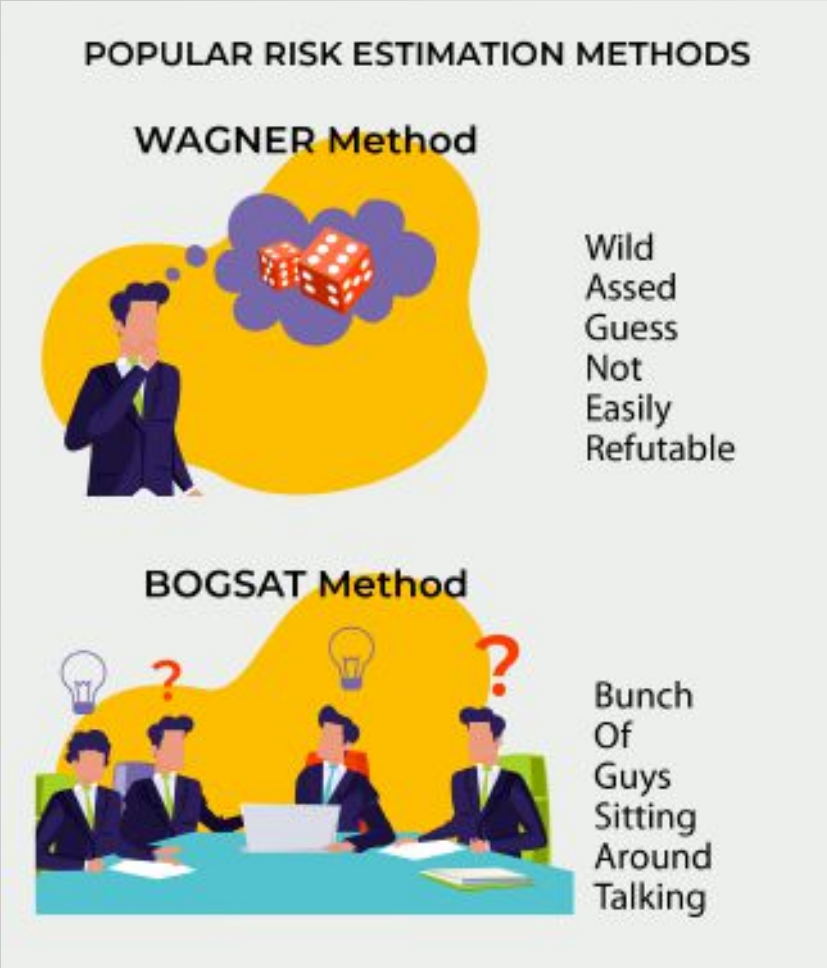
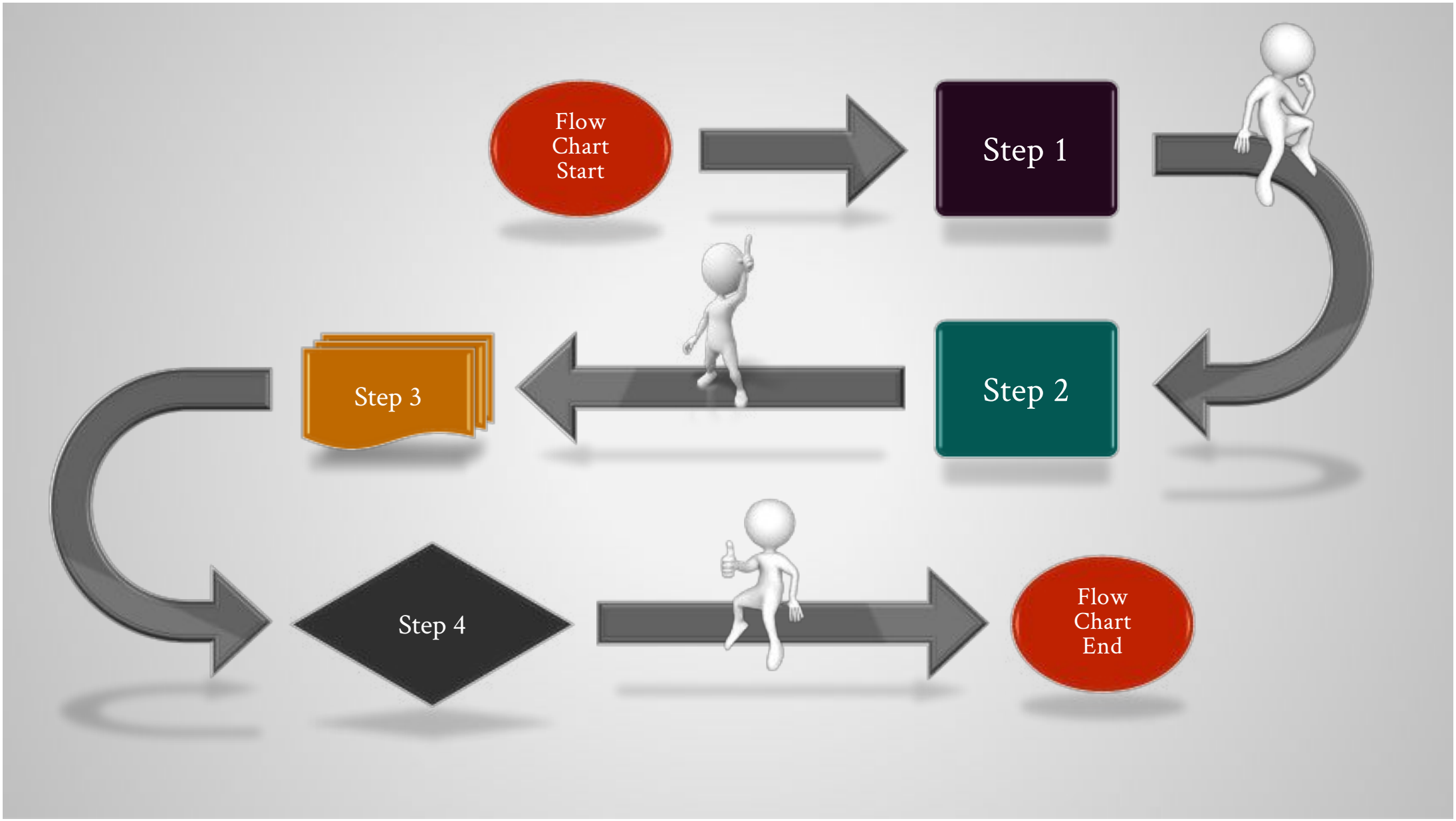
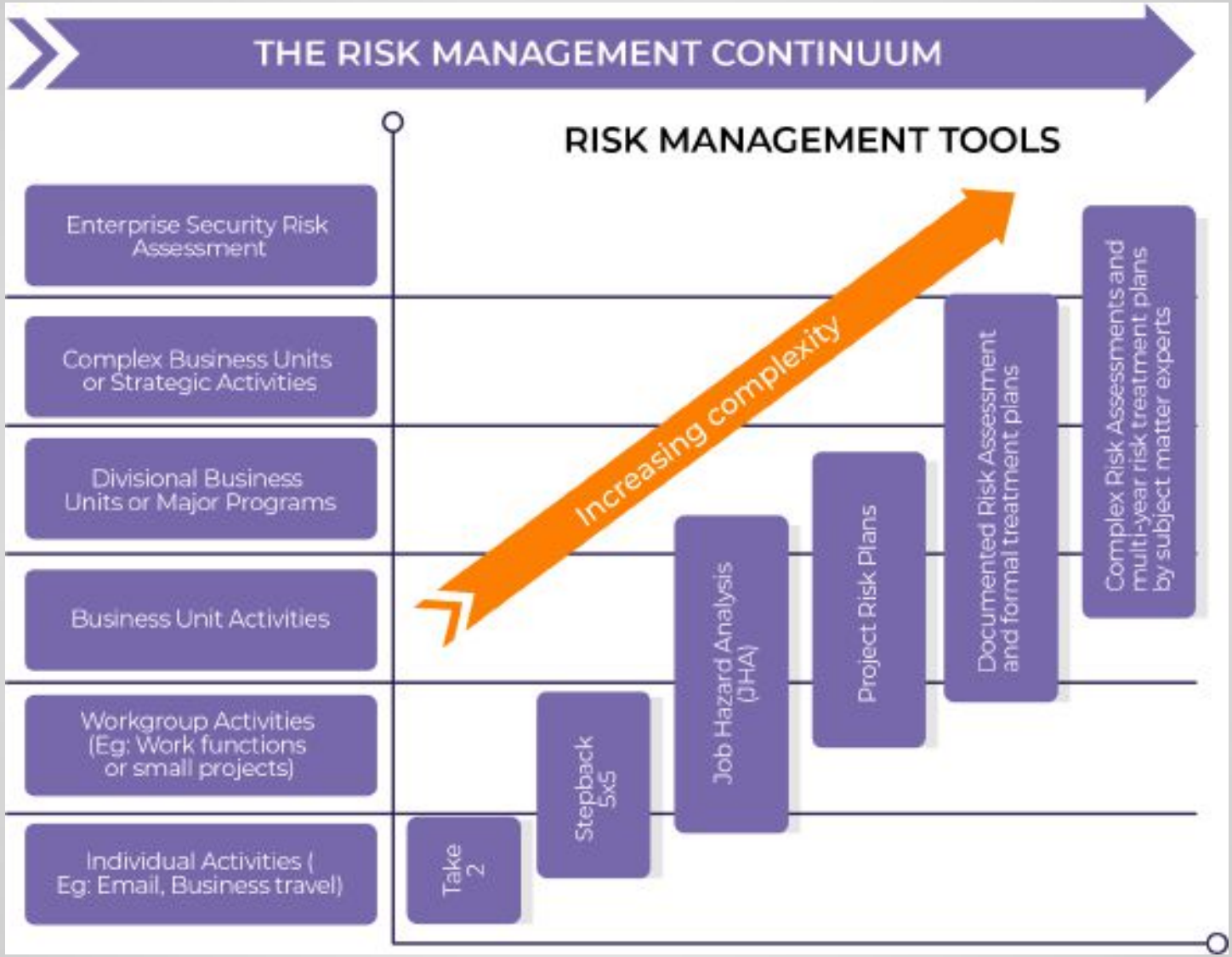
Security Risk Assessment

