₀ =[14]	0.19019842	0.30000001	0.1920929	0.36014712	0.19019842	0	0.19715405	0.0116229	0.19715405
[20] Evaluate countries where risk is higher due t...	0.62528299	0.49968827		0.62528299	0.49968827			Student failure of course T ₀ =[14]	0.18902931	0.20734	0.25221374	0.03824113	0.18902931	0.20000000	0.298032	0.23320113	0.04709976
[13] Manpower and project planning for upcoming pr...	0.78604709	0.42646545		0.78604709	0.42646545			Improper planning of language needs T ₀ =[18]	0.19715405		0	0.19715405	0.0116229	0.19715405		0	0.19715405
[10] Proper training of new hires	0.08743455	0.13783737		0.08743455	0.13783737			Loss of competitive advantage in bidding for ... T ₀ =[18]	0.20000000	0.290232	0.23320113	0.04709976	0.20000000	0.290232	0.23320113	0.04709976	
[17] Development of process and procedures	0.86254166	0.4356972		0.86254166	0.4356972			Security of campus defense contractors T ₀ =[22]	0.37934491	0.5	0.37934491	0.2275833	0.37934491	0.5	0.37934491	0.2275833	
[22] Personal Safety	0.32143171	1		0.32143171	0.8899933			Weather events that might affect client monit... T ₀ =[22]	0.0984828		0	0.0984828	0.02158465	0.0984828		0	0.0984828

Figure 45 - Loss Exceedance Curve - Data

7. Optimization

We learned in class that the relative likelihood of success is the complement of the relative likelihood of failure. When optimizing a portfolio of events or projects, the anticipated benefits can be discounted for risk by multiplying the anticipated benefit of each event or project by its relative likelihood of success.

For optimization we decided to use two different scenarios. The purpose is to demonstrate the purpose of selecting proper controls.

Figure 46 below was optimized by selecting a risk reduction of 30%. In order to have this result, Riskion identifies that we only need one control, this control has the highest effectiveness (S.A reduction). This control is highlighted in darker yellow.

This is a great idea when presenting to upper managers. Sometime managers want to see different scenarios before making a decision. Sometime there is a cap on risk or a cap on budget.

Further below we have the efficient frontier curve. In this case, the efficient frontier is very useful to analyze the relationship between controls cost and optimized risk.

[From Investopedia](#): The efficient frontier is the set of optimal portfolios that offers the highest expected return for a defined level of risk or the lowest risk for a given level of expected return.

