DNSC6254 - Risk Management

Government Travel Credit Card (GTCC)

Risk Analysis

GROUP PROJECT

The George Washington University School of Business

October 2019

by

Blake Helander

and

Luana Bertoletti

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Table of Contents

ABSTRACT

Considering the importance of using the bank-issued Government Travel Credit Card (GTCC) only for appropriate government-related business, the DoD Risk Management Team decided to evaluate what is the overall risk associated with the use of the card, over a one-year period.

The risk analysis has been conducted using Riskion® software and the principles of the Analytic Hierarchy Process (AHP) which produce far more accurate results than from more traditional methods such as “BOGSAT” or assigning ordinal values to likelihood and consequence, which are mathematically meaningless.

The sections that follow describe how the risk model has been structured, present risk analysis results using computed versus simulated results, as well as results with and without controls.

Through strategic implementation of control measures, DoD’s GTCC RM Team successfully lowered the probability and consequence of several risks occurring over the next fiscal year. This will result in cost savings for the program as well as higher likelihood of achieving objectives. Ultimately, the DoD lessened the possibility of laws being broken, negative media stories, and users being unable to access their accounts or pay their bills in a timely fashion.

I. Introduction

Members of the Department of Defense, including uniformed service members of the military, Government Civilians and DoD Contractors are required to appropriately use a bank-issued Government Travel Credit Card (GTCC) for all official government travel and related expenses. The card may only be used when the user is travelling on orders in an official capacity for the U.S. Government, to cover travel related expenses, such as air fare, car rental, hotel, parking, ATM cash withdrawals, food and other incidentals.

Because the GTCC bills are paid by the U.S. Government, i.e. U.S. taxpayers are funding their payment, government officials seek to ensure that the credit cards are only used for appropriate government-related business. In recent years, government

officials noticed an uptick in incidents of GTCC misuse such as users buying goods and services unrelated to official government travel. Also, the threat of cyber-attacks has increased and an event like this could cripple the system's ability to ensure DoD employees can pay for and get reimbursed for official travel.

Considering the importance of this topic, the DoD Risk Management Team decided to evaluate what is the overall risk associated with the use of the GTCC, over a one-year period. The risk analysis has been conducted using Riskion® software and the steps required to develop the model are presented in the sections that follow.

II. Model structure

The first steps for setting up the risk analysis model is to identify some of the risk elements, such as risk events, threats, and consequences to objectives, as described below.

A. Risk events

Risks are uncertain future events that will negatively impact an organization's mission if realized. Risks involve potential losses that matter.

Subject matter experts (SMEs) within the Department of Defense (DoD) identified 11 potential risk events associated with the use of the GTCC card, identified in Figure 1. If any of these events were to occur, the DoD would suffer meaningful losses to their mission objectives. These risks involve accidents, intentional fraud, technological issues or malice on the part of bad actors.

Unique ID		Events
[01]		Credit Limit Exceeded by Users
[02]		Unauthorized users makes purchases (stolen card)
[03]		Hackers improperly access system or clone cards to make unauthorized purchases
[04]		Authorized users make improper purchases by mistake
[05]		Authorized users make improper purchases intentionally
[06]		Cyber attack prevents access to GTCC website
[07]		News Media reports incidents of improper GTCC use
[08]		Users fail to pay bill on time
[09]		Private information of cardholders is stolen by hackers
[10]		Card declined at point of sale when used properly
[11]		Users fail to properly complete voucher to pay bill

Figure 1: Risk events associated with the use of GTCC card

B. Sources & Vulnerabilities Grid

In the risk analysis conducted by the DoD Risk Management Team, all risk events have been associated with at least one threat, allocated in three different categories: Human Error, Criminal Behavior and Technological. Threats are incidents which directly result in risk events occurring. Within these three threat clusters, reside nine specific threats that could lead to one or more risks occurring. Figure 2 illustrates the hierarchy of threats/sources.

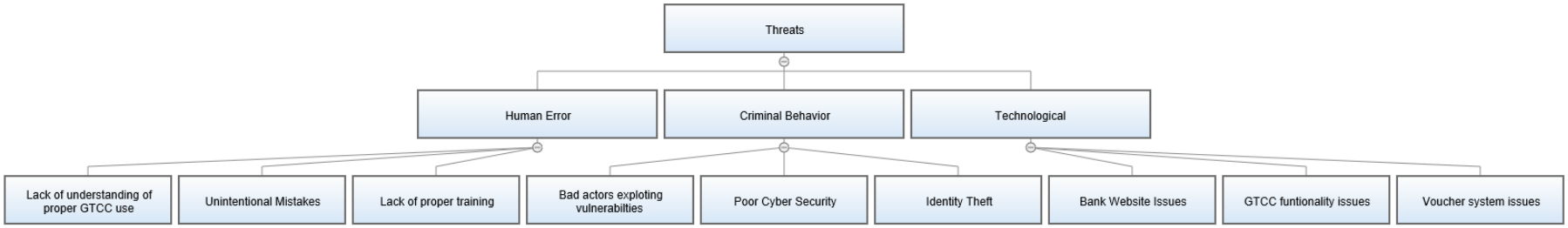


Figure 2: Threats associated with GTCC risk events

Figure 3 illustrates the vulnerabilities grid, through which the Team identified the threats that contribute to the risk events. This logical fashion leads to the establishment of a method that will be later used by the key team members to evaluate the likelihood of events given the threats.

Events	Threats								
	Human Error			Criminal Behavior			Technological		
	Lack of understand	Unintentional Mista	Lack of proper trai	Bad actors explotin	Poor Cyber Securi	Identity Theft	Bank Website Issu	GTCC funtionality	Voucher system is
Credit Limit Exceeded by Users	☑	☑	☑	☐	☐	☐	☑	☑	☑
Unauthorized users makes purchases (stolen card)	☐	☐	☑	☑	☑	☑	☐	☐	☐
Hackers improperly access system or clone cards to make unauthorized purchases	☐	☐	☐	☑	☑	☑	☑	☑	☐
Authorized users make improper purchases by mistake	☑	☑	☑	☐	☐	☐	☐	☐	☐
Authorized users make improper purchases intentionally	☑	☐	☑	☑	☐	☐	☐	☐	☐
Cyber attack prevents access to GTCC website	☐	☐	☐	☑	☑	☑	☑	☑	☐
News Media reports incidents of improper GTCC use	☑	☑	☐	☑	☑	☑	☐	☐	☐
Users fail to pay bill on time	☑	☑	☑	☐	☐	☐	☑	☑	☑
Private information of cardholders is stolen by hackers	☐	☐	☐	☑	☑	☑	☑	☐	☐
Card declined at point of sale when used properly	☑	☑	☑	☐	☐	☐	☐	☑	☐
Users fail to properly complete voucher to pay bill	☑	☑	☑	☐	☐	☐	☑	☐	☑

Figure 3: Vulnerabilities grid - Risk events x threats

C. Objectives & Consequences Grid

Senior leaders identify and communicate their organization's objectives to all of its members. Clearly defined objectives indicate what goals need to be achieved for organizational success. When risk events occur, objectives experience losses and organizations move farther away from the achievement of goals.

