Software Engineering Institute

Managing Cyber Risks

Express Control Impact and Risk Analysis

Muhammad Bin Oiad - Yaman Yu - Lucas Falivene - Fabio Beltran Vasquez - Sarah Sha

Advised by Brett Tucker

Carnegie Mellon University
HeinzCollege
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Sarah Sha | *Project Manager*

Fabio Beltran Vasquez | *Financial Manager*

Yaman Yu | *Data Science Lead*

Muhammad Bin Oiad | *Technical Lead*

Lucas Falivene | *R&D Lead*

Brett Tucker | *Advisor*

Carnegie Mellon University
HeinzCollege
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Agenda

Background

Project Scope

Process

Q&A

Background

National Institute of Standards and Technology (NIST) 800-53

- Catalog of controls for all U.S. federal information systems
- Established to provide guidance for the protection of agency- and citizen-owned private data

Companies have existing Enterprise Risk Management (ERM) Process

- Risk Appetite definitions
- Threats and Risk Identification

Problem Statement

Struggle to answer the following questions:

How much less risk will we have if we spend a given budget on certain security controls?

Which controls should be prioritized and implemented?

Objective

Develop a method and tool to help analyze the impact a given set of controls has on cyber risks estimation

Scope

Purpose

Helps determine how much less risk an organization will have if certain controls are implemented and reduce financial loss

Building blocks

Factor Analysis of Information Risk (FAIR)

