(ISC)²® | SECURITY CONGRESS

EMPOWER

a Safer, More Secure Cyber World

Congress.isc2.org | #ISC2Congress

Enterprise Security Risk Assessment (ESRA)

Julian Talbot CISSP FISRM

Risk Assessment

WAGNER

BOGSAT

WTF

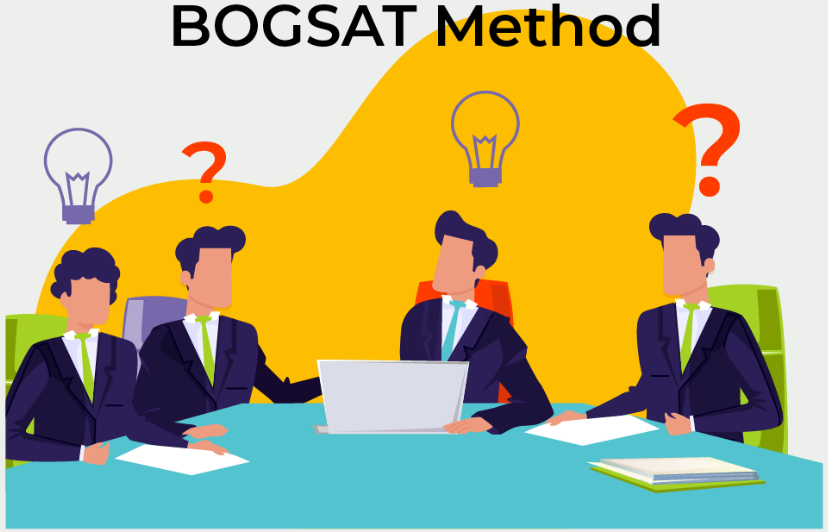
MS EXCEL & A RISK MATRIX

WTF

WAGNER Method

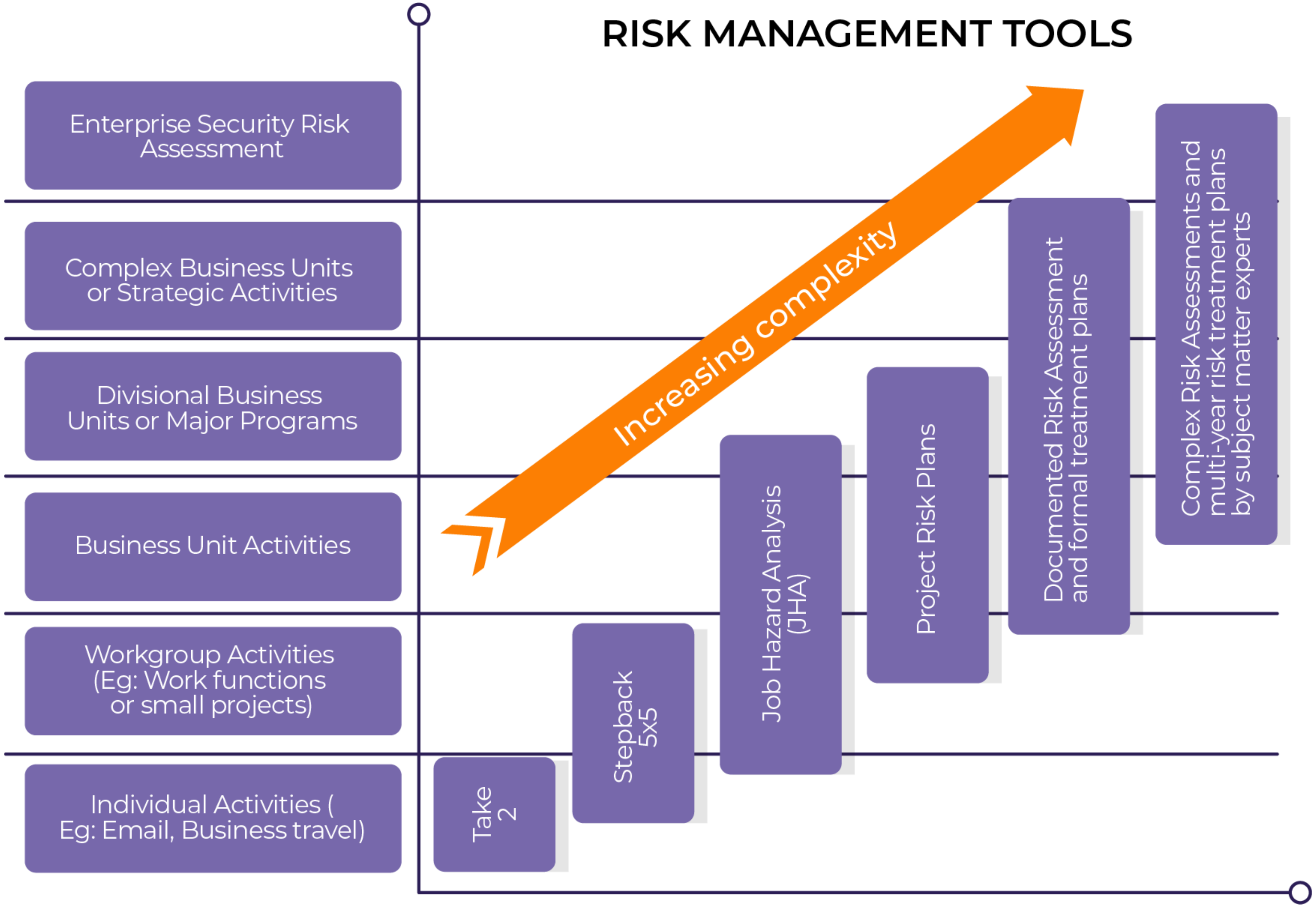
Wild
Assed
Guess
Not
Easily
Refutable

BOGSAT Method



Bunch
Of
Guys
Sitting
Around
Talking

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

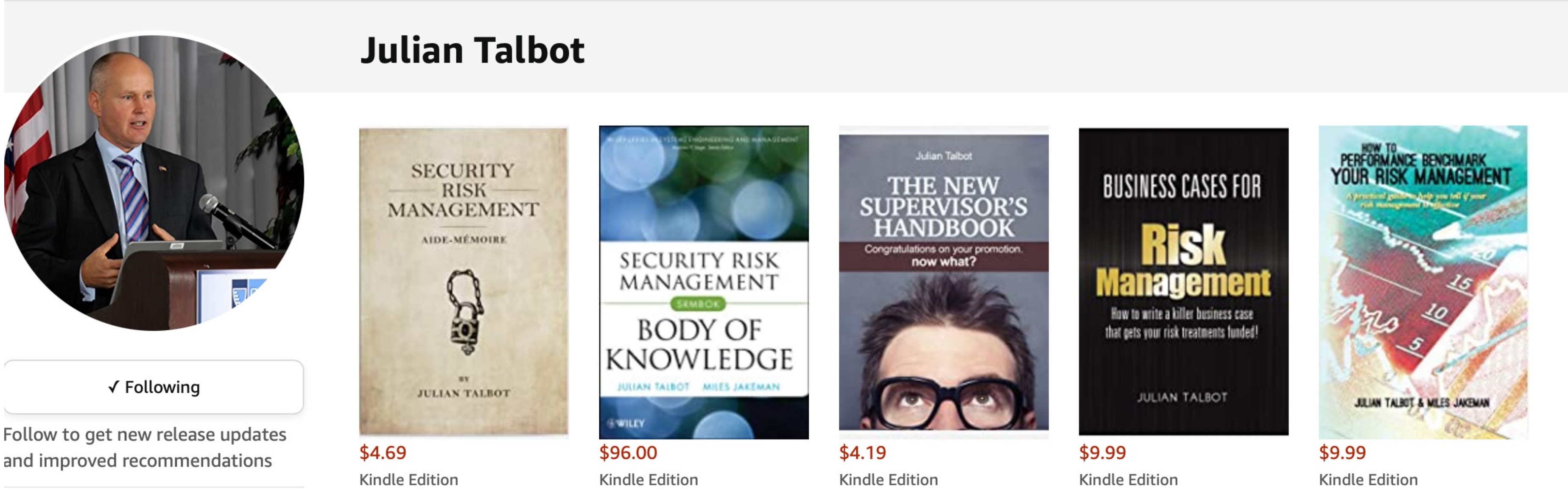
Job Hazard Analysis (JHA)

Project Risk Plans

Documented Risk Assessment and formal treatment plans

Complex Risk Assessments and multi-year risk treatment plans by subject matter experts

A short history of …



Julian Talbot

✓ Following

Follow to get new release updates and improved recommendations

$4.69	$96.00	$4.19	$9.99	$9.99
Kindle Edition	Kindle Edition	Kindle Edition	Kindle Edition	Kindle Edition

SECURITY RISK MANAGEMENT
AIDE-MÉMOIRE
BY JULIAN TALBOT
SECURITY RISK MANAGEMENT
SRMBOK
BODY OF KNOWLEDGE
JULIAN TALBOT MILES JAKEMAN
WILEY
Julian Talbot
THE NEW SUPERVISOR'S HANDBOOK
Congratulations on your promotion. now what?
BUSINESS CASES FOR
Risk Management
How to write a killer business case that gets your risk treatments funded!
JULIAN TALBOT
HOW TO PERFORMANCE BENCHMARK YOUR RISK MANAGEMENT
JULIAN TALBOT & MILES JAKEMAN

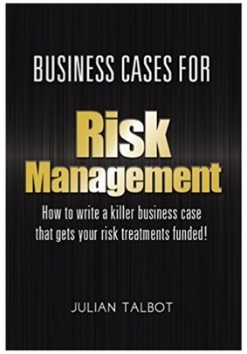
Julian Talbot CISSP F.ISRM

SECTARA™

www.juliantalbot.com

SRMBOK

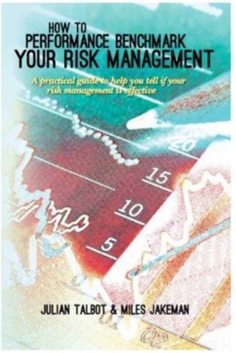
Security Risk Management Body Of Knowledge


BUSINESS CASES FOR

Risk Management

How to write a killer business case that gets your risk treatments funded!

