caiS Inteligência em Cibersegurança RNP

Method for Cyber Risk Assessment

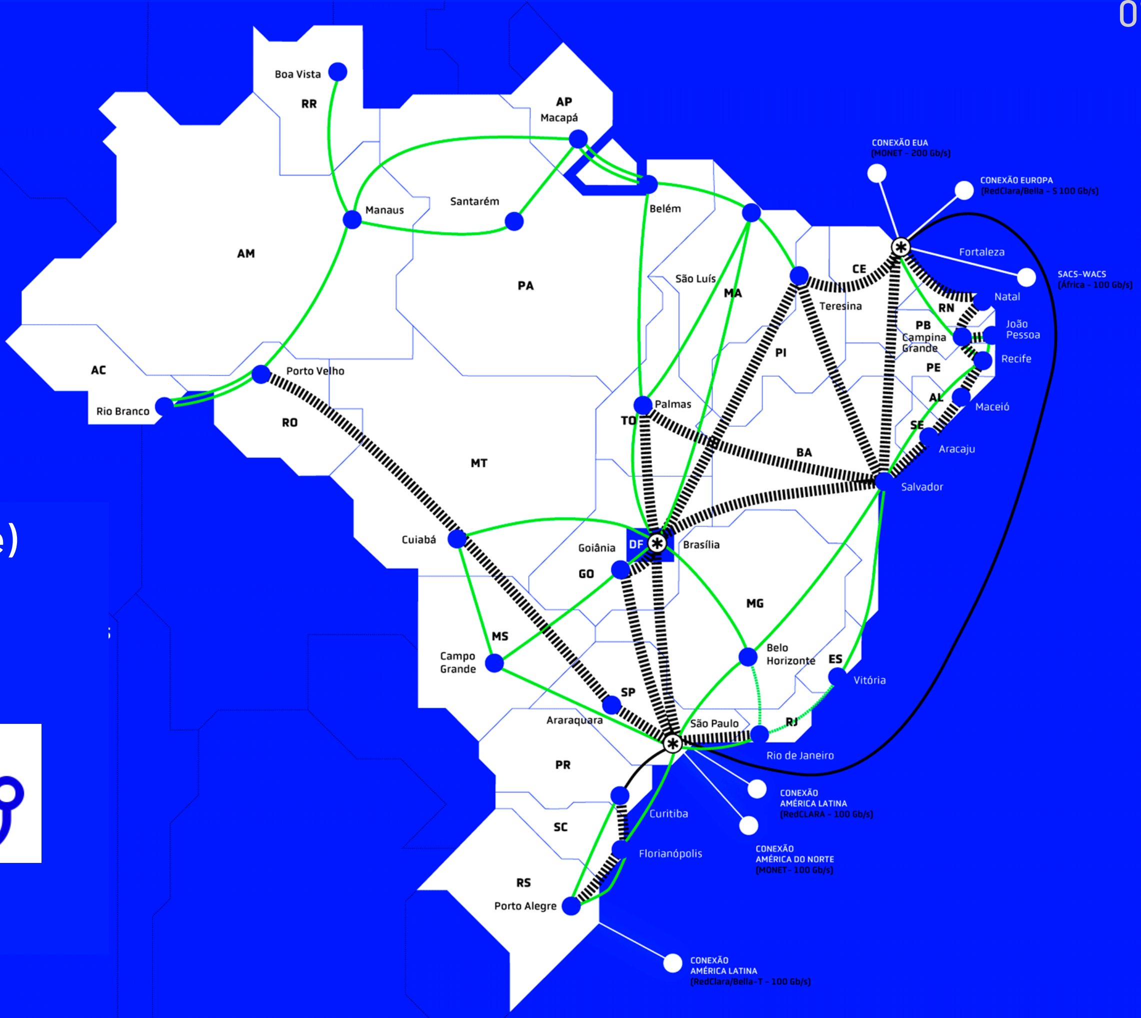
Developing risk assessment capabilities in NRENs

Humberto Forsan

Information Security Manager

About RNP

- Brazilian National Research and Education Network (RNP).
- Created in 1989.
- 1800 institutions connected (RedeIpê)
- 27 Points of Presence (PoPs)



WHERE DO YOU APPLY SECURITY?

In Everything?

Can you do it?

Do you know where to apply more security?

TLP:CLEAR

Do you know where to apply more security?

How do you know where to apply more security?

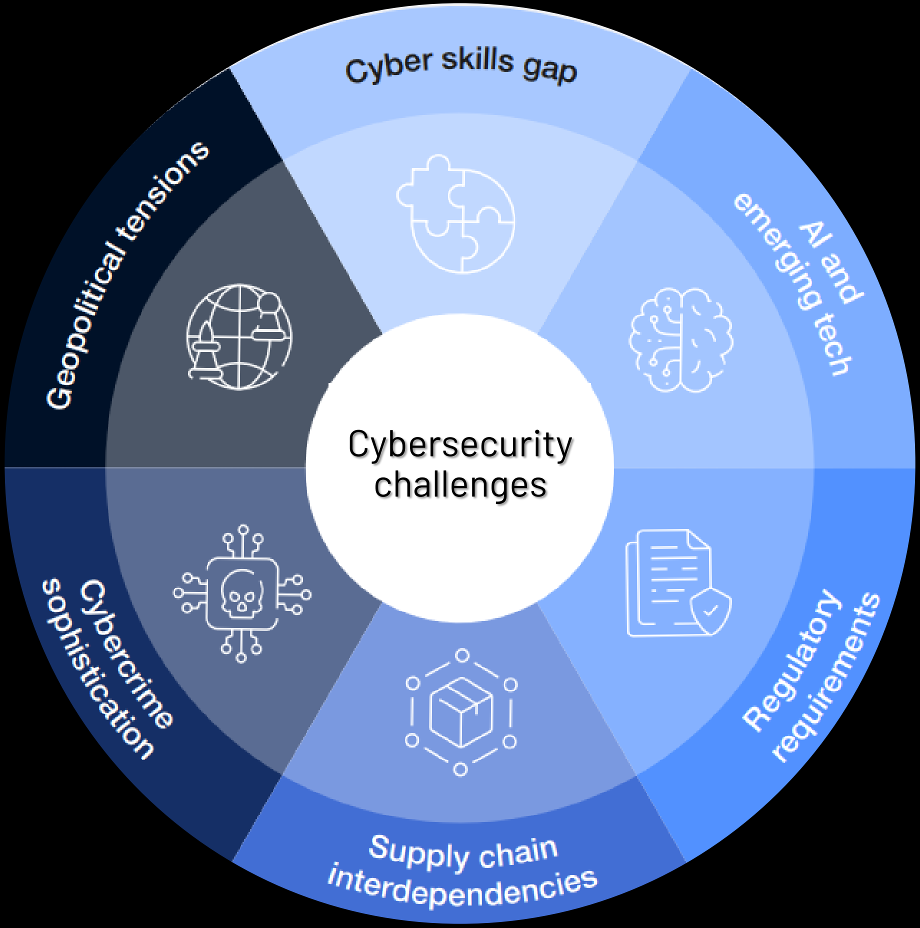
Risks!

