How To CISO

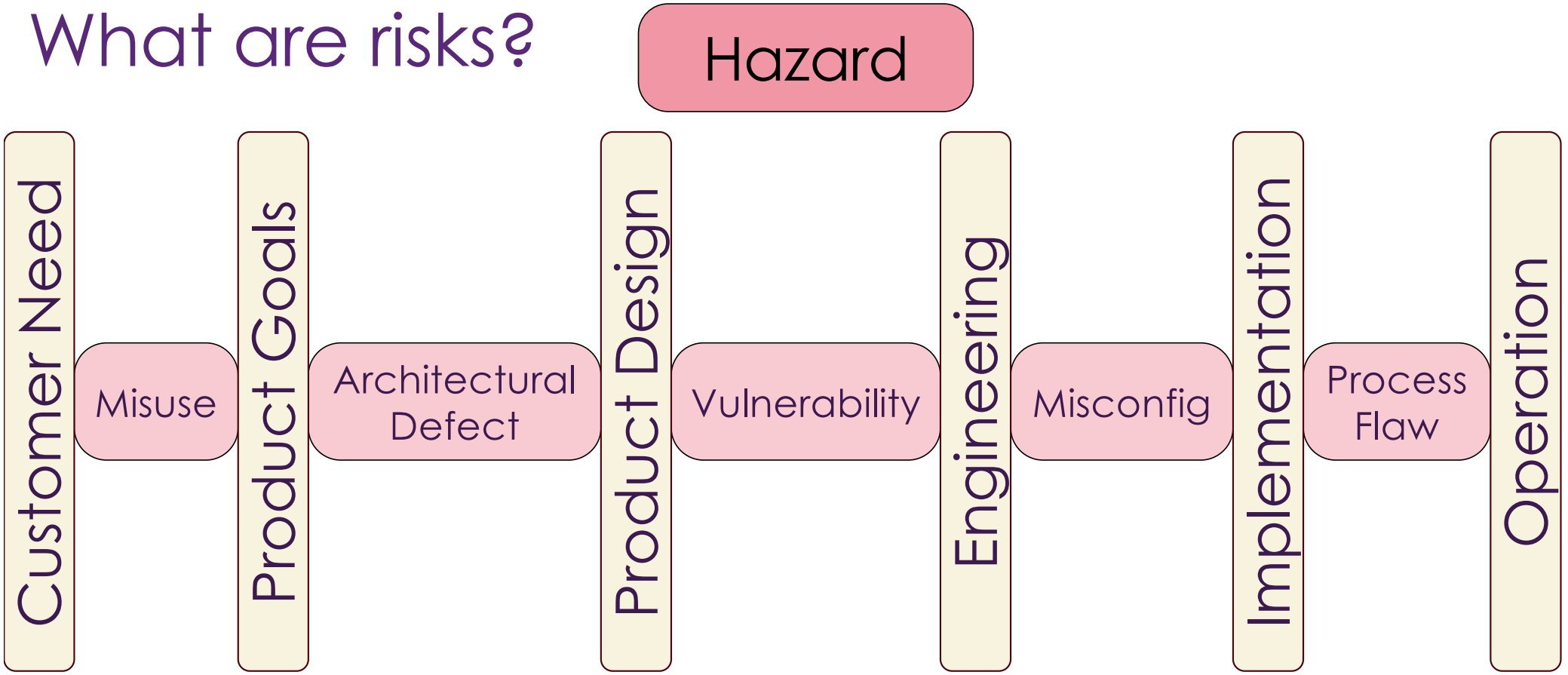
The Immeasurable Challenges of Risk Measurement

Andy Ellis



How To CISO

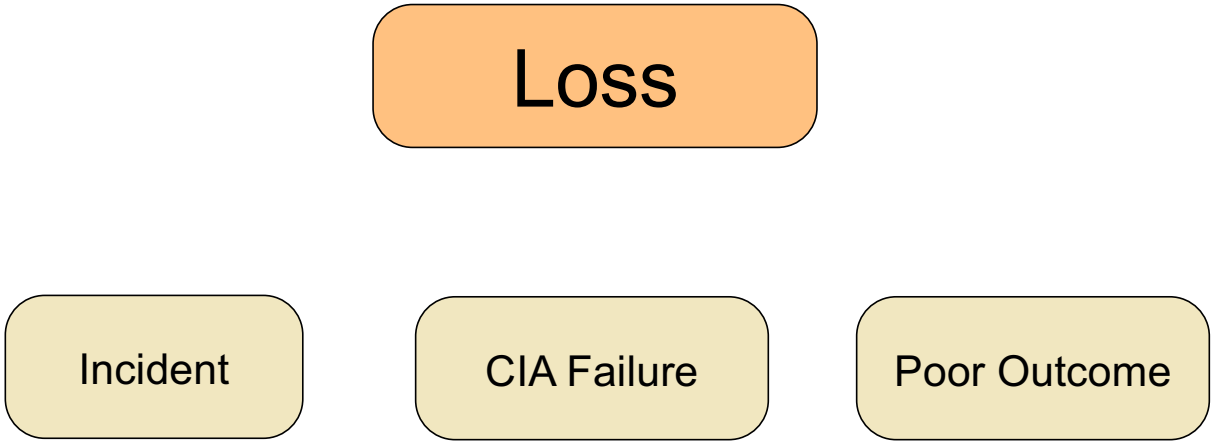
What are risks?



Mind the Gap!

How To CISO

What are risks?

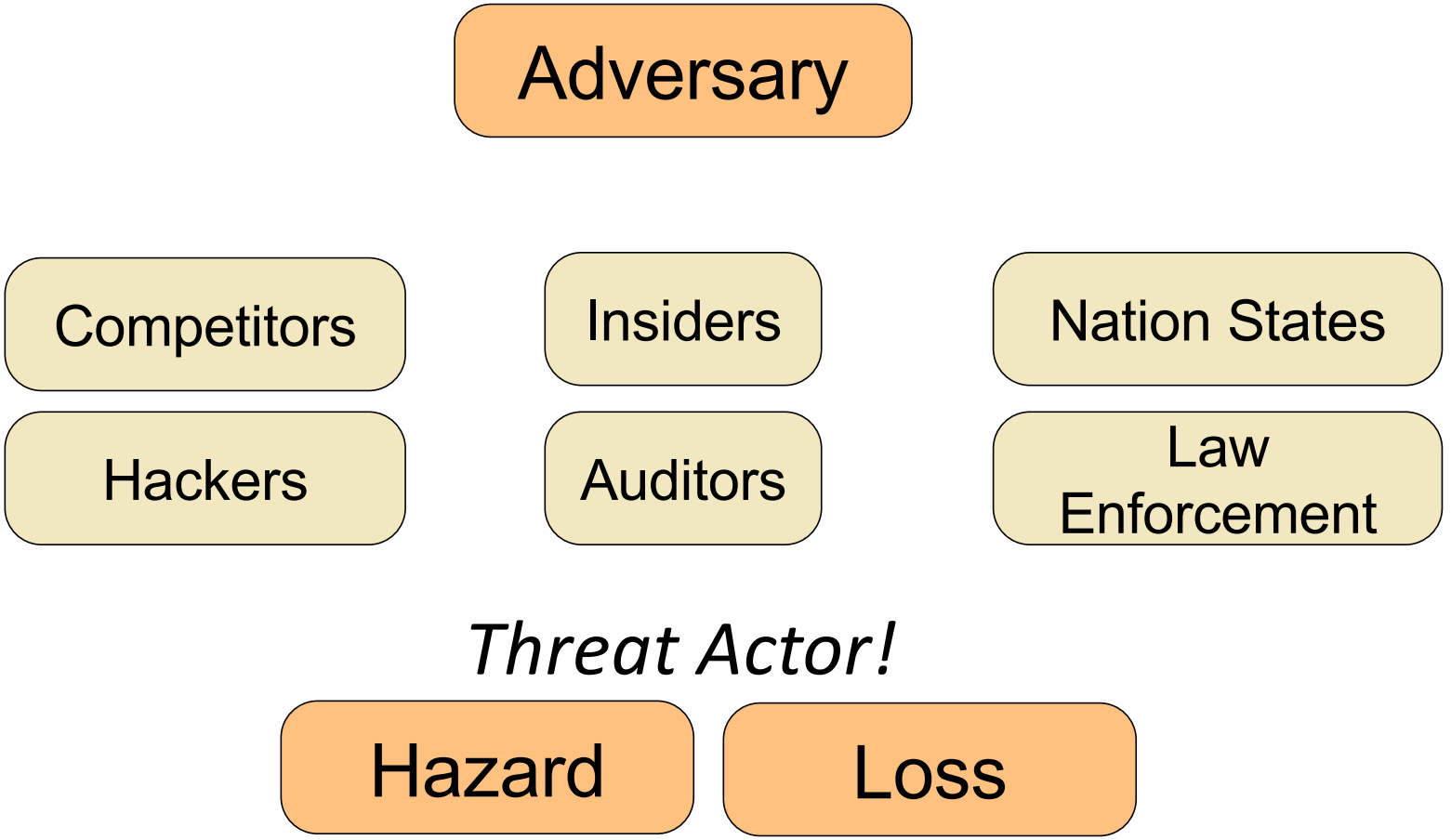


Unacceptable Loss!

Hazard

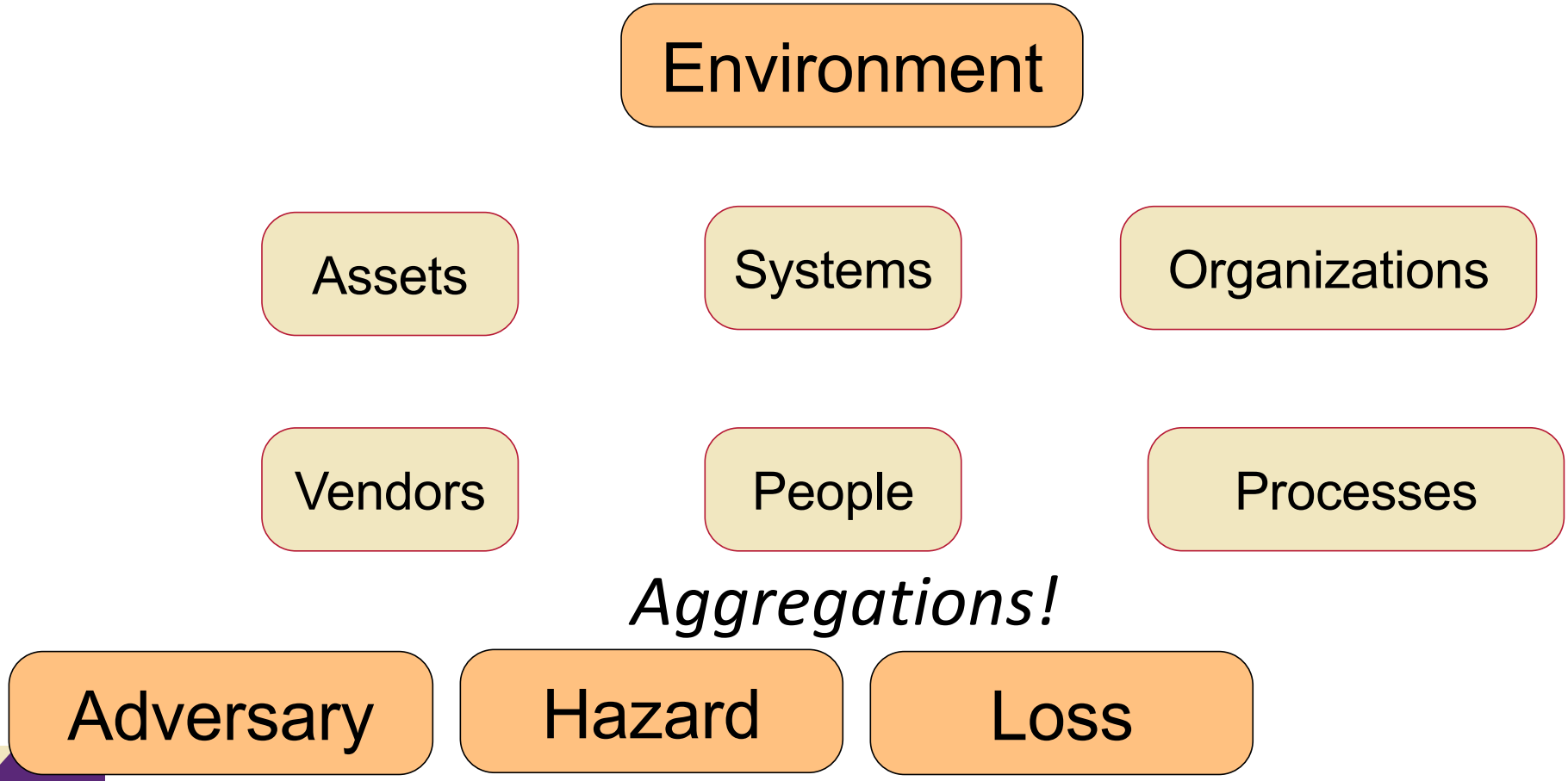
How To CISO

What are risks?



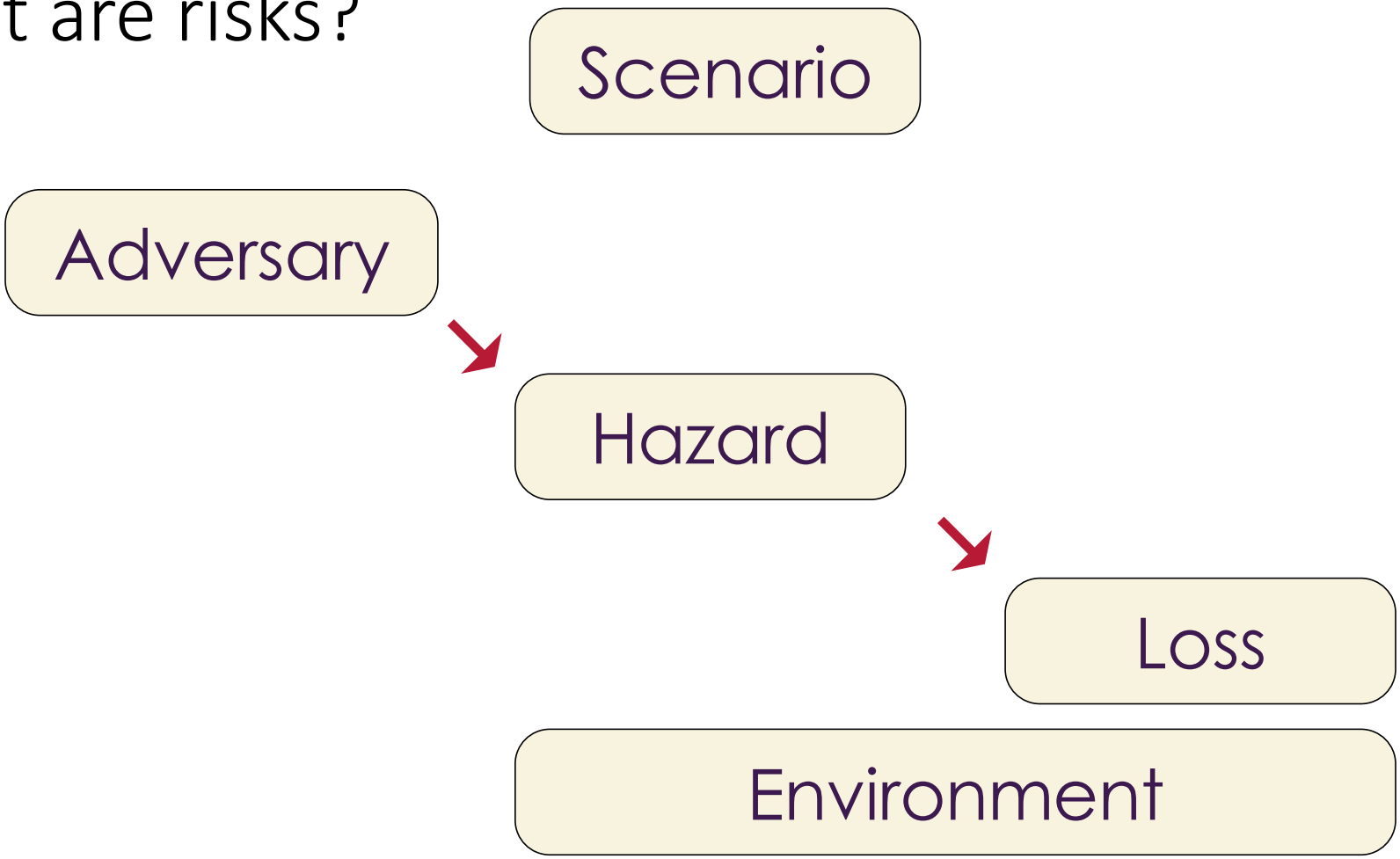
How To CISO

What are risks?



How To CISO

What are risks?



