Modernizing Government Technology Act

Managing Risk in Government Technology Upgrade

The George Washington University

DNSC6254 Risk Management (RM)

October 21, 2018

Team Members:

Ryan Moorman

Qiao Wang

Contents

1. Executive Summary

1.1 Overview

2. Risk Analysis Methodology

2.1. Identification of Risk Events

2.2. Identifying Sources

2.3. How Sources May Contribute to an Event

2.4. Identifying Objectives

3. Risk Measurement & Evaluation Process

3.1. Participants and their Roles

3.2. Measurement Methods

4. Risk Analysis Synthesized Results

4.1. Synthesis: Likelihood of Events and Sources

4.2. Synthesis: Impact of Events and Objectives

5. Risk Review and Landscape

5.1 Overall Risk without Controls

6. Implementation of Risk Controls

7. Risk with Controls

8. Conclusion

1 Executive Summary

The Executive Office of the President of Management and Budget provided heads of executive departments and agencies the opportunity to invest in modern technology solutions to improve service delivery to the public, secure sensitive systems and data, and save tax payers dollars by signing the Modernization of Government Technology act. Laid out in the MGT is guidance and expectations for agencies to adhere to including the submittal process for projects, project submittal expectations, project board review process and implementation information, all of which are aimed at improving Government Technology. With this in mind our team performed a risk assessment to prepare the Office of Management and Budget the expectations of risk involved in improving government technology through the MGT act. Our team used riskion software to quantify risk through a measurement and synthetization process which would give a decision maker involved useful insight towards risk mitigation. This report provides a detailed summary our findings.

1.1 Overview

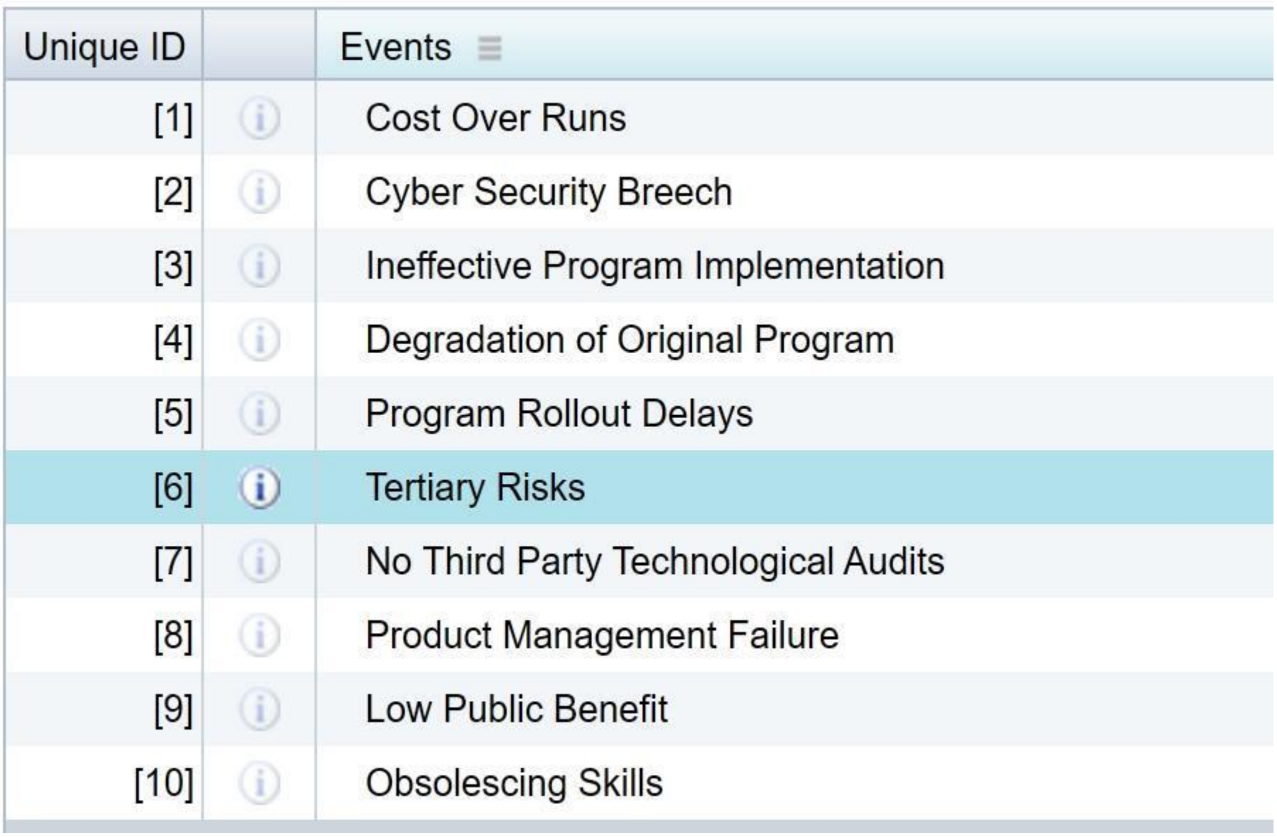
In December 2017 Congress enacted the Modernizing Government Technology Act. As a part of Fiscal Year 2018 National Defense Authorization Act the act has a primary provision of establishing a $800 million centralized Technology Modernization Fund over the course of two years and also establishing a Technology Modernization Board. The TMB will consist of a seven person board who come from the Federal Government programs in IT, finance, cybersecurity, and acquisition to serve alongside the Federal CIO who will act as the Chairman. The roles and responsibility of the board will be to distribute information and communications of TMF while also reviewing project proposals to determine viability to the MGT. As evidenced by other costly and sometimes unsuccessful government projects such as HealthCare.gov and Canada's Phoenix cost overruns and delays are common place. There are inherent risks in technological and security updates within the US government to consider given the age and capabilities of the technology systems and the board would like to mitigate the failures that those projects had. The OMB would like to ensure that the TMF is being used to provide the government with viable improvements to technology that are beneficial, cost effective, and secure.

2 Risk Analysis Methodology

Our team decided to execute its risk assessment process objectively using Riskion. Risk assessment requires a systematic process for identifying and analyzing events that can affect the achievement of objectives. For this reason, Riskion was chosen as the preferred software to aid in this process as it provides a theoretically sound and practical process for us to identify the likelihood of an event occurring and its potential impact on the objectives. We used a bottom-up approach during this process by first identifying the potential events that could result in a loss, the sources of those events, and then the impact of those events on the objectives.

2.1 Identification of Risk Events

By using the Riskion software, we identified ten risk events that could impact the Implementation of the Modernizing Government Technology Act. These ten events were brainstormed and prioritized based on potential impact and cause of loss to the overall project.

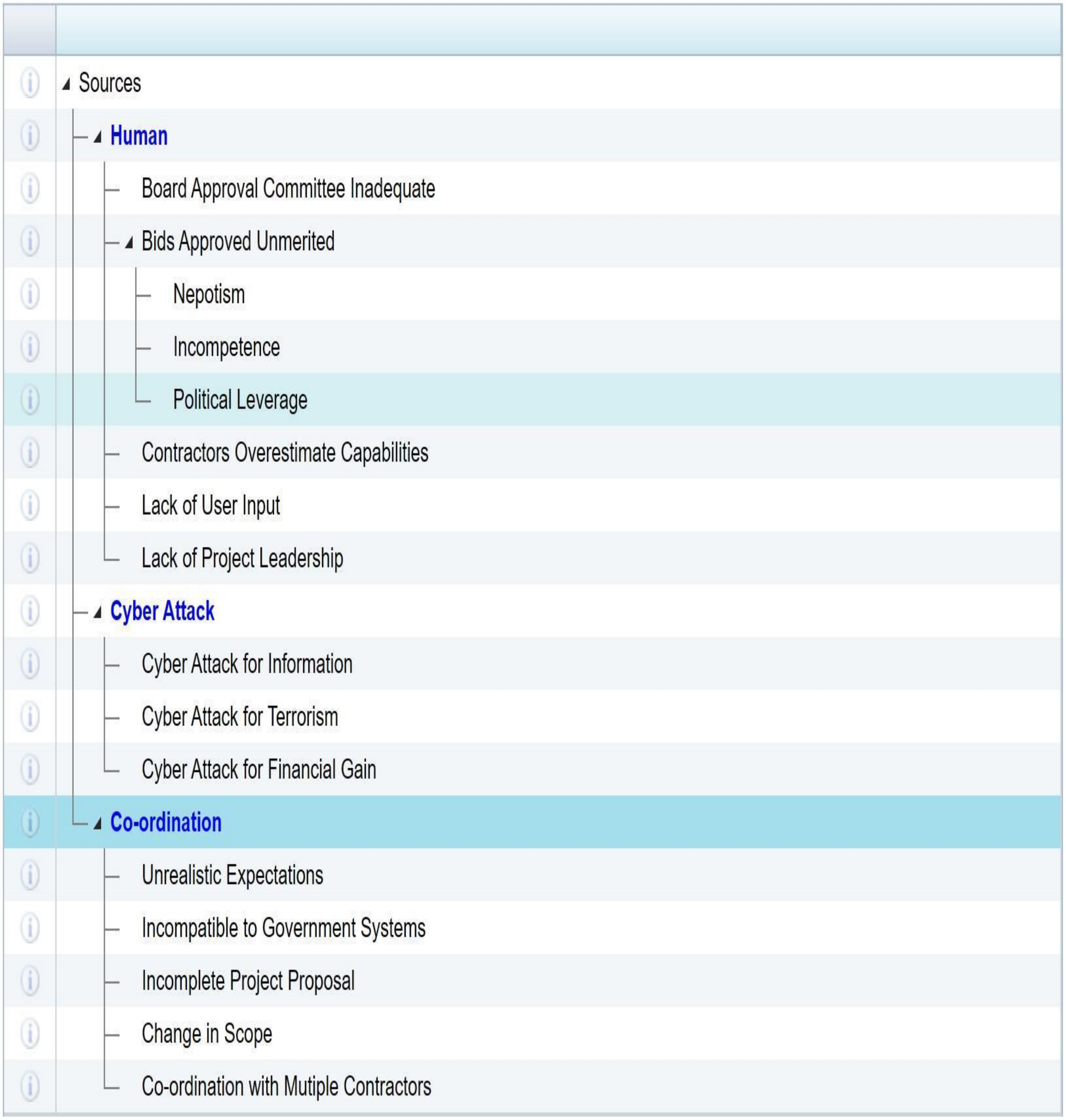


Unique ID		Events
[1]	ⓘ	Cost Over Runs
[2]	ⓘ	Cyber Security Breech
[3]	ⓘ	Ineffective Program Implementation
[4]	ⓘ	Degradation of Original Program
[5]	ⓘ	Program Rollout Delays
[6]	ⓘ	Tertiary Risks
[7]	ⓘ	No Third Party Technological Audits
[8]	ⓘ	Product Management Failure
[9]	ⓘ	Low Public Benefit
[10]	ⓘ	Obsolescing Skills

2.1 Risk Events

2.2 Identifying Sources

The figure below shows the sources to the risk events. We identified three main sources that could cause an event to result in a loss. We also identified sub-sources to further elaborate on the assumable threats.