Julian Talbot

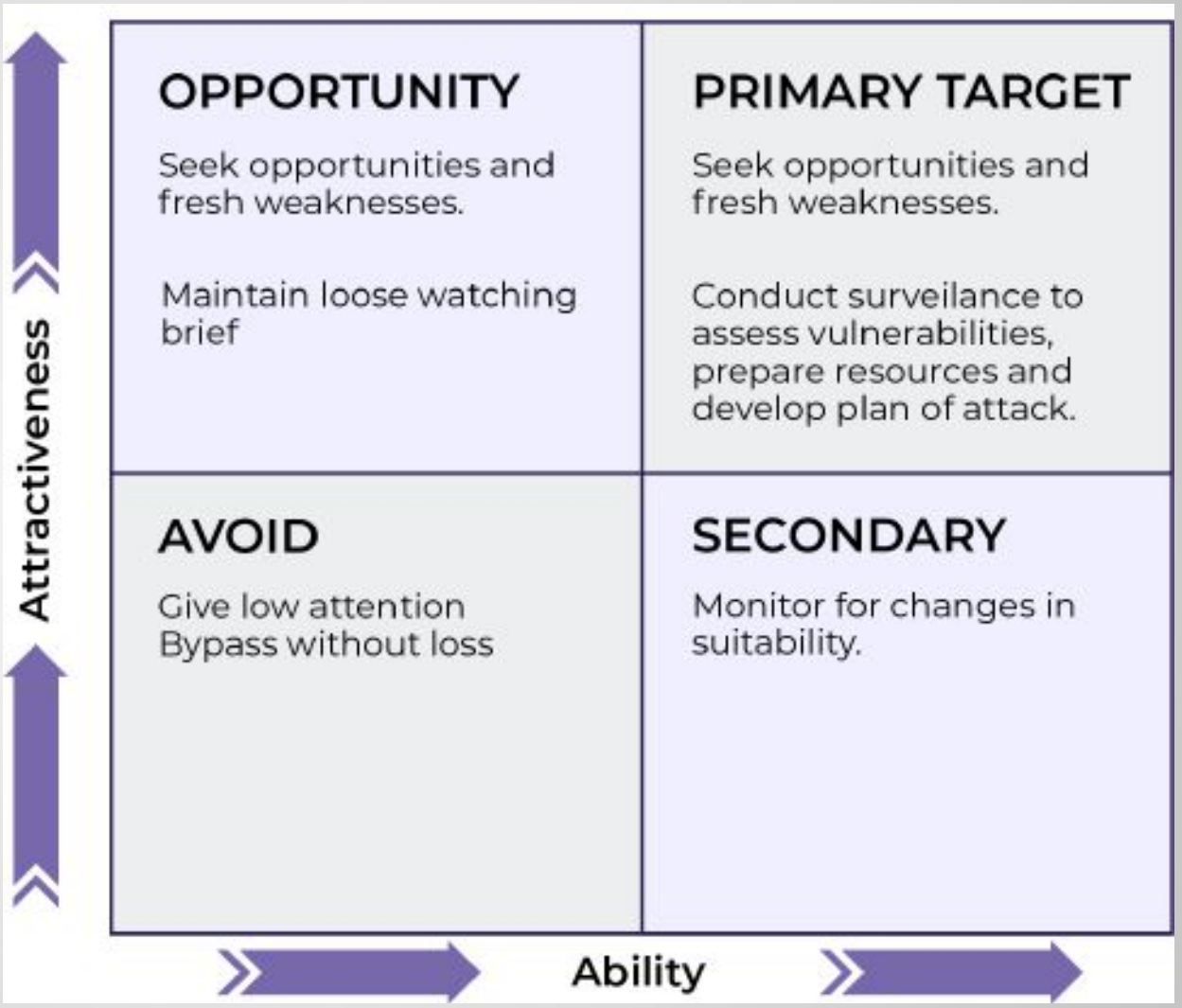


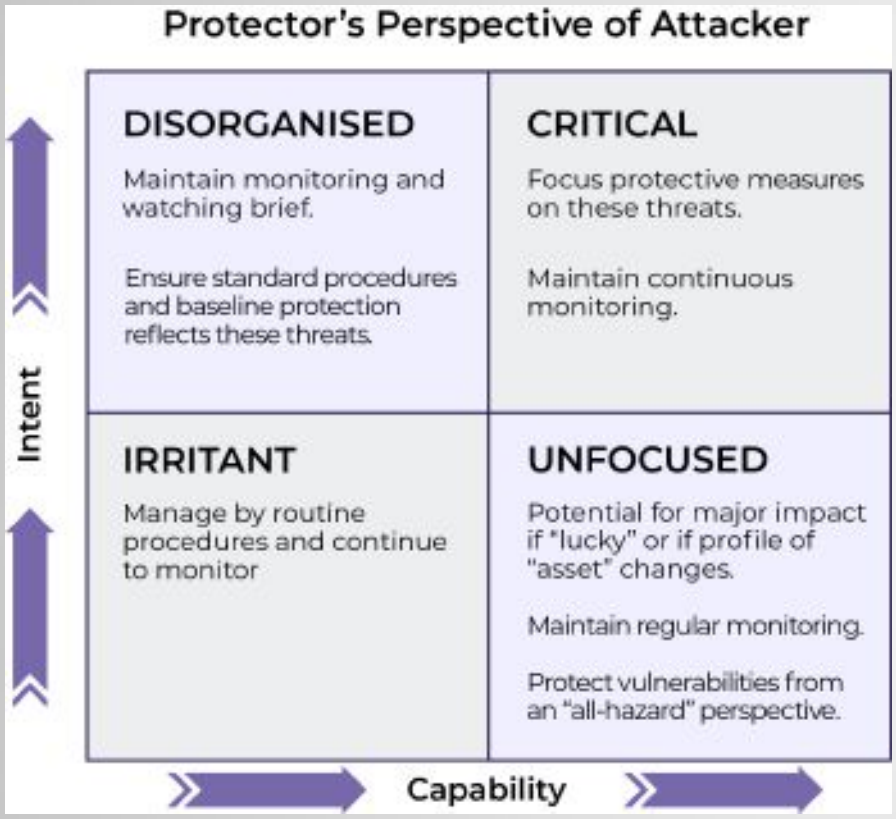
Risk Assessment


Flow Chart Start
Step 1
Step 2
Step 3
Step 4
Flow Chart End


THE RISK MANAGEMENT CONTINUUM
RISK MANAGEMENT TOOLS
Enterprise Security Risk Assessment
Complex Business Units or Strategic Activities
Divisional Business Units or Major Programs
Business Unit Activities
Workgroup Activities (Eg: Work functions or small projects)
Individual Activities (Eg: Email, Business travel)
Increasing complexity
Take 2
Stepback 5x5
Job Hazard Analysis (JHA)
Project Risk Plans
Documented Risk Assessment and formal treatment plans
Complex Risk Assessments and multi-year risk treatment plans by subject matter experts