How To CISO

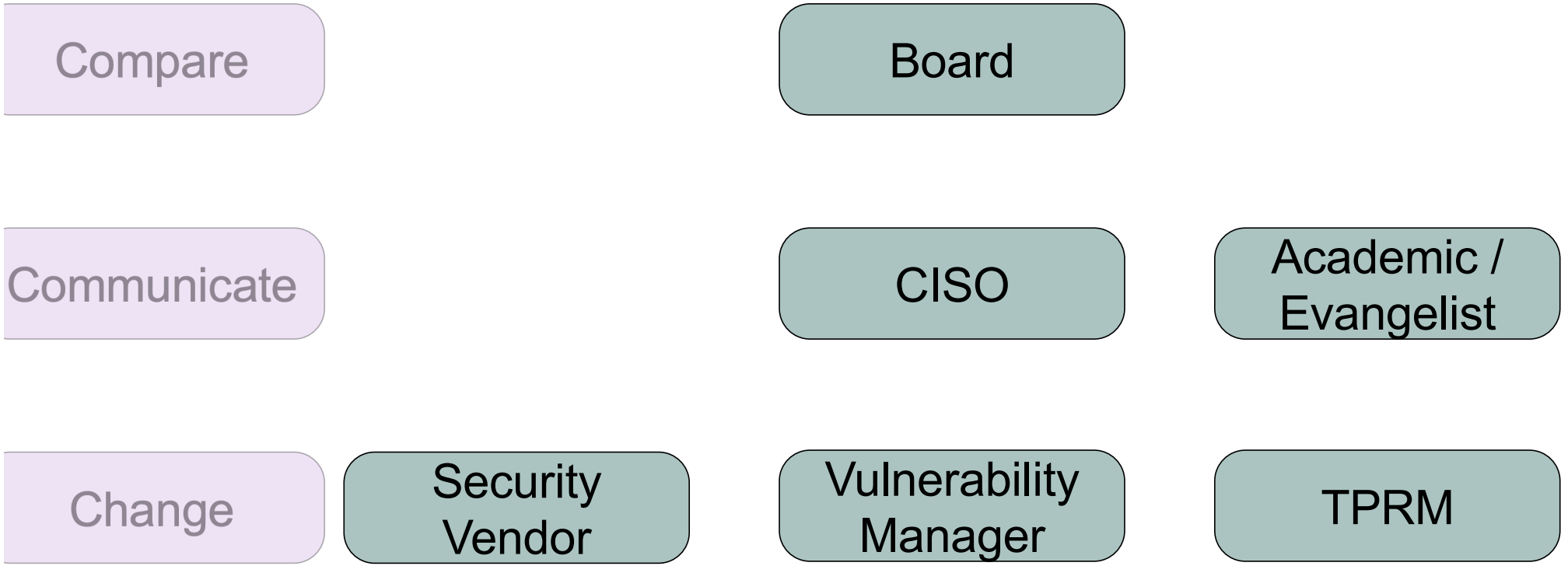
Why we measure risk

Compare

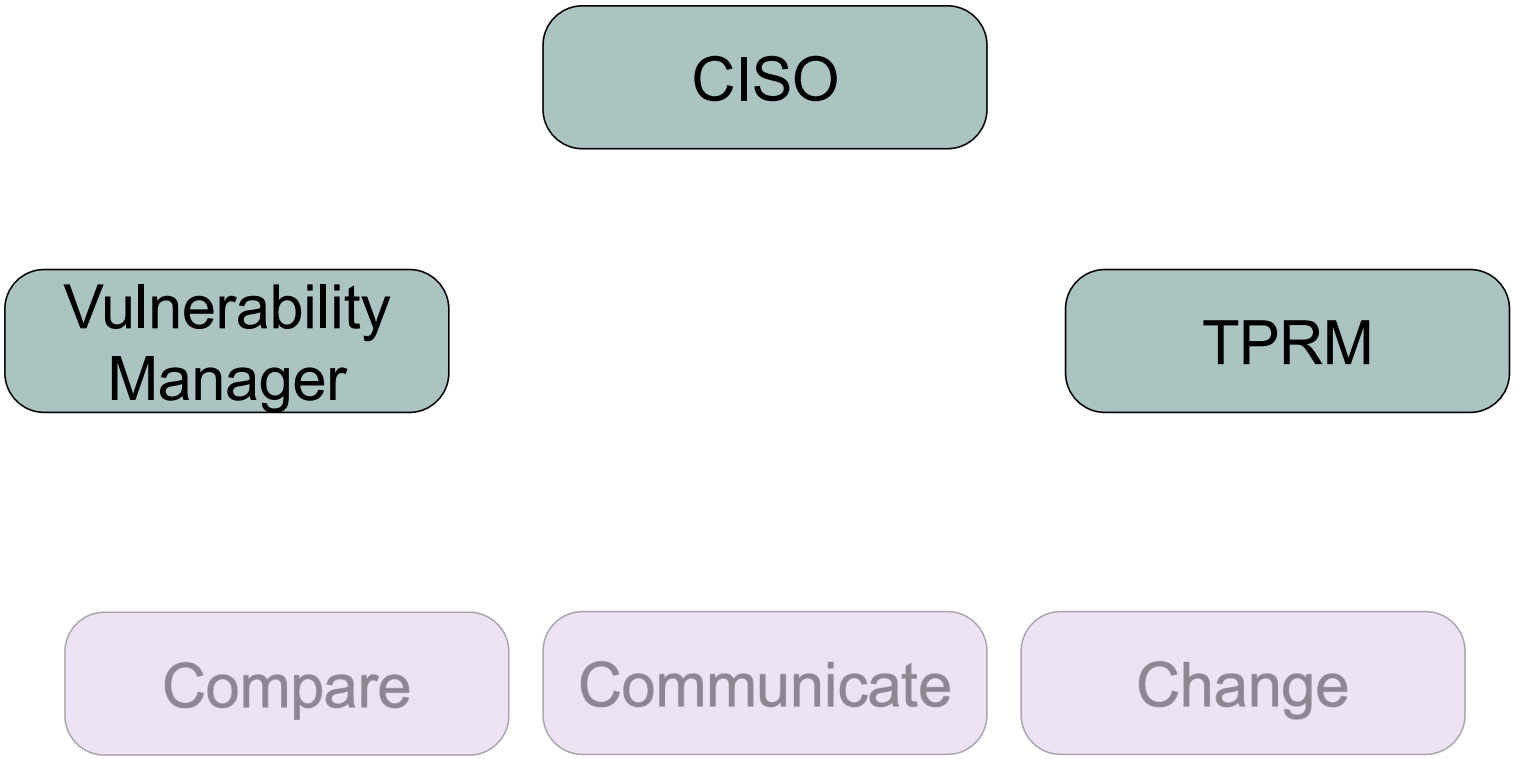
Communicate

Change

Who wants to measure risk, anyway?



Who wants to measure risk, anyway?



Risk Identification and Triage

Discovery
-Find a risk
-Preliminary evaluation

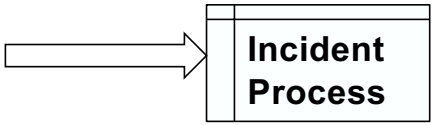
Evaluation
-Explore implications
-Assess remediations
-**Risk evaluation**

Prioritization
-Cost:benefit analysis
-Feasibility of success
-Business tradeoffs

Execution
-Define success criteria
-Establish program
-Executive oversight

Risk Identification and Triage

Discovery
-Find a risk
-Preliminary evaluation

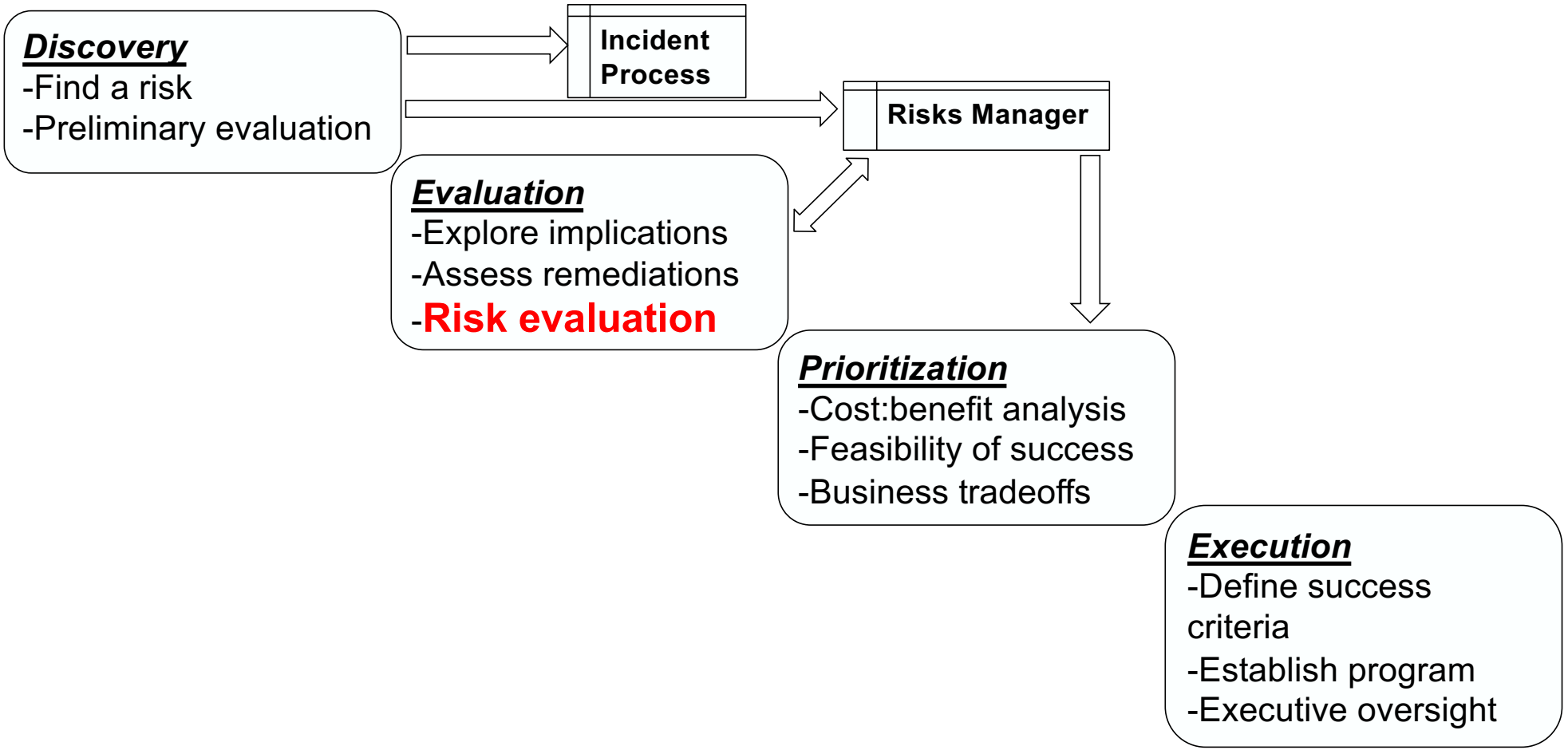


Evaluation
-Explore implications
-Assess remediations
-**Risk evaluation**

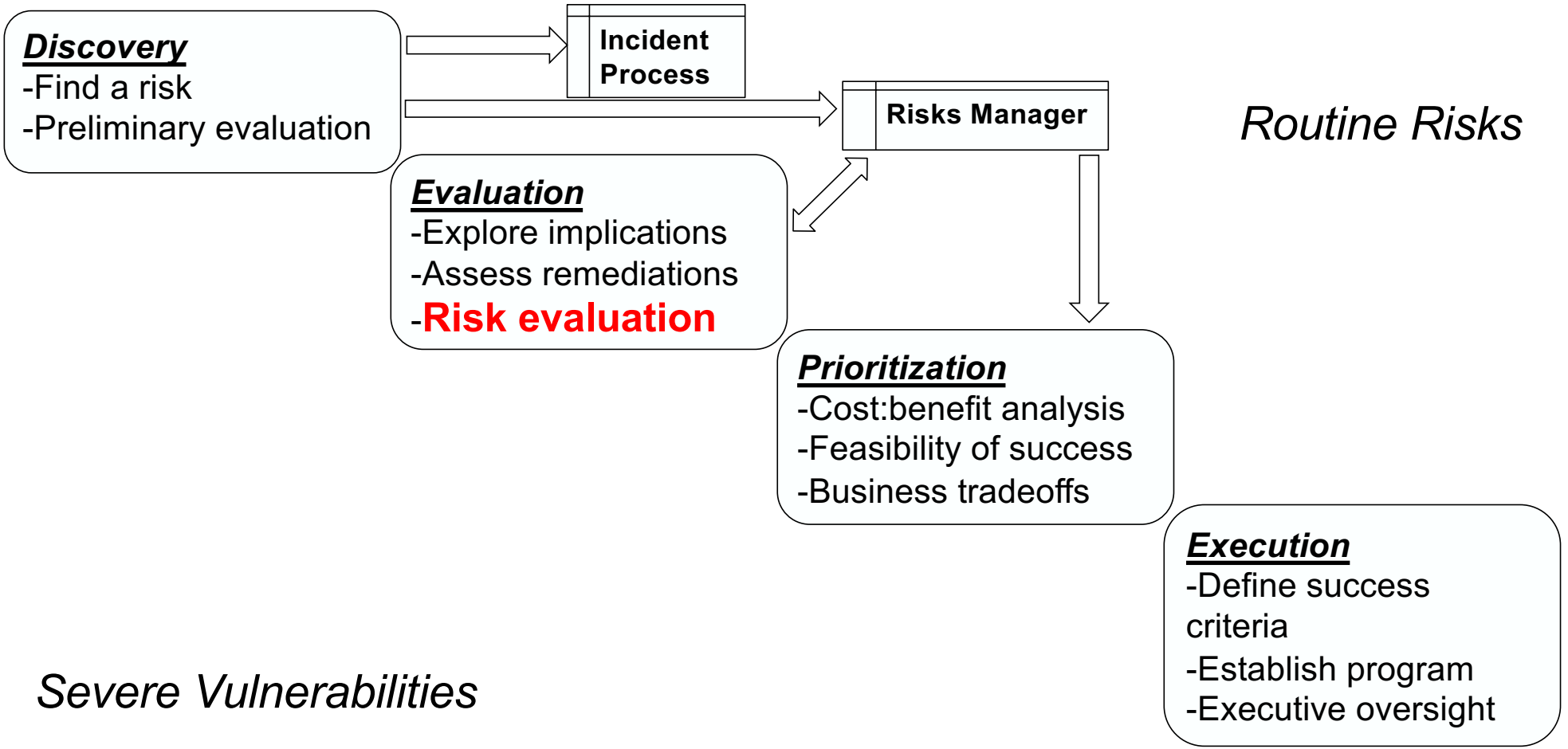
Prioritization
-Cost:benefit analysis
-Feasibility of success
-Business tradeoffs