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro from SEI

Threat Assessment & Remediation Analysis (TARA) from MITRE

NIST Cybersecurity Framework

NIST SP 800-53 controls

Expected Outputs

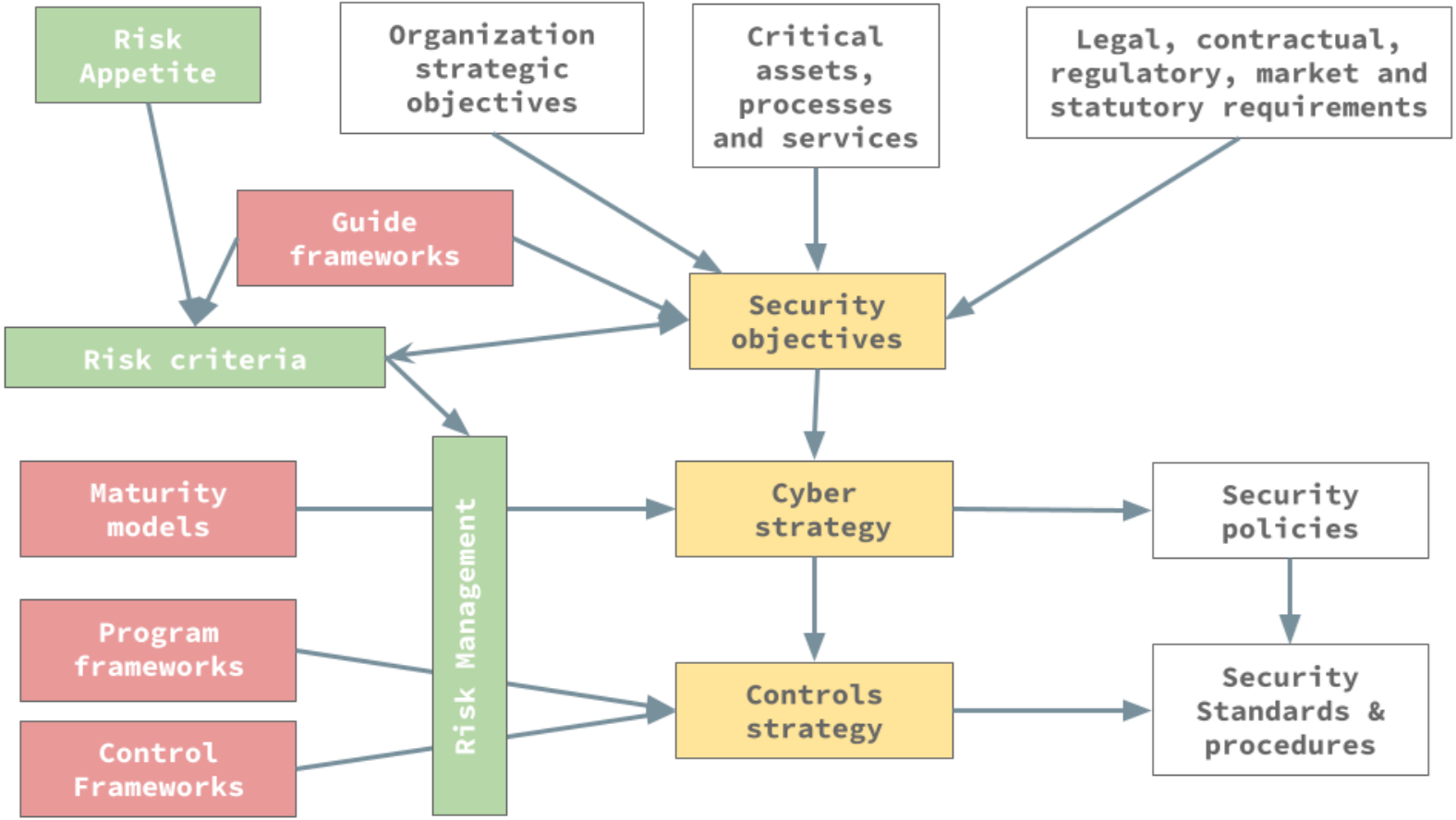
Cybersecurity strategy development

Prioritization of compliance, plans, and investments

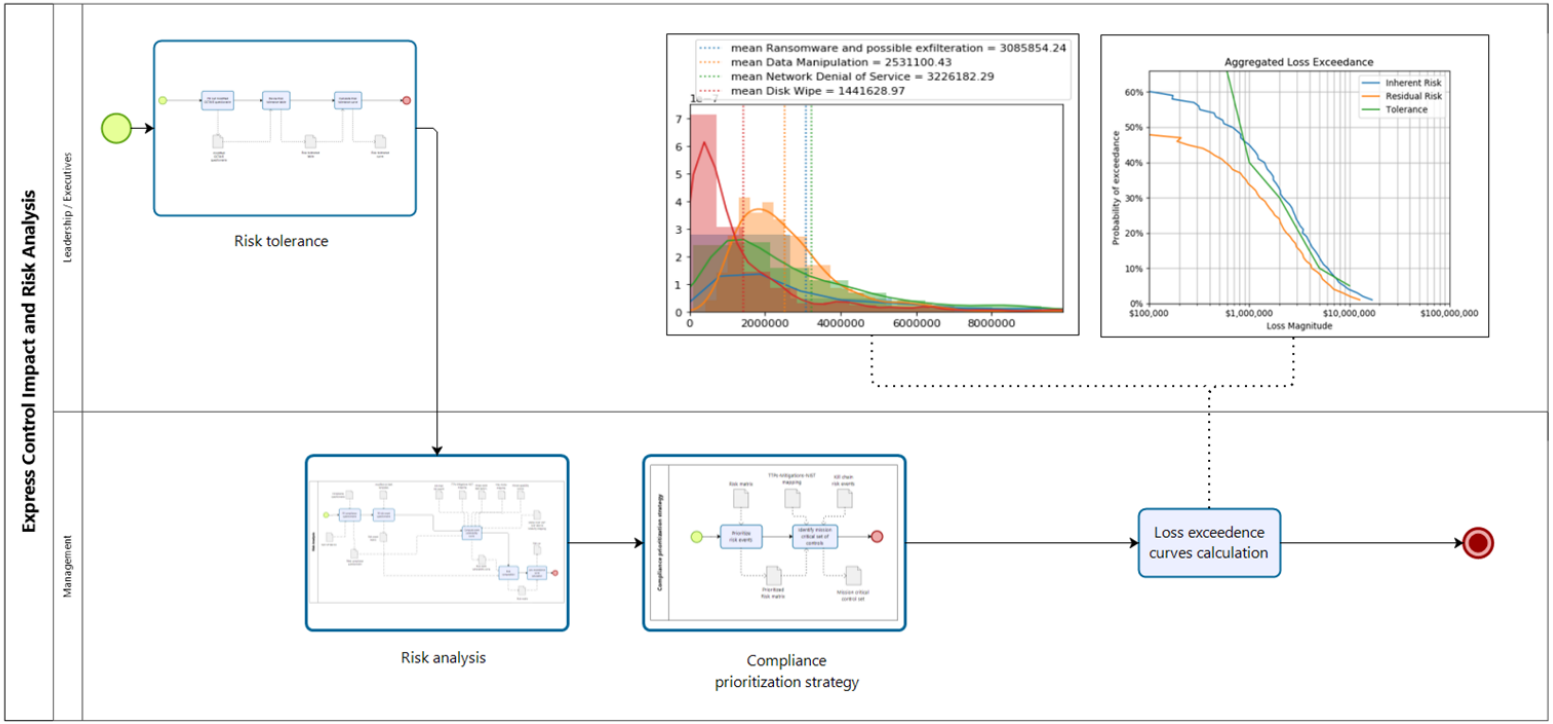
Risk based decision making

Budget allocation & justification

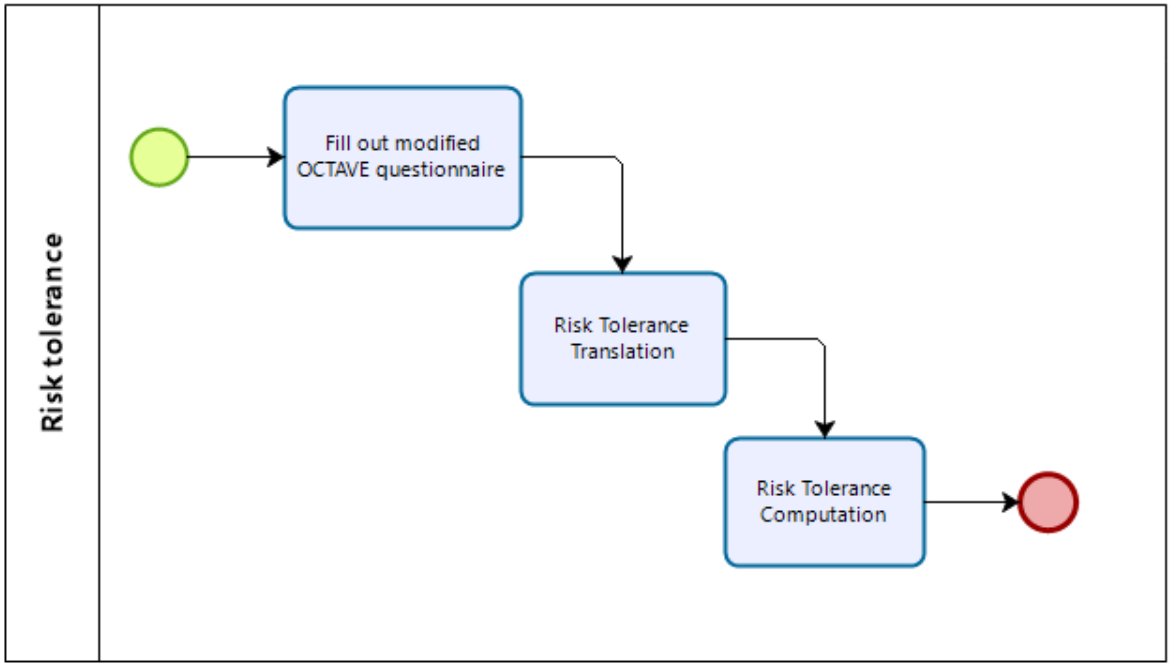
How does ECI&RA helps CISOs?