Attacker / Red Team Perspective

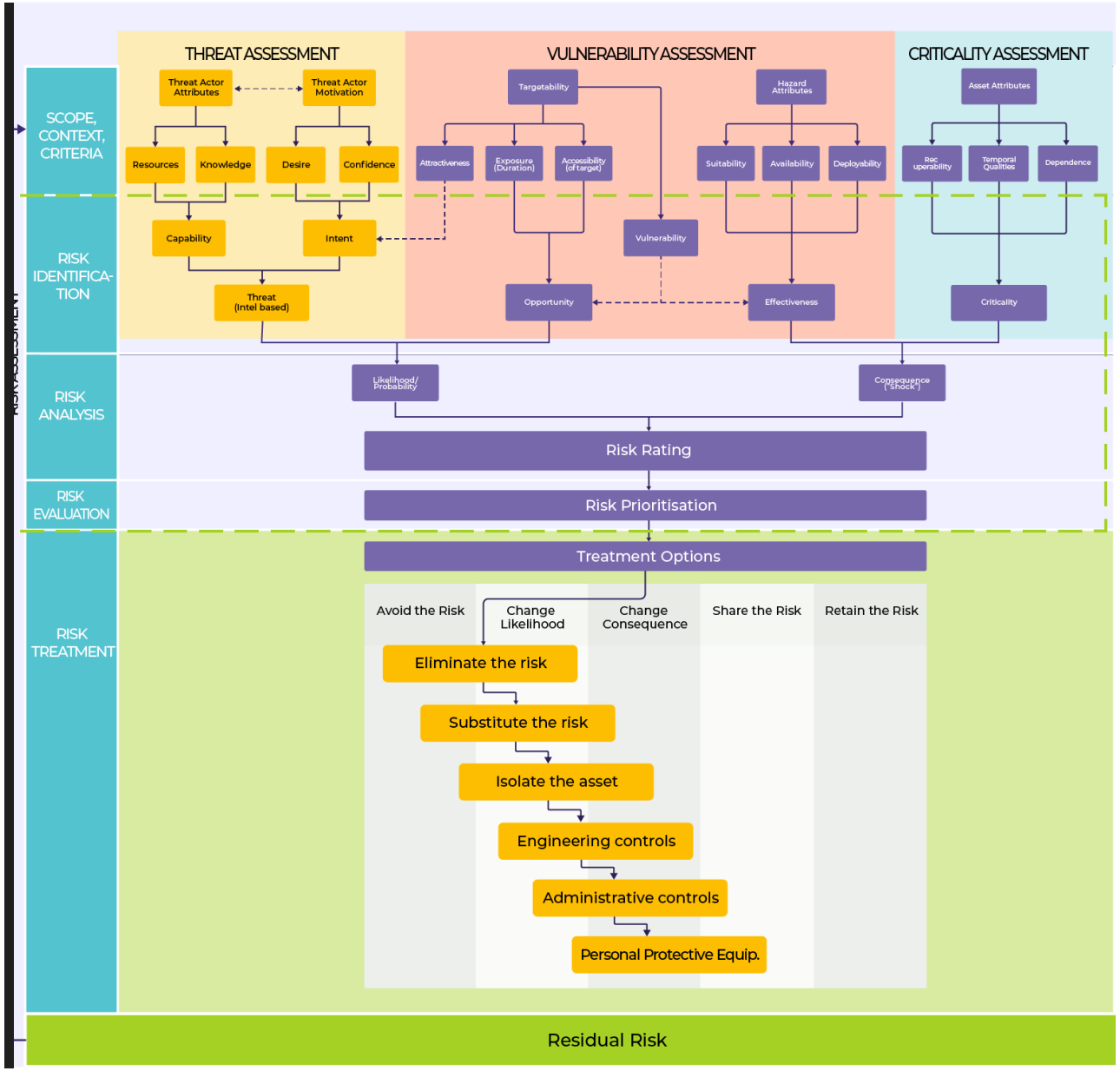




Your perspective

- Security's perspective of potential attackers

SRMBOK SRA Model



Insert your own text here

Heading
Your text goes here.

Heading
Your text goes here.

Heading
Your text goes here.

Heading
Your text goes here.

Heading
Your text goes here.

Heading
Your text goes here.
Your text goes here.
Your text goes here.
Your text goes here.
Your text goes here.
Your text goes here.

Heading
Your text goes here.
Your text goes here.
Your text goes here.
Your text goes here.
Your text goes here.
Your text goes here.

Heading
Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here.

Heading
Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here.

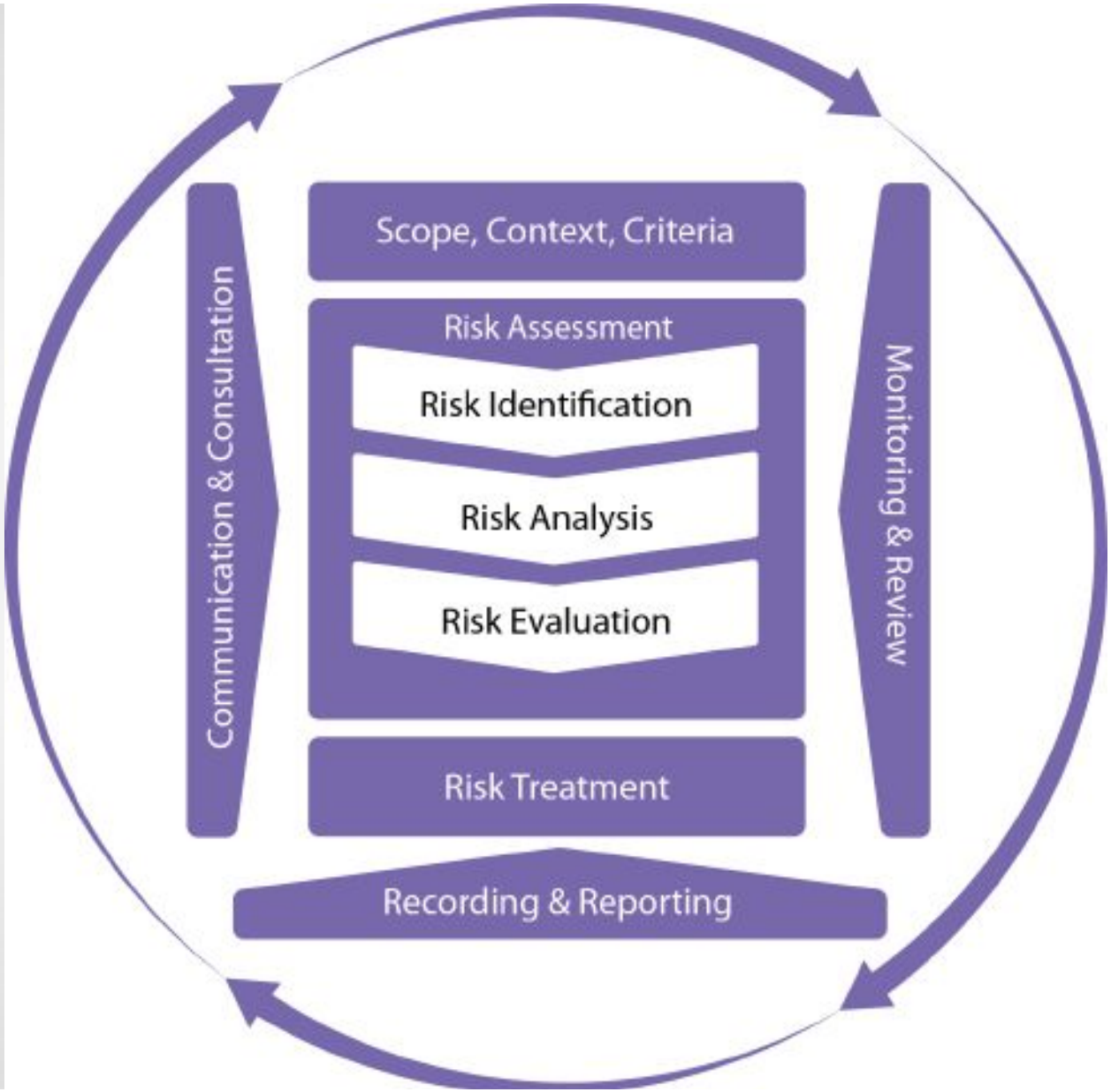
Heading
Your text goes here. Your text goes here.

Heading
Your text goes here. Your text goes here.

Enterprise Security Risk Assessment

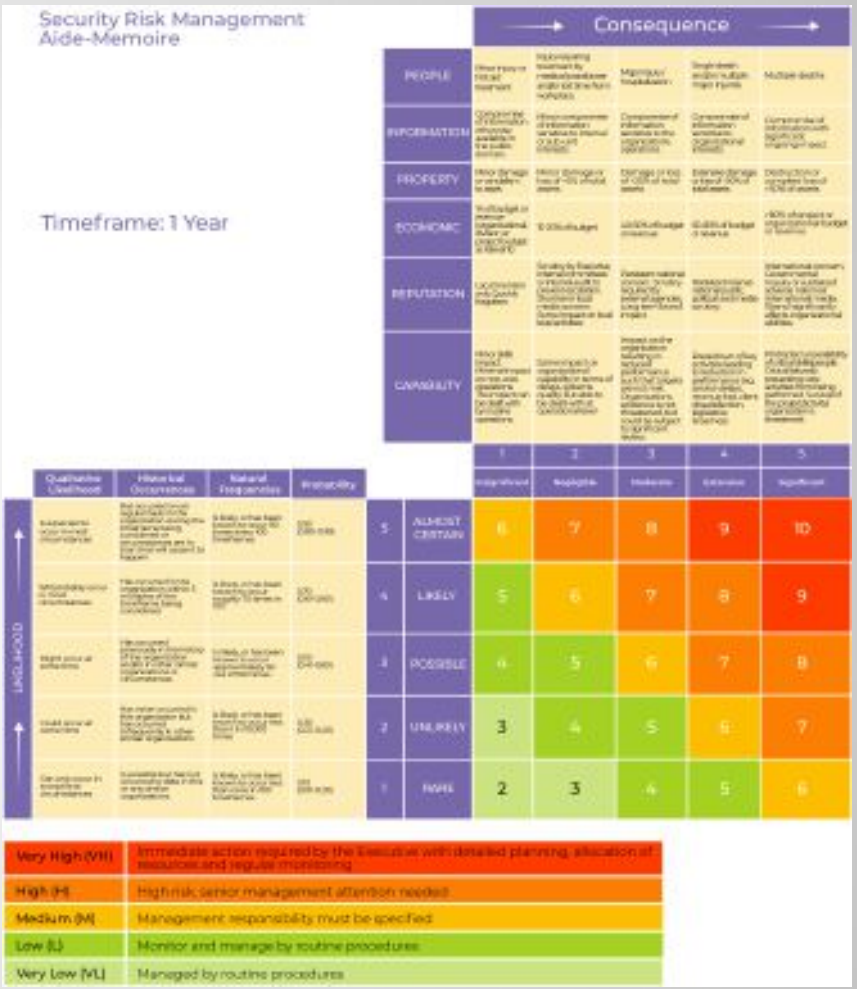
The way we do it at our company

ISO31000


Scope, Context, Criteria
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
Communication & Consultation
Monitoring & Review
Recording & Reporting

Sources
Assets (Resources)
Events
Likelihood
Consequences

RISK Matrix


Security Risk Management
Aide-Memoire
Consequence
PEOPLE
INFORMATION
PROPERTY
ECONOMIC
REPUTATION
CAPABILITY
Timeframe: 1 Year
Qualitative Likelihood
Historical Occurrences
Natural Frequencies
Probability
LIKELIHOOD
5 ALMOST CERTAIN 6 7 8 9 10
4 LIKELY 5 6 7 8 9
3 POSSIBLE 4 5 6 7 8
2 UNLIKELY 3 4 5 6 7
1 RARE 2 3 4 5 6
Very High (VH) Immediate action required by the Executive with detailed planning, allocation of resources and regular monitoring
High (H) High risk, senior management attention needed
Medium (M) Management responsibility must be specified
Low (L) Monitor and manage by routine procedures
Very Low (VL) Managed by routine procedures

Elements of a Risk Statement

- Compromise of sensitive information (*Resource*) due to untrained staff (*Source*) inadvertently posting incorrect files to a public website (*Event*) causing competitive disadvantage and resulting in financial losses (*Consequence*).