Execution
-Define success criteria
-Establish program
-Executive oversight

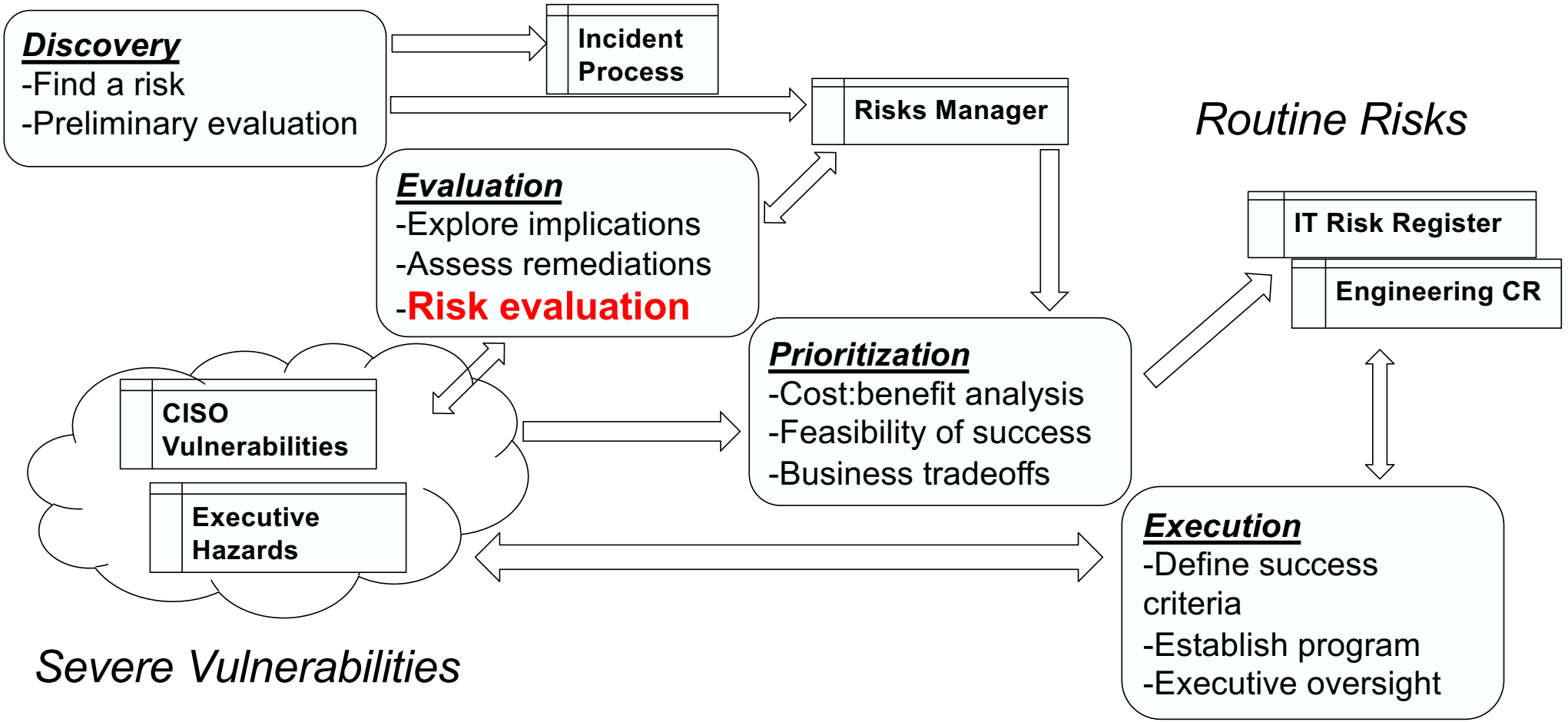
Risk Identification and Triage



Risk Identification and Triage



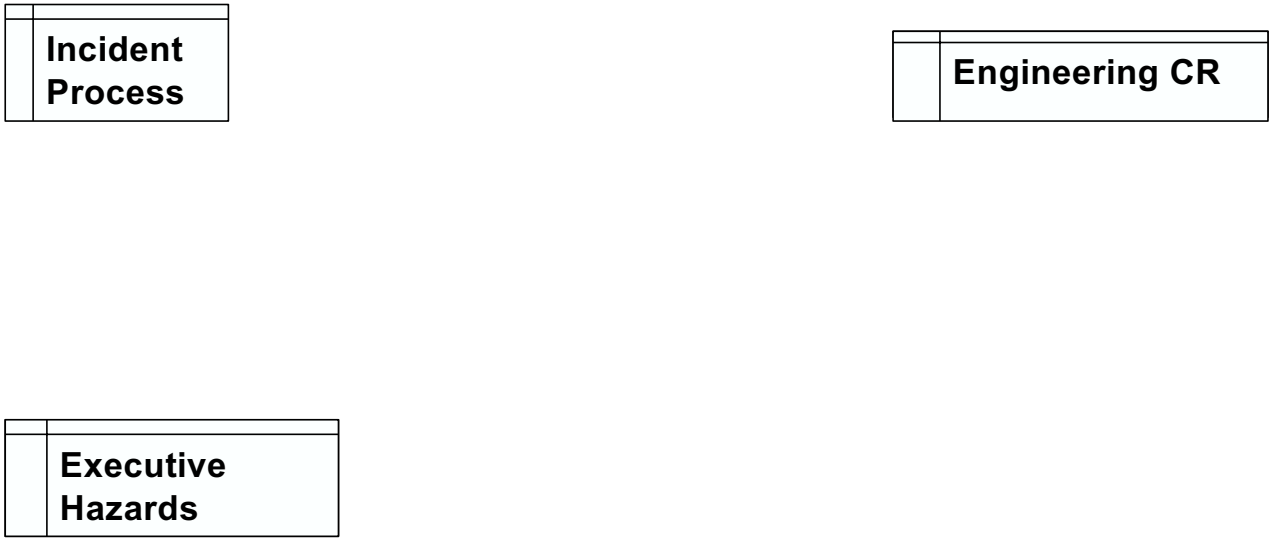
Risk Identification and Triage



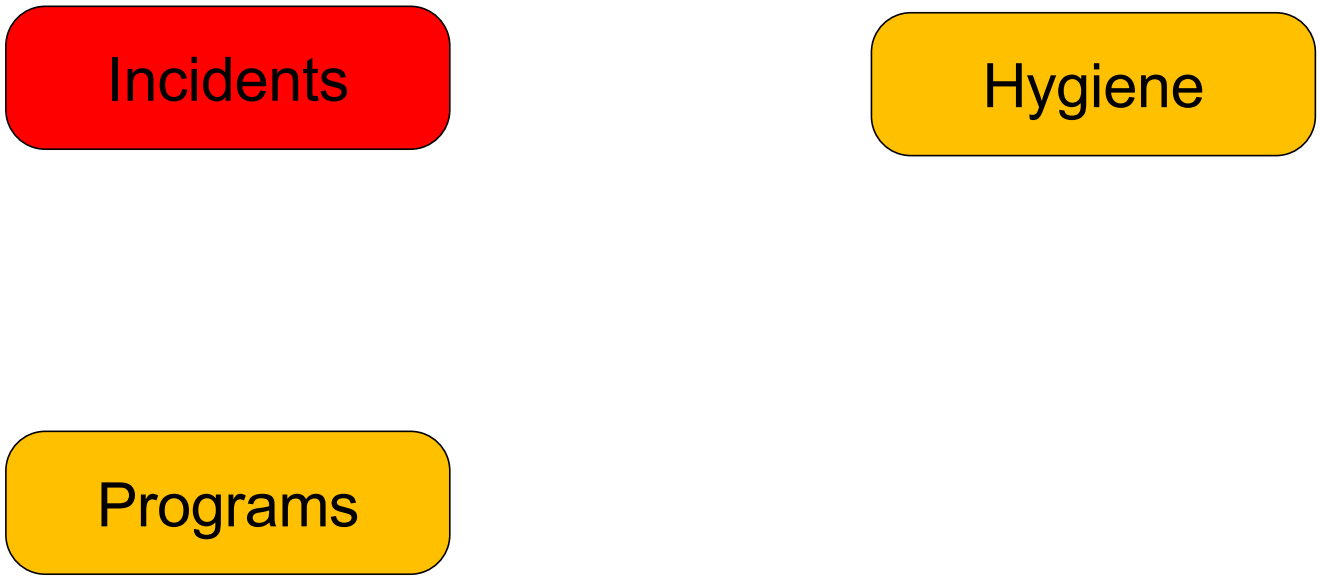
Risk Identification and Triage



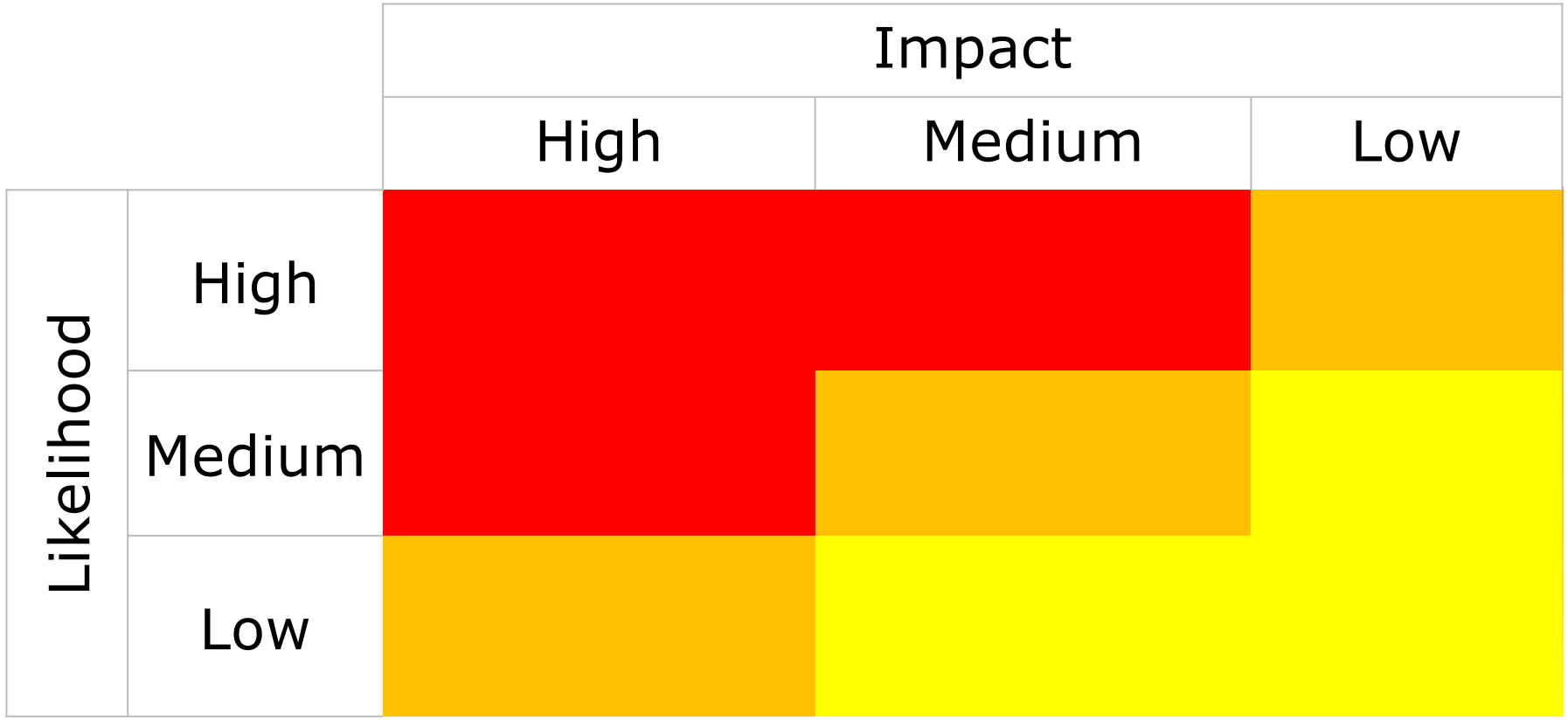
Risk Identification and Triage



