Surviving the Sands of Cyber Entropy, Conflict, Risk and Resiliency

1 August 2023

Phenomenati Consulting

Scott Foote, Managing Director

Steve Foote, Managing Director

Welcome

Building on Last Year's Talk…

"Top 10 Challenges (Ty's and Cy's) of Cyber Resiliency"

System-related Challenges

1. Cyber Entropy™
2. Complexity
3. Dependency
4. Vulnerability
5. Fragility

Acquisition-related Challenges

6. Urgency
7. Simplicity
8. Commodity
9. Efficiency
10. Fantasy

1:00

Cyber Entropy, Conflict, Risk and Resilience

Survival Strategies

1. Develop “Meta” Systems
2. Cultivate Domain Awareness
3. Promote Risk Awareness
4. Invest in Contingencies & Controls
5. Establish Risk Level Agreements™
6. Integrate Business Operations ←→ Security Operations
7. Insist on Governance

Bring Order to Entropy

Acknowledge Conflict

Embrace Risk

Plan for Resilience

2:00

1. Develop "Meta" Systems

What is a "*Meta*" System?

- Comprehensive Knowledge ABOUT the System(s)
  - Technology → Business Processes → Business Objectives
- Knowledge Management (KM) Systems
- Examples
  - Digital "Blueprints"
  - "Digital Twins"
  - Operational Control Systems (e.g., SCADA, ICS)
- Organizational Commitment to Systems Engineering Discipline
  - ***Designs***, Baselines, Asset Management, Change Management, Risk Management

Example Knowledge

- Functional Requirements
- Non-Functional Requirements
  - Measures of Performance, Effectiveness, Suitability
  - These ARE the **Resiliency Requirements**
- Design Documentation
- Original Engineering Tradeoffs
- Dependencies, Criticality, Contingences

Awareness is Based on *Knowledge*

3:00

2. Cultivate Domain Awareness

Mission or Business Awareness

- Business Objectives
- Dependency Discovery
- Eliminate Assumptions
- Single Points of Failure
- Dependency Lifecycle Management
- Business Impact Analysis (BIA)

Network Awareness

- Asset Discovery
  - Information Assets
  - Service Assets
  - Software Assets
  - “Hardware” Assets
  - Networks
- Asset Classification
- Asset Lifecycle Management
- Access Controls (I, A, A, A)
- Attack Surface Management

Threat Awareness

External Threat Intelligence	(e.g., Threat Actors)
Emerging Obligations	(e.g., Privacy Laws)
Disruptive Market Forces	(e.g., Generative AI)
Internal Threat Intelligence	(e.g., Undisciplined Change)
Insider Threats	(e.g., Staff, Executives)
Supply Chain Threats	(e.g., Contractors, Vendors)

Awareness Informs *Decisions*

3:00

3. Promote Risk Awareness

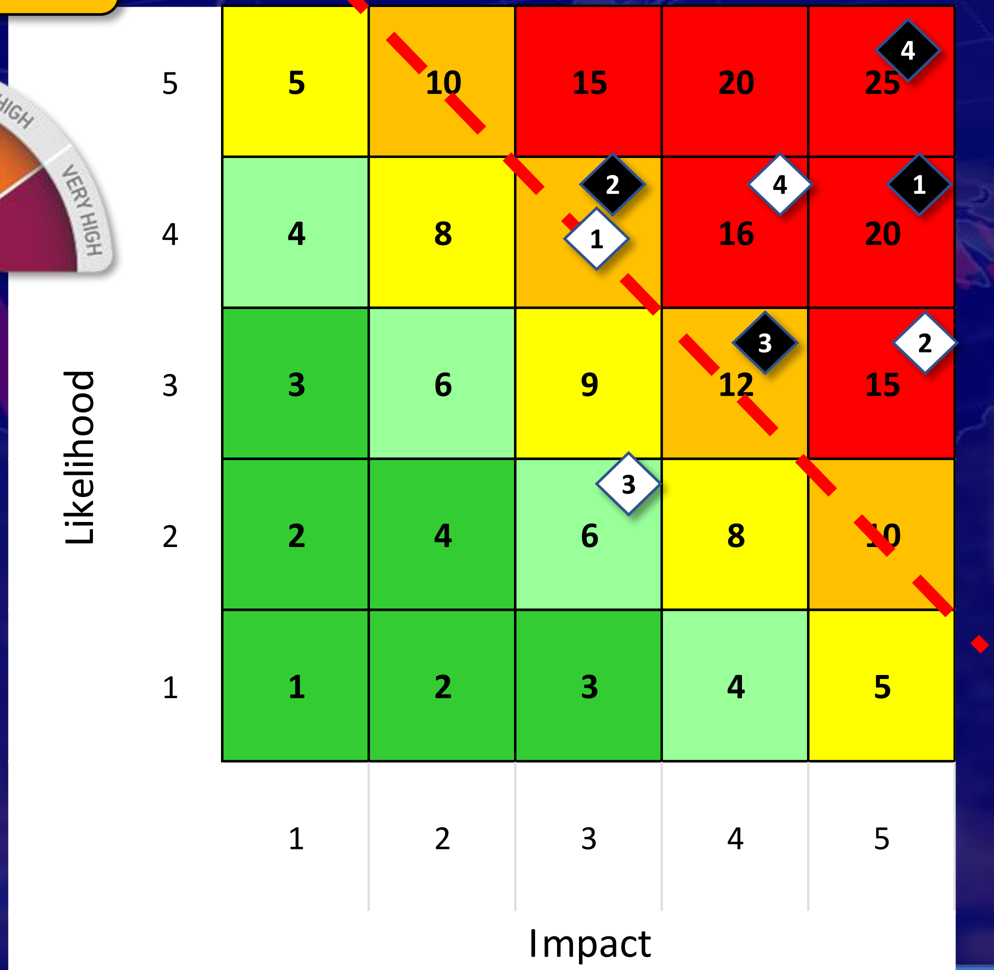
Risk Awareness

- Scenario Analysis
- Risk Identification
- Risk Assessment (Qualitative & Quantitative)
- Risk Evaluation (above/below tolerance)

From Abstract to Concrete

	Risk ID	Description	Likelihood	Impact
1	IR001	Loss of **Confidentiality** of Content provided TO Gen AI service(s)	4 → 1	3
2	IR002	Poor **Integrity** of Content received FROM Gen AI service(s)	3 → 2	5 → 2
3	IR003	Content received FROM Gen AI service(s) may violate **Copyrights**	2	3
1	ER001	Gen AI service(s) selected as an **alternative** to COMPANY Service(s)	4 → 3	5 → 4
4	IR004	New COMPANY Offering/Service becomes critically dependent on **Availability** of Gen AI service	4 → 2	4 → 3
2	ER002	Threat actors use Gen AI to exploit open source intel for **Reconnaissance** on your staff, business, customers	4 → 3	3
3	ER003	**Social Engineering attacks** (phishing, smishing, vishing, live, etc.) are becoming much more effective	3 → 2	4 → 2
4	ER004	**Malware** is being rapidly **refactored** and **enhanced** (e.g., polymorphic improvements)	5 → 4	5

Cyber Risk Landscape



Likelihood					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Impact				

Actionable Scenarios

3:00

4. Invest in Contingencies & Controls

Phenomenati

People

Process

Technology

Contingency Readiness

- Redundant System Components
- “Hot”, “Warm”, “Cold” Backups
- Alternative Ops Centers
- ***Exercise*** Your Contingencies

Contingency Identification & Selection

- Eliminate Vulnerabilities in Critical Dependencies
- Resiliency in Conflict is ***not*** simply a ***Technical*** Problem
- Address Vulnerabilities in People, Processes, Technologies