Macroprocess



Stage I: Risk Tolerance

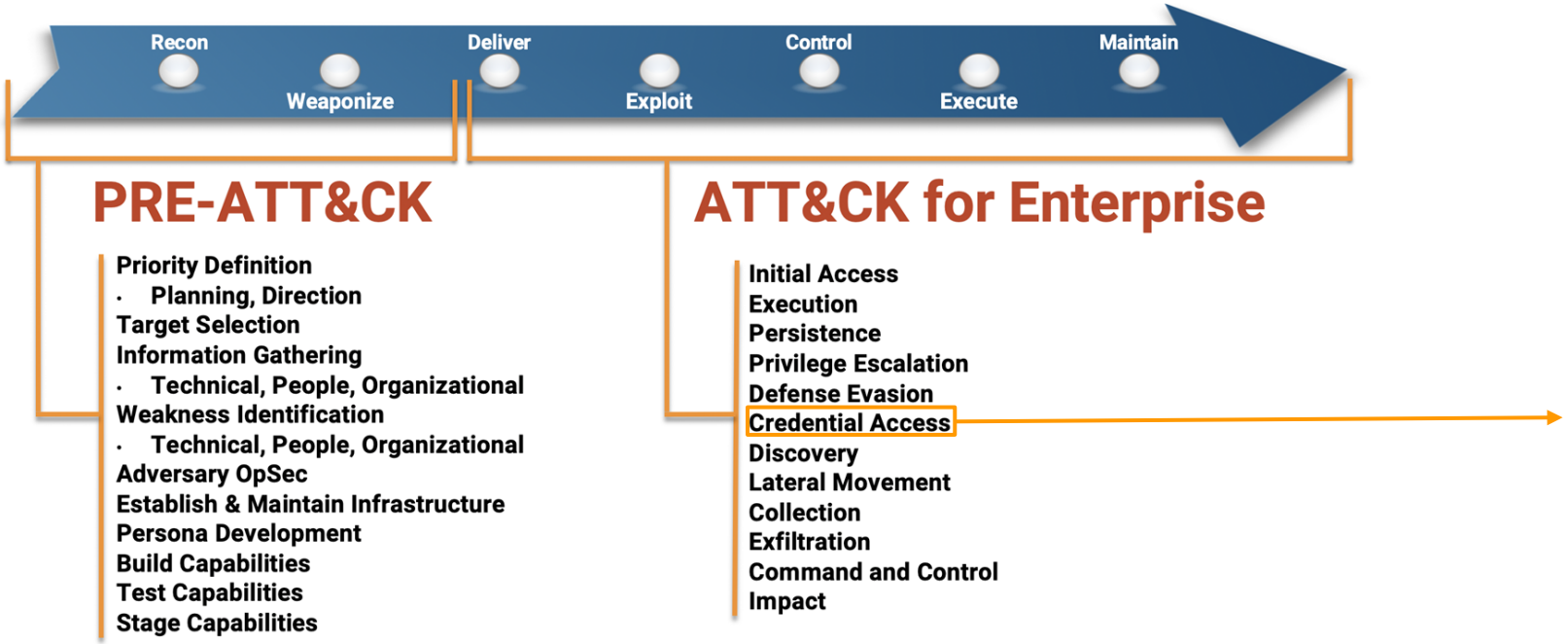


Pre-Defined Risk Events for Stage II

The project will consist of a list of predefined loss events that are depicted from MITRE impact and exfiltration tactics.

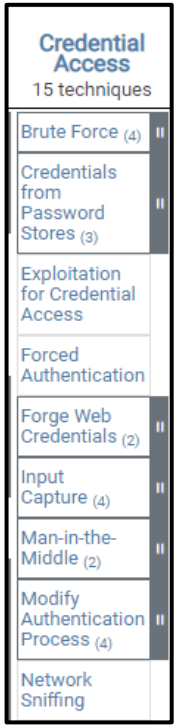
The events will consist of MITRE tactics, techniques, and procedures (TTPs) to complete a cyber kill chain for each.

MITRE - Tactics and Cyber Kill-Chain

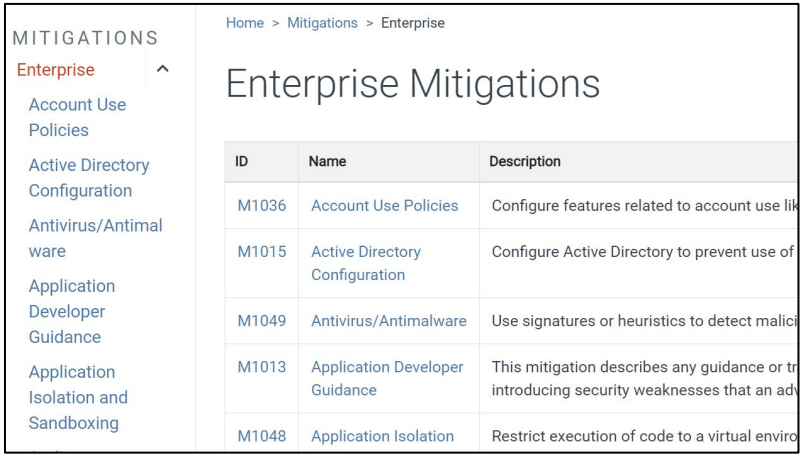


MITRE - Techniques and Mitigation

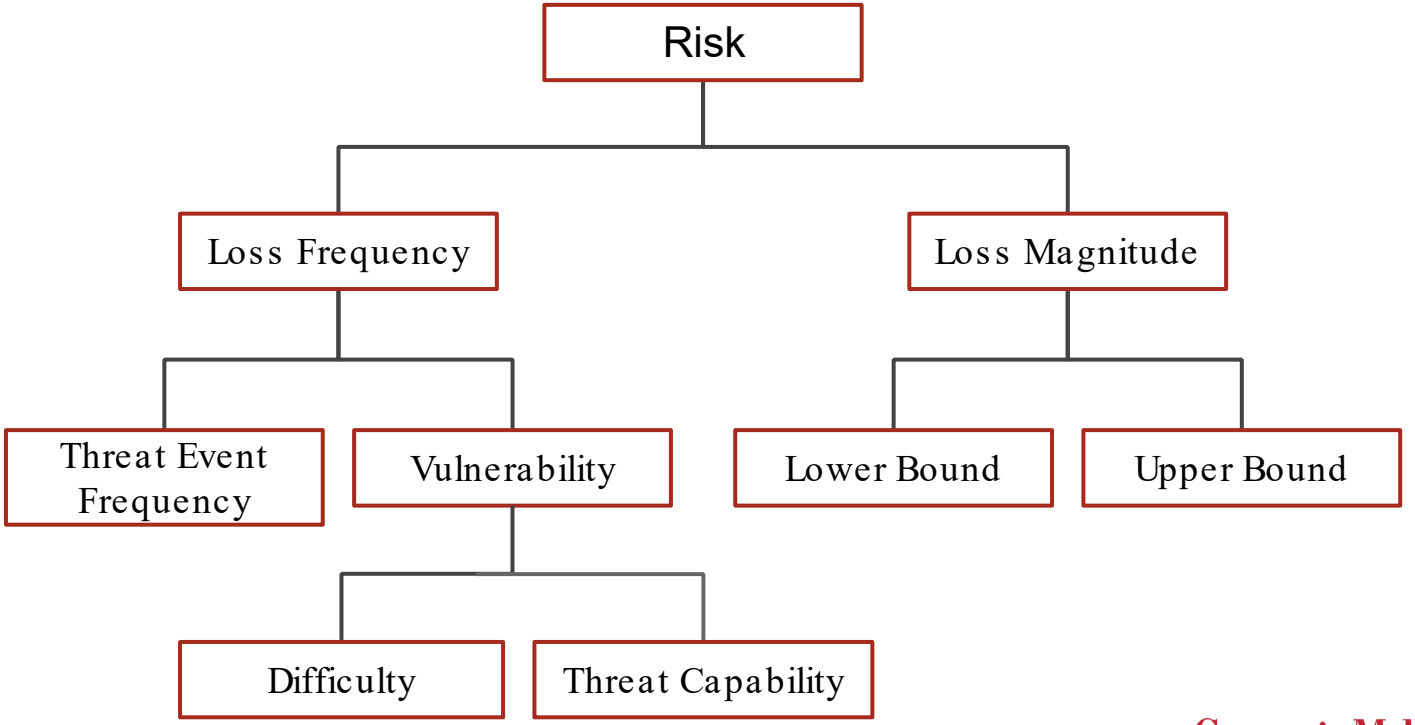
Adversary techniques library for all attack phases