Risk Identification and Triage

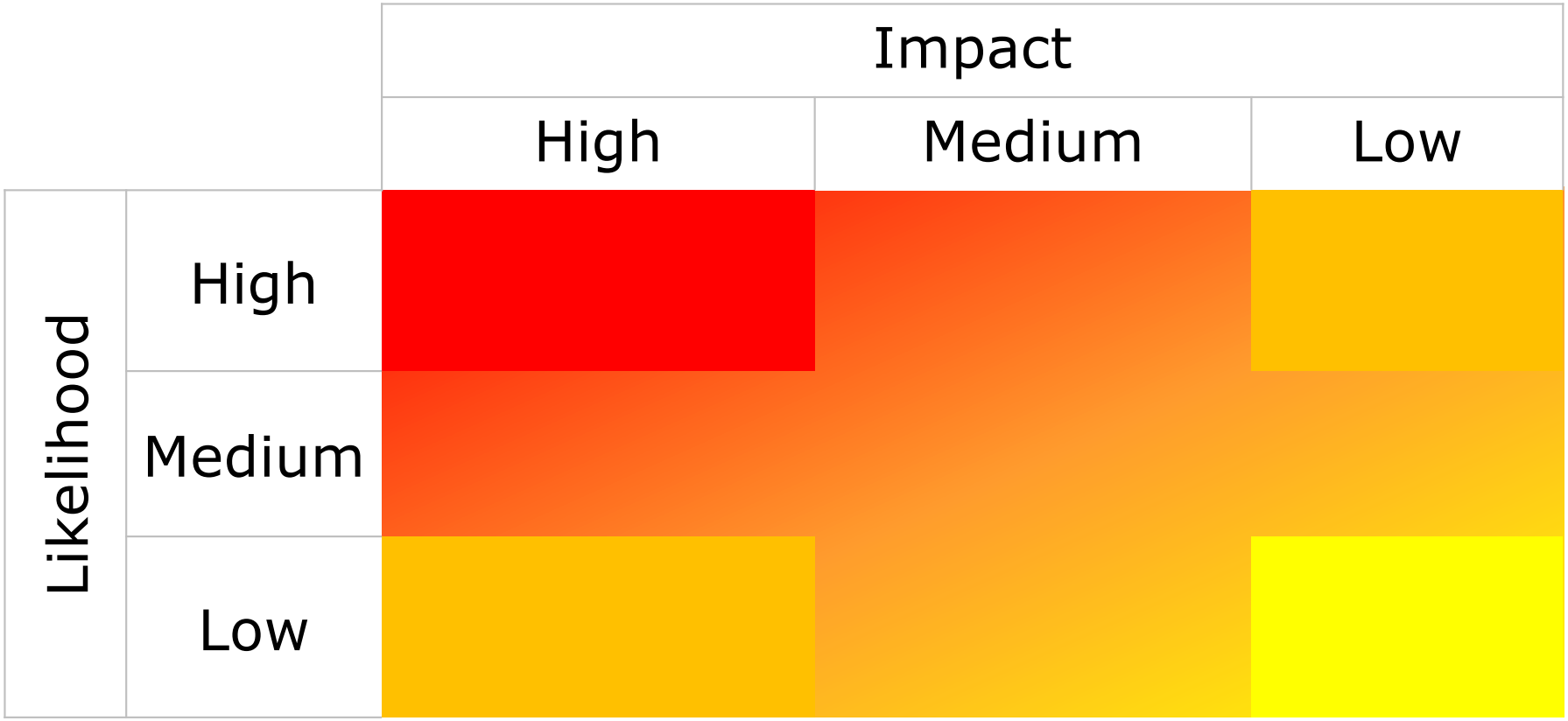


Nine-Box



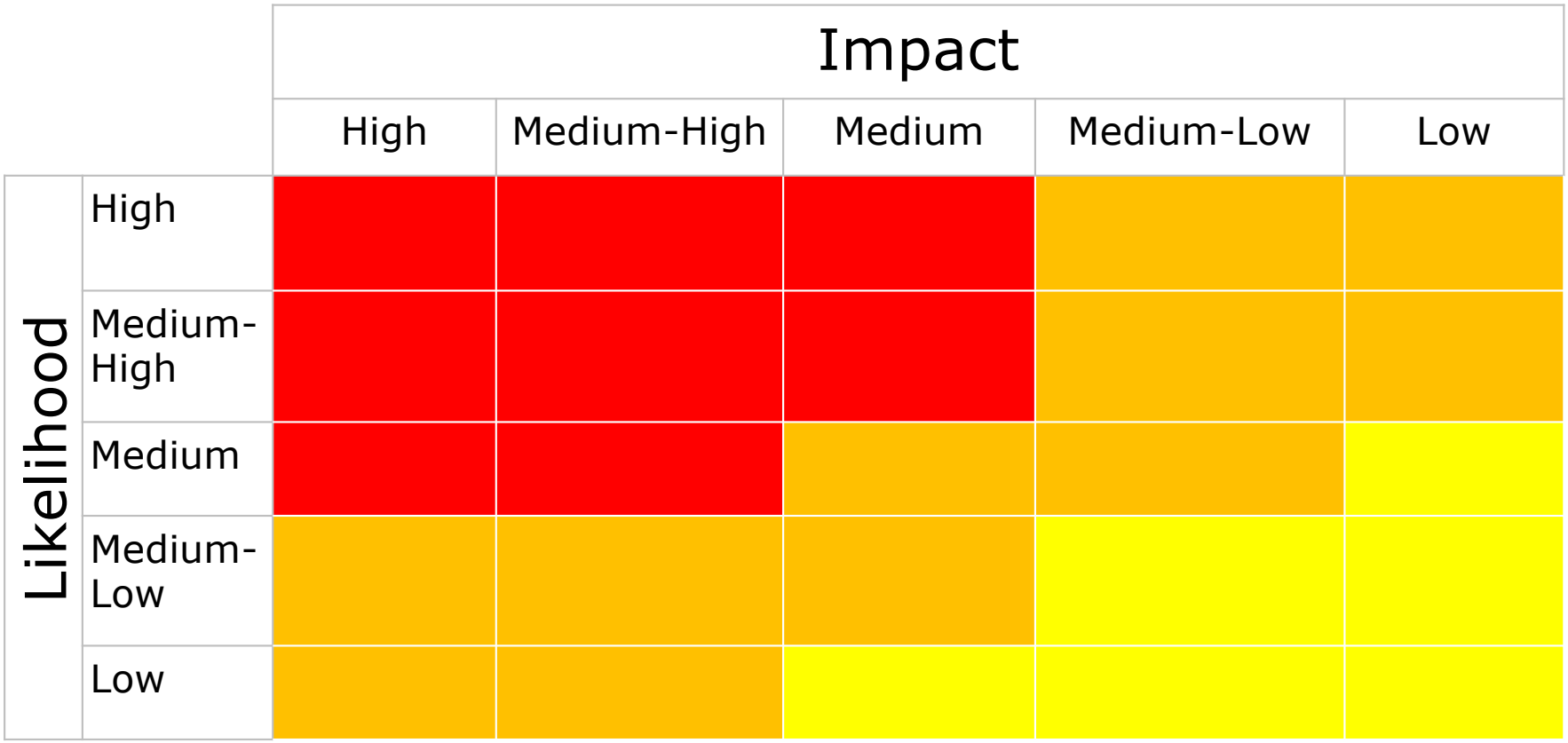
How To CISO

Five-Box



How To CISO

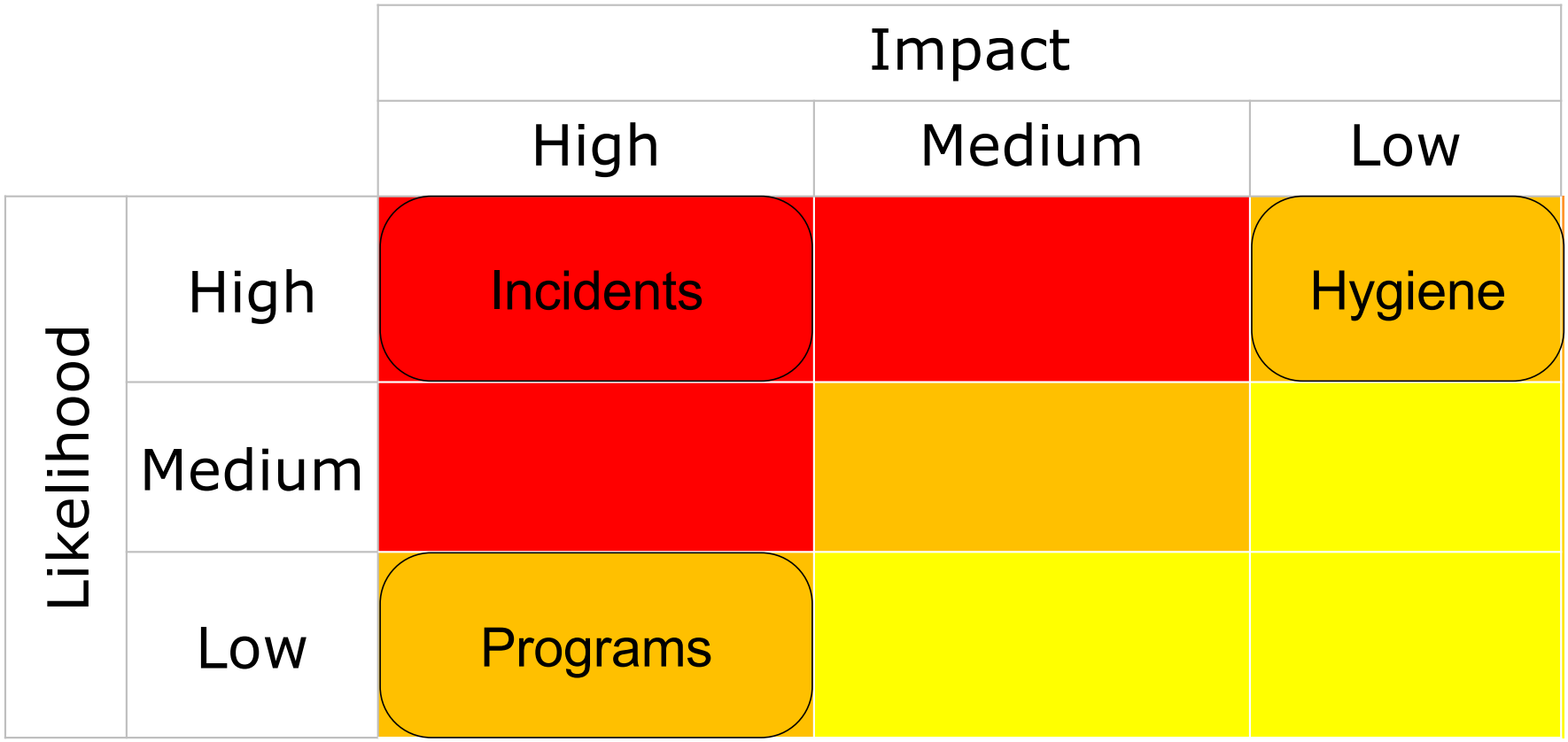
25-Box



How To CISO

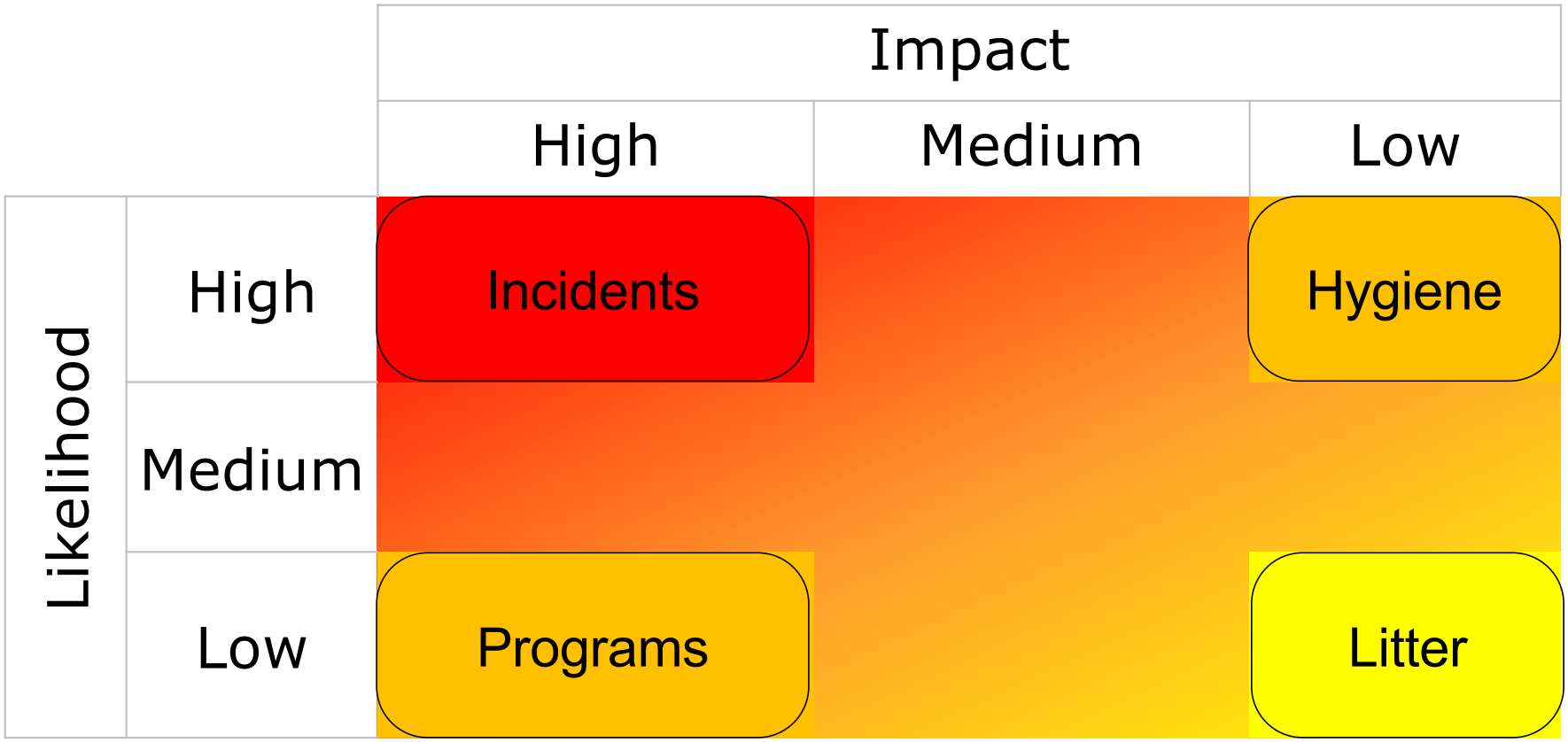
Nine-Box

Qualitative

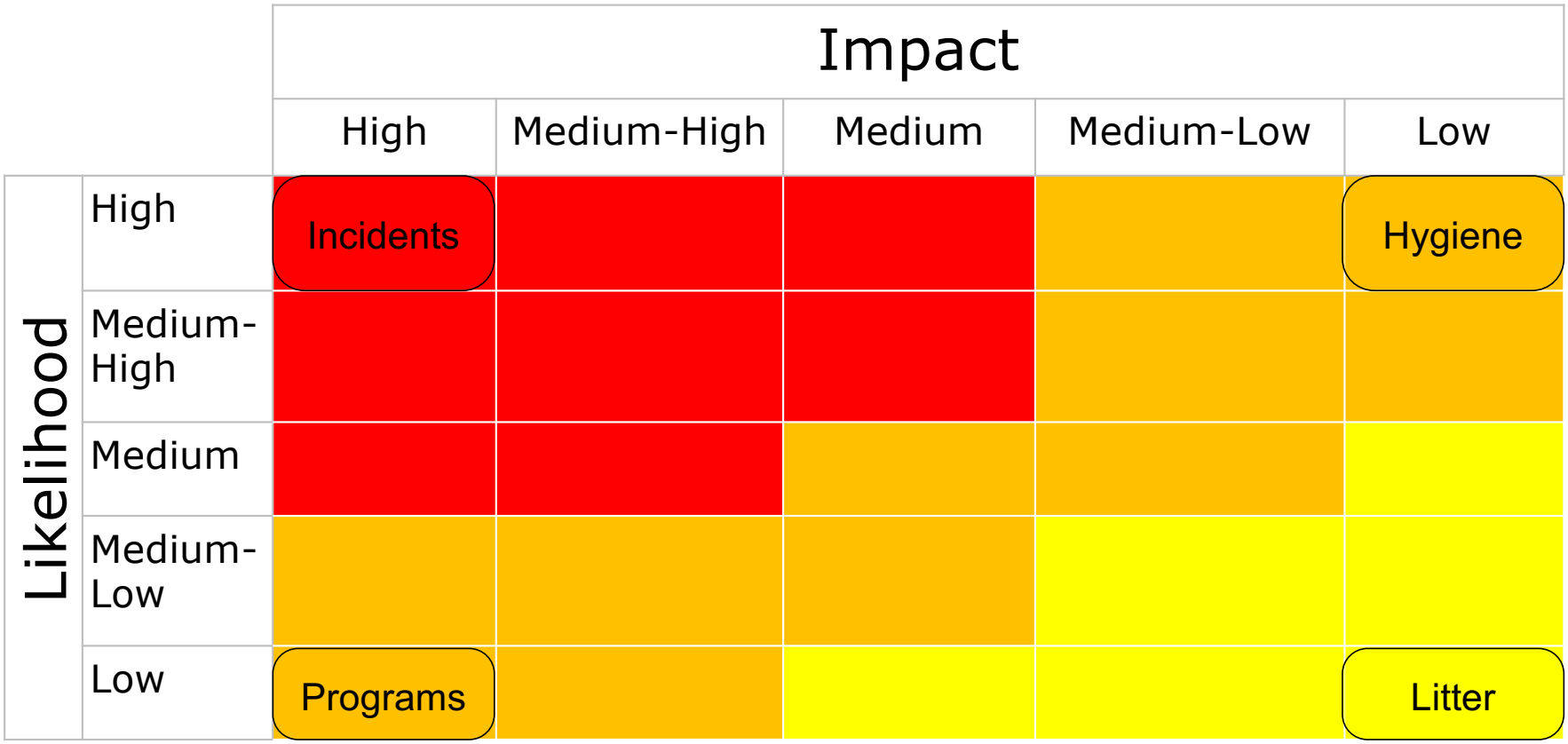


Five-Box

Qualitative



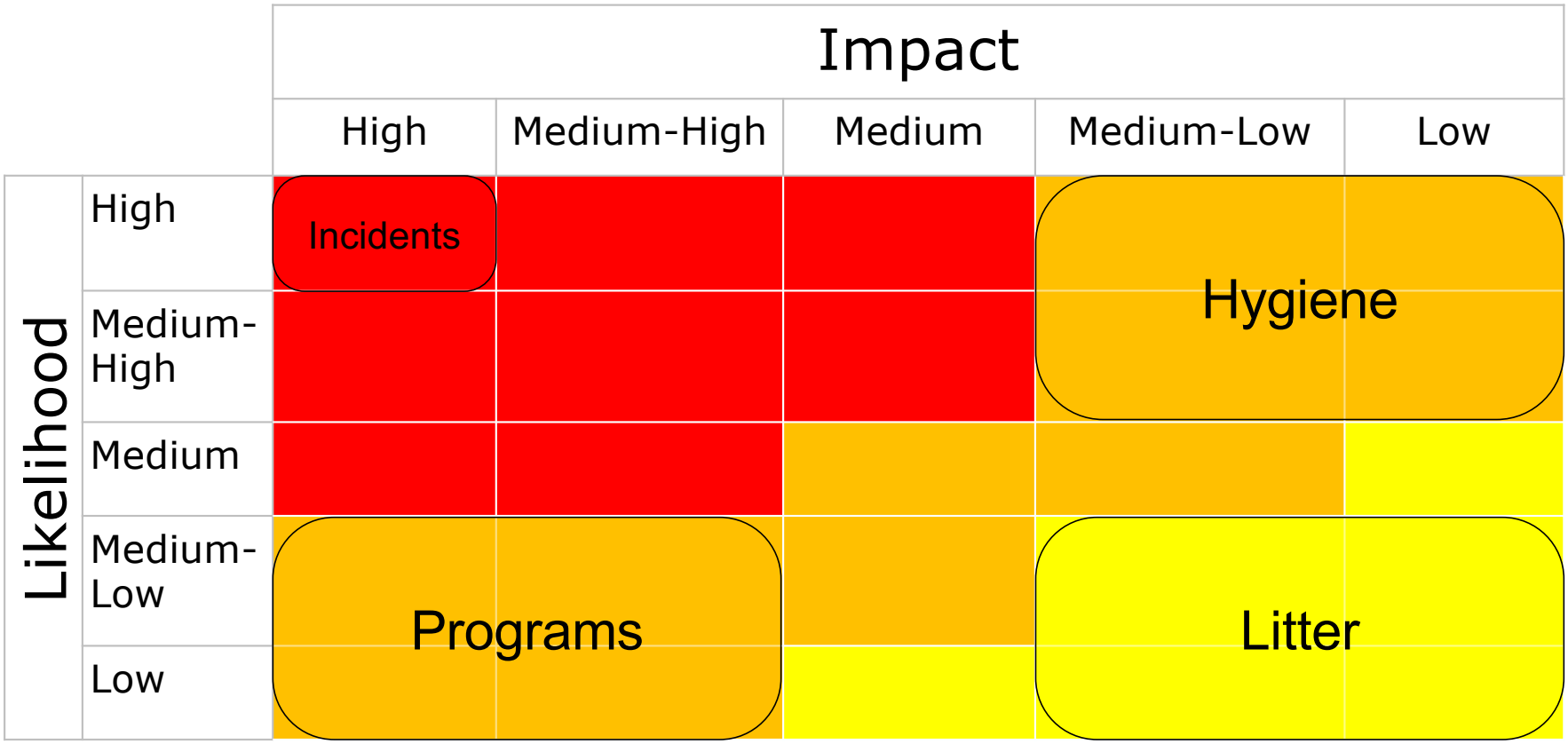
