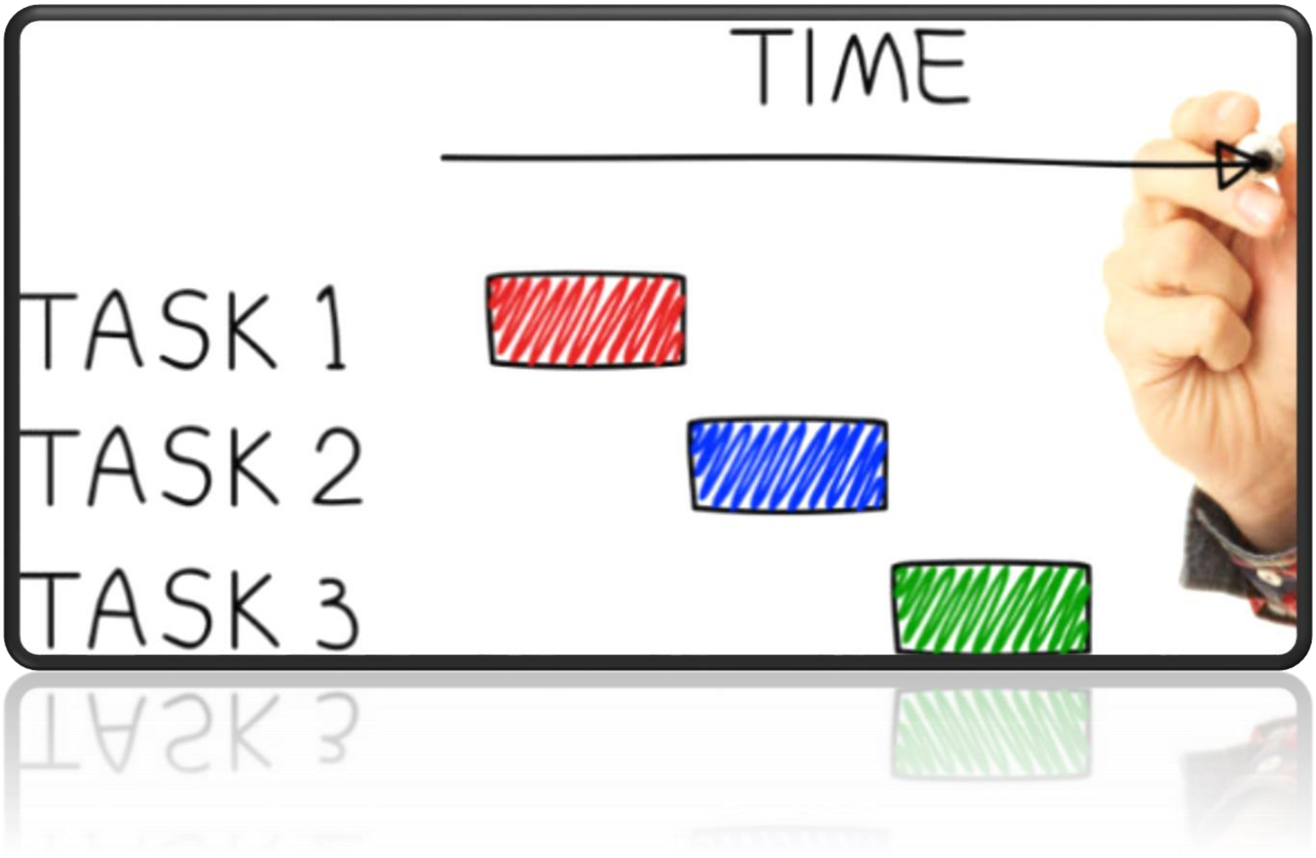
QuickTask Risk Management Framework:

Assessing Risk in use and upgrade of military application to the cloud.



DNSC 6254 Risk Management: Fall 2018

Mary Huggins and Lisa Henry

Table of Contents

1. Introduction

1.1. Background

The Department of Defense (DoD) is conducting a security control assessment of the QuickTask application located at Fort Bragg, NC during the period of 09/5/2018-09/30/2018. The overall risk will be determined by assessing the implementation of the assigned security controls baseline with consideration of the impact of any vulnerabilities if exploited and the likelihood of occurrence. All aggravating or mitigating factors will be considered as part of this assessment.

The objective of this assessment is to evaluate compliance with DoD requirements and regulations. Specifically, NIST SP 800-53 and DodI 8510.01. The risk assessment is being conducted with the intent to give this application the Authority to Operate (ATO) and thus enabling the DoD to move the application to the Cloud if needed in the future. This assessment will identify security controls that are needed.

QuickTask is an IT solution which is interoperable with several other required task systems within the Department of Defense. It is not a public facing application and is restricted by use of access cards, pin numbers, and network access. QuickTask is used to store and process Personally Identifiable Information (PII) but does not create new PII.

The scope of the assessment includes the entirety of the physical boundary, processes, and devices included within the QuickTask authorization boundaries.

1.2 Analysis

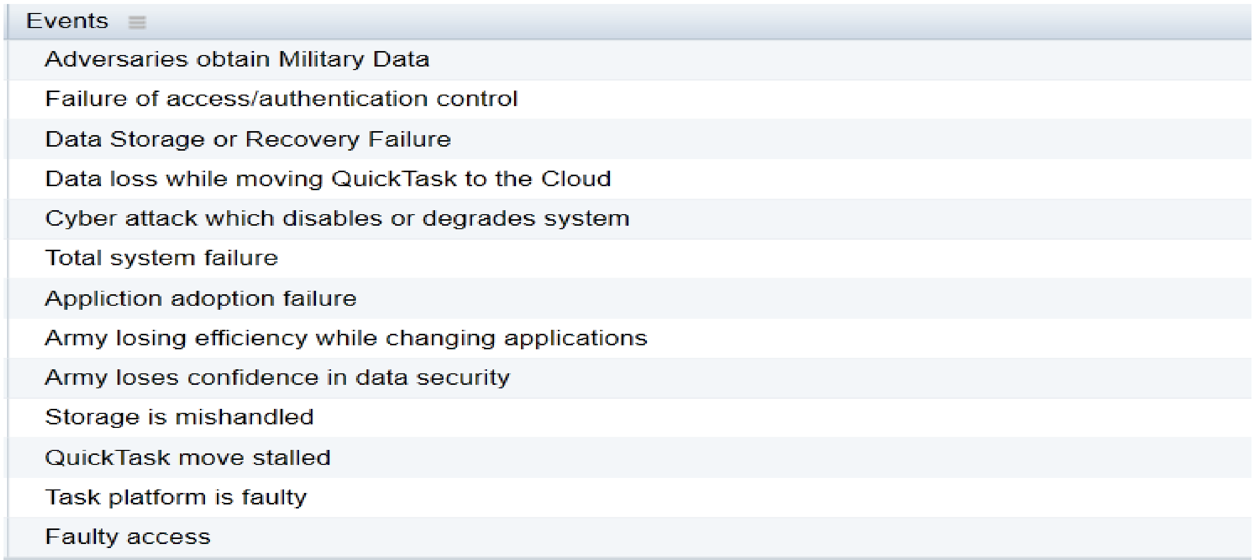
To complete QuickTask Risk Management Assessment, we used Riskion Application to:

- identify events
- structure, measure and synthesis the likelihood of events
- structure, measure and synthesis the impact of events
- identify and evaluate risk
- perform controls

2. Project Structure

2.1 Identifying Risk Events

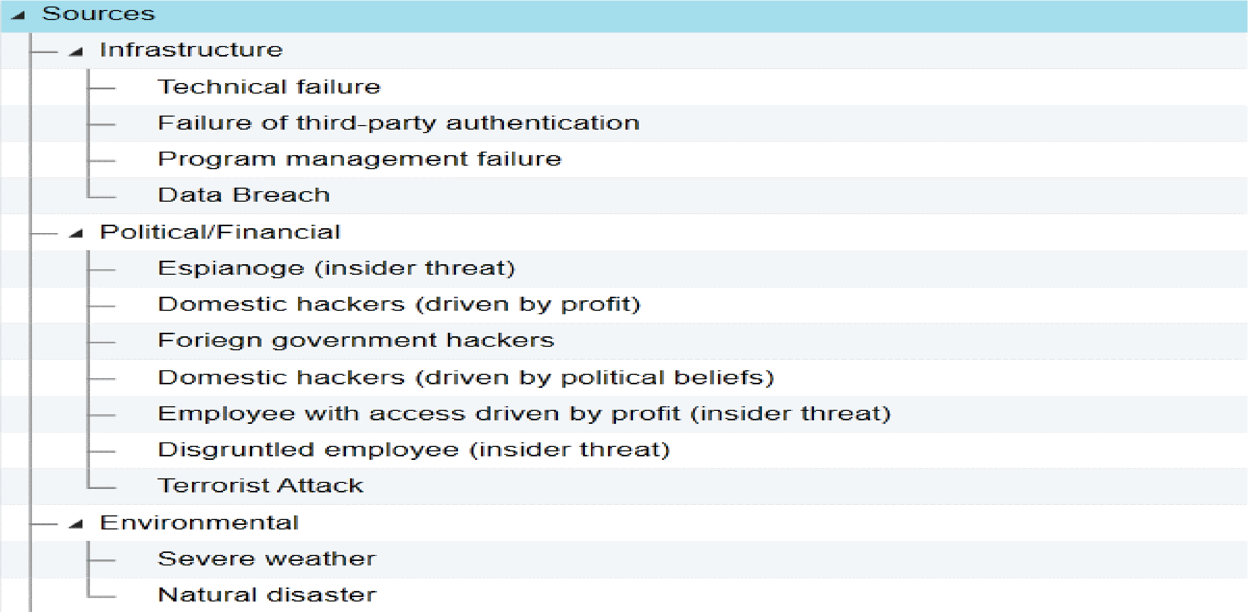
The first step in this project was to meet and interview AWS Cloud Services, IT professionals from the DC community, and review a real-world RMF Security Control Assessment (SCA). In addition, DoDI 8510.01, NIST SP 800-53 rev 4, and CNSSI 1253 Version 2 were reviewed. The QuickTask team read through the report details of the Army Knowledge Online real-world assessment (outdated). From these artifacts, the QuickTask team identified 13 common risk events associated with the adoption, general usage, and movement to cloud service which are faced by DoD applications.



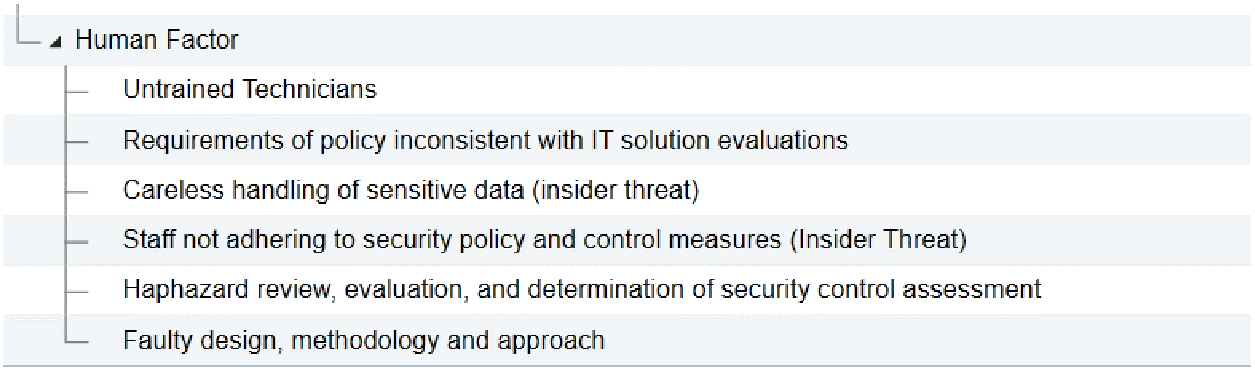
Events
Adversaries obtain Military Data
Failure of access/authentication control
Data Storage or Recovery Failure
Data loss while moving QuickTask to the Cloud
Cyber attack which disables or degrades system
Total system failure
Appliction adoption failure
Army losing efficiency while changing applications
Army loses confidence in data security
Storage is mishandled
QuickTask move stalled
Task platform is faulty
Faulty access

2.2 Identifying Risk Sources

After identifying the events, the QuickTask team worked backwards using logic to find the obvious sources and to divide them into four groups: Infrastructure, Political/Financial, Environmental, and Human.