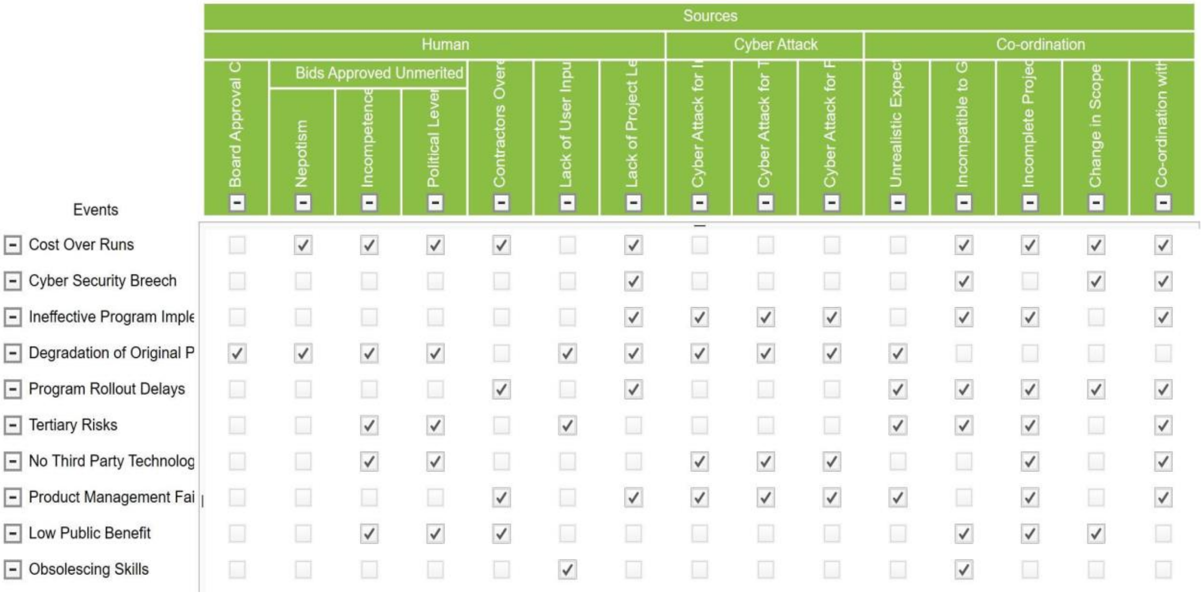


- Sources
  - Human
    - Board Approval Committee Inadequate
    - Bids Approved Unmerited
      - Nepotism
      - Incompetence
      - Political Leverage
    - Contractors Overestimate Capabilities
    - Lack of User Input
    - Lack of Project Leadership
  - Cyber Attack
    - Cyber Attack for Information
    - Cyber Attack for Terrorism
    - Cyber Attack for Financial Gain
  - Co-ordination
    - Unrealistic Expectations
    - Incompatible to Government Systems
    - Incomplete Project Proposal
    - Change in Scope
    - Co-ordination with Mutiple Contractors

2.2 Hierarchy of Sources

2.3 How Sources May Contribute to an Event

Once the risk events and potential sources were identified, the team began to associate the risk event with the sources that may contribute to its occurrence. As shown in figure 3, multiple sources can contribute to a risk event.

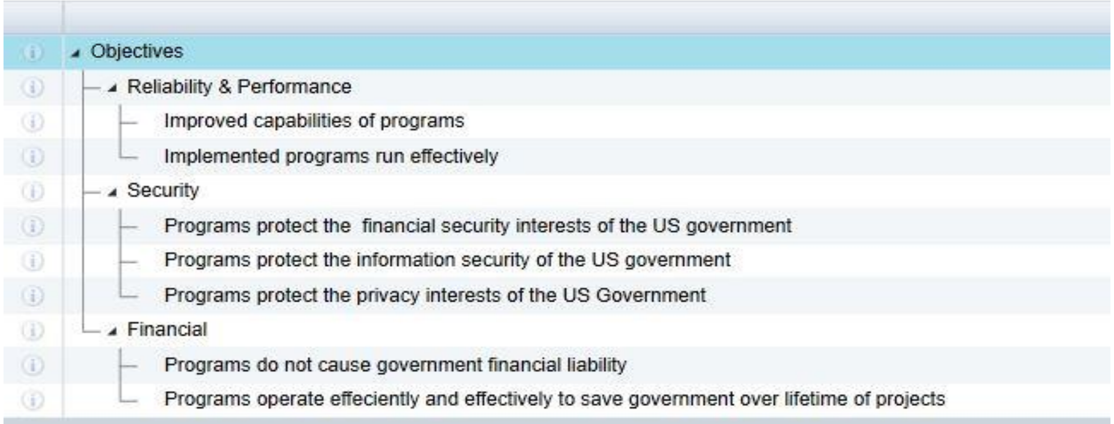


	Sources														
	Human							Cyber Attack			Co-ordination				
		Bids Approved Unmerited													
Events	Board Approval C	Nepotism	Incompetence	Political Lever	Contractors Over	Lack of User Inpu	Lack of Project Le	Cyber Attack for I	Cyber Attack for T	Cyber Attack for F	Unrealistic Expec	Incompatible to G	Incomplete Projec	Change in Scope	Co-ordination with
Cost Over Runs	□	☑	☑	☑	☑	□	☑	□	□	□	□	☑	☑	☑	☑
Cyber Security Breech	□	□	□	□	□	□	☑	□	□	□	□	☑	□	☑	☑
Ineffective Program Imple	□	□	□	□	□	□	☑	☑	☑	☑	□	☑	☑	□	☑
Degradation of Original P	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	□	□	□	□
Program Rollout Delays	□	□	□	□	☑	□	☑	□	□	□	☑	☑	☑	☑	☑
Tertiary Risks	□	□	☑	☑	□	☑	□	□	□	□	☑	☑	☑	□	☑
No Third Party Technolog	□	□	☑	☑	□	□	□	☑	☑	☑	□	□	☑	□	☑
Product Management Fai	□	□	□	□	☑	□	☑	☑	☑	☑	☑	□	☑	□	☑
Low Public Benefit	□	□	☑	☑	☑	□	□	□	□	□	□	☑	☑	☑	□
Obsolescing Skills	□	□	□	□	□	☑	□	□	□	□	□	☑	□	□	□

2.3 Vulnerabilities Grid

2.4 Identifying Objectives

In collaboration with Office of Management and Budget, we assigned a list of objectives based on the purpose and goals of upgrading government technology. These objectives are listed in a hierarchical format in the figure below.



- Objectives
  - Reliability & Performance
    - Improved capabilities of programs
    - Implemented programs run effectively
  - Security
    - Programs protect the financial security interests of the US government
    - Programs protect the information security of the US government
    - Programs protect the privacy interests of the US Government
  - Financial
    - Programs do not cause government financial liability
    - Programs operate effeciently and effectively to save government over lifetime of projects

2.4 Hierarchy of Objectives

3 Risk Measurement & Evaluation Process

With the use of the Riskion software, the team can ensure that its assessment is mathematically meaningful by deriving priorities through the use of aggregated judgements made by the people that are critical in the decision-making process for the consolidation of the contracts.

3.1 Participants and their Roles

- Ryan Moorman - Project Manager
- Qiao Wang - Assistant Project Manager
- Mick Mulvaney - Committee Oversight
- Jeanette Manfra - Cyber Security
- Bill Zielinski - General Service Admin
- David Powner - IT Management
- Margaret Weichert - Management and Budget

These participants were asked to evaluate each threat event, occurrence, and impact on objectives based on their individual judgements.

3.2 Measurement Methods

The Riskion software program is built upon the Analytical Hierarchy Process, which helps to reduce personal biases or imperfect judgements the participants might have, and translate them into ratio scale priorities through the use of eigenvectors. The following measurement methods were employed:

- Likelihood of Events: Measurement Methods used for Sources
    - Pairwise with Given Likelihood – this method allows for the team to specify the known or assumed likelihood of occurrence for one of the events that will be compared.
- Likelihood of Events: Measurement Method used for Events
    - Pairwise Comparisons – this method is used to derive ratio scale likelihoods for the relative importance of each source amongst each other within its assigned category.

    - Pairwise with Given Likelihood – this method allows for the team to specify the known or assumed likelihood of occurrence for one of the events that will be compared.
- Impact of Events: Measurement Method used for Objectives
    - Pairwise Comparisons – this method is used to derive ratio scale likelihoods for the relative importance of each source amongst each other within its assigned category.
- Impact of Events: Measurement Method used for Events
    - Pairwise Comparisons – this method is used to derive ratio scale likelihoods for the relative importance of each source amongst each other within its assigned category.

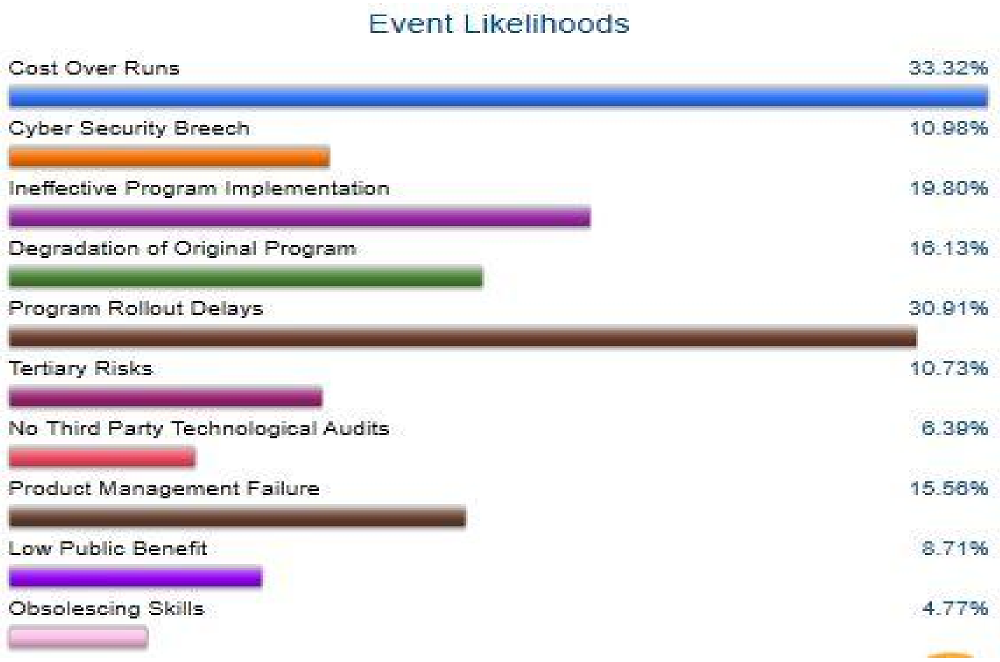
Once the measurement scales were established, all seven participants were asked to enter their independent judgements by providing a rating of the elements within the categories they were assigned based on areas of expertise and responsibility. These judgements were later synthesized for aggregated analysis.

4. Risk Analysis Synthesized Results

After our evaluations were complete our team reviewed Riskion’s “synthesized” results to review all of the data gathered and determine if there were any outliers. The following shows our results found using dynamic and performance sensitivity analysis.

4.1. Synthesis: Likelihood of Events and Sources

As seen in figure 4.1.1 below there are two events that would pose greatest threat the modernizing government technology program. The first being cost over runs associated with projects and the second being program roll out delays both of which are above 30% likelihood. Obsolescing skills pose the smallest threat to projects that can be rolled out through the act by having less than 5% likelihood of occurring.