Contingency Planning

- Hope is ***not*** a Strategy
- Proactive Investment → Effective Response
- Cross Functional Planning Team(s)
- Identify and Evaluate Options, Alternatives, Redundancies
- Use Cost-Benefit Analyses to Inform Investment Decisions
- Establish the Crisis Decision Making Process & Authorities

Resiliency
Is Built on
Preparedness

2:00

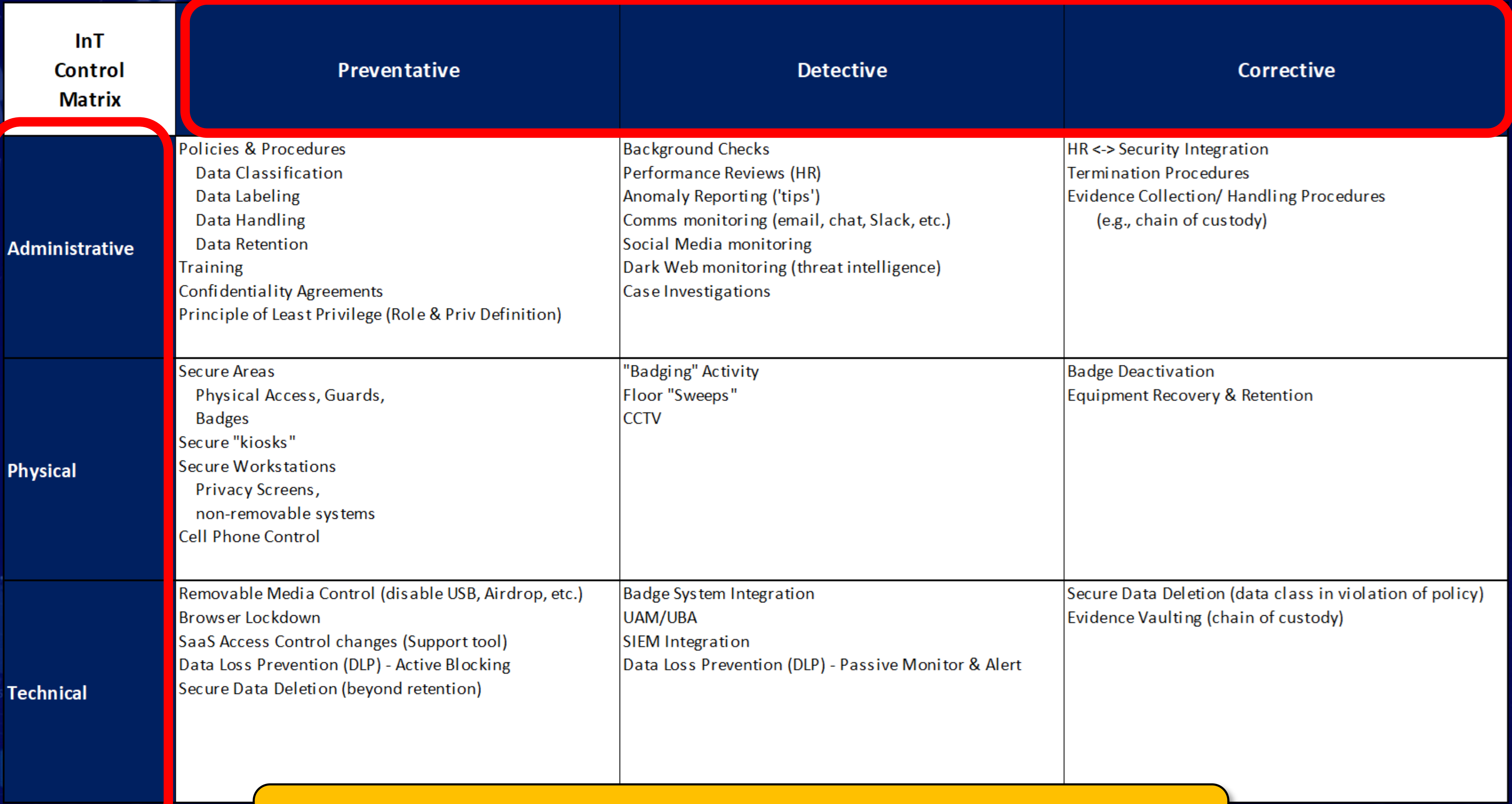
4. Invest in Contingencies & Controls

Control Types:

- Administrative
- Physical
- Technical

Control Objective:

- Preventative
- Detective
- Corrective



InT Control Matrix	Preventative	Detective	Corrective
Administrative	Policies & Procedures Data Classification Data Labeling Data Handling Data Retention Training Confidentiality Agreements Principle of Least Privilege (Role & Priv Definition)	Background Checks Performance Reviews (HR) Anomaly Reporting ('tips') Comms monitoring (email, chat, Slack, etc.) Social Media monitoring Dark Web monitoring (threat intelligence) Case Investigations	HR <-> Security Integration Termination Procedures Evidence Collection/ Handling Procedures (e.g., chain of custody)
Physical	Secure Areas Physical Access, Guards, Badges Secure "kiosks" Secure Workstations Privacy Screens, non-removable systems Cell Phone Control	"Badging" Activity Floor "Sweeps" CCTV	Badge Deactivation Equipment Recovery & Retention
Technical	Removable Media Control (disable USB, Airdrop, etc.) Browser Lockdown SaaS Access Control changes (Support tool) Data Loss Prevention (DLP) - Active Blocking Secure Data Deletion (beyond retention)	Badge System Integration UAM/UBA SIEM Integration Data Loss Prevention (DLP) - Passive Monitor & Alert	Secure Data Deletion (data class in violation of policy) Evidence Vaulting (chain of custody)