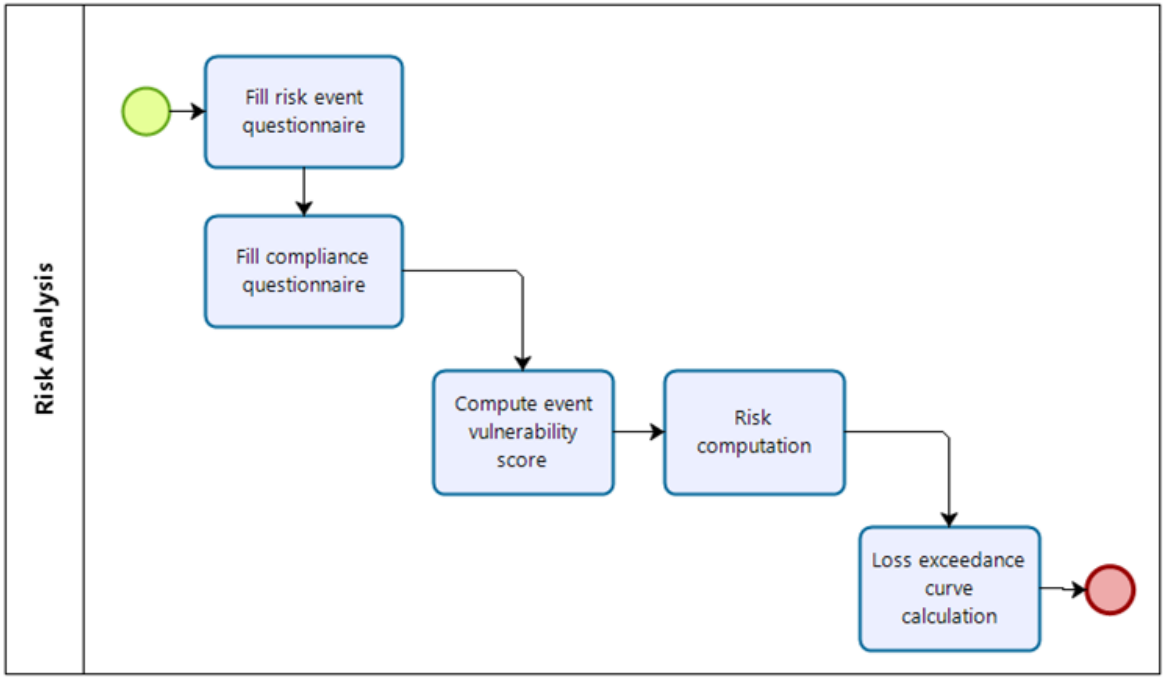
For all adversary techniques Mitre proposed 42 mitigation strategies



Factor Analysis of Information Risk (FAIR)



Stage II: Risk Analysis



Stage II: Risk Event Questionnaire

Frameworks

OCTAVE Allegro templates

Questionnaires

Amended OCTAVE Allegro templates

For Event X

what is your expected losses and threat event frequency (TEF)

Output

For each risk event

Upper and lower boundaries for impact

Threat Event Frequency (TEF)

Stage II: Compliance Questionnaire

Frameworks

NIST 800.53 controls

Questionnaires

Controls compliance questionnaire

For Control X

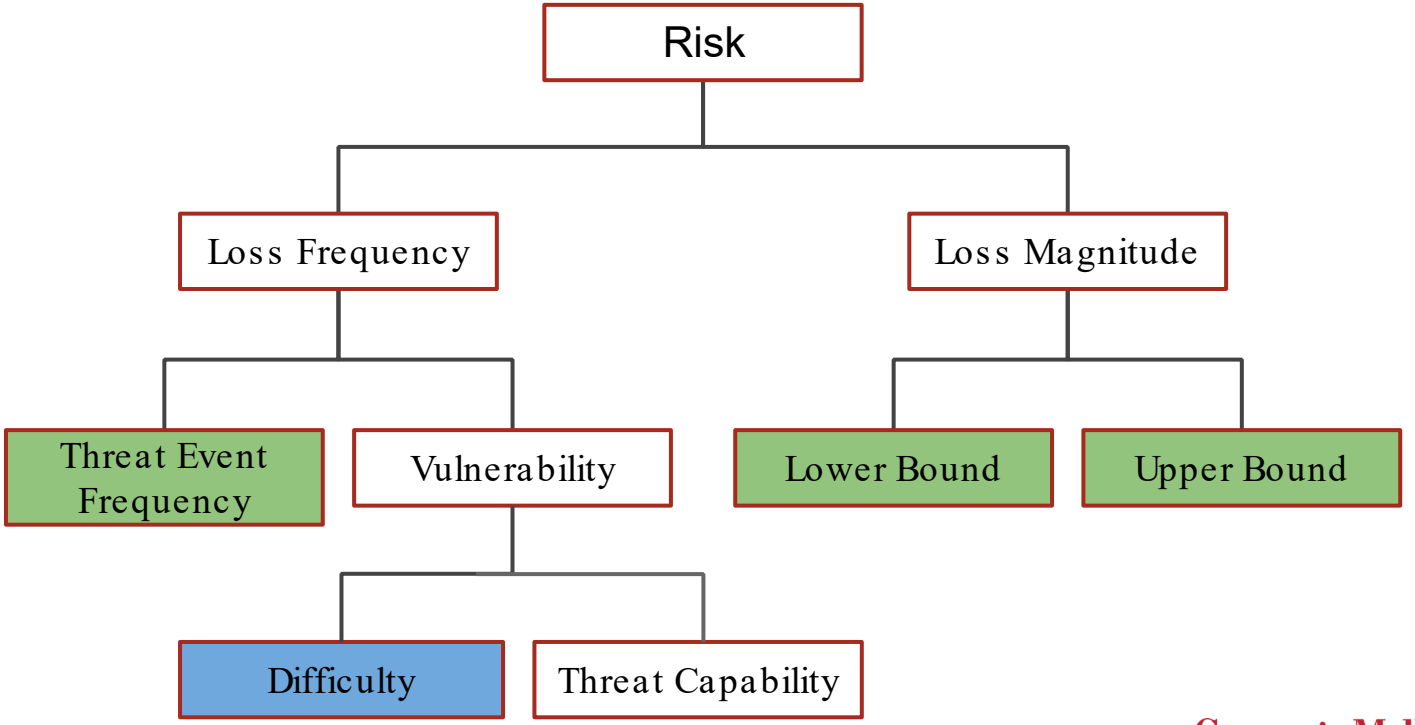
What is your compliance level?