25-Box



How To CISO

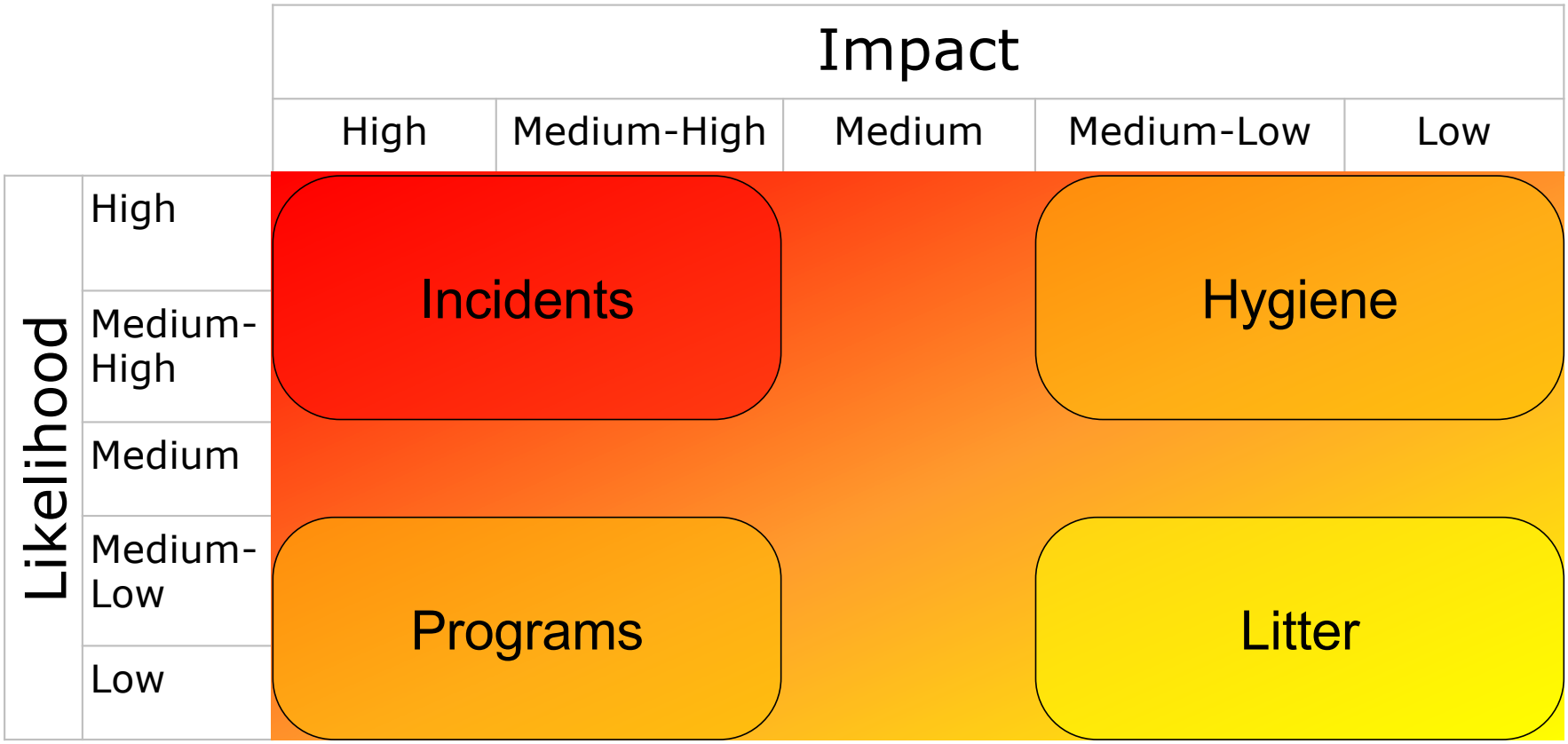
25-Box

Qualitative



25-Box

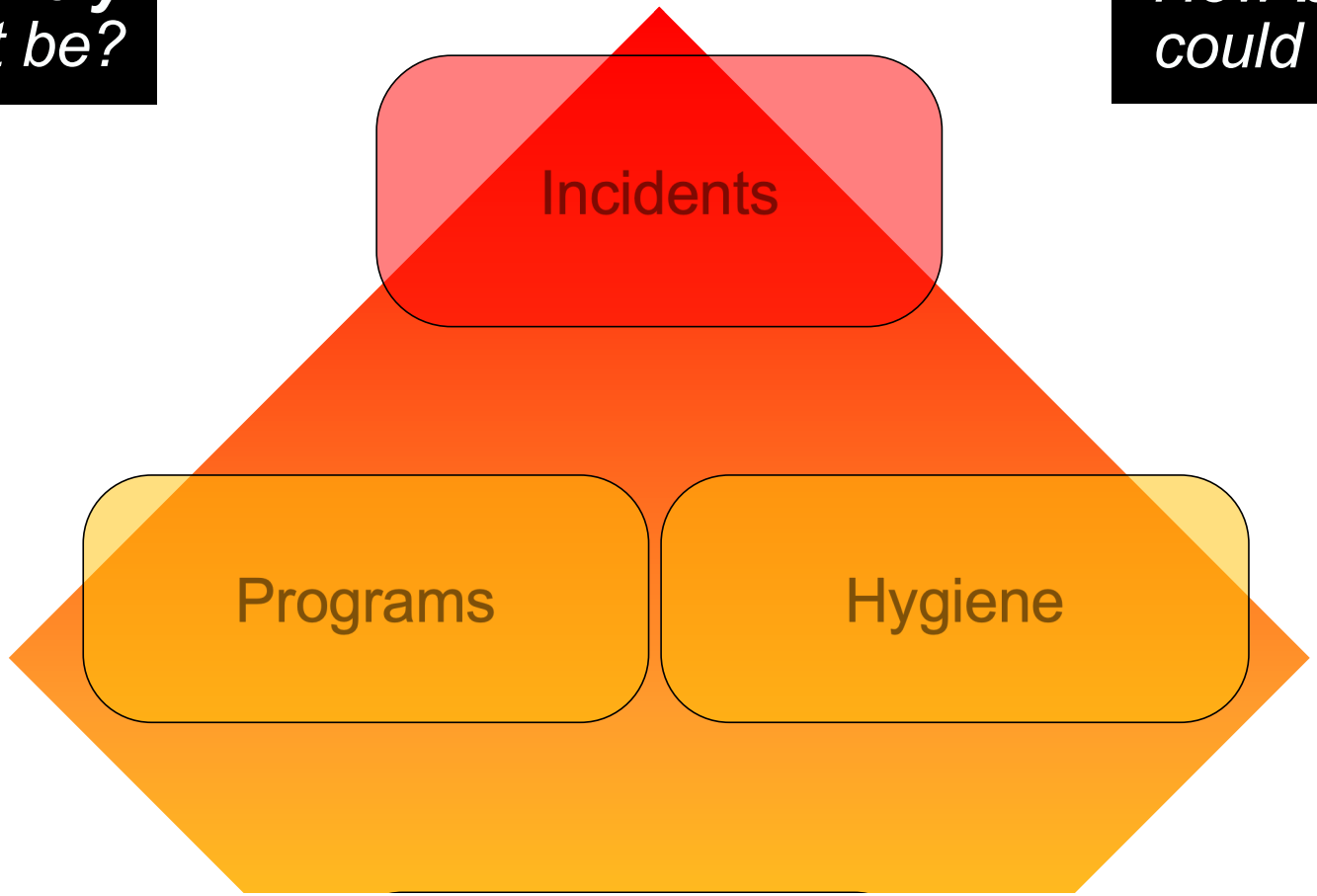
Qualitative



Qualitative

*How **likely** would it be?*

*How **bad** could it be?*

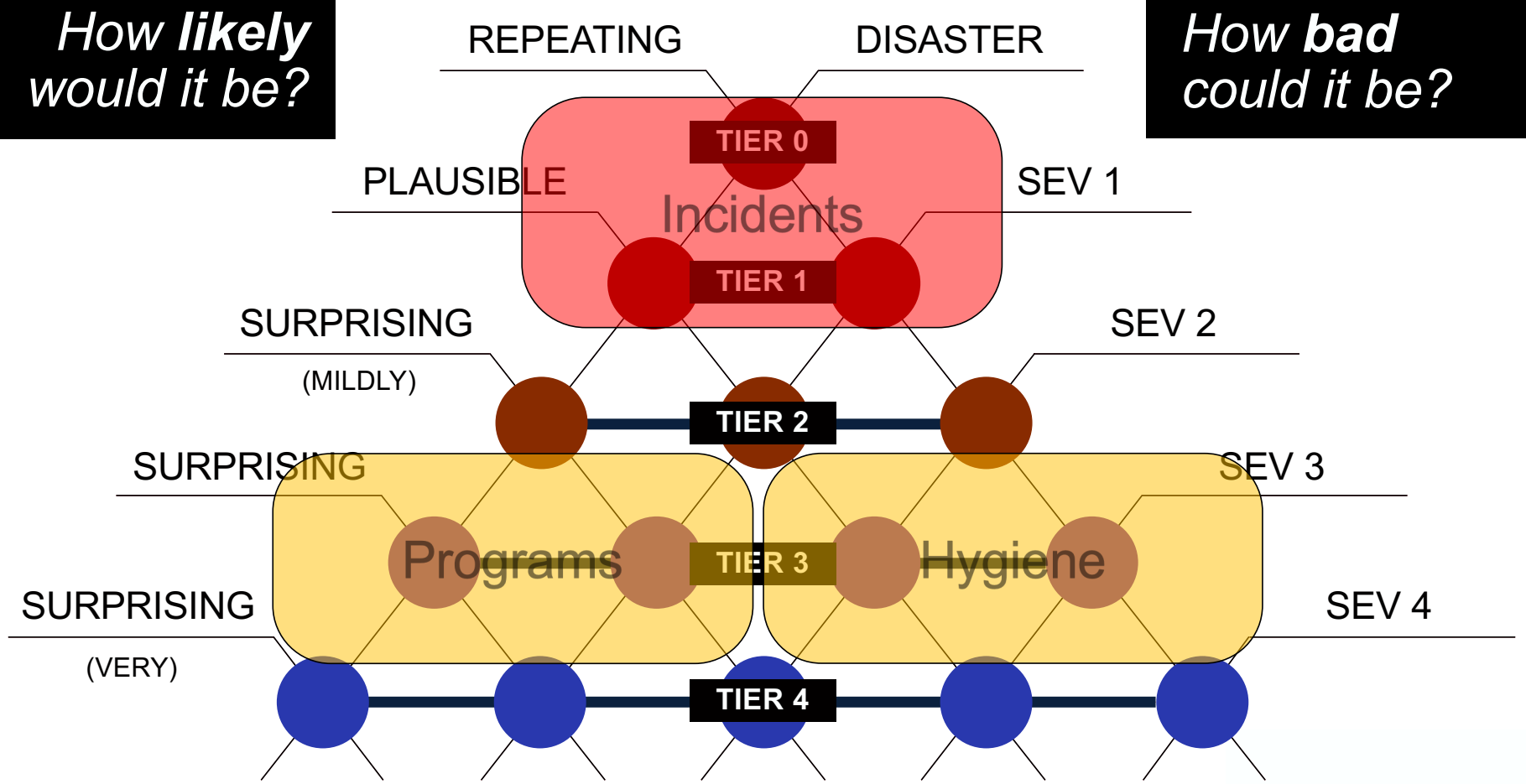


Impact Analysis

Qualitative

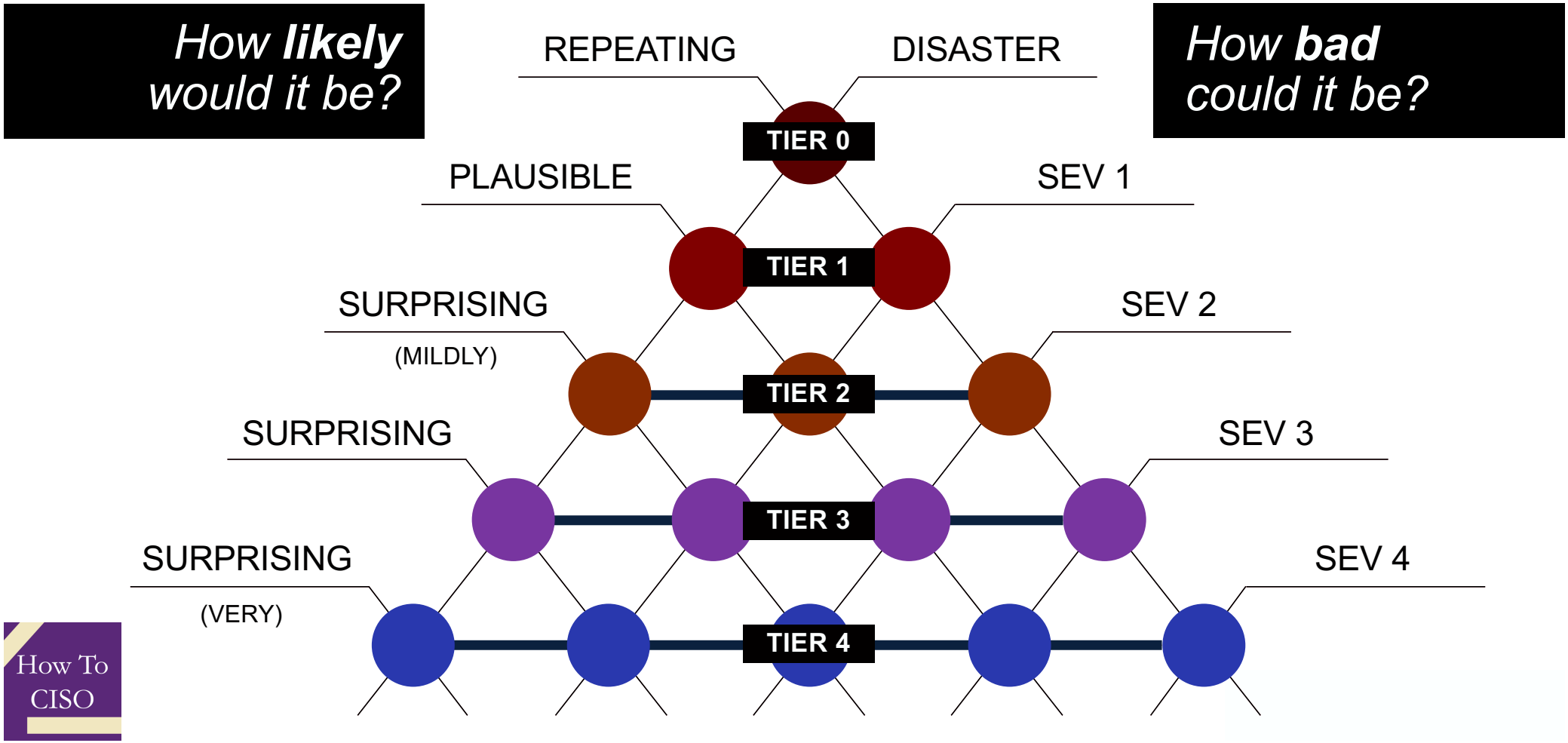
How likely would it be?

How bad could it be?