The definition of risk according to ISO 27001 is the effect of uncertainty on objectives.

Risk is the combination of the probability of something happening and the impact.

What the hell is this kid going to do?

We cannot protect everything



and perhaps, we should not even try

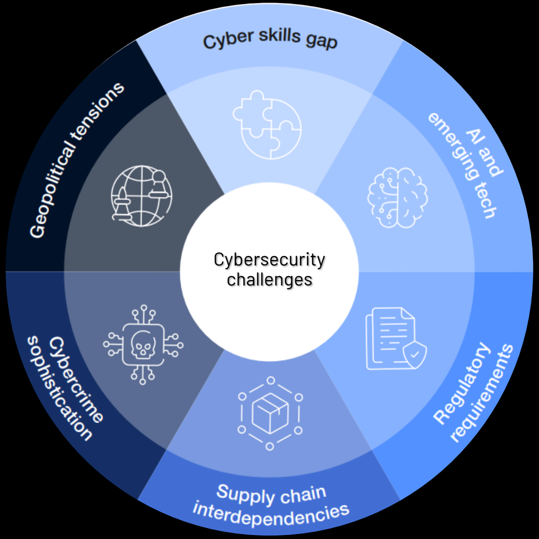
Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

TLP:CLEAR

What's important
to you?

Everything?

...But, can you protect everything?



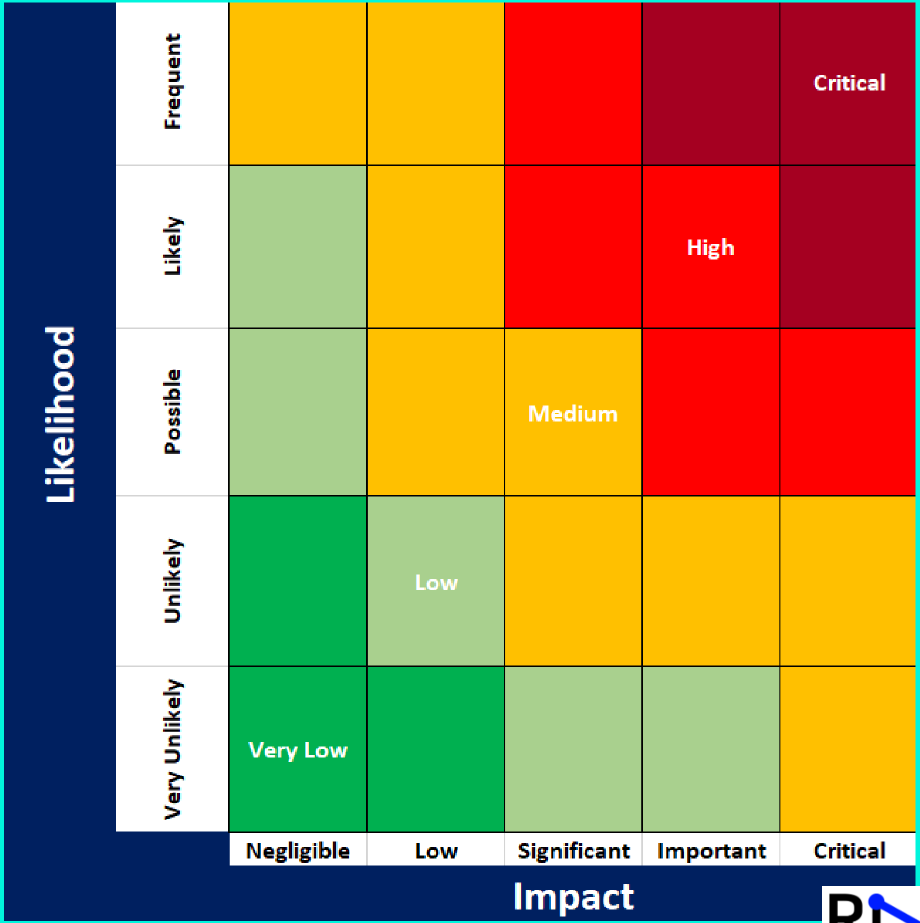
What really matters to you?

How to know what really matters to you?