Output

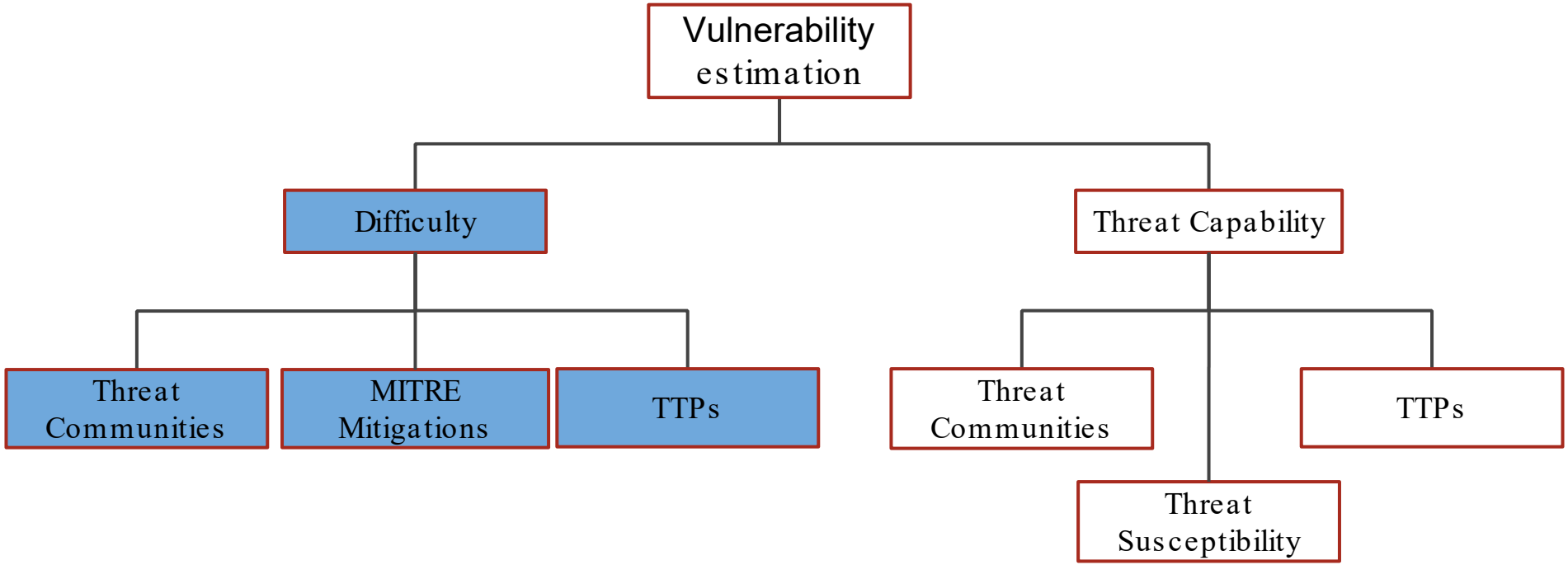
Compliance sheet

Carnegie Mellon University
HeinzCollege
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Factor Analysis of Information Risk (FAIR)



Inputs for Vulnerability Estimation



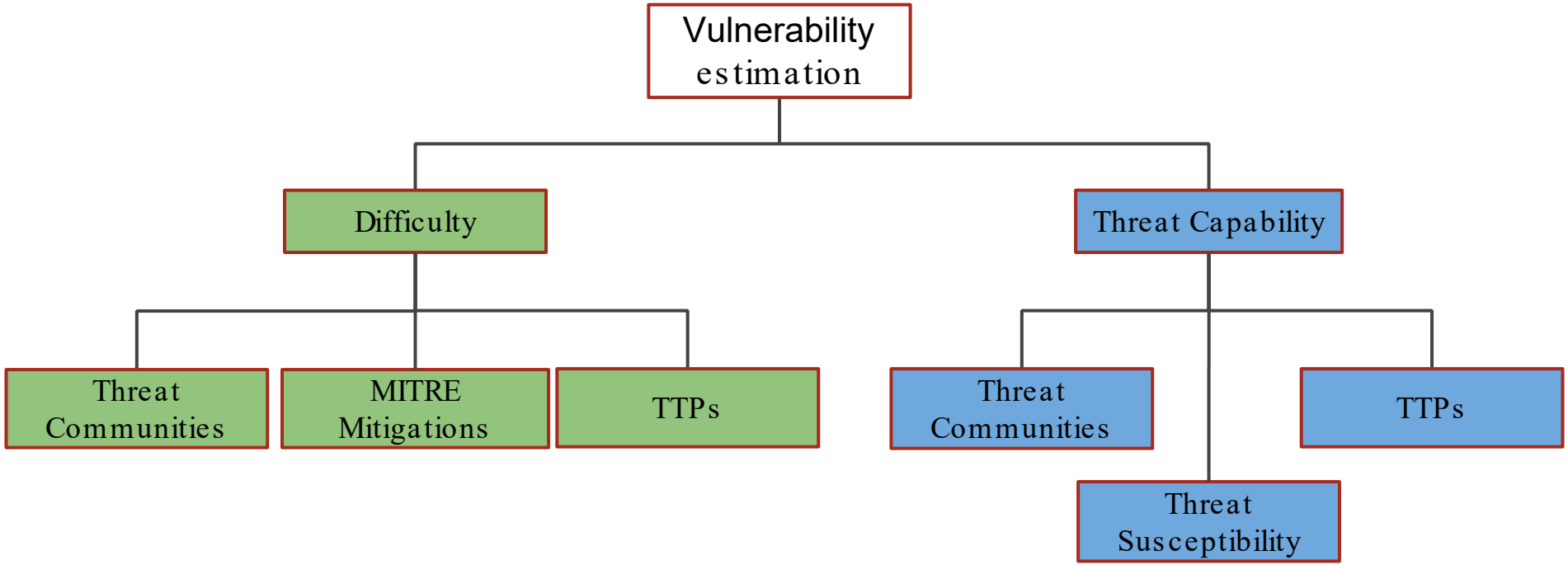
TTPs - MITRE Mitigations - NIST 800.53

TTP ID	Subtechnique	ID	Techniques Name	Mitigation ID	Mitigation Name	Nist Controls
T1110		T1110	Brute Force	M1036	Account Use Policies	IA-5
T1110	0.001	T1110.001	Password Guessing	M1036	Account Use Policies	IA-5
T1110	0.003	T1110.003	Password Spraying	M1036	Account Use Policies	IA-5
T1110	0.004	T1110.004	Credential Stuffing	M1036	Account Use Policies	IA-5
T1134	0.005	T1134.005	Access Token Manipulation: SID-History Injection	M1015	Active Directory Configuration	CM-2
T1606	0.002	T1606.002	Forge Web Credentials: SAML Tokens	M1015	Active Directory Configuration	CM-2
T1003		T1003	OS Credential Dumping	M1015	Active Directory Configuration	CM-2
T1003	0.006	T1003.006	DCSync	M1015	Active Directory Configuration	CM-2
T1003	0.005	T1003.005	Cached Domain Credentials	M1015	Active Directory Configuration	CM-2
T1072		T1072	Software Deployment Tools	M1015	Active Directory Configuration	CM-2
T1558		T1558	Steal or Forge Kerberos Tickets	M1015	Active Directory Configuration	CM-2
T1558	0.001	T1558.001	Golden Ticket	M1015	Active Directory Configuration	CM-2
T1552		T1552	Unsecured Credentials	M1015	Active Directory Configuration	CM-2
T1552	0.006	T1552.006	Group Policy Preferences	M1015	Active Directory Configuration	CM-2
T1550	0.003	T1550.003	se Alternate Authentication Material: Pass the Tick	M1015	Active Directory Configuration	CM-2