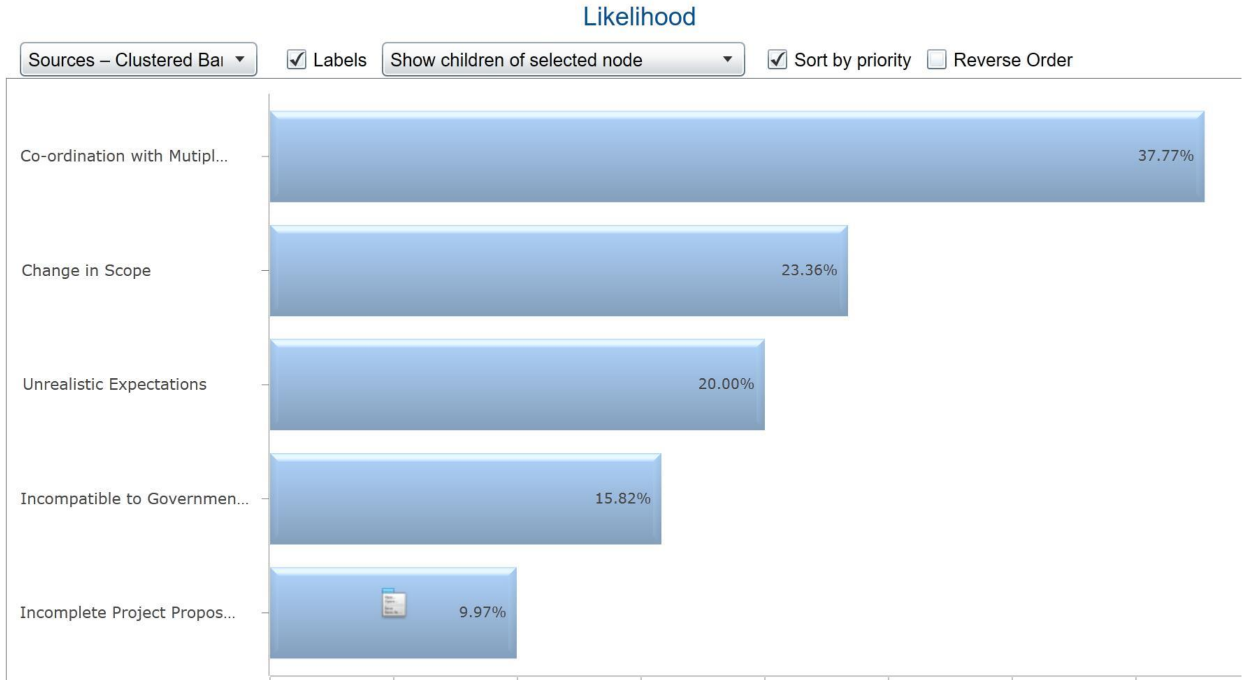
4.1.1 Synthesis: Impact of Events and Objectives

Additionally, Figure 4.1.2 indicates that sources relating to "Co-ordination with Multiple Contractors" category has significant overall priority than the other categories of threat sources, ranking at over 37%.

significantly higher likelihood than ..

.

with a likelihood exceeding 37%


Likelihood

Sources – Clustered Bar ▾ ☑ Labels Show children of selected node ▾ ☑ Sort by priority □ Reverse Order

Co-ordination with Mutipl... 37.77%
Change in Scope 23.36%
Unrealistic Expectations 20.00%
Incompatible to Governmen... 15.82%
Incomplete Project Propos... 9.97%

Figure 4.1.2

Additionally, the above is only with respect to the Co-Ordination Causes. See video: https://www.screencast.com/t/tGSmEM538 for the likelihood of all of the causes not just those due to Co-ordination.

When the team performed a Dynamic and Performance analyses (figures 4.1.3 & 4.1.4) to see to what degree these priority changes by shifting the level of importance of the sources, “Co-ordination with Multiple Contractors” still seems to outweigh the other categories in terms of priority.

The above is not correct. The dynamic is good to see 'movement' but not as a still screen capture. What it does show however is the likelihoods of the sources on the left and the resultant event likelihoods on the right

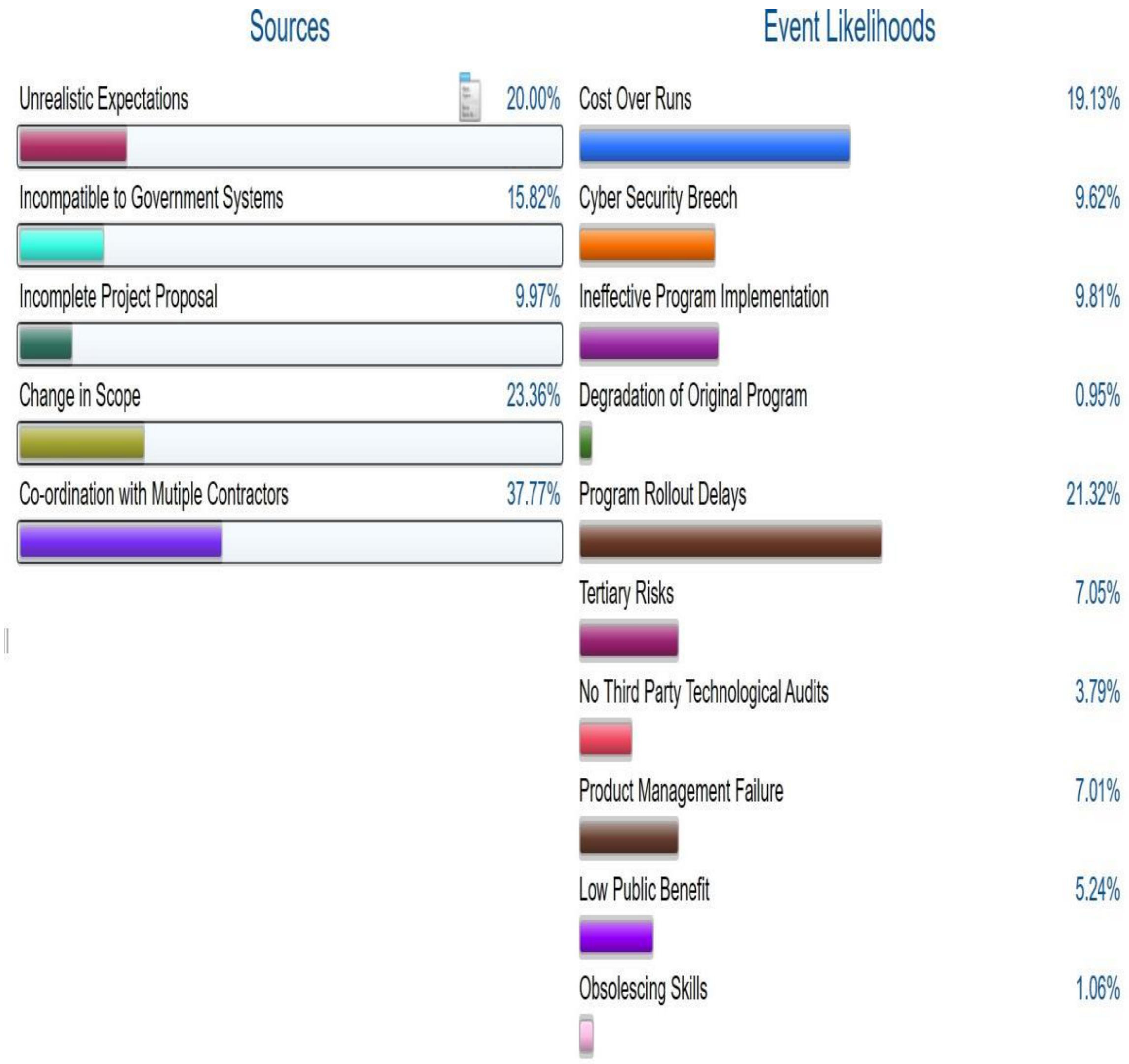
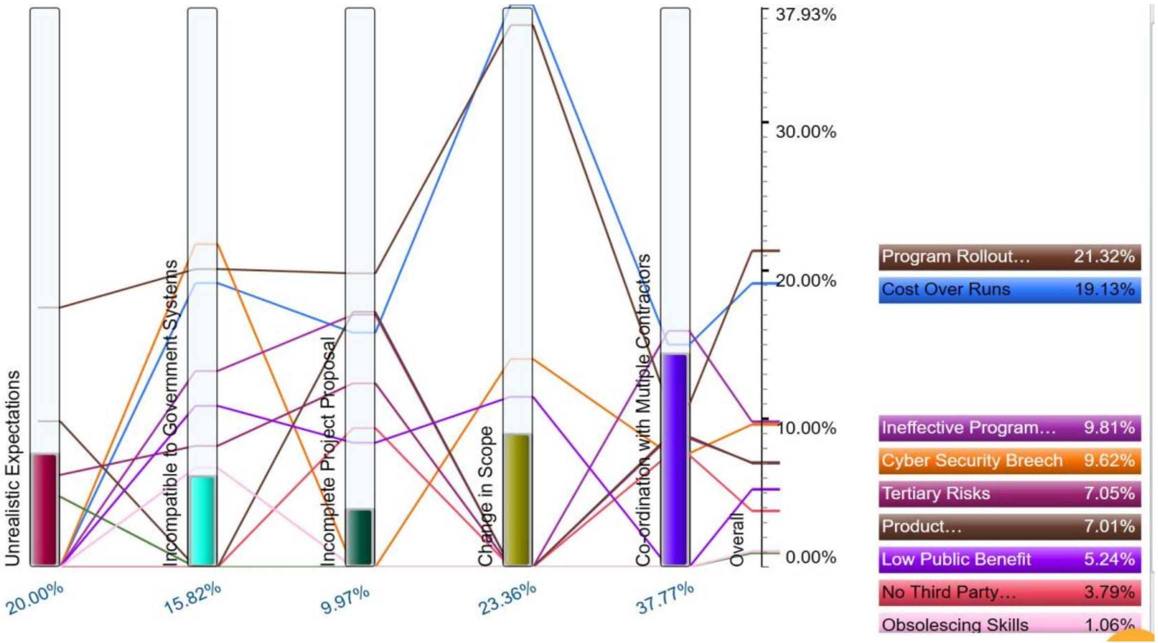


Figure 4.1.3

However, again, these are only with respect to Co-ordination causes. I don't think you need to show the sensitivities at all.

Write up a separate paragraph describing what is in Figure 4.1.4 -- that is, the likelihoods of the sources



However, these are also only with respect to the Co-ordination cluster of causes. Don't need to show or discuss in the paper.

Figure 4.1.4

4.2. Synthesis: Impact of Events

A synthesis of the objective importance and the event consequences on the objectives results in the impact on objectives, shown in Figure 4.2.1. (Figures should be capitalized).

While synthesizing the impact of events and objectives in comparion in figure 4.2.1, we found that there are a few events that have a much higher impact on objectives towards modernizing government technology. The first being tertiary risks and the second being product management failure which are both above 50% threat levels which can be seen in figure 5. When digging deeper into each objective it can be seen that these are the most consistently seen as risks that can have financial, security and reliability & performance implications. In contrast, the degradation of the original program was synthesized to have the least perceived impact at only 5% and can be attributed to the small risk it carries to the projects' objectives.

Awkward. Reword.