Risk Assessment

Inside the Risk

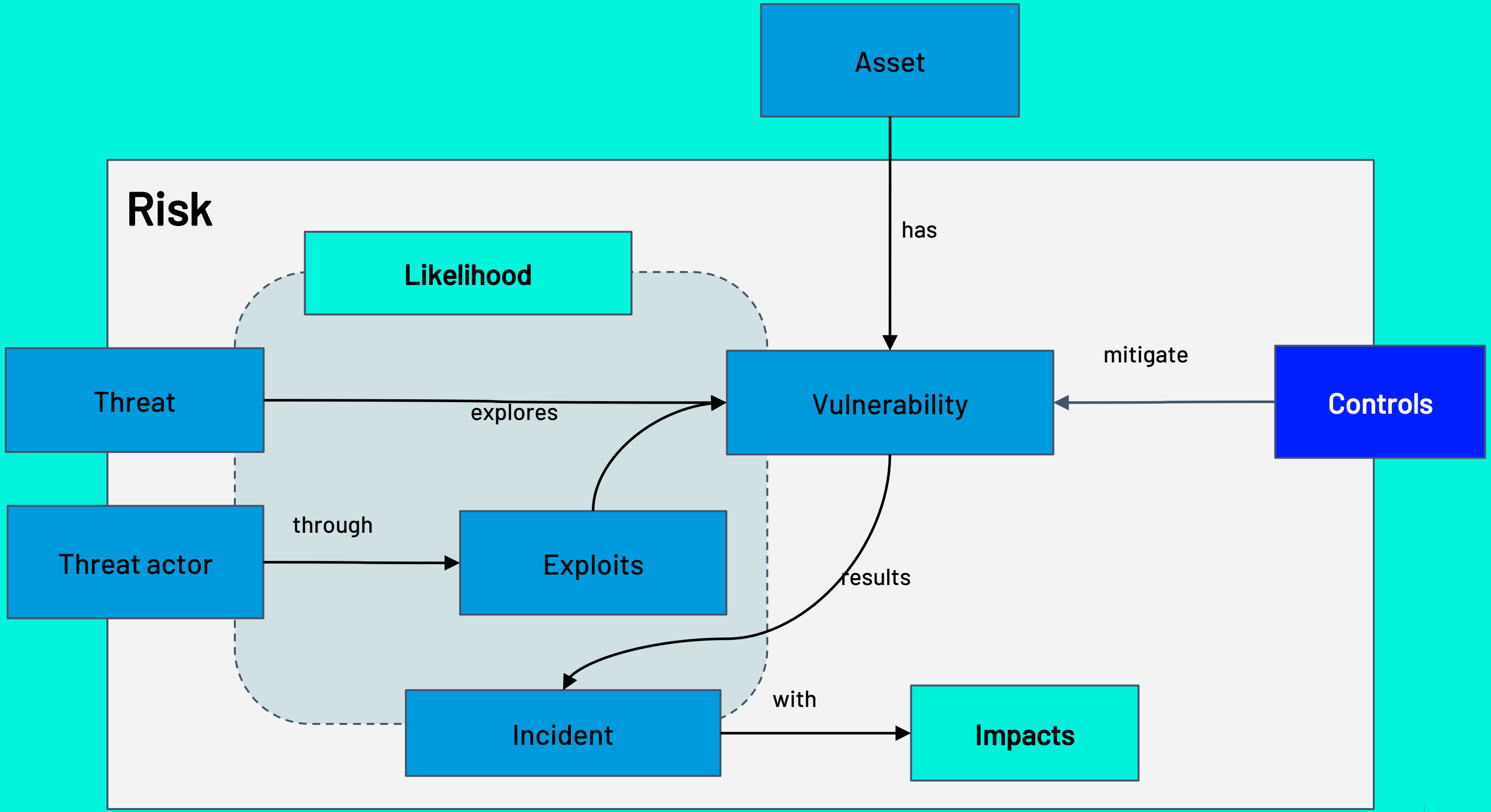
LIKELIHOOD × IMPACT → RISK



Likelihood		Negligible	Low	Significant	Important	Critical
Likelihood	Frequent					Critical
	Likely				High	
	Possible			Medium		
	Unlikely		Low			
	Very Unlikely	Very Low				

Impact

Inside the Risk



"BIA" (Business Impact Analysis) It is crucial for Risk Assessment

BIA identify critical business activities: Understand which processes are essential for the organization's mission. ***(Here you know where apply more efforts in cybersecurity)***

This includes financial, operational, reputational and legal resulting from a loss of confidentiality, integrity, or availability of information.

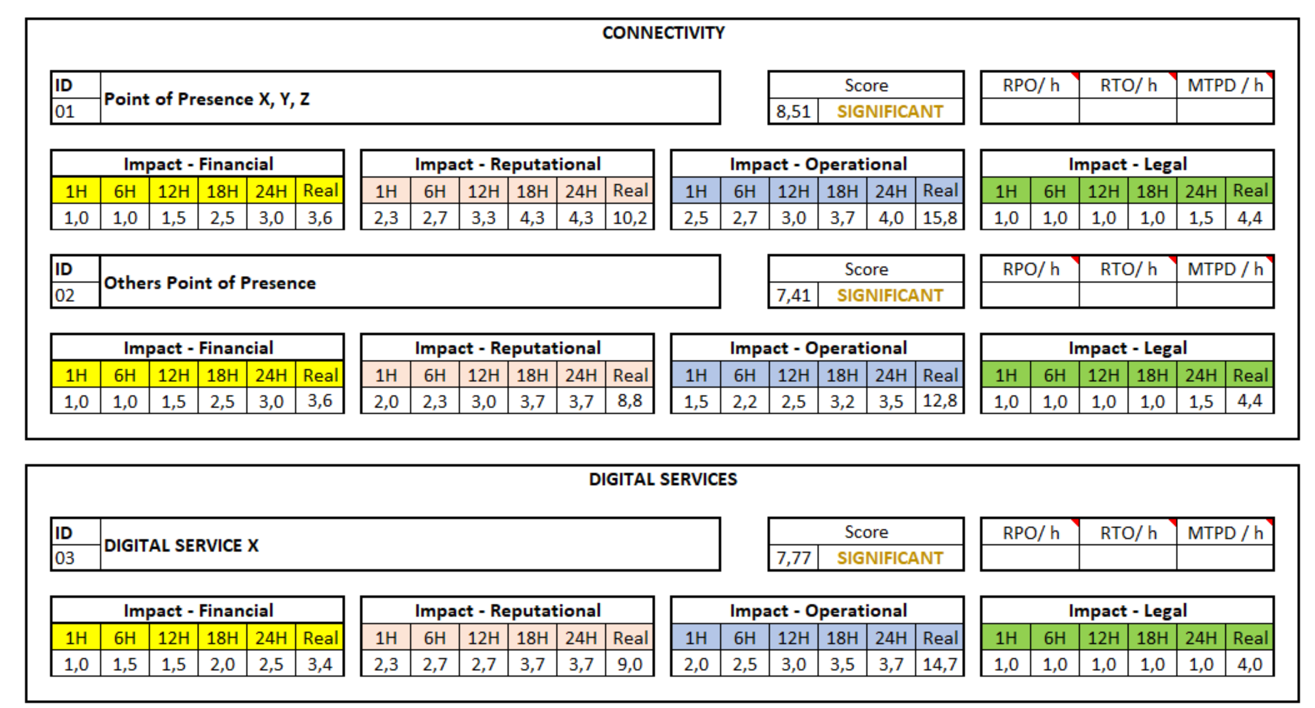
Determine maximum tolerable downtime (MTD), recovery time objectives (RTOs) and recovery point objectives (RPOs)

