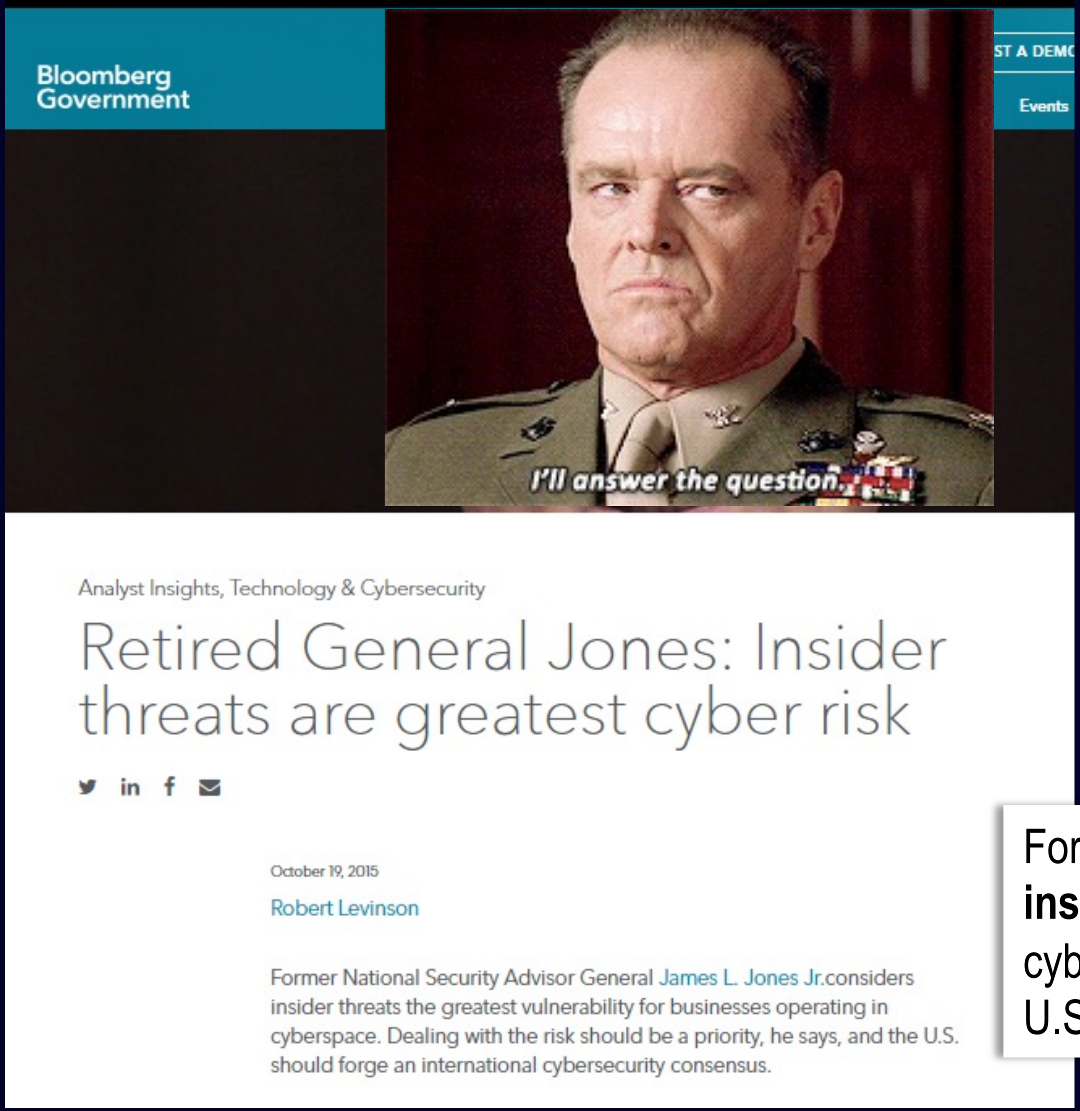
ROLL THE DICE

Refining the “R” in GRC @ Scale

Building credibility with cybersecurity and the business

Mike Radigan
miradiga@cisco.com

FAIR22 CONFERENCE



Analyst Insights, Technology & Cybersecurity

Retired General Jones: Insider threats are greatest cyber risk

October 19, 2015

Robert Levinson

Former National Security Advisor General James L. Jones Jr.considers insider threats the greatest vulnerability for businesses operating in cyberspace. Dealing with the risk should be a priority, he says, and the U.S. should forge an international cybersecurity consensus.

Insider threats are ...?

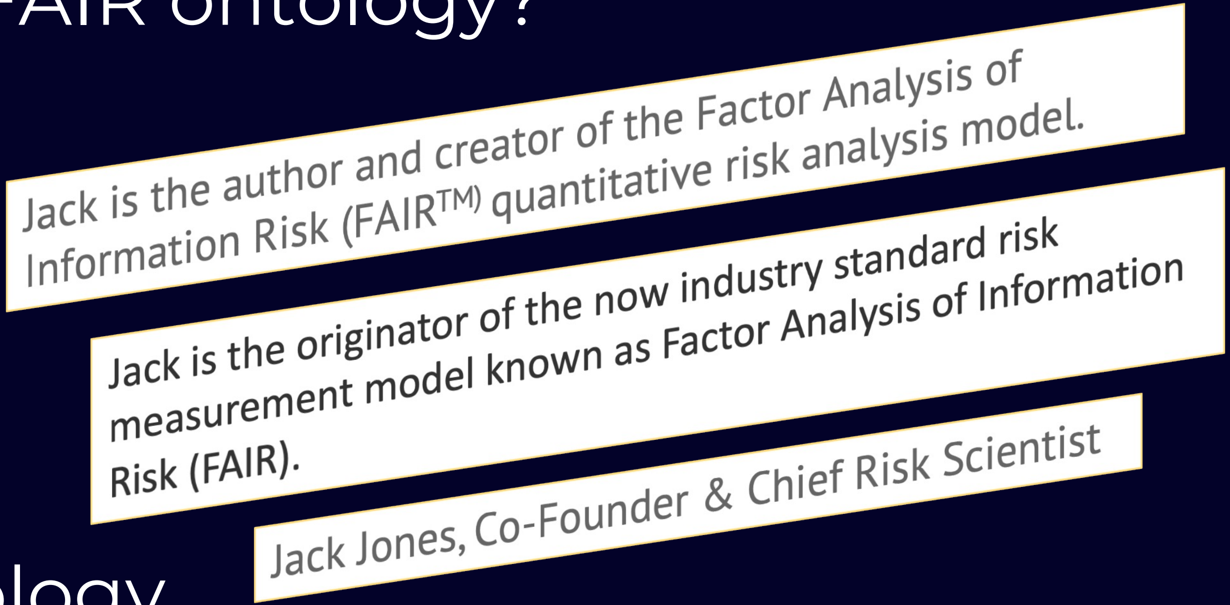
A.) Greatest vulnerability
B.) Greatest cyber risk
C.) All of the above
D.) None of the above
E.) IDK, need more context

Former National Security Advisor General James L. Jones Jr. considers **insider threats** the **greatest vulnerability** for businesses operating in cyberspace. Dealing with **the risk** should be a priority, he says, and the U.S. should forge an international cybersecurity consensus.

FAIR Insights / Trivia

Which best describes the FAIR ontology?

1. Invention
2. Innovation
3. Discovery
4. Applied Science
5. Theory
6. Religion
7. Alternative Methodology
8. Academic Exercise
9. The engine to create “risk snobs”



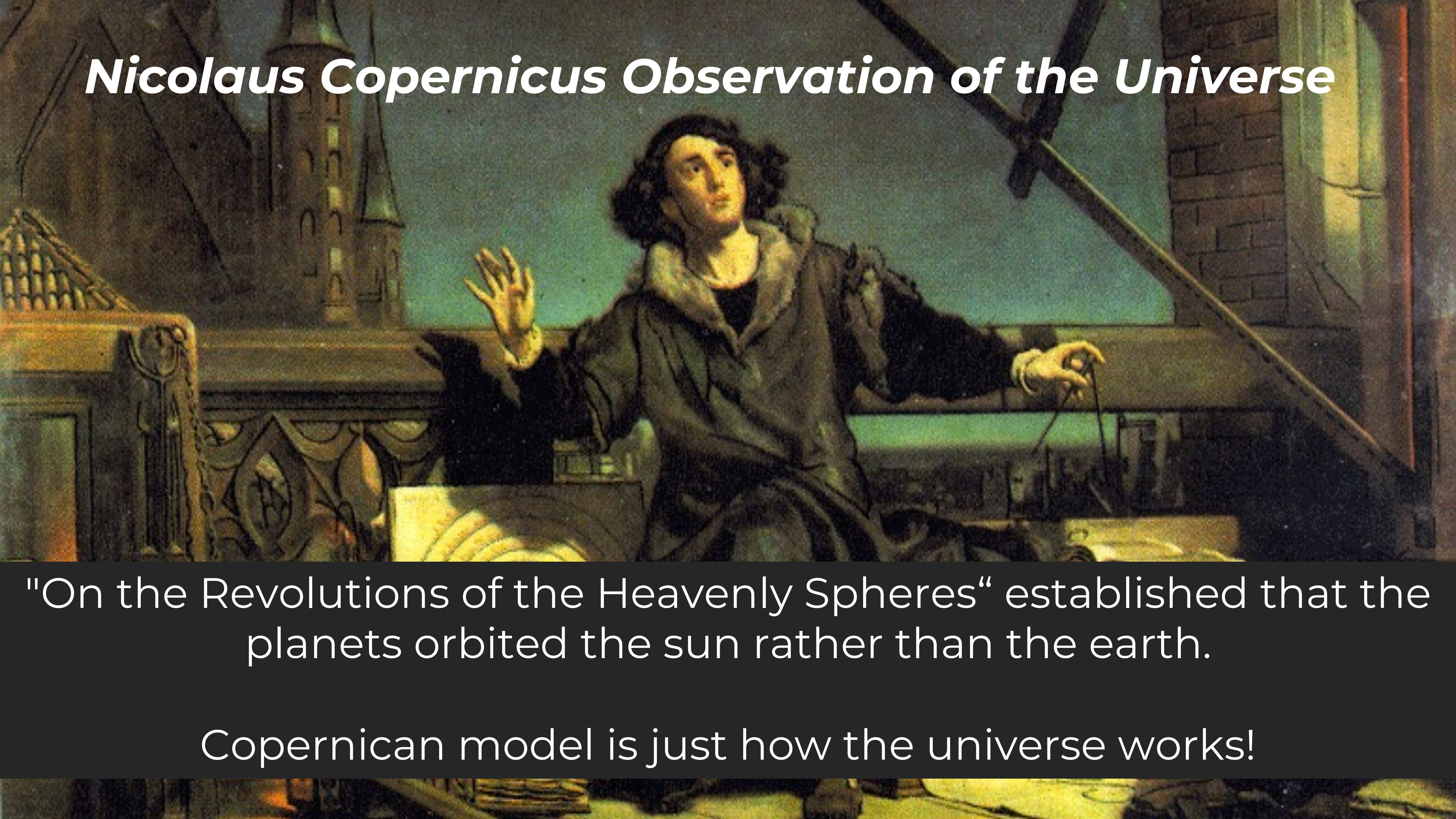
Jack is the author and creator of the Factor Analysis of Information Risk (FAIR™) quantitative risk analysis model.

Jack is the originator of the now industry standard risk measurement model known as Factor Analysis of Information Risk (FAIR).