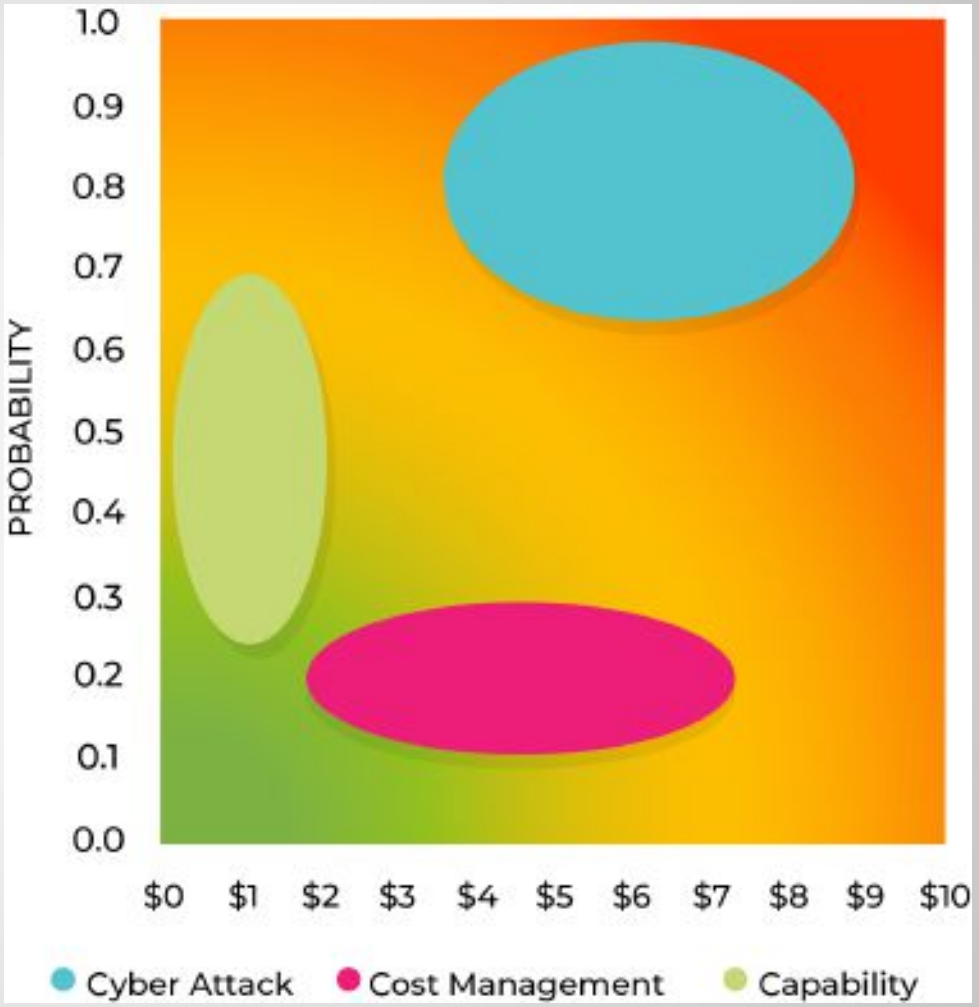
Risk ID	Risk No. 5
Event	Espionage
Source	Competitors
Resource	Information
Consequence	Financial
Cons. Rating	Moderate
L'hood Rating	Likely
RISK RATING	HIGH

SOURCE	EVENT	RESOURCE	CONSEQUENCE
Competitors	Espionage	Information	Financial
Organized Criminals	Espionage	Information	Financial
Untrained Staff	Unauthorized Release	Information	Reputation
Organized Criminals	Theft	Equipment	Capability
Petty Criminals	Theft	Equipment	Financial

Risk Analysis

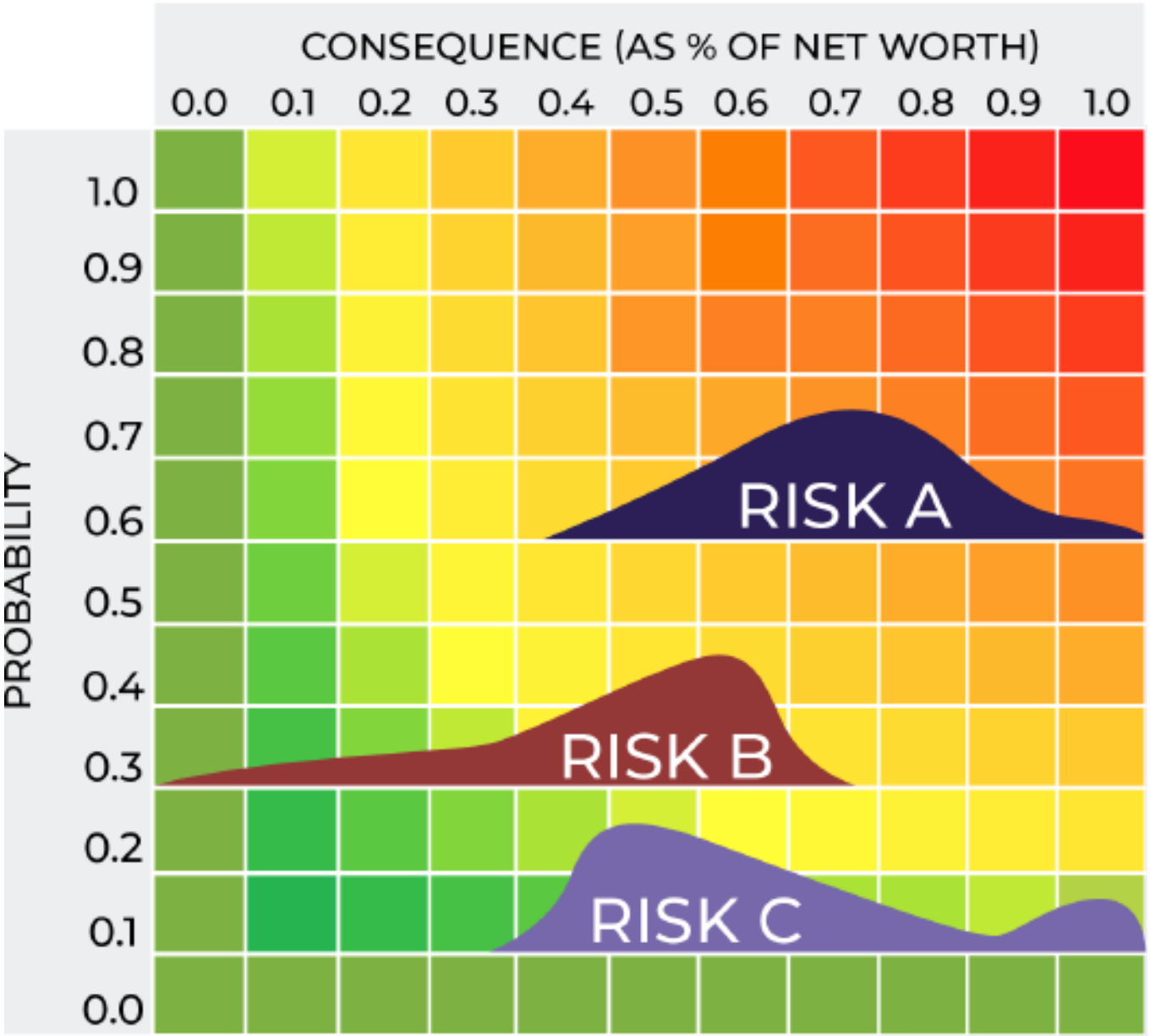
- Limitations of matrices
- Limitations of quantitative analysis
- Causation and connectedness

BUBBLE CHART



Risk Matrices

- Risk is not a 'point value' on a matrix
- Probability distribution curve
- Outliers