Map out the IT systems, people, and third-party services crucial for these critical activities. ***(Here you know where apply more efforts in cybersecurity)***

The BIA provides the necessary input for prioritizing information security efforts and developing appropriate resilience and recovery strategies.

"BIA" (Business Impact Analysis) Example

BIA is done through interviews and activity mapping



CONNECTIVITY

ID	Point of Presence X, Y, Z
01	

Score	
8,51	SIGNIFICANT

RPO/ h	RTO/ h	MTPD / h

Impact - Financial						Impact - Reputational						Impact - Operational						Impact - Legal					
1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real
1,0	1,0	1,5	2,5	3,0	3,6	2,3	2,7	3,3	4,3	4,3	10,2	2,5	2,7	3,0	3,7	4,0	15,8	1,0	1,0	1,0	1,0	1,5	4,4

ID	Others Point of Presence
02	

Score	
7,41	SIGNIFICANT

RPO/ h	RTO/ h	MTPD / h

Impact - Financial						Impact - Reputational						Impact - Operational						Impact - Legal					
1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real
1,0	1,0	1,5	2,5	3,0	3,6	2,0	2,3	3,0	3,7	3,7	8,8	1,5	2,2	2,5	3,2	3,5	12,8	1,0	1,0	1,0	1,0	1,5	4,4

DIGITAL SERVICES

ID	DIGITAL SERVICE X
03	

Score	
7,77	SIGNIFICANT

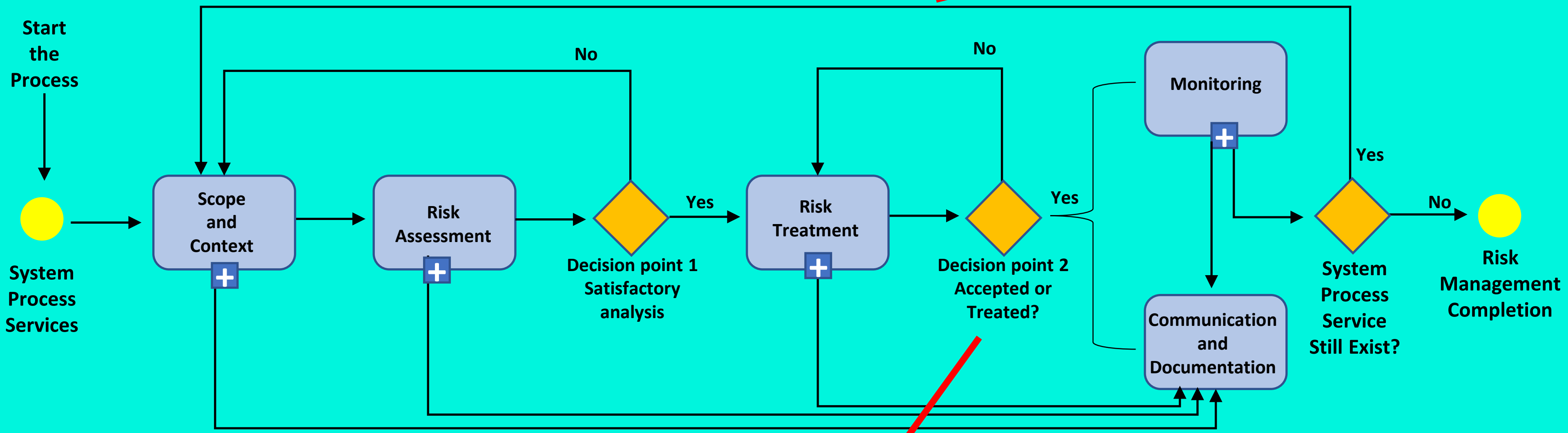
RPO/ h	RTO/ h	MTPD / h

Impact - Financial						Impact - Reputational						Impact - Operational						Impact - Legal					
1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real	1H	6H	12H	18H	24H	Real
1,0	1,5	1,5	2,0	2,5	3,4	2,3	2,7	2,7	3,7	3,7	9,0	2,0	2,5	3,0	3,5	3,7	14,7	1,0	1,0	1,0	1,0	1,0	4,0