JULIAN TALBOT


HOW TO PERFORMANCE BENCHMARK YOUR RISK MANAGEMENT

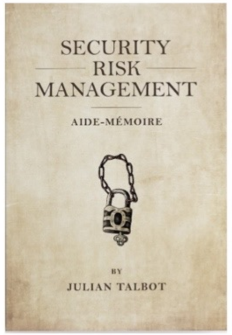
A practical guide to help you tell if your risk management is effective

JULIAN TALBOT & MILES JAKEMAN

Julian Talbot

THE NEW SUPERVISOR'S HANDBOOK

Congratulations on your promotion. now what?


SECURITY RISK MANAGEMENT

AIDE-MÉMOIRE

BY

JULIAN TALBOT

SECTARA™

srmbok.fyi.to/ISC2

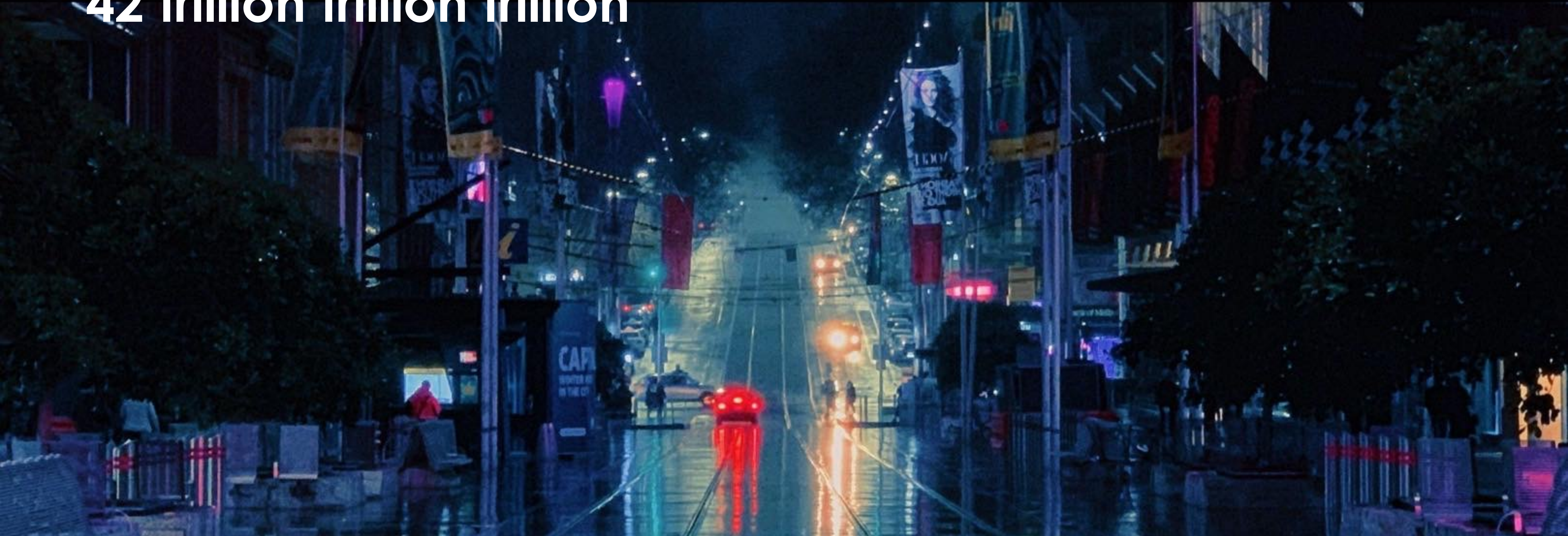
Why

Enterprise Security Risk Assessments

2^128 = 340,282,366,920,938,463,463,374,607,431,768,211,456

In practical terms 'only'
2^125 or 4.2 x 10^37 (42 undecillion) 'things' can connect