The DoD RM Team identified 5 clusters of objectives associated with the GTCC program: Legal, Financial, Reputational, Compliance, and Technical. Included within the hierarchy of objectives are nine sub-objectives. When risks occur, the DoD will likely fail to meet one or more of these objectives. Figure 4 illustrates the hierarchy of objectives.

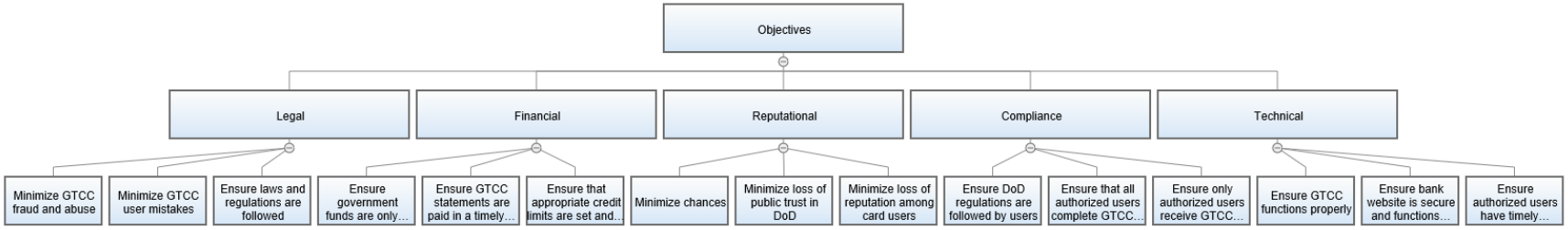


Figure 4: Objectives associated with GTCC risk events

Through the consequences grid illustrated in Figure 5, the RM Team identified the objectives that are negatively impacted by the different risk events. Similarly to the vulnerabilities grid described above, these relationships will be used to collect the evaluation of the team members on the risk events consequences to the objectives.

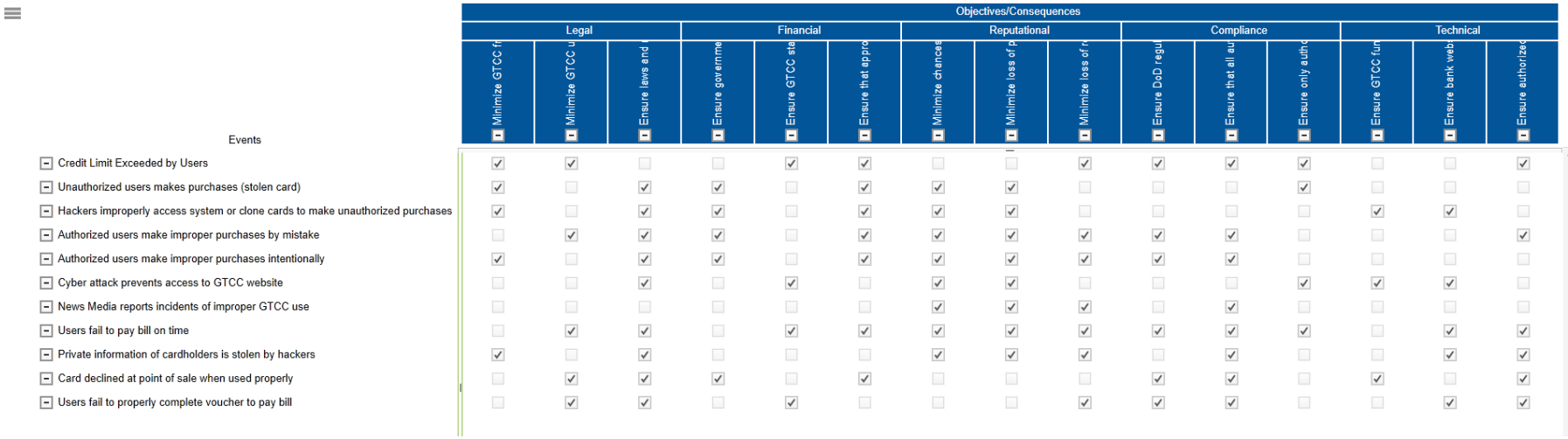


Figure 5: Consequences grid - Risk Events x objectives

D. Measurement Methods

The DoD RM Team evaluated the likelihood of threats and risk events, and the objectives priority and consequences using the following methods:

1. Threats likelihood: pairwise comparison (between categories) and rating scale (within categories);
2. Risk events likelihood: rating scale;
3. Priority of objectives: pairwise comparison;
4. Consequences to objectives: rating scale.

The rating scale method involves the use of specified intensities (example: low, moderate, and high) associated with defined

likelihoods/ impacts. The pairwise comparison involves defining priorities for the cluster of threats/objectives as well within the clusters. Figure 6 illustrates the methods selected to measure the likelihood of threats.

Measure Event Likelihoods	Measurement Type Default: Rating Scale	Measurement Scale or Given Likelihood	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# D (
◢ Threats						
◢ Human Error						
Lack of understanding of proper GTCC u	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	7	7	
Unintentional Mistakes	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	6	6	
Lack of proper training	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	7	7	
◢ Criminal Behavior						
Bad actors exploting vulnerabilties	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	6	6	
Poor Cyber Security	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	5	5	
Identity Theft	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	5	5	
◢ Technological						
Bank Website Issues	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	6	6	
GTCC funtionality issues	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	5	5	
Voucher system issues	Rating Scale	MID LIKELIHOOD RATING SCALE	Copy Edit	3	3	