Excel spreadsheet example

Risk Assessment Methodology

Define the frequency of risk assessment

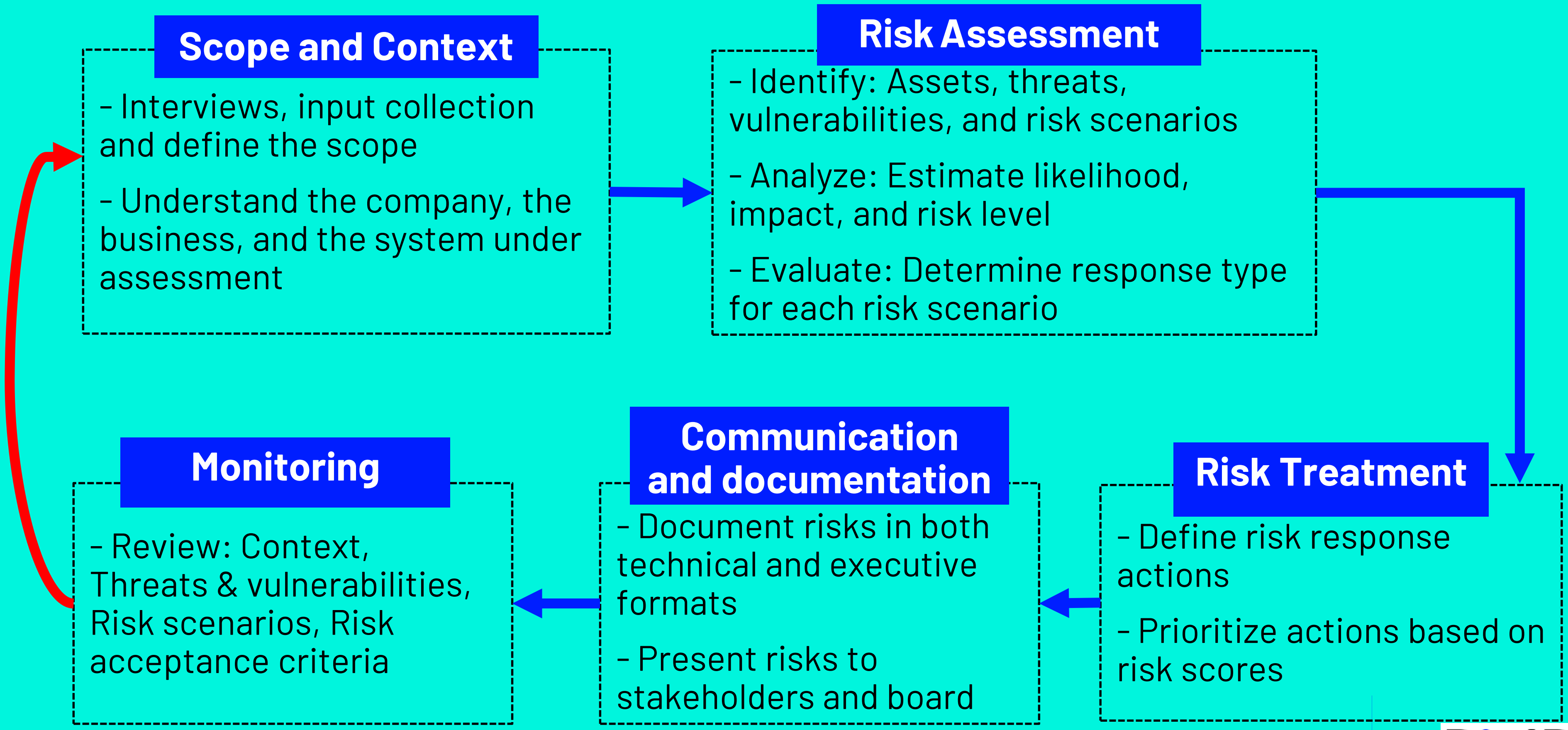


Define who accepts the risk, by criticality

TLP:CLEAR

RNP

Risk Assessment Methodology



Scope and Context

- Interviews, input collection and define the scope

- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios

- Analyze: Estimate likelihood, impact, and risk level

- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions

- Prioritize actions based on risk scores

Communication and documentation

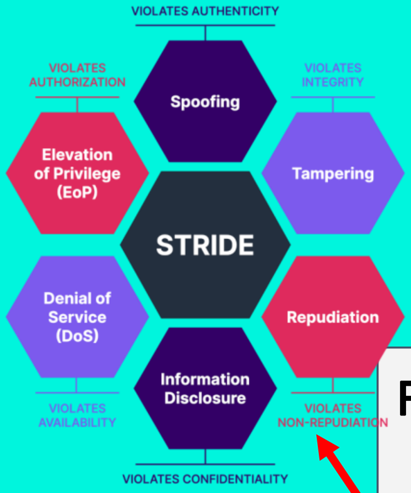
- Document risks in both technical and executive formats

- Present risks to stakeholders and board

Monitoring

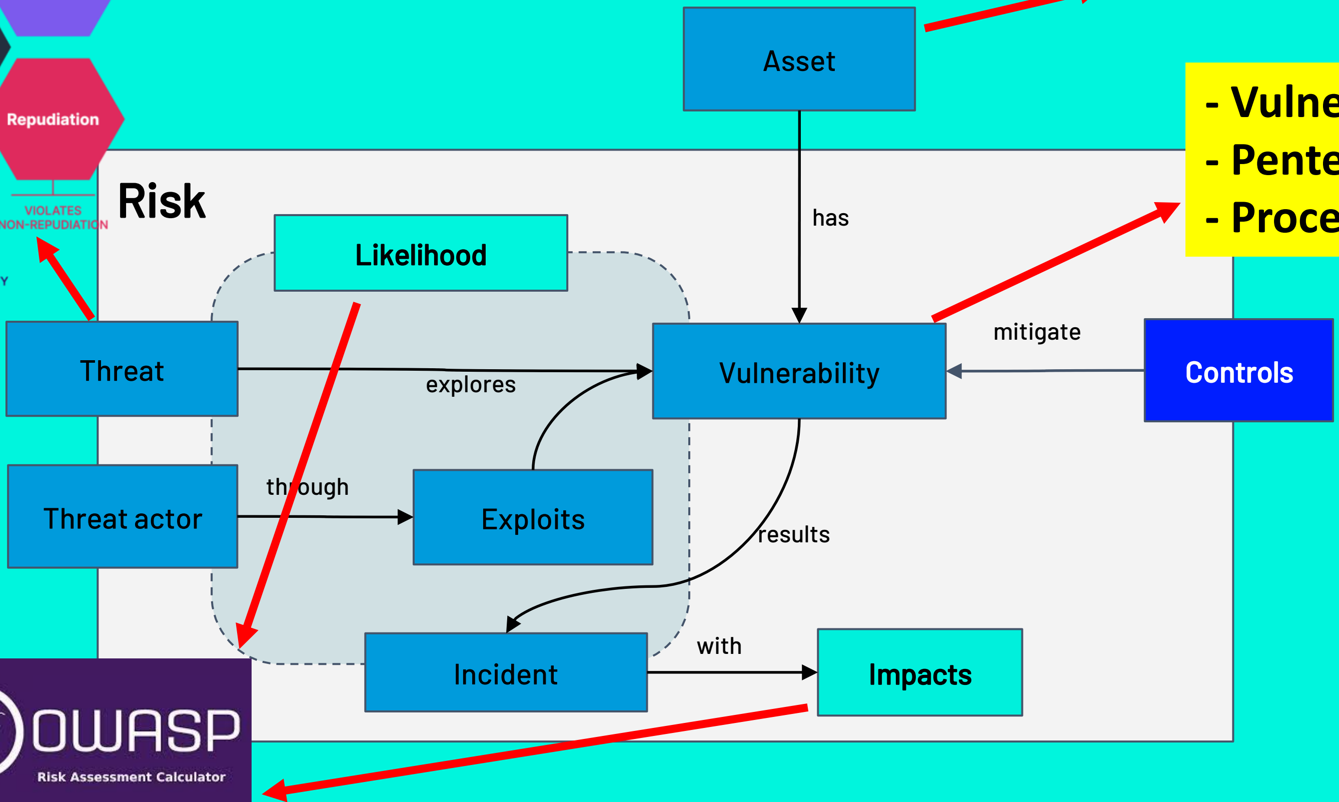
- Review: Context, Threats & vulnerabilities, Risk scenarios, Risk acceptance criteria