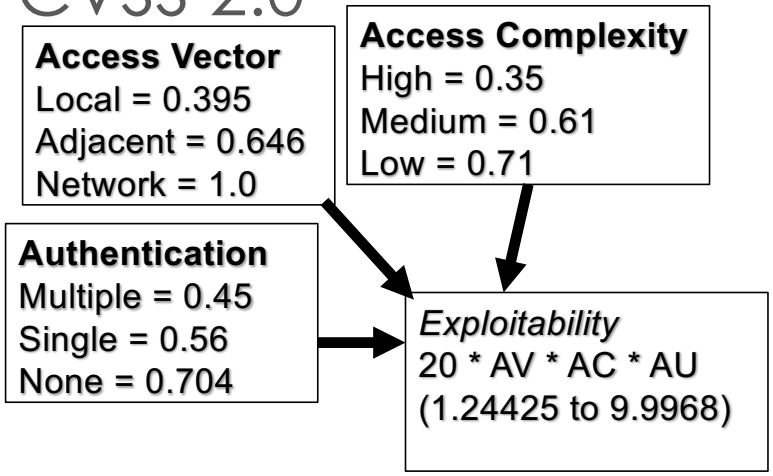


How To CISO

Pyramid of Pain



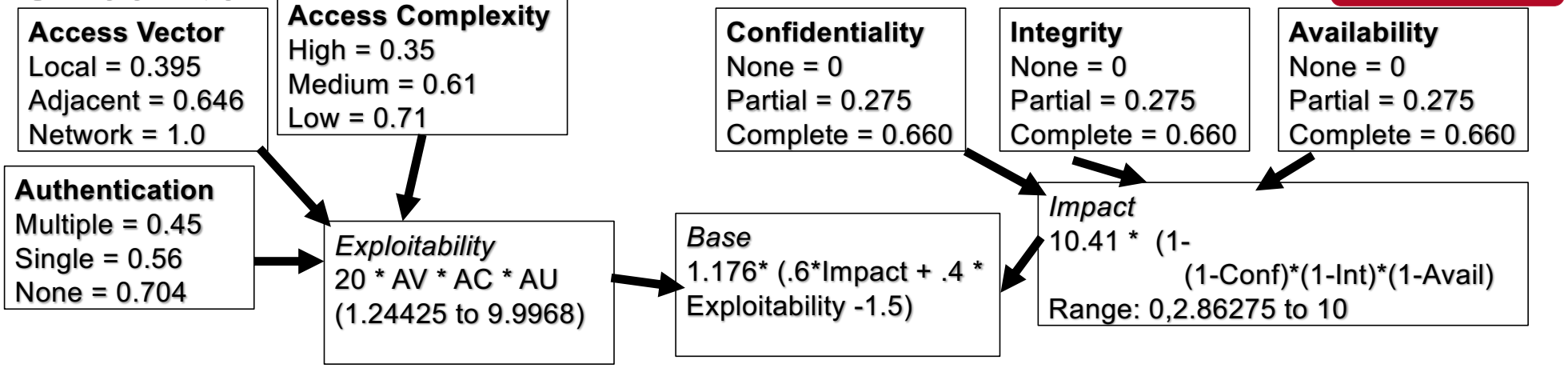
CVSS 2.0



Fermi

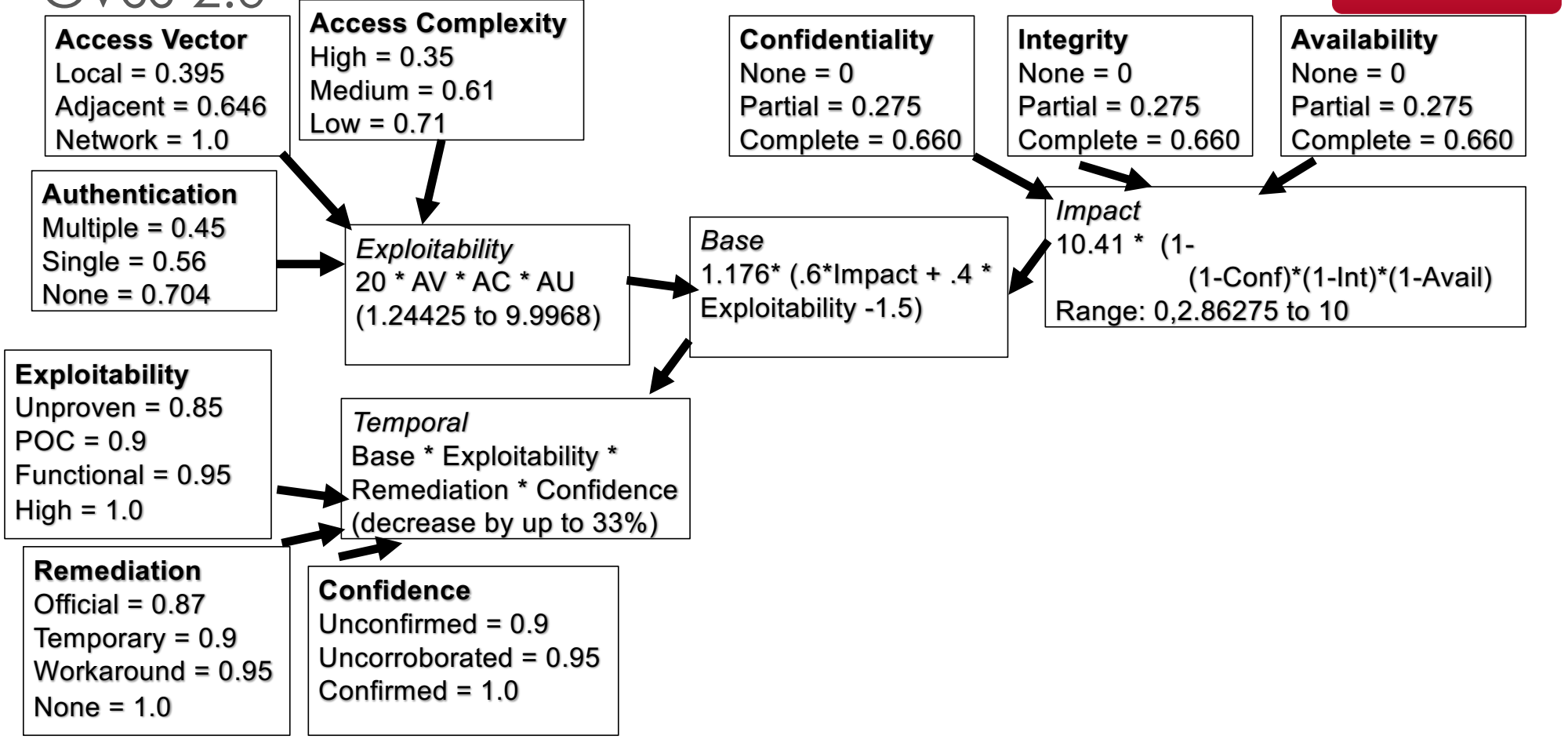
CVSS 2.0

Fermi

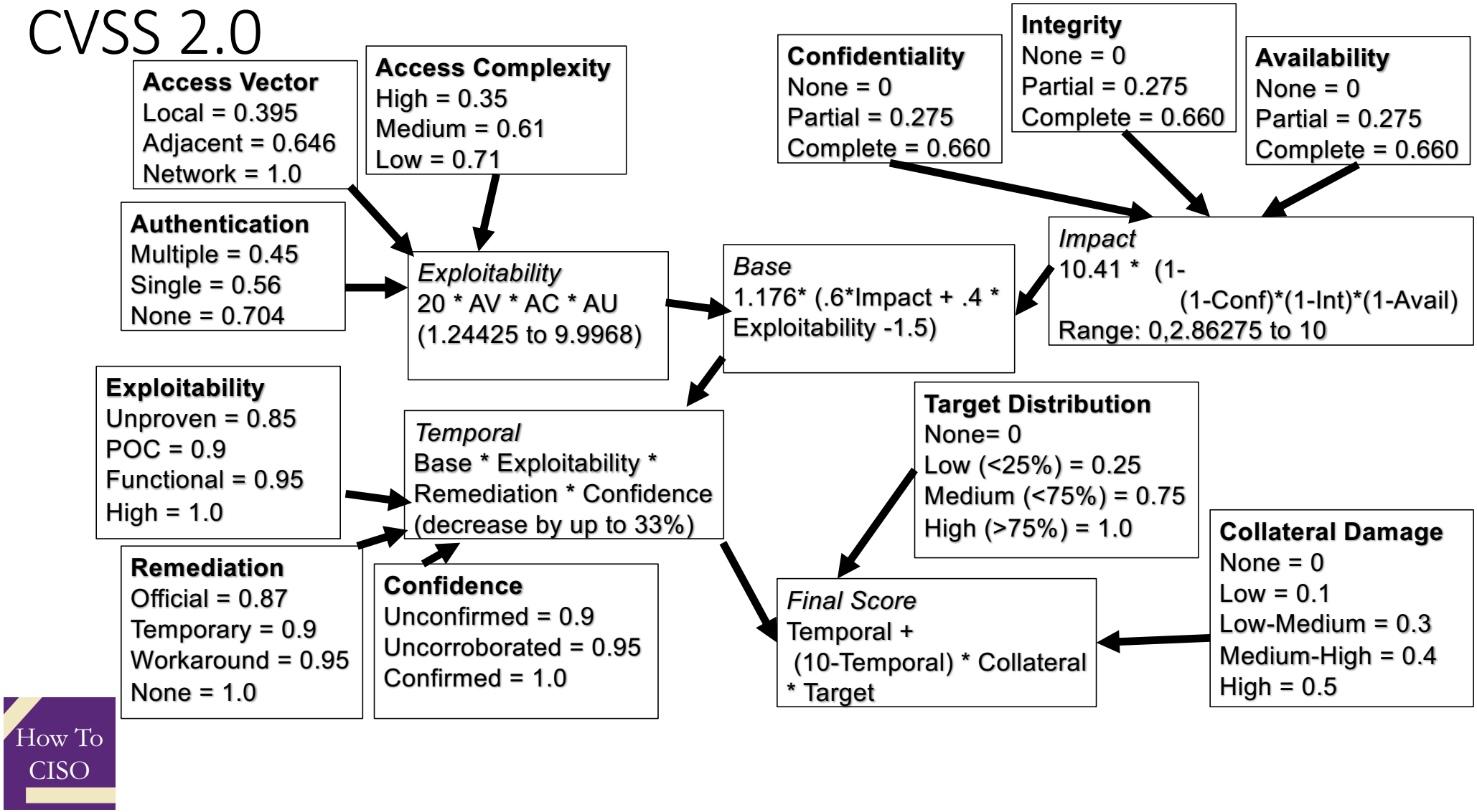


CVSS 2.0

Fermi



CVSS 2.0

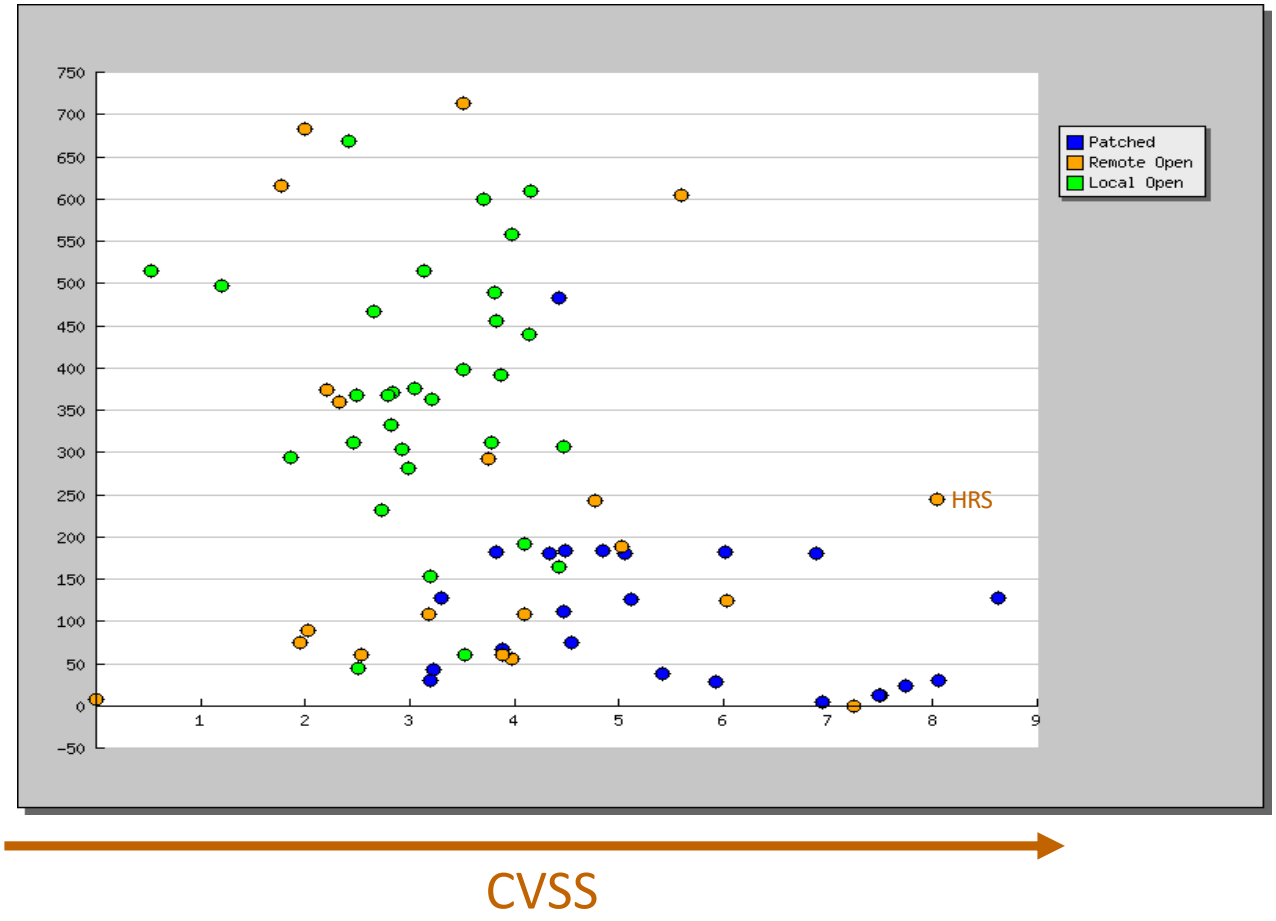


How To CISO

700K possibilities! (45M with customization)



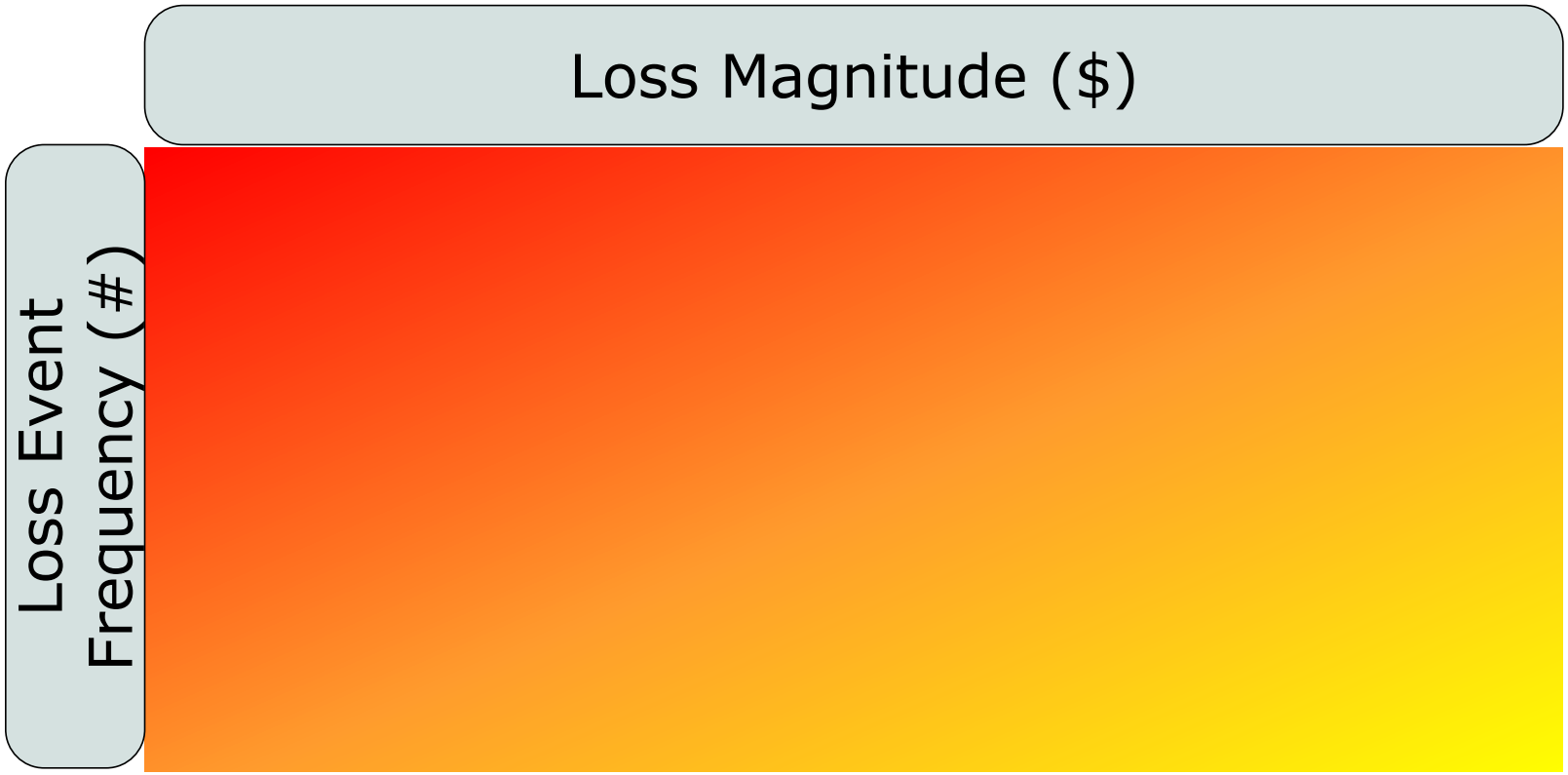
Or maybe about 30….