You can use the Figure shown here (show components) to make your point about the impacts are mostly on Reliability and Performance. https://www.screencast.com/t/tGSmEM538

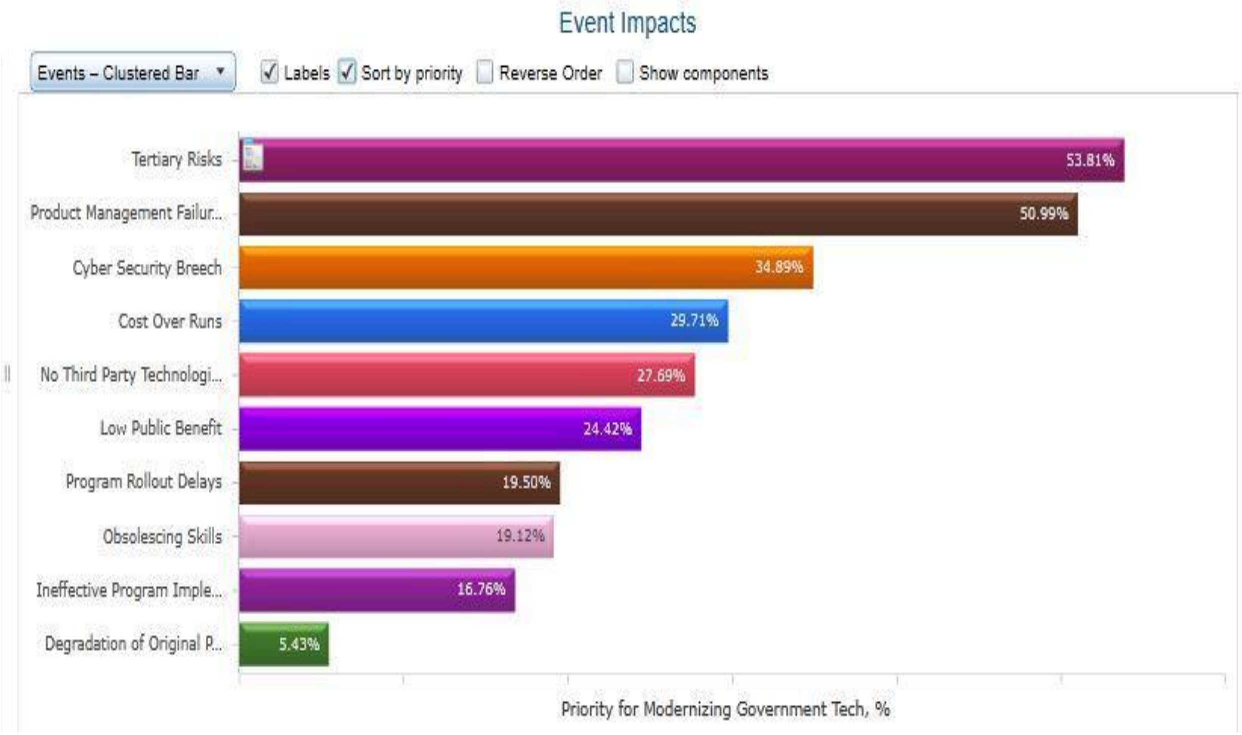
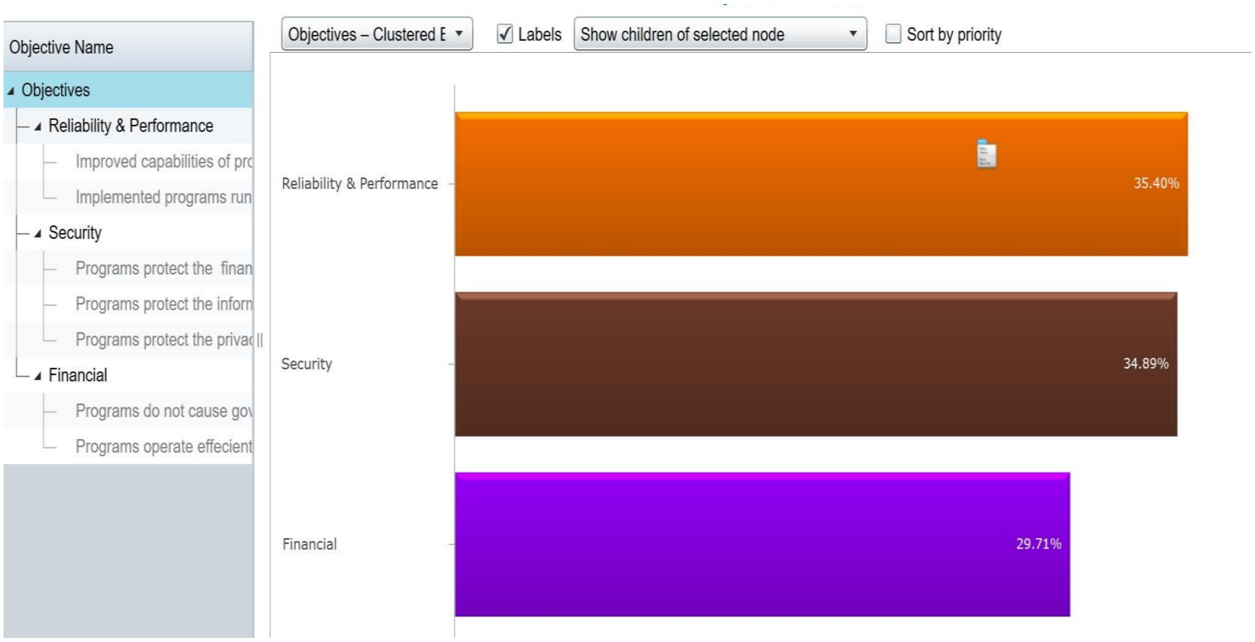

Events – Clustered Bar ▾ ☑ Labels ☑ Sort by priority □ Reverse Order □ Show components

Figure 4.2.1 Event Impacts

Additionally, figure 4.2.2 shows "Reliability & Performance" and "Security" are rated at the highest overall priority of with respect to objectives of 35%. "Financial" is 29%.

Figure 4.2.2 shows the relative importance of the thee main objectives.

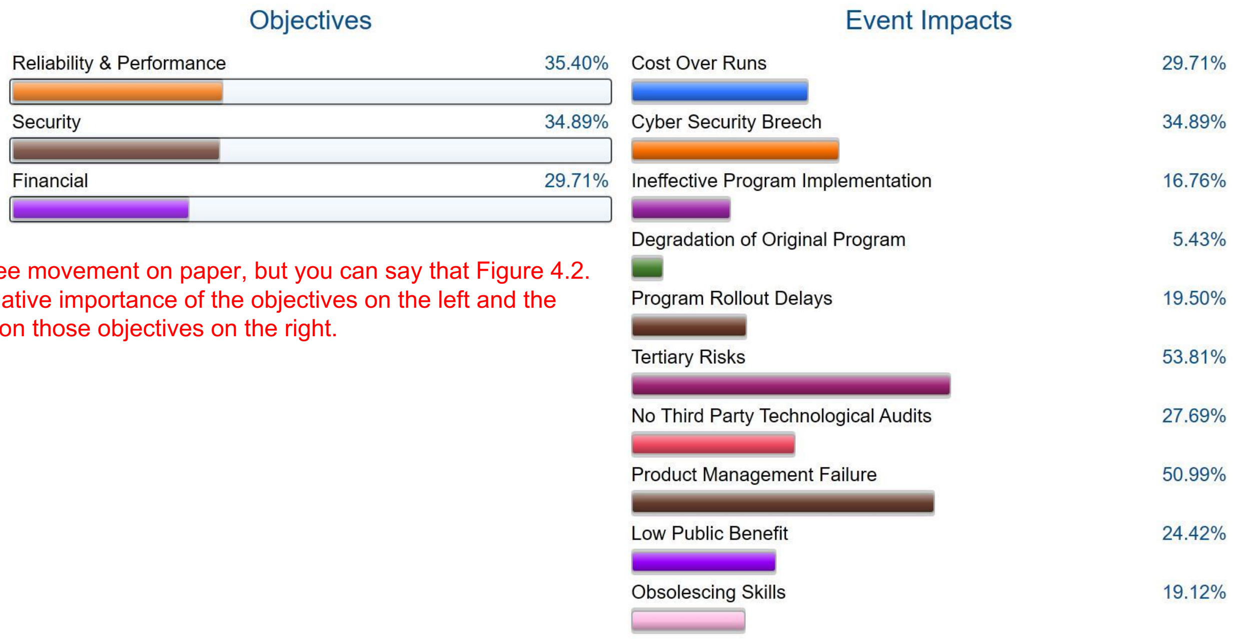

Objectives – Clustered E ▾ ☑ Labels Show children of selected node ▾ □ Sort by priority

Objective Name

- Objectives
  - Reliability & Performance
    - Improved capabilities of pro
    - Implemented programs run
  - Security
    - Programs protect the finan
    - Programs protect the inform
    - Programs protect the privac
  - Financial
    - Programs do not cause gov
    - Programs operate effecient

Figure 4.2.2

In order to understand how fluid the priorities are WRT each objective, the team performed both Dynamic (Figure 4.2.3) and Performance (Figure 4.2.4) Sensitivity Analyses to see what impact any change would have on the priorities of the event.



Reader can't see movement on paper, but you can say that Figure 4.2.3 shows the relative importance of the objectives on the left and the Event Impacts on those objectives on the right.

Figure 4.2.3

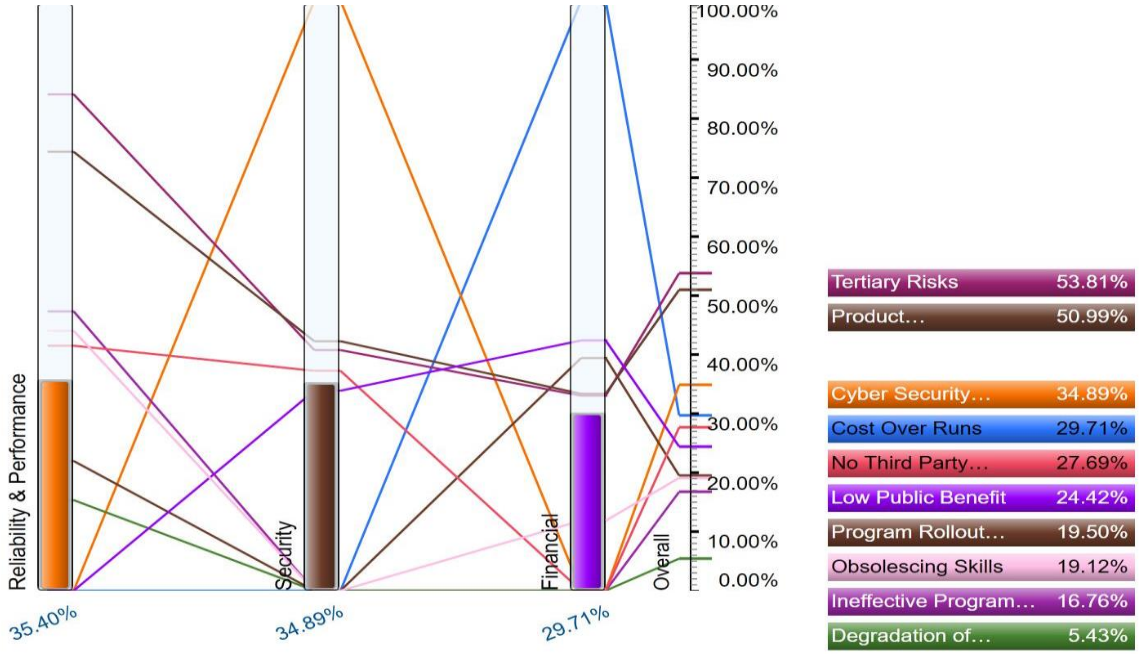


Figure 4.2.4

If you include this, you should describe it --- Shows the relative importance of the top level objectives as bars and the consequences of each of the events on these top level objectives.