Jack Jones, Co-Founder & Chief Risk Scientist

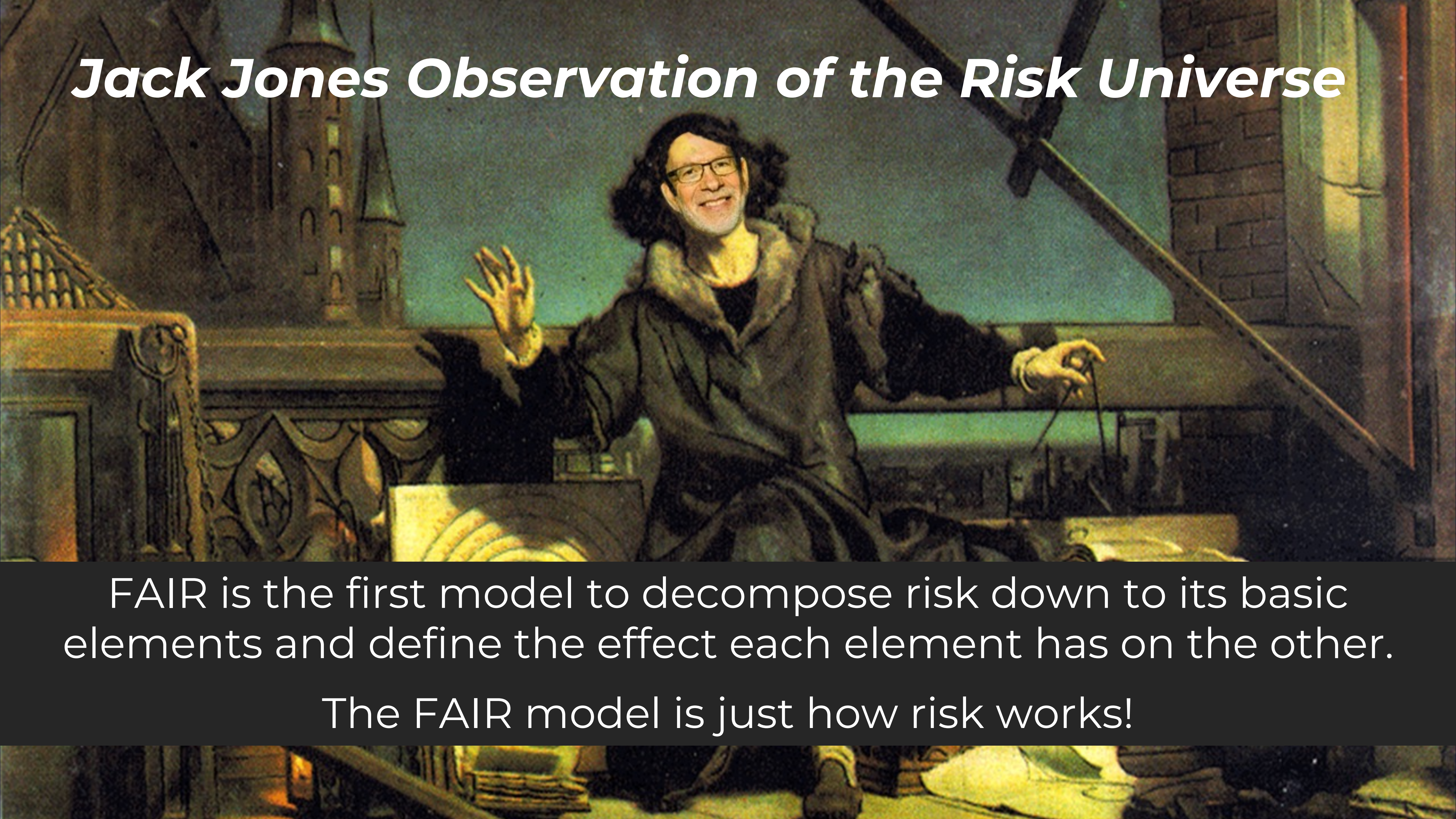
FAIR22 CONFERENCE

Nicolaus Copernicus Observation of the Universe



"On the Revolutions of the Heavenly Spheres“ established that the planets orbited the sun rather than the earth.

Copernican model is just how the universe works!



Jack Jones Observation of the Risk Universe

FAIR is the first model to decompose risk down to its basic elements and define the effect each element has on the other.

The FAIR model is just how risk works!

Refining the “R” in GRC @ Scale

Building credibility with cybersecurity and the business

Mike Radigan
miradiga@cisco.com

ROLL THE DICE

FAIR 22 CONFERENCE

Refining the “R” in GRC @ Scale

Key Objectives:

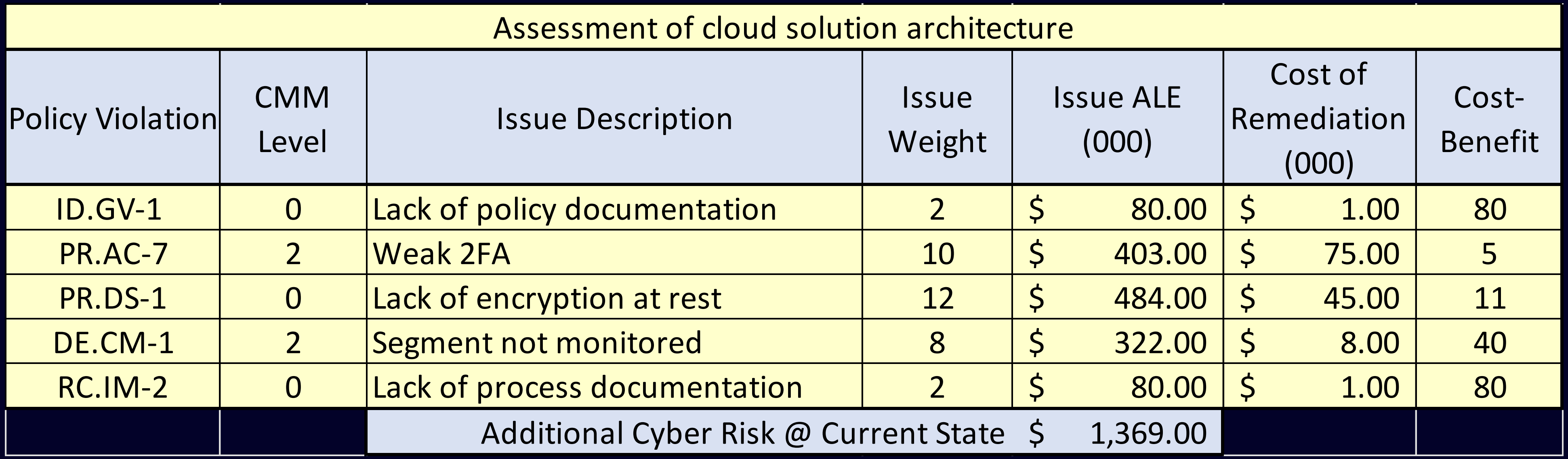
- Align security and the business around risk
- Enable business to make well informed decisions
  - Cost-benefit informed mitigation plans
- Build GRC credibility with security and the business
- Business leadership risk awareness and visibility
  - Risk portfolio (debt) vs Risk appetite
  - Financial metrics to assess and report risk debt
  - Demonstrate “progress”, risk reduction credit

Assessment of cloud solution architecture

Solution cyber risk at policy: $230,000 ALE

Solution cyber risk w/ Issues: $1,600,000 ALE

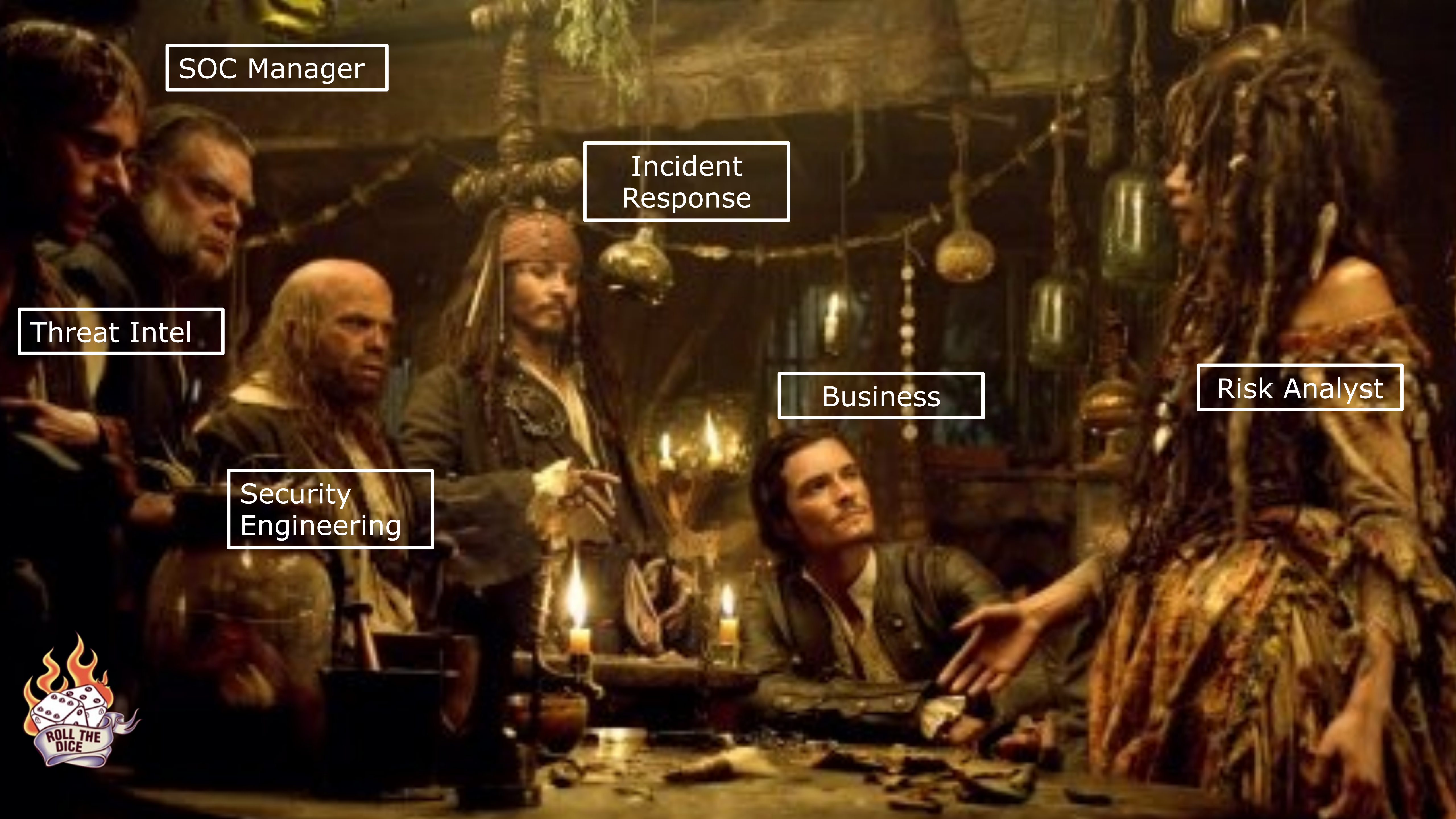
Cyber Risk due to non-compliance: $1,370,00 ALE