FAIR

Fermi

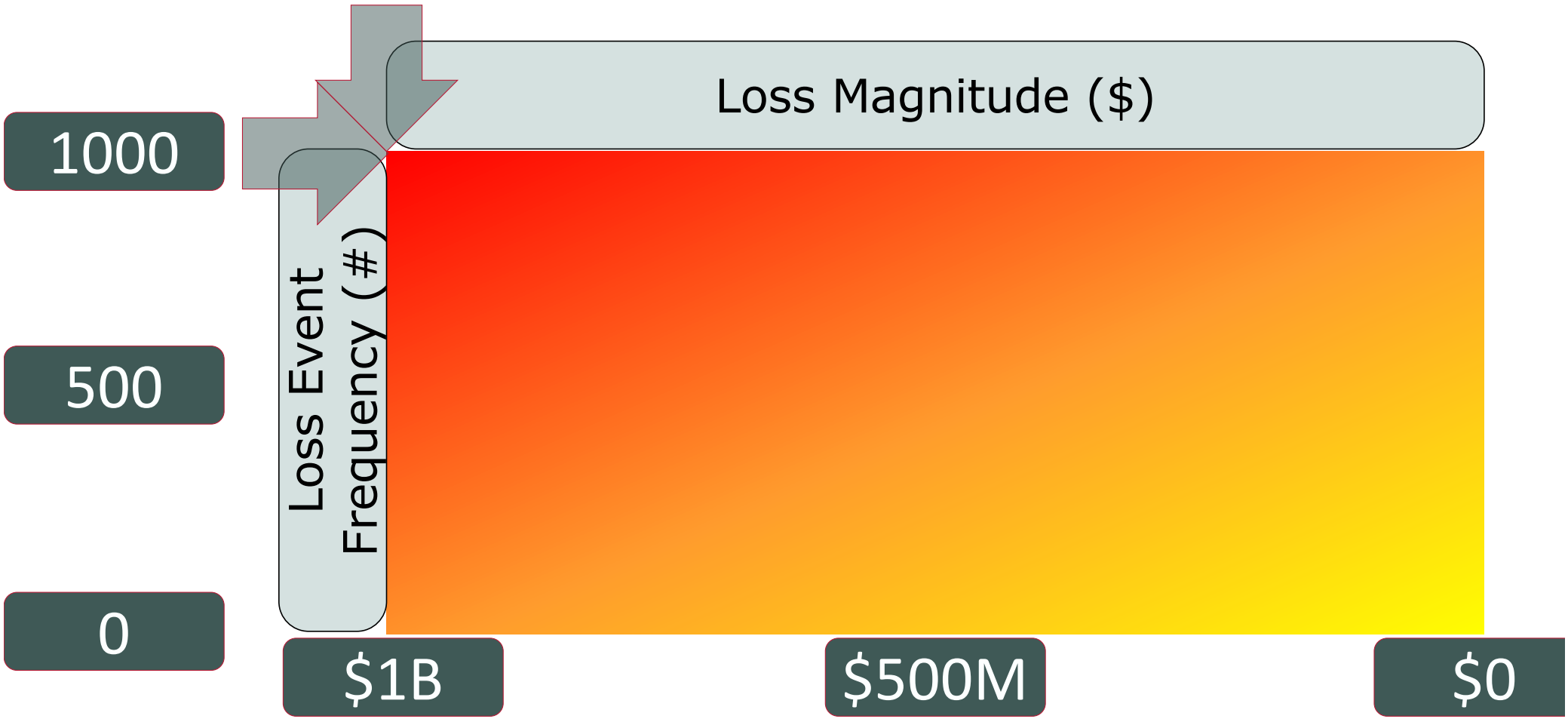
Actuarial



FAIR

Fermi

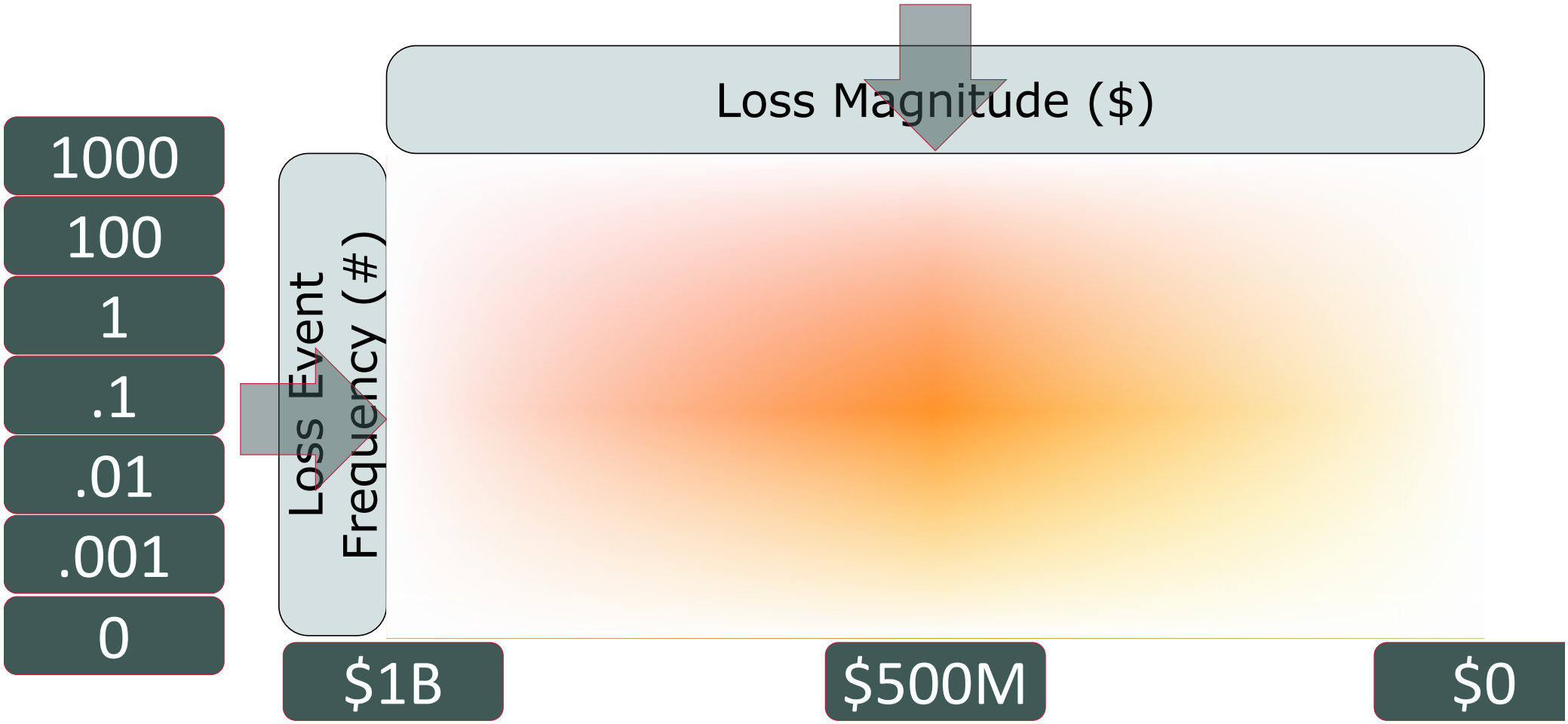
Actuarial



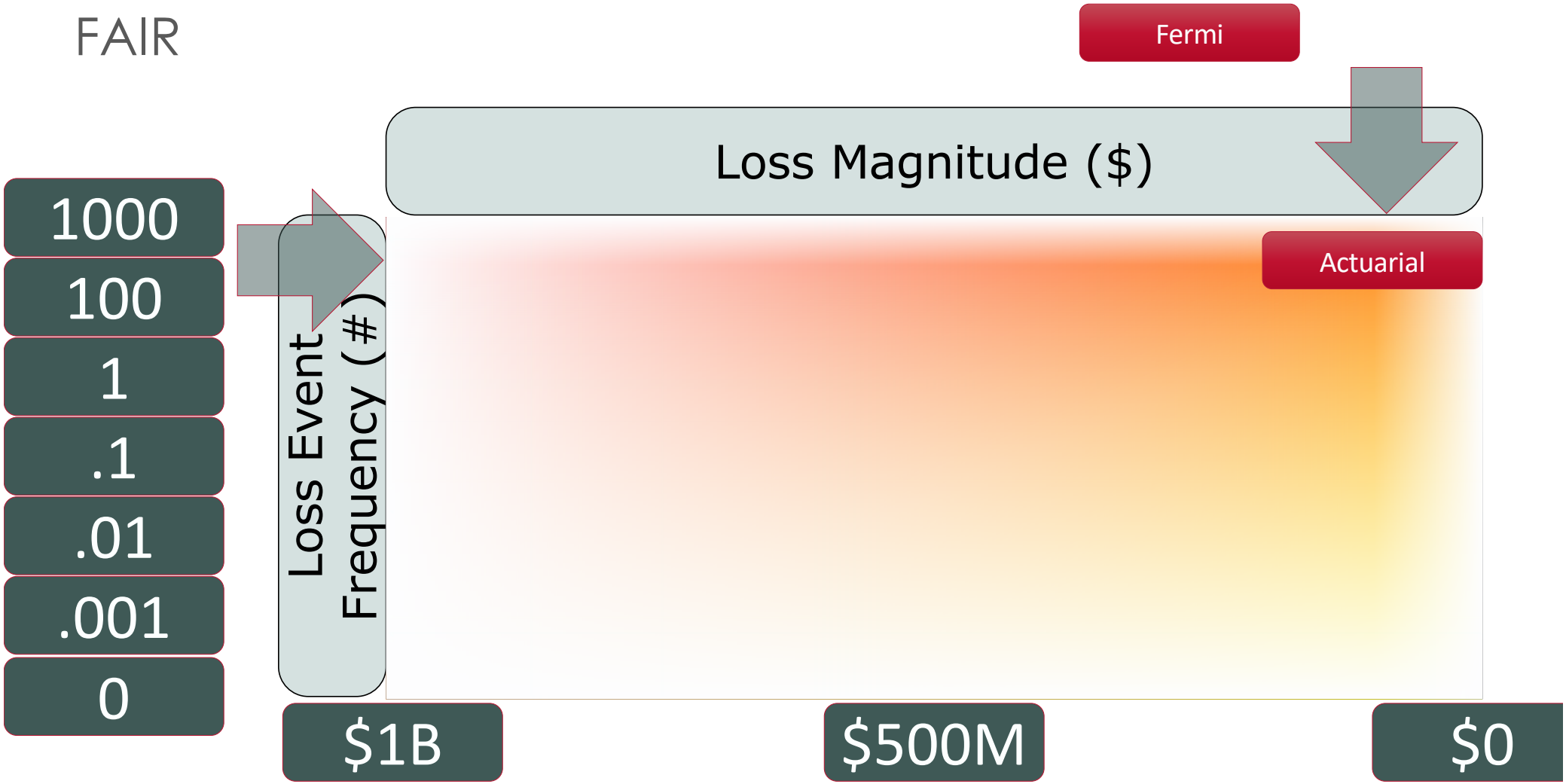
FAIR

Fermi

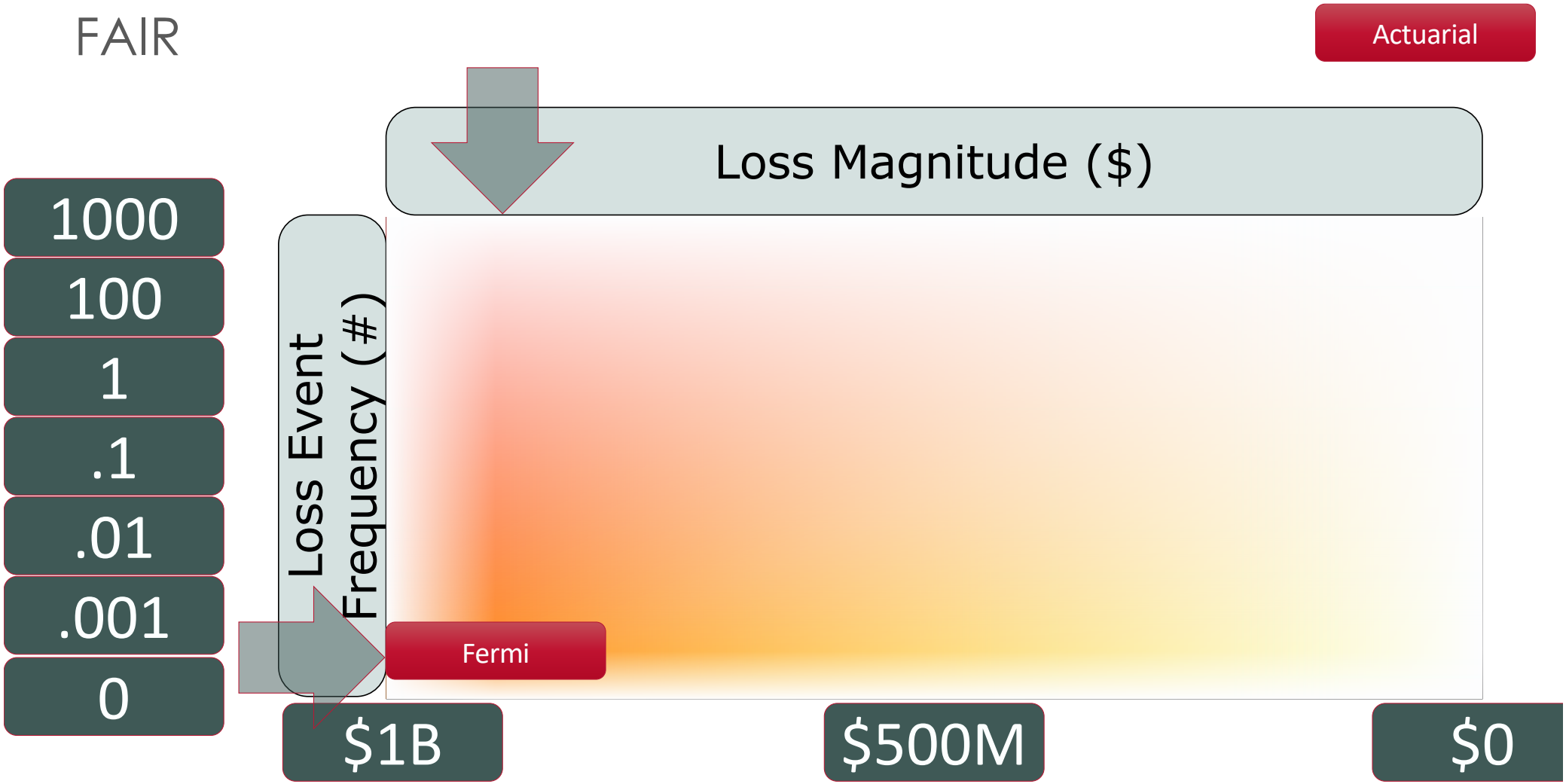
Actuarial



FAIR


Fermi
Loss Magnitude ($)
Actuarial
1000
100
1
.1
.01
.001
0
Loss Event Frequency (#)
$1B
$500M
$0

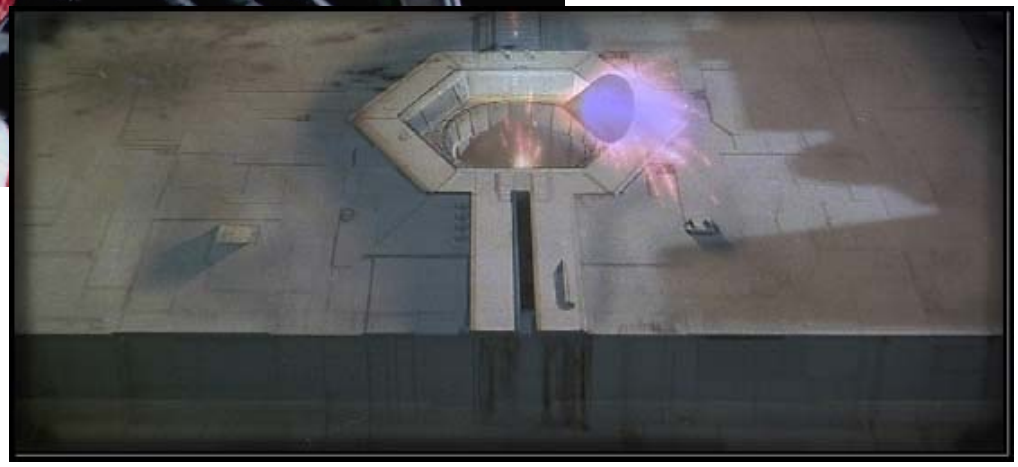
FAIR


Actuarial
Loss Magnitude ($)
1000
100
1
.1
.01
.001
0
Loss Event Frequency (#)
Fermi
$1B
$500M
$0