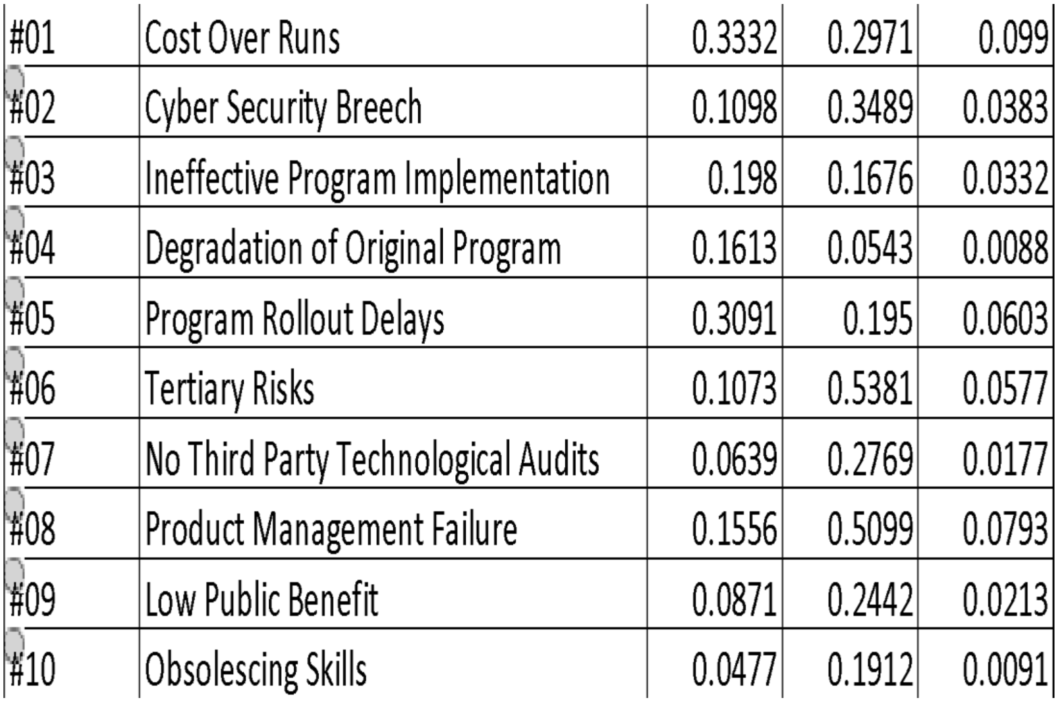
5. Risk Review and Landscape

According to Figure 5.1 – 5.8, when looking at the impacts of events and the likelihood of events by themselves it would appear as if the modernizing government technology act would be a grave undertaking and carry more risk than reward. However, when looking at the heat risk heat map a different picture is shown. As can be seen in the overall risk map when impact and likelihood are evaluated for an event the threat appears to be less evident than before. The importance of the risk map becomes evident when we look to apply controls as we can use warmer areas of likelihood and impact to reduce risk. Our overall risk as calculated without controls was 42%. When simulated our value was closer to 32% without controls.

How can you say this when you don't know what the 'reward' would be?

This doesn't make sense. Before what? Why 'threat'? What is shown are likelihoods and impacts and threat

Why not show the risk results? The chart below has no headings. You also need to explain simulation and why it is necessary.



#01	Cost Over Runs	0.3332	0.2971	0.099
#02	Cyber Security Breech	0.1098	0.3489	0.0383
#03	Ineffective Program Implementation	0.198	0.1676	0.0332
#04	Degradation of Original Program	0.1613	0.0543	0.0088
#05	Program Rollout Delays	0.3091	0.195	0.0603
#06	Tertiary Risks	0.1073	0.5381	0.0577
#07	No Third Party Technological Audits	0.0639	0.2769	0.0177
#08	Product Management Failure	0.1556	0.5099	0.0793
#09	Low Public Benefit	0.0871	0.2442	0.0213
#10	Obsolescing Skills	0.0477	0.1912	0.0091

5.1 Overall Risk without Control

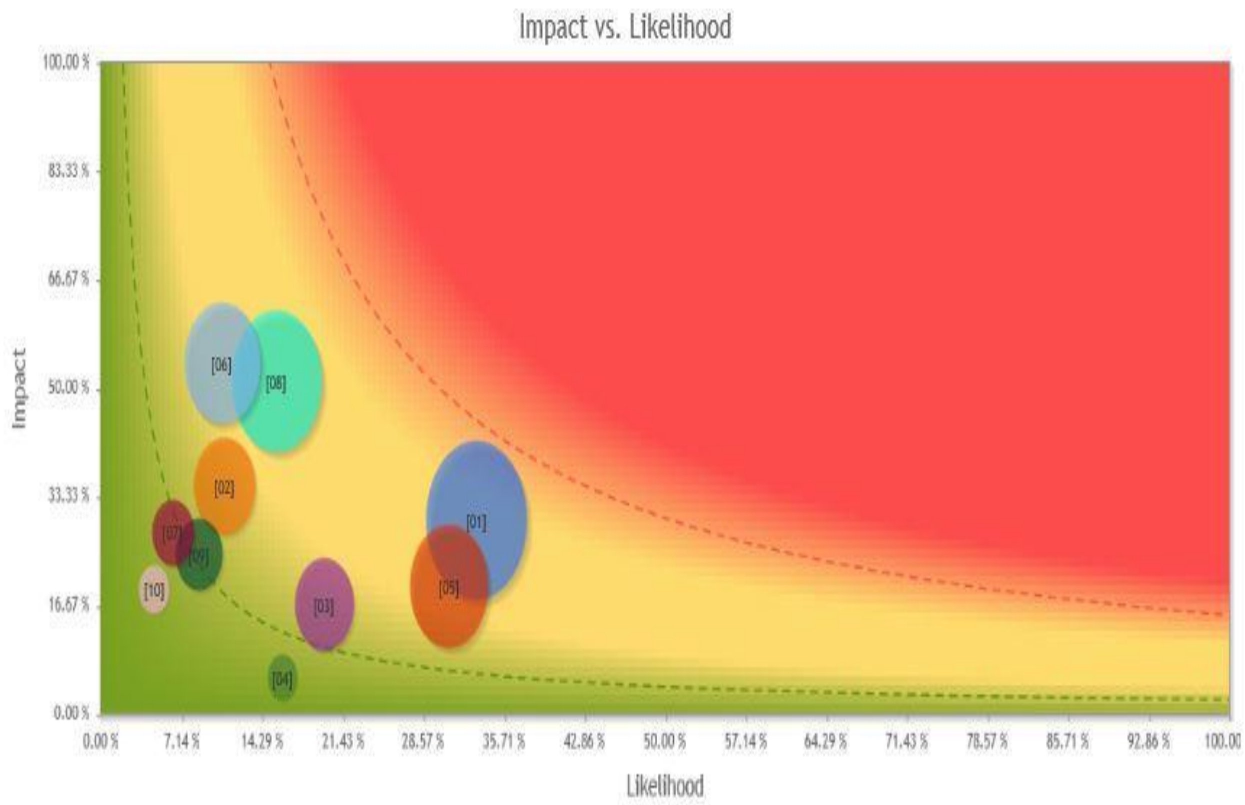
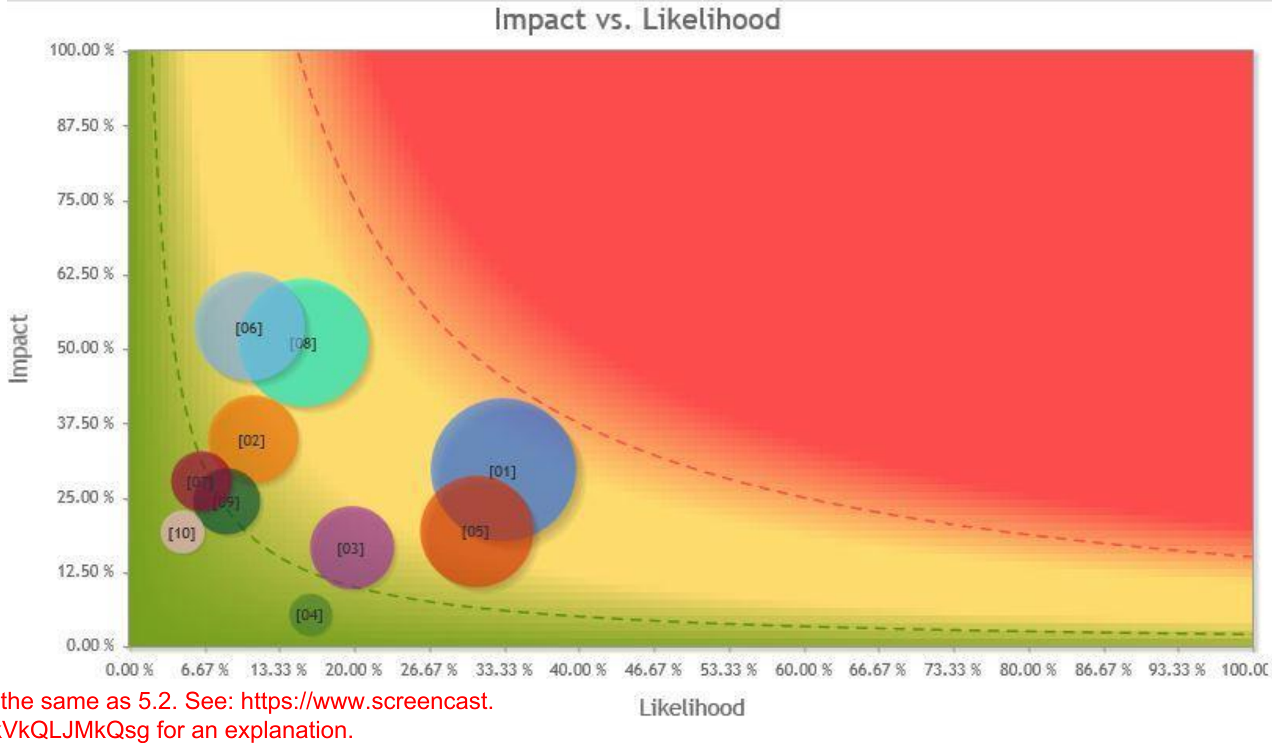
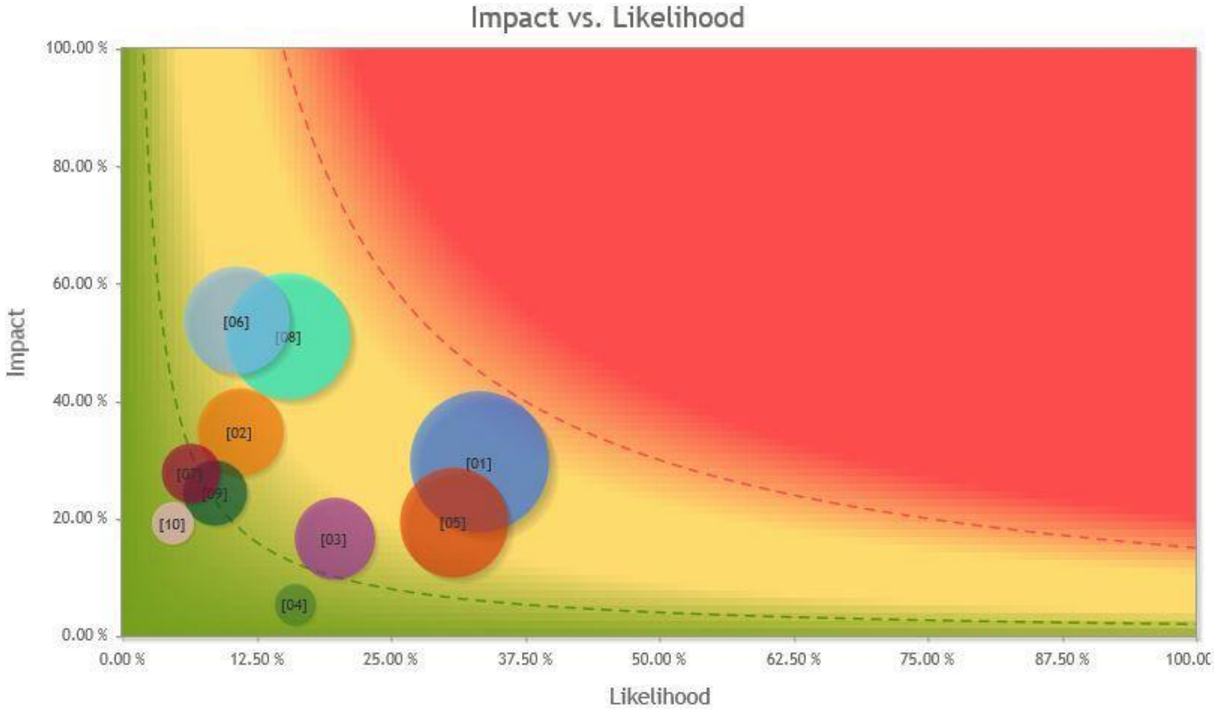