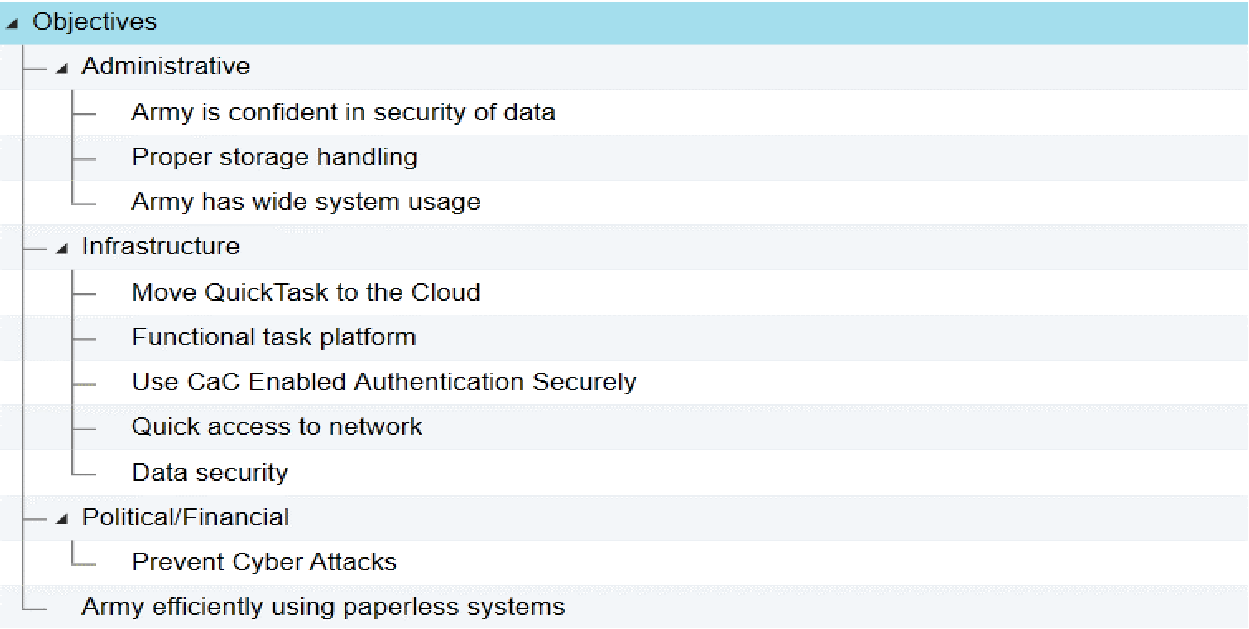
- Sources
  - Infrastructure
    - Technical failure
    - Failure of third-party authentication
    - Program management failure
    - Data Breach
  - Political/Financial
    - Espianoge (insider threat)
    - Domestic hackers (driven by profit)
    - Foriegn government hackers
    - Domestic hackers (driven by political beliefs)
    - Employee with access driven by profit (insider threat)
    - Disgruntled employee (insider threat)
    - Terrorist Attack
  - Environmental
    - Severe weather
    - Natural disaster



- Human Factor
  - Untrained Technicians
  - Requirements of policy inconsistent with IT solution evaluations
  - Careless handling of sensitive data (insider threat)
  - Staff not adhering to security policy and control measures (Insider Threat)
  - Haphazard review, evaluation, and determination of security control assessment
  - Faulty design, methodology and approach

2.3 Identifying Objectives

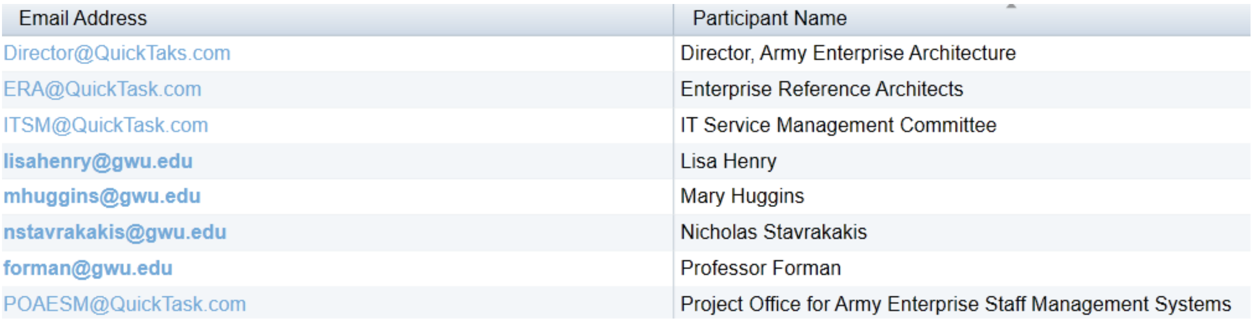
To identify objectives, we considered what needed to happen to have the Quick Task application be a success. Objectives were the discussed among the team and categorized into three groups: Administrative, Infrastructure, and Political/Financial.



- Objectives
  - Administrative
    - Army is confident in security of data
    - Proper storage handling
    - Army has wide system usage
  - Infrastructure
    - Move QuickTask to the Cloud
    - Functional task platform
    - Use CaC Enabled Authentication Securely
    - Quick access to network
    - Data security
  - Political/Financial
    - Prevent Cyber Attacks
  - Army efficiently using paperless systems

2.4 Participant Roles

The QuickTask team was composed of 8 individuals. Two quality assurance professionals (Nicholas Stavrakakis and Professor Forman), the technical architect, service management committee, and the project managers. Most of these participants were in one way or another involved in developing and implementing the QuickTask Risk Assessment. Decision makers are listed below.

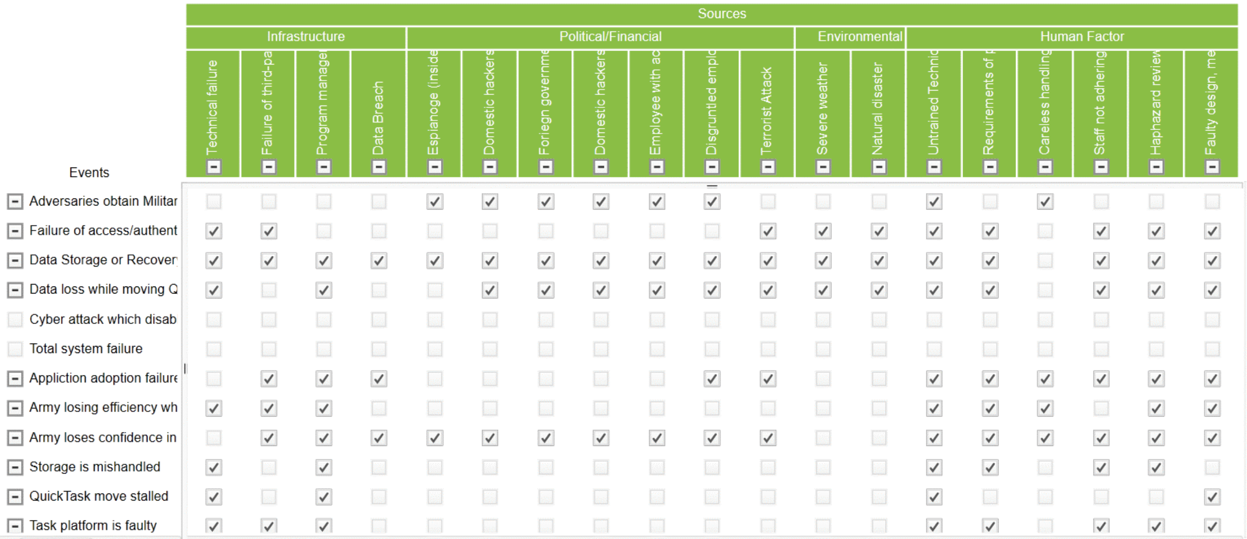


Email Address	Participant Name
Director@QuickTaks.com	Director, Army Enterprise Architecture
ERA@QuickTask.com	Enterprise Reference Architects
ITSM@QuickTask.com	IT Service Management Committee
lisahenry@gwu.edu	Lisa Henry
mhuggins@gwu.edu	Mary Huggins
nstavrakakis@gwu.edu	Nicholas Stavrakakis
forman@gwu.edu	Professor Forman
POAESM@QuickTask.com	Project Office for Army Enterprise Staff Management Systems

3. Events and Source Mapping

3.1 Likelihood of Events

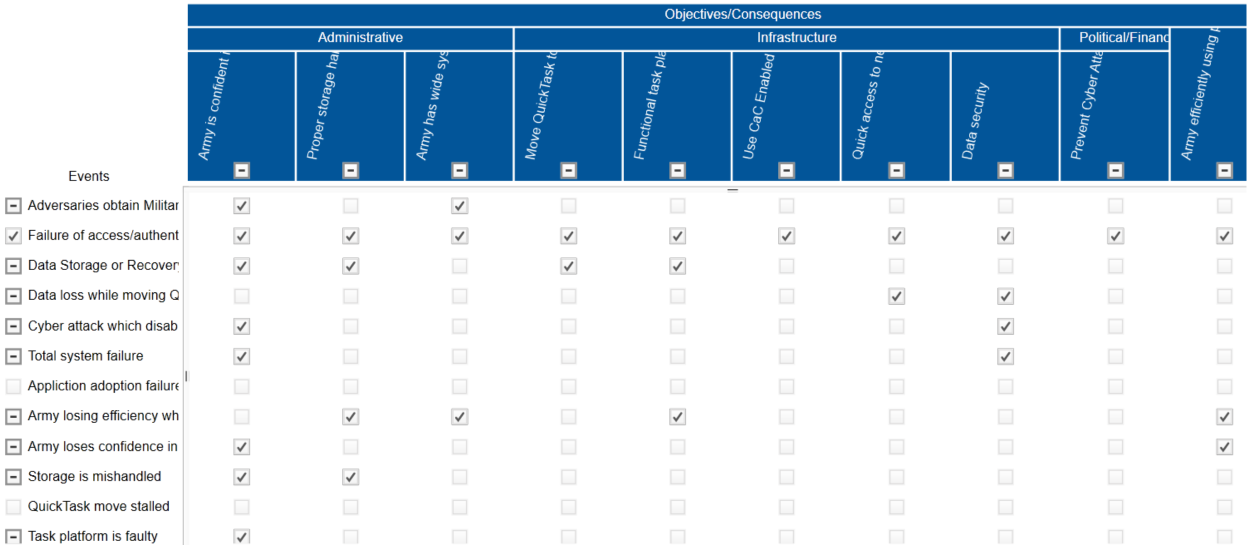
Riskion ties events and sources together by providing a data grid where both can be matched appropriately. Using Riskion's visual brainstorming tool, the events and likelihoods were paired. Relationships were determined by analyzing sources and events. The Vulnerabilities grid below depicts sources and its relationships with events.



	Sources																		
	Infrastructure				Political/Financial							Environmental		Human Factor					
Events	Technical failure	Failure of third-pa	Program manage	Data Breach	Espianoge (inside	Domestic hackers	Foriegn governme	Domestic hackers	Employee with ac	Disgruntled emplo	Terrorist Attack	Severe weather	Natural disaster	Untrained Technic	Requirements of p	Careless handling	Staff not adhering	Haphazard review	Faulty design, me
Adversaries obtain Militar	□	□	□	□	☑	☑	☑	☑	☑	☑	□	□	□	☑	□	☑	□	□	□
Failure of access/authent	☑	☑	□	□	□	□	□	□	□	□	☑	☑	☑	☑	☑	□	☑	☑	☑
Data Storage or Recover	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	☑	☑	☑
Data loss while moving Q	☑	□	☑	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	☑	☑	☑
Cyber attack which disab	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Total system failure	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Appliction adoption failure	□	☑	☑	☑	□	□	□	□	□	☑	☑	□	□	☑	☑	☑	☑	☑	☑
Army losing efficiency wh	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	☑	☑	☑	□	☑	☑
Army loses confidence in	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□	☑	☑	☑	☑	☑	☑
Storage is mishandled	☑	□	☑	□	□	□	□	□	□	□	□	□	□	☑	☑	□	☑	☑	□
QuickTask move stalled	☑	□	☑	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	☑
Task platform is faulty	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	☑	☑	□	☑	☑	☑

3.2 Impact of Events

Similar to the Vulnerabilities grid, the Consequence grid depicts objectives/consequences and their relationship with events. For example, one event, Failure of third party authentication shows a relationship with all nine objectives, whereas the event, Adversaries obtain military data only shows relationships with two objectives. These relationships were determined during subjective conversations and by using judgement.

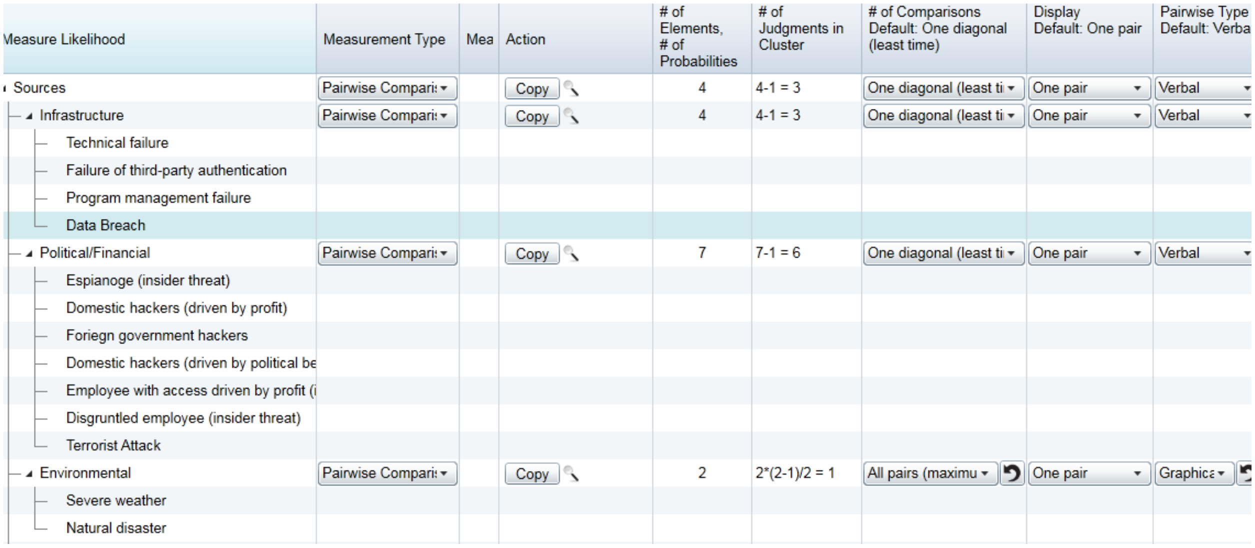


	Objectives/Consequences									
	Administrative			Infrastructure					Political/Financ	
Events	Army is confident ⊟	Proper storage ha ⊟	Army has wide sys ⊟	Move QuickTask to ⊟	Functional task pla ⊟	Use CaC Enabled ⊟	Quick access to ne ⊟	Data security ⊟	Prevent Cyber Atta ⊟	Army efficiently using ⊟
⊟ Adversaries obtain Militar	☑	□	☑	□	□	□	□	□	□	□
☑ Failure of access/authent	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
⊟ Data Storage or Recover	☑	☑	□	☑	☑	□	□	□	□	□
⊟ Data loss while moving Q	□	□	□	□	□	□	☑	☑	□	□
⊟ Cyber attack which disab	☑	□	□	□	□	□	□	☑	□	□
⊟ Total system failure	☑	□	□	□	□	□	□	☑	□	□
□ Appliction adoption failure	□	□	□	□	□	□	□	□	□	□
⊟ Army losing efficiency wh	□	☑	☑	□	☑	□	□	□	□	☑
⊟ Army loses confidence in	☑	□	□	□	□	□	□	□	□	☑
⊟ Storage is mishandled	☑	☑	□	□	□	□	□	□	□	□
□ QuickTask move stalled	□	□	□	□	□	□	□	□	□	□
⊟ Task platform is faulty	☑	□	□	□	□	□	□	□	□	□

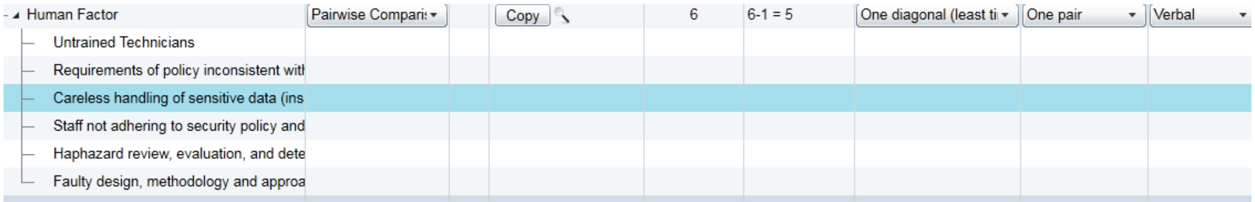
4. Risk Measurement Method

4.1 Likelihood of Events for Sources

Next we focused on measurement and data synthesis. The events for sources were categorized into Infrastructure, Political/Financial, Environmental, and Human. Grouping these items helped keep the project organized and to identify controls. We measured the likelihood of events by measuring the likelihood of sources/ threats/ vulnerabilities and measuring the likelihood of events given sources. Pairwise was used for both. Pairwise Comparison "is any process of comparing entities in pairs to judge which entity is preferred, or has a greater amount of some quantitative property, or whether or not the two entities are identical."