MITRE Mitigations - NIST Controls - FAIR Factors

Mitigation ID	Mitigation Name	Nist Controls	Nist Controls	Nist Controls	Nist Controls	FAIR Factor
M1031	Network Intrusion Prevention	SI-4	SC-7	SI-10		Diff
M1015	Active Directory Configuration	CM-2	AC-2			Diff
M1043	Credential Access Protection	AC-2	AC-4	SI-12		TCap
M1017	User Training	AT-2	AT-3	AT-4	AT-5	TCap

Inputs for Vulnerability Estimation



MITRE ATT&CK TTPs- Threat Communities

Threat groups and attack techniques

Threat Community	MITRE ATT&CK TTPS				
admin@338	uses-T1087-001	uses-T1059-003	uses-T1203	uses-T1083	uses-T1036-005
APT-C-36	uses-T1059-005	uses-T1105	uses-T1036-004	uses-T1571	uses-T1027
APT1	uses-T1087-001	uses-T1583-001	uses-T1560-001	uses-T1119	uses-T1059-003
APT12	uses-T1568-003	uses-T1203	uses-T1566-001	uses-T1204-002	uses-T1
APT16	uses-T1584-004				
APT17	uses-T1583-006	uses-T1585			
APT18	uses-T1071-001	uses-T1071-004	uses-T1547-001	uses-T1059-003	uses-T1133
APT19	uses-T1071-001	uses-T1547-001	uses-T1059	uses-T1059-001	uses-T1543-003
APT28	uses-T1134-001	uses-T1583-001	uses-T1071-003	uses-T1071-001	uses-T1560
APT29	uses-T1548-002	uses-T1583-006	uses-T1547-001	uses-T1547-009	uses-T1059-001
APT3	uses-T1087-001	uses-T1098	uses-T1560-001	uses-T1547-001	uses-T1110-002
APT30	uses-T1566-001	uses-T1204-002			
APT32	uses-T1087-001	uses-T1071-001	uses-T1071-003	uses-T1560	uses-T1547-001

Threat groups classification

State Sponsored	Cybercriminial
admin@338	APT18
APT-C-36	APT32
APT1	BlackTech
APT12	Blue Mockingbird
APT16	Bouncing Golf
APT17	Carbanak
APT19	Charming Kitten
APT28	Cobalt Group
APT29	Darkhotel
APT3	DarkHydrus
APT30	DarkVishnya
APT33	Dragonfly
APT37	DragonOK

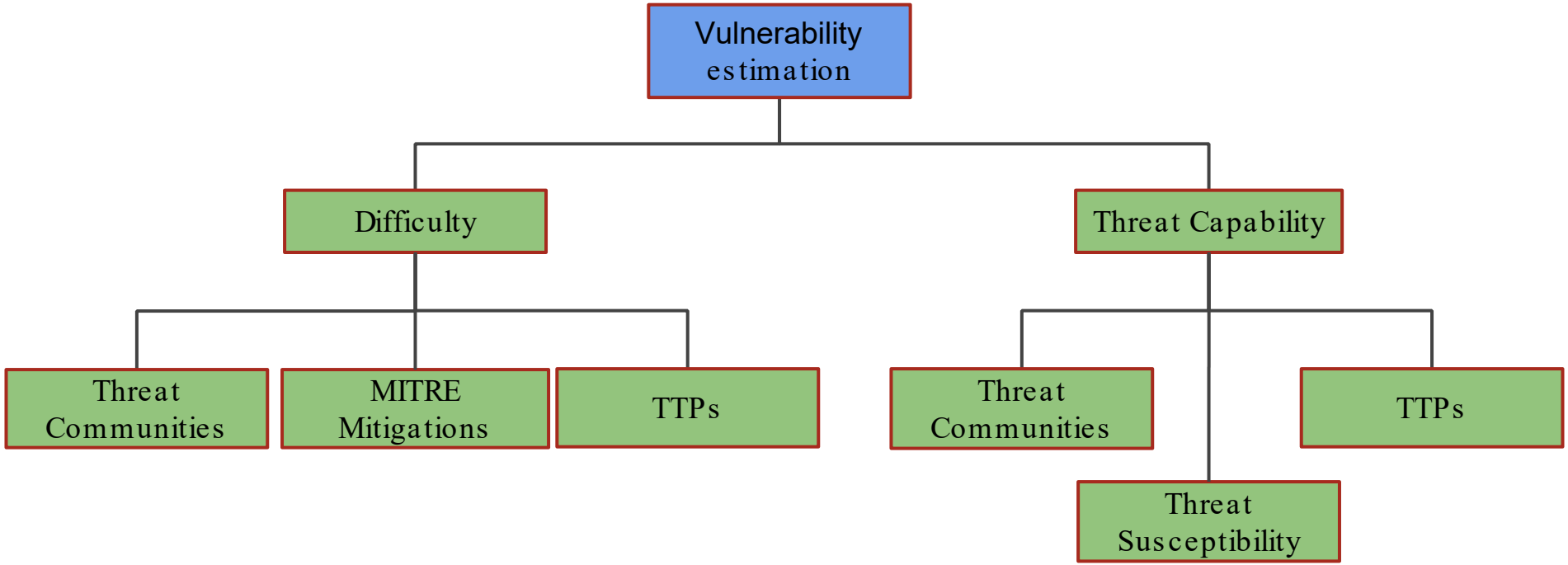
Threat Communities - TARA Susceptibility

TTP ID	Techniques Name	States APT groups	Cybercriminal Orgs APT groups
T1110	Brute Force	0.0577	0.0351
T1110	Password Guessing	0.0192	0.0000
T1110	Password Spraying	0.0769	0.0000
T1110	Credential Stuffing	0.0000	0.0000
T1134	Access Token Manipulation: SID-History Injection	0.0000	0.0000
T1606	Forge Web Credentials: SAML Tokens	0.0192	0.0000
T1003	OS Credential Dumping	0.0769	0.0877
T1003	DCSync	0.0192	0.0000
T1003	Cached Domain Credentials	0.0769	0.0000
T1072	Software Deployment Tools	0.0000	0.0526