42 trillion trillion trillion



Cybersecurity = Convergence

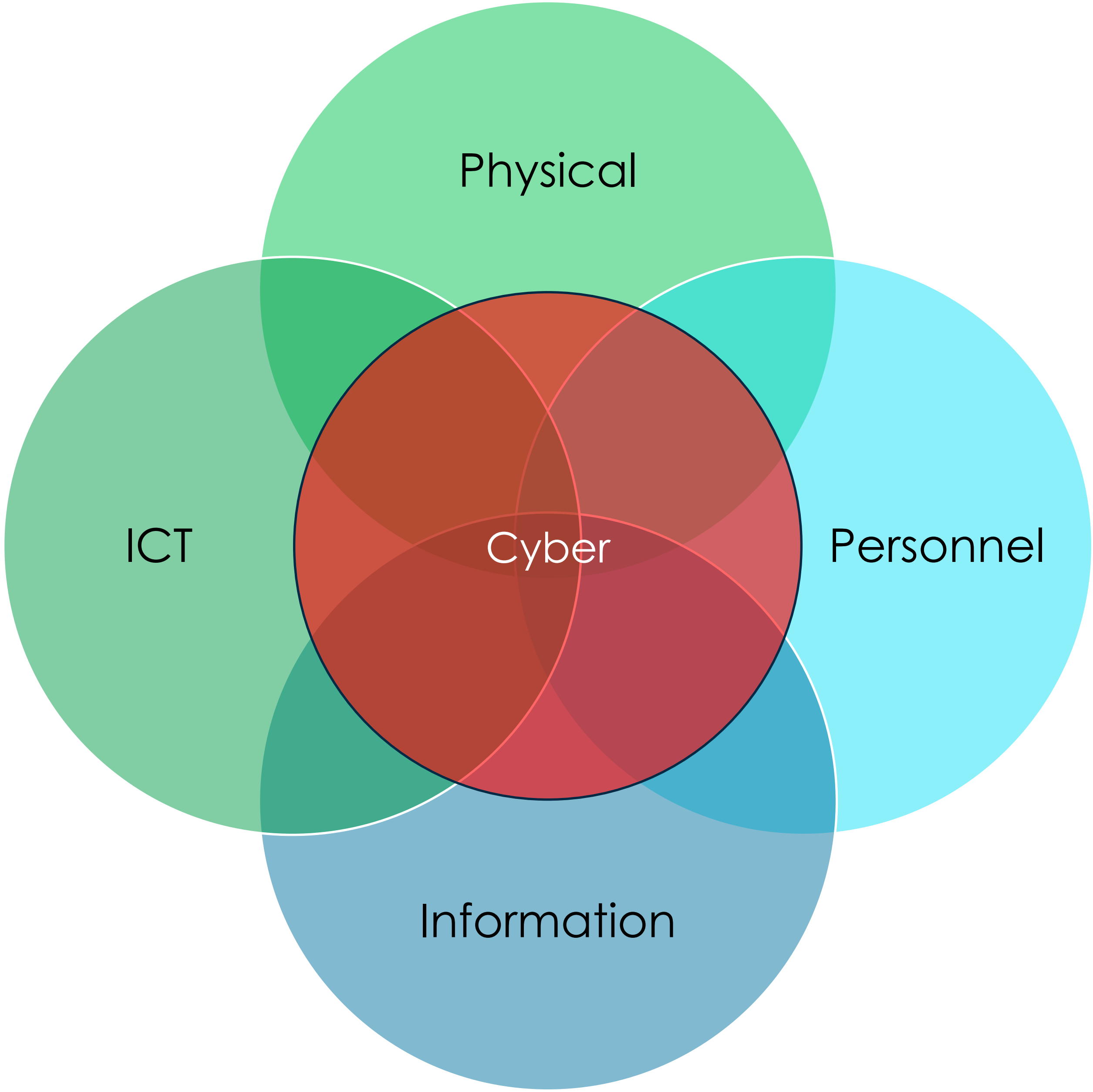
Artificial intelligence

Nanotechnology

Genetics

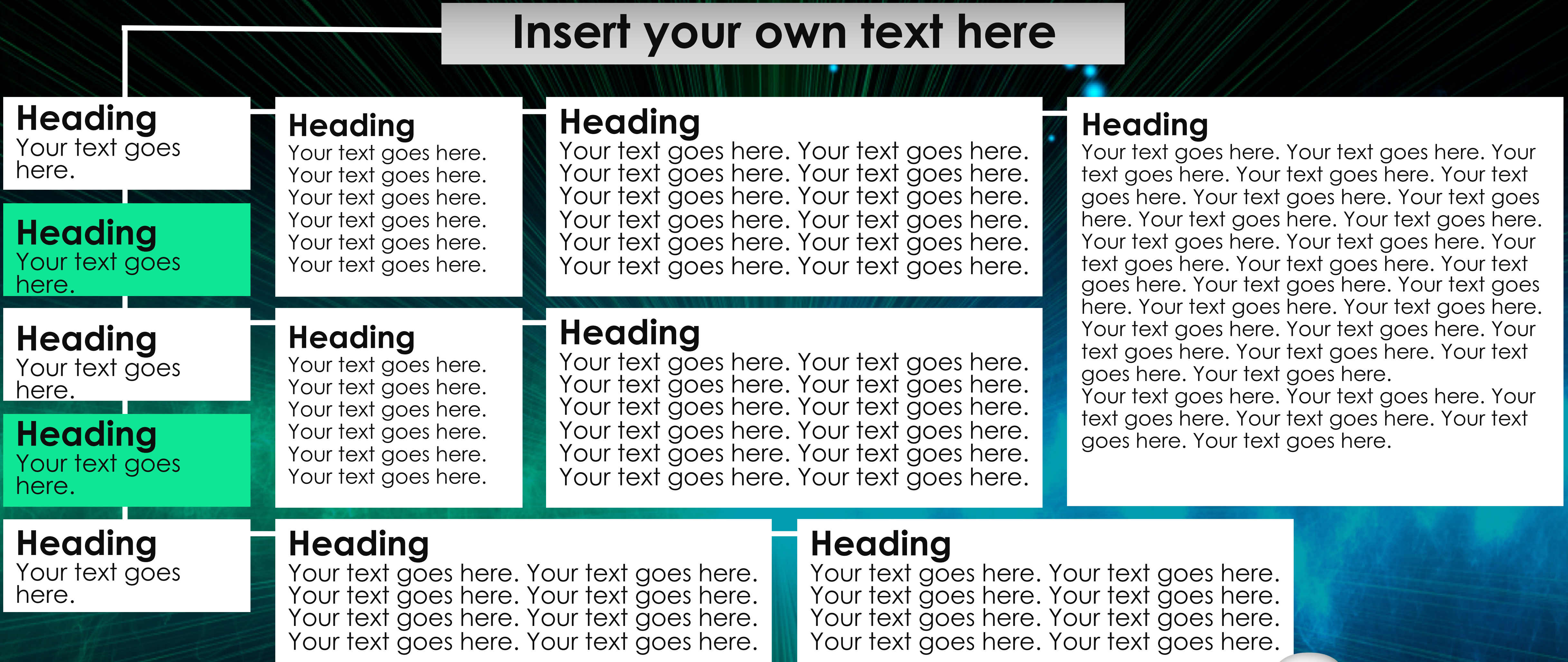
Robotics

Cybersecurity



What

Enterprise Security Risk Assessments



Insert your own text 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. 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. 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.

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. 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.

Heading
Your text goes here.

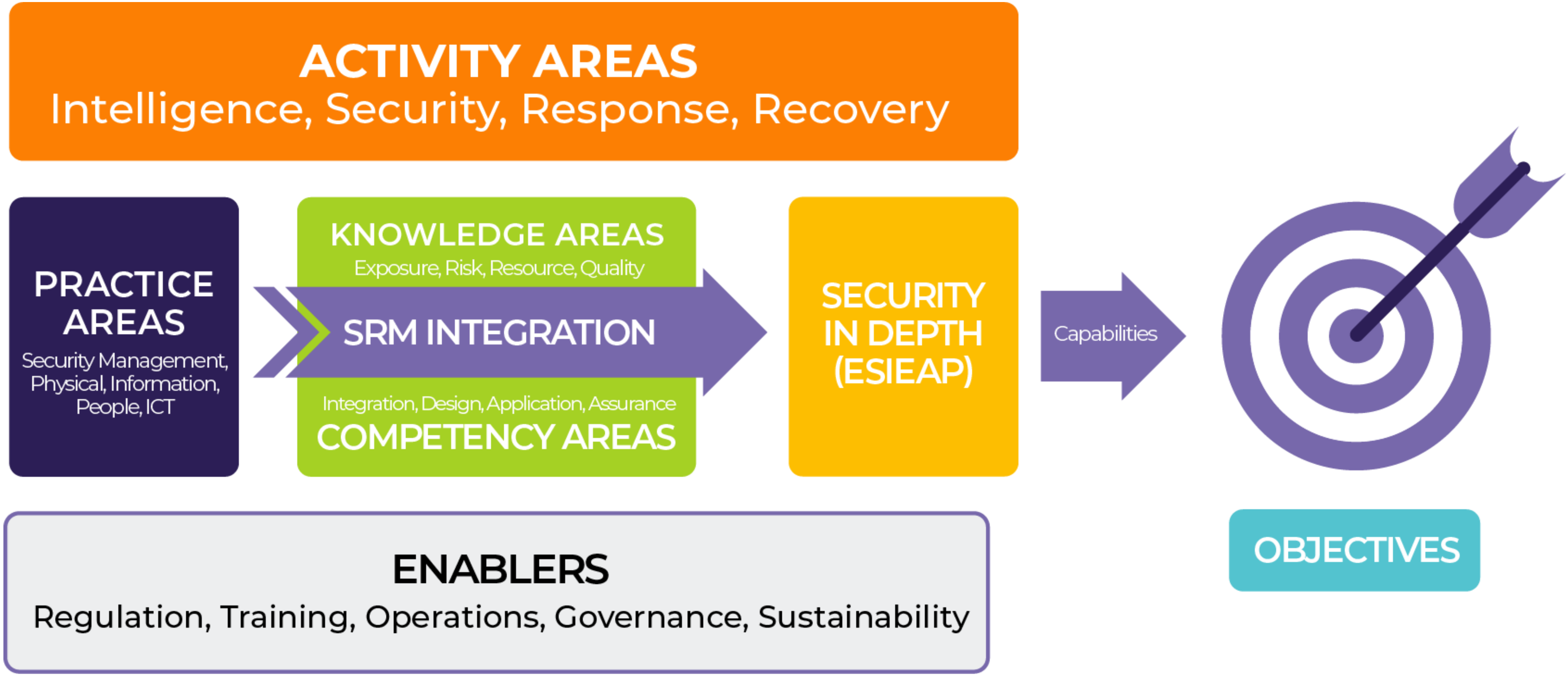
Heading
Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here. Your text goes here.

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.

Enterprise Security Risk Assessment

The way we do it at our company

Risk management = Future management



ACTIVITY AREAS

Intelligence, Security, Response, Recovery

PRACTICE AREAS

Security Management, Physical, Information, People, ICT

KNOWLEDGE AREAS

Exposure, Risk, Resource, Quality

SRM INTEGRATION

Integration, Design, Application, Assurance

COMPETENCY AREAS

SECURITY IN DEPTH (ESIEAP)