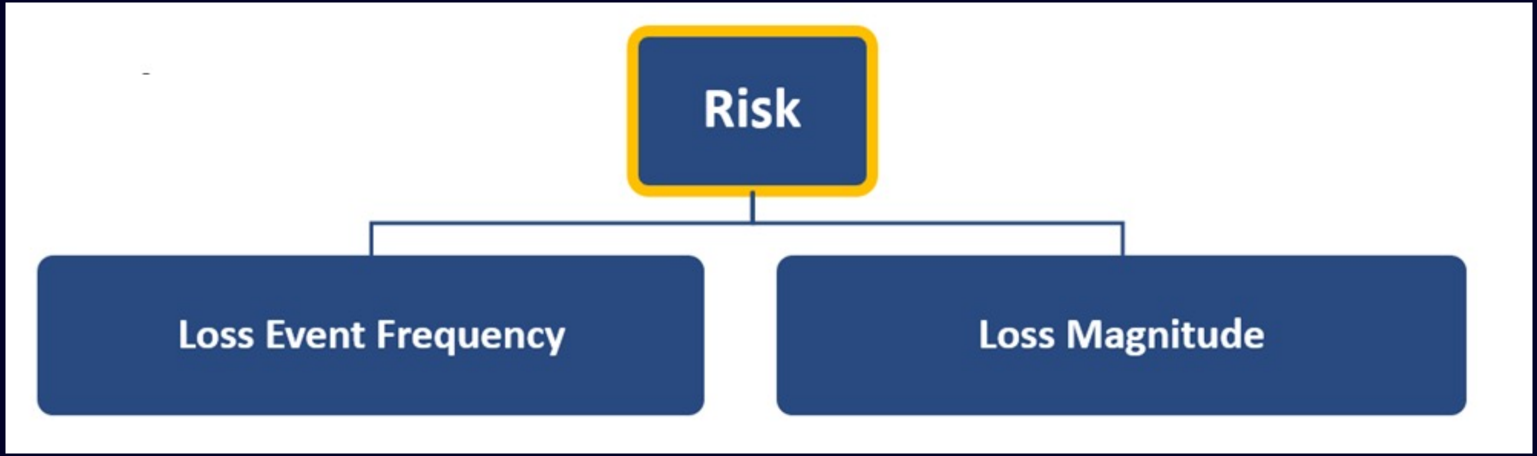
Assessment of cloud solution architecture

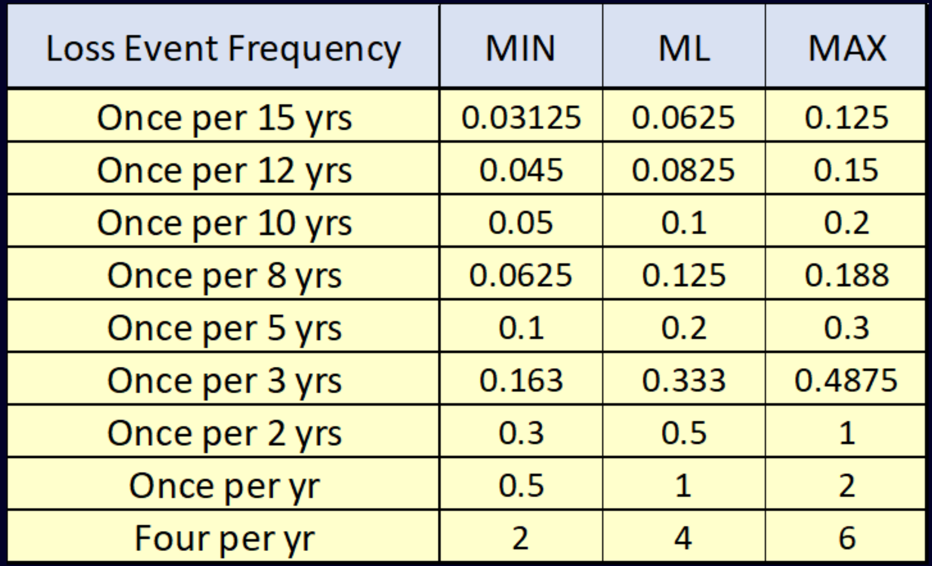
Policy Violation	CMM Level	Issue Description	Issue Weight	Issue ALE (000)	Cost of Remediation (000)	Cost-Benefit
ID.GV-1	0	Lack of policy documentation	2	$ 80.00	$ 1.00	80
PR.AC-7	2	Weak 2FA	10	$ 403.00	$ 75.00	5
PR.DS-1	0	Lack of encryption at rest	12	$ 484.00	$ 45.00	11
DE.CM-1	2	Segment not monitored	8	$ 322.00	$ 8.00	40
RC.IM-2	0	Lack of process documentation	2	$ 80.00	$ 1.00	80
		Additional Cyber Risk @ Current State		$ 1,369.00		

Mitigation cost = $130k 10:1

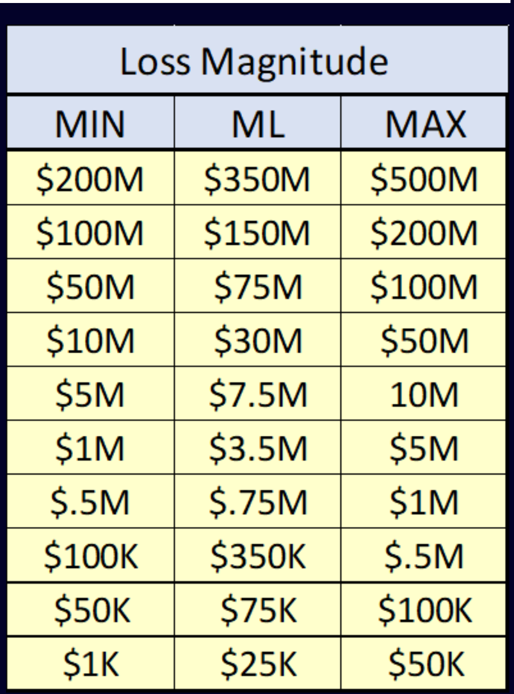

SOC Manager
Incident Response
Threat Intel
Business
Risk Analyst
Security Engineering
ROLL THE DICE

Risk Analysis





Loss Event Frequency	MIN	ML	MAX
Once per 15 yrs	0.03125	0.0625	0.125
Once per 12 yrs	0.045	0.0825	0.15
Once per 10 yrs	0.05	0.1	0.2
Once per 8 yrs	0.0625	0.125	0.188
Once per 5 yrs	0.1	0.2	0.3
Once per 3 yrs	0.163	0.333	0.4875
Once per 2 yrs	0.3	0.5	1
Once per yr	0.5	1	2
Four per yr	2	4	6



Loss Magnitude		
MIN	ML	MAX
$200M	$350M	$500M
$100M	$150M	$200M
$50M	$75M	$100M
$10M	$30M	$50M
$5M	$7.5M	10M
$1M	$3.5M	$5M
$.5M	$.75M	$1M
$100K	$350K	$.5M
$50K	$75K	$100K
$1K	$25K	$50K

Loss Event Frequency
SOC
Incident Response
Security Engineering
Pen Test
Threat Intelligence

Loss Magnitude
Legal
Compliance
HR
Sales & Marketing
Line of Business

Refining the “R” in GRC @ Scale

Design parameters and constraints

- 500+ Standard assessments w/ Issues
- Minimize risk analyst participation in process
- Derive assessment level cyber risk
  - Derive issue level cyber risk
  - Preserve artifacts and document rationale
- Minimize “gaming the system”
- Risk analysis is data entry exercise w/in RiskLens
- Security engineer / assessor as SME
- Business self-serves financial loss estimates
  - Calibrated estimates required from un-calibrated estimators

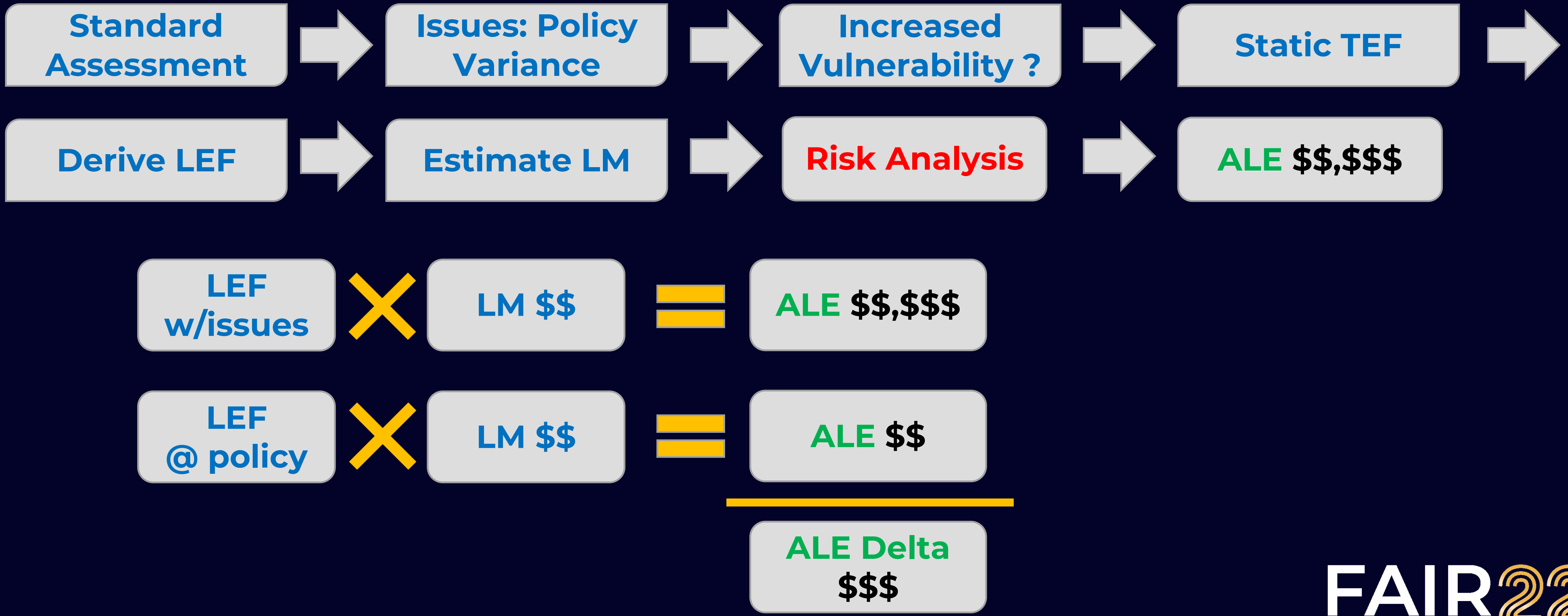
Decompose the problem

- Assets and Systems have a risk posture “@ policy”
- Assessments measure variance from policy
  - Control & capabilities deficiencies
- Variance from policy may have an adverse affect on risk
- Risk analysis measures affect on risk due to variance