Figure 5.2 Overall Risk Map



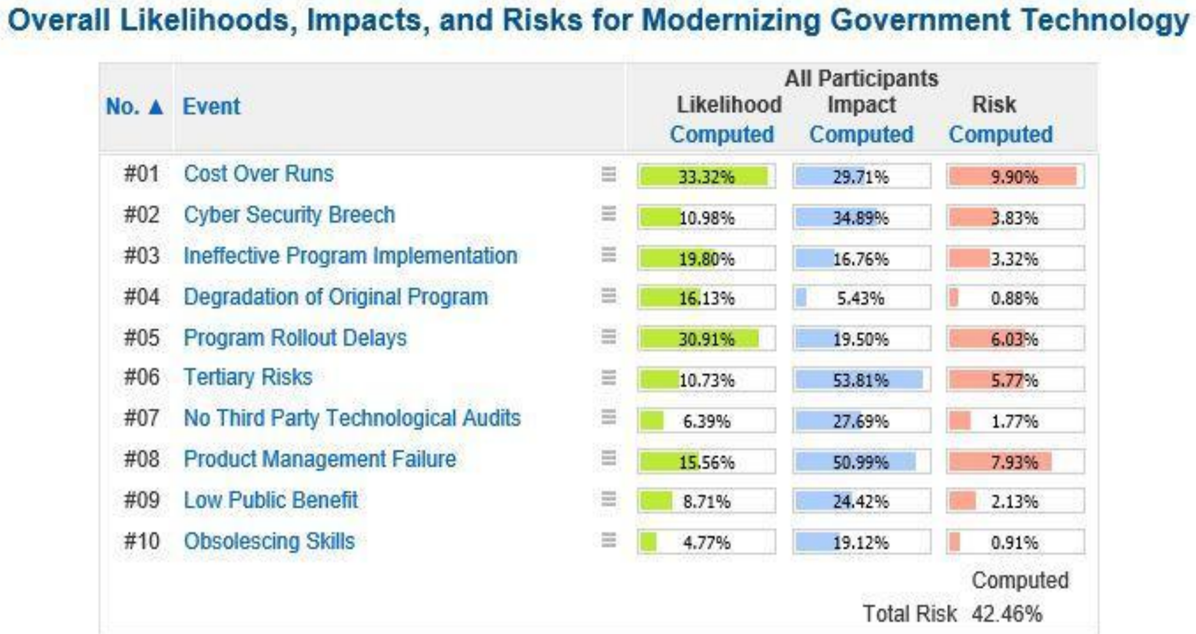
This is the same as 5.2. See: https://www.screencast.com/t/kVkQLJMkQsg for an explanation.

Figure 5.3 From Sources



Similarly for this.... see: https://www.screencast.com/t/YHztN25hwhV

Figure 5.4 To Objectives



Overall Likelihoods, Impacts, and Risks for Modernizing Government Technology

		All Participants		
No. ▲	Event	Likelihood Computed	Impact Computed	Risk Computed
#01	Cost Over Runs	33.32%	29.71%	9.90%
#02	Cyber Security Breech	10.98%	34.89%	3.83%
#03	Ineffective Program Implementation	19.80%	16.76%	3.32%
#04	Degradation of Original Program	16.13%	5.43%	0.88%
#05	Program Rollout Delays	30.91%	19.50%	6.03%
#06	Tertiary Risks	10.73%	53.81%	5.77%
#07	No Third Party Technological Audits	6.39%	27.69%	1.77%
#08	Product Management Failure	15.56%	50.99%	7.93%
#09	Low Public Benefit	8.71%	24.42%	2.13%
#10	Obsolescing Skills	4.77%	19.12%	0.91%
			Total Risk	Computed 42.46%

Why are you showing computed instead of simulated? Why not show $ amounts in addition to or instead of percentages?

Figure 5.5 Overall Risk Without Control

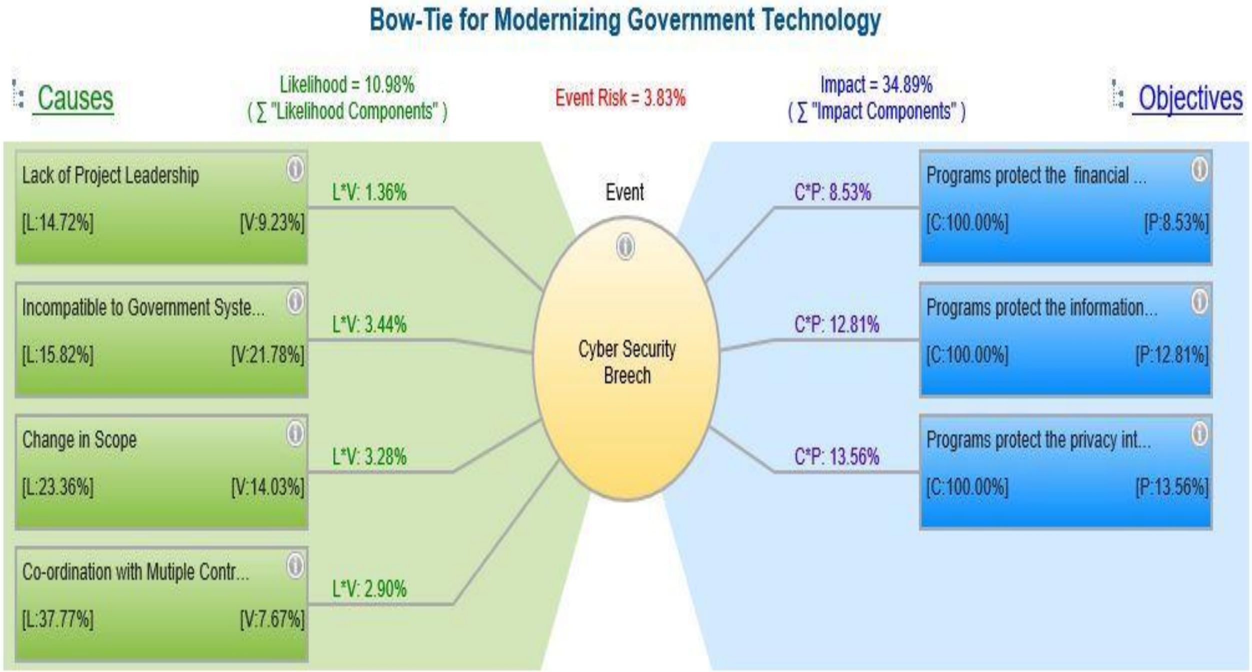
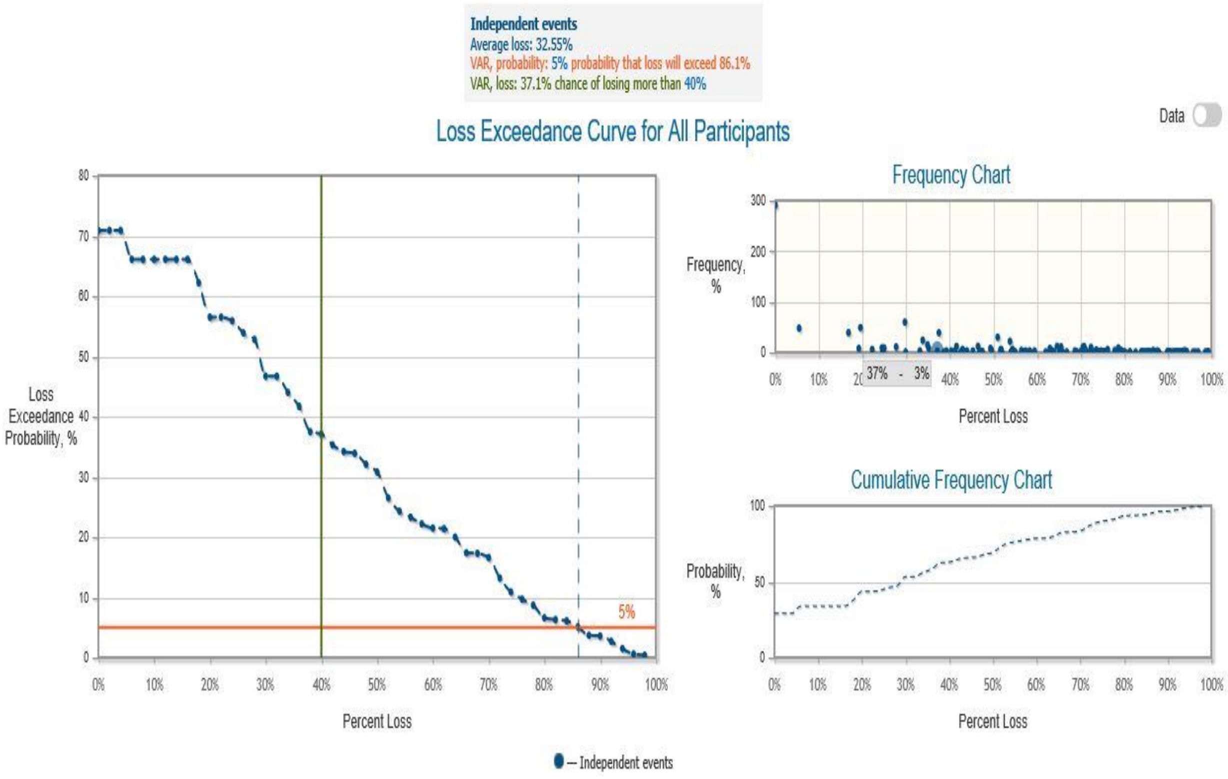
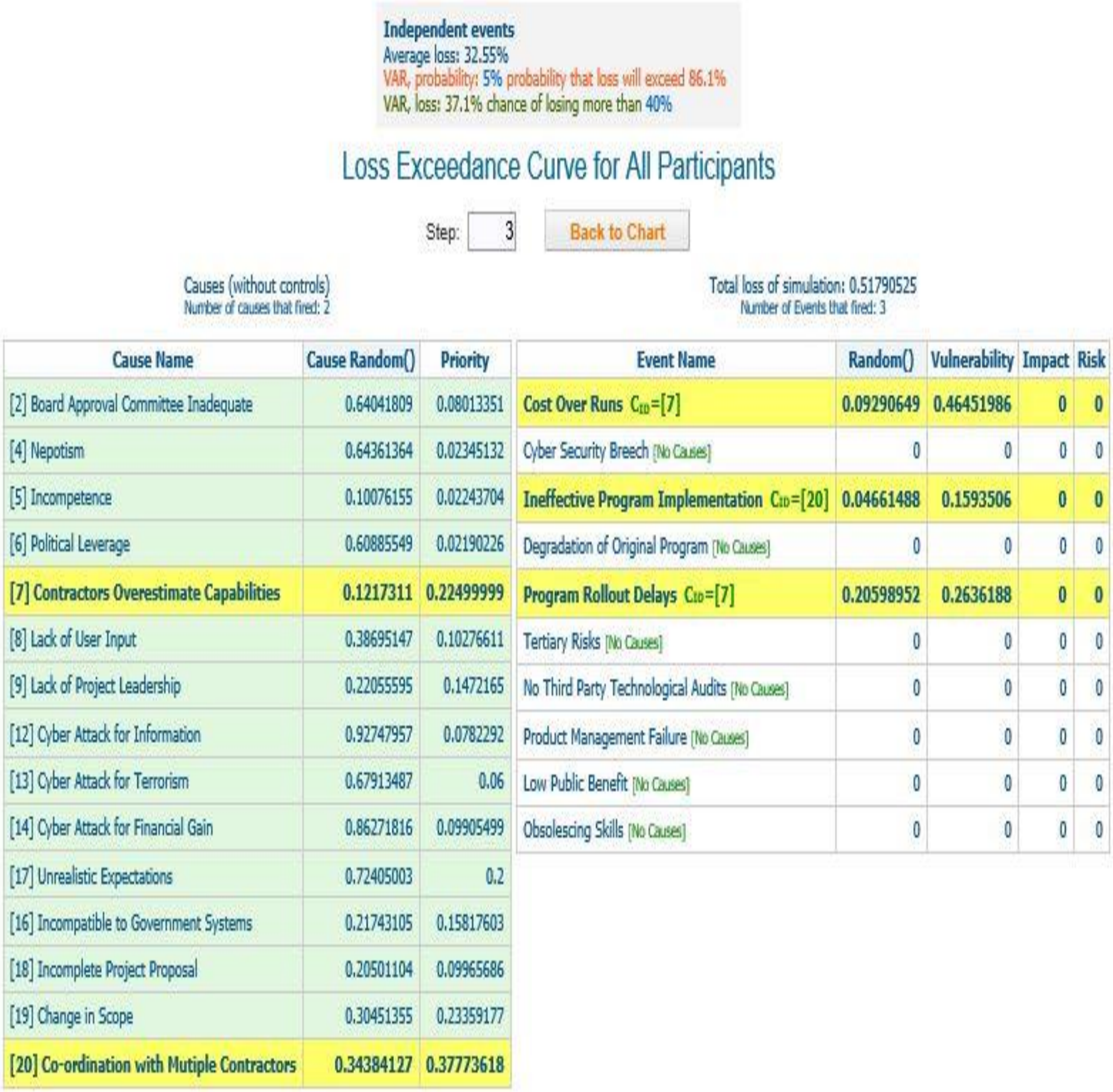