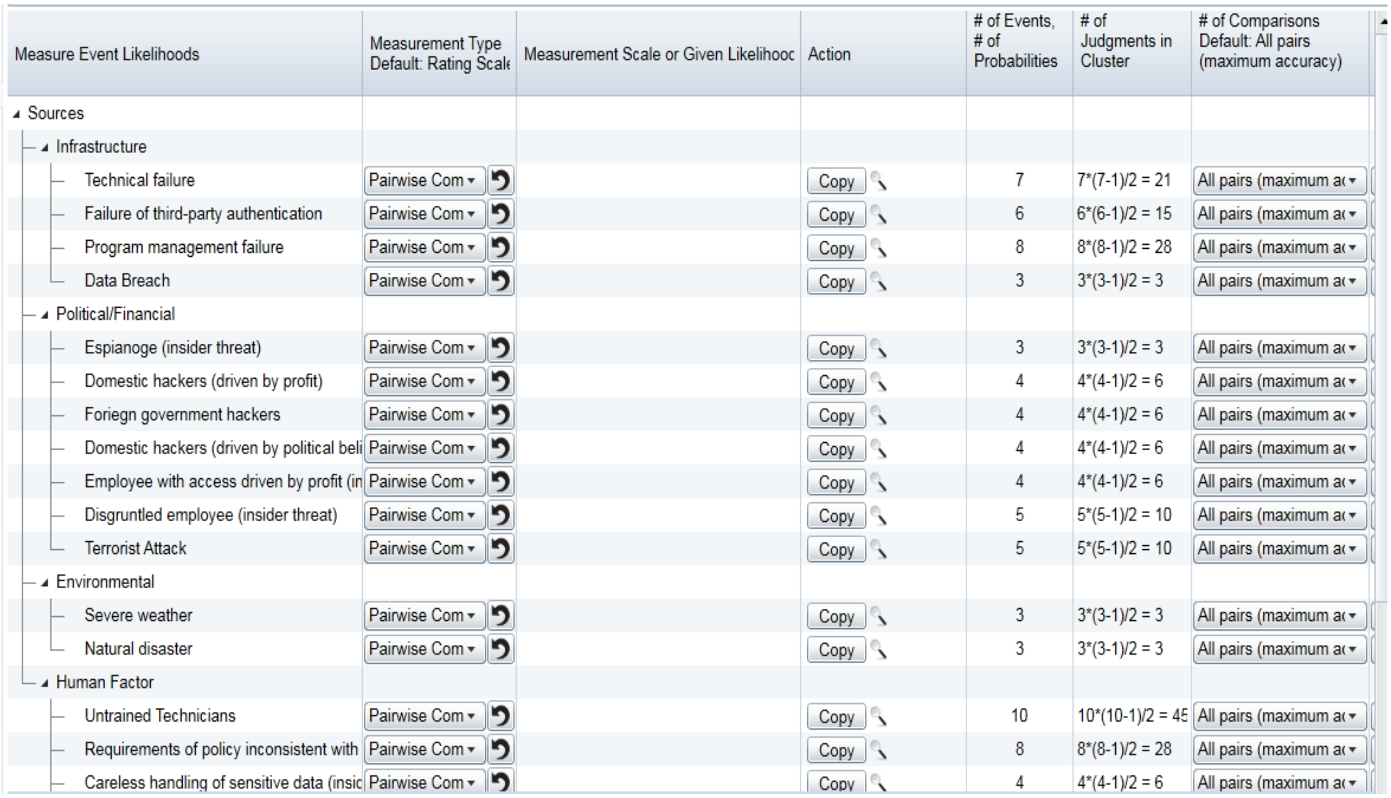
Measure Likelihood	Measurement Type	Mea	Action	# of Elements, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: One diagonal (least time)	Display Default: One pair	Pairwise Type Default: Verba
Sources	Pairwise Comparis		Copy	4	4-1 = 3	One diagonal (least ti	One pair	Verbal
Infrastructure	Pairwise Comparis		Copy	4	4-1 = 3	One diagonal (least ti	One pair	Verbal
Technical failure								
Failure of third-party authentication								
Program management failure								
Data Breach								
Political/Financial	Pairwise Comparis		Copy	7	7-1 = 6	One diagonal (least ti	One pair	Verbal
Espianoge (insider threat)								
Domestic hackers (driven by profit)								
Foriegn government hackers								
Domestic hackers (driven by political be								
Employee with access driven by profit (i								
Disgruntled employee (insider threat)								
Terrorist Attack								
Environmental	Pairwise Comparis		Copy	2	2*(2-1)/2 = 1	All pairs (maximu	One pair	Graphica
Severe weather								
Natural disaster								



Human Factor	Pairwise Comparis ▾		Copy	6	6-1 = 5	One diagonal (least ti ▾	One pair ▾	Verbal ▾
Untrained Technicians								
Requirements of policy inconsistent witl								
Careless handling of sensitive data (ins								
Staff not adhering to security policy and								
Haphazard review, evaluation, and dete								
Faulty design, methodology and approa								

4.2 Likelihood of Events by Event

Event likelihoods were measured using Pairwise comparisons. This method of measurement compares likelihoods against each other rather than against an arbitrary scale.[1]



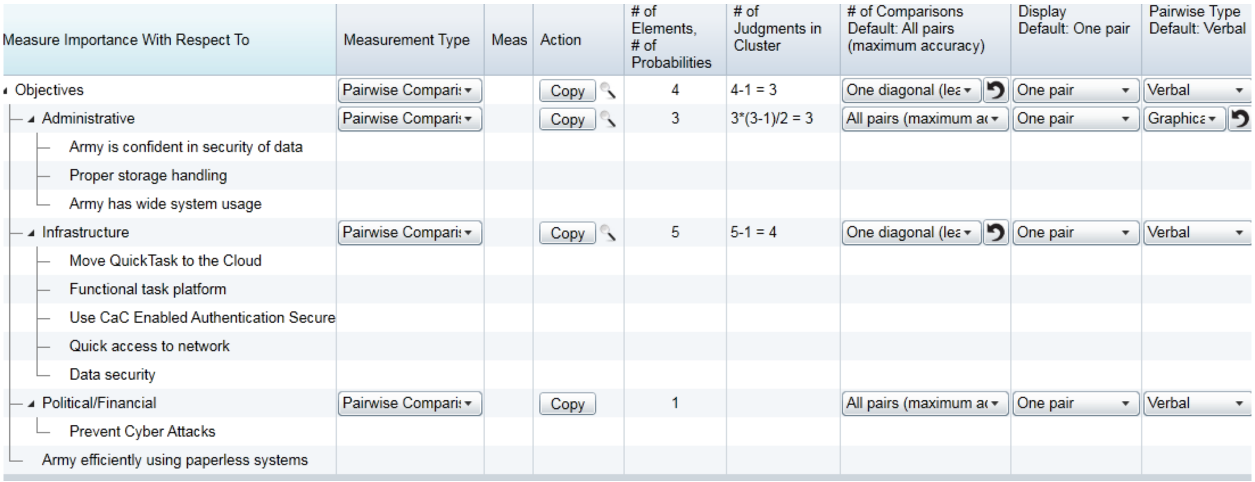
Measure Event Likelihoods	Measurement Type Default: Rating Scale	Measurement Scale or Given Likelihooc	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)
Sources						
Infrastructure						
Technical failure	Pairwise Com ▾		Copy	7	7*(7-1)/2 = 21	All pairs (maximum ac ▾
Failure of third-party authentication	Pairwise Com ▾		Copy	6	6*(6-1)/2 = 15	All pairs (maximum ac ▾
Program management failure	Pairwise Com ▾		Copy	8	8*(8-1)/2 = 28	All pairs (maximum ac ▾
Data Breach	Pairwise Com ▾		Copy	3	3*(3-1)/2 = 3	All pairs (maximum ac ▾
Political/Financial						
Espianoge (insider threat)	Pairwise Com ▾		Copy	3	3*(3-1)/2 = 3	All pairs (maximum ac ▾
Domestic hackers (driven by profit)	Pairwise Com ▾		Copy	4	4*(4-1)/2 = 6	All pairs (maximum ac ▾
Foriegn government hackers	Pairwise Com ▾		Copy	4	4*(4-1)/2 = 6	All pairs (maximum ac ▾
Domestic hackers (driven by political beli	Pairwise Com ▾		Copy	4	4*(4-1)/2 = 6	All pairs (maximum ac ▾
Employee with access driven by profit (in	Pairwise Com ▾		Copy	4	4*(4-1)/2 = 6	All pairs (maximum ac ▾
Disgruntled employee (insider threat)	Pairwise Com ▾		Copy	5	5*(5-1)/2 = 10	All pairs (maximum ac ▾
Terrorist Attack	Pairwise Com ▾		Copy	5	5*(5-1)/2 = 10	All pairs (maximum ac ▾
Environmental						
Severe weather	Pairwise Com ▾		Copy	3	3*(3-1)/2 = 3	All pairs (maximum ac ▾
Natural disaster	Pairwise Com ▾		Copy	3	3*(3-1)/2 = 3	All pairs (maximum ac ▾
Human Factor						
Untrained Technicians	Pairwise Com ▾		Copy	10	10*(10-1)/2 = 45	All pairs (maximum ac ▾
Requirements of policy inconsistent with	Pairwise Com ▾		Copy	8	8*(8-1)/2 = 28	All pairs (maximum ac ▾
Careless handling of sensitive data (insic	Pairwise Com ▾		Copy	4	4*(4-1)/2 = 6	All pairs (maximum ac ▾

4.3

Impact for Events by Objectives

We also measured the impact of events by measuring the importance of objectives and measuring consequences of events on objectives. Pairwise was used for the measurement of objectives.

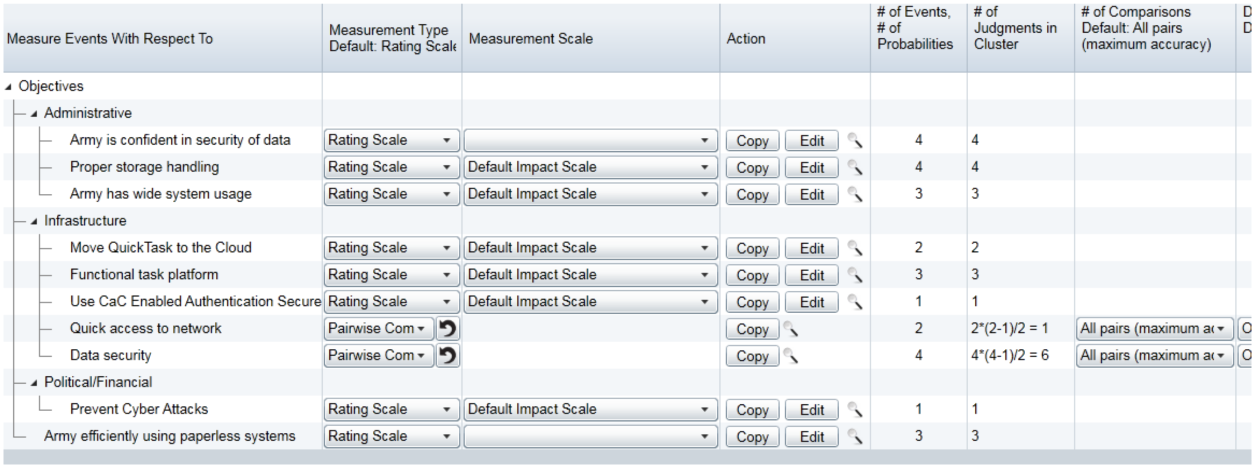
[1] In many common risk analysis matrices, the numbers 1-5 are used as a scale. Comparing likelihoods against each other is more accurate.



Measure Importance With Respect To	Measurement Type	Meas	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 Comparis		Copy	4	4-1 = 3	One diagonal (lea	One pair	Verbal
Administrative	Pairwise Comparis		Copy	3	3*(3-1)/2 = 3	All pairs (maximum ac	One pair	Graphica
Army is confident in security of data								
Proper storage handling								
Army has wide system usage								
Infrastructure	Pairwise Comparis		Copy	5	5-1 = 4	One diagonal (lea	One pair	Verbal
Move QuickTask to the Cloud								
Functional task platform								
Use CaC Enabled Authentication Secure								
Quick access to network								
Data security								
Political/Financial	Pairwise Comparis		Copy	1		All pairs (maximum ac	One pair	Verbal
Prevent Cyber Attacks								
Army efficiently using paperless systems								

4.4 Impact of Events by Event

Pairwise and ratings scale was used for the measurement of events.