Control function effect on risk

(Risk @ policy)-(Risk out of policy) = Risk debt

Block Diagram of process



FAIR22 CONFERENCE

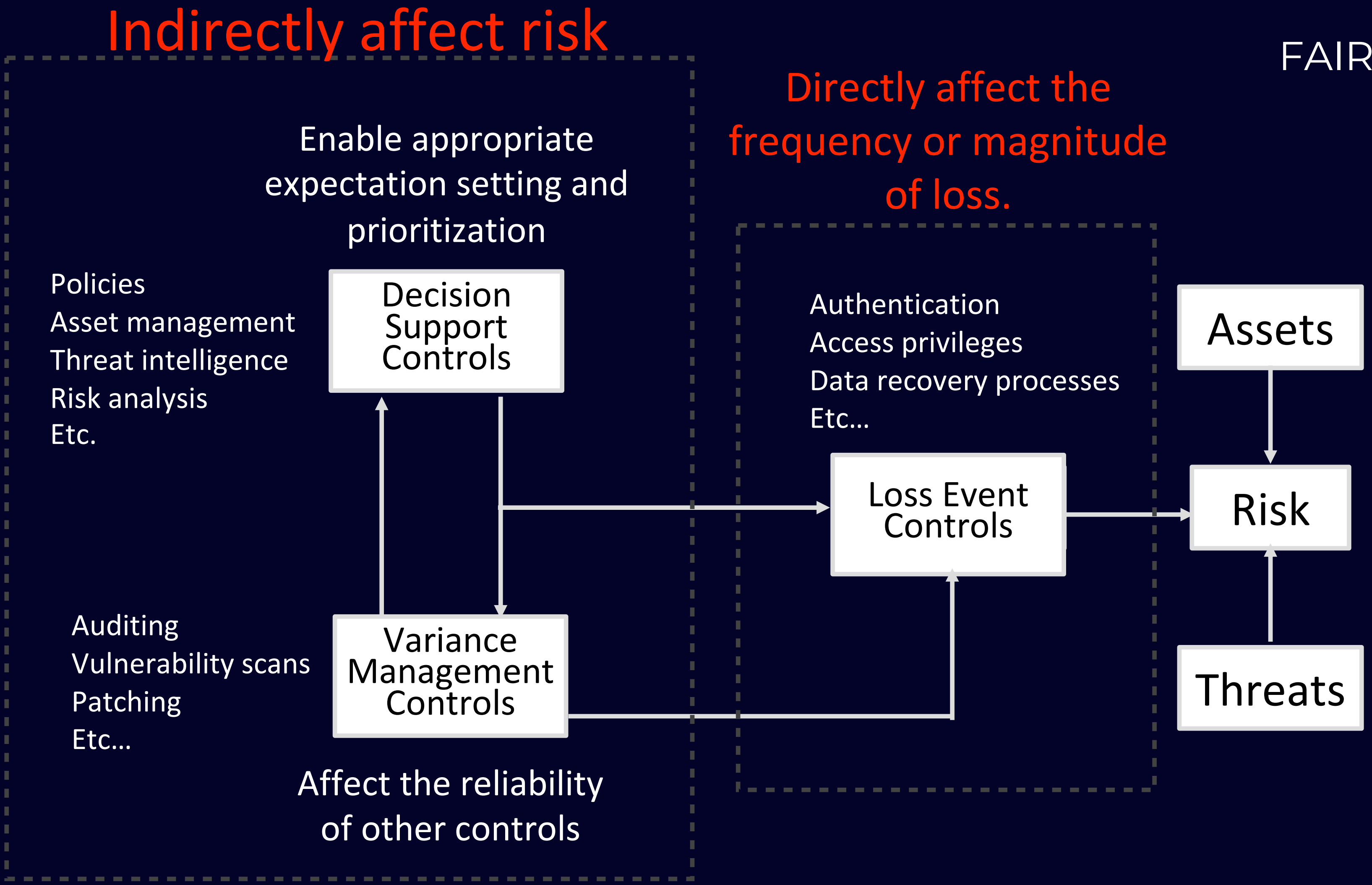
FAIR based solution

1. Map control Functions (FAIR-CAM)
2. Weight controls based on effect on risk
3. Account for Assessor discretion (CMM, CVSS, etc.)
4. Catalog controls assessed per assessment
5. Determine “at policy” Susceptibility to Compromise
6. Determine scale for degraded StC
7. Simplify scenarios to be analyzed: threats (Ext, Int) and loss effects (CIA)
8. Build LEF Scale for Organization
9. Map STC to the LEF Scale
10. Define scenarios clearly for business loss inputs
11. Business SME provides financial loss estimates (CIA)
12. Risk analysis is performed with derived inputs
13. Assessed (current) vs @ Policy risk is presented

Steps 1-3

Controls can affect risk directly or indirectly

FAIR-CAM



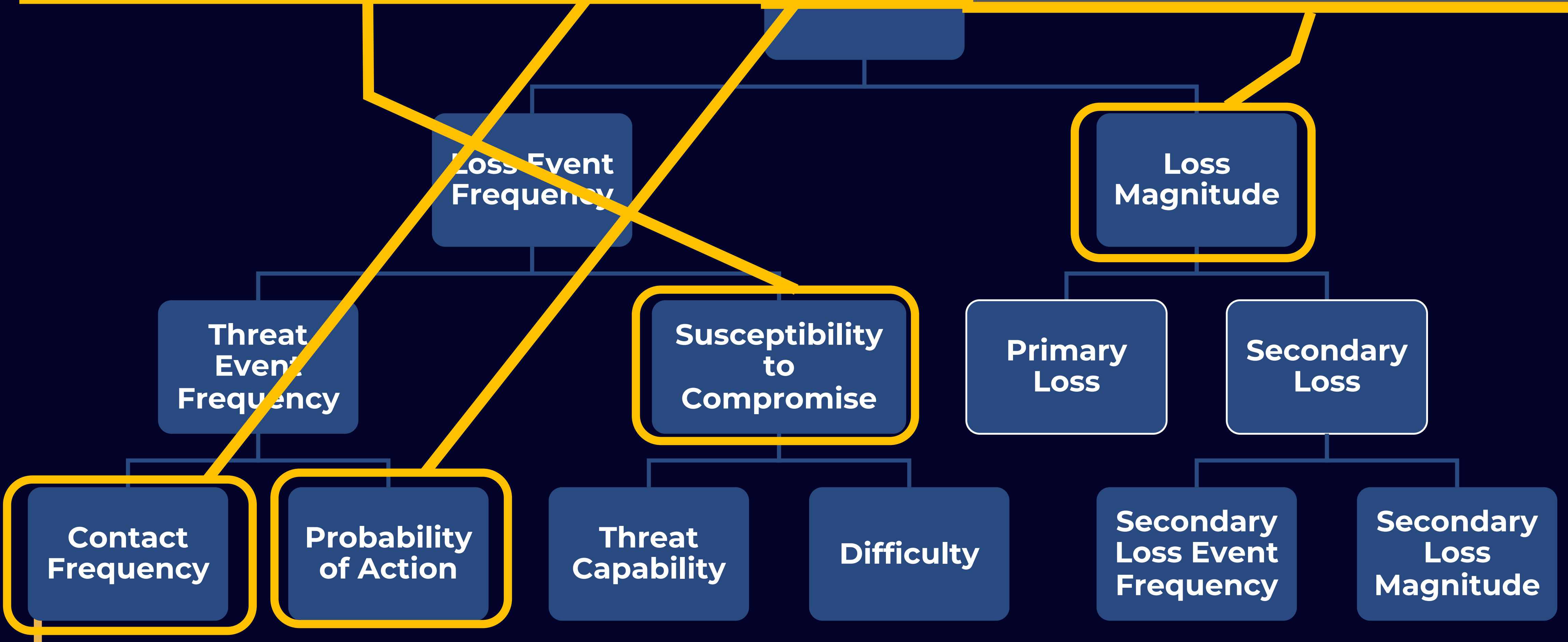
Copyright © 2022 FAIR Institute all rights reserved

FAIR22 CONFERENCE

Resistance Controls
Affect the probability that a threat's action will result in loss

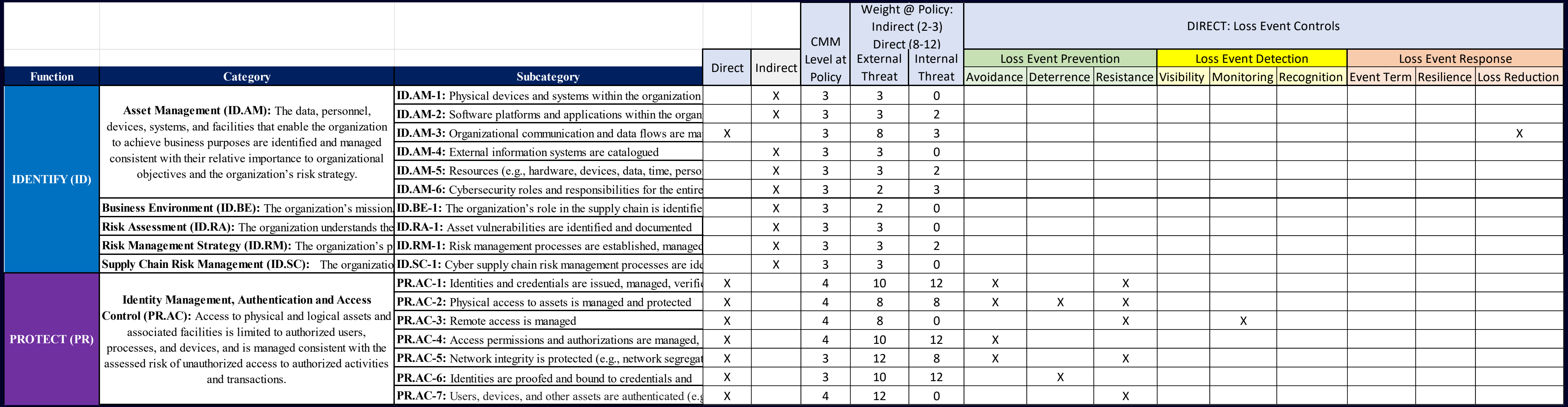
Avoidance Co
Affect the freq
encountering

Responsive Controls
Affect the amount of loss that result from a threat's action



Steps 1-3

Using FAIR-CAM to Catalog Controls



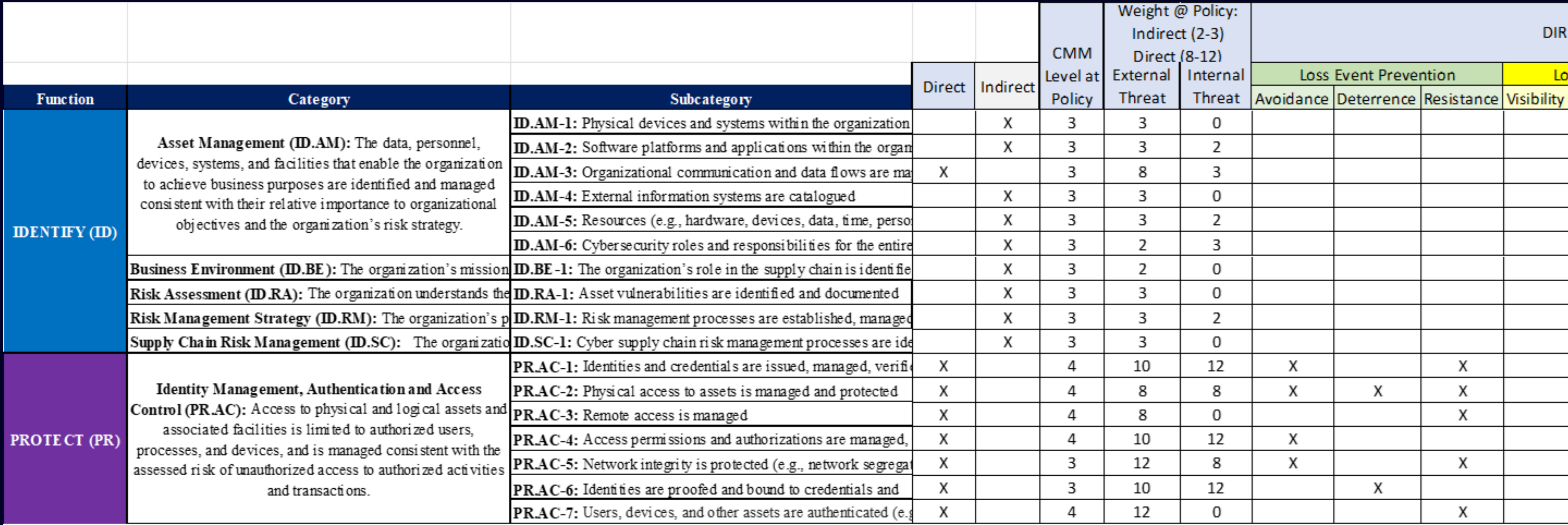
					CMM	Weight @ Policy: Indirect (2-3) Direct (8-12)		DIRECT: Loss Event Controls								
					Level at			Loss Event Prevention			Loss Event Detection			Loss Event Response		
Function	Category	Subcategory	Direct	Indirect	Policy	External Threat	Internal Threat	Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Event Term	Resilience	Loss Reduction
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization		X	3	3	0									
		ID.AM-2: Software platforms and applications within the organ		X	3	3	2									
		ID.AM-3: Organizational communication and data flows are ma	X		3	8	3									X
		ID.AM-4: External information systems are catalogued		X	3	3	0									
		ID.AM-5: Resources (e.g., hardware, devices, data, time, perso		X	3	3	2									
		ID.AM-6: Cybersecurity roles and responsibilities for the entire		X	3	2	3									
	Business Environment (ID.BE): The organization's mission,	**ID.BE-1:** The organization's role in the supply chain is identifie		X	3	2	0									
	Risk Assessment (ID.RA): The organization understands the	**ID.RA-1:** Asset vulnerabilities are identified and documented		X	3	3	0									
	Risk Management Strategy (ID.RM): The organization's p	**ID.RM-1:** Risk management processes are established, managed		X	3	3	2									
	Supply Chain Risk Management (ID.SC): The organizatio	**ID.SC-1:** Cyber supply chain risk management processes are ide		X	3	3	0									
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verifi	X		4	10	12	X		X						
		PR.AC-2: Physical access to assets is managed and protected	X		4	8	8	X	X	X						
		PR.AC-3: Remote access is managed	X		4	8	0			X		X				
		PR.AC-4: Access permissions and authorizations are managed,	X		4	10	12	X								
		PR.AC-5: Network integrity is protected (e.g., network segregat	X		3	12	8	X		X						
		PR.AC-6: Identities are proofed and bound to credentials and	X		3	10	12		X							
		PR.AC-7: Users, devices, and other assets are authenticated (e.g	X		4	12	0			X						