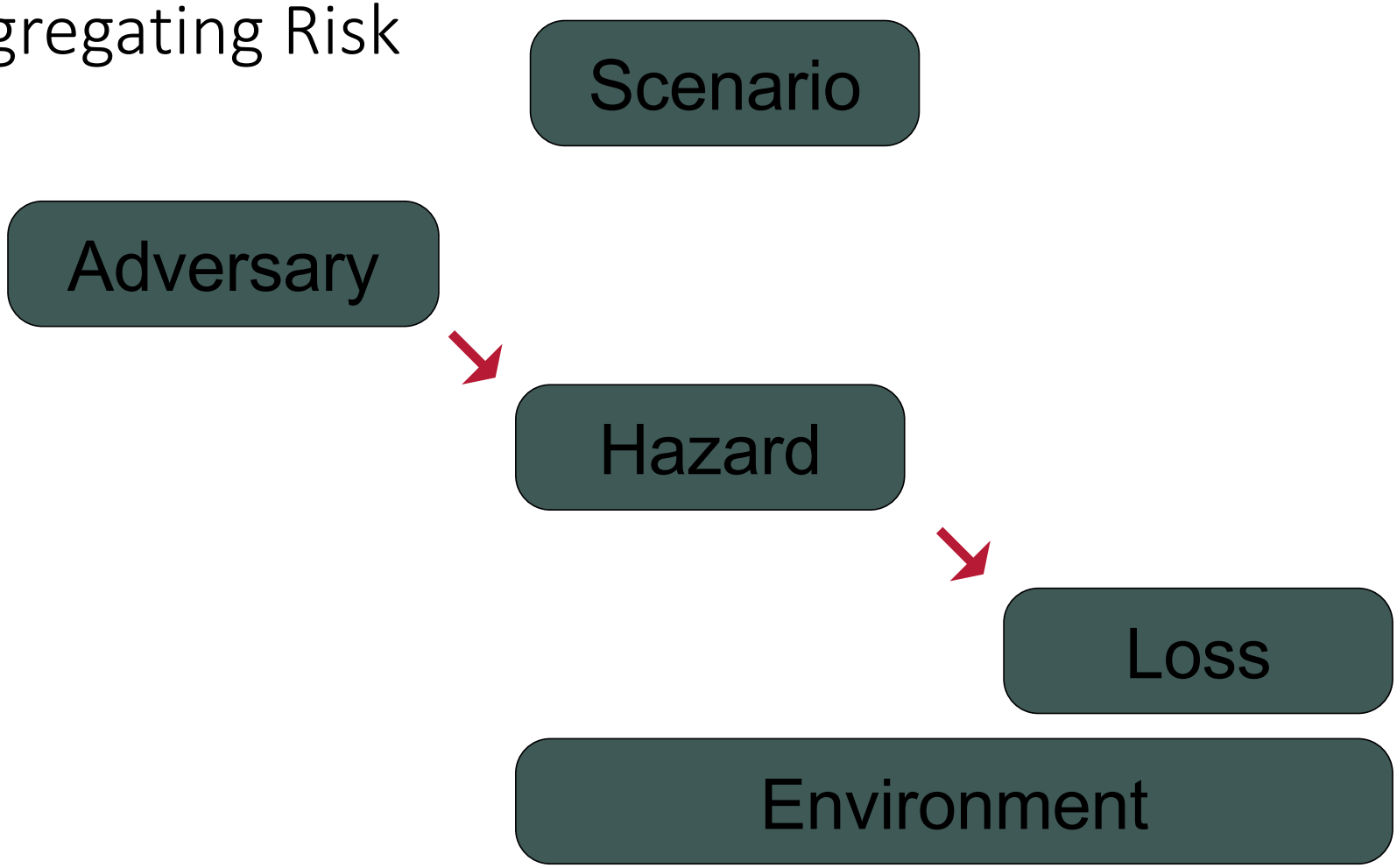
Unique Events are Hard

Fermi

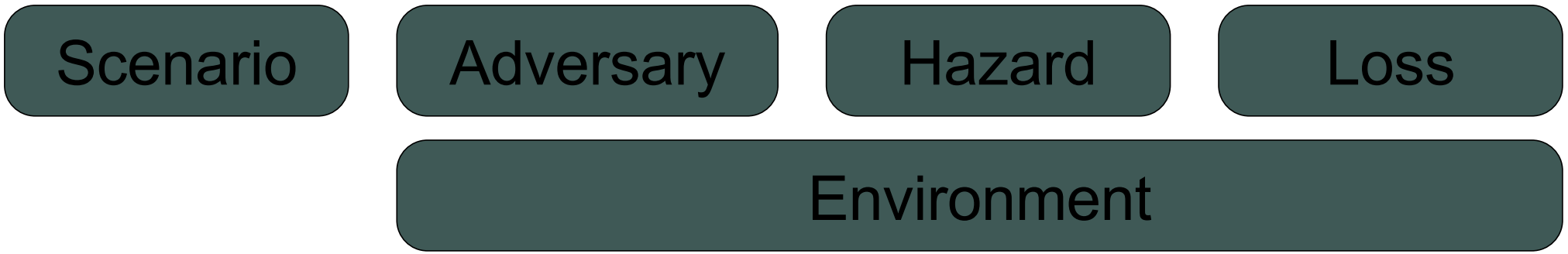




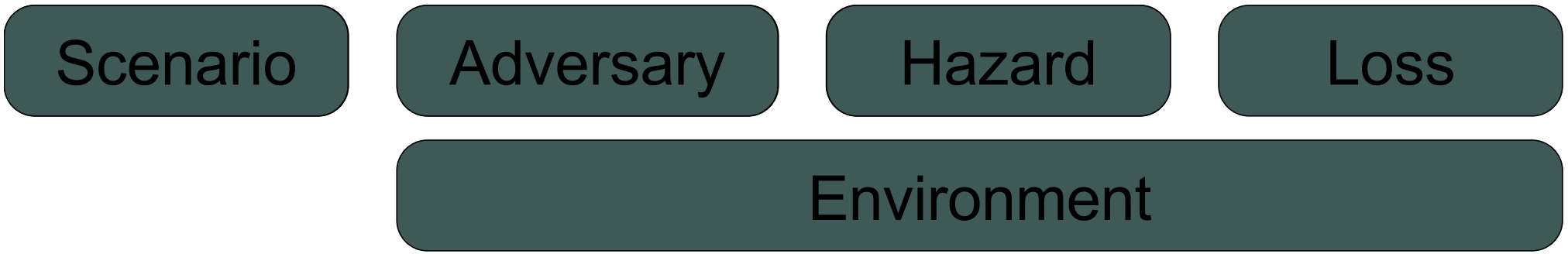
Aggregating Risk



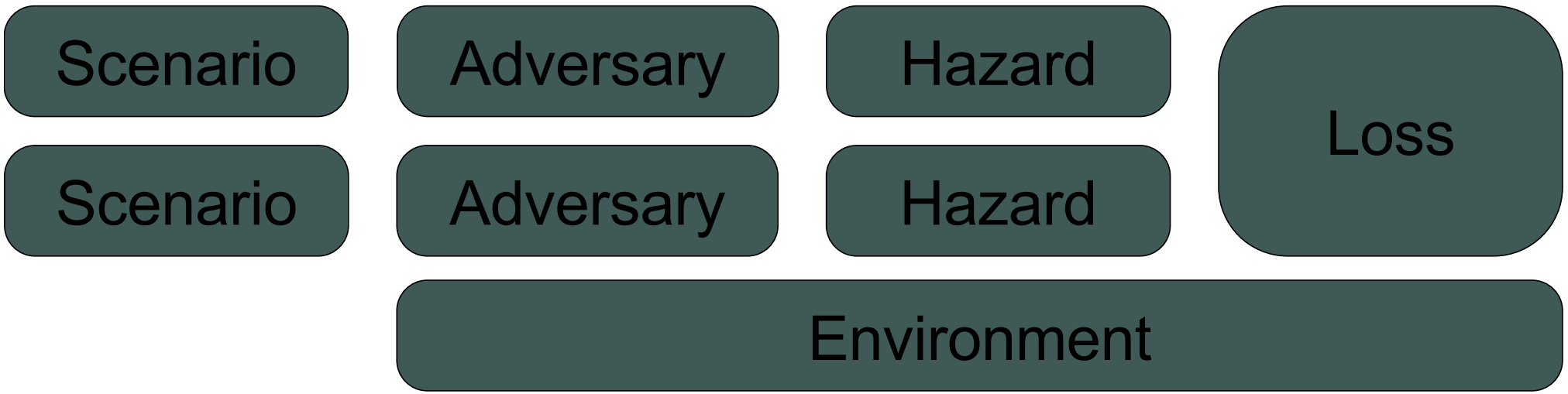
Aggregating Risk



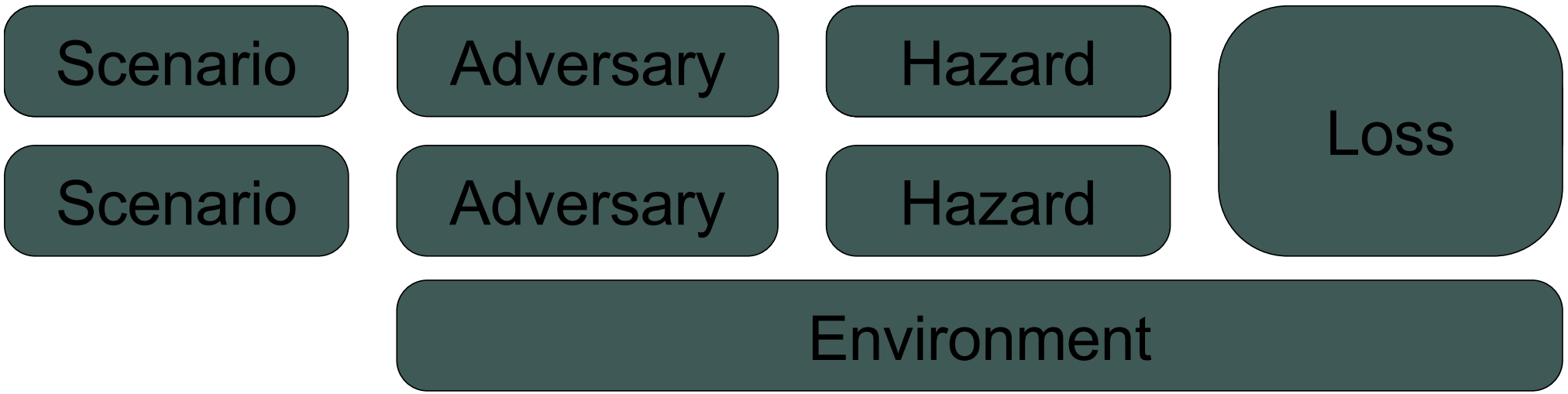
Aggregating Risk



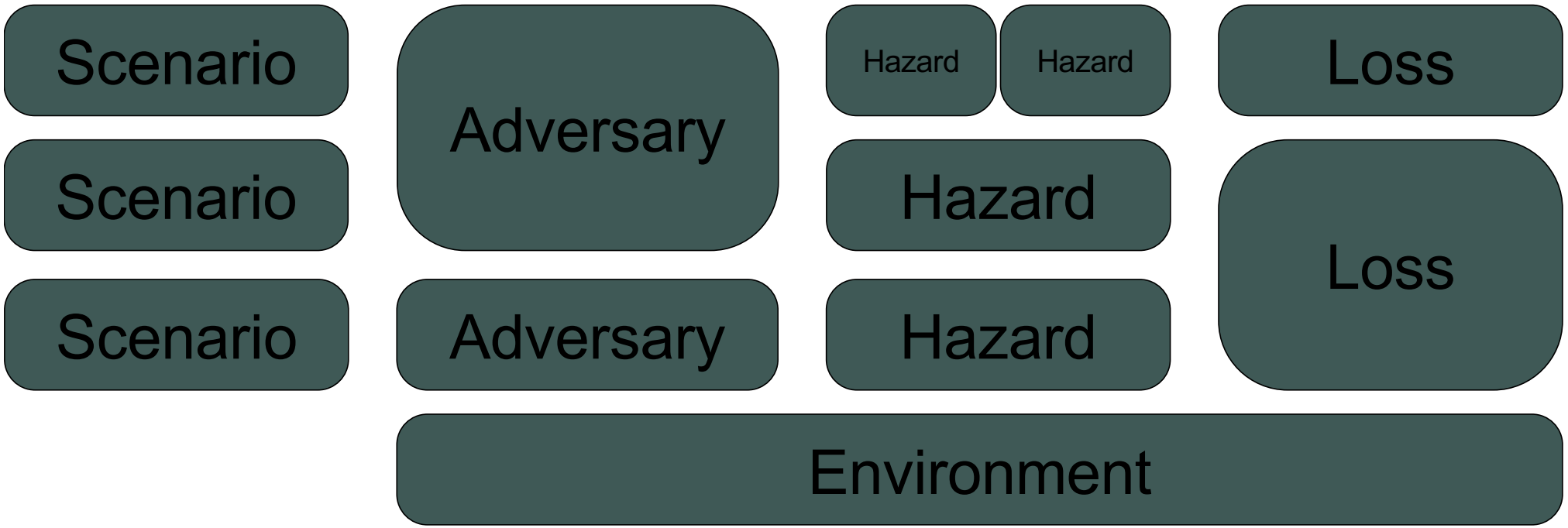
Aggregating Risk



Aggregating Risk

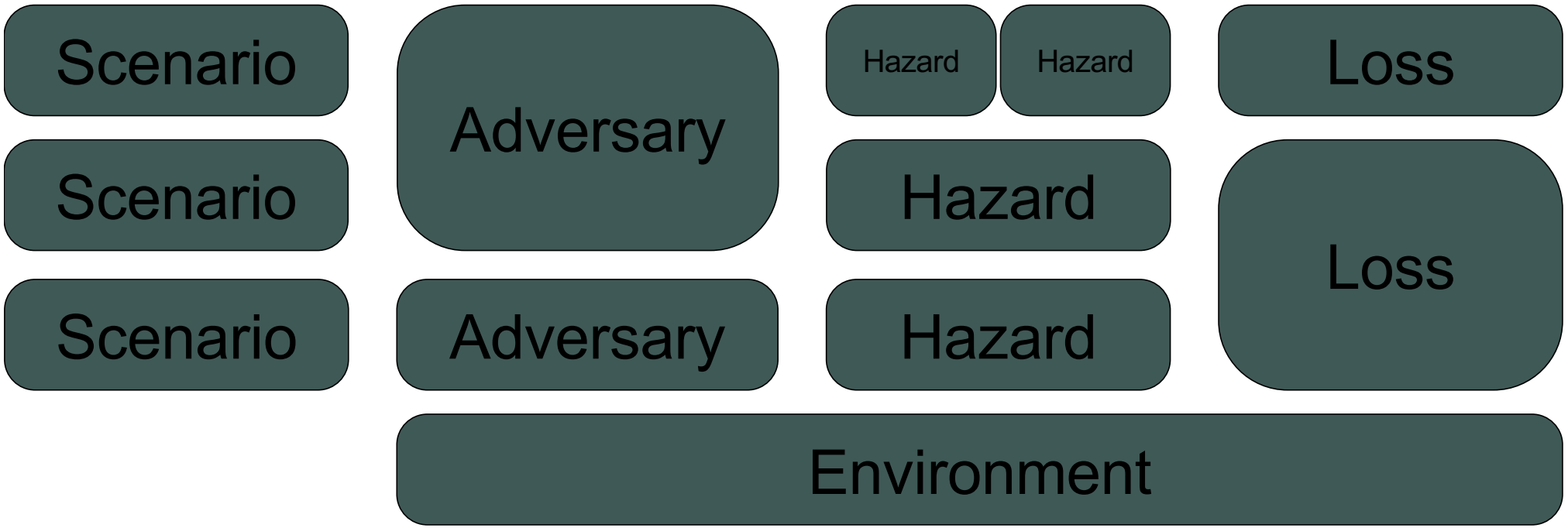


Aggregating Risk



Aggregating Risk

Apply: How does thinking about more risk vectors change perceived risk?



Aggregating Risk

Apply: How does thinking about more risk vectors change perceived risk?

Imagine Company C. Consider it has a risk score of Y.

Imagine Company X. Consider it has a risk score of Y.

Company C and Company X merge. What is the risk score of the new company?

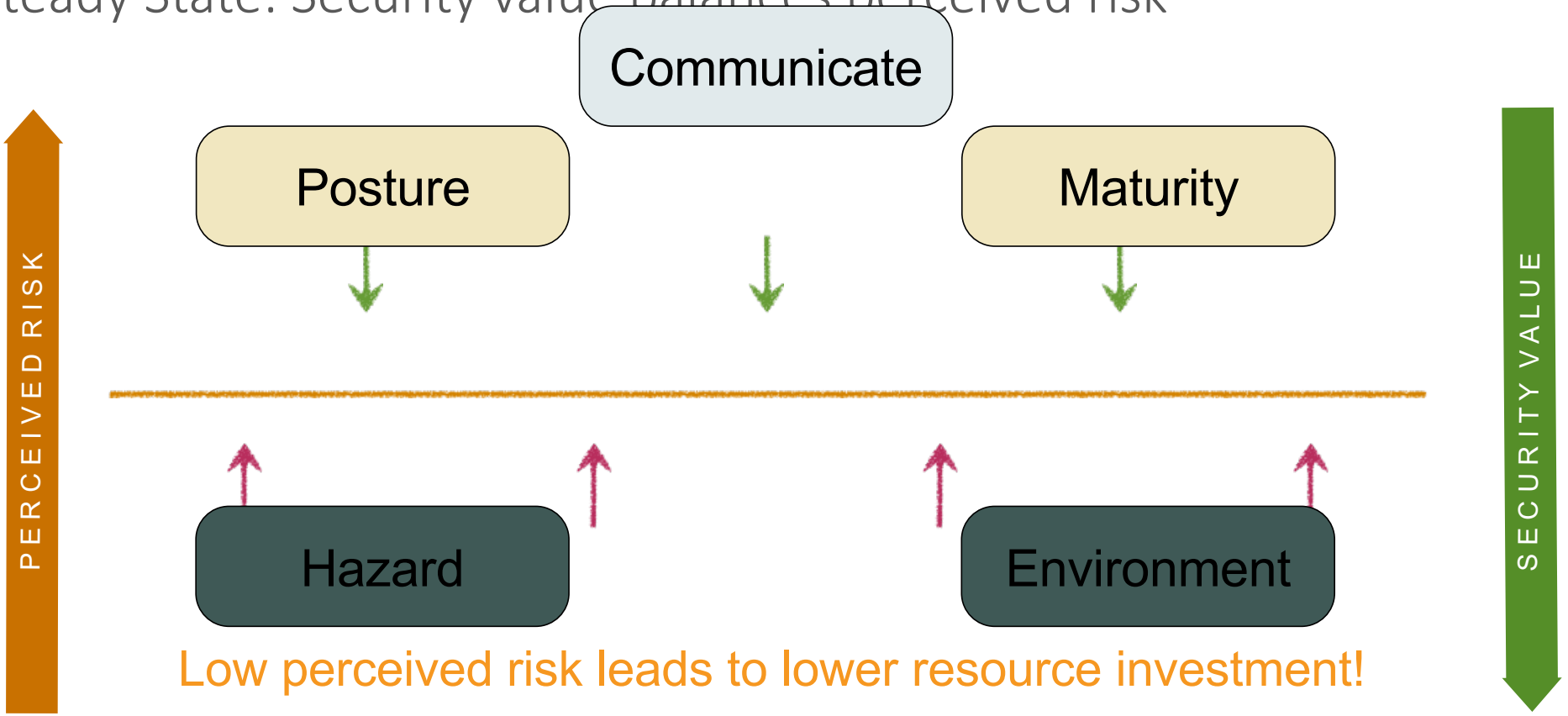
Risk Communication Goals

Compare

Communicate

Change

Steady State: Security value balances perceived risk



Low perceived risk leads to lower resource investment!

Low perceived capability leads to lower perceived risk!

Posture vs Maturity

Communicate

Posture

Posture is your ceiling

Do I have defenses in place right now?

Maturity

Maturity is your floor

Will I maintain my defenses in the future?

Posture vs Maturity vs Compliance

Communicate

Posture

Posture is your ceiling

Do I have defenses in place right now?

Compliance

Compliance is your footprint

How often do we visit this defense?

Maturity

Maturity is your floor

Will I maintain my defenses in the future?

Risk *Communication*

Compare

Communicate

Change

Dashboards

Communicate



Maturity

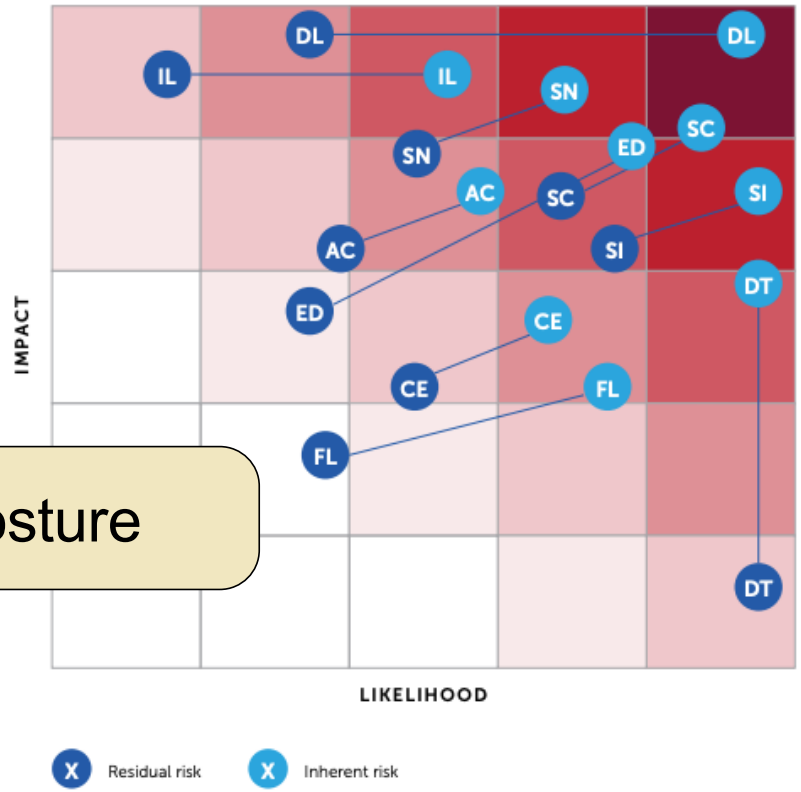
Posture

Environment

RSAC-ESAF

Communicate

Change



DL	**Data Loss**	Loss of customer data through social engineering attacks whereby employees divulge information
SC	**Software Compromised**	Software development compromised, and malicious code distributed to customers
SI	**Systems Inoperable**	Systems inoperable via hijacking of network
ED	**E-Commerce Disruptions**	E-commerce disruptions due to web application tampering
SN	**Services Non-Accessible**	Services non-accessible due to denial-of-service (DDoS) attacks
IL	**Information Leakage**	Sensitive or competitive information leakage via insider information trafficking
AC	**Accounts Compromised**	Customer accounts taken over via brute force attacks which automate customer logins using collections of stolen credentials
CE	**Cyber Extortion**	Cyber extortion via ransomware whereby data is encrypted and held hostage
DT	**Data Theft**	Customer data theft via exploitation of known software vulnerabilities ("back doors")
FL	**Financial Loss**	Financial loss due to fraudulent use of financial applications

Loss

Scenario

Posture

OWASP

Communicate

Compliance

	Metric Type	Metric Definition	Q1 2022	Q2 2022	Q3 2022	Q4 2022	Trend	Goal
Technology	Vulnerability Management	**Mean Time To Remediate Endpoints** - Avg # of days it takes to close an endpoint vulnerability	90	60	70	30		30
		Mean Time To Remediate Servers - Avg # of days it takes to close a server vulnerability	90	15	35	20		15
		Endpoint Patching Compliance- The % of endpoints with vulnerabilities < 60 days	95%	97%	93%	99%		100%
		Server Patching Compliance- The % of servers with vulnerabilities < 30 days	85%	83%	83%	82%		100%
	Secure Configuration	**Antivirus Compliance**- The % of Endpoints that run Antivirus with signatures < 30 days old	97%	97%	97%	96%		100%
		CIS Benchmark Compliance- The % of Servers that comply with CIS Benchmarks	80%	80%	82%	85%		100%
People	Cyber Vigilance	**Phishing Reporting Rate**- % of Users who reported phishing exercises	7.5%	5.0%	11.0%	3.0%	N/A	5% > Benchmark
		Phishing Reporting Exercise Benchmark- % of Users who reported phishing exercise across industry	10%	7%	11%	5%	N/A	N/A
		Phishing Click Rate- % of Users who clicked phishing exercises	15%	18%	33%	20%	N/A	2% < Benchmark
		Phishing Click Rate Exercise Benchmark- % of Users who clicked phishing exercise across industry	10%	15%	20%	25%	N/A	N/A
Process	3rd Party Compliance	**3rd Party Reviews**- % of 3rd Party Risk Vendors with a current CAIQ/SIG (< 24 months old)	100%	100%	100%	98%		100%
		3rd Party Certification- % of 3rd Parties with a current ISO 27001/SOC 2 Type 2 Certification	40%	35%	40%	41%		100%
		3rd Party Penetration Tests- % of 3rd Parties with a current Pentest (< 1 year old)	50%	45%	60%	70%		100%
	Disaster Recovery	**Annual Restore Testing**- % of Critical Applications that restored from a Read Only Backup in < 24 hours	60%	80%	80%	100%		100%
		Annual Failover Testing- % of Critical Apps that successfully failed over to alternate data center	80%	75%	70%	60%		100%
Environment	Active Threats	**Stopped Phishing Attacks**- # of Actual Phishing Attacks Reported by Employees	100	200	150	175		N/A
		Stopped Malware Attacks- # of Cyber Attacks stopped by Antivirus	350	500	150	356		N/A
		Cyber Incidents- # of Cyber Incidents Responded to by Incident Response Team / Help Desk	15	39	25	47		N/A

Hazard

Change

NIST-CSF

Environment

Compare

Maturity

NIST Cybersecurity Framework

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Score	Maturity Level	Description
7	**Optimized**	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified**	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process**	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4	**Partially Documented Standards and/or Procedures**	Your organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy**	Your organization has a formal policy in place that has been approved by senior management.
2	**Informally Done**	Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by senior management.
1	**Not Performed**	Activities, processes, and technologies are not in place to achieve the referenced objective.