Capabilities

OBJECTIVES

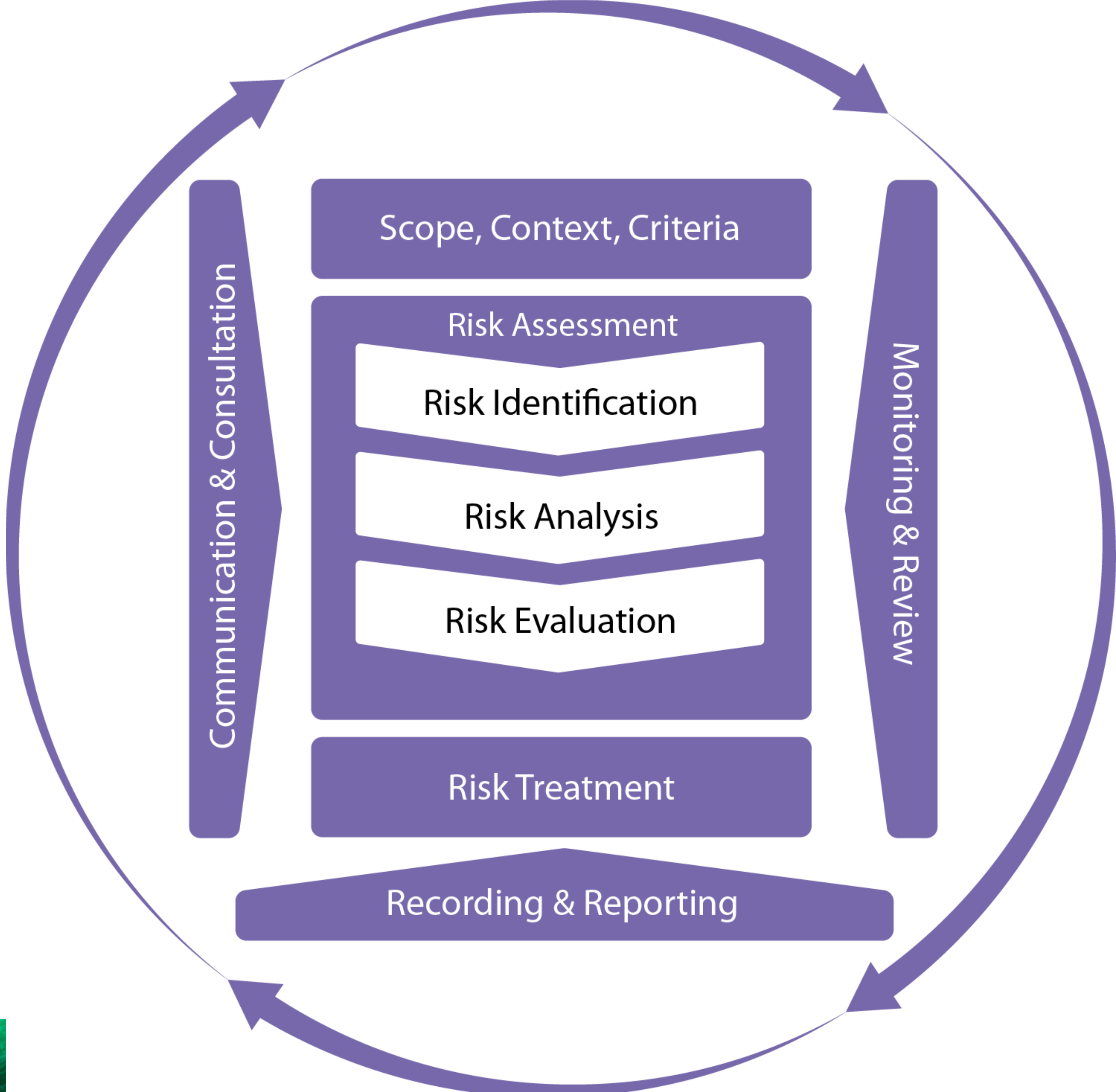
ENABLERS

Regulation, Training, Operations, Governance, Sustainability

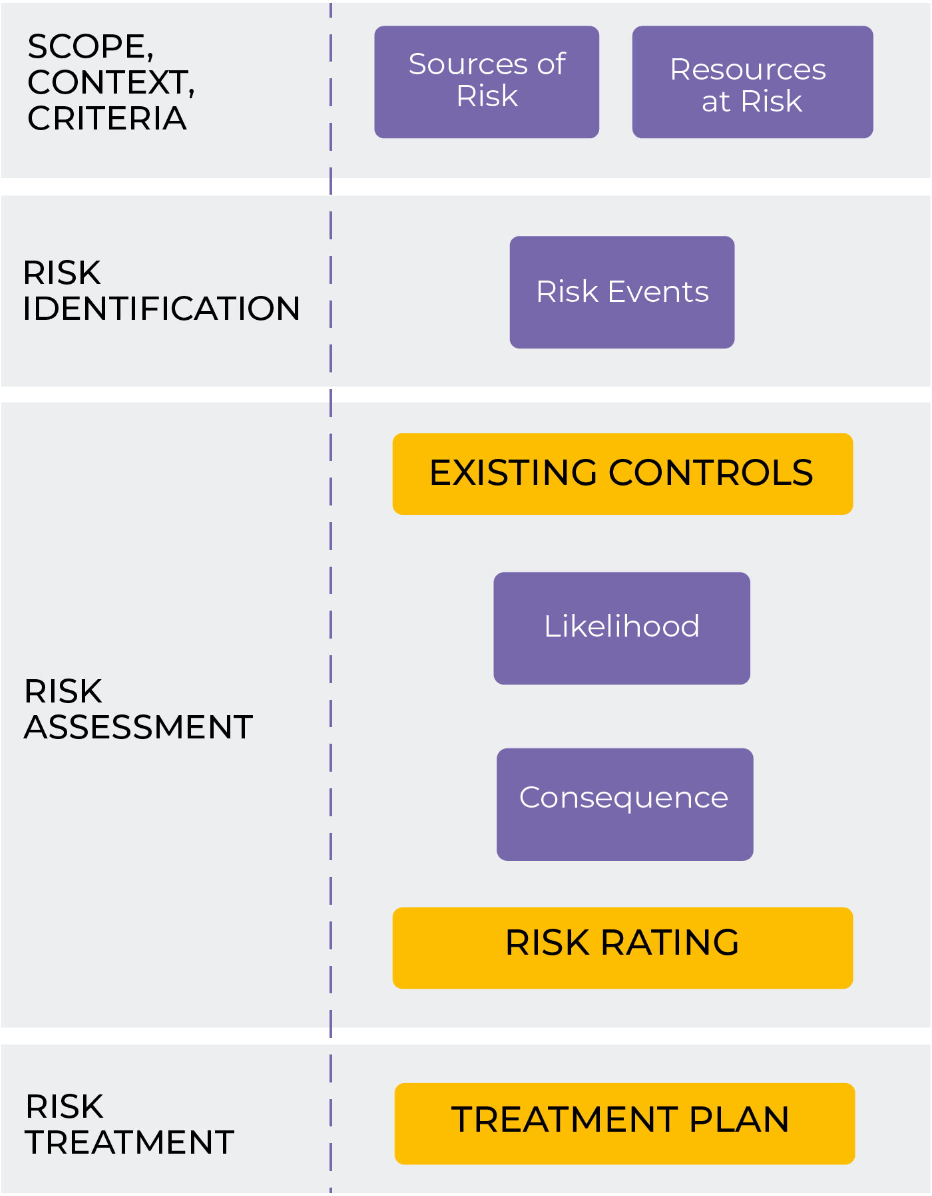
How

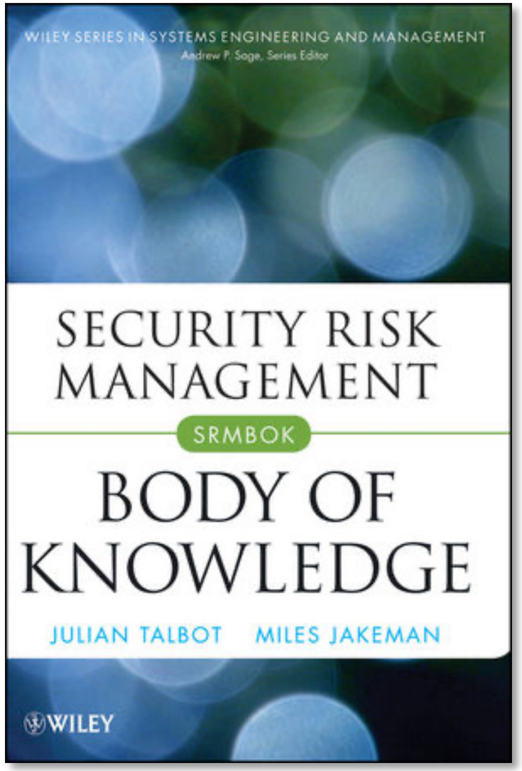
Enterprise Security Risk Assessments

ISO31000


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

Sources
Assets (Resources)
Events
Likelihood
Consequences





WILEY SERIES IN SYSTEMS ENGINEERING AND MANAGEMENT
Andrew P. Sage, Series Editor

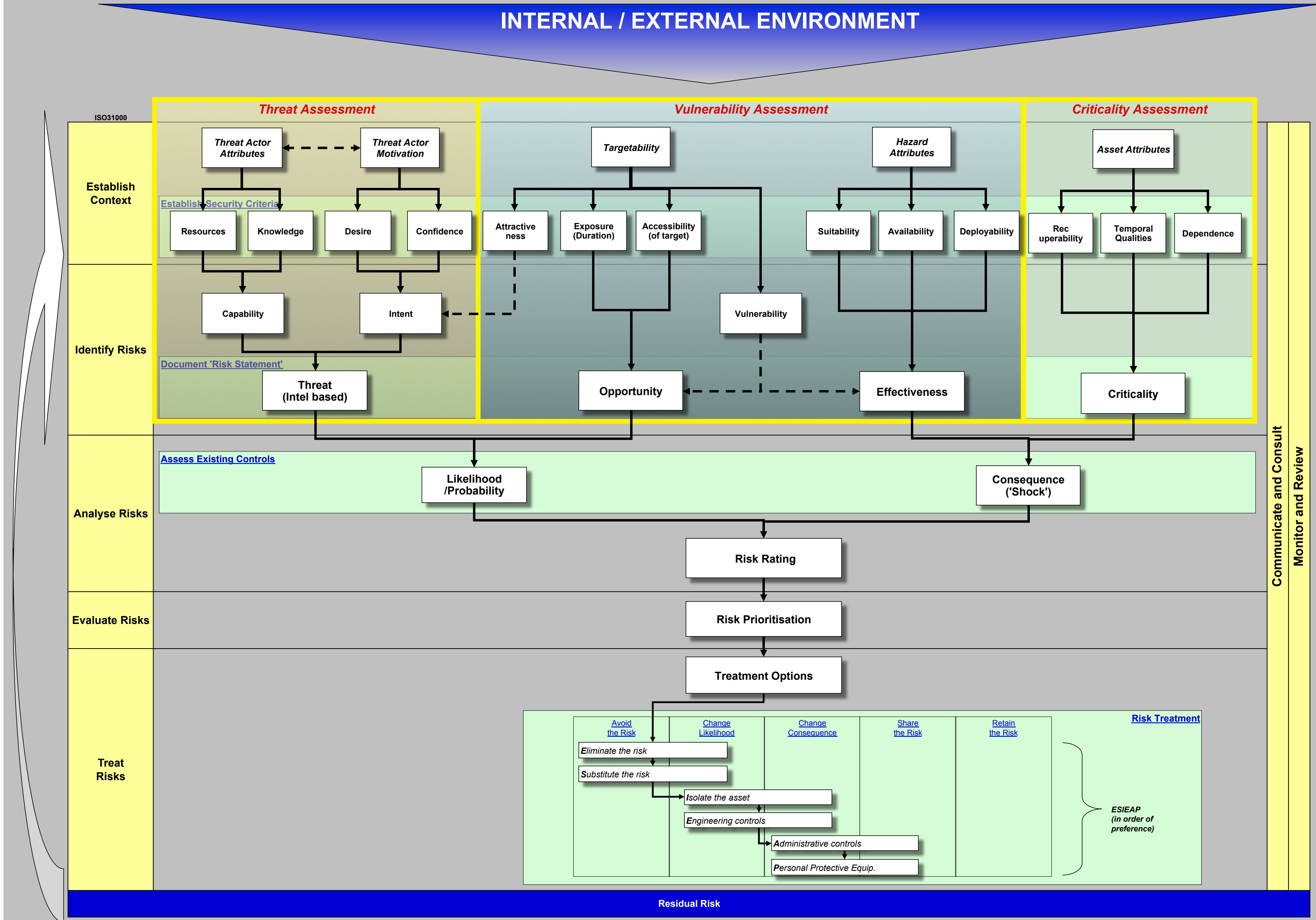
SECURITY RISK MANAGEMENT

SRMBOK

BODY OF KNOWLEDGE

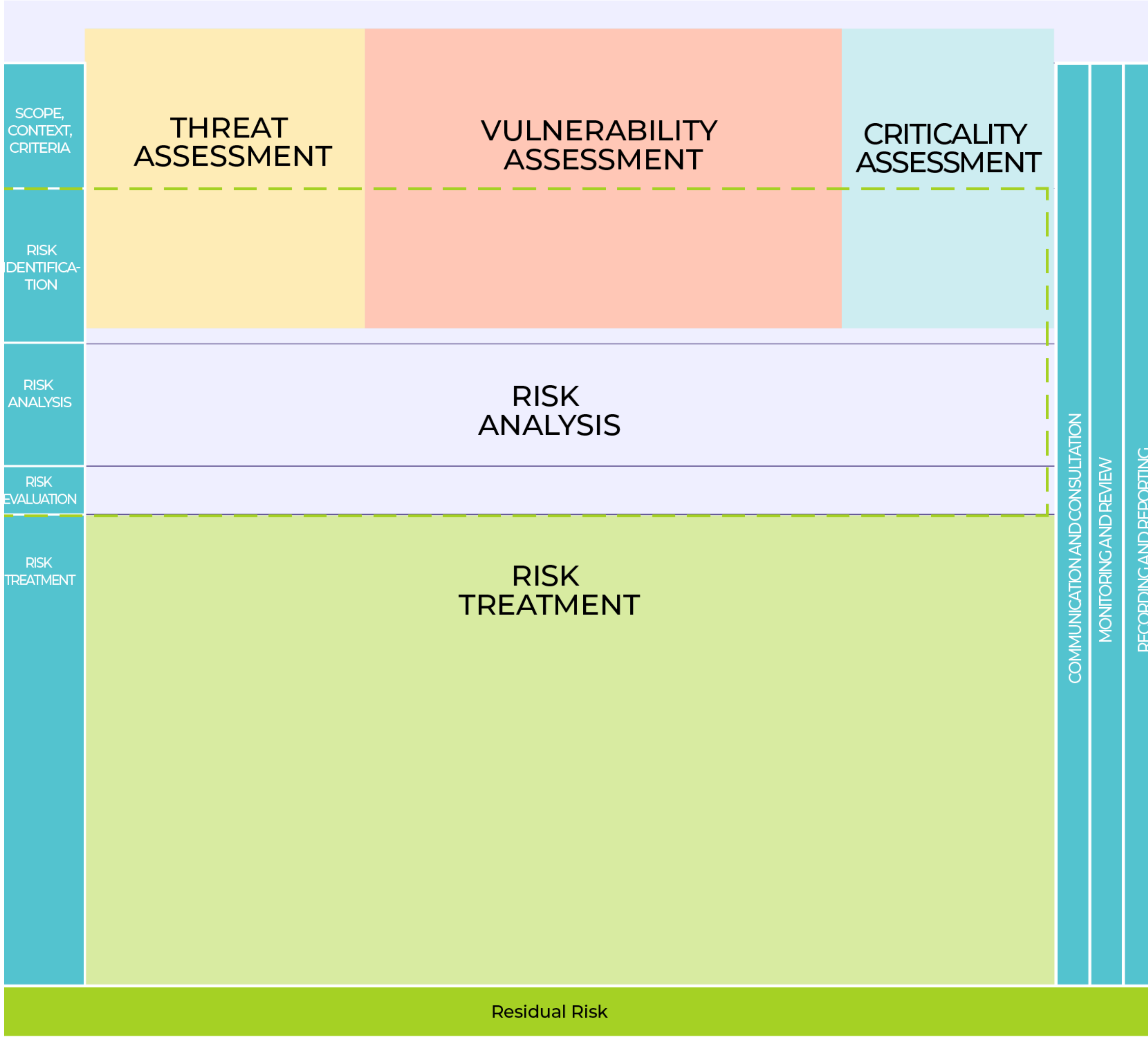
JULIAN TALBOT MILES JAKEMAN

WILEY



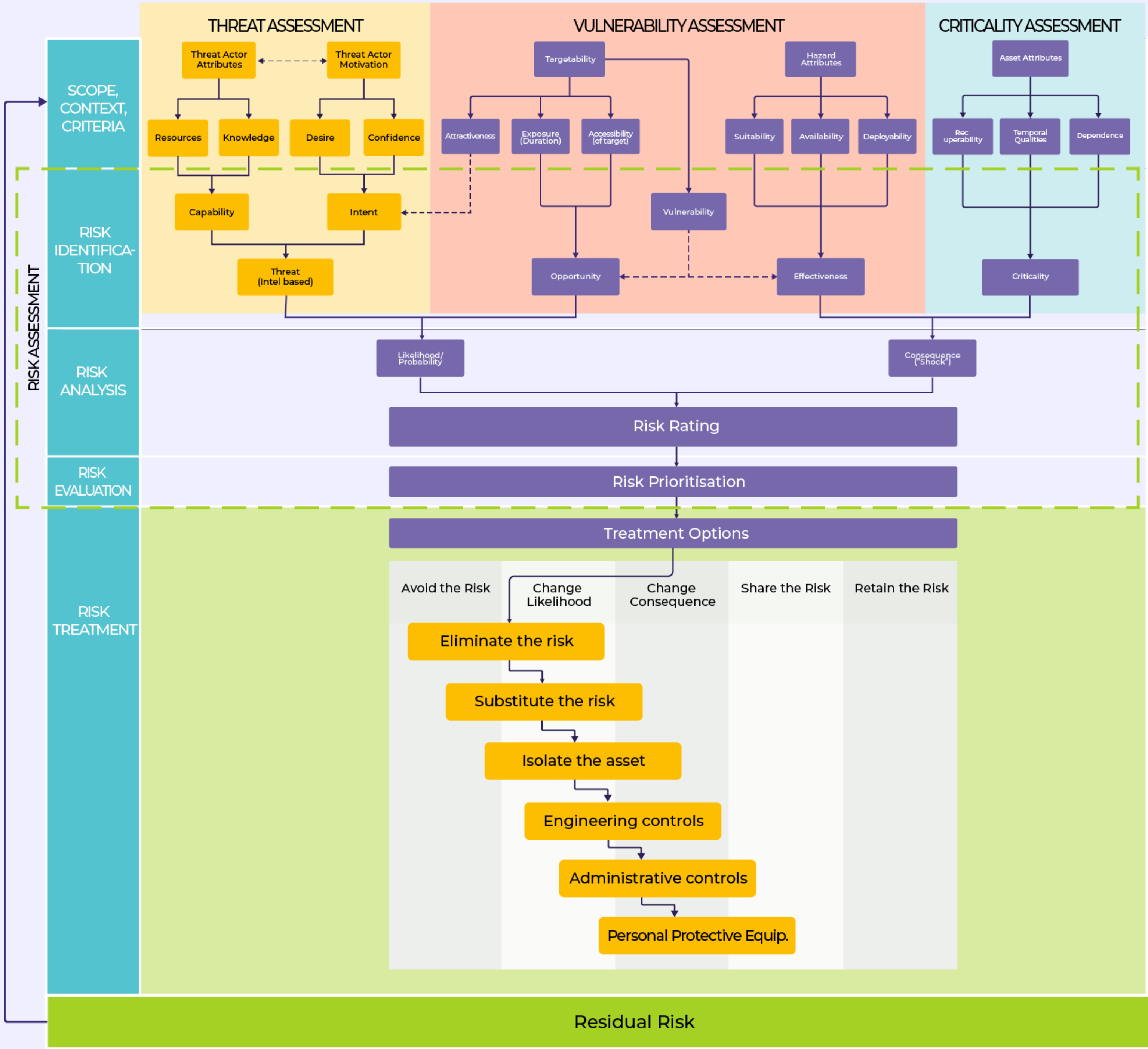
The big picture for enterprise security risk assessment

ISO3100:2018 Risk Management Standard



SRMBOK SRA Model

ISO31000, OCTAVE, CARVER, THREAT, ESIEAP, ++



SCOPE, CONTEXT, CRITERIA

RISK IDENTIFICA-TION

RISK ANALYSIS

RISK EVALUATION

RISK TREATMENT

RISK ASSESSMENT

THREAT ASSESSMENT

Threat Actor Attributes

Threat Actor Motivation

Resources

Knowledge

Desire

Confidence

Capability

Intent

Threat (Intel based)

VULNERABILITY ASSESSMENT

Targetability

Attractiveness

Exposure (Duration)

Accessibility (of target)

Vulnerability

Opportunity

Hazard Attributes

Suitability

Availability

Deployability

Effectiveness

CRITICALITY ASSESSMENT

Asset Attributes

Rec uperability

Temporal Qualities

Dependence

Criticality

Likelihood/ Probability

Consequence ("Shock")

Risk Rating

Risk Prioritisation

Treatment Options

Avoid the Risk

Change Likelihood

Change Consequence

Share the Risk

Retain the Risk

Eliminate the risk

Substitute the risk

Isolate the asset

Engineering controls

Administrative controls

Personal Protective Equip.