How many states APT groups used this technique

Total number of states APT groups

Inputs for Vulnerability Estimation



Stage II: Vulnerability Estimation

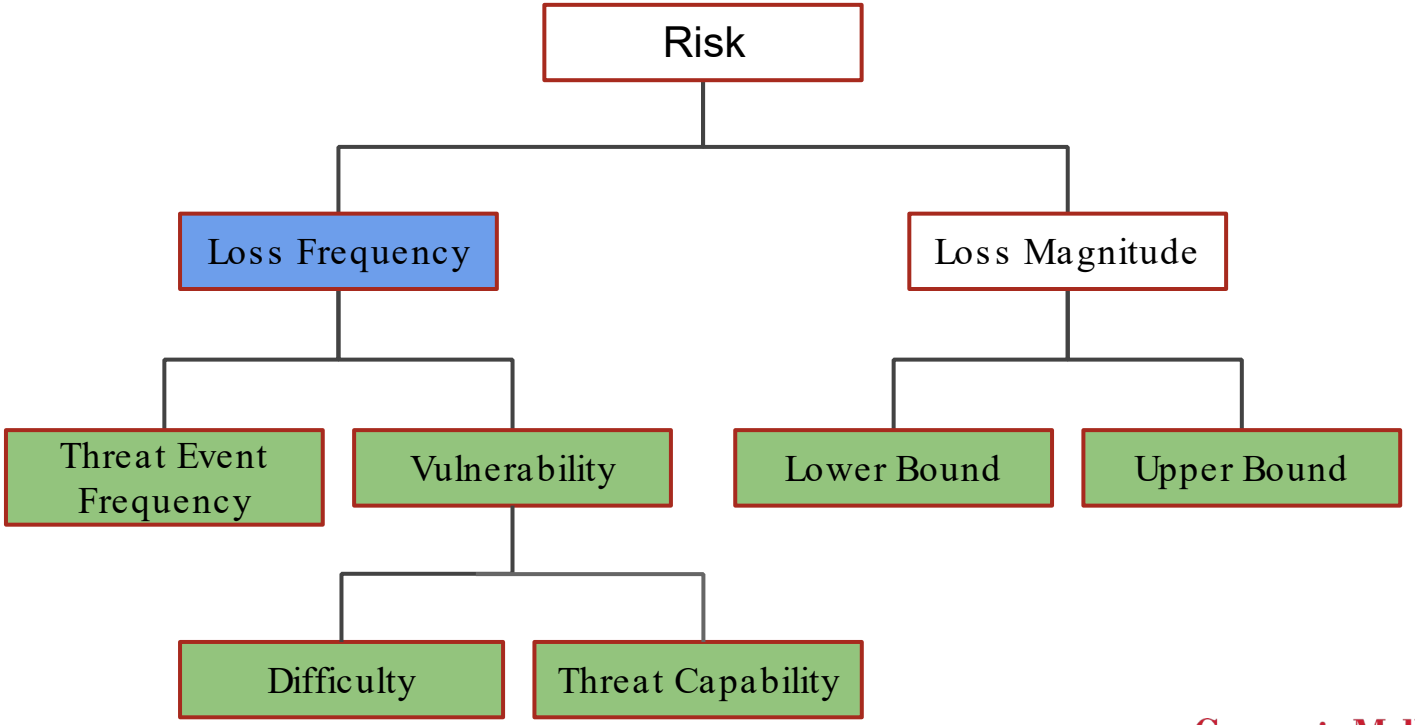
Output

For each event

Average effectiveness of NIST 800.53 controls (Avr. Eff.)

Vulnerability factor (= (1-Avr. Eff.) * TCap)

Factor Analysis of Information Risk (FAIR)



Stage II: Compute Risk

Simulation inputs

Vulnerability factor

Upper and lower bounds for impact

Threat Event Frequency (TEF)

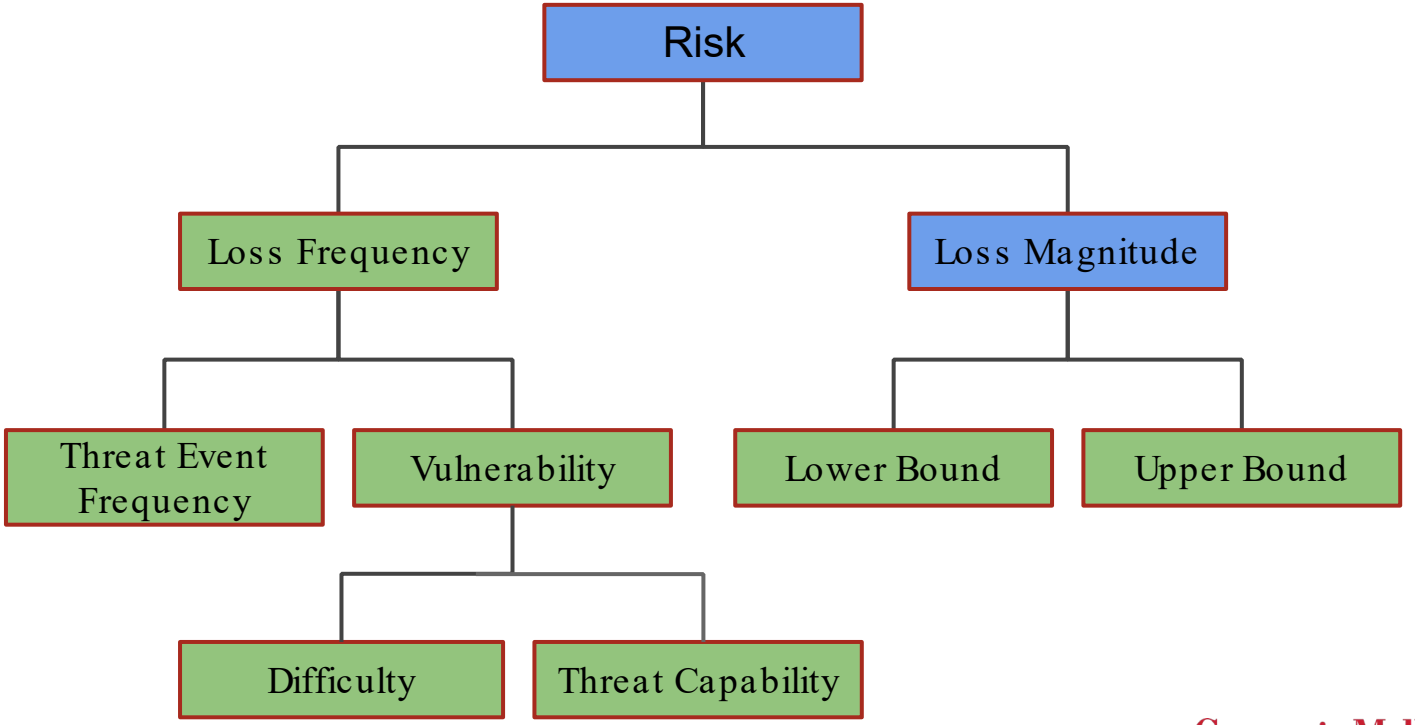
=> Probability = Vuln. * TEF

Stage II: Compute Risk

Loss Event VULN and TEF factors => Prob(LossEvent)