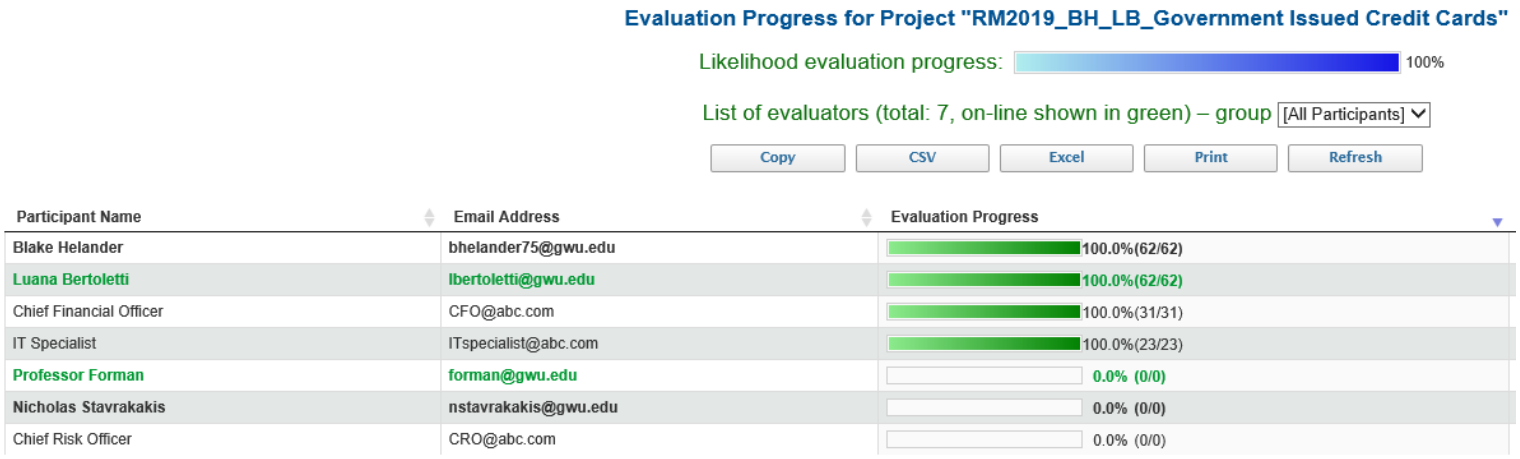
Figure 6: Example of measurement methods - Likelihood of threats

E. Participant roles

The participants chosen to evaluate the sources, risks and objectives include two Project Managers (Blake and Luana), the Chief Risk Officer, the Chief Financial Officer, and the Chief Information Officer. The evaluations can be tailored so that subject matter experts only make judgements based on their own specific expertise. In this case the PMs evaluated all judgements while the other participants evaluated only the judgements related to their specialty.

Figure 7 and Figure 8 illustrate the evaluations assigned to the Chief Financial Officer (cells in green), and an example of the evaluation progress, which indicates different number of judgements required based on the team member expertise.

Figure 7: Evaluation grid - green cells indicate evaluations that should be performed by SME



Participant Name	Email Address	Evaluation Progress
Blake Helander	bhelander75@gwu.edu	100.0%(62/62)
Luana Bertoletti	lbertoletti@gwu.edu	100.0%(62/62)
Chief Financial Officer	CFO@abc.com	100.0%(31/31)
IT Specialist	ITspecialist@abc.com	100.0%(23/23)
Professor Forman	forman@gwu.edu	0.0% (0/0)
Nicholas Stavrakakis	nstavrakakis@gwu.edu	0.0% (0/0)
Chief Risk Officer	CRO@abc.com	0.0% (0/0)

Figure 8: Evaluation progress - Overall and per SME

III. Risk evaluation without controls

A. Computed risks

The evaluation results, illustrated in Figure 9, revealed which events could result in the highest likelihood and consequence for the DoD. The risk ranking shows that “Hackers improperly accessing system” and “Private information of cardholders stolen by hackers” are the two highest level risks that the team should be most concerned about. It is important to understand which risks are the most problematic because there are not enough financial resources available to mitigate all risk. Senior leaders must make informed decisions about which risks to dedicate limited resources to in order to lower their probability and impact. At this time no control measures have been implemented.

Overall Likelihoods, Impacts, and Risks for RM2019_BH_LB_Government Issued Credit Cards

No.	Event	All Participants Likelihood Computed	All Participants Impact Computed	All Participants Risk Computed ▼
[03]	Hackers improperly access system or clone cards to make unauthorized purchases	14.49%	41.43%	6.00%
[09]	Private information of cardholders is stolen by hackers	16.15%	30.46%	4.92%
[02]	Unauthorized users makes purchases (stolen card)	16.18%	26.65%	4.31%
[06]	Cyber attack prevents access to GTCC website	13.71%	30.16%	4.13%
[08]	Users fail to pay bill on time	15.46%	16.19%	2.50%
[05]	Authorized users make improper purchases intentionally	5.90%	37.03%	2.18%
[11]	Users fail to properly complete voucher to pay bill	13.82%	13.94%	1.93%
[04]	Authorized users make improper purchases by mistake	9.39%	18.78%	1.76%
[01]	Credit Limit Exceeded by Users	6.05%	19.24%	1.16%
[10]	Card declined at point of sale when used properly	7.79%	10.36%	0.81%
[07]	News Media reports incidents of improper GTCC use	4.48%	11.21%	0.50%
			Computed Total Risk	30.22%

Figure 9: Risk events ranked based on overall computed risks - no controls implemented

B. Simulated risks

Next, the RM Team determined what could potentially occur through running Monte Carlo simulations to estimate the probability that a combination of risks could fire when no resources were dedicated to control measures. Monte Carlo simulations are important since they account for the "flaw of averages", meaning that they avoid double counting by assuming that a risk event will be fired by the occurrence of one threat at a time. When occurrences of risk are "double counted" then each individual likelihood values can add up to exceed 100% and predictions became less realistic. Figure 10 illustrates the results of 10,000 simulations.

Overall Likelihoods, Impacts, and Risks for RM2019_BH_LB_Government Issued Credit Cards

No.	Event	All Participants Likelihood Simulated	Impact Simulated	Risk Simulated ▼
[03]	Hackers improperly access system or clone cards to make unauthorized purchases	13.45%	27.93%	3.76%
[09]	Private information of cardholders is stolen by hackers	15.09%	21.17%	3.19%
[02]	Unauthorized users makes purchases (stolen card)	14.82%	19.23%	2.85%
[06]	Cyber attack prevents access to GTCC website	12.64%	21.65%	2.74%
[08]	Users fail to pay bill on time	14.60%	13.87%	2.02%
[05]	Authorized users make improper purchases intentionally	5.66%	27.71%	1.57%
[11]	Users fail to properly complete voucher to pay bill	12.73%	11.71%	1.49%
[04]	Authorized users make improper purchases by mistake	9.08%	16.05%	1.46%
[01]	Credit Limit Exceeded by Users	5.80%	16.09%	0.93%
[10]	Card declined at point of sale when used properly	7.09%	9.03%	0.64%
[07]	News Media reports incidents of improper GTCC use	4.52%	6.84%	0.31%
				Simulated
			Total Risk (Average Loss)	20.96%

Figure 10: Risk events ranked based on overall simulated risks - no controls implemented

C. Bow-tie diagram

A bow-tie diagram shows the probability of each threat contributing to a risk event and also shows the level of consequence to objectives if the risks were to occur. The diagram in Figure 11 shows the likelihood and vulnerability to the highest Risk in the register and the resulting consequences and the loss to objectives (if this risk fired). Though the probability of hackers accessing the system is relatively low, the Impact is quite high and would have a considerable adverse impact on DoD's mission objectives.