- Map the control functions to FAIR-CAM
- Direct effect on risk (loss event controls)
- Indirect effect on risk (variance and decision)
- Weight based on relative effect / efficacy, at policy maturity level

Steps 1-3

Using FAIR-CAM to Catalog Controls

ROLL THE DICE



						Weight @ Policy: Indirect (2-3) Direct (8-12)		DIR			
								Loss Event Prevention			Lo
Function	**Category**	**Subcategory**	Direct	Indirect	CMM Level at Policy	External Threat	Internal Threat	Avoidance	Deterrence	Resistance	Visibility
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization		X	3	3	0				
		ID.AM-2: Software platforms and applications within the organi		X	3	3	2				
		ID.AM-3: Organizational communication and data flows are ma	X		3	8	3				
		ID.AM-4: External information systems are catalogued		X	3	3	0				
		ID.AM-5: Resources (e.g., hardware, devices, data, time, perso		X	3	3	2				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire		X	3	2	3				
	Business Environment (ID.BE): The organization's mission	**ID.BE-1:** The organization's role in the supply chain is identifie		X	3	2	0				
	Risk Assessment (ID.RA): The organization understands the	**ID.RA-1:** Asset vulnerabilities are identified and documented		X	3	3	0				
	Risk Management Strategy (ID.RM): The organization's p	**ID.RM-1:** Risk management processes are established, managed		X	3	3	2				
	Supply Chain Risk Management (ID.SC): The organizatio	**ID.SC-1:** Cyber supply chain risk management processes are ide		X	3	3	0				
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verifi	X		4	10	12	X		X	
		PR.AC-2: Physical access to assets is managed and protected	X		4	8	8	X	X	X	
		PR.AC-3: Remote access is managed	X		4	8	0			X	
		PR.AC-4: Access permissions and authorizations are managed,	X		4	10	12	X			
		PR.AC-5: Network integrity is protected (e.g., network segregat	X		3	12	8	X		X	
		PR.AC-6: Identities are proofed and bound to credentials and	X		3	10	12		X		
		PR.AC-7: Users, devices, and other assets are authenticated (e.g	X		4	12	0			X	

FAIR22 CONFERENCE

Step 4

Calculate assessment baseline

Assessment against specific control objectives

- Each control objective has a base weight @ policy
- Maximum @ policy weight per assessment
- Findings at a lower CMM will degrade total

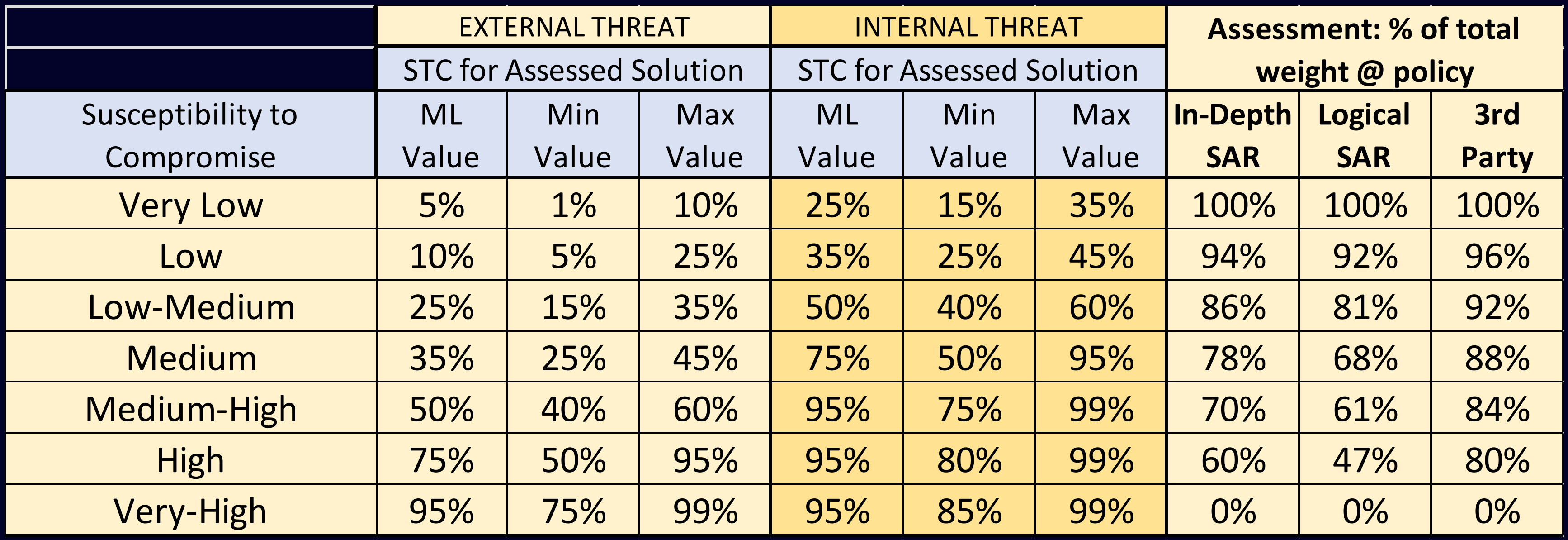
Assessment Baseline	Number of Sub-Categories Assessed	Total Weight of Assessed Sub-Categories
NIST CSF Security Review (Medium)	40	260
NIST CSF Security Review (Low)	8	80
NIST CSF Industrial Risk Assessment	90	530

Steps 5 & 6

Matrix assessment results to derive Susceptibility to Compromise

Assessment level Susceptibility to Compromise (StC)

1. Determine “at policy” Susceptibility to Compromise
2. Determine scale for degraded StC



	EXTERNAL THREAT			INTERNAL THREAT			Assessment: % of total weight @ policy		
	STC for Assessed Solution			STC for Assessed Solution					
Susceptibility to Compromise	ML Value	Min Value	Max Value	ML Value	Min Value	Max Value	**In-Depth SAR**	**Logical SAR**	**3rd Party**
Very Low	5%	1%	10%	25%	15%	35%	100%	100%	100%
Low	10%	5%	25%	35%	25%	45%	94%	92%	96%
Low-Medium	25%	15%	35%	50%	40%	60%	86%	81%	92%
Medium	35%	25%	45%	75%	50%	95%	78%	68%	88%
Medium-High	50%	40%	60%	95%	75%	99%	70%	61%	84%
High	75%	50%	95%	95%	80%	99%	60%	47%	80%
Very-High	95%	75%	99%	95%	85%	99%	0%	0%	0%

StC @ Policy

Step 7

Simplify scenarios to be analyzed

I.D. solution characteristics that will drive assessment level risk scenario components

1. Simplify threats (Ext, Int)
2. Derive loss effects (CIA)

Solution Characteristics	Scenario Components			
	C	I	A	APT
Sensitive Data	X			
Intellectual Property	X			X
Business Criticality			X	
10,000+ Users			X	
Financial Reporting		X		

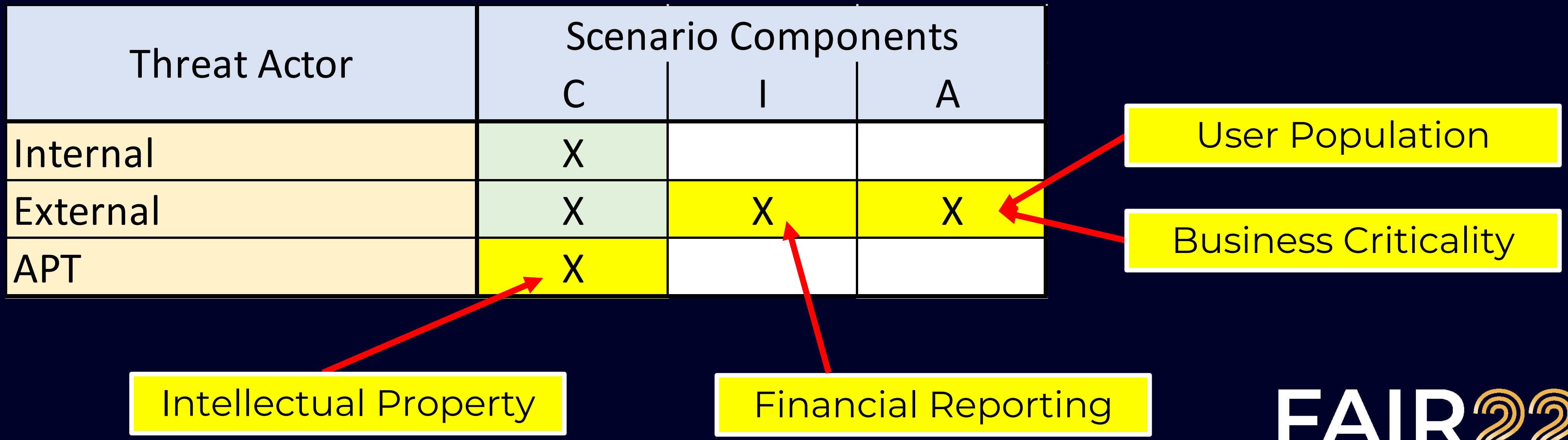
Threat Community	TRUE
External Activist	n/a
External Criminal	Yes
External Script Kiddie	n/a
State-Sponsored APT	TBD
Internal Unintentional	n/a
Internal Malicious	Yes

Step 7

Simplify scenarios to be analyzed

I.D. solution characteristics that will drive assessment level risk scenario components

1. Simplify threats (Ext, Int)
2. Derive loss effects (CIA)



Threat Actor	Scenario Components		
	C	I	A
Internal	X		
External	X	X	X
APT	X		

User Population

Business Criticality

Intellectual Property

Financial Reporting

Step 7

Simplify scenarios to be analyzed

I.D. solution characteristics that will drive assessment level risk scenario components

1. Simplify threats (Ext, Int)
2. Derive loss effects (CIA)

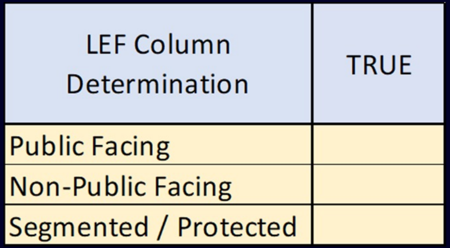
#	Scenario	Asset	Threat Actor	Loss Effect
1a	Exfiltration of sesitive data	Sensitive Data	Extnernal	Confidentiality
2a	Exfiltration of sesitive data	Sensitive Data	Internal	Confidentiality
3a	Exfiltration of sesitive data	Intellectual Prop	APT	Confidentiality
4a	Loss of Integrity of Financial Data	Sensitive Data	External	Integrity
5a	Loss of availability	Sensitive Data	Extnernal	Availability
1b	Exfiltration of sesitive data	Sensitive Data	Extnernal	Confidentiality
2b	Exfiltration of sesitive data	Sensitive Data	Internal	Confidentiality
3b	Exfiltration of sesitive data	Intellectual Prop	APT	Confidentiality
4b	Loss of Integrity of Financial Data	Sensitive Data	External	Integrity
5b	Loss of availability	Sensitive Data	Extnernal	Availability