Inside Risk Assessment



BIA (Define your target)

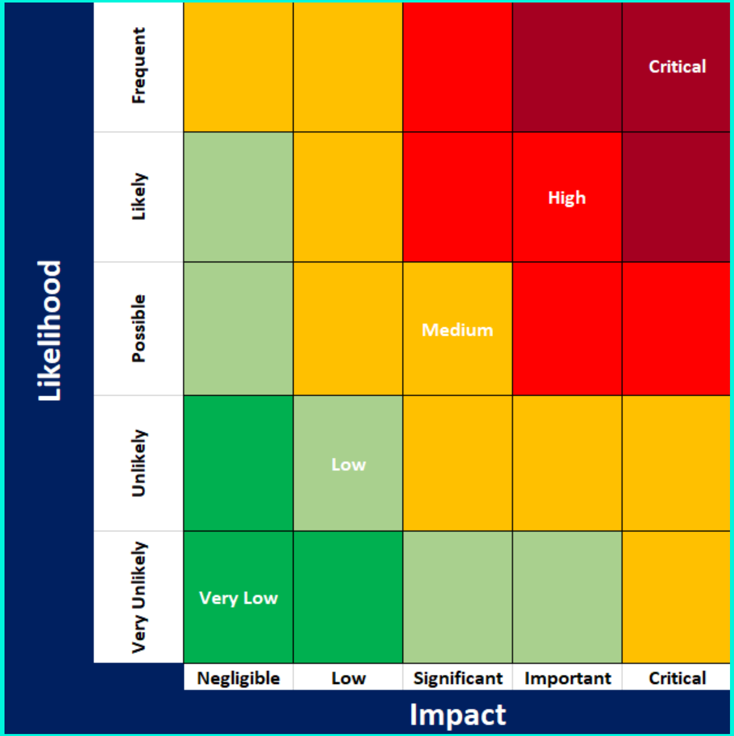
- **Vulnerability Scan**
- **Pentest**
- **Processes**



OWASP
Risk Assessment Calculator

TLP:CLEAR

Inside Risk Assessment



Likelihood					
Frequent					Critical
Likely				High	
Possible			Medium		
Unlikely		Low			
Very Unlikely	Very Low				
	Negligible	Low	Significant	Important	Critical
	Impact				