Figure 5.6 Example of Bow Tie Diagram



Independent events
Average loss: 32.55%
VAR, probability: 5% probability that loss will exceed 86.1%
VAR, loss: 37.1% chance of losing more than 40%

Figure 5.7



Independent events
Average loss: 32.55%
VAR, probability: 5% probability that loss will exceed 86.1%
VAR, loss: 37.1% chance of losing more than 40%

Loss Exceedance Curve for All Participants

Causes (without controls)
Number of causes that fired: 2

Cause Name	Cause Random()	Priority
[2] Board Approval Committee Inadequate	0.64041809	0.08013351
[4] Nepotism	0.64361364	0.02345132
[5] Incompetence	0.10076155	0.02243704
[6] Political Leverage	0.60885549	0.02190226
[7] Contractors Overestimate Capabilities	**0.1217311**	**0.22499999**
[8] Lack of User Input	0.38695147	0.10276611
[9] Lack of Project Leadership	0.22055595	0.1472165
[12] Cyber Attack for Information	0.92747957	0.0782292
[13] Cyber Attack for Terrorism	0.67913487	0.06
[14] Cyber Attack for Financial Gain	0.86271816	0.09905499
[17] Unrealistic Expectations	0.72405003	0.2
[16] Incompatible to Government Systems	0.21743105	0.15817603
[18] Incomplete Project Proposal	0.20501104	0.09965686
[19] Change in Scope	0.30451355	0.23359177
[20] Co-ordination with Mutiple Contractors	**0.34384127**	**0.37773618**

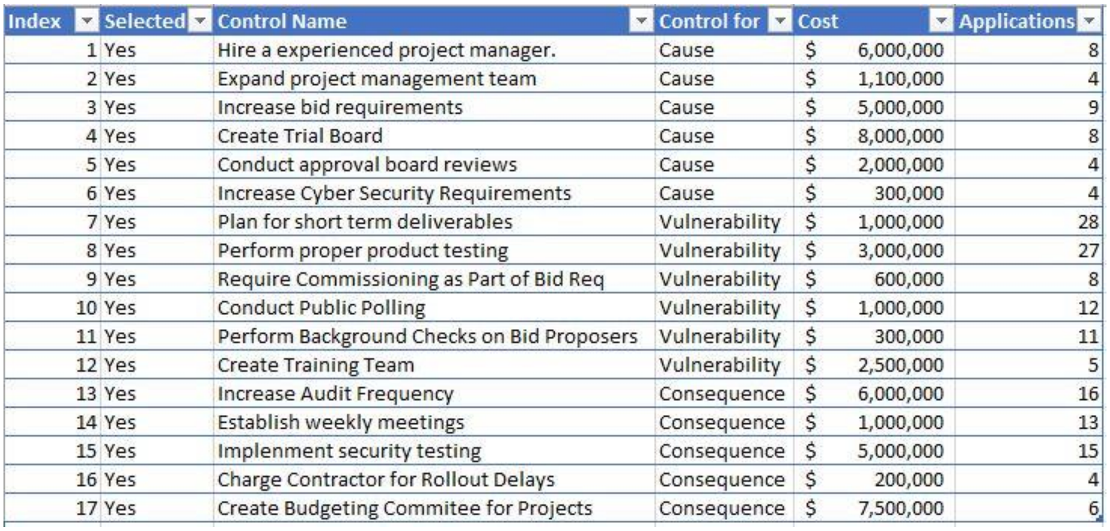
Total loss of simulation: 0.51790525
Number of Events that fired: 3

Event Name	Random()	Vulnerability	Impact	Risk
Cost Over Runs C_{ID}=[7]	**0.09290649**	**0.46451986**	**0**	**0**
Cyber Security Breech [No Causes]	0	0	0	0
Ineffective Program Implementation C_{ID}=[20]	**0.04661488**	**0.1593506**	**0**	**0**
Degradation of Original Program [No Causes]	0	0	0	0
Program Rollout Delays C_{ID}=[7]	**0.20598952**	**0.2636188**	**0**	**0**
Tertiary Risks [No Causes]	0	0	0	0
No Third Party Technological Audits [No Causes]	0	0	0	0
Product Management Failure [No Causes]	0	0	0	0
Low Public Benefit [No Causes]	0	0	0	0
Obsolescing Skills [No Causes]	0	0	0	0

Figure 5.8

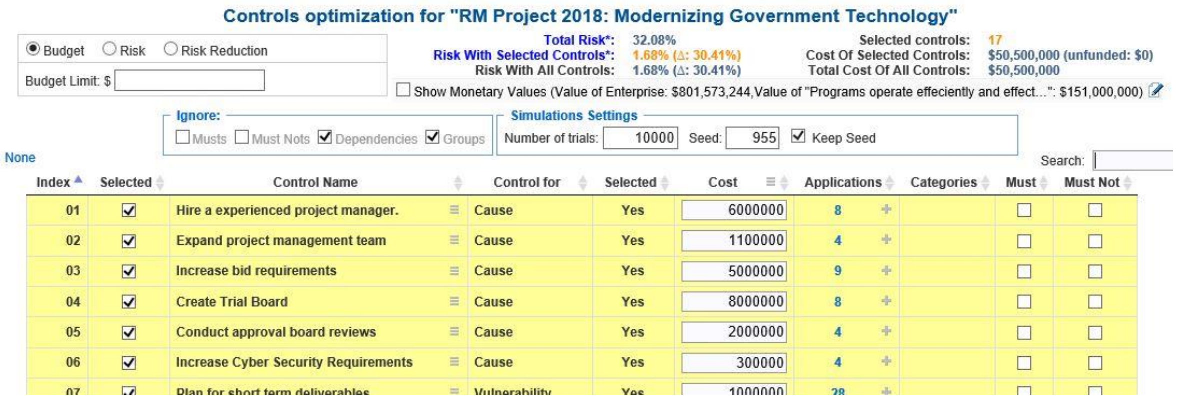
6 Implementation of Risk Controls

Once our team identified potential risk events, we proceeded to determine seventeen controls that, when applied to the causes, vulnerabilities, or consequences could help to reduce or avoid any potential loss as shown in figure 6.1 – 6.3. These controls when applied to sources, vulnerabilities or consequences could potentially reduce the losses associated with applications they are associated with. Potential controls were brainstormed and implemented into the riskion software.



Index	Selected	Control Name	Control for	Cost	Applications
1	Yes	Hire a experienced project manager.	Cause	$ 6,000,000	8
2	Yes	Expand project management team	Cause	$ 1,100,000	4
3	Yes	Increase bid requirements	Cause	$ 5,000,000	9
4	Yes	Create Trial Board	Cause	$ 8,000,000	8
5	Yes	Conduct approval board reviews	Cause	$ 2,000,000	4
6	Yes	Increase Cyber Security Requirements	Cause	$ 300,000	4
7	Yes	Plan for short term deliverables	Vulnerability	$ 1,000,000	28
8	Yes	Perform proper product testing	Vulnerability	$ 3,000,000	27
9	Yes	Require Commissioning as Part of Bid Req	Vulnerability	$ 600,000	8
10	Yes	Conduct Public Polling	Vulnerability	$ 1,000,000	12
11	Yes	Perform Background Checks on Bid Proposers	Vulnerability	$ 300,000	11
12	Yes	Create Training Team	Vulnerability	$ 2,500,000	5
13	Yes	Increase Audit Frequency	Consequence	$ 6,000,000	16
14	Yes	Establish weekly meetings	Consequence	$ 1,000,000	13
15	Yes	Implenment security testing	Consequence	$ 5,000,000	15
16	Yes	Charge Contractor for Rollout Delays	Consequence	$ 200,000	4
17	Yes	Create Budgeting Commitee for Projects	Consequence	$ 7,500,000	6

Figure 6.1



Controls optimization for "RM Project 2018: Modernizing Government Technology"

● Budget ○ Risk ○ Risk Reduction

Budget Limit: $

Total Risk*: 32.08%
Risk With Selected Controls*: 1.68% (Δ: 30.41%)
Risk With All Controls: 1.68% (Δ: 30.41%)

Selected controls: 17
Cost Of Selected Controls: $50,500,000 (unfunded: $0)
Total Cost Of All Controls: $50,500,000

□ Show Monetary Values (Value of Enterprise: $801,573,244,Value of "Programs operate effeciently and effect...": $151,000,000)