Resiliency derives from **Control *Effectiveness***

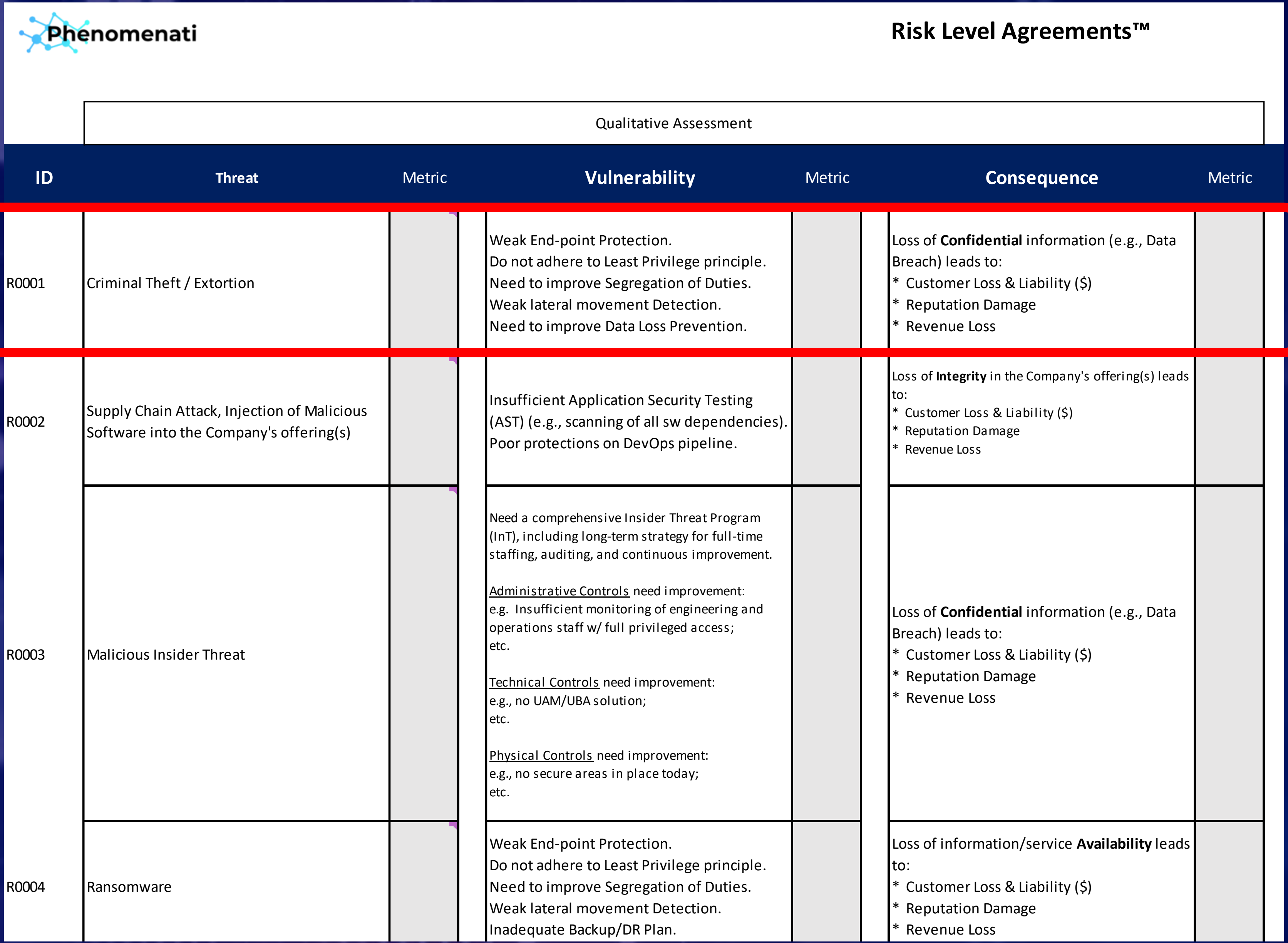
2:00

5. Establish Risk Level Agreements™

Phenomenati

Identify Scenarios through:

- Business Analysis
- Audit Findings
- Change Management



Phenomenati

Risk Level Agreements™

	Qualitative Assessment					
ID	**Threat**	Metric	**Vulnerability**	Metric	**Consequence**	Metric
R0001	Criminal Theft / Extortion		Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.		Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)		Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.		Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	
R0003	Malicious Insider Threat		Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.		Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	
R0004	Ransomware		Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.		Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	

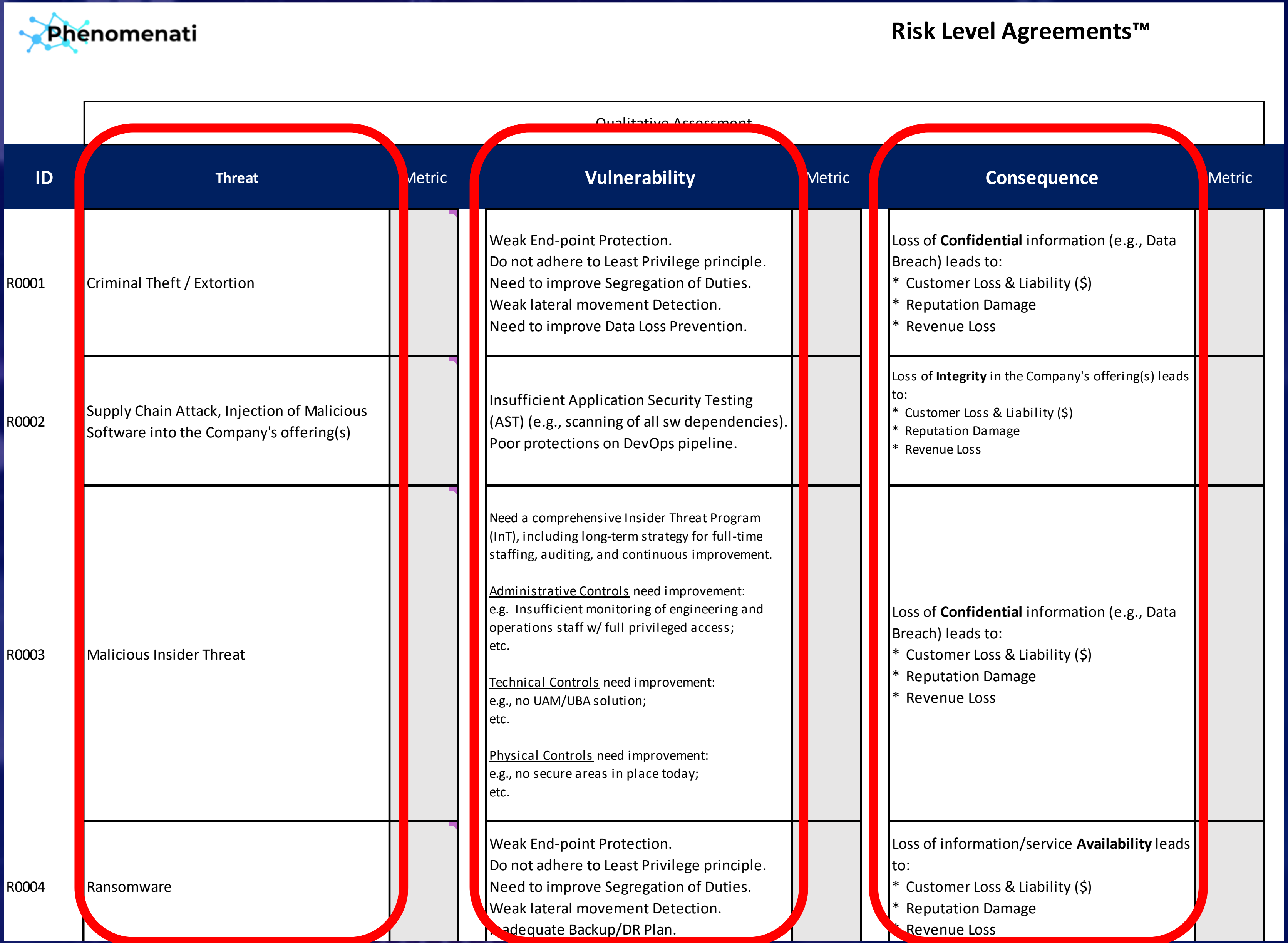
0:30

5. Establish Risk Level Agreements™

Phenomenati

Decompose Risk into:

- Threats
- Vulnerabilities
- Consequences



Phenomenati

Risk Level Agreements™

Qualitative Assessment

ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric
R0001	Criminal Theft / Extortion		Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.		Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)		Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.		Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	
R0003	Malicious Insider Threat		Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.		Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	
R0004	Ransomware		Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.		Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	