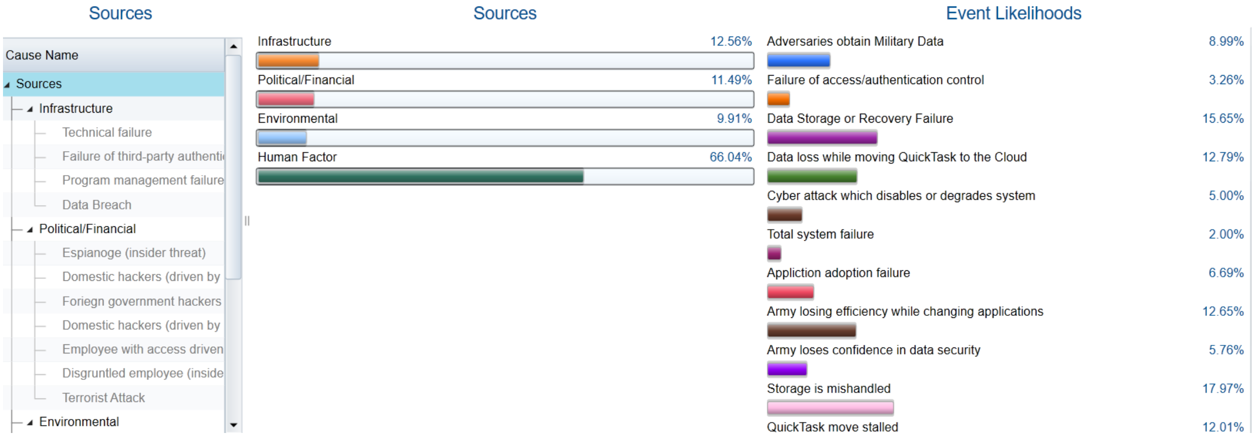
Measure Events With Respect To	Measurement Type Default: Rating Scale	Measurement Scale	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	D D
Objectives							
Administrative							
Army is confident in security of data	Rating Scale		Copy Edit	4	4		
Proper storage handling	Rating Scale	Default Impact Scale	Copy Edit	4	4		
Army has wide system usage	Rating Scale	Default Impact Scale	Copy Edit	3	3		
Infrastructure							
Move QuickTask to the Cloud	Rating Scale	Default Impact Scale	Copy Edit	2	2		
Functional task platform	Rating Scale	Default Impact Scale	Copy Edit	3	3		
Use CaC Enabled Authentication Secure	Rating Scale	Default Impact Scale	Copy Edit	1	1		
Quick access to network	Pairwise Com		Copy	2	2*(2-1)/2 = 1	All pairs (maximum ac	O
Data security	Pairwise Com		Copy	4	4*(4-1)/2 = 6	All pairs (maximum ac	O
Political/Financial							
Prevent Cyber Attacks	Rating Scale	Default Impact Scale	Copy Edit	1	1		
Army efficiently using paperless systems	Rating Scale		Copy Edit	3	3		

5. Synthesis/Sensitivity Analysis

5.1 Likelihood of Sources

From the above comparisons, the QuickTask team was able to determine the likelihood of the sources of events and the events themselves. The below graphs are of high importance as they illustrate items that needed to be watched.

During synthesis, we used the sensitivity report to reveal how sources corresponded to the likelihood of events based on percentages. Human factor is the highest source with 66.4%, followed by Infrastructure with 12.56%, Political/Financial with 11.49% and Environmental with 9.91%.



Sources

Cause Name

- Sources
  - Infrastructure
    - Technical failure
    - Failure of third-party authenti
    - Program management failure
    - Data Breach
  - Political/Financial
    - Espianoge (insider threat)
    - Domestic hackers (driven by
    - Foriegn government hackers
    - Domestic hackers (driven by
    - Employee with access driven
    - Disgruntled employee (inside
    - Terrorist Attack
  - Environmental

Sources

Infrastructure	12.56%
Political/Financial	11.49%
Environmental	9.91%
Human Factor	66.04%

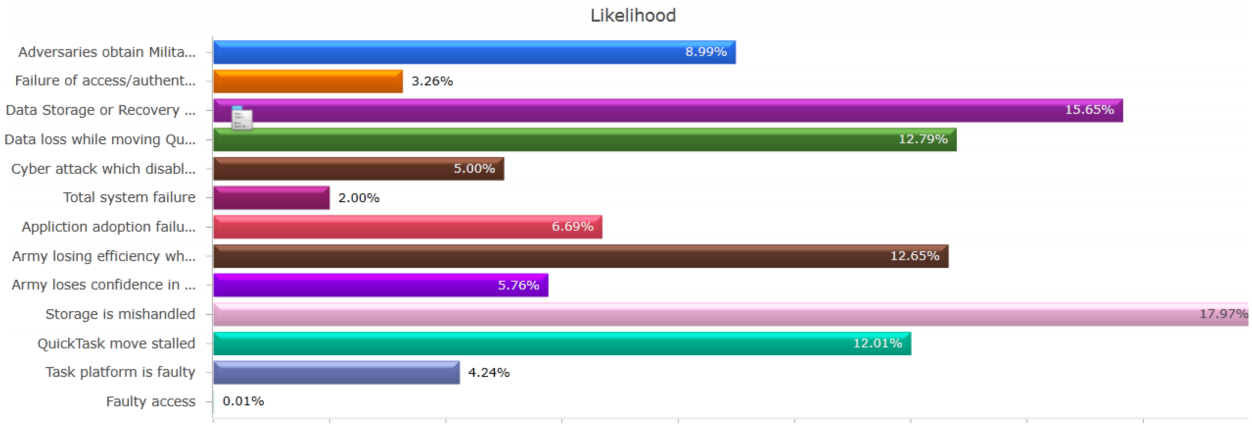
Event Likelihoods

Adversaries obtain Military Data	8.99%
Failure of access/authentication control	3.26%
Data Storage or Recovery Failure	15.65%
Data loss while moving QuickTask to the Cloud	12.79%
Cyber attack which disables or degrades system	5.00%
Total system failure	2.00%
Appliction adoption failure	6.69%
Army losing efficiency while changing applications	12.65%
Army loses confidence in data security	5.76%
Storage is mishandled	17.97%
QuickTask move stalled	12.01%

\

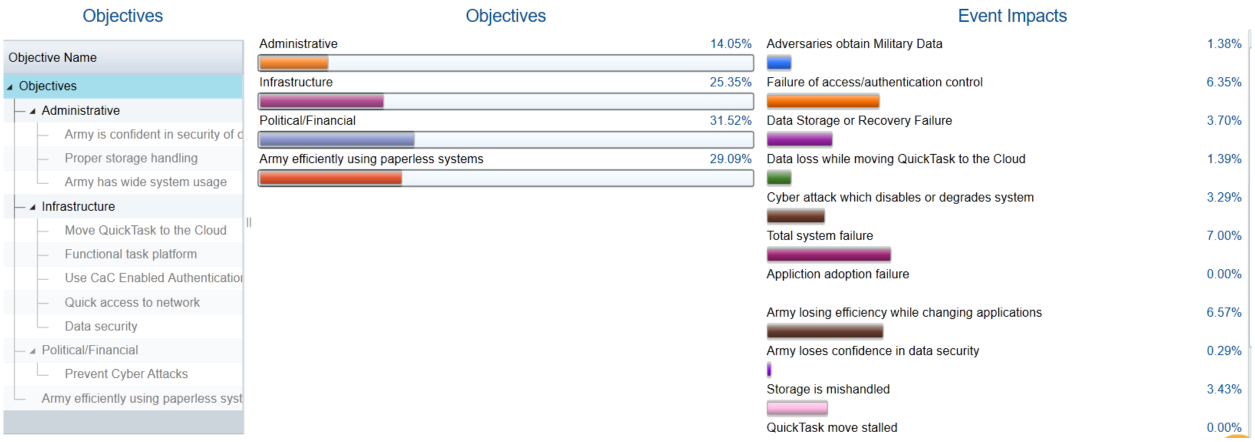
5.2 Likelihood of Events

The highest risk event for QuickTask as it relates to a potential occurrence is Storage is mishandled. The lowest is Faulty access. The median is Application adoption failure. Potential of occurrence is due to threats/sources are shown above.



5.3 Impact of Events on Objectives

Adversaries Obtaining Military Data has an Event Impact of 1.38%, but the likelihood of this event is 8.99%. Conversely, Total System Failure has an Event Impact of 7% but the likelihood is only 2%. The top three risk events with the greatest impact to the objectives were Total system failure, Army losing efficiency with changing applications, and failure access/authentication control.



Objectives

Objective Name

- Objectives
  - Administrative
    - Army is confident in security of d
    - Proper storage handling
    - Army has wide system usage
  - Infrastructure
    - Move QuickTask to the Cloud
    - Functional task platform
    - Use CaC Enabled Authenticatio
    - Quick access to network
    - Data security
  - Political/Financial
    - Prevent Cyber Attacks
  - Army efficiently using paperless syst

Objectives

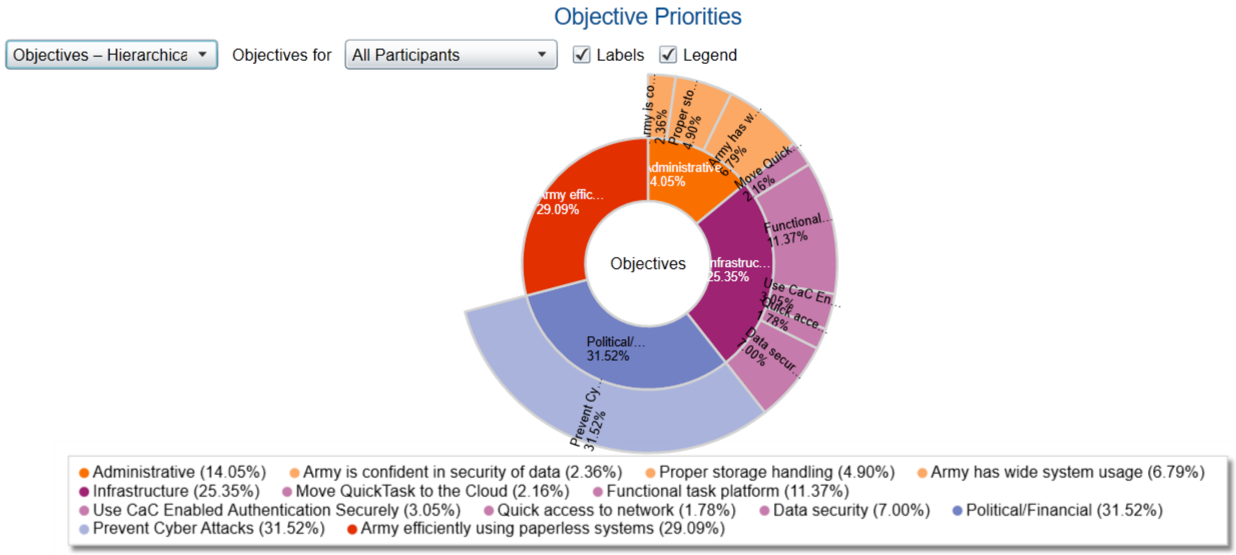
Objective	%
Administrative	14.05%
Infrastructure	25.35%
Political/Financial	31.52%
Army efficiently using paperless systems	29.09%

Event Impacts

Event	%
Adversaries obtain Military Data	1.38%
Failure of access/authentication control	6.35%
Data Storage or Recovery Failure	3.70%
Data loss while moving QuickTask to the Cloud	1.39%
Cyber attack which disables or degrades system	3.29%
Total system failure	7.00%
Appliction adoption failure	0.00%
Army losing efficiency while changing applications	6.57%
Army loses confidence in data security	0.29%
Storage is mishandled	3.43%
QuickTask move stalled	0.00%

5.3 Objective Priorities

This objective priorities pie chart sorts all objectives into their groups and ranks them based on priority comparison measures.