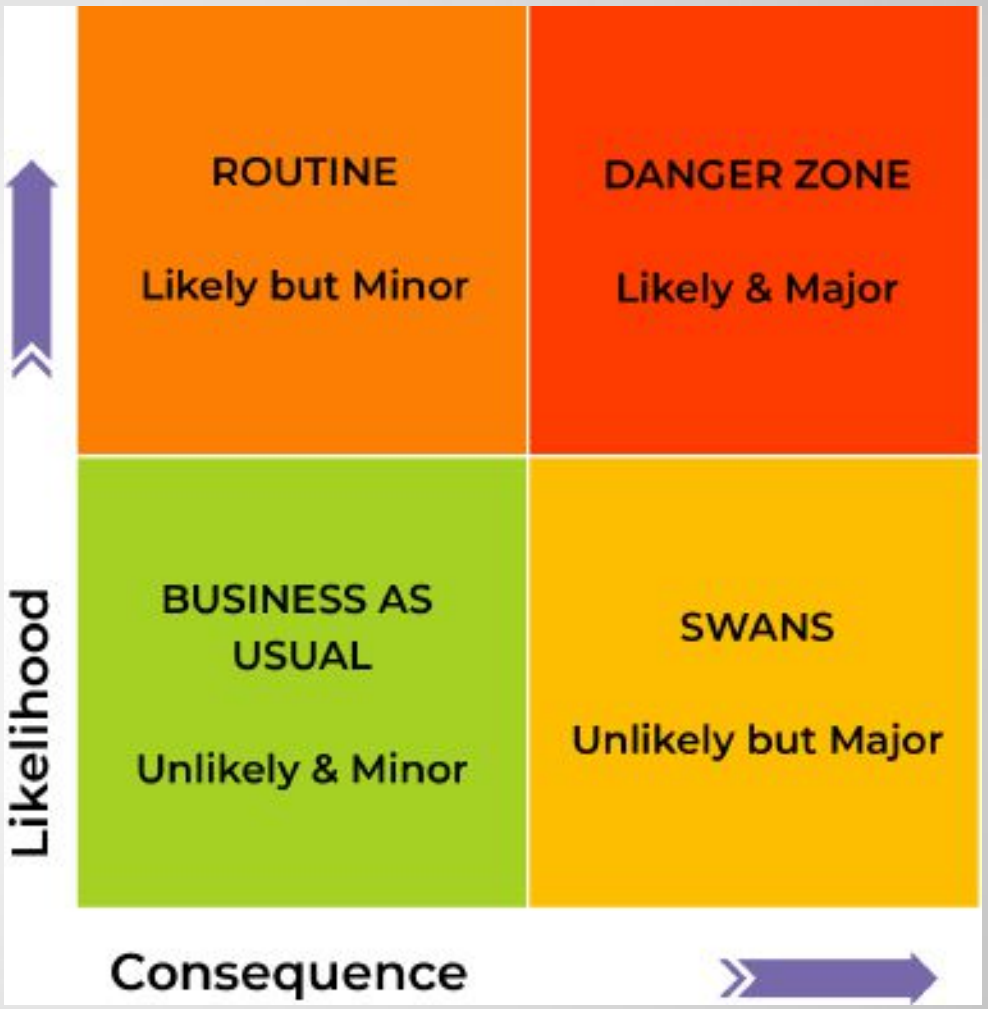


EMV

- Expected
- Monetary
- Value

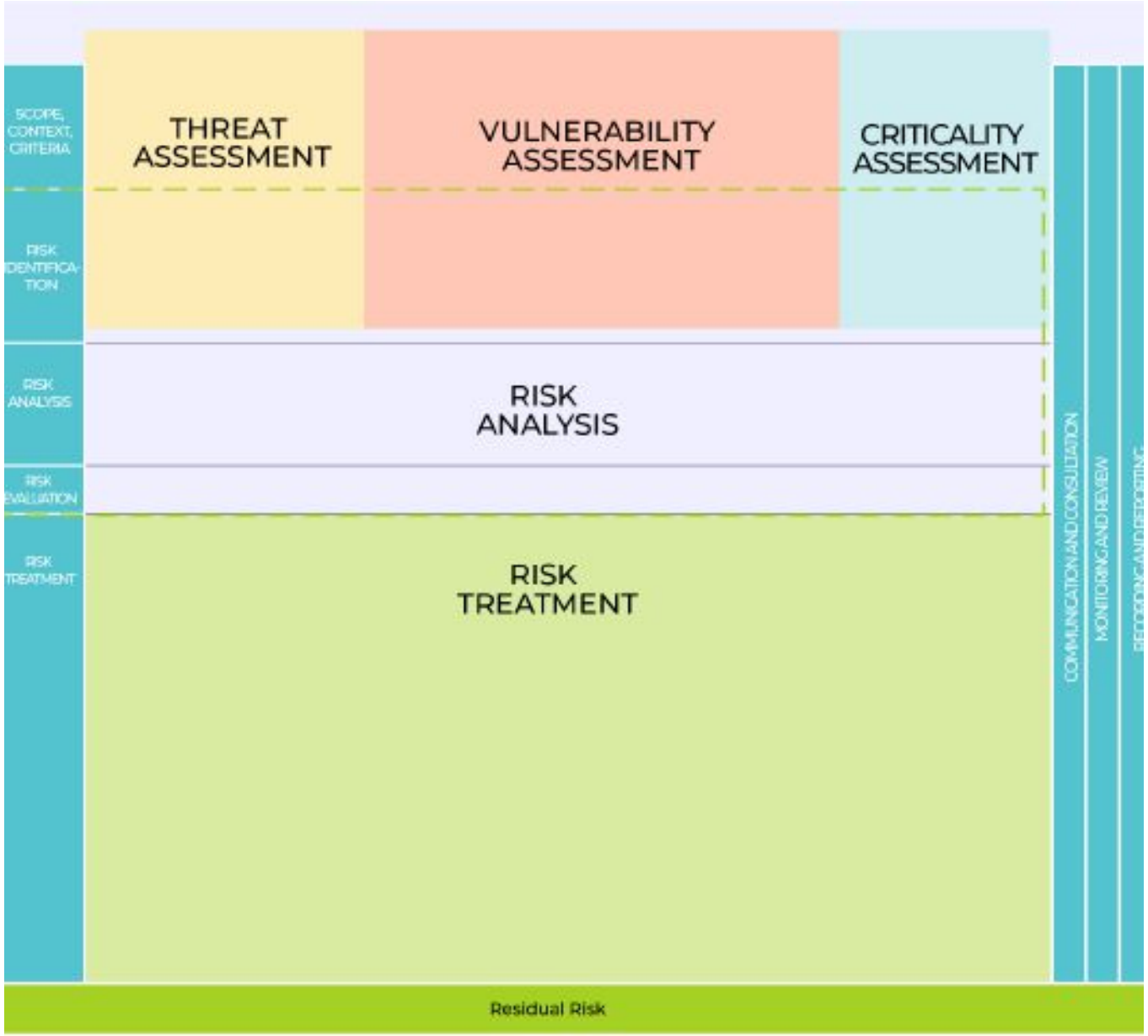
A) 30% chance of $1,000,000 loss ($300,000)
B) 20% chance of $500,000 loss ($100,000)
C) 50% chance of $100,000 loss ($50,000)