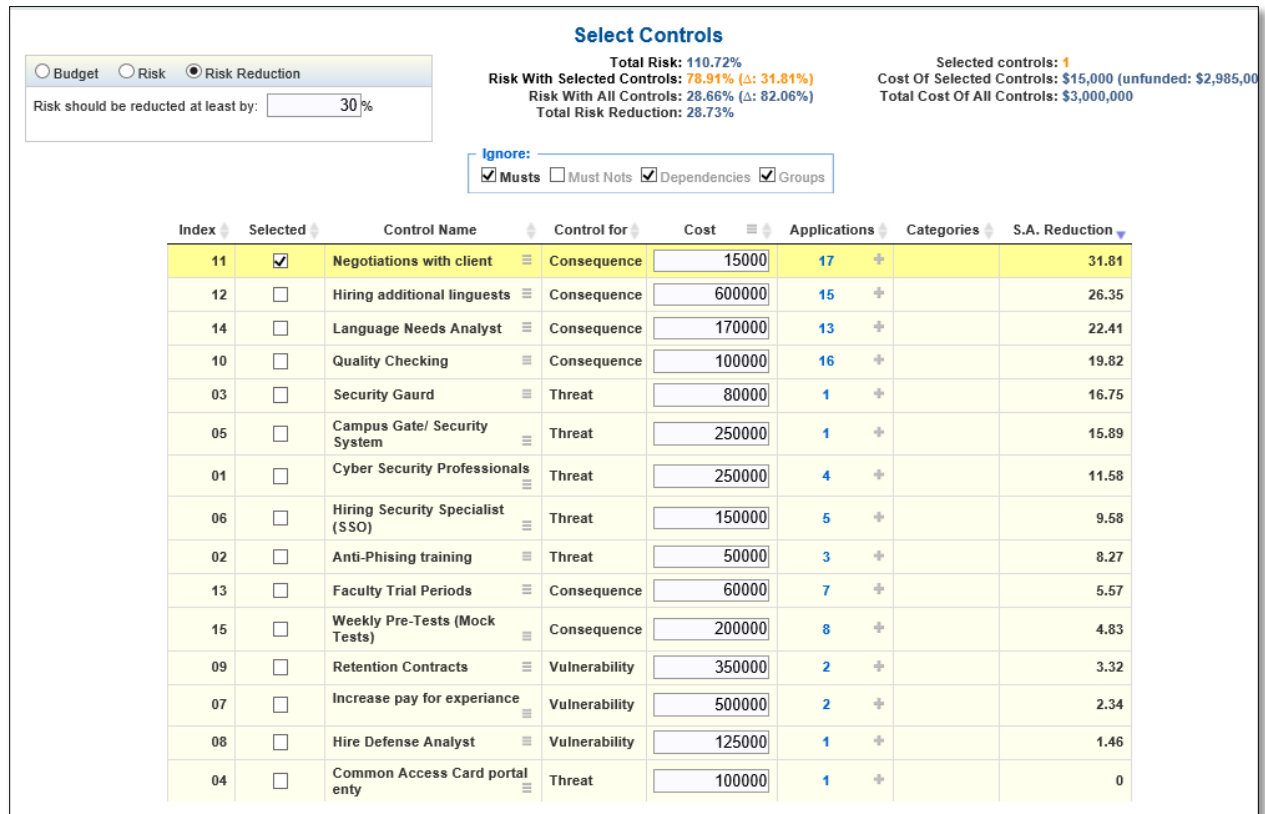


Figure 46 - Optimization Results 30% reduction of risk

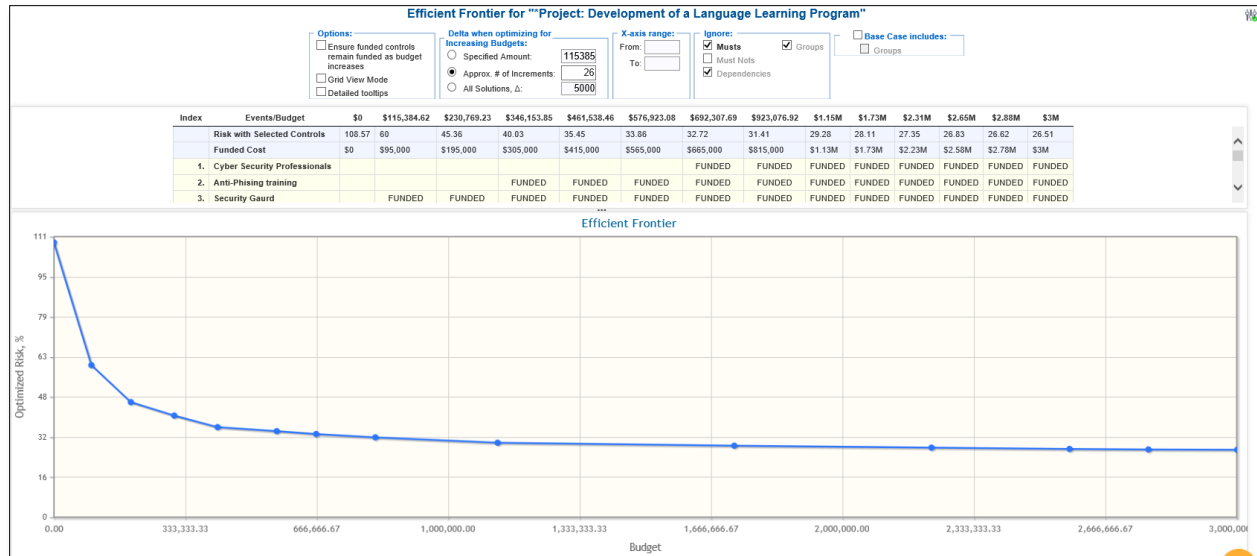


Figure 47 - Efficient Frontier

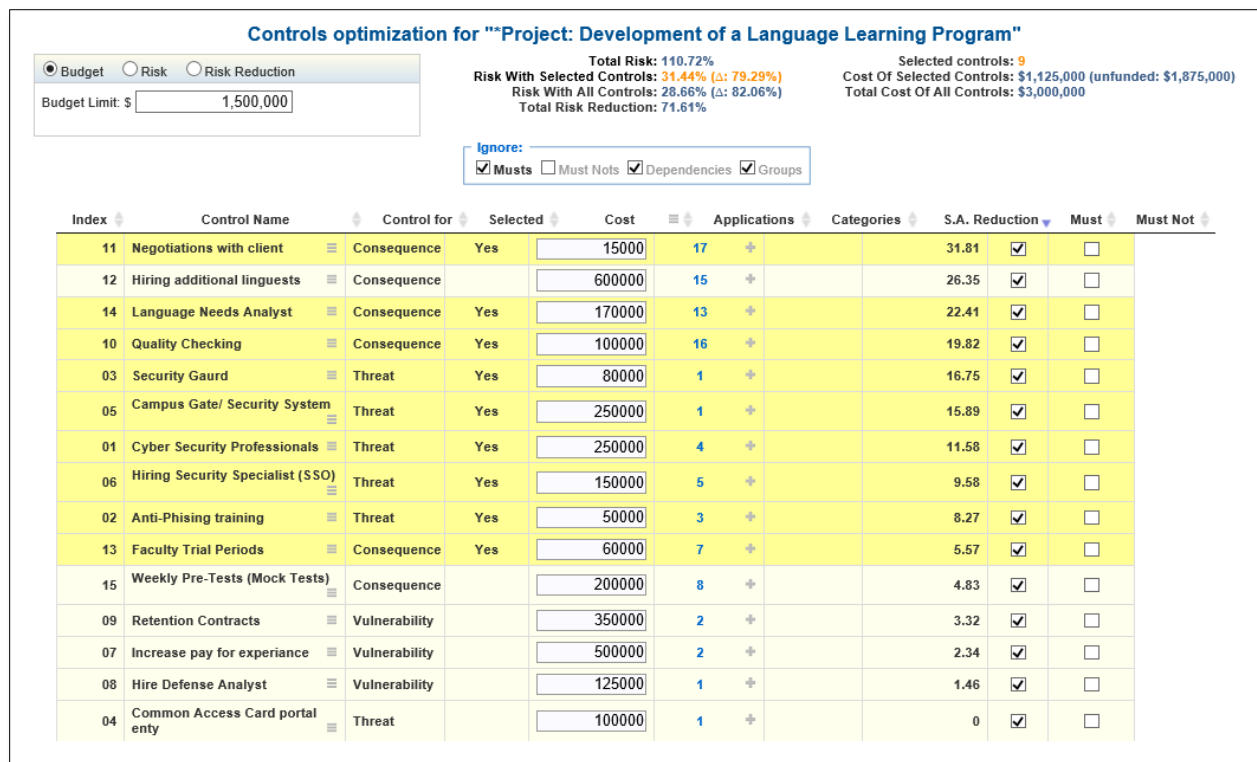


Figure 48 - Optimization Results \$1.5MM budget for reduction of risk

We found the scenario in figure 48 to be very interesting. In this case, we optimized the risk by constraining the budget for controls to \$1.5MM. Note that the cost to implement all controls is \$3MM. What we found interesting about this case is that using \$1.25MM of the budget, we have

risk with selected controls 31.44% instead of risk with all controls of 28.66%. What we liked about Riskion is that it is a great tool for communication as this type of scenario analysis is key for organizations.

8. Conclusion

We have identified risk events, threat or sources, objectives or consequences. We also identified key participants and assigned roles. Once we identified those key elements, we created a solid model structure and mapped the information. After that, we selected measurement methods understanding the importance of how Riskion uses measurements to produce mathematically meaningful results. What this means is that in order for mathematical operations with numbers to be 'meaningful', the numbers must possess certain level of measurement. As an example, care must be taken not to multiply or add ordinal measures. It is meaningful to multiply to ratio scale numbers, or a ratio scale number by an interval scale measure, but not to multiply to interval level measures.

We used "Bow-Tie" diagram to show, for each risk, the causes, vulnerabilities and impact on objectives and we used the "Heat Map" bubble plot of likelihood vs. impact for each event the bubble size proportional to the risk.

We used the provided mechanism that Riskion has in order to collaborate in identifying treatments to reduce risks and to estimate the relative effectiveness of those treatments. The Riskion process enable decision makers to use different methods to determine which risk events to address and/or which treatments to implement. Synthesizing the likelihood of events as the sum products of the likelihoods of the event's causes and the vulnerabilities of the event to the causes.