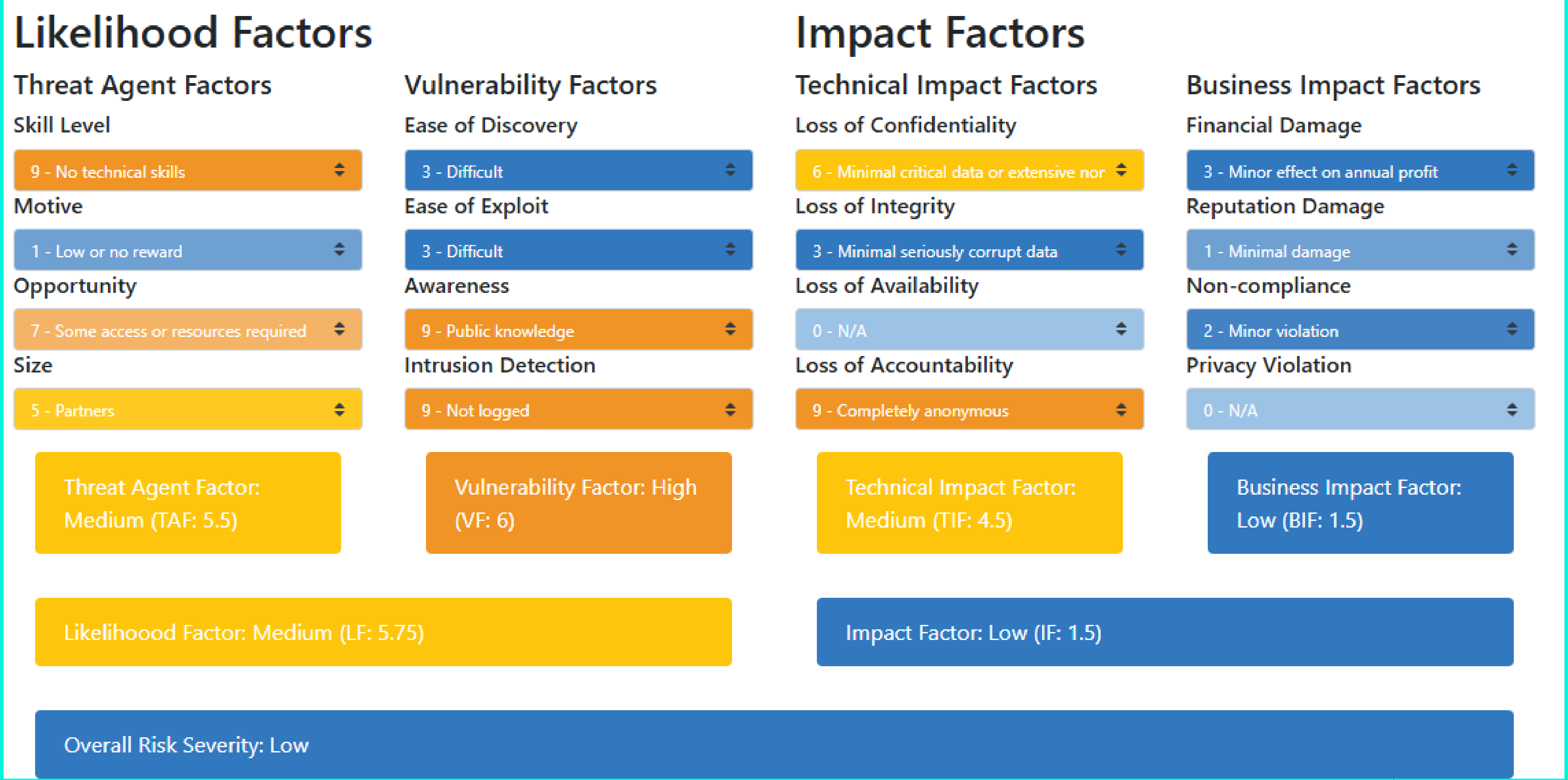
To help calculate the risk

OWASP

Risk Assessment Calculator

https://owasp-risk-rating.com

OWASP Risk Rating Calculator



Likelihood Factors

Threat Agent Factors

Skill Level: 9 - No technical skills

Motive: 1 - Low or no reward

Opportunity: 7 - Some access or resources required

Size: 5 - Partners

Vulnerability Factors

Ease of Discovery: 3 - Difficult

Ease of Exploit: 3 - Difficult

Awareness: 9 - Public knowledge

Intrusion Detection: 9 - Not logged

Impact Factors

Technical Impact Factors

Loss of Confidentiality: 6 - Minimal critical data or extensive nor

Loss of Integrity: 3 - Minimal seriously corrupt data

Loss of Availability: 0 - N/A

Loss of Accountability: 9 - Completely anonymous

Business Impact Factors

Financial Damage: 3 - Minor effect on annual profit

Reputation Damage: 1 - Minimal damage

Non-compliance: 2 - Minor violation

Privacy Violation: 0 - N/A

Threat Agent Factor: Medium (TAF: 5.5)

Vulnerability Factor: High (VF: 6)

Technical Impact Factor: Medium (TIF: 4.5)

Business Impact Factor: Low (BIF: 1.5)

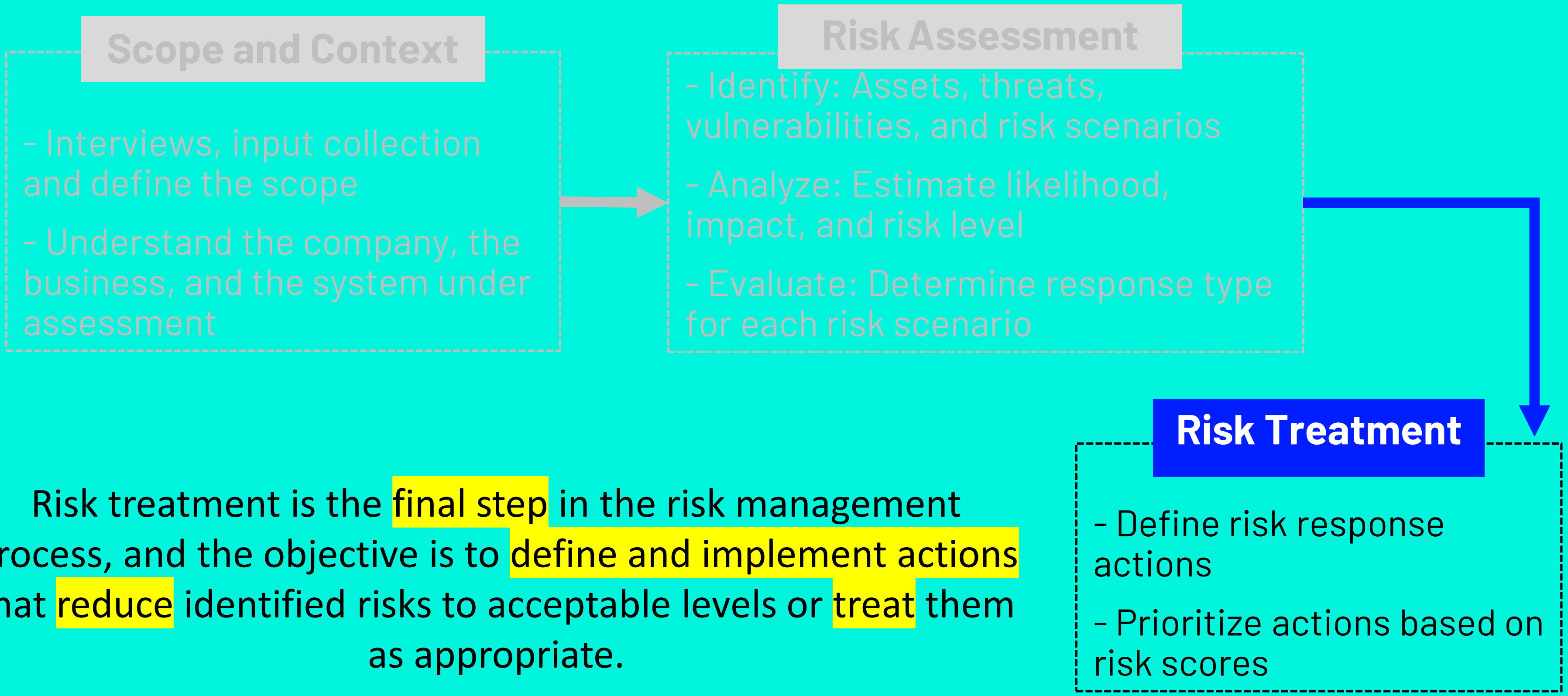
Likelihoood Factor: Medium (LF: 5.75)