STROUD Matrix

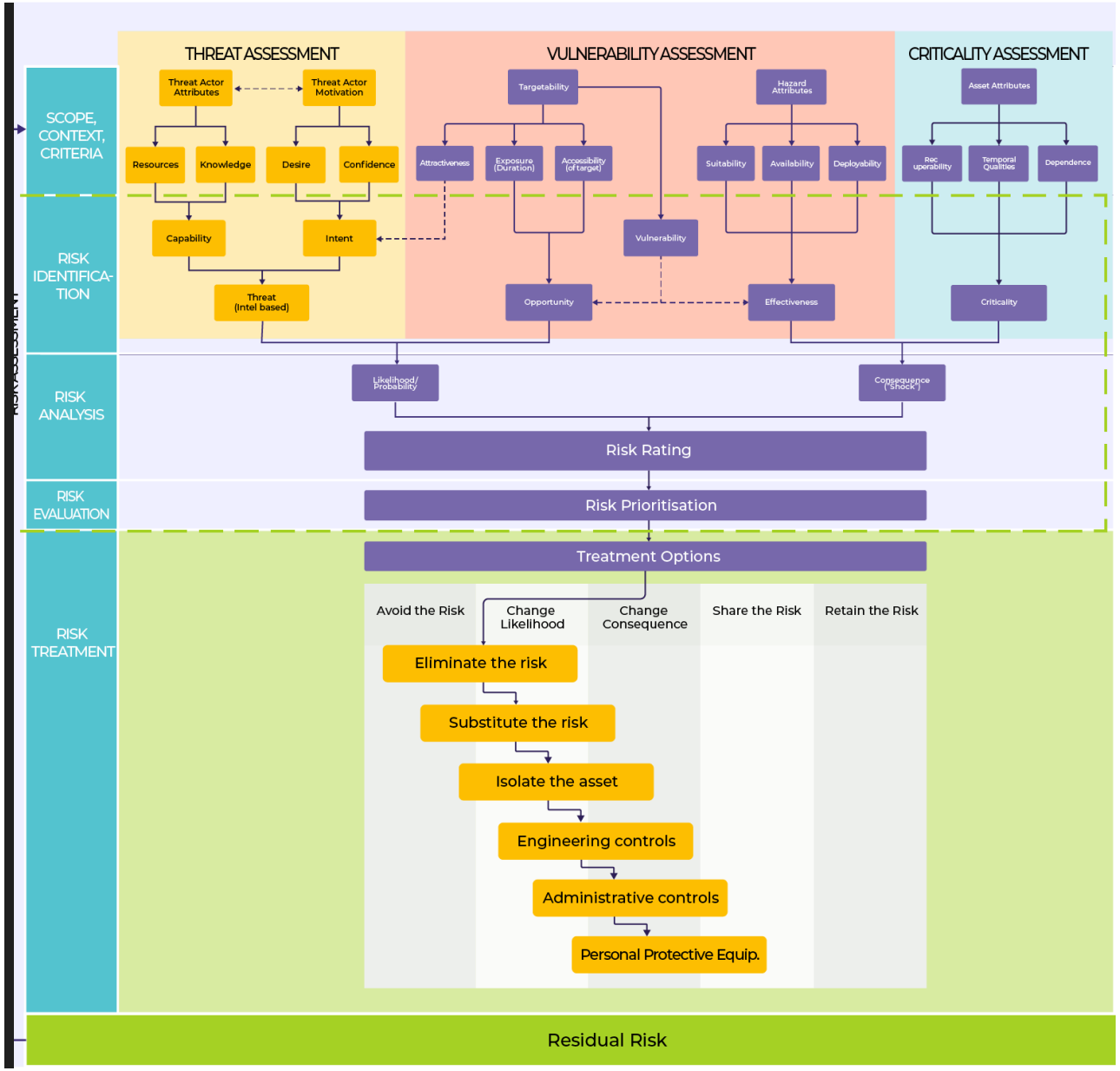


ISO3100

- The big picture for enterprise security risk assessment



SRMBOK SRA Model



External Context

Internal Context

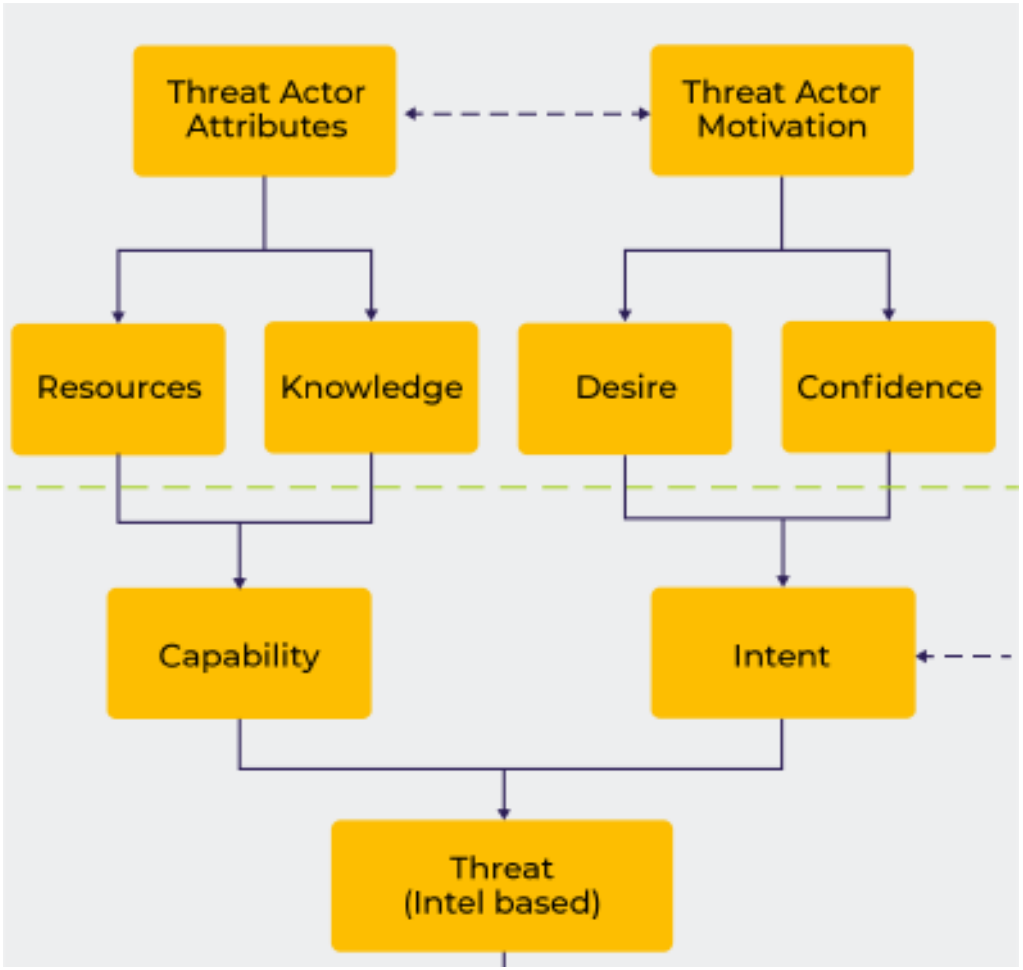
Source: Security Risk Management Aide-Mémoire
www.srmam.com

Threat

- Intent
- Capability

CAPABILITY	None	Little	Expressed	Determined	Dedicated
Extensive	S	H	E	E	E
Advanced	S	S	H	E	E
Developed	M	S	S	H	E
Moderate	L	M	S	S	H
Low	L	L	M	S	S

Low
Moderate
Significant
High
Extreme



Threat

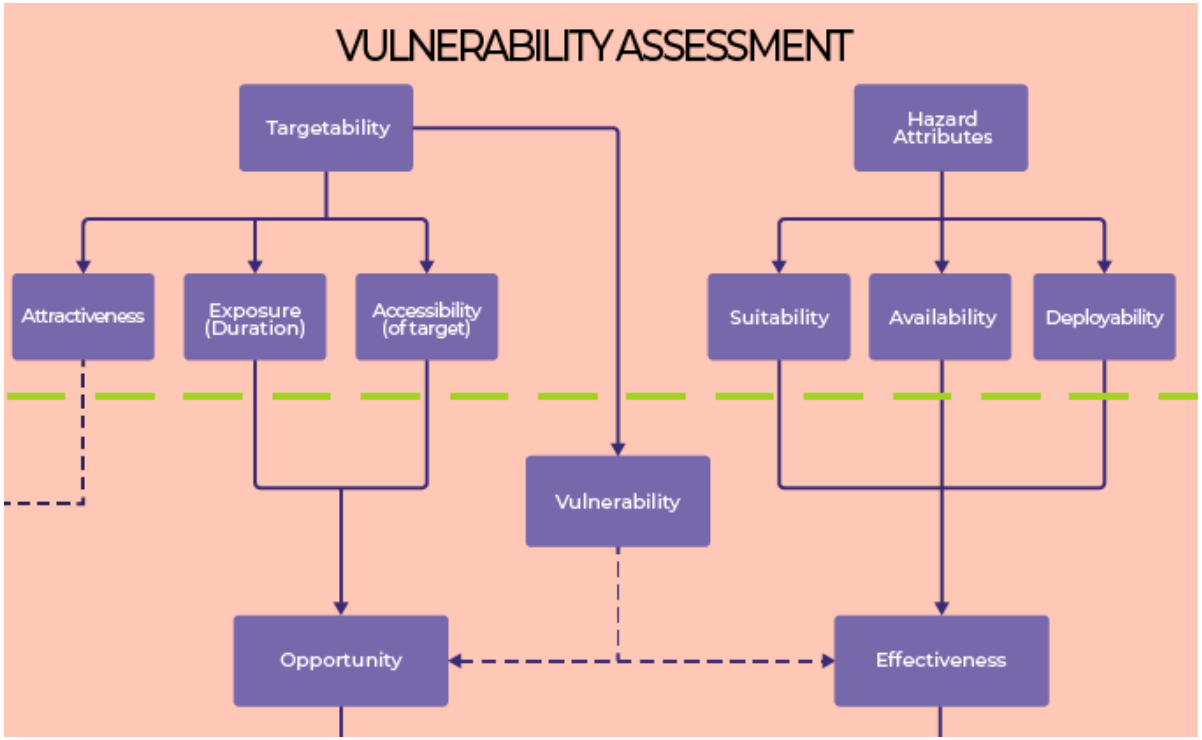
- Modelling the inputs
- Attributes
- Motvations
- Threat level

Threat Assessment

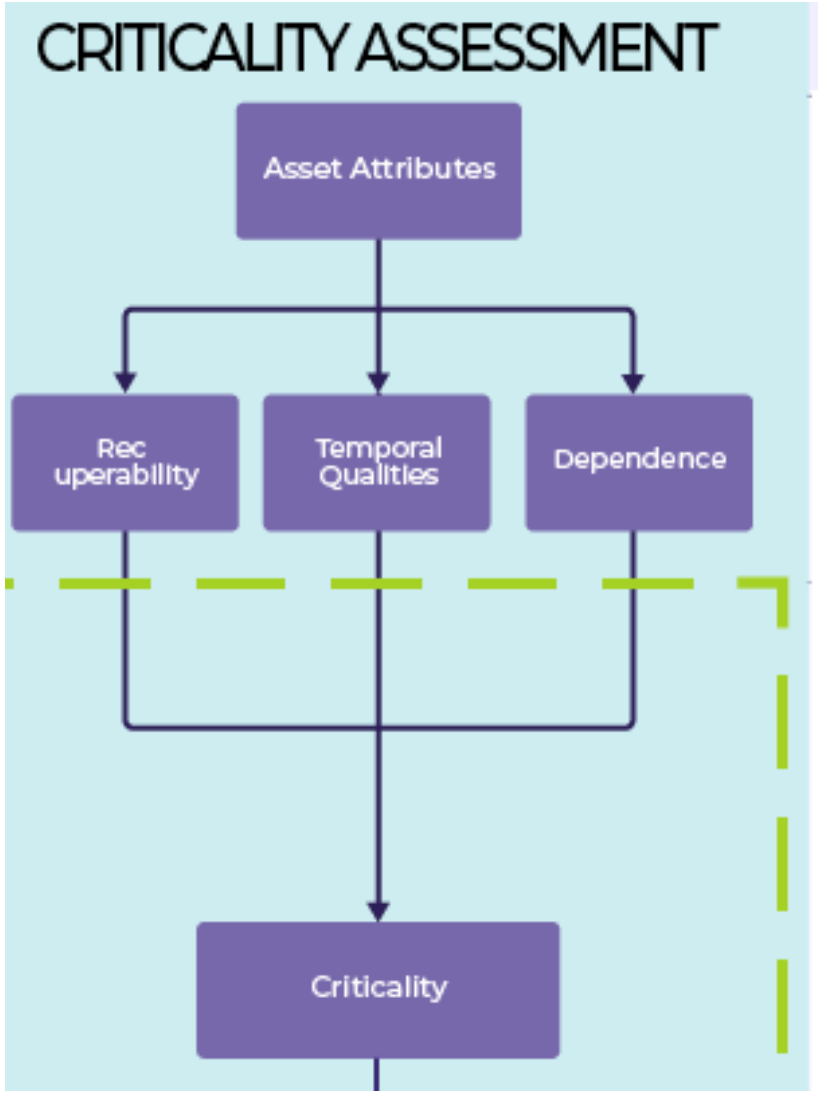
- Capability
  - Resources
  - Knowledge
- Intent
  - Desire
  - Confidence

ID Category Threat Actors		T1
		Foreign Intelligence Services
		State Sponsored Commercial Espionage Groups
Attributes	Resources	These groups are generally highly resourced and well funded.
		5. Fully funded and resourced.
	Knowledge	Significant actors in this arena are usually extensively trained and have access to reliable intelligence.
		5. Highly skilled and comprehensively trained.
	CAPABILITY	A very capable and well prepared adversary with high tolerance for risk but with almost always operating covertly.
		5
Motivation	Desire	Aggressively seeking classified or related intelligence via any and all means.
		4. High degree of desire with limited room for compromise and potential to use extreme measures.
	Confidence	This group have a high level of confidence that over a sufficiently long time frame th will be successful in at least a significant number of their endeavours.
		4. Threat actor competence and capabilities are such that they have high expectations of achieving a successful attack.
	INTENT	Economic advantage over our Organization or on the world stage.
		4
THREAT		4.5