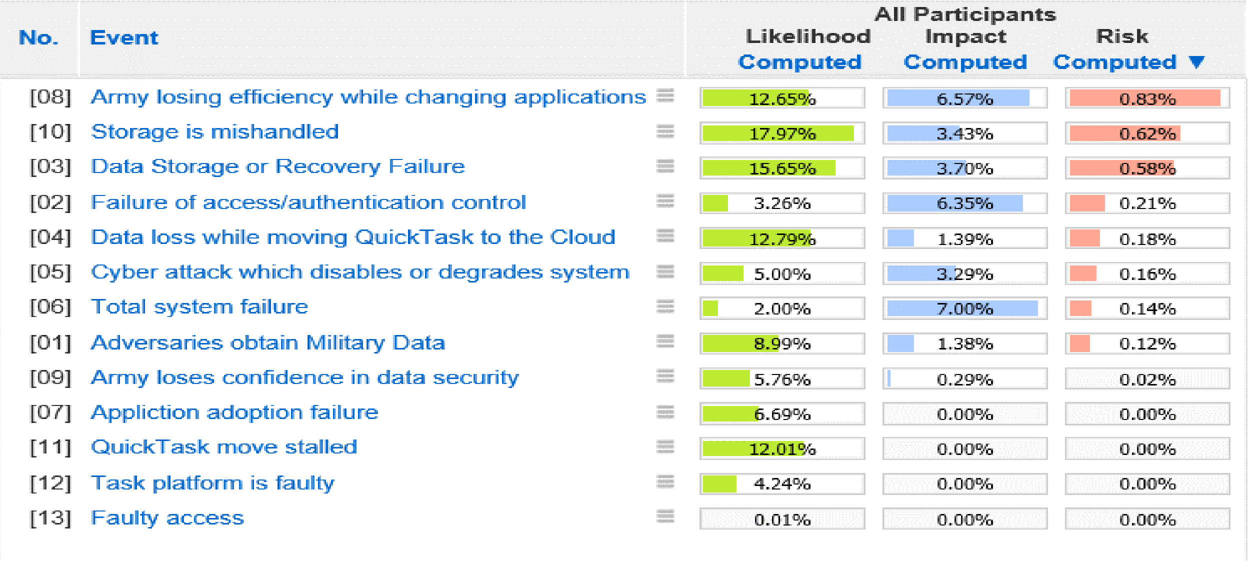
Objective Priorities

Objectives – Hierarchica ▾ Objectives for All Participants ▾ ☑ Labels ☑ Legend

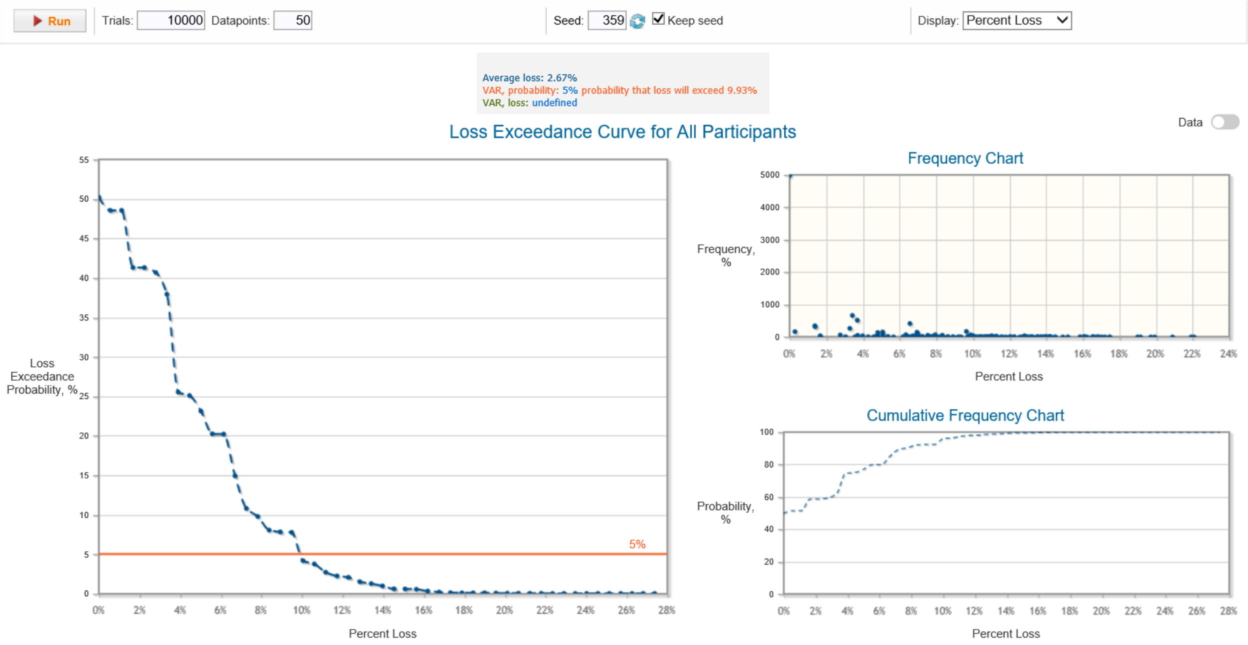
6. Risk Review

6.1 Overall Risk

Below is the first look at the project risks which was calculated by multiplying likelihood times Impact. The most likely event was the Army Loses Efficiency While Changing Applications. Even being the greatest risk, it was computed to be low at .83 percent.



No.	Event	All Participants Likelihood Computed	 Impact Computed	 Risk Computed ▼
[08]	Army losing efficiency while changing applications	12.65%	6.57%	0.83%
[10]	Storage is mishandled	17.97%	3.43%	0.62%
[03]	Data Storage or Recovery Failure	15.65%	3.70%	0.58%
[02]	Failure of access/authentication control	3.26%	6.35%	0.21%
[04]	Data loss while moving QuickTask to the Cloud	12.79%	1.39%	0.18%
[05]	Cyber attack which disables or degrades system	5.00%	3.29%	0.16%
[06]	Total system failure	2.00%	7.00%	0.14%
[01]	Adversaries obtain Military Data	8.99%	1.38%	0.12%
[09]	Army loses confidence in data security	5.76%	0.29%	0.02%
[07]	Appliction adoption failure	6.69%	0.00%	0.00%
[11]	QuickTask move stalled	12.01%	0.00%	0.00%
[12]	Task platform is faulty	4.24%	0.00%	0.00%
[13]	Faulty access	0.01%	0.00%	0.00%



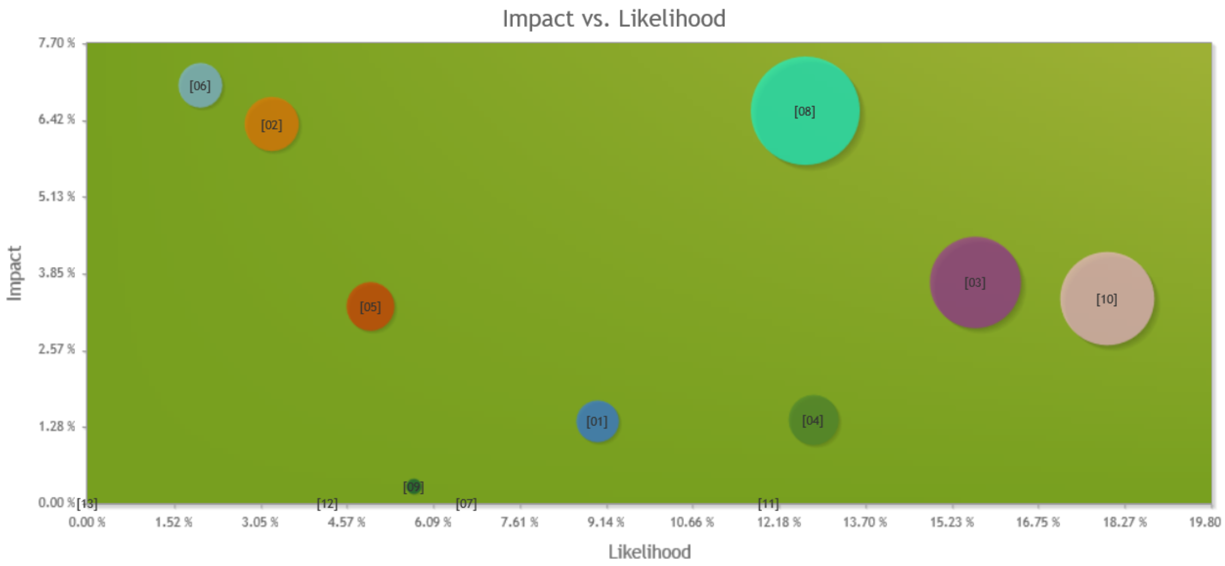
▶ Run Trials: 10000 Datapoints: 50 Seed: 359 ☑ Keep seed Display: Percent Loss

Average loss: 2.67%
VAR, probability: 5% probability that loss will exceed 9.93%
VAR, loss: undefined

6.2 Risk Heat Map

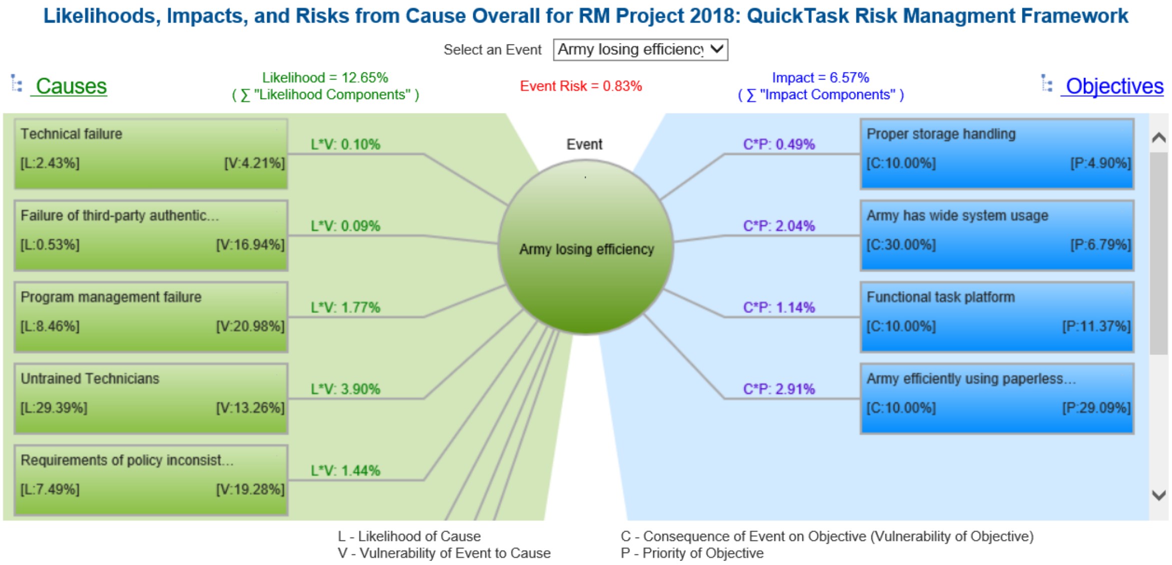
The Heat Map displays impacts and likelihood of events with and without controls. The likelihood is displayed on the x axis and the impact on the y showing the resulting correlations.

The heat map visually displays the data 6.1.



6.3 Bowtie Diagram "Army Losing Efficiency"

In the Riskion system, bowtie diagrams can be large and there is one for each item. A good example is listed below. On the left the causes are displayed, and on the right, the objectives. QuickTask risk events are given a score by synthesizing judgements from participants. Sources/Threats/Causes to QuickTask are shown in green.


Likelihoods, Impacts, and Risks from Cause Overall for RM Project 2018: QuickTask Risk Managment Framework

Select an Event: Army losing efficiency

Causes

Likelihood = 12.65% (∑ "Likelihood Components")

Event Risk = 0.83%

Impact = 6.57% (∑ "Impact Components")

Objectives

Technical failure [L:2.43%] [V:4.21%] — L*V: 0.10%

Failure of third-party authentic... [L:0.53%] [V:16.94%] — L*V: 0.09%

Program management failure [L:8.46%] [V:20.98%] — L*V: 1.77%

Untrained Technicians [L:29.39%] [V:13.26%] — L*V: 3.90%

Requirements of policy inconsist... [L:7.49%] [V:19.28%] — L*V: 1.44%

Event: Army losing efficiency

C*P: 0.49% — Proper storage handling [C:10.00%] [P:4.90%]

C*P: 2.04% — Army has wide system usage [C:30.00%] [P:6.79%]

C*P: 1.14% — Functional task platform [C:10.00%] [P:11.37%]

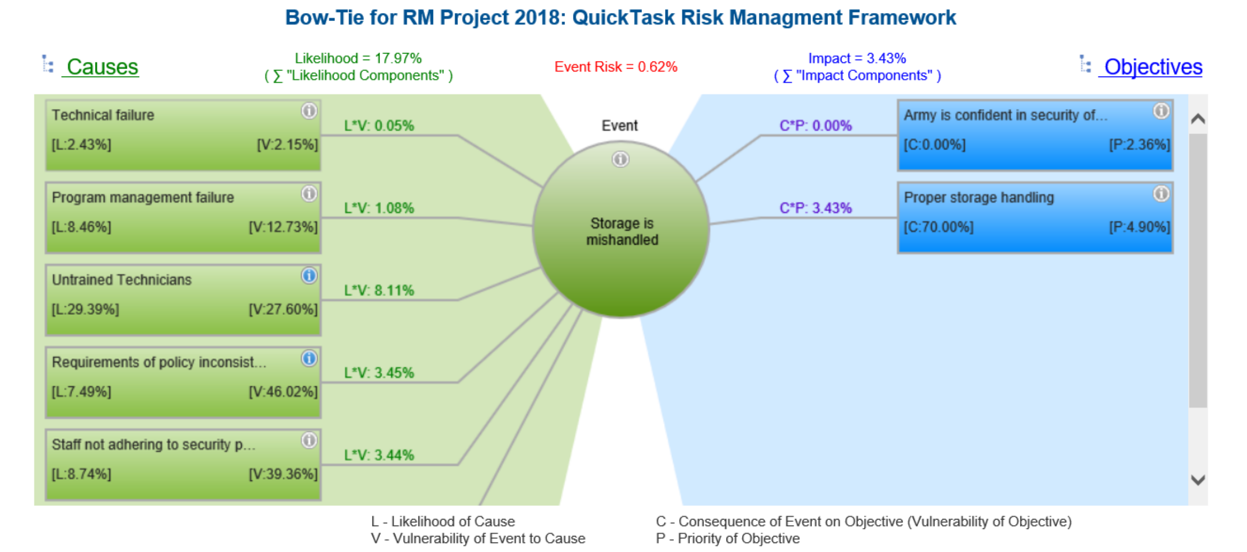
C*P: 2.91% — Army efficiently using paperless... [C:10.00%] [P:29.09%]

L - Likelihood of Cause
V - Vulnerability of Event to Cause

C - Consequence of Event on Objective (Vulnerability of Objective)
P - Priority of Objective

6.4 Bowtie Diagram for "Storage is Mishandled"

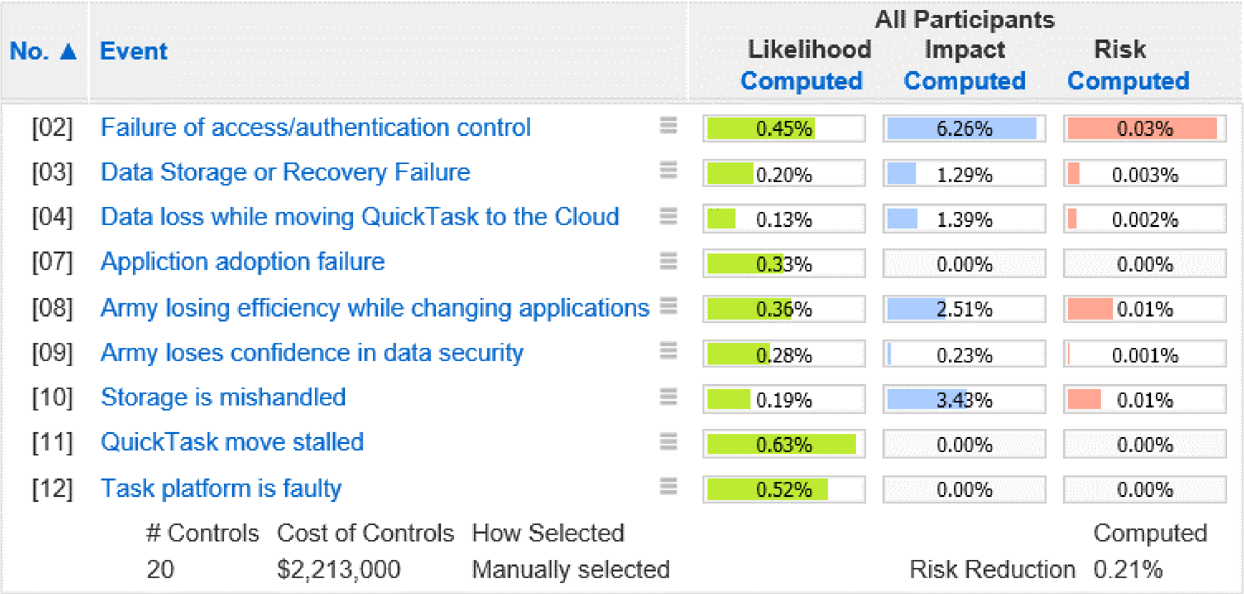
Below is a second example.