0:30

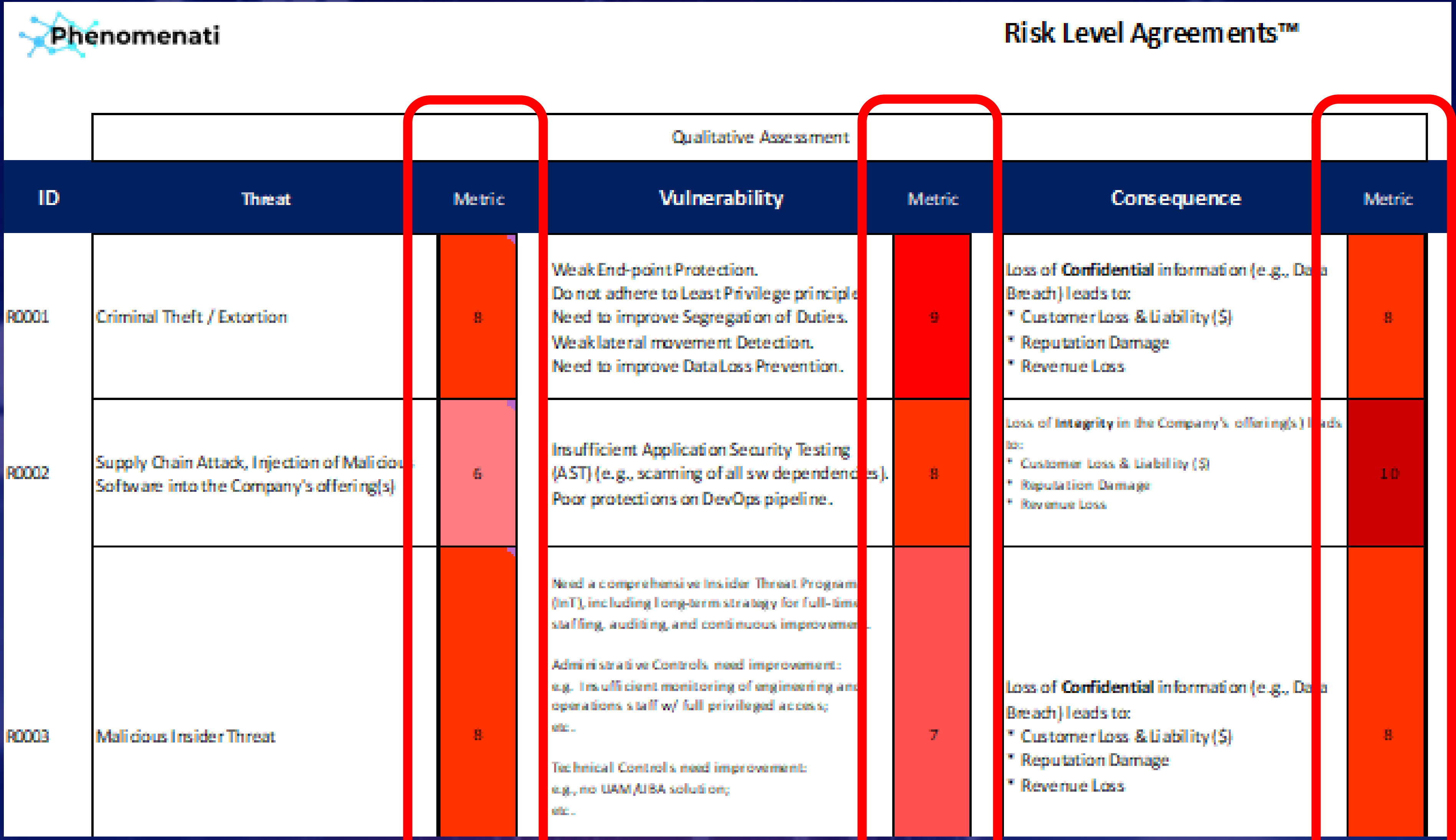
5. Establish Risk Level Agreements™

Qualify Each Risk:

- Threat
- Vulnerability
- Consequence

Employ a Numeric Scale, for example:

1. Negligible
2. Minor
3. Moderate
4. Major
5. Significant



Phenomenati

Risk Level Agreements™

		Qualitative Assessment				
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	10
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc.	7	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8

www.risklevelagreements.com

0:30

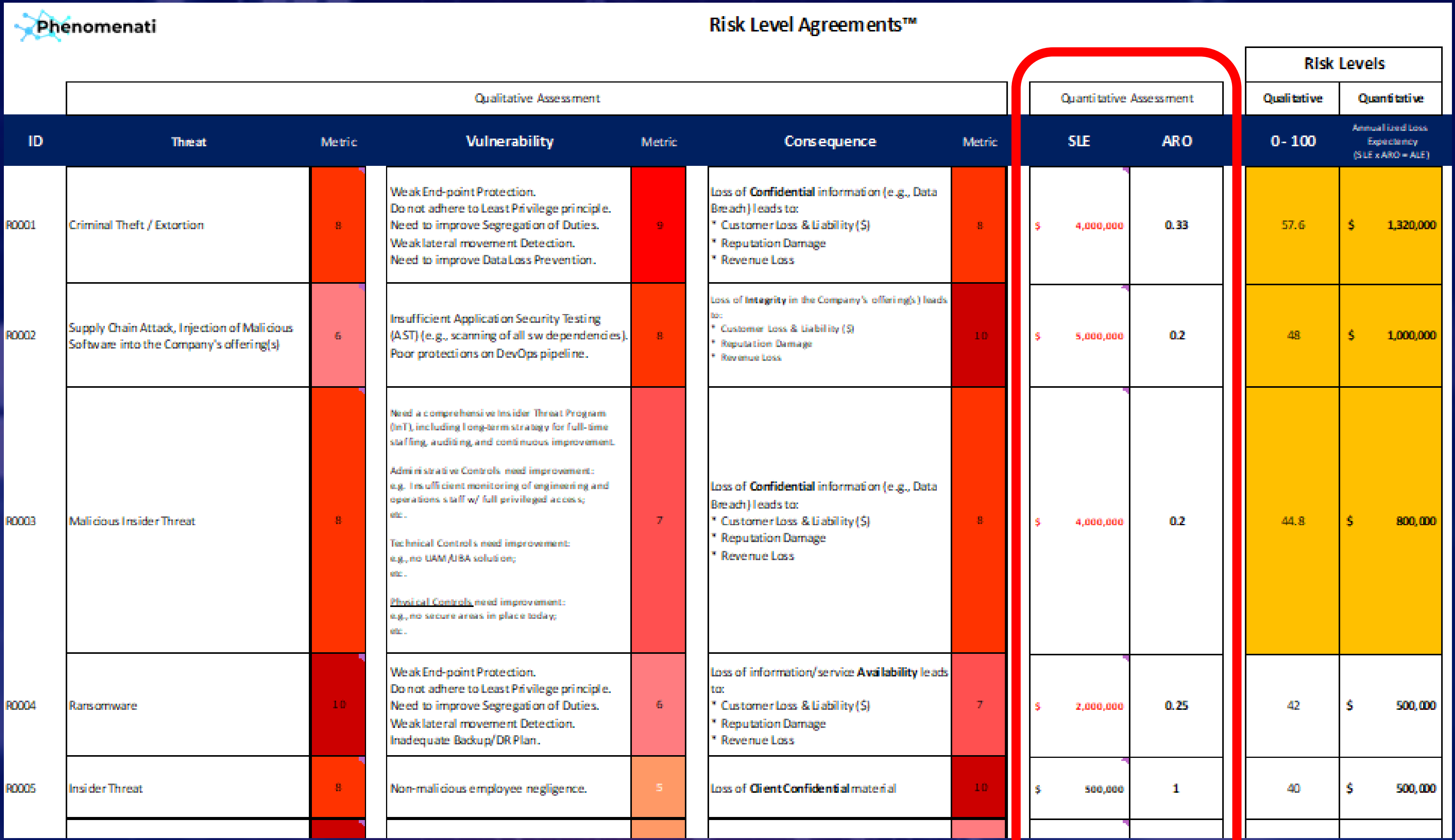
5. Establish Risk Level Agreements™

Quantify **Each Risk:**

- Consequence

Develop Estimates:

- Single Loss Expectancy (SLE)
- Annualized Rate of Occurrence (ARO)
- Annualized Loss Expectancy (ALE)



Phenomenati

Risk Level Agreements™

									Risk Levels	
	Qualitative Assessment						Quantitative Assessment		Qualitative	Quantitative
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric	SLE	ARO	0 - 100	Annualized Loss Expectancy (SLE x ARO = ALE)
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.33	57.6	$ 1,320,000
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	10	$ 5,000,000	0.2	48	$ 1,000,000
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.	7	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.2	44.8	$ 800,000
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	7	$ 2,000,000	0.25	42	$ 500,000
R0005	Insider Threat	8	Non-malicious employee negligence.	5	Loss of **Client Confidential** material	10	$ 500,000	1	40	$ 500,000

www.risklevelagreements.com

0:30

5. Establish Risk Level Agreements™

Phenomenati

Prioritize Risks:

- Sort by **Qualitative** Risk **First**

Open Discussion:

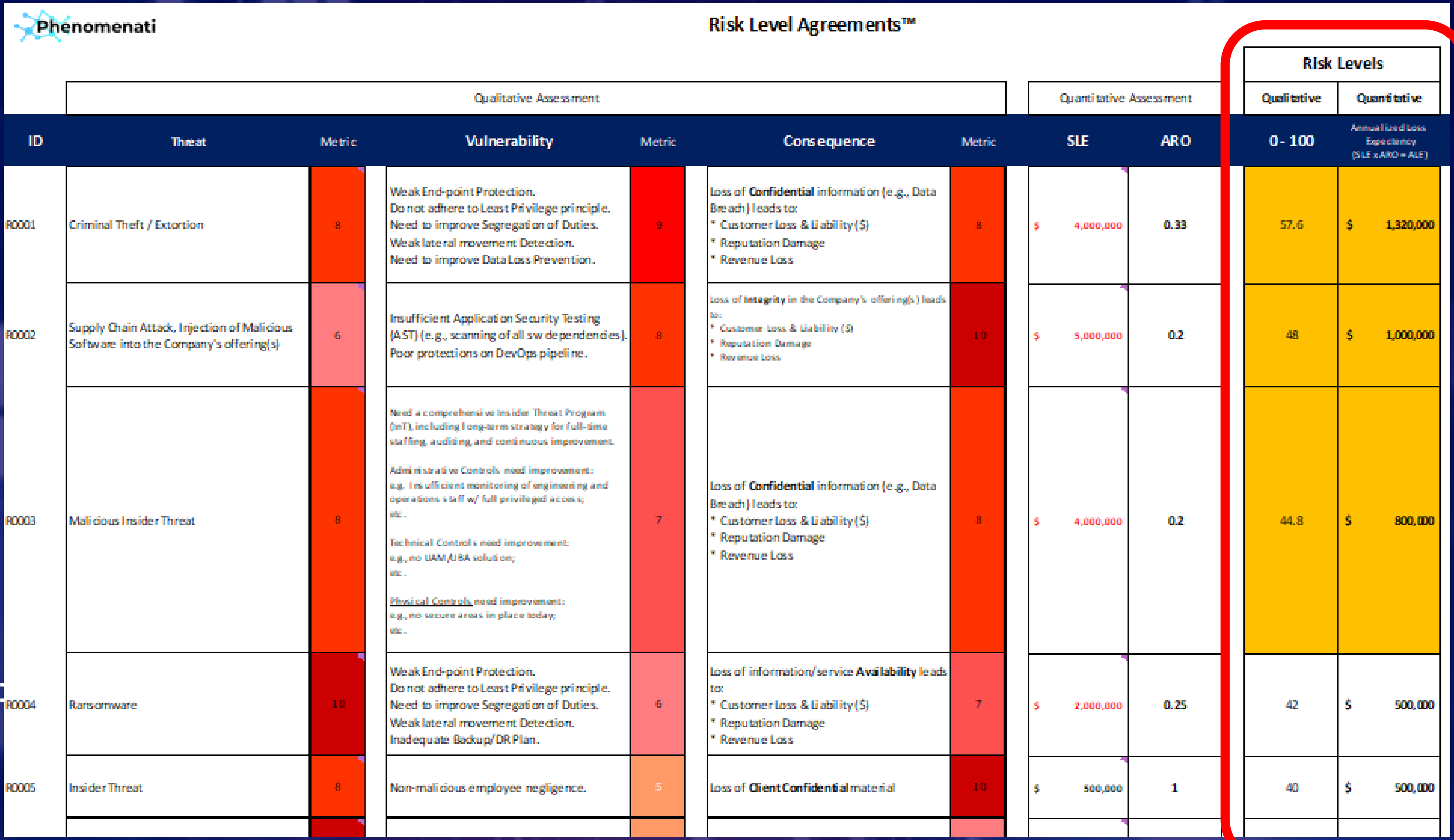
- Revisit the 1 to N rankings, comparatively

Move On To:

- Sort by **Quantitative** Risk

Assess Risk Tolerance:

- **For EACH Scenario**



Phenomenati

Risk Level Agreements™

									Risk Levels	
	Qualitative Assessment						Quantitative Assessment		Qualitative	Quantitative
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric	SLE	ARO	0 - 100	Annualized Loss Expectancy (SLE x ARO = ALE)
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.33	57.6	$ 1,320,000
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	10	$ 5,000,000	0.2	48	$ 1,000,000
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.	7	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.2	44.8	$ 800,000
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	7	$ 2,000,000	0.25	42	$ 500,000
R0005	Insider Threat	8	Non-malicious employee negligence.	5	Loss of **Client Confidential** material	10	$ 500,000	1	40	$ 500,000

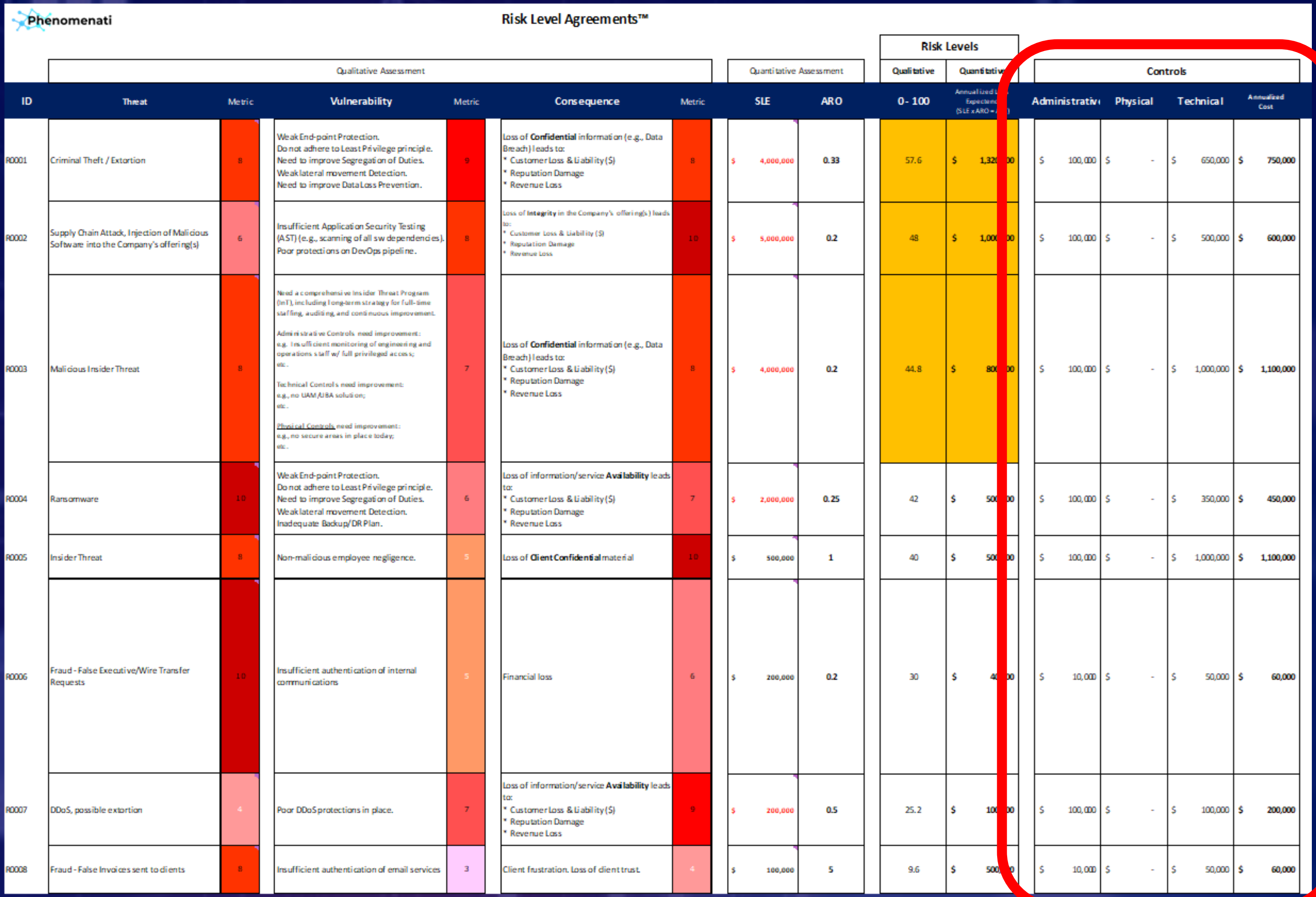
0:30

www.risklevelagreements.com

5. Establish Risk Level Agreements™

Estimate Control Costs:

- Consider Total Cost of Ownership (TCO)
- Annualize the TCO for each Control/Set



Phenomenati

Risk Level Agreements™

	Qualitative Assessment						Quantitative Assessment		Risk Levels		Controls			
									Qualitative	Quantitativ				
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric	SLE	ARO	0 - 100	Annualized L[illegible] Expectanc[illegible] (SLE x ARO = A[illegible])	Administrativ	Physical	Technical	Annualized Cost
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.33	57.6	$ 1,32[illegible]00	$ 100,000	$ -	$ 650,000	$ 750,000
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	10	$ 5,000,000	0.2	48	$ 1,00[illegible]00	$ 100,000	$ -	$ 500,000	$ 600,000
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.	7	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.2	44.8	$ 80[illegible]00	$ 100,000	$ -	$ 1,000,000	$ 1,100,000
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	7	$ 2,000,000	0.25	42	$ 50[illegible]00	$ 100,000	$ -	$ 350,000	$ 450,000
R0005	Insider Threat	8	Non-malicious employee negligence.	5	Loss of **Client Confidential** material	10	$ 500,000	1	40	$ 50[illegible]00	$ 100,000	$ -	$ 1,000,000	$ 1,100,000
R0006	Fraud - False Executive/Wire Transfer Requests	10	Insufficient authentication of internal communications	5	Financial loss	6	$ 200,000	0.2	30	$ 4[illegible]00	$ 10,000	$ -	$ 50,000	$ 60,000
R0007	DDoS, possible extortion	4	Poor DDoS protections in place.	7	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	9	$ 200,000	0.5	25.2	$ 10[illegible]00	$ 100,000	$ -	$ 100,000	$ 200,000
R0008	Fraud - False Invoices sent to clients	8	Insufficient authentication of email services	3	Client frustration. Loss of client trust.	4	$ 100,000	5	9.6	$ 500,[illegible]0	$ 10,000	$ -	$ 50,000	$ 60,000

0:30

www.risklevelagreements.com

5. Establish Risk Level Agreements™

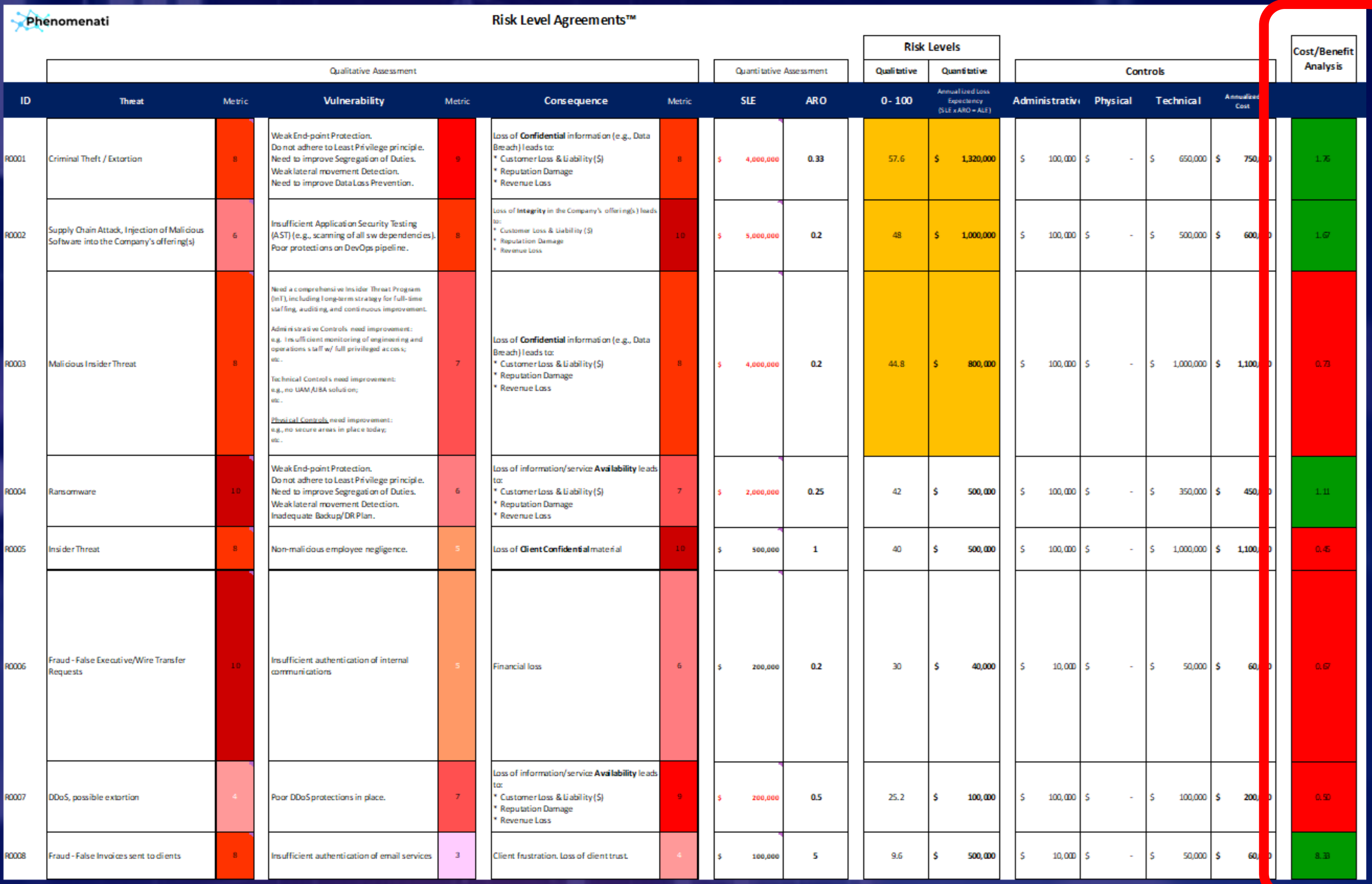
Phenomenati

Cost–Benefit Analysis:

- Reduction of Quantifiable Risk
- Cost of Control(s)

B/C Ratio:

- > 1, good investment
- < 1, weak investment



Phenomenati

Risk Level Agreements™

									Risk Levels						
	Qualitative Assessment						Quantitative Assessment		Qualitative	Quantitative	Controls				Cost/Benefit Analysis
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric	SLE	ARO	0- 100	Annualized Loss Expectancy (SLE x ARO = ALE)	Administrativ	Physical	Technical	Annualized Cost	
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.33	57.6	$ 1,320,000	$ 100,000	$ -	$ 650,000	$ 750,[illegible]	1.76
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	10	$ 5,000,000	0.2	48	$ 1,000,000	$ 100,000	$ -	$ 500,000	$ 600,[illegible]	1.67
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.	7	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.2	44.8	$ 800,000	$ 100,000	$ -	$ 1,000,000	$ 1,100,[illegible]	0.73
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	7	$ 2,000,000	0.25	42	$ 500,000	$ 100,000	$ -	$ 350,000	$ 450,[illegible]	1.11
R0005	Insider Threat	8	Non-malicious employee negligence.	5	Loss of **Client Confidential** material	10	$ 500,000	1	40	$ 500,000	$ 100,000	$ -	$ 1,000,000	$ 1,100,[illegible]	0.45
R0006	Fraud - False Executive/Wire Transfer Requests	10	Insufficient authentication of internal communications	5	Financial loss	6	$ 200,000	0.2	30	$ 40,000	$ 10,000	$ -	$ 50,000	$ 60,[illegible]	0.67
R0007	DDoS, possible extortion	4	Poor DDoS protections in place.	7	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	9	$ 200,000	0.5	25.2	$ 100,000	$ 100,000	$ -	$ 100,000	$ 200,[illegible]	0.50
R0008	Fraud - False Invoices sent to clients	8	Insufficient authentication of email services	3	Client frustration. Loss of client trust.	4	$ 100,000	5	9.6	$ 500,000	$ 10,000	$ -	$ 50,000	$ 60,[illegible]	8.33

0:30

www.risklevelagreements.com

5. Establish Risk Level Agreements™

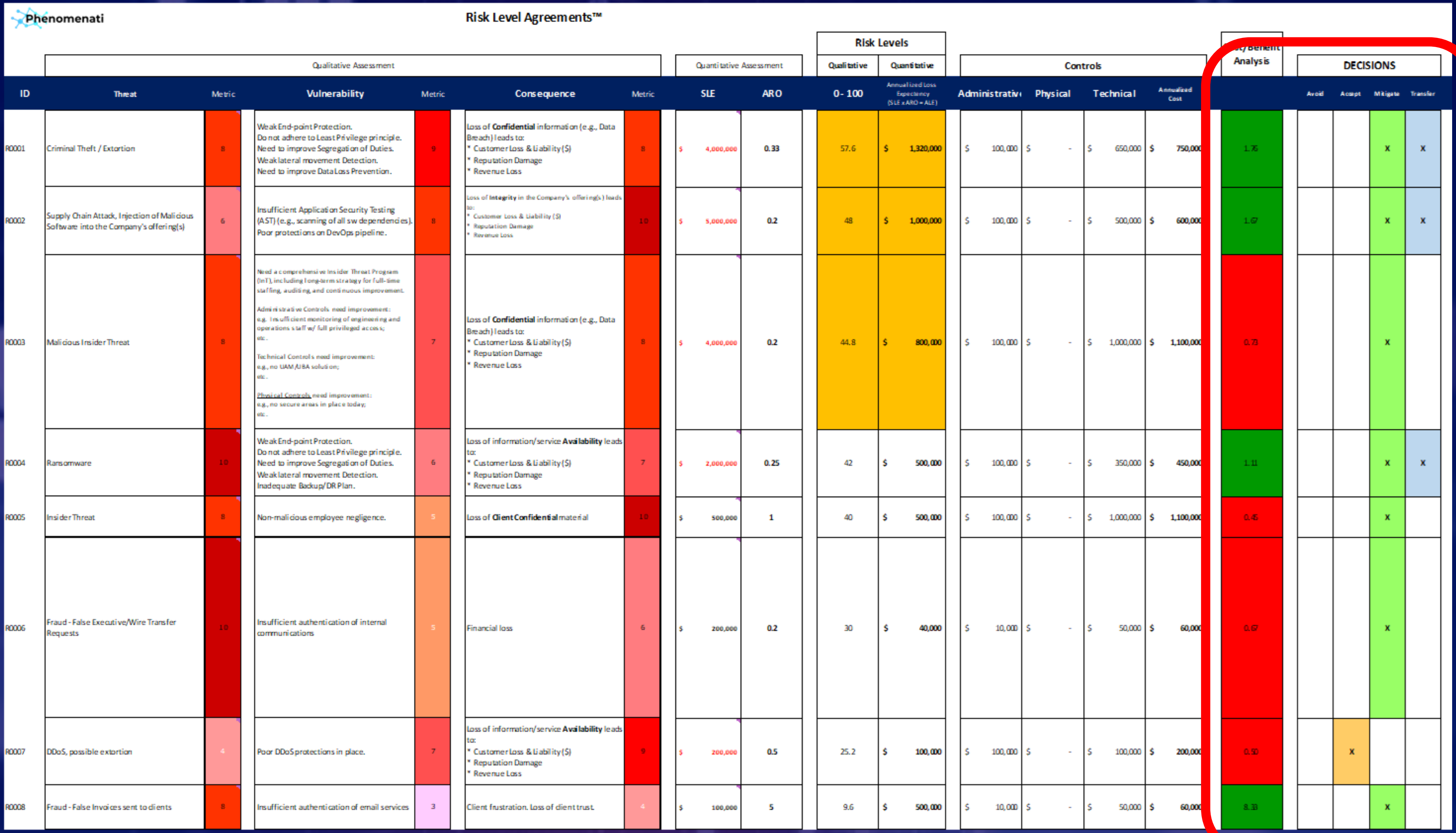
Phenomenati

Decisions:

- Avoid the Risk
- Accept the Risk
- Mitigate the Risk
- Transfer the Risk

Combining Options:

- Mitigate some Risk,
- & Transfer some Risk



Phenomenati

Risk Level Agreements™

	Qualitative Assessment						Quantitative Assessment		Risk Levels		Controls				Cost/Benefit Analysis	DECISIONS			
									Qualitative	Quantitative									
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric	SLE	ARO	0-100	Annualized Loss Expectancy (SLE x ARO = ALE)	Administrativ	Physical	Technical	Annualized Cost		Avoid	Accept	Mitigate	Transfer
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.33	57.6	$ 1,320,000	$ 100,000	$ -	$ 650,000	$ 750,000	1.76			X	X
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of **Integrity** in the Company's offering(s) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	10	$ 5,000,000	0.2	48	$ 1,000,000	$ 100,000	$ -	$ 500,000	$ 600,000	1.67			X	X
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc.	7	Loss of **Confidential** information (e.g., Data Breach) leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	8	$ 4,000,000	0.2	44.8	$ 800,000	$ 100,000	$ -	$ 1,000,000	$ 1,100,000	0.73			X	
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	7	$ 2,000,000	0.25	42	$ 500,000	$ 100,000	$ -	$ 350,000	$ 450,000	1.11			X	X
R0005	Insider Threat	8	Non-malicious employee negligence.	5	Loss of **Client Confidential** material	10	$ 500,000	1	40	$ 500,000	$ 100,000	$ -	$ 1,000,000	$ 1,100,000	0.45			X	
R0006	Fraud - False Executive/Wire Transfer Requests	10	Insufficient authentication of internal communications	5	Financial loss	6	$ 200,000	0.2	30	$ 40,000	$ 10,000	$ -	$ 50,000	$ 60,000	0.67			X	
R0007	DDoS, possible extortion	4	Poor DDoS protections in place.	7	Loss of information/service **Availability** leads to: * Customer Loss & Liability ($) * Reputation Damage * Revenue Loss	9	$ 200,000	0.5	25.2	$ 100,000	$ 100,000	$ -	$ 100,000	$ 200,000	0.50		X		
R0008	Fraud - False Invoices sent to clients	8	Insufficient authentication of email services	3	Client frustration. Loss of client trust.	4	$ 100,000	5	9.6	$ 500,000	$ 10,000	$ -	$ 50,000	$ 60,000	8.33			X	