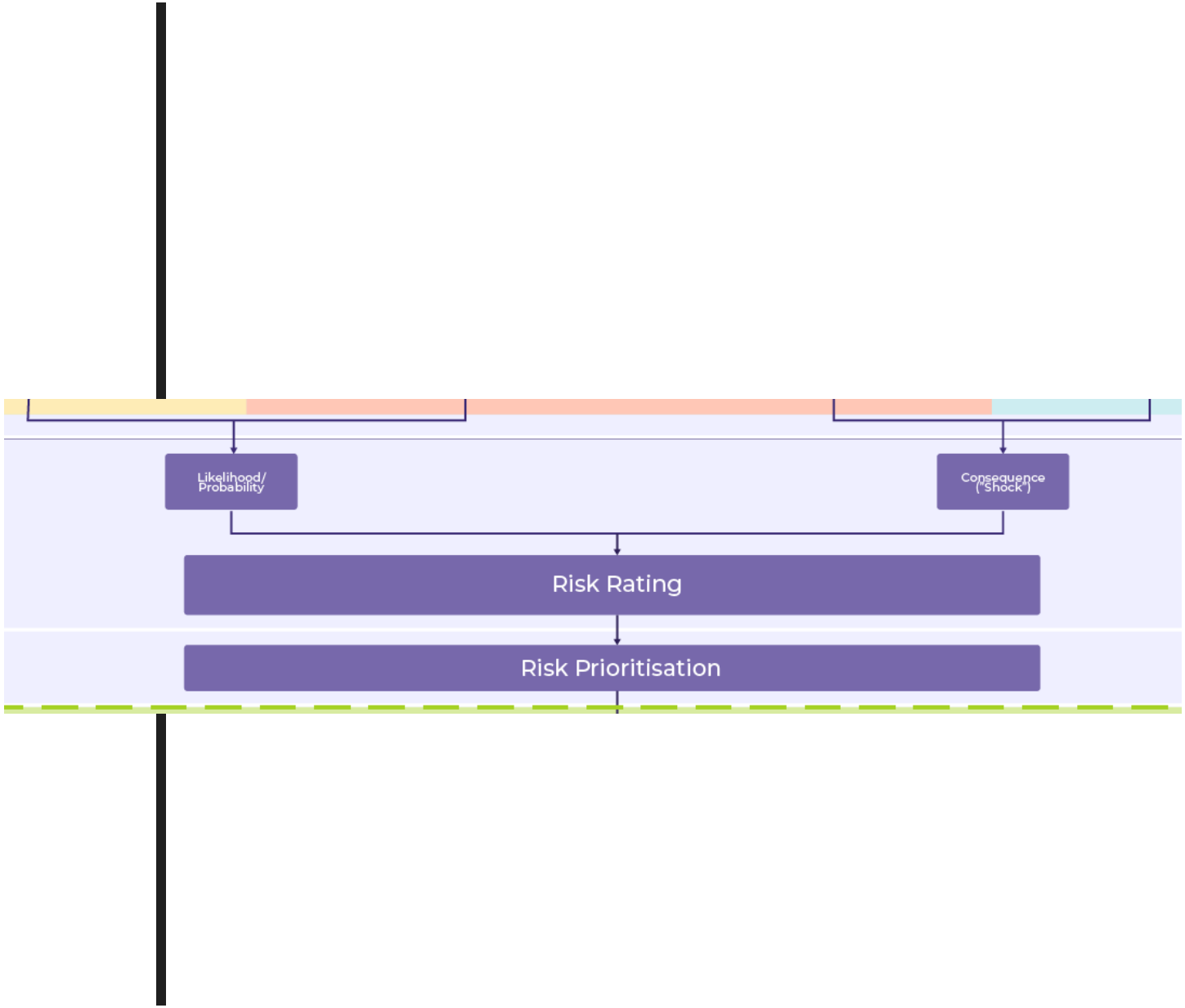
Vulnerability



Criticality



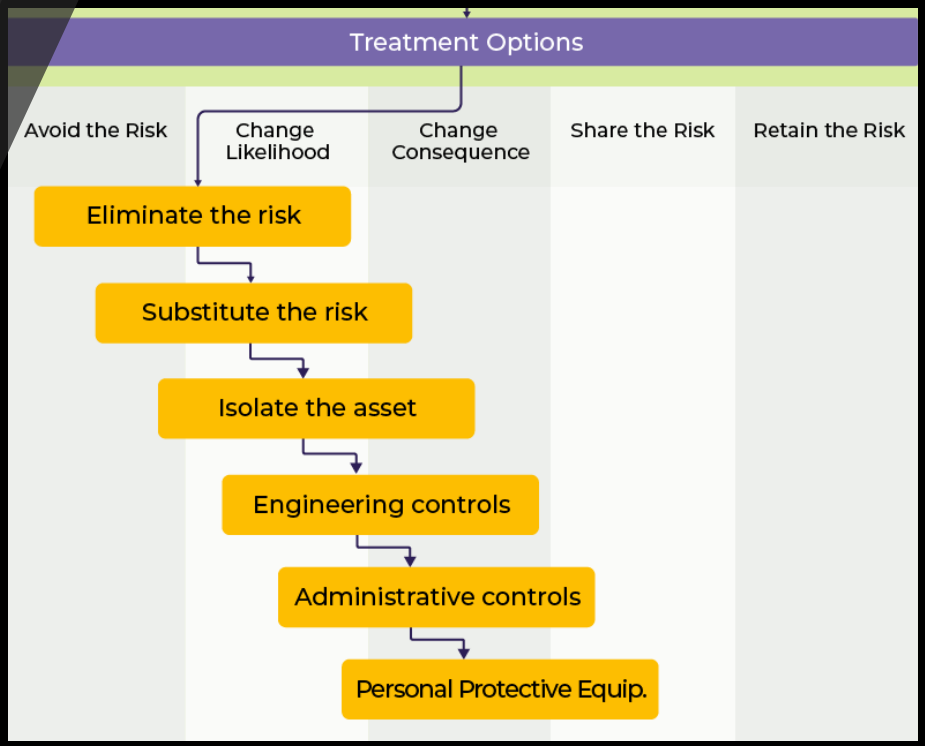
Risk


Likelihood/ Probability
Consequence ("Shock")
Risk Rating
Risk Prioritisation

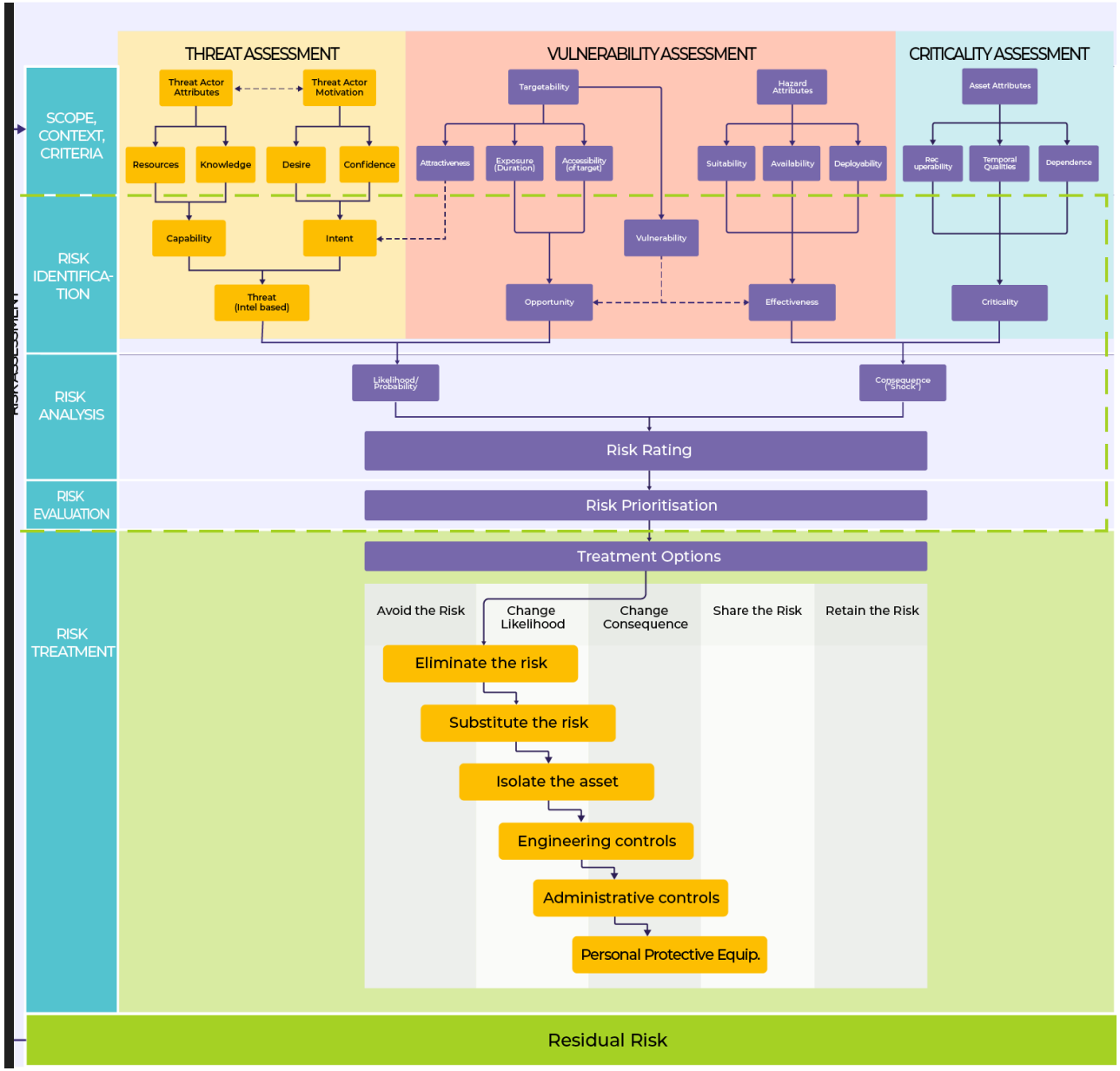
Treatment

- Avoid
- Change Likelihood
- Change Consequences
- Share the risk
- Retain the risk