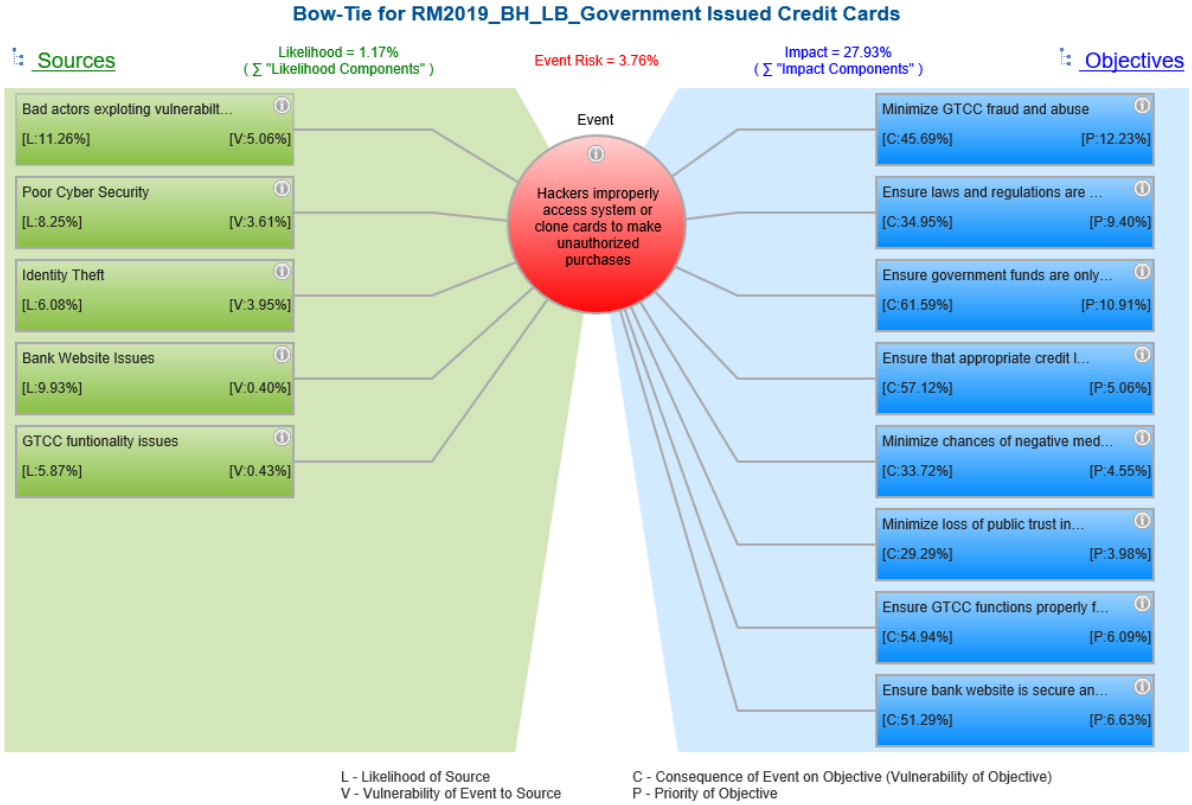


Figure 11: Bow-tie diagram for the highest ranked risk associated with hackers improperly accessing system

D. Heat Map

A heat map displays where risks lie on a spectrum of importance where the green zone is low, yellow is medium and red is high. The risk model developers can define the colored regions of the heat map and indicate what are the risk ranges associated with those. The RM Team hopes that the Risks (represented by circles) can be brought closer to the lower left-hand corner (green zone area) through the strategic implementation of controls.

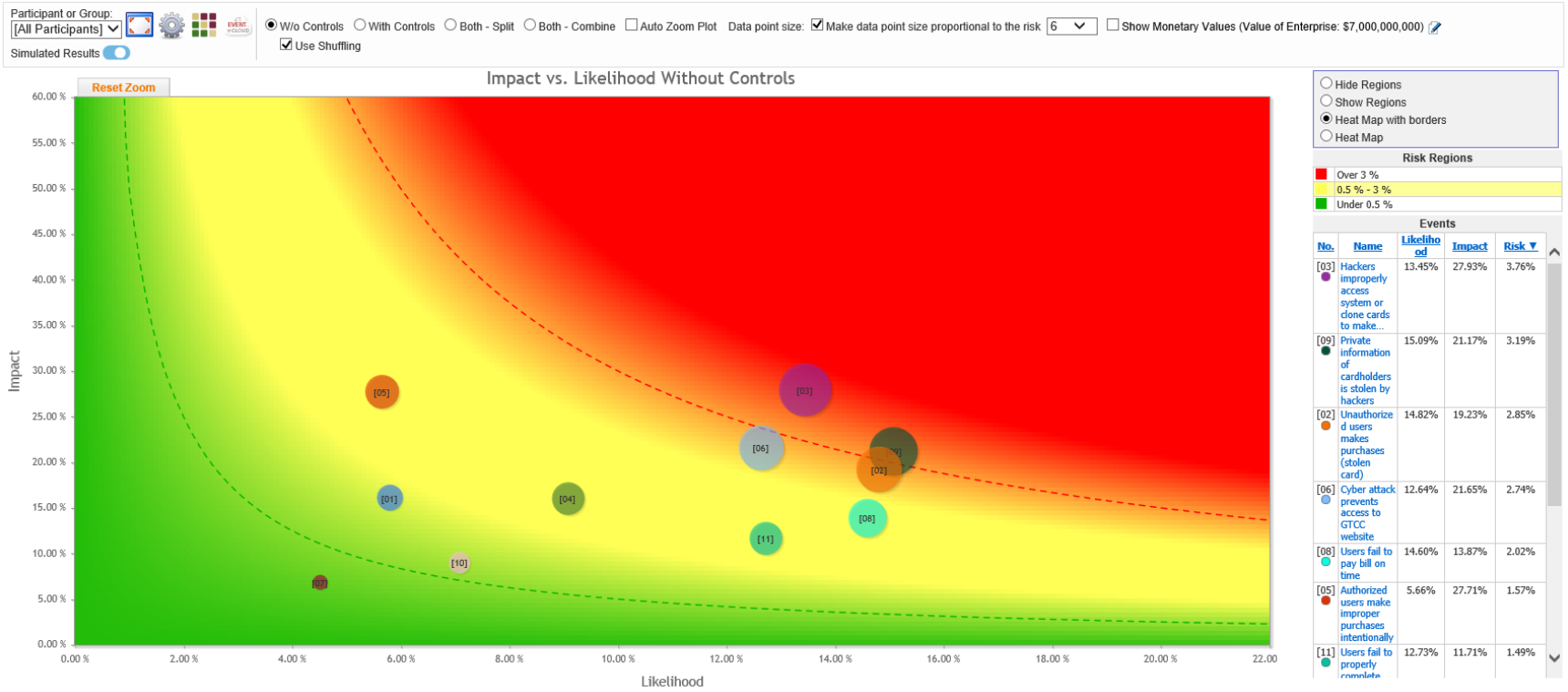


Figure 12: Heat map for simulated risk results without controls

E. Loss Exceedance Curve

A loss exceedance curve shows the probability that various levels of loss will occur and informs management on the level of risk they are willing to take (risk tolerance). After running simulations, results show that the average loss due to risks occurring is 20.96% of the program's total value, as indicated in Figure 13. The loss exceedance curve also shows that there is a 40% chance of a loss of more than 15%, and a 5% chance that losses from risks will exceed 73%. The risk is far too high, and the RM Team decided that controls must be added to reduce risk levels.