Residual Risk

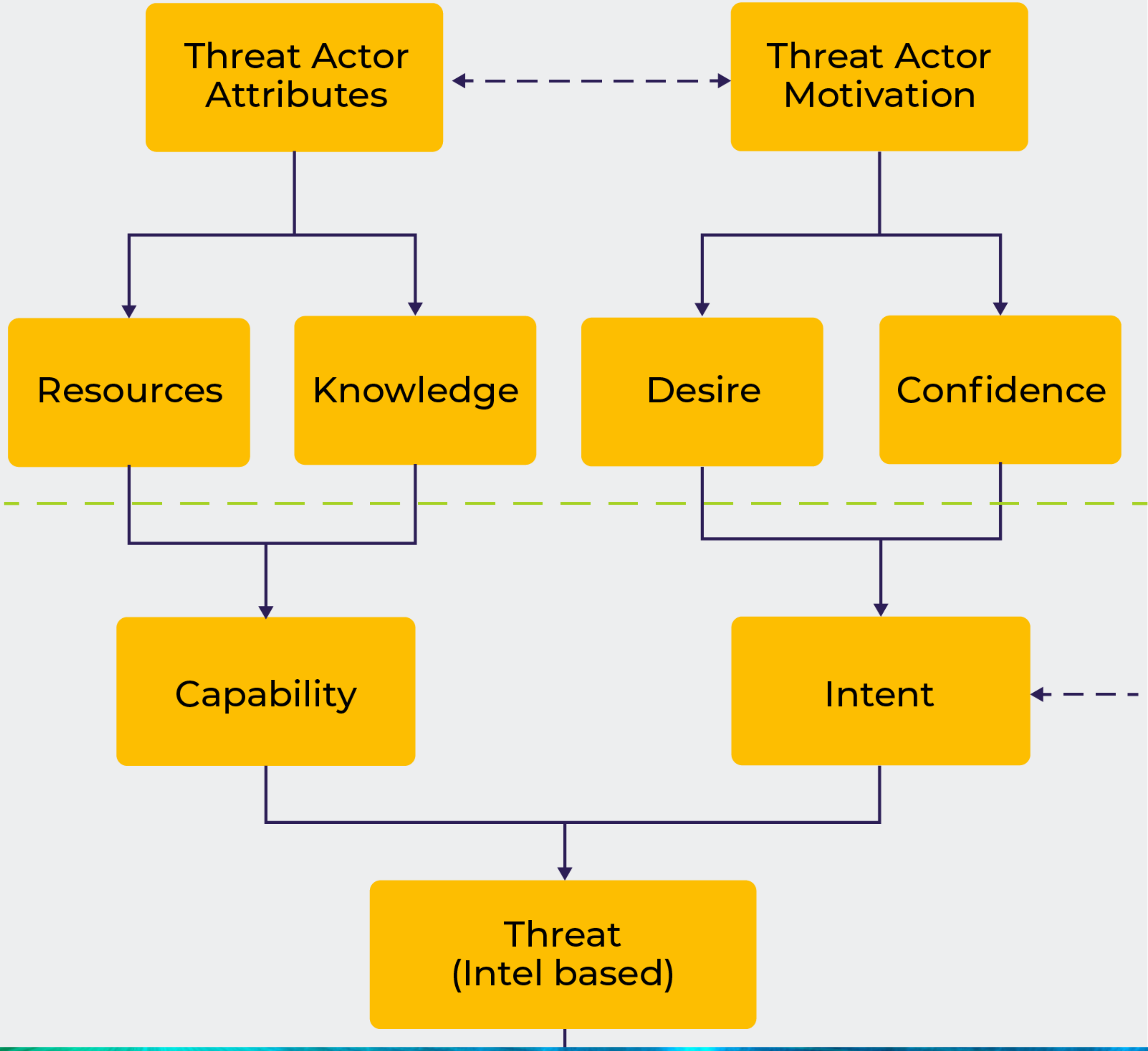
Threat

Intent + Capability

		None	Little	Expressed	Determined	Dedicated
CAPABILITY	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

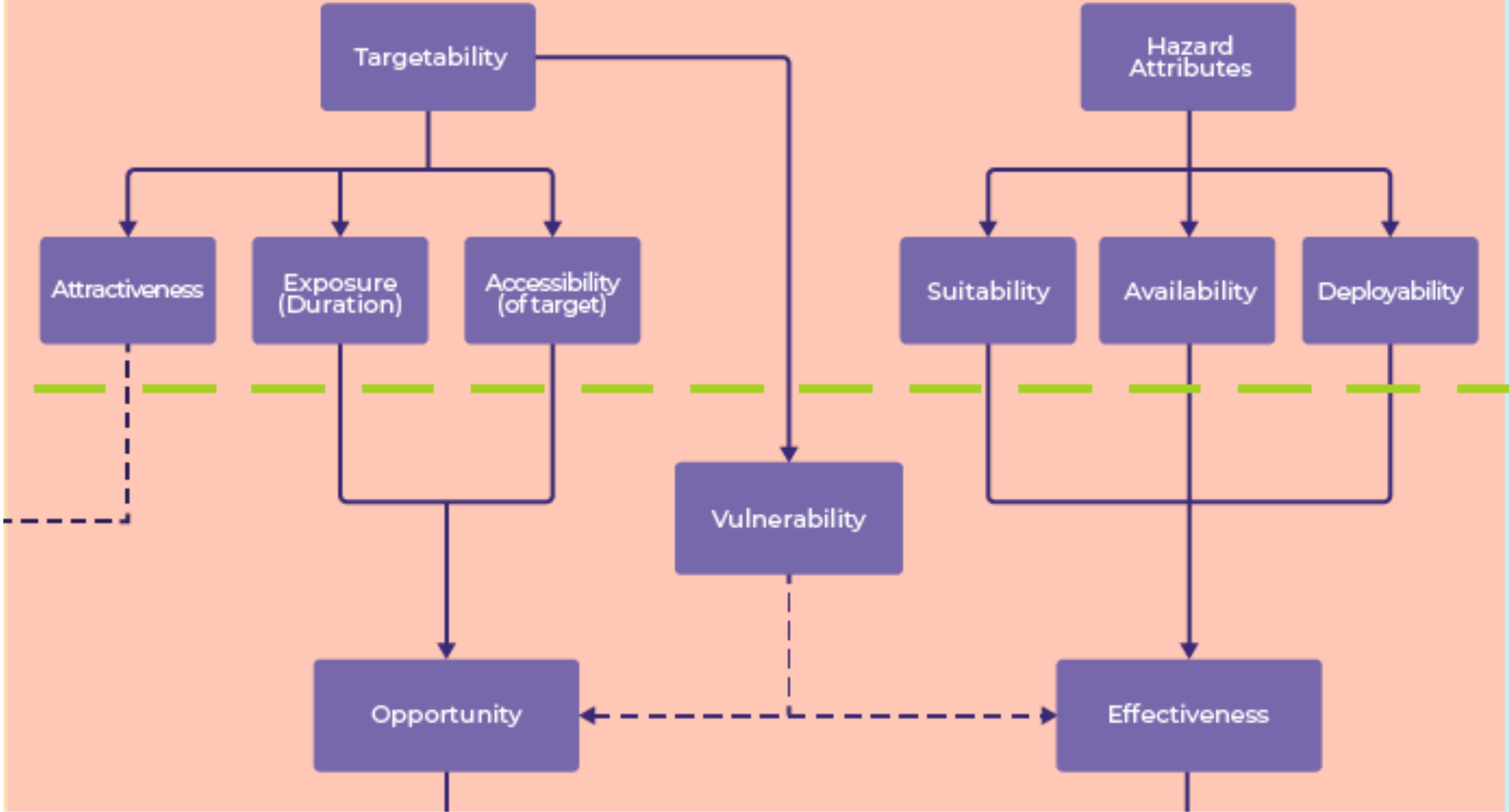
Threat


Threat Actor Attributes
Threat Actor Motivation
Resources
Knowledge
Desire
Confidence
Capability
Intent
Threat (Intel based)