Out of policy

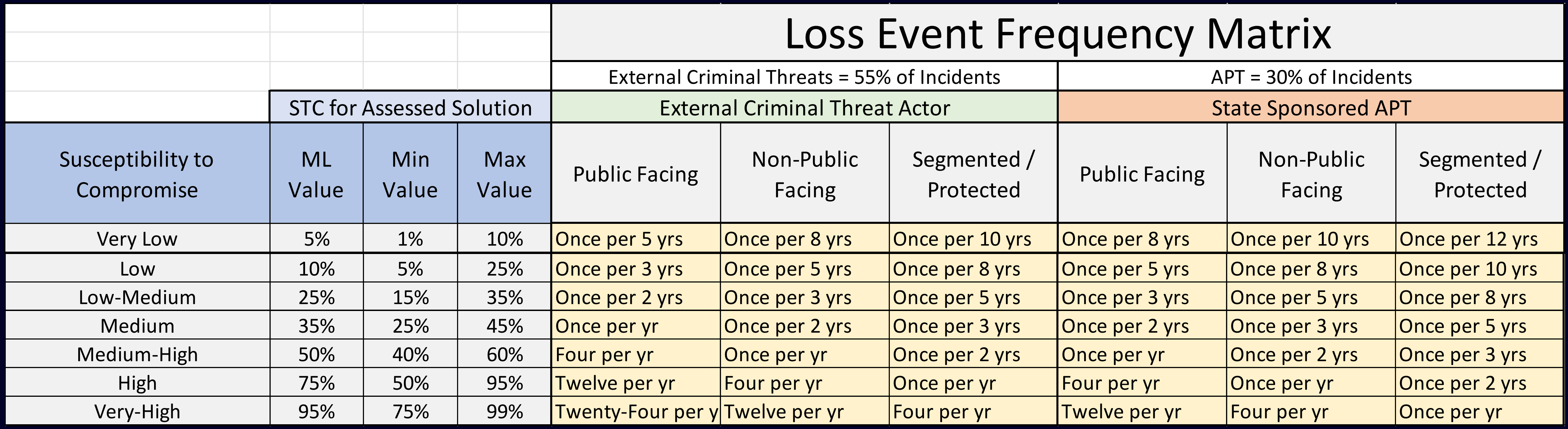
@ policy

Step 8 & 9

Matrix to derive the LEF from STC



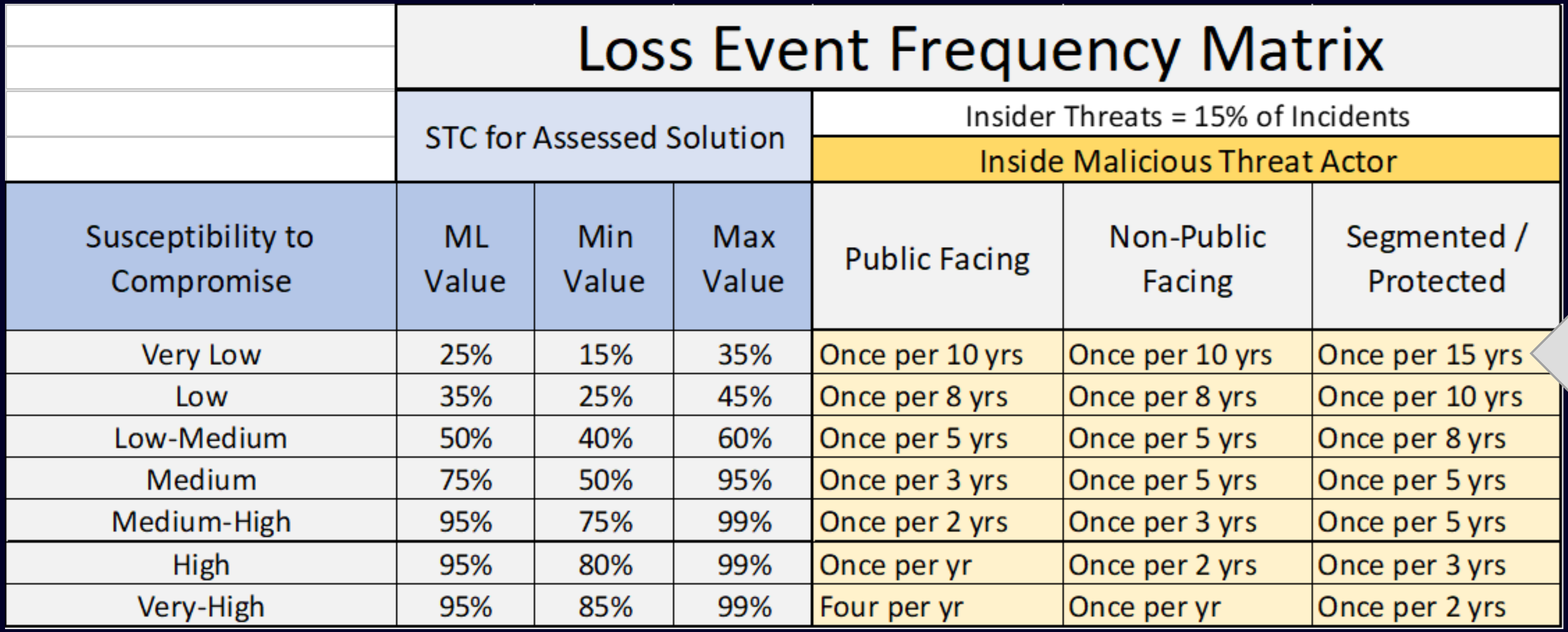
LEF Column Determination	TRUE
Public Facing	
Non-Public Facing	
Segmented / Protected	



				Loss Event Frequency Matrix					
				External Criminal Threats = 55% of Incidents			APT = 30% of Incidents		
	STC for Assessed Solution			External Criminal Threat Actor			State Sponsored APT		
Susceptibility to Compromise	ML Value	Min Value	Max Value	Public Facing	Non-Public Facing	Segmented / Protected	Public Facing	Non-Public Facing	Segmented / Protected
Very Low	5%	1%	10%	Once per 5 yrs	Once per 8 yrs	Once per 10 yrs	Once per 8 yrs	Once per 10 yrs	Once per 12 yrs
Low	10%	5%	25%	Once per 3 yrs	Once per 5 yrs	Once per 8 yrs	Once per 5 yrs	Once per 8 yrs	Once per 10 yrs
Low-Medium	25%	15%	35%	Once per 2 yrs	Once per 3 yrs	Once per 5 yrs	Once per 3 yrs	Once per 5 yrs	Once per 8 yrs
Medium	35%	25%	45%	Once per yr	Once per 2 yrs	Once per 3 yrs	Once per 2 yrs	Once per 3 yrs	Once per 5 yrs
Medium-High	50%	40%	60%	Four per yr	Once per yr	Once per 2 yrs	Once per yr	Once per 2 yrs	Once per 3 yrs
High	75%	50%	95%	Twelve per yr	Four per yr	Once per yr	Four per yr	Once per yr	Once per 2 yrs
Very-High	95%	75%	99%	Twenty-Four per y	Twelve per yr	Four per yr	Twelve per yr	Four per yr	Once per yr

Step 8 & 9

Matrix to derive the LEF from STC



	Loss Event Frequency Matrix					
	STC for Assessed Solution			Insider Threats = 15% of Incidents		
				Inside Malicious Threat Actor		
Susceptibility to Compromise	ML Value	Min Value	Max Value	Public Facing	Non-Public Facing	Segmented / Protected
Very Low	25%	15%	35%	Once per 10 yrs	Once per 10 yrs	Once per 15 yrs
Low	35%	25%	45%	Once per 8 yrs	Once per 8 yrs	Once per 10 yrs
Low-Medium	50%	40%	60%	Once per 5 yrs	Once per 5 yrs	Once per 8 yrs
Medium	75%	50%	95%	Once per 3 yrs	Once per 5 yrs	Once per 5 yrs
Medium-High	95%	75%	99%	Once per 2 yrs	Once per 3 yrs	Once per 5 yrs
High	95%	80%	99%	Once per yr	Once per 2 yrs	Once per 3 yrs
Very-High	95%	85%	99%	Four per yr	Once per yr	Once per 2 yrs

StC @ Policy

Example walk-through

Steps 1-9

Derive Loss Event Frequency

Assessment intake: Solution profile

1. Asset = Sensitive Data
2. Loss Effects: Confidentiality & Availability
3. External & Internal Threats
4. Three (3) scenarios @ policy + Three (3) scenarios @ current

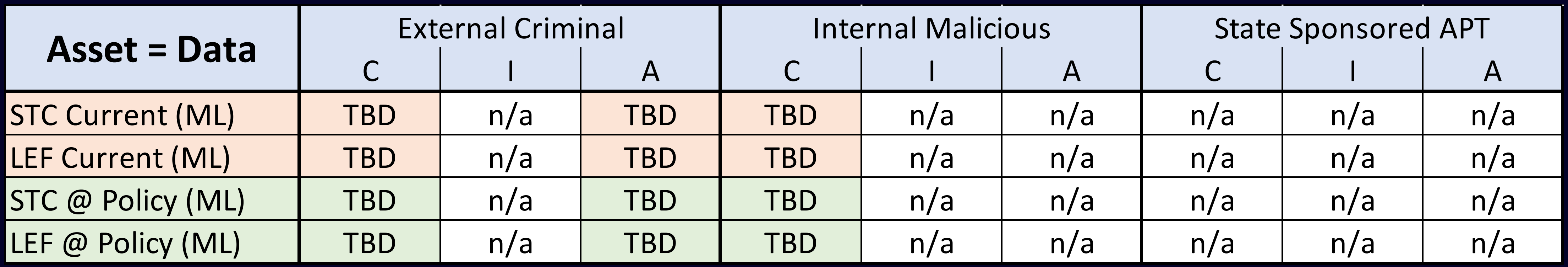
Solution Components	Scenario Components			
	C	I	A	APT
Sensitive Data	☑			
Intellectual Property				✗
Business Criticality			☑	
10,000+ Users			☑	
Financial Reporting		✗		

LEF Column Determination	TRUE
Public Facing	
Non-Public Facing	☑
Segmented / Protected	

Scenario Determination

Assessment intake: Solution profile

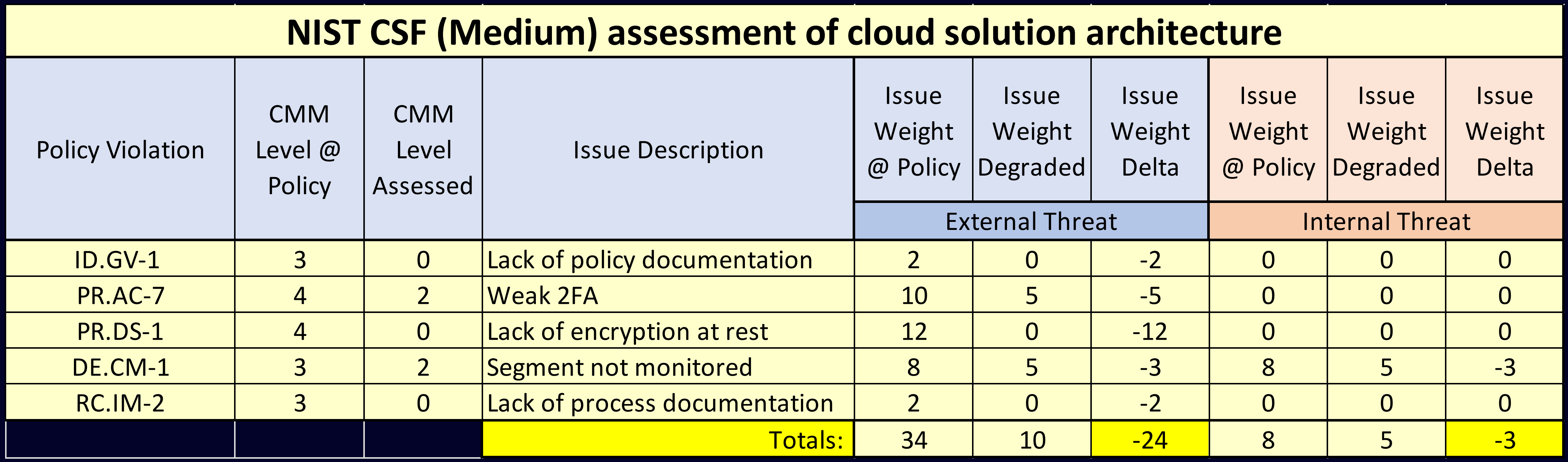
1. Asset = Sensitive Data
2. Loss Effects: Confidentiality & Availability
3. External & Internal Threats
4. Three (3) scenarios @ policy + Three (3) scenarios @ current