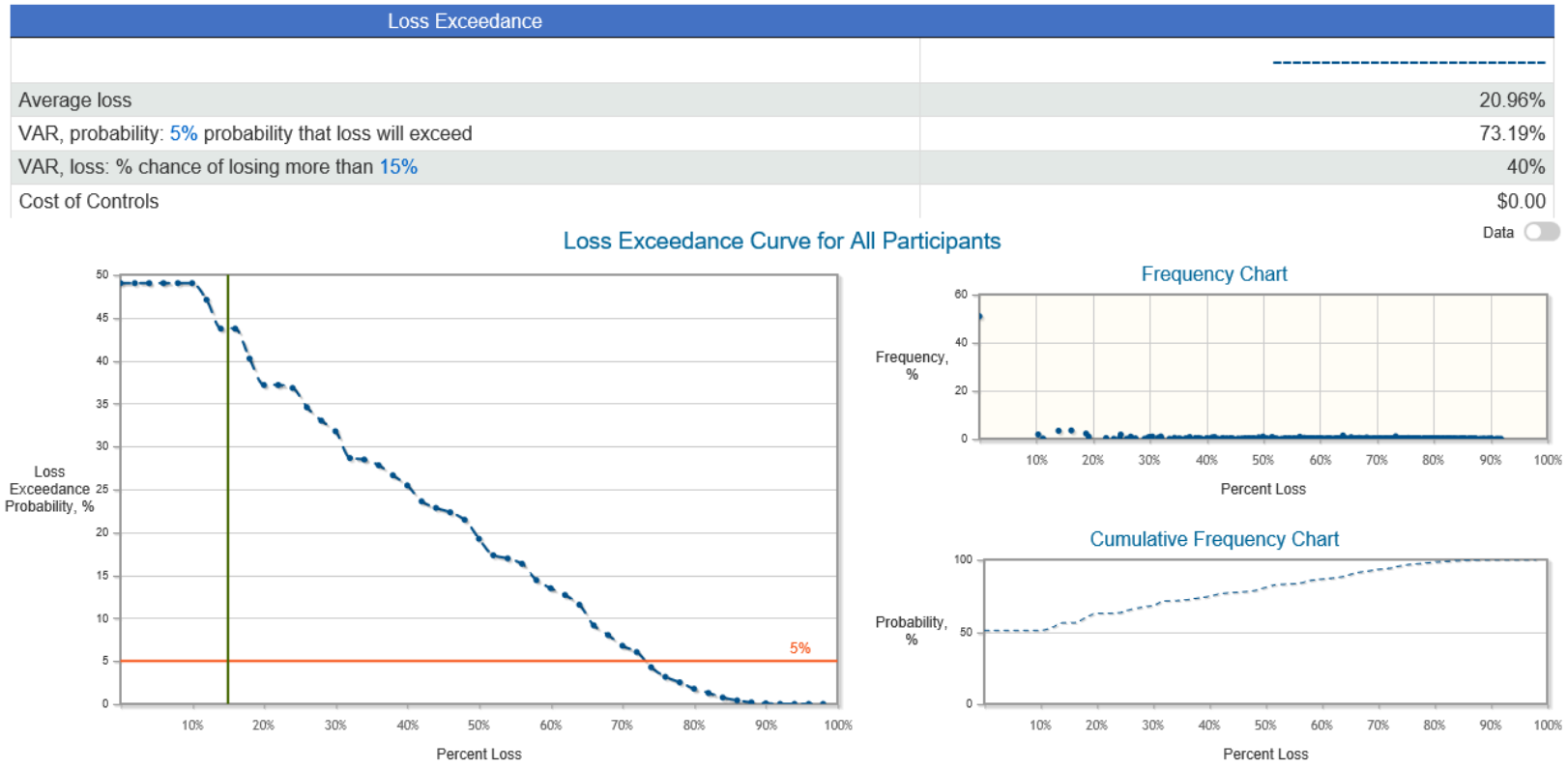


Figure 13: Loss exceedance curve for simulated risk results without controls

IV. Controls (source/events/objectives)

Controls are the mechanisms, rules and procedures implemented by an organization to ensure the integrity of financial and non-financial information, hold people accountable, and minimize fraud. Simply put, controls ensure that what is supposed to happen, does happen. Controls can involve checks and balances, security measures, levels of approval, physical items such as locks and security cameras and providing training (among other things). Effective controls measures lower risk and raise the probability of the success of an organization's critical business processes. The RM Team identified 20 control measures for sources (threats), vulnerabilities (risks) and consequences to objectives, listed in Figure 14. Though controls are expensive to implement they will likely pay for themselves due to the money saved from risks not occurring. A mistake senior leaders make too often is to not implement sufficient critical control measures since the risks may not occur. Humans are "loss averse" by nature meaning that they do not want to invest for future negative events. The Monte Carlo simulations show that though most of the time risks may not occur, they will eventually. In general, when risks do occur, the cost to fix the damage is far greater than the control measures would have been.

Controls for "RM2019_BH_LB_Government Issued Credit Cards"

Selected controls: 9
Cost Of Selected Controls: $326,000,000 (unfunded: $685,000,000)
Total Cost Of All Controls: $1,011,000,000

Index		Control Name	Control for	Selected	Cost	Applications	Categories	Must	Must Not
01	☐	Required annual training for all users	Source	Yes	75000000	3		☑	☐
05	☐	Continuous updates of anti-virus software	Source	Yes	150000000	4		☑	☐
06	☐	Require 30-day password update for users	Source	Yes	5000000	4		☑	☐
09	☐	Implement penalties for abuse	Source	Yes	20000000	3		☑	☐
11	☐	Required annual training for all users	Vulnerability	Yes	0	3		☑	☐
13	☐	Continuous updates of anti-virus software	Vulnerability	Yes	0	3		☑	☐
02	☐	Initial training requirement prior to get card	Source		75000000	3		☐	☐
03	☐	Remedial training requirement when users make mistakes	Source		45000000	1		☐	☐
04	☐	DOD partnership with federal law enforcement	Source		50000000	4		☐	☐
07	☐	Purchase limits on GTCC	Source	Yes	1000000	1		☐	☐
08	☐	24-hour free customer service line for users	Source	Yes	75000000	8		☐	☐
10	☐	24 hours technical support for website issues	Source		100000000	4		☐	☐
12	☐	24-hour free customer service line for users	Vulnerability	Yes	0	3		☐	☐
14	☐	DOD partnership with federal law enforcement	Vulnerability		0	3		☐	☐
15	☐	24 hour technical support for website issues	Vulnerability		0	3		☐	☐
16	☐	Public Relations effort to respond to negative publicity	Consequence		50000000	3	Reputational	☐	☐
17	☐	Inspector General Audit	Consequence		50000000	9	Compliance	☐	☐
18	☐	Legal Reviews by Office of the General Council	Consequence		65000000	5	Legal	☐	☐
19	☐	Ernst and Young financial audit	Consequence		100000000	4	Financial	☐	☐
20	☐	Hire additional IT Contractors in case of Cyber Attack	Consequence		150000000	7	Technical	☐	☐

Figure 14: Controls for threats, risk events, and consequences to the objectives

A. Controls Dependencies

Considering that some of the controls identified by the DoD RM Team are common to threats and risk events, the team identified their dependencies in Riskion® (Figure 15) so that their cost is only accounted for one time. Such controls may be selected either manually or via optimization. It is important to note that even though some controls are shared between threats and sources their effectiveness may be different. For example, a control measure for a risk may have a different level of effectiveness than the same measure has for a source.