7. Controls

7.1 Risks with Controls

In our first look at risks with controls, we see that overall risk was reduced by .21 percent.



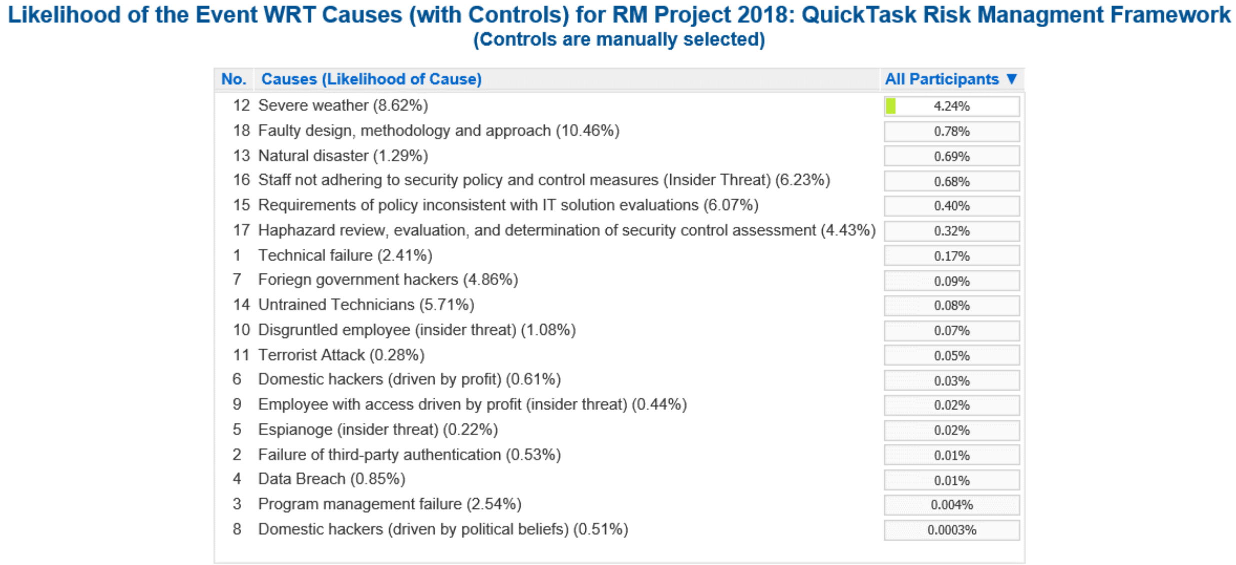
No. ▲	Event	All Participants Likelihood Computed	 Impact Computed	 Risk Computed
[02]	Failure of access/authentication control	0.45%	6.26%	0.03%
[03]	Data Storage or Recovery Failure	0.20%	1.29%	0.003%
[04]	Data loss while moving QuickTask to the Cloud	0.13%	1.39%	0.002%
[07]	Appliction adoption failure	0.33%	0.00%	0.00%
[08]	Army losing efficiency while changing applications	0.36%	2.51%	0.01%
[09]	Army loses confidence in data security	0.28%	0.23%	0.001%
[10]	Storage is mishandled	0.19%	3.43%	0.01%
[11]	QuickTask move stalled	0.63%	0.00%	0.00%
[12]	Task platform is faulty	0.52%	0.00%	0.00%

# Controls	Cost of Controls	How Selected		Computed
20	$2,213,000	Manually selected	Risk Reduction	0.21%

7.2 Likelihood of Events with Controls

It makes sense that severe weather would be the most likely event with controls. We can control the risk of the objective but not the source in this case.

For QuickTask, we look at the computed value for likelihood, impact and risk against the simulated value of likelihood, impact and risk. We use Monte Carlo simulations to see what's likely to happen given chance.

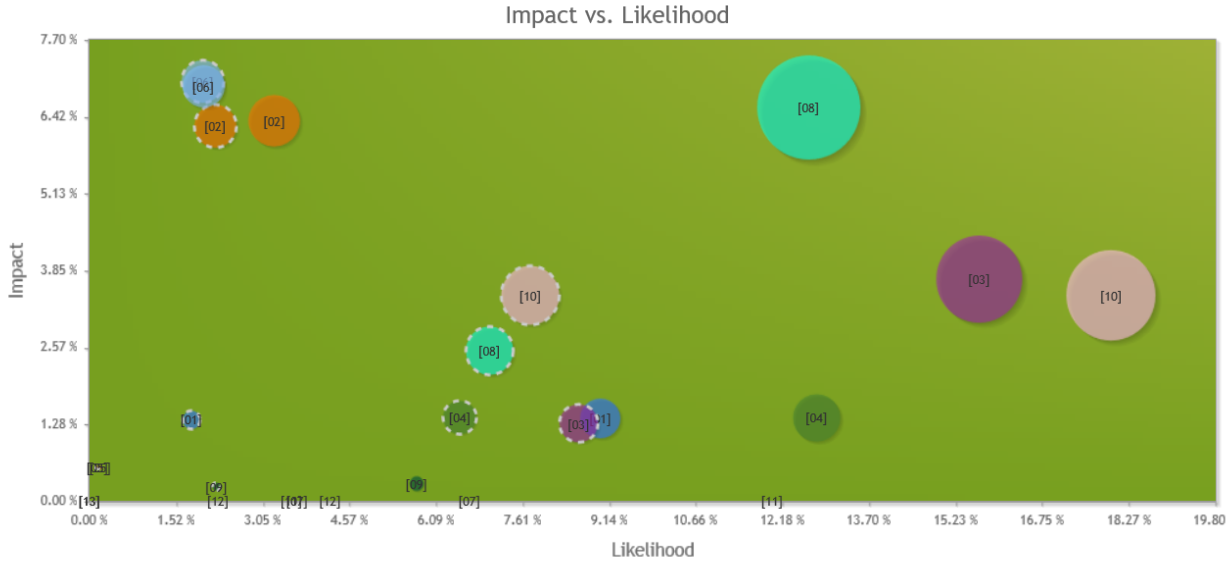


Likelihood of the Event WRT Causes (with Controls) for RM Project 2018: QuickTask Risk Managment Framework
(Controls are manually selected)

No.	Causes (Likelihood of Cause)	All Participants ▼
12	Severe weather (8.62%)	4.24%
18	Faulty design, methodology and approach (10.46%)	0.78%
13	Natural disaster (1.29%)	0.69%
16	Staff not adhering to security policy and control measures (Insider Threat) (6.23%)	0.68%
15	Requirements of policy inconsistent with IT solution evaluations (6.07%)	0.40%
17	Haphazard review, evaluation, and determination of security control assessment (4.43%)	0.32%
1	Technical failure (2.41%)	0.17%
7	Foriegn government hackers (4.86%)	0.09%
14	Untrained Technicians (5.71%)	0.08%
10	Disgruntled employee (insider threat) (1.08%)	0.07%
11	Terrorist Attack (0.28%)	0.05%
6	Domestic hackers (driven by profit) (0.61%)	0.03%
9	Employee with access driven by profit (insider threat) (0.44%)	0.02%
5	Espianoge (insider threat) (0.22%)	0.02%
2	Failure of third-party authentication (0.53%)	0.01%
4	Data Breach (0.85%)	0.01%
3	Program management failure (2.54%)	0.004%
8	Domestic hackers (driven by political beliefs) (0.51%)	0.0003%

7.3 Heat Map with Controls and Without

This heat map illustrates what our risks were before and after implementing controls. The solid circles represent the risks before implementing controls, and the dotted circles represent risks with controls applied.



8. Conclusion

When controls were implemented on this project, all but three of the events become zero risk or nearly zero. One reason these are brought down so low is that many risks are covered by more than one control. Having dual coverage (triple, or more…) brings the risk to effectively zero percent. The event with the most risks after controls are implemented is the Mishandling of Storage.

The optimization feature in Riskion measures control cost and effectiveness on overall risk, giving the project the most efficient path for managing risk. Many of the controls come with low or no cost, so when optimizing the effectiveness of the controls, the program suggested removing certain controls. The QuickTask team rejects this suggestion on the grounds that those two items are DoD requirements.

Lessons learned: In future risk management projects, a dollar value will need to be assigned for every control, regardless if the organization is paying directly for the control. This shows a more realistic picture of the value rather than just the cost of applying the control.

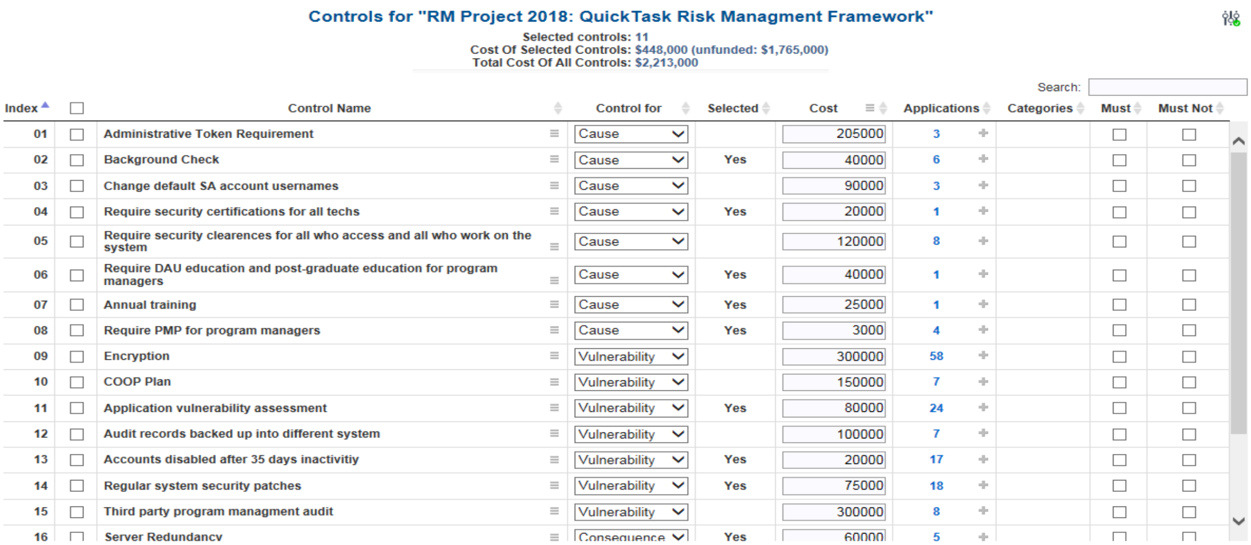
9. Lessons Learned

We decided to focus on our lessons learned post project closure. Specifically, to address risk controls/treatment. Risk for QuickTask was identified, assessed, and managed based on one or more of the following categories: Avoidance, Reduction, Sharing, or Retention. We focused on the budget for QuickTask and what action we will take to reduce the potential harm of going over budget or maintaining the budget at an acceptable level. We decided to consider potential financial loses and take action to reduce this loss.

Identify and Select Controls/Treatments

We identified controls for sources/threats, event vulnerabilities, and impact mitigation. Controls are activities that DoD can implement to mitigate these items.

Utilizing a list of events, sources, and objectives, we evaluated likelihoods, impacts and risk of our QuickTask project. We identified 20 controls and assigned categories of cause, vulnerability, or consequence. After assigning applicable costs for each control, all controls totaled $2.2M

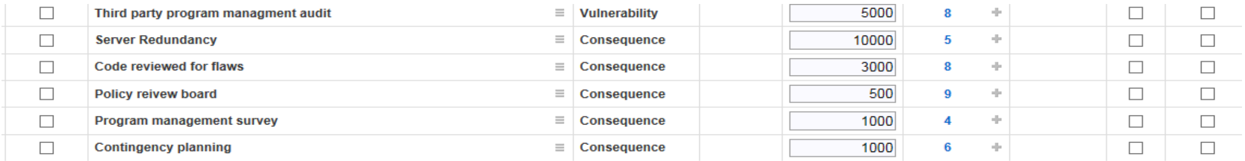


Controls for "RM Project 2018: QuickTask Risk Managment Framework"

Selected controls: 11
Cost Of Selected Controls: $448,000 (unfunded: $1,765,000)
Total Cost Of All Controls: $2,213,000

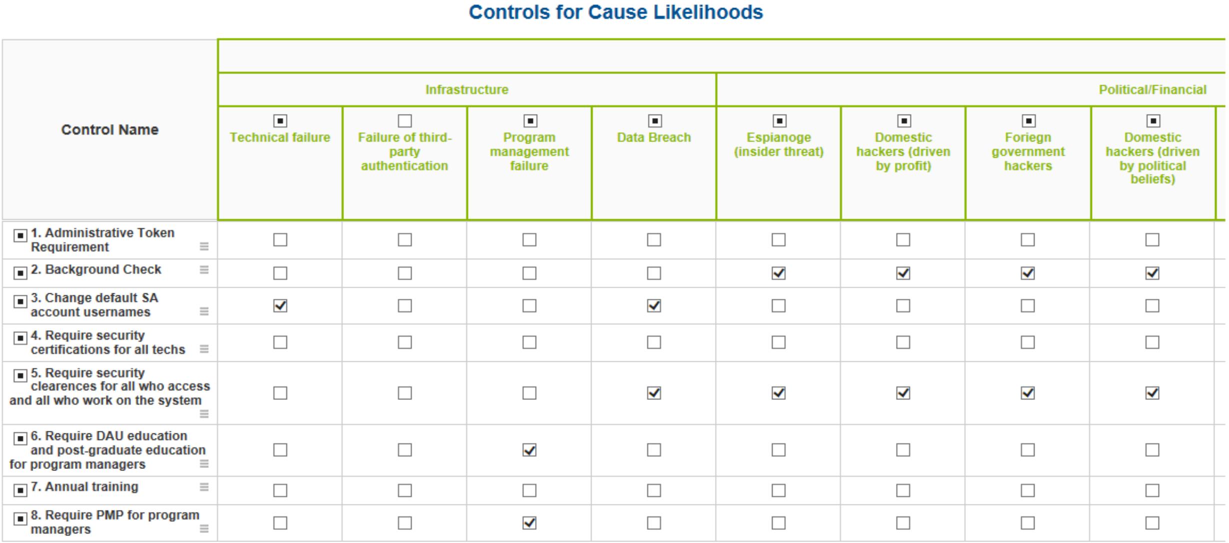
Search:

Index	□	Control Name	Control for	Selected	Cost	Applications	Categories	Must	Must Not
01	□	Administrative Token Requirement	Cause		205000	3		□	□
02	□	Background Check	Cause	Yes	40000	6		□	□
03	□	Change default SA account usernames	Cause		90000	3		□	□
04	□	Require security certifications for all techs	Cause	Yes	20000	1		□	□
05	□	Require security clearences for all who access and all who work on the system	Cause		120000	8		□	□
06	□	Require DAU education and post-graduate education for program managers	Cause	Yes	40000	1		□	□
07	□	Annual training	Cause	Yes	25000	1		□	□
08	□	Require PMP for program managers	Cause	Yes	3000	4		□	□
09	□	Encryption	Vulnerability		300000	58		□	□
10	□	COOP Plan	Vulnerability		150000	7		□	□
11	□	Application vulnerability assessment	Vulnerability	Yes	80000	24		□	□
12	□	Audit records backed up into different system	Vulnerability		100000	7		□	□
13	□	Accounts disabled after 35 days inactivitiy	Vulnerability	Yes	20000	17		□	□
14	□	Regular system security patches	Vulnerability	Yes	75000	18		□	□
15	□	Third party program managment audit	Vulnerability		300000	8		□	□
16	□	Server Redundancy	Consequence	Yes	60000	5		□	□



□	Third party program managment audit	Vulnerability		5000	8	□	□
□	Server Redundancy	Consequence		10000	5	□	□
□	Code reviewed for flaws	Consequence		3000	8	□	□
□	Policy reivew board	Consequence		500	9	□	□
□	Program management survey	Consequence		1000	4	□	□
□	Contingency planning	Consequence		1000	6	□	□

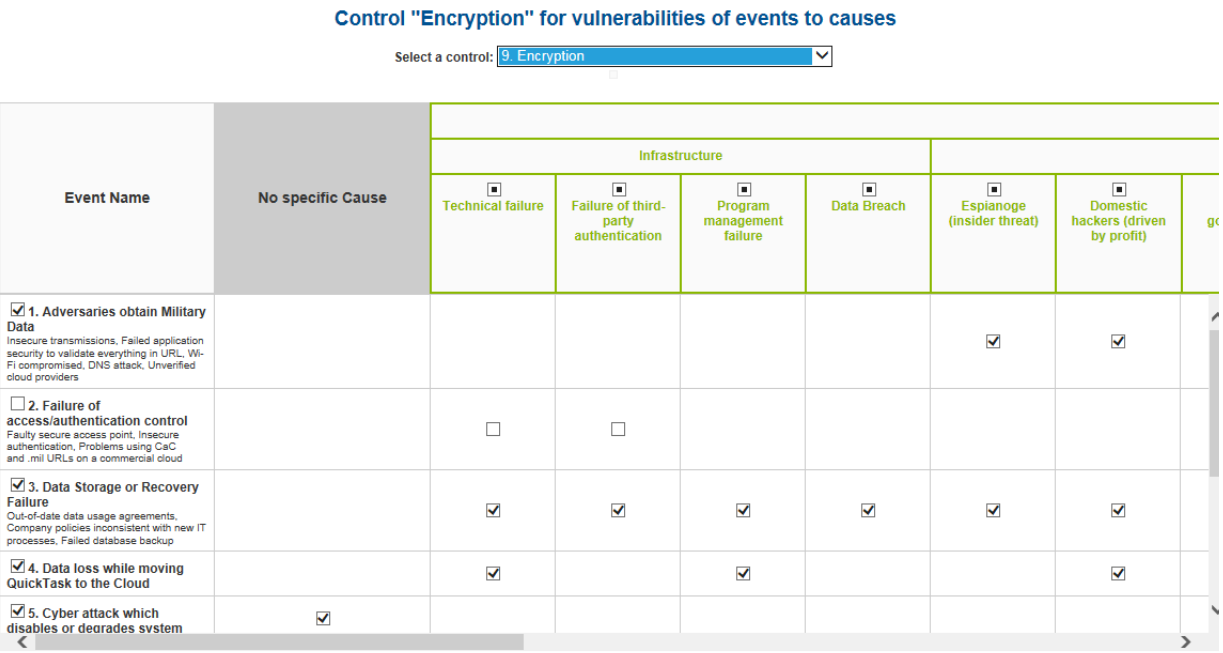
We then determined relationships for each of the controls and the likelihood of causes.



Controls for Cause Likelihoods

Control Name								
	Infrastructure				Political/Financial			
	▣ Technical failure	□ Failure of third-party authentication	▣ Program management failure	▣ Data Breach	▣ Espianoge (insider threat)	▣ Domestic hackers (driven by profit)	▣ Foriegn government hackers	▣ Domestic hackers (driven by political beliefs)
▣ 1. Administrative Token Requirement	□	□	□	□	□	□	□	□
▣ 2. Background Check	□	□	□	□	☑	☑	☑	☑
▣ 3. Change default SA account usernames	☑	□	□	☑	□	□	□	□
▣ 4. Require security certifications for all techs	□	□	□	□	□	□	□	□
▣ 5. Require security clearences for all who access and all who work on the system	□	□	□	☑	☑	☑	☑	☑
▣ 6. Require DAU education and post-graduate education for program managers	□	□	☑	□	□	□	□	□
▣ 7. Annual training	□	□	□	□	□	□	□	□
▣ 8. Require PMP for program managers	□	□	☑	□	□	□	□	□

Here is an example of a control and the associated events and causes assigned.



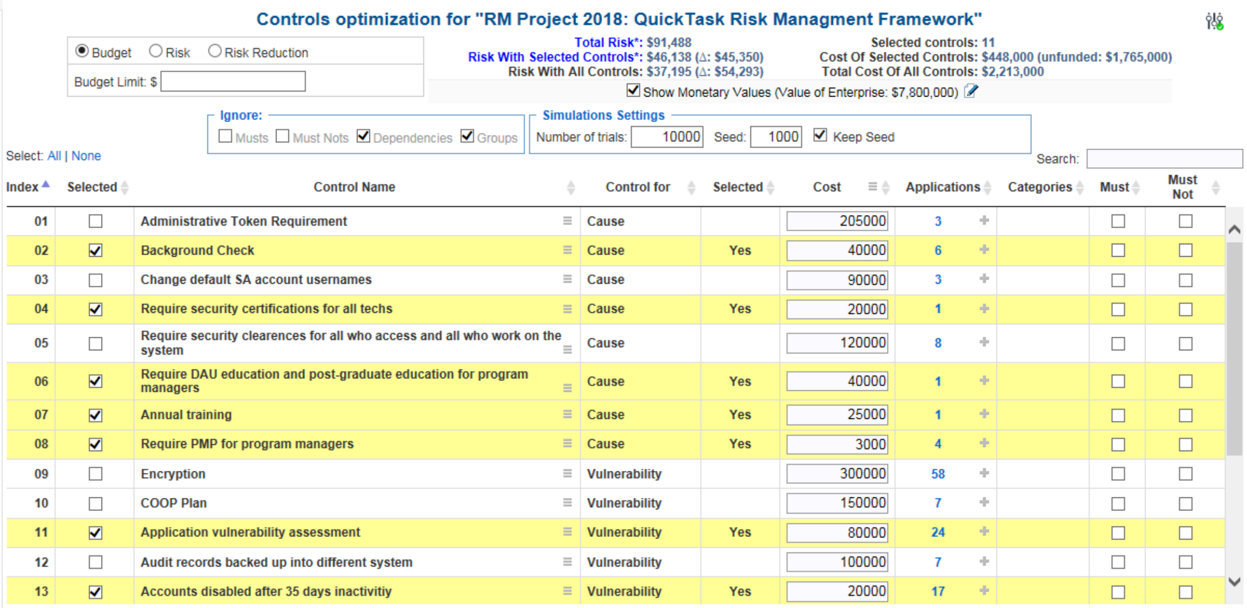
Control "Encryption" for vulnerabilities of events to causes

Select a control: 9. Encryption

Event Name	No specific Cause	▣ Technical failure	▣ Failure of third-party authentication	▣ Program management failure	▣ Data Breach	▣ Espianoge (insider threat)	▣ Domestic hackers (driven by profit)
		Infrastructure					
☑ 1. Adversaries obtain Military Data Insecure transmissions, Failed application security to validate everything in URL, Wi-Fi compromised, DNS attack, Unverified cloud providers						☑	☑
□ 2. Failure of access/authentication control Faulty secure access point, Insecure authentication, Problems using CaC and .mil URLs on a commercial cloud		□	□				
☑ 3. Data Storage or Recovery Failure Out-of-date data usage agreements, Company policies inconsistent with new IT processes, Failed database backup		☑	☑	☑	☑	☑	☑
☑ 4. Data loss while moving QuickTask to the Cloud		☑		☑			☑
☑ 5. Cyber attack which disables or degrades system	☑						

The total cost of all controls was $2.2M and assumed a given budget for Quick Task was: $450K. Our monetary value for Objectives/Enterprise was $7.8M

We selected 11 controls with a total cost of $448K to stay within budget and in an attempt to lessen resulting risk while also taking into account what essential controls would be needed by DOD. This resulted in $1.7M of controls to be unfunded.



Controls optimization for "RM Project 2018: QuickTask Risk Managment Framework"

● Budget ○ Risk ○ Risk Reduction

Budget Limit: $

Total Risk*: $91,488
Risk With Selected Controls*: $46,138 (Δ: $45,350)
Risk With All Controls: $37,195 (Δ: $54,293)

Selected controls: 11
Cost Of Selected Controls: $448,000 (unfunded: $1,765,000)
Total Cost Of All Controls: $2,213,000

☑ Show Monetary Values (Value of Enterprise: $7,800,000)

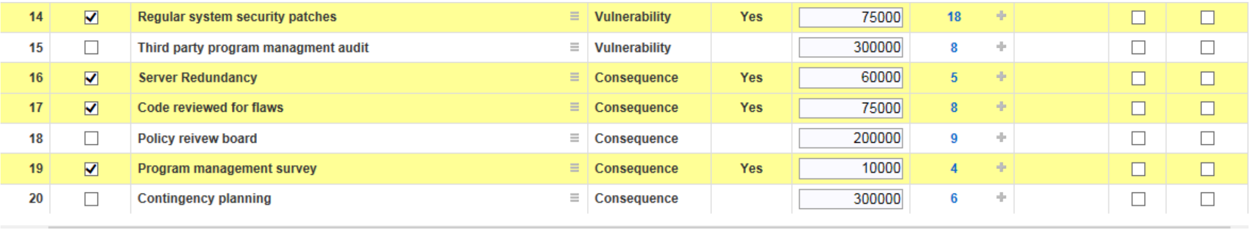
Ignore: □ Musts □ Must Nots ☑ Dependencies ☑ Groups

Simulations Settings: Number of trials: 10000 Seed: 1000 ☑ Keep Seed

Select: All | None

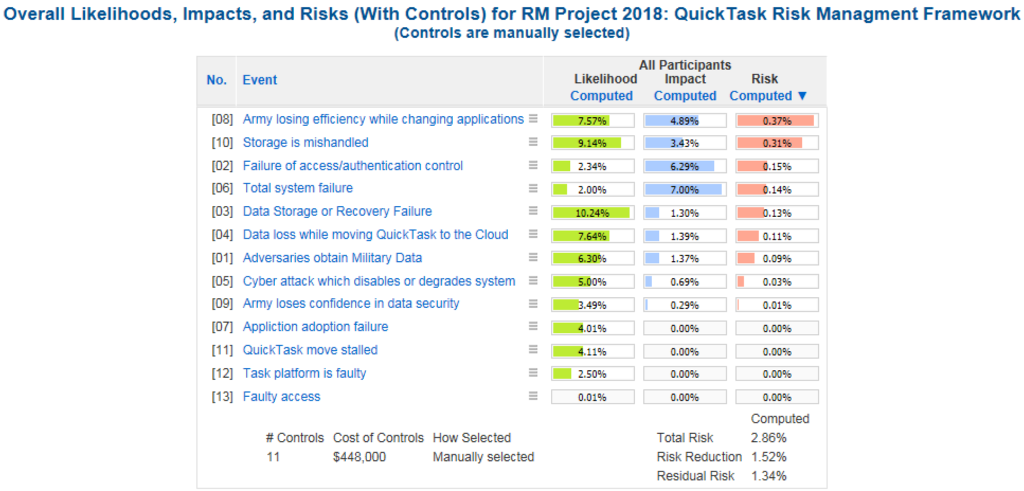
Search:

Index	Selected	Control Name	Control for	Selected	Cost	Applications	Categories	Must	Must Not
01	□	Administrative Token Requirement	Cause		205000	3		□	□
02	☑	Background Check	Cause	Yes	40000	6		□	□
03	□	Change default SA account usernames	Cause		90000	3		□	□
04	☑	Require security certifications for all techs	Cause	Yes	20000	1		□	□
05	□	Require security clearences for all who access and all who work on the system	Cause		120000	8		□	□
06	☑	Require DAU education and post-graduate education for program managers	Cause	Yes	40000	1		□	□
07	☑	Annual training	Cause	Yes	25000	1		□	□
08	☑	Require PMP for program managers	Cause	Yes	3000	4		□	□
09	□	Encryption	Vulnerability		300000	58		□	□
10	□	COOP Plan	Vulnerability		150000	7		□	□
11	☑	Application vulnerability assessment	Vulnerability	Yes	80000	24		□	□
12	□	Audit records backed up into different system	Vulnerability		100000	7		□	□
13	☑	Accounts disabled after 35 days inactivitiy	Vulnerability	Yes	20000	17		□	□