0:30

www.risklevelagreements.com

5. Establish Risk Level Agreements™

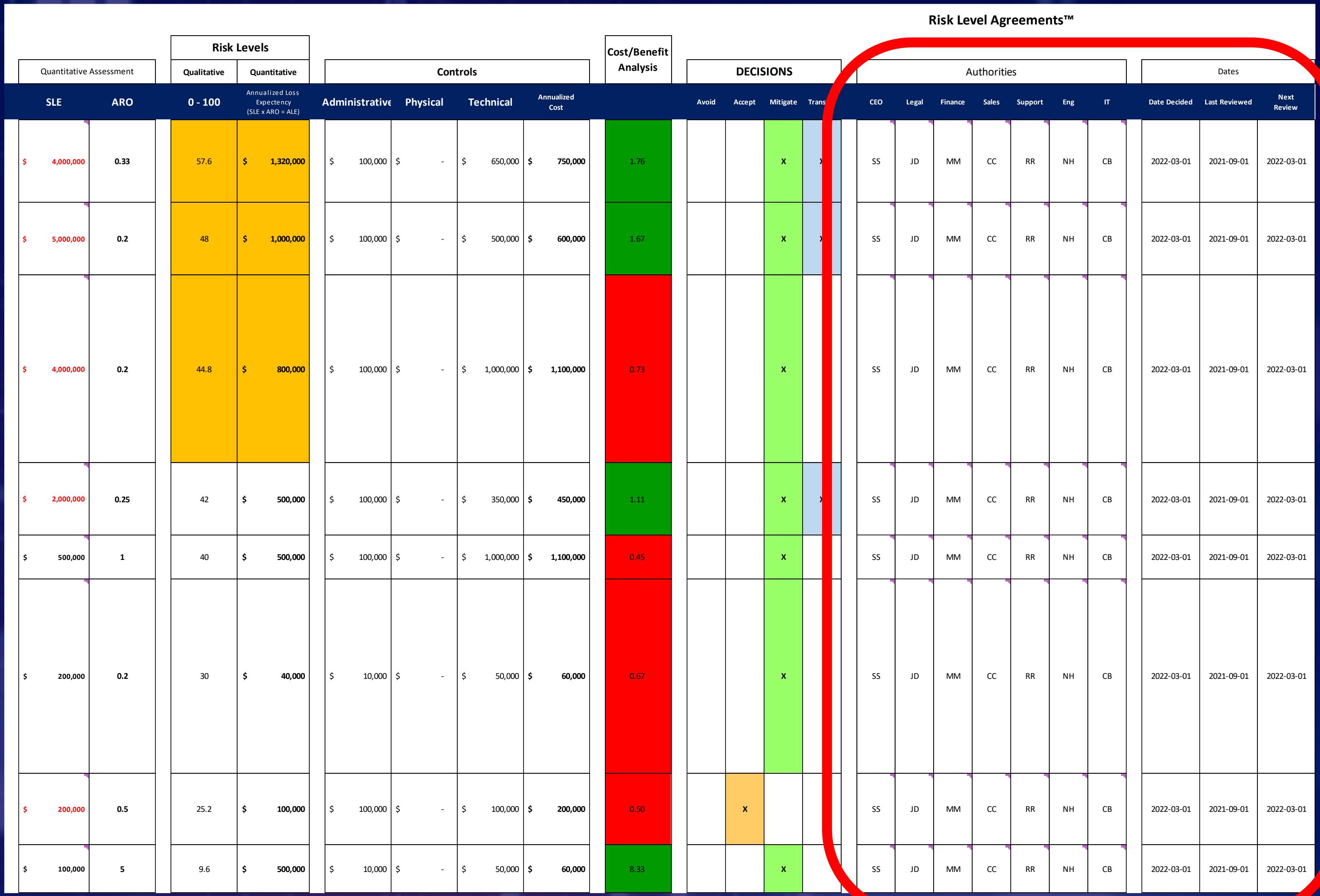
Phenomenati

Record:

- Decision made
- Date
- Exec Team Members

Track:

- Last Reviewed Date
- Next Review Date



Risk Level Agreements™

Quantitative Assessment		Risk Levels		Controls				Cost/Benefit Analysis	DECISIONS				Authorities							Dates		
		Qualitative	Quantitative																			
SLE	ARO	0 - 100	Annualized Loss Expectency (SLE x ARO = ALE)	Administrative	Physical	Technical	Annualized Cost		Avoid	Accept	Mitigate	Trans	CEO	Legal	Finance	Sales	Support	Eng	IT	Date Decided	Last Reviewed	Next Review
$ 4,000,000	0.33	57.6	$ 1,320,000	$ 100,000	$ -	$ 650,000	$ 750,000	1.76			X	X	SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 5,000,000	0.2	48	$ 1,000,000	$ 100,000	$ -	$ 500,000	$ 600,000	1.67			X	X	SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 4,000,000	0.2	44.8	$ 800,000	$ 100,000	$ -	$ 1,000,000	$ 1,100,000	0.73			X		SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 2,000,000	0.25	42	$ 500,000	$ 100,000	$ -	$ 350,000	$ 450,000	1.11			X	X	SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 500,000	1	40	$ 500,000	$ 100,000	$ -	$ 1,000,000	$ 1,100,000	0.45			X		SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 200,000	0.2	30	$ 40,000	$ 10,000	$ -	$ 50,000	$ 60,000	0.67			X		SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 200,000	0.5	25.2	$ 100,000	$ 100,000	$ -	$ 100,000	$ 200,000	0.50		X			SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01
$ 100,000	5	9.6	$ 500,000	$ 10,000	$ -	$ 50,000	$ 60,000	8.33			X		SS	JD	MM	CC	RR	NH	CB	2022-03-01	2021-09-01	2022-03-01

www.risklevelagreements.com

0:30

6. Integrate Business Operations ←→ Security Operations

Phenomenati

Monitoring and Detection

- Early Warning Systems (e.g., Canaries)
- Normal vs. Suspicious Activity, Behavior
- Indicators of Attack, Behaviors, Compromise

Correction and Recovery

- Network Failover, Recovery & Restoration
- System Failover, Recovery & Restoration
- Service Failover, Recovery & Restoration
- Information Failover, Recovery & Restoration
- User Failover, Recovery & Restoration
- Business Process Failover, Recovery & Restoration

Prevention

- Asset Classification & Labeling
- Disciplined Access Control
- "Need To Know"
- "Least Privilege"
- "Zero Trust" Architecture Patterns
- Data Loss Prevention (DLP)

Deception and Disruption

- Honeypots, Honeynets
- Counter-Intelligence, Investigation
- Disruptive Engagement
- Disinformation (Poison the Exfiltrated Data)

Integration Informs *Decisions*

3:00

7. Insist on Governance

Phenomenati

Change Management

- Business Impact Assessment
- Privacy Impact Assessment
- Risk Assessment
- Available Mitigations
- Risk Informed Decisions

Crisis Management

- Incident Response Plan (IRP)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Crisis Communications Plan (CCP)
- Practice, Exercise, Test

Risk Management

- (discussed earlier)

Threat Modeling

- Political Threats
- Economic Threats
- Social Threats
- Technological Threats
- Legal Threats
- Environmental Threats

Vendor Management

- Initial Assessment
- Contractual Commitments
- Service Level Agreement (SLA) Monitoring
- Regular Audits
- Planned Obsolescence

Governance
Prepares for
Resiliency

3:00

Summary

Survival Strategies

1. Develop “Meta” Systems
2. Cultivate Domain Awareness
3. Promote Risk Awareness
4. Invest in Contingencies & Controls
5. Establish Risk Level Agreements™
6. Integrate Business Operations ←→ Security Operations
7. Insist on Governance

Bring Order to Entropy

Acknowledge Conflict

Embrace Risk

Plan for Resilience

1:00

Questions?

Phenomenati