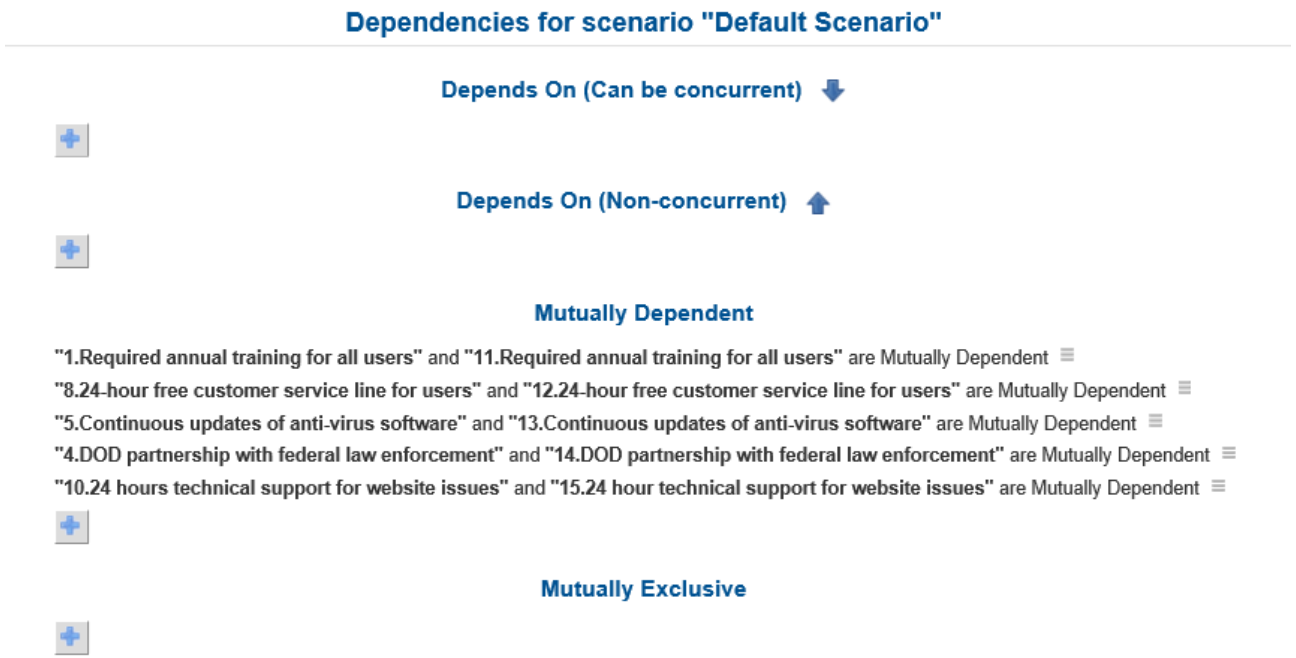


Figure 15: Controls dependencies in Riskion®

B. Measurement methods

The DoD RM Team evaluated the controls effectiveness using the direct input method. Figure 16 illustrates the selection of the measurement method for the source controls.

Measurement Methods for Controls for Sources

Control Name	Threats								
	Human Error			Criminal Behavior			Technological		
	Lack of understanding of proper GTCC use	Unintentional Mistakes	Lack of proper training	Bad actors exploting vulnerabilties	Poor Cyber Security	Identity Theft	Bank Website Issues	GTCC funtionality issues	Voucher system issues
01. Required annual training for all users	Direct	Direct	Direct						
02. Initial training requirement prior to get card	Direct	Direct	Direct						
03. Remedial training requirement when users make mistakes	Direct								
04. DOD partnership with federal law enforcement				Direct	Direct	Direct	Direct		
05. Continuous updates of anti-virus software				Direct	Direct	Direct	Direct		
06. Require 30-day password update for users				Direct	Direct	Direct	Direct		
07. Purchase limits on GTCC		Direct							
08. 24-hour free customer service line for users	Direct	Direct	Direct	Direct		Direct	Direct	Direct	Direct
09. Implement penalties for abuse	Direct			Direct		Direct			
10. 24 hours technical support for website issues					Direct		Direct	Direct	Direct

Figure 16: Measurement method selection for source controls

C. Controls effectiveness

Figure 17 illustrates the effectiveness values used for the source controls. As an example, if the required annual training for all users is selected as one of the source controls, it reduces the likelihood of “Lack of understanding of proper GTCC use” by 60%. Subject Matter Experts for the DoD GTCC were interviewed in order to capture the estimates for control effectiveness.

Effectiveness of Source Controls

Control Name	Threats								
	Human Error			Criminal Behavior			Technological		
	Lack of understanding of proper GTCC use	Unintentional Mistakes	Lack of proper training	Bad actors exploting vulnerabilties	Poor Cyber Security	Identity Theft	Bank Website Issues	GTCC funtionality issues	Voucher system issues
01. Required annual training for all users	0.6	0.6	0.5						
02. Initial training requirement prior to get card	0.7	0.6	0.6						
03. Remedial training requirement when users make mistakes	0.8								
04. DOD partnership with federal law enforcement				0.4	0.33	0.4	0.1		
05. Continuous updates of anti-virus software				0.95	0.9	0.8	0.5		
06. Require 30-day password update for users				0.4	0.33	0.33	0.2		
07. Purchase limits on GTCC		0.75							
08. 24-hour free customer service line for users	0.75	0.65	0.75	0.75		0.75	0.85	0.8	0.75
09. Implement penalties for abuse	0.6			0.6		0.7			
10. 24 hours technical support for website issues					0.6		0.75	0.7	0.8

Figure 17: Effectiveness of source controls

D. Efficient Frontier

Efficient Frontier is a type of report which clearly indicates the optimal level of financial resources that should be allocated to reduce risk. The DoD RM Team used the optimization method for selecting controls for threats, risk events, and consequences to objectives. Through this method, one can ensure that the lowest risk is achieved for given a specific limited budget.