Threat Assessment

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

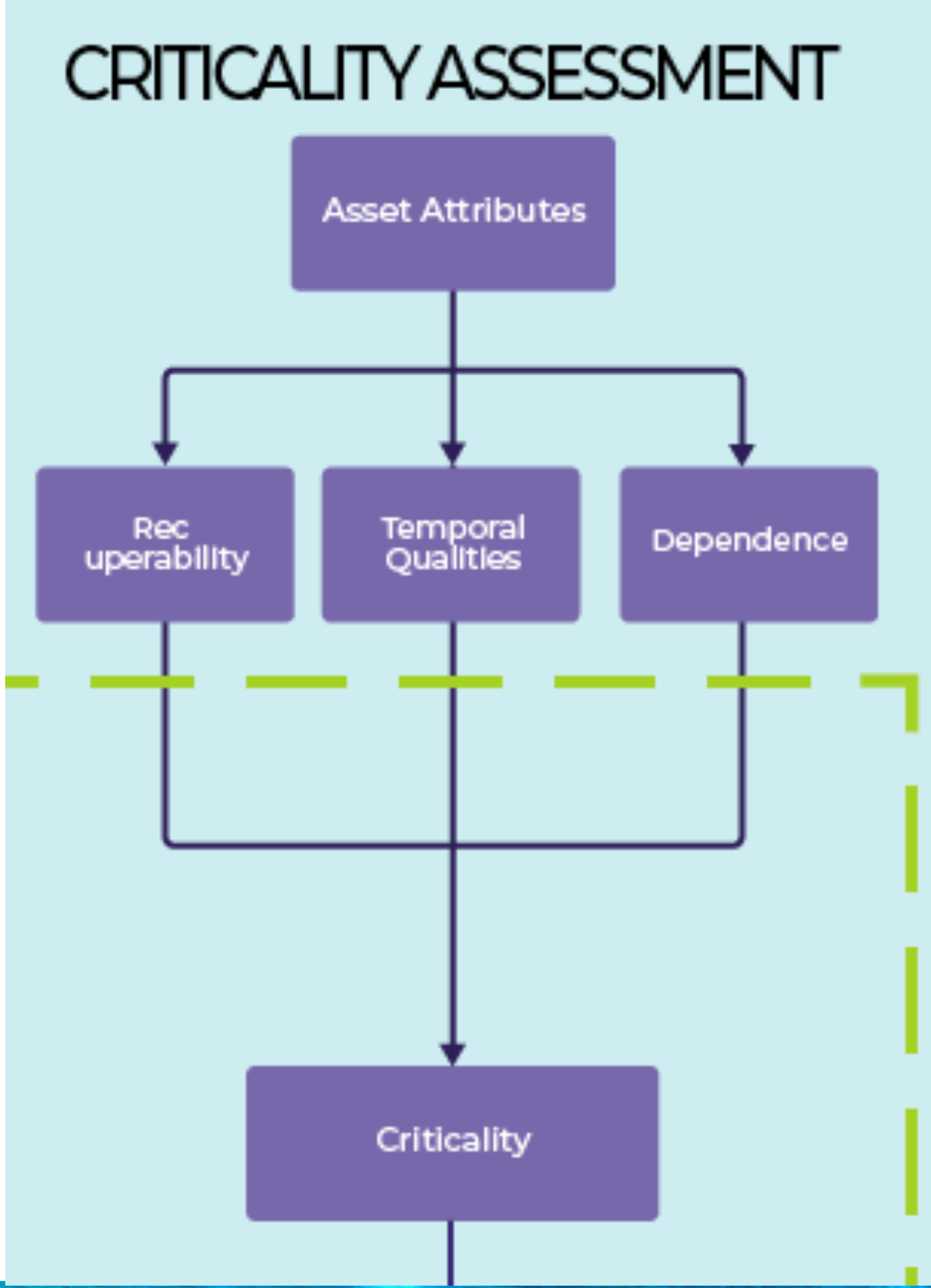
VULNERABILITY ASSESSMENT



Criticality

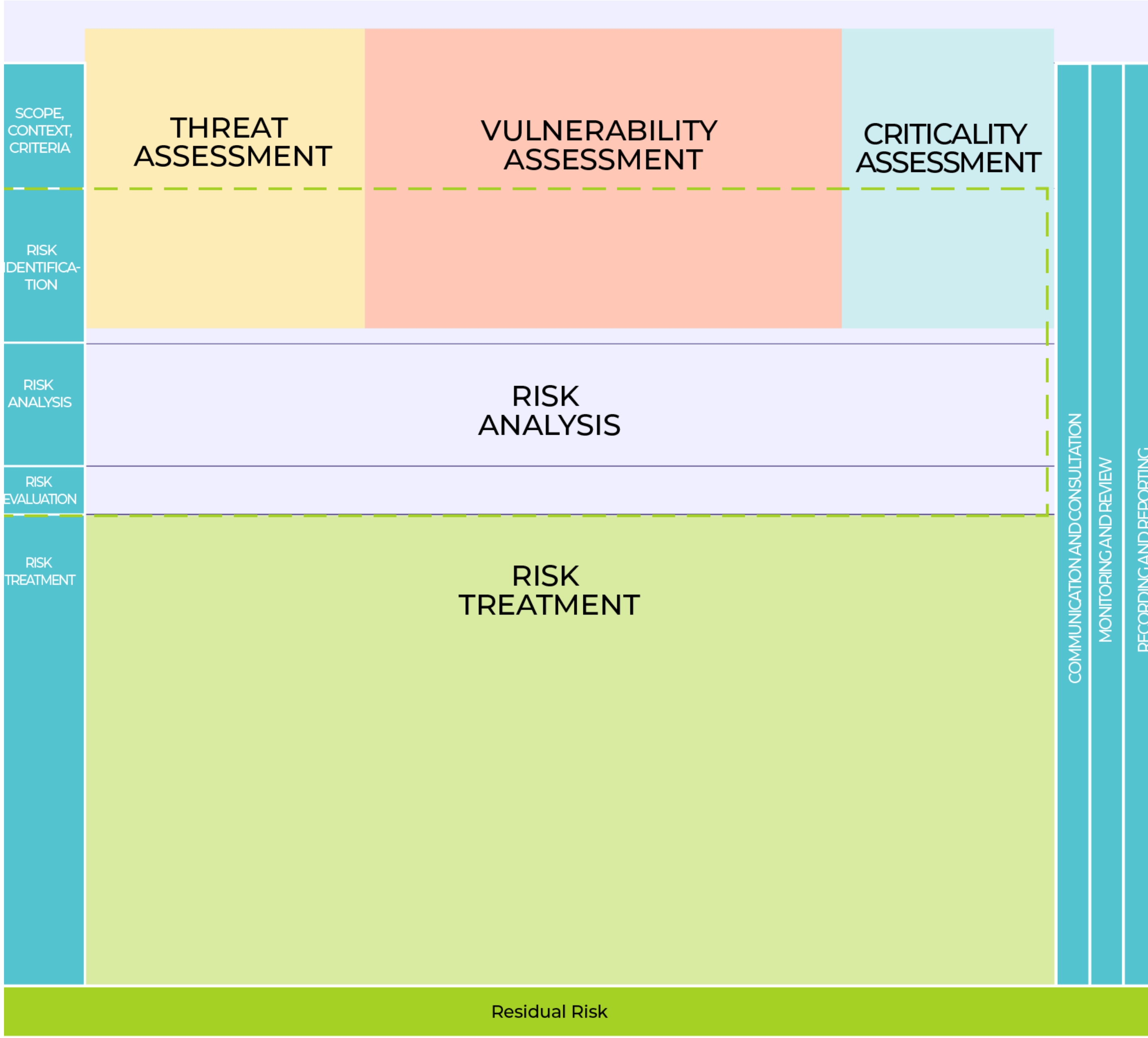
Business Impact Assessment

MAO



The big picture for enterprise security risk assessment

ISO3100:2018 Risk Management Standard



SCOPE, CONTEXT, CRITERIA

RISK IDENTIFICATION

RISK ANALYSIS

RISK EVALUATION

RISK TREATMENT

THREAT ASSESSMENT

VULNERABILITY ASSESSMENT

CRITICALITY ASSESSMENT

RISK ANALYSIS

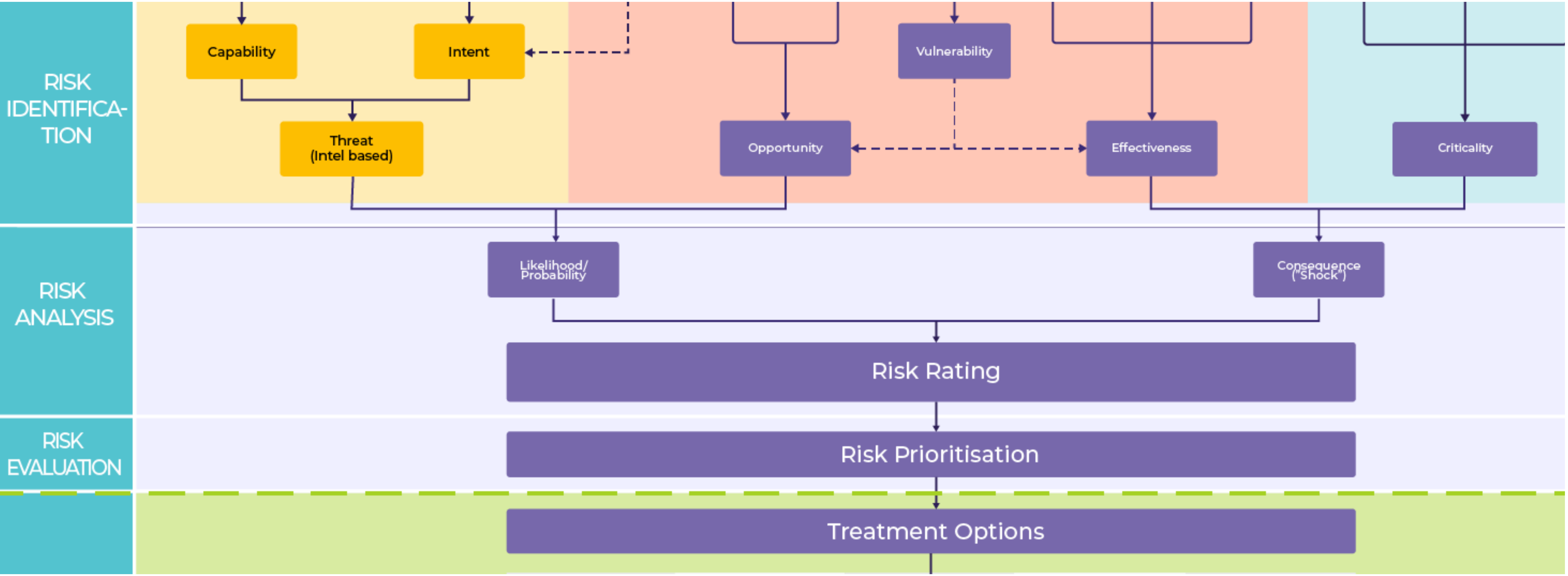
RISK TREATMENT

COMMUNICATION AND CONSULTATION

MONITORING AND REVIEW

RECORDING AND REPORTING

Residual Risk


RISK IDENTIFICA-TION
Capability
Intent
Threat (Intel based)
Vulnerability
Opportunity
Effectiveness
Criticality
RISK ANALYSIS
Likelihood/ Probability
Consequence ("Shock")
Risk Rating
RISK EVALUATION
Risk Prioritisation
Treatment Options

RISK Matrix

Timeframe: 1 Year

INFORMATION	Compromise of information otherwise available in the public domain.	Minor compromise of information sensitive to internal or sub-unit interests.	Compromise of information sensitive to the organizations operations.	Compromise of information sensitive to organizational interests.	Compromise of information with significant ongoing impact.
PROPERTY	Minor damage or vandalism to asset.	Minor damage or loss of <5% of total assets	Damage or loss of <20% of total assets	Extensive damage or loss of ~50% of total assets	Destruction or complete loss of >50% of assets
ECOMONIC	1% of budget or revenue (organizational, division or project budget as relevant)	10-20% of budget	40-60% of budget or revenue	60-80% of budget or revenue	>80% of project or organizational budget or revenue
REPUTATION	Local mention only. Quickly forgotten.	Scrutiny by Executive, internal committees or internal audit to prevent escalation. Short term local media concern. Some impact on local level activities	Persistent national concern. Scrutiny required by external agencies. Long term 'brand' impact.	Persistent intense national public, political and media scrutiny.	International concern, Governmental Inquiry or sustained adverse national/ international media. 'Brand' significantly affects organizational abilities.