Impact Factor: Low (IF: 1.5)

Overall Risk Severity: Low

TLP:CLEAR

Inside Risk Treatment



Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Risk treatment is the final step in the risk management process, and the objective is to define and implement actions that reduce identified risks to acceptable levels or treat them as appropriate.

Inside Risk Treatment

Risk treatment involves coordination between three main actors:

Evaluator: Responsible for assessing risks and providing technical and strategic recommendations for mitigation.

Responsible for the System: Manager or person directly responsible for the system, with authority over the security controls to be implemented.

Interested Parties/Stakeholders: Involves leadership and other relevant areas that may be impacted by mitigation actions or that have decision-making authority.

RNP

TLP:CLEAR

Inside Risk Treatment

Action Plan is responsible for:

Manage identified risks: The plan provides a structured approach to addressing risks identified during the risk assessment process.

Implement controls: It outlines the specific steps and actions needed to implement controls that mitigate or eliminate the identified risks.

Reduce impact and likelihood: The plan aims to reduce the potential negative consequences and probability of risks occurring.

Responsibilities: The plan assigns individuals or teams responsible for implementing and monitoring the risk treatment actions.

Actions and timelines: It specifies the specific actions that will be taken to implement the chosen strategy, including timelines for completion.

Required resources: It identifies the resources needed to carry out the planned actions, such as budget, personnel, and technology.

Communication and Documentation - Monitoring

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

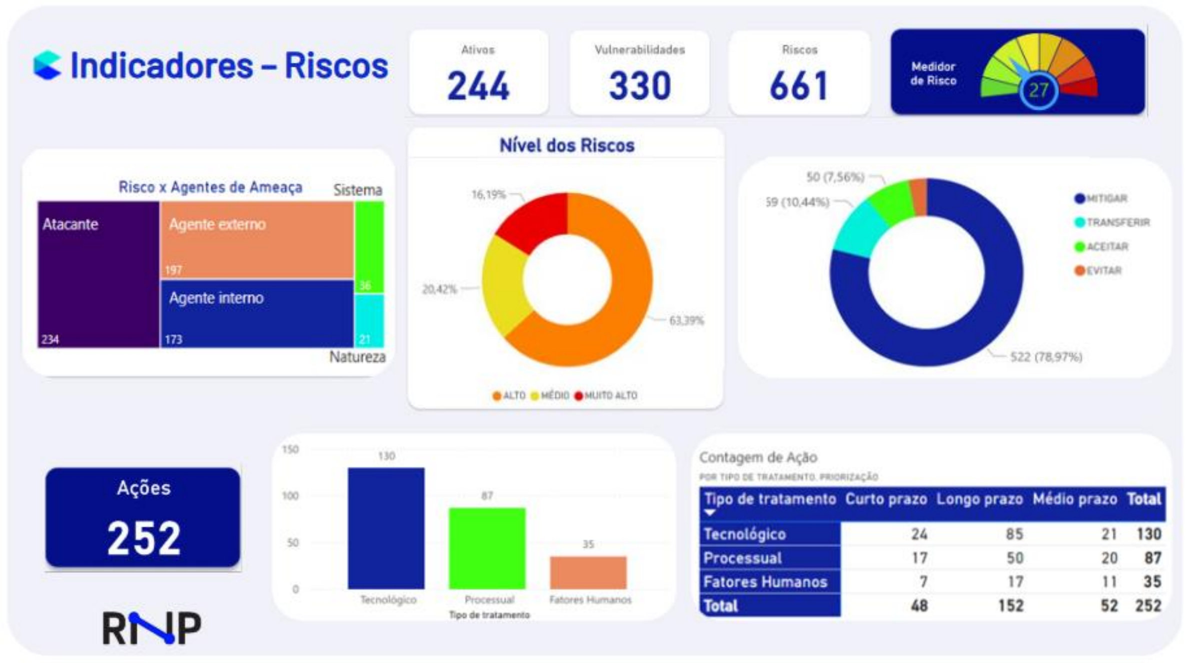
- Define risk response actions
- Prioritize actions based on risk scores

Communication and documentation

- Document risks in both technical and executive formats
- Present risks to stakeholders and board

Monitoring

- Review: Context, Threats & vulnerabilities, Risk scenarios, Risk acceptance criteria



Indicadores – Riscos

Ativos 244

Vulnerabilidades 330

Riscos 661

Medidor de Risco 27

Ações 252

Contagem de Ação

POR TIPO DE TRATAMENTO, PRIORIZAÇÃO

Tipo de tratamento	Curto prazo	Longo prazo	Médio prazo	Total
Tecnológico	24	85	21	130
Processual	17	50	20	87
Fatores Humanos	7	17	11	35
Total	48	152	52	252

Lessons Learned

- **Risk management is continuous** – Always ask: "What’s changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone’s responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.
- **Start small, scale smart** – Begin with limited scopes; expand as maturity grows.
- **Communicate directly** – No intermediaries. Clarity drives buy-in.
- **Expect (and overcome) resistance** – Discomfort means you’re changing the status quo.
- **When in doubt, assume the worst** – Be cautious in your assessments.
- **Risks reveal priorities** – They turn limited resources into strategic actions.

A risk-based strategy isn’t just protection – it’s the art of making uncertainty work for you.

That's working smarter with focus

Ingrid Barbosa

THANK YOU!

humberto.forsan@rnp.br