Asset = Data	External Criminal			Internal Malicious			State Sponsored APT		
	C	I	A	C	I	A	C	I	A
STC Current (ML)	TBD	n/a	TBD	TBD	n/a	n/a	n/a	n/a	n/a
LEF Current (ML)	TBD	n/a	TBD	TBD	n/a	n/a	n/a	n/a	n/a
STC @ Policy (ML)	TBD	n/a	TBD	TBD	n/a	n/a	n/a	n/a	n/a
LEF @ Policy (ML)	TBD	n/a	TBD	TBD	n/a	n/a	n/a	n/a	n/a

Derive Susceptibility to Compromise

Determine degraded assessment weight



NIST CSF (Medium) assessment of cloud solution architecture									
Policy Violation	CMM Level @ Policy	CMM Level Assessed	Issue Description	Issue Weight @ Policy	Issue Weight Degraded	Issue Weight Delta	Issue Weight @ Policy	Issue Weight Degraded	Issue Weight Delta
				External Threat			Internal Threat		
ID.GV-1	3	0	Lack of policy documentation	2	0	-2	0	0	0
PR.AC-7	4	2	Weak 2FA	10	5	-5	0	0	0
PR.DS-1	4	0	Lack of encryption at rest	12	0	-12	0	0	0
DE.CM-1	3	2	Segment not monitored	8	5	-3	8	5	-3
RC.IM-2	3	0	Lack of process documentation	2	0	-2	0	0	0
			Totals:	34	10	-24	8	5	-3

Derive Susceptibility to Compromise

Determine degraded assessment %

NIST CSF (Medium) assessment of cloud solution architecture	Number of Sub-Categories Assessed	Total Weight of Assessed Sub-Categories	Total Issue Weight Delta	% of Total Weigh @ Policy
External Threat	40	260	-24	91%
Internal Threat	40	180	-3	98%

Derive Susceptibility to Compromise

Map degraded % weight to StC

	EXTERNAL THREAT			INTERNAL THREAT			**Assessment: % of total weight @ policy**		
	STC for Assessed Solution			STC for Assessed Solution					
Susceptibility to Compromise	ML Value	Min Value	Max Value	ML Value	Min Value	Max Value	**NIST Medium**	**NIST Low**	**NIST Industrial**
Very Low	5%	1%	10%	25%	15%	35%	100%	100%	100%
Low	10%	5%	25%	35%	25%	45%	94%	92%	96%
Low-Medium	25%	15%	35%	50%	40%	60%	86%	81%	92%
Medium	35%	25%	45%	75%	50%	95%	78%	68%	88%
Medium-High	50%	40%	60%	95%	75%	99%	70%	61%	84%
High	75%	50%	95%	95%	80%	99%	60%	47%	80%
Very-High	95%	75%	99%	95%	85%	99%	0%	0%	0%

Derive Susceptibility to Compromise

Map degraded % weight to StC

	EXTERNAL THREAT			INTERNAL THREAT			Assessment: % of total weight @ policy		
	STC for Assessed Solution			STC for Assessed Solution					
Susceptibility to Compromise	ML Value	Min Value	Max Value	ML Value	Min Value	Max Value	NIST Medium	NIST Low	NIST Industrial
Very Low	5%	1%	10%	25%	15%	35%	100%	100%	100%
Low	10%	5%	25%	35%	25%	45%	94%	92%	96%
Low-Medium	25%	15%	35%	50%	40%	60%	86%	81%	92%
Medium	35%	25%	45%	75%	50%	95%	78%	68%	88%
Medium-High	50%	40%	60%	95%	75%	99%	70%	61%	84%
High	75%	50%	95%	95%	80%	99%	60%	47%	80%
Very-High	95%	75%	99%	95%	85%	99%	0%	0%	0%

Derive Loss Event Frequency

Map degraded StC to Loss Event Frequency (External)

Solution Profile: Non-Public Facing				LEF Matrix		
				External Criminal Threats = 55% of Incidents		
Susceptibility to Compromise	STC for Assessed Solution			External Criminal Threat Actor		
	ML Value	Min Value	Max Value	Public Facing	Non-Public Facing	Segmented / Protected
Very Low	5%	1%	10%	Once per 5 yrs	Once per 8 yrs	Once per 10 yrs
Low	10%	5%	25%	Once per 3 yrs	Once per 5 yrs	Once per 8 yrs
Low-Medium	25%	15%	35%	Once per 2 yrs	Once per 3 yrs	Once per 5 yrs
Medium	35%	25%	45%	Once per yr	Once per 2 yrs	Once per 3 yrs
Medium-High	50%	40%	60%	Four per yr	Once per yr	Once per 2 yrs
High	75%	50%	95%	Twelve per yr	Four per yr	Once per yr
Very-High	95%	75%	99%	Twenty-Four per	Twelve per yr	Four per yr

Derive Loss Event Frequency

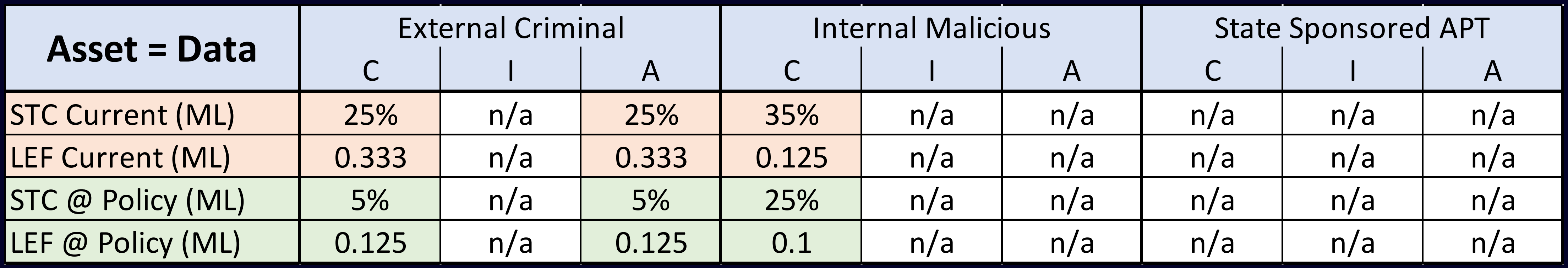
Map degraded StC to Loss Event Frequency (Internal)

Solution Profile: Non-Public Facing	Loss Event Frequency Matrix					
	STC for Assessed Solution			Insider Threats = 15% of Incidents		
				Inside Malicious Threat Actor		
Susceptibility to Compromise	ML Value	Min Value	Max Value	Public Facing	Non-Public Facing	Segmented / Protected
Very Low	25%	15%	35%	Once per 10 yrs	Once per 10 yrs	Once per 15 yrs
Low	35%	25%	45%	Once per 8 yrs	Once per 8 yrs	Once per 10 yrs
Low-Medium	50%	40%	60%	Once per 5 yrs	Once per 5 yrs	Once per 8 yrs
Medium	75%	50%	95%	Once per 3 yrs	Once per 5 yrs	Once per 5 yrs
Medium-High	95%	75%	99%	Once per 2 yrs	Once per 3 yrs	Once per 5 yrs
High	95%	80%	99%	Once per yr	Once per 2 yrs	Once per 3 yrs
Very-High	95%	85%	99%	Four per yr	Once per yr	Once per 2 yrs

Populate Scenario Inputs

Scenarios and artifacts

- Issues documented / policy variance is measured
- STC is recorded as supporting rationale
- Exclusion of loss effect “I” supported
- Exclusion of APT is supported
- (6) scenarios to be analyzed



Asset = Data	External Criminal			Internal Malicious			State Sponsored APT		
	C	I	A	C	I	A	C	I	A
STC Current (ML)	25%	n/a	25%	35%	n/a	n/a	n/a	n/a	n/a
LEF Current (ML)	0.333	n/a	0.333	0.125	n/a	n/a	n/a	n/a	n/a
STC @ Policy (ML)	5%	n/a	5%	25%	n/a	n/a	n/a	n/a	n/a
LEF @ Policy (ML)	0.125	n/a	0.125	0.1	n/a	n/a	n/a	n/a	n/a

Risk Analysis of defined scenarios

Scenario analysis

- (6) scenarios to be analyzed
- Financial impact provided by the business
- Data entry exercise into RiskLens

#	Scenario	Asset	Threat Actor	Loss Effect	Incident Frequency			Financial Impact		
					MIN	ML	MAX	MIN	ML	MAX
1a	Exfiltration of sesitive data	Sensitive Data	Extnernal	Confidentiality	0.163	0.333	0.4875	$.25M	$1M	$5M
2a	Exfiltration of sesitive data	Sensitive Data	Internal	Confidentiality	0.1	0.2	0.333	$.25M	$1M	$5M
3a	Loss of availability of sensitive data	Sensitive Data	Extnernal	Availability	0.163	0.333	0.4875	$20K	$.5M	$1M
1b	Exfiltration of sesitive data	Sensitive Data	Extnernal	Confidentiality	0.0625	0.125	0.188	$.25M	$1M	$5M
2b	Exfiltration of sesitive data	Sensitive Data	Internal	Confidentiality	0.05	0.1	0.2	$.25M	$1M	$5M
3b	Loss of availabilit of sensitive data	Sensitive Data	Extnernal	Availability	0.0625	0.125	0.188	$20K	$.5M	$1M

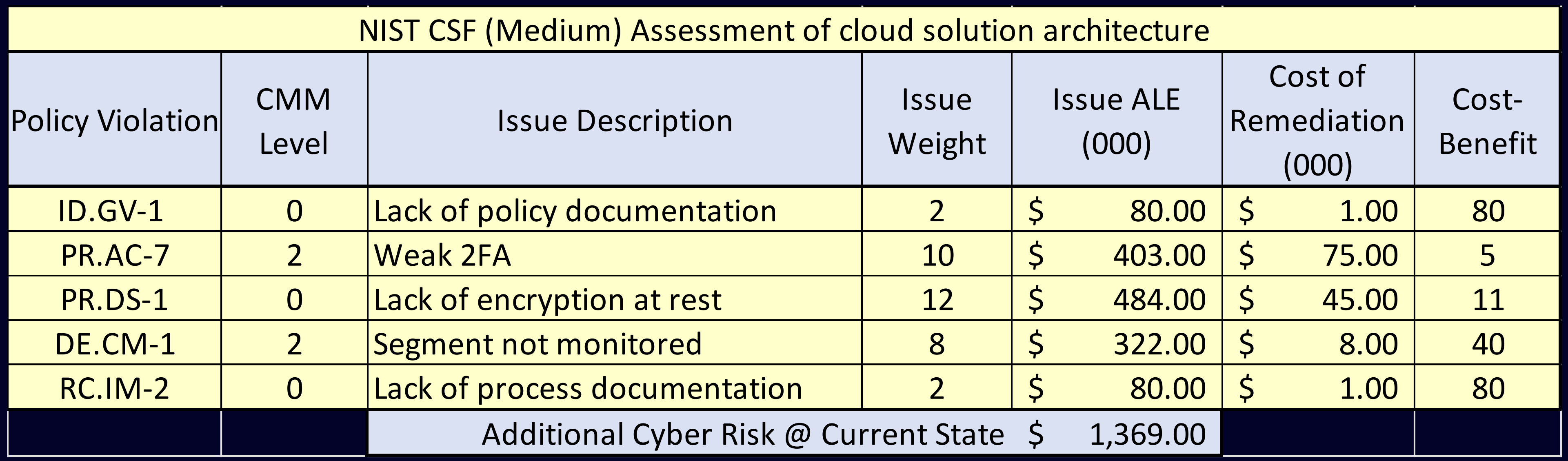
Derive the “R” in GRC

Business is well-informed

Solution cyber risk at policy: $230,000 ALE

Solution cyber risk w/ Issues: $1,599,000 ALE

Cyber Risk due to non-compliance: $1,369,00 ALE



NIST CSF (Medium) Assessment of cloud solution architecture

Policy Violation	CMM Level	Issue Description	Issue Weight	Issue ALE (000)	Cost of Remediation (000)	Cost-Benefit
ID.GV-1	0	Lack of policy documentation	2	$ 80.00	$ 1.00	80
PR.AC-7	2	Weak 2FA	10	$ 403.00	$ 75.00	5
PR.DS-1	0	Lack of encryption at rest	12	$ 484.00	$ 45.00	11
DE.CM-1	2	Segment not monitored	8	$ 322.00	$ 8.00	40
RC.IM-2	0	Lack of process documentation	2	$ 80.00	$ 1.00	80
		Additional Cyber Risk @ Current State		$ 1,369.00		