Based on the Efficient Frontier analysis illustrated in Figure 18, by funding up to $350 million for controls, the average risk loss is reduced in 19.88% (residual risk on 1.09%) and the probability of risk losses greater than 15% reduced from 43.73% to 2.80%. The risk analysis for control costs of $326 million is presented on item V. The Efficient Frontier data clearly shows that

the optimal amount of money that should be spent on controls is $326 million. Spending more than this amount would not lower the probability of risks occurring to a great enough degree to justify the extra expenditure. The RM Team will present the findings to leadership and recommend that budgeting $326 million towards implementing control measures will end up saving far more money in the long run.

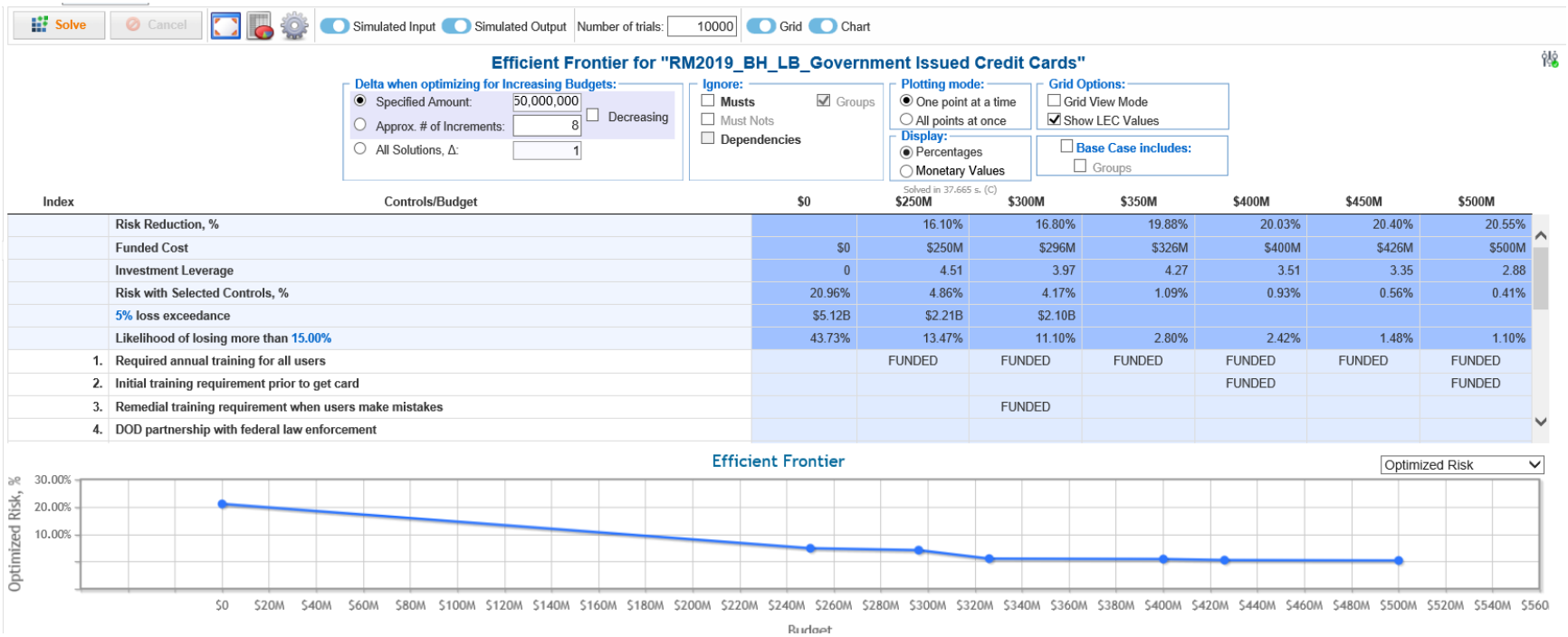


Figure 18: Efficient Frontier analysis

V. Risk evaluation with optimized controls

The risk analysis without controls, previously presented on item 0, indicated that the “Hackers improperly accessing system” and “Private information of cardholders stolen by hackers” were the two highest level risks. After the implementation of the control measures, those two risks were significantly reduced from 3.76% to 0.14% and 3.19% to 0.11%, respectively, and are no longer the two highest risks related to the use of the GTCC.

Overall Likelihoods, Impacts, and Risks (With Controls) for RM2019_BH_LB_Government Issued Credit Cards
(Controls are optimized based on simulated input and output)

No.	Event	All Participants Likelihood Simulated	Impact Simulated	Risk Simulated ▼
[11]	Users fail to properly complete voucher to pay bill	1.63%	12.82%	0.21%
[08]	Users fail to pay bill on time	1.29%	14.74%	0.19%
[03]	Hackers improperly access system or clone cards to make unauthorized purchases	0.40%	33.88%	0.14%
[09]	Private information of cardholders is stolen by hackers	0.43%	25.33%	0.11%
[02]	Unauthorized users makes purchases (stolen card)	0.41%	22.53%	0.09%
[05]	Authorized users make improper purchases intentionally	0.27%	34.16%	0.09%
[10]	Card declined at point of sale when used properly	0.75%	9.92%	0.07%
[01]	Credit Limit Exceeded by Users	0.36%	17.55%	0.06%
[06]	Cyber attack prevents access to GTCC website	0.25%	24.69%	0.06%
[04]	Authorized users make improper purchases by mistake	0.30%	17.53%	0.05%
[07]	News Media reports incidents of improper GTCC use	0.07%	8.09%	0.01%

# Controls	Cost of Controls	How Selected
9	$326,000,000	Optimized based on simulated input and output with budget of $350,000,000

	Simulated
Total Risk (Average Loss)	20.96%
Risk Reduction	19.88%
Residual Risk	1.09%
Investment Leverage	4.27

Likelihood (L) Impact (I) Risk (R)

Figure 19: Risk events ranked based on overall simulated risks - optimized controls implemented

A. Bow-Tie Diagram

The diagram in Figure 20 shows the likelihood and vulnerability to the highest Risk in the register and the resulting consequences and the loss to objectives. After selecting the optimized controls, the highest ranked risk is “Users fail to properly complete voucher to pay bill”, which was ranked at seventh place before the control’s implementation.