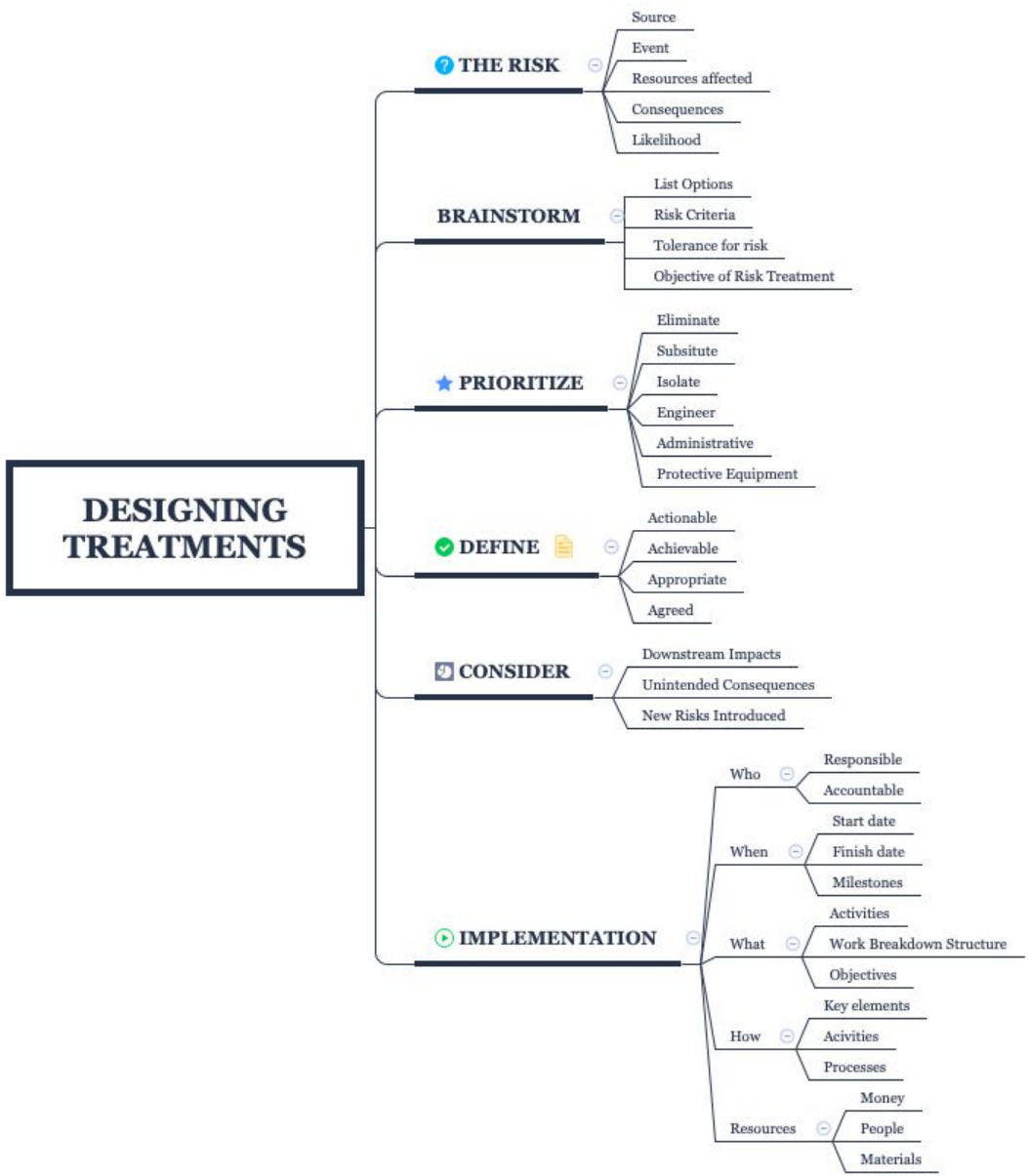
- ESIEAP



SRMBOK & ISO31000 Security Risk Assessment Model



Treatments


DESIGNING TREATMENTS
THE RISK
Source
Event
Resources affected
Consequences
Likelihood
BRAINSTORM
List Options
Risk Criteria
Tolerance for risk
Objective of Risk Treatment
PRIORITIZE
Eliminate
Subsitute
Isolate
Engineer
Administrative
Protective Equipment
DEFINE
Actionable
Achievable
Appropriate
Agreed
CONSIDER
Downstream Impacts
Unintended Consequences
New Risks Introduced
IMPLEMENTATION
Who
Responsible
Accountable
When
Start date
Finish date
Milestones
What
Activities
Work Breakdown Structure
Objectives
How
Key elements
Acivities
Processes
Resources
Money
People
Materials

DESIGNING TREATMENTS

- **THE RISK**
  - Source
  - Event
  - Resources affected
  - Consequences
  - Likelihood
- **BRAINSTORM**
  - List Options
  - Risk Criteria
  - Tolerance for risk
  - Objective of Risk Treatment
- **PRIORITIZE**
  - Eliminate
  - Subsitute
  - Isolate
  - Engineer
  - Administrative
  - Protective Equipment
- **DEFINE**
  - Actionable
  - Achievable
  - Appropriate
  - Agreed
- Downstream Impacts

DESIGNING TREATMENTS

- **DEFINE**
  - Actionable
  - Achievable
  - Appropriate
  - Agreed
- **CONSIDER**
  - Downstream Impacts
  - Unintended Consequences
  - New Risks Introduced
- **IMPLEMENTATION**
  - Who
    - Responsible
    - Accountable
  - When
    - Start date
    - Finish date
    - Milestones
  - What
    - Activities
    - Work Breakdown Structure
    - Objectives
  - How
    - Key elements
    - Acivities
    - Processes
  - Resources
    - Money
    - People
    - Materials

One Page Per Treatment Security Plan

DSP10-8. Security Training Program – Comprehensive

Description	Review and update competency based security training programs
Actions:	Implement global Training & Education Program - to inform staff of new or revised Security Policies (e.g. new policy documents, policy structure and format, email & multi-media policies, staff surveys, etc) to be implemented as a result of the ESRA, across all JTC Groups.
Achieved when:	Endorsed and promulgated by CEO
Risks Treated:	All security risks. <INSERT DATA FROM ESRA20>
Agreed by:	CEO and SGC.
Scope:	All JT.com assets and activities
Schedule:	2018-2019
Resources:	Internal labour plus $800,000 external labour plus significant staffing implications
Quality:	Endorsement by relevant external subject matter experts (eg: XYZ, Super Spies, No Such Agency, etc)
Actionee:	CEO
Implementation Parameters	Australian Quality Training Framework (AQTF) guidelines.

One Page Per Treatment Security Plan

Description:

Actions:

Achieved when:

Risks Treated:

Agreed by:

Scope:

Schedule:

Resources:

Quality:

Actionee:

Implementation Parameters:

The Weakest Link = Swiss Cheese

Equally important is the causal chain

Unintended consequences

Downstream events


ESCALATION FACTORS
ESCALATION FACTORS
SOURCE
HAZARD
THREATS
RISK EVENT
EFFECT
CONSEQUENCE
ESCALATION CONTROLS
CONSEQUENCE CONTROLS
LIKELIHOOD CONTROLS
ESCALATION CONTROLS
LIKELIHOOD MANAGEMENT
CONSEQUENCE MANAGEMENT

Bow-Tie Table

Overview	A summary of hazards or opportunities which have the potential to impact objectives. e.g., To effect health and safety, property, products, the environment, production quotas, or profit.
Description	A description of the Risk(s) or category of Risks that are of particular interest.
Scope	The primary locations or other relevant scoping statements if relevant.
Sources	Something with the potential to release a **'Hazard'** or **'Opportunity'** and to cause an **'Event'**.
Controls	A protective measure reduces the likelihood of **'Sources'** creating a risk event. Controls might be physical, procedural or any form which is relevant to the organization and the risk(s) being analyzed.
Likelihood Escalation Factors	Conditions that modify risk likelihood due to unintended modification of **Controls** (e.g., cuts to maintenance budgets, loss of trained staff)
Likelihood Escalation Controls	Measures to manage **Likelihood Escalation Factors** effect on **Likelihood Controls**. These may be hardware (e.g., Firewalls, Handrails), but will generally be procedural barriers (e.g., audit and inspection of the design).
Event(s)	The occurrence or change in circumstances associated with the source(s) of risk.
Consequence Controls	Technical, operational, procedural or organizational measures that modify **Consequences** arising from an **Event**.
Consequence Escalation Factors	Conditions that lead to changes in risk levels associated with changes in **Consequence Controls**.
Consequence Escalation Controls	Measures to modify **Consequence Escalation Factors** to support the achievement of objectives. These may be hardware (e.g., signage and emergency lighting directing personnel to emergency equipment) or procedural barriers (e.g., inspection, testing, and maintenance of safety equipment).
Consequences	Outcome of an **Event** which can effect Objectives.

Thanks

julian@juliantalbot.com