14	☑	Regular system security patches	≡	Vulnerability	Yes	75000	18	+		□	□
15	□	Third party program managment audit	≡	Vulnerability		300000	8	+		□	□
16	☑	Server Redundancy	≡	Consequence	Yes	60000	5	+		□	□
17	☑	Code reviewed for flaws	≡	Consequence	Yes	75000	8	+		□	□
18	□	Policy reivew board	≡	Consequence		200000	9	+		□	□
19	☑	Program management survey	≡	Consequence	Yes	10000	4	+		□	□
20	□	Contingency planning	≡	Consequence		300000	6	+		□	□

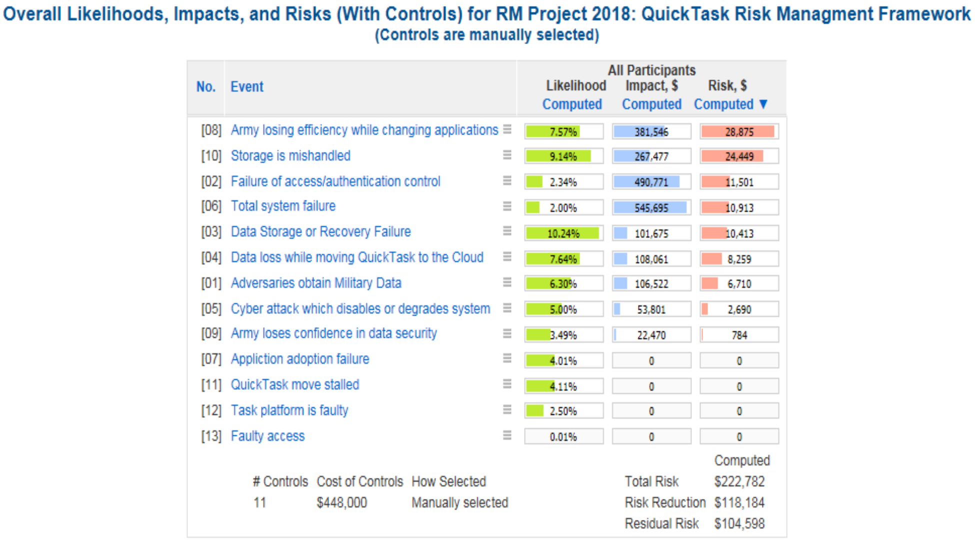
We assigned a monetary value for the objectives of $7.8M to reveal monetary value and percentage value. The computer values are shown first for overall likelihood, impacts, and risk. After creating a project budget of $448k based on our assumed financial resources, we were able to determine a total risk of 2.86%, a risk reduction of 1.52% and a residual risk of 1.34%. Monetary values are also identified below.



Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018: QuickTask Risk Managment Framework
(Controls are manually selected)

No.	Event	All Participants Likelihood Computed	 Impact Computed	 Risk Computed ▼
[08]	Army losing efficiency while changing applications ≡	7.57%	4.89%	0.37%
[10]	Storage is mishandled ≡	9.14%	3.43%	0.31%
[02]	Failure of access/authentication control ≡	2.34%	6.29%	0.15%
[06]	Total system failure ≡	2.00%	7.00%	0.14%
[03]	Data Storage or Recovery Failure ≡	10.24%	1.30%	0.13%
[04]	Data loss while moving QuickTask to the Cloud ≡	7.64%	1.39%	0.11%
[01]	Adversaries obtain Military Data ≡	6.30%	1.37%	0.09%
[05]	Cyber attack which disables or degrades system ≡	5.00%	0.69%	0.03%
[09]	Army loses confidence in data security ≡	3.49%	0.29%	0.01%
[07]	Appliction adoption failure ≡	4.01%	0.00%	0.00%
[11]	QuickTask move stalled ≡	4.11%	0.00%	0.00%
[12]	Task platform is faulty ≡	2.50%	0.00%	0.00%
[13]	Faulty access ≡	0.01%	0.00%	0.00%

# Controls	Cost of Controls	How Selected		Computed
11	$448,000	Manually selected	Total Risk	2.86%
			Risk Reduction	1.52%
			Residual Risk	1.34%



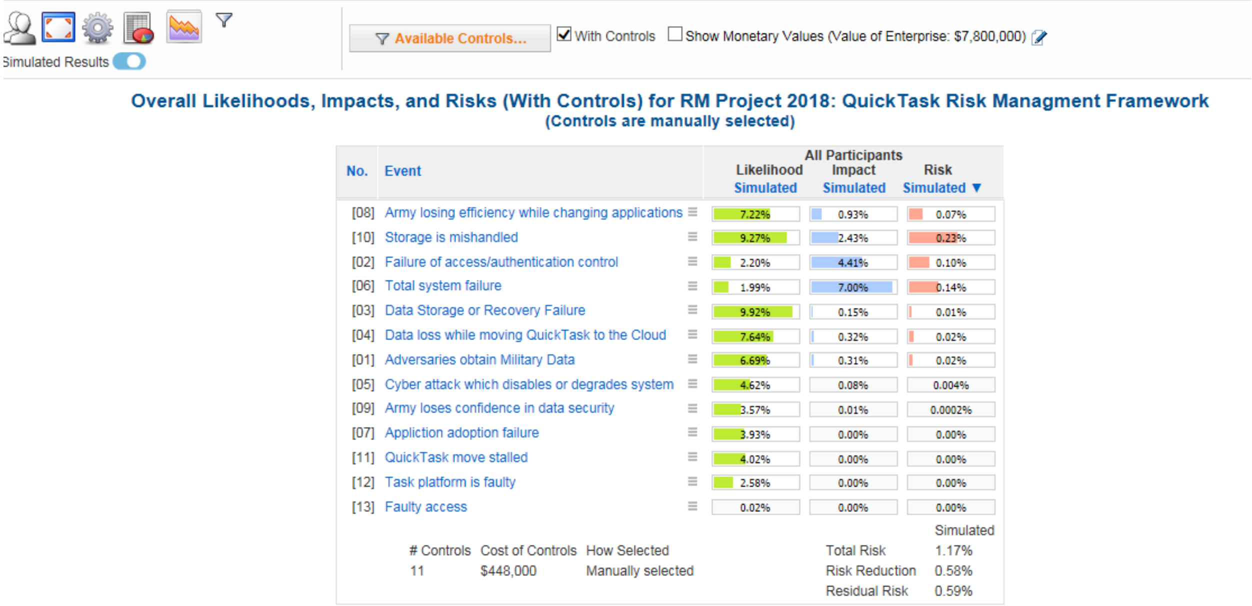
Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018: QuickTask Risk Managment Framework
(Controls are manually selected)

No.	Event	All Participants Likelihood Computed	 Impact, $ Computed	 Risk, $ Computed ▼
[08]	Army losing efficiency while changing applications ≡	7.57%	381,546	28,875
[10]	Storage is mishandled ≡	9.14%	267,477	24,449
[02]	Failure of access/authentication control ≡	2.34%	490,771	11,501
[06]	Total system failure ≡	2.00%	545,695	10,913
[03]	Data Storage or Recovery Failure ≡	10.24%	101,675	10,413
[04]	Data loss while moving QuickTask to the Cloud ≡	7.64%	108,061	8,259
[01]	Adversaries obtain Military Data ≡	6.30%	106,522	6,710
[05]	Cyber attack which disables or degrades system ≡	5.00%	53,801	2,690
[09]	Army loses confidence in data security ≡	3.49%	22,470	784
[07]	Appliction adoption failure ≡	4.01%	0	0
[11]	QuickTask move stalled ≡	4.11%	0	0
[12]	Task platform is faulty ≡	2.50%	0	0
[13]	Faulty access ≡	0.01%	0	0

# Controls	Cost of Controls	How Selected		Computed
11	$448,000	Manually selected	Total Risk	$222,782
			Risk Reduction	$118,184
			Residual Risk	$104,598

We then simulated the results using Monte Carlo Simulation. Monte Carlo Simulation is used to assess probability of curves to determine the likelihood of an outcome. It's much more accurate than double counting because it shows the likelihood of an event taking place based on multiple simulations and random sampling to obtain numerical results. Below are the simulated results.

Please note that, Data Recovery Storage has the highest likelihood of occurring with 7.64% but only contributes $11k to the overall costs and is low risk. Whereas, Total System Failure have a likelihood of less than 2% but a monetary impact of over $500k and is identified as the event with the 2nd highest risk. Monte Carlo Simulations is very useful in showing accuracy using probabilities and likelihoods in the Riskion application.



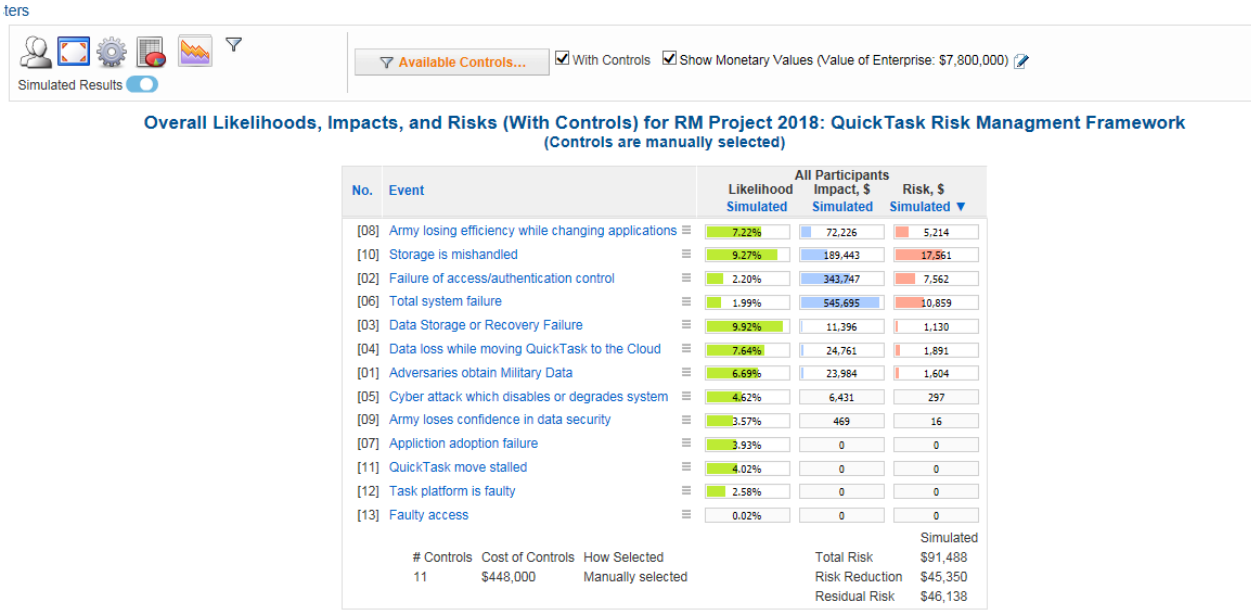
☑ With Controls □ Show Monetary Values (Value of Enterprise: $7,800,000)

Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018: QuickTask Risk Managment Framework
(Controls are manually selected)

No.	Event	All Participants Likelihood Simulated	Impact Simulated	Risk Simulated ▼
[08]	Army losing efficiency while changing applications	7.22%	0.93%	0.07%
[10]	Storage is mishandled	9.27%	2.43%	0.23%
[02]	Failure of access/authentication control	2.20%	4.41%	0.10%
[06]	Total system failure	1.99%	7.00%	0.14%
[03]	Data Storage or Recovery Failure	9.92%	0.15%	0.01%
[04]	Data loss while moving QuickTask to the Cloud	7.64%	0.32%	0.02%
[01]	Adversaries obtain Military Data	6.69%	0.31%	0.02%
[05]	Cyber attack which disables or degrades system	4.62%	0.08%	0.004%
[09]	Army loses confidence in data security	3.57%	0.01%	0.0002%
[07]	Appliction adoption failure	3.93%	0.00%	0.00%
[11]	QuickTask move stalled	4.02%	0.00%	0.00%
[12]	Task platform is faulty	2.58%	0.00%	0.00%
[13]	Faulty access	0.02%	0.00%	0.00%

# Controls	Cost of Controls	How Selected
11	$448,000	Manually selected

	Simulated
Total Risk	1.17%
Risk Reduction	0.58%
Residual Risk	0.59%



☑ With Controls ☑ Show Monetary Values (Value of Enterprise: $7,800,000)

Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018: QuickTask Risk Managment Framework
(Controls are manually selected)

No.	Event	All Participants Likelihood Simulated	Impact, $ Simulated	Risk, $ Simulated ▼
[08]	Army losing efficiency while changing applications	7.22%	72,226	5,214
[10]	Storage is mishandled	9.27%	189,443	17,561
[02]	Failure of access/authentication control	2.20%	343,747	7,562
[06]	Total system failure	1.99%	545,695	10,859
[03]	Data Storage or Recovery Failure	9.92%	11,396	1,130
[04]	Data loss while moving QuickTask to the Cloud	7.64%	24,761	1,891
[01]	Adversaries obtain Military Data	6.69%	23,984	1,604
[05]	Cyber attack which disables or degrades system	4.62%	6,431	297
[09]	Army loses confidence in data security	3.57%	469	16
[07]	Appliction adoption failure	3.93%	0	0
[11]	QuickTask move stalled	4.02%	0	0
[12]	Task platform is faulty	2.58%	0	0
[13]	Faulty access	0.02%	0	0

# Controls	Cost of Controls	How Selected
11	$448,000	Manually selected

	Simulated
Total Risk	$91,488
Risk Reduction	$45,350
Residual Risk	$46,138

Conclusively, in managing risk tolerance, we were not willing to have a high risk tolerance by spending money to go over budget even though we may potentially get better results. The 11 controls reduce this risk of going over budget to a tolerable amount. We opted for a low risk tolerance to maintain the budget for our QuickTask application. This risk affected our decision with what controls we were going to choose. The DoD has many applications that are tested but are never rolled out. We didn't want to go over budget for a cloud application that may not be utilized in the near future. Simultaneously, we made sure to use all controls under DoD requirements.