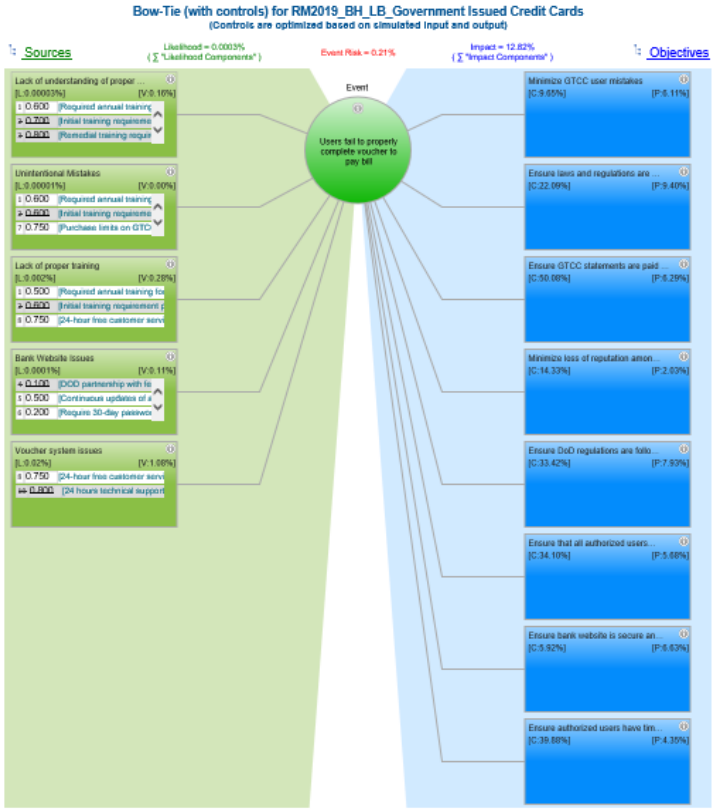


Figure 20: Bow-tie diagram for the highest ranked risk associated with users failing to properly complete voucher to pay bill

B. Heat Map comparison - With and without controls

After the implementation of the control measures, all risk events lie on the green zone of the heat map (Figure 21), which was the desired outcome of the process. This great reduction on the risk levels can be attributed to the fact that most of the controls selected by the optimization process are the ones with the highest effectiveness in reducing the threats/risk events likelihoods.

From the comparison of the heat maps with (right) and without controls (left) it is possible to infer that the controls selected via optimization were more effective in reducing the risk events likelihoods than their impact on the objectives.

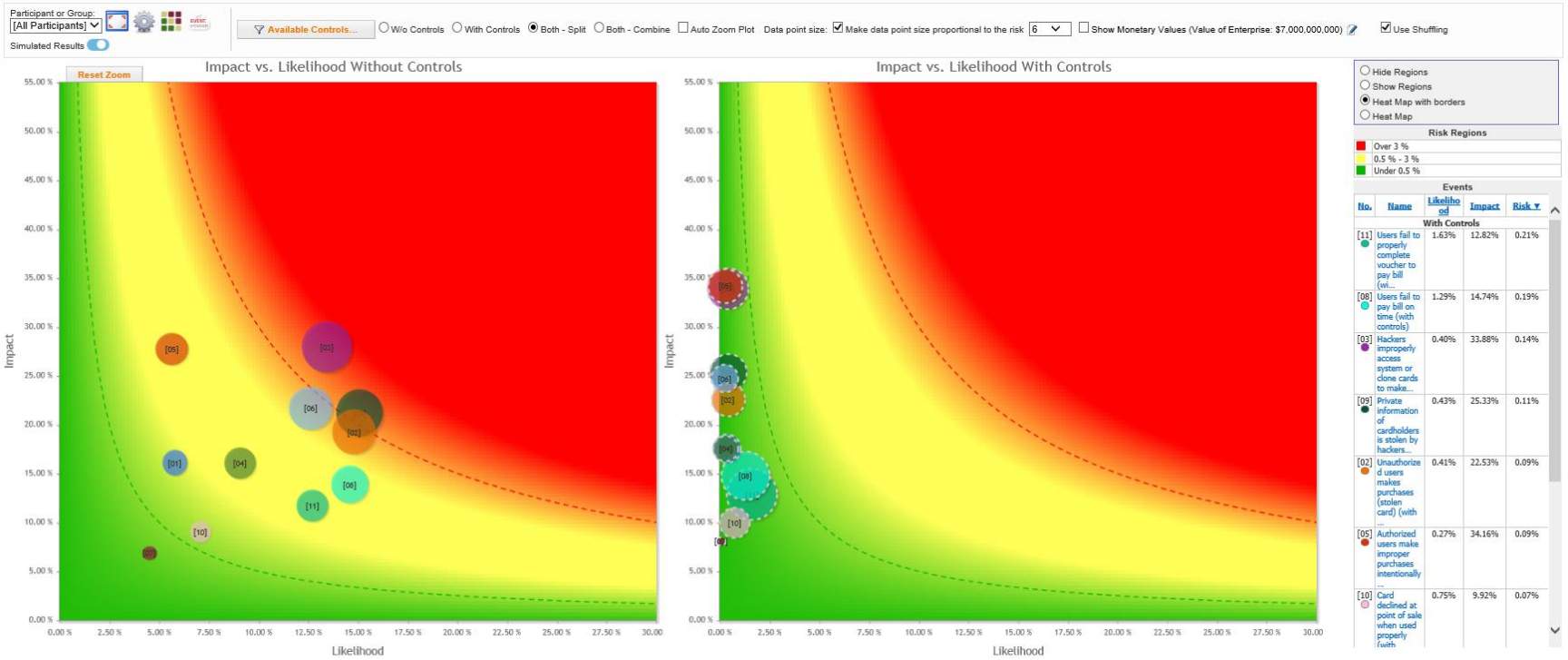


Figure 21: Heat map for simulated risk results with (right) and without (left) controls

VI. Conclusion and Lessons Learned

From the risk analysis presented in this paper, it is evident that decision making utilizing the principles of the Analytic Hierarchy Process (AHP) will produce far more accurate results than from more traditional methods such as “BOGSAT” or assigning ordinal values to likelihood and consequence, which are mathematically meaningless. Another important aspect of risk evaluation is defining project participants roles, so that experts only make judgements on their specific areas, allowing for more meaningful output of data. Also, evaluating the importance of objectives using ratio-scale measures and choosing the best alternatives through expert judgements and pairwise comparisons produces meaningful scientific data to inform managers’ decisions.

When performing risk analysis utilizing the principles of AHP, it is also important to use simulated rather than computed results, which eliminates double-counting and provides a more realistic risk analysis.

When it comes to controls selection, a combination of manually adding and taking away controls in addition to utilizing the Optimization method will provide managers with a variety of helpful what-if scenarios. The use of sensitivity analysis related to control measures, such as Efficient Frontier, helps inform decision makers on the optimal amount to spend on controls and will aid leadership with defining risk tolerance (i.e. what level of risk can we live with?).

Through strategic implementation of control measures, DoD’s GTCC RM Team successfully lowered the probability and consequence of several risks occurring over the next fiscal year. This will result in cost savings for the program as well as higher likelihood of achieving objectives. Ultimately, the DoD lessened the possibility of laws being broken, negative media stories, and users being unable to access their accounts or pay their bills in a timely fashion.

VII. References

Forman, E. H., Forman, H. S., & Ludden, E. A. (2019). *Risks-We-Face and Risks-We-Take - Enterprise Risk Management.* Unpublished manuscript.