Ignore: □ Musts □ Must Nots ☑ Dependencies ☑ Groups

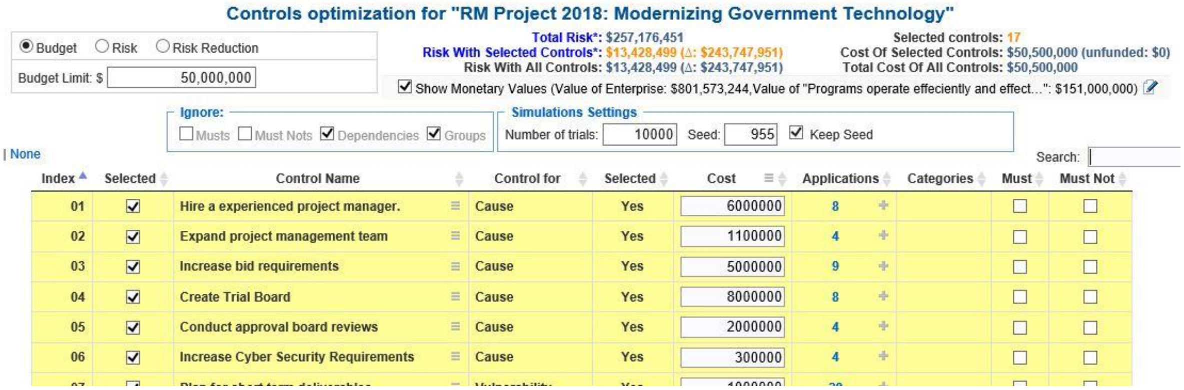
Simulations Settings: Number of trials: 10000 Seed: 955 ☑ Keep Seed

None

Search:

Index	Selected	Control Name	Control for	Selected	Cost	Applications	Categories	Must	Must Not
01	☑	Hire a experienced project manager.	Cause	Yes	6000000	8		□	□
02	☑	Expand project management team	Cause	Yes	1100000	4		□	□
03	☑	Increase bid requirements	Cause	Yes	5000000	9		□	□
04	☑	Create Trial Board	Cause	Yes	8000000	8		□	□
05	☑	Conduct approval board reviews	Cause	Yes	2000000	4		□	□
06	☑	Increase Cyber Security Requirements	Cause	Yes	300000	4		□	□
07	☑	Plan for short term deliverables	Vulnerability	Yes	1000000	28		□	□

Figure 6.2



Controls optimization for "RM Project 2018: Modernizing Government Technology"

● Budget ○ Risk ○ Risk Reduction

Budget Limit: $ 50,000,000

Total Risk*: $257,176,451
Risk With Selected Controls*: $13,428,499 (Δ: $243,747,951)
Risk With All Controls: $13,428,499 (Δ: $243,747,951)

Selected controls: 17
Cost Of Selected Controls: $50,500,000 (unfunded: $0)
Total Cost Of All Controls: $50,500,000

☑ Show Monetary Values (Value of Enterprise: $801,573,244,Value of "Programs operate effeciently and effect...": $151,000,000)

Ignore: □ Musts □ Must Nots ☑ Dependencies ☑ Groups

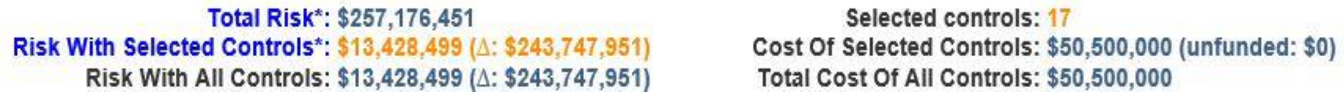
Simulations Settings: Number of trials: 10000 Seed: 955 ☑ Keep Seed

| None

Search:

Index	Selected	Control Name	Control for	Selected	Cost	Applications	Categories	Must	Must Not
01	☑	Hire a experienced project manager.	Cause	Yes	6000000	8		□	□
02	☑	Expand project management team	Cause	Yes	1100000	4		□	□
03	☑	Increase bid requirements	Cause	Yes	5000000	9		□	□
04	☑	Create Trial Board	Cause	Yes	8000000	8		□	□
05	☑	Conduct approval board reviews	Cause	Yes	2000000	4		□	□
06	☑	Increase Cyber Security Requirements	Cause	Yes	300000	4		□	□
07	☑	Plan for short term deliverables	Vulnerability	Yes	1000000	[illegible]		□	□

Figure 6.3

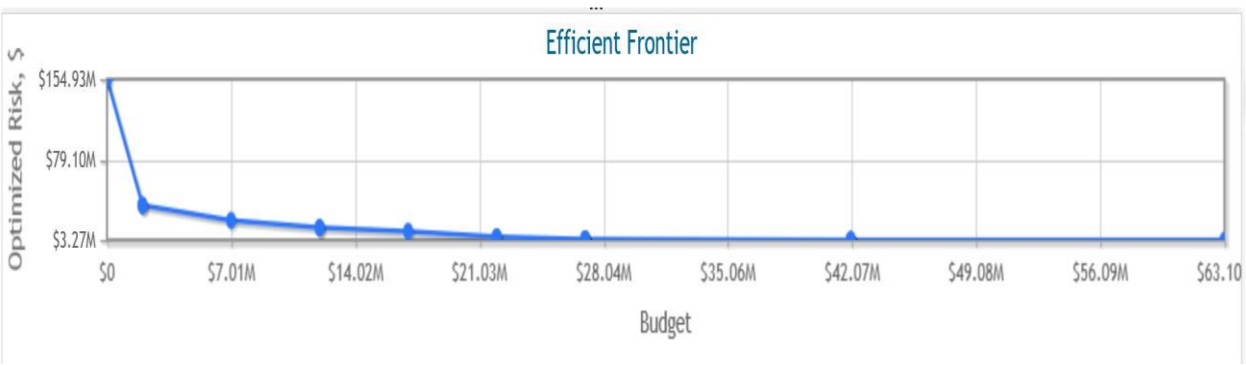


Total Risk*: $257,176,451
Risk With Selected Controls*: $13,428,499 (Δ: $243,747,951)
Risk With All Controls: $13,428,499 (Δ: $243,747,951)

Selected controls: 17
Cost Of Selected Controls: $50,500,000 (unfunded: $0)
Total Cost Of All Controls: $50,500,000

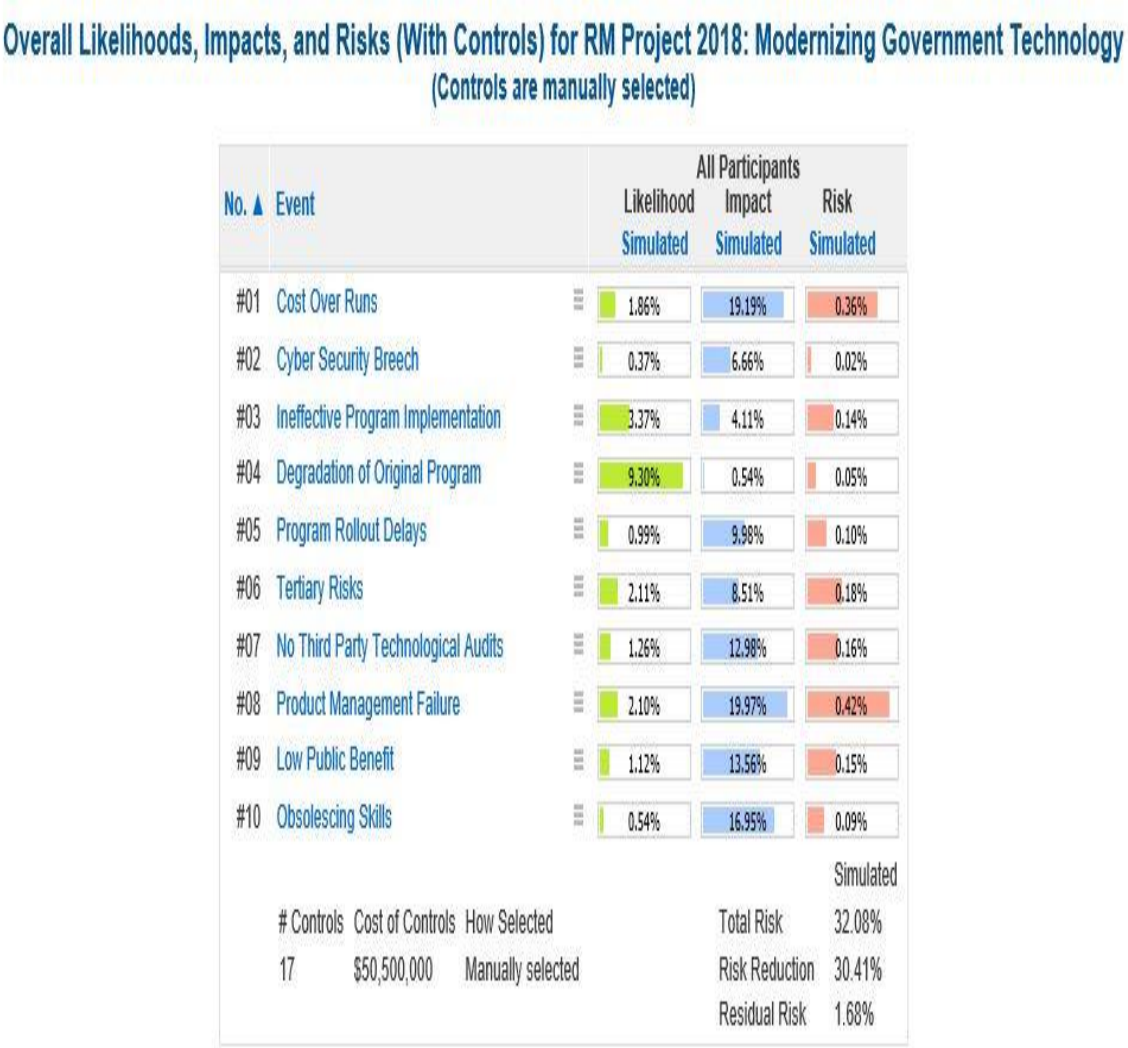
Figure 6.4 Total Risk Reduction

As shown in figure 6.5, the team also analyzed the efficient frontier curve to help decide which optimal controls to fund at each budget level as the more money spent, the less risks the team would face.



7 Risk with Controls

As figure 7.1 shown, according to the selection and implementation of the six controls as above, the team's overall risk will be reduced by 30.41%, down from 32.08%. Given the established risk appetite of 32%, a reduction of 30% is very well within an acceptable range of risk the team is willing to undertake. However, the cost of controls is $50 million which is costly in comparison to the overall budget of the TMF's $800 million. Dependent on the acceptable risk appetite a balance of controls cost and acceptable risk could be found somewhere in the middle of not being as costly but with more risk involved.



Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018: Modernizing Government Technology
(Controls are manually selected)

No. ▲	Event	All Participants Likelihood Simulated	 Impact Simulated	 Risk Simulated
#01	Cost Over Runs	1.86%	19.19%	0.36%
#02	Cyber Security Breech	0.37%	6.66%	0.02%
#03	Ineffective Program Implementation	3.37%	4.11%	0.14%
#04	Degradation of Original Program	9.30%	0.54%	0.05%
#05	Program Rollout Delays	0.99%	9.98%	0.10%
#06	Tertiary Risks	2.11%	8.51%	0.18%
#07	No Third Party Technological Audits	1.26%	12.98%	0.16%
#08	Product Management Failure	2.10%	19.97%	0.42%
#09	Low Public Benefit	1.12%	13.56%	0.15%
#10	Obsolescing Skills	0.54%	16.95%	0.09%

# Controls	Cost of Controls	How Selected
17	$50,500,000	Manually selected

	Simulated
Total Risk	32.08%
Risk Reduction	30.41%
Residual Risk	1.68%

8 Conclusion

The highest risk our team faces was without a doubt “Cost Over Run” which is very plausible considering that government projects very frequently run over budget for various reasons. Through our risk analysis using the riskion software, our team was able to identify primary sources of those cost over runs and also establish plans to mitigate or minimize the effects of threat events. Our team also identified options to minimize the effect on Modernizing Government Technology projects that have had a threat event happen to them. Based on how much risk would like be minimalized up to $50 million dollars worth can be spent to drastically reduce risk involved. Our team is confident that moving forward projects through the MGT pipeline can proceed forward in a manner that will benefit the public, be cost effective and be secure.