Mitigation cost = $130k 10:1

Refining the “R” in GRC @ Scale

Mike Radigan
miradiga@cisco.com

Resources

Steps 1-3

Clarifying terms

Controls

“Anything used to directly or indirectly affect the frequency or magnitude of loss”

Examples:

Policies

Passwords

Auditing

Data backups

Patching

Control Functions

“How a control directly or indirectly affects the frequency or magnitude of loss”

Examples:

Loss event prevention

Loss event detection

Variance prevention

Variance correction

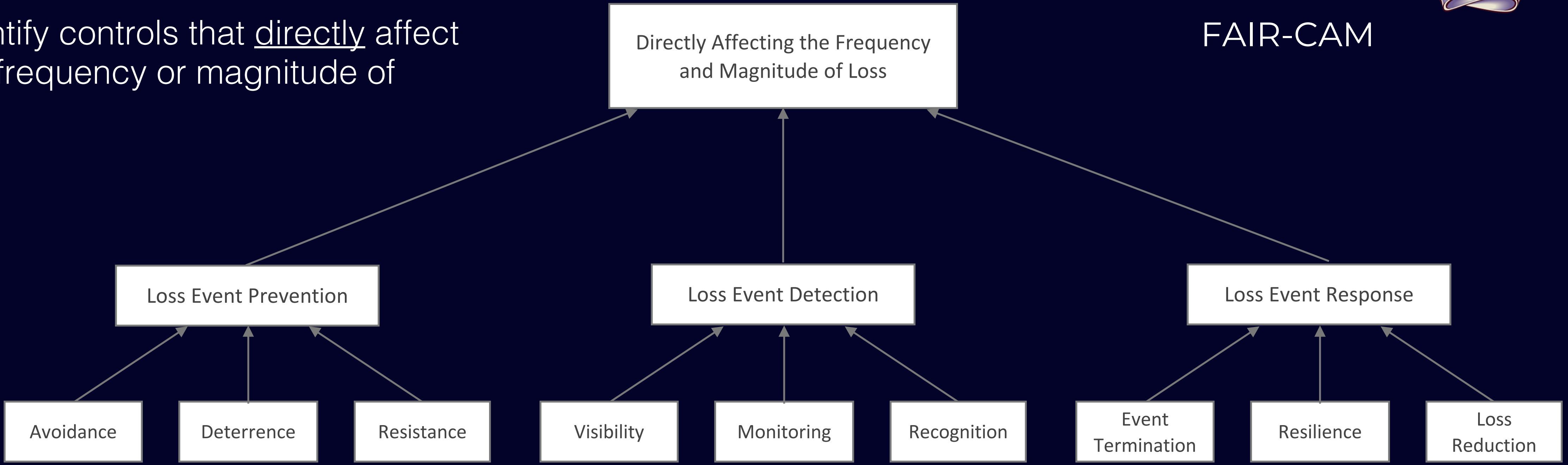
ID misaligned decisions

Copyright © 2022 FAIR Institute all rights reserved

Direct: Loss Event Controls

Identify controls that directly affect the frequency or magnitude of loss

FAIR-CAM



Directly Affecting the Frequency and Magnitude of Loss

Loss Event Prevention

- Avoidance
- Deterrence
- Resistance

Loss Event Detection

- Visibility
- Monitoring
- Recognition

Loss Event Response

- Event Termination
- Resilience
- Loss Reduction

Avoidance:

- Perimeter anti-malware
- URL filtering…

Resistance:

- Endpoint anti-malware
- Personnel ability to recognize phishing…

Visibility:

- Anti-malware
- Host-based Intrusion detection…

Monitoring:

- Anti-malware
- Host-based Intrusion detection…

Recognition:

- Anti-malware
- Host-based Intrusion detection…

Event Termination:

- Incident response
- Forensics…

Resilience:

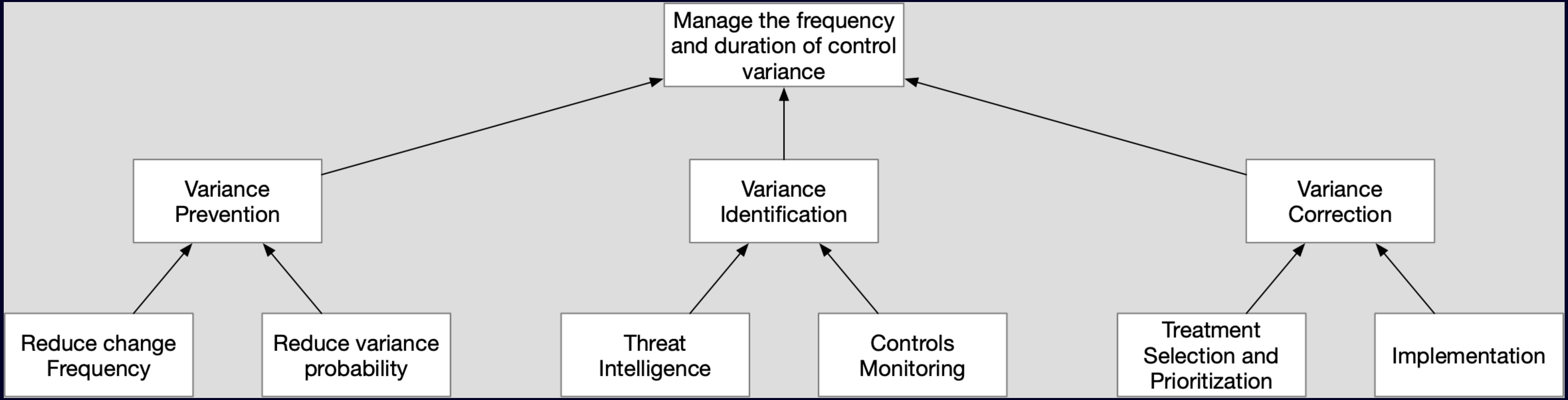
- Data backups
- Recovery processes…

Loss Reduction:

- Insurance…

Copyright © 2022 FAIR Institute all rights reserved

Indirect: Variance Management



Manage the frequency and duration of control variance

- Variance Prevention
  - Reduce change Frequency
  - Reduce variance probability
- Variance Identification
  - Threat Intelligence
  - Controls Monitoring
- Variance Correction
  - Treatment Selection and Prioritization
  - Implementation

- Local admin restrictions…

- Centralized anti-malware management

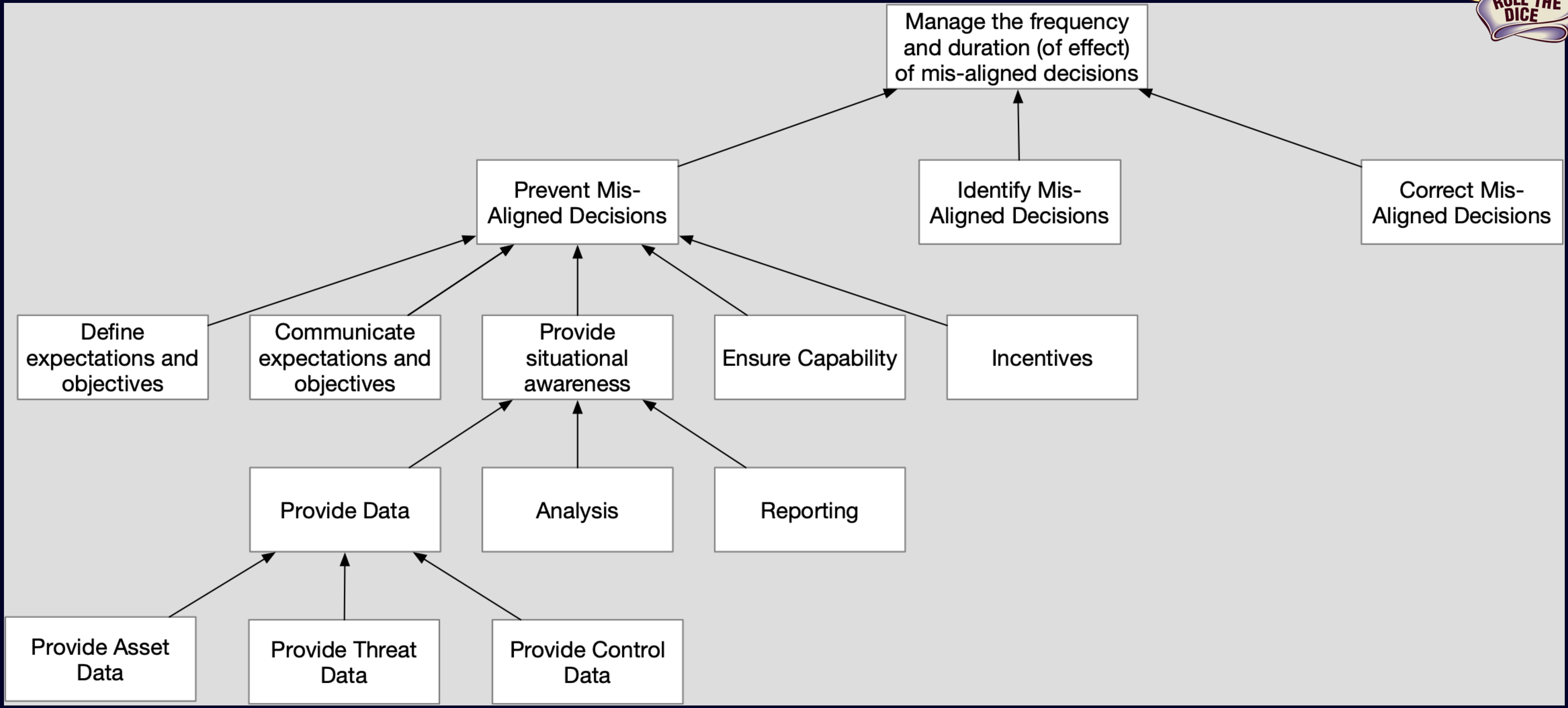
- Anti-malware provider…

- Centralized anti-malware reporting

- Centralized anti-malware signature updates…

Copyright © 2022 FAIR Institute all rights reserved

Indirect: Decision Support


Manage the frequency and duration (of effect) of mis-aligned decisions
Prevent Mis-Aligned Decisions
Identify Mis-Aligned Decisions
Correct Mis-Aligned Decisions
Define expectations and objectives
Communicate expectations and objectives
Provide situational awareness
Ensure Capability
Incentives
Provide Data
Analysis
Reporting
Provide Asset Data
Provide Threat Data
Provide Control Data

Copyright © 2022 FAIR Institute all rights reserved