TEF (Threat Event Frequency	VULN (Prob(Event | Threat))	Prob
5	2.62%	13.08%

Factor Analysis of Information Risk (FAIR)



Stage II: Compute Risk

Ransomware Also impacts Confidentiality. 30% of Ransomware incidents exfiltrate information before encrypting

Only Conf/Int	Only Disp	Both
0%	70%	30%

From External research and customer **Elicitation**

90% Interval CI (Conf/Int)		90% CI (Availability)			
Lower Bound	Upper Bound	Duration of Outage (hours)		Cost per Hour ($)	
$ 100,000	$ 10,000,000	1.00	50.00	$ 50,000	$ 250,000

Stage II: Compute Risk

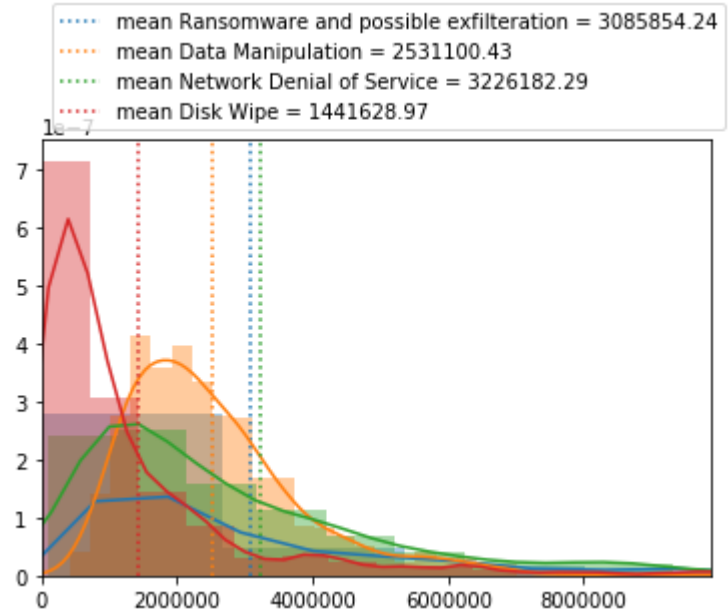
Calculations

Monte Carlo simulation for all events

Output

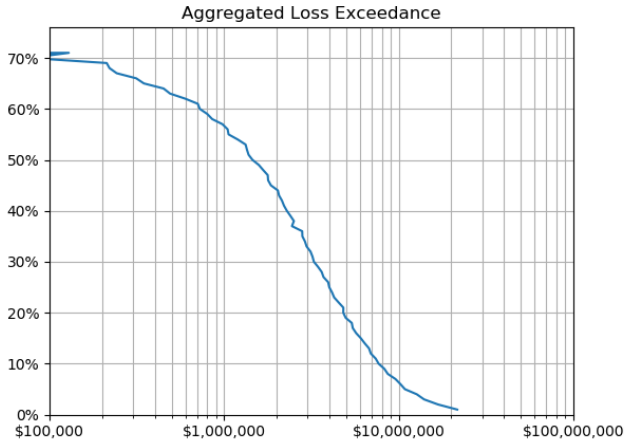
Estimated risk ($) for each event

Loss exceedance curve for all events



Stage II: Loss Exceedance Curve

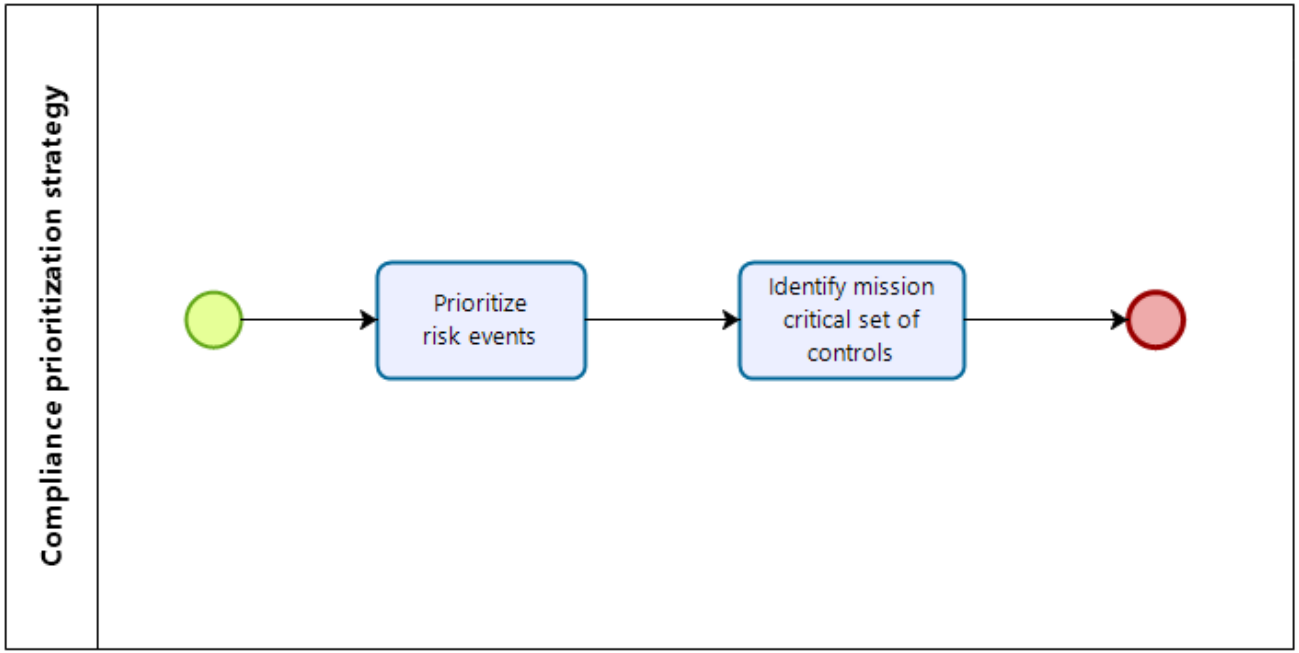
Expected Losses Assuming 90% CI in elicitation or customer estimations**:**



Loss Expected	**$ 666,503**		
Probability of Loss Exceeding	$1,000,000	is	10%

This example is for a RANSOMWARE event

Stage III: Compliance Prioritization Strategy



Stage III: Prioritize Risk Events

Process

Select and rank high impact risks

Output

Suggest the set of controls that need to be improved to address these risk

Stage III: Prioritize Risk Events

Impact ID	Loss Event	Final Result
T1486 and T1537	Ransomware and possible exfilteration	$1,150,943
T1565	Data Manipulation	$785,981
T1498	Network Denial of Service	$231,864
T1561	Disk Wipe	$57,233

Stage III: Identify Mission Critical Controls

Process

Select the associated controls for the previously identified impact risks

Output

List the controls that address the risk events and ask the user to re-enter improved compliance values

Q&A

Thank you