CAPABILITY	Minor skills impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations.	Some impact on organizational capability in terms of delays, systems quality but able to be dealt with at operational level	Impact on the organization resulting in reduced performance such that targets are not met. Organizations existence is not threatened, but could be subject to significant review.	Breakdown of key activities leading to reduction in performance (eg. service delays, revenue loss, client dissatisfaction, legislative breaches).	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/ organization is threatened.
	1	2	3	4	5

	Qualitative Likelihood	Historical Occurrences	Natural Frequencies	Probability			Insignificant	Negligible	Moderate	Extensive	Significant
LIKELIHOOD	Is expected to occur in most circumstances	Has occurred on an regular basis in the organization during the timeframe being considered or circumstances are in train that will cause it to happen	Is likely, or has been known to occur 90 times every 100 timeframes	0.90 (0.80-0.99)	5	ALMOST CERTAIN	6	7	8	9	10
	Will probably occur in most circumstances	Has occurred in the organization within 3 multiples of the timeframe being considered.	Is likely, or has been known to occur roughly 70 times in 100	0.70 (0.61-0.80)	4	LIKELY	5	6	7	8	9
	Might occur at some time	Has occurred previously in the history of the organization and/or in other similar organizations or circumstances	Is likely, or has been known to occur approximately 50 out of 100 times	0.50 (0.41-0.60)	3	POSSIBLE	4	5	6	7	8
	Could occur at some time	Has never occurred in this organizaion but has occurred infrequently in other similar organizations	Is likely, or has been known to occur less than 1 in 10,000 times	0.30 (0.21-0.40)	2	UNLIKELY	3	4	5	6	7
	Can only occur in exceptional circumstances	Is possible but has not occurred to date in this or any similar organizations	Is likely, or has been known to occur less than once in 100 timeframes	0.10 (0.01-0.20)	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

The CASE for Risk Identification

Compromise of our pricing information (*Asset/Resource*)

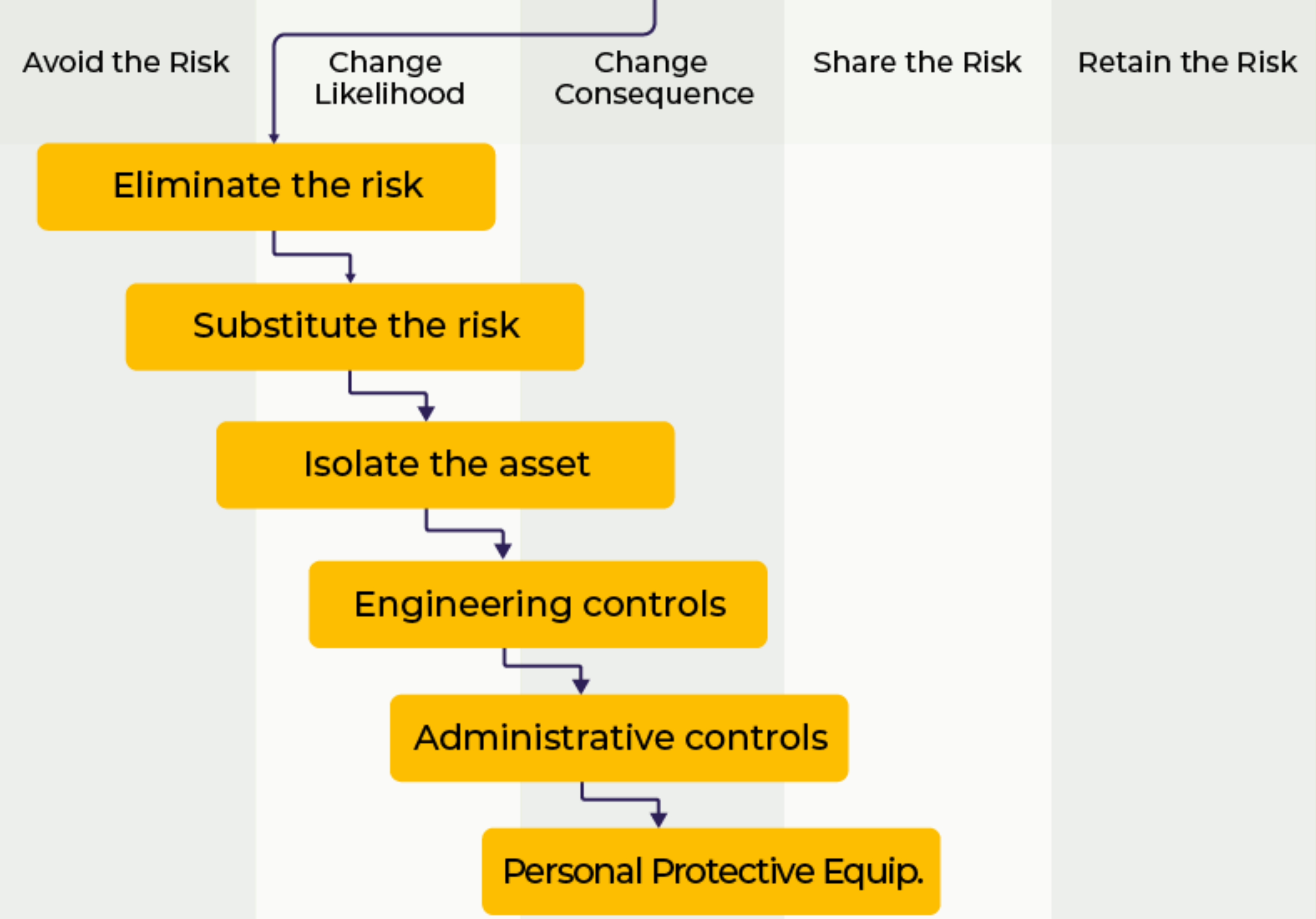
due to our competitor (*Source*)

listening to our meetings via a compromised phone (*Event*)

causing lost sales and reduced profit (Consequence).

Risk ID	Risk No. 5
Event	Espionage
Source	Competitors
Resource	Information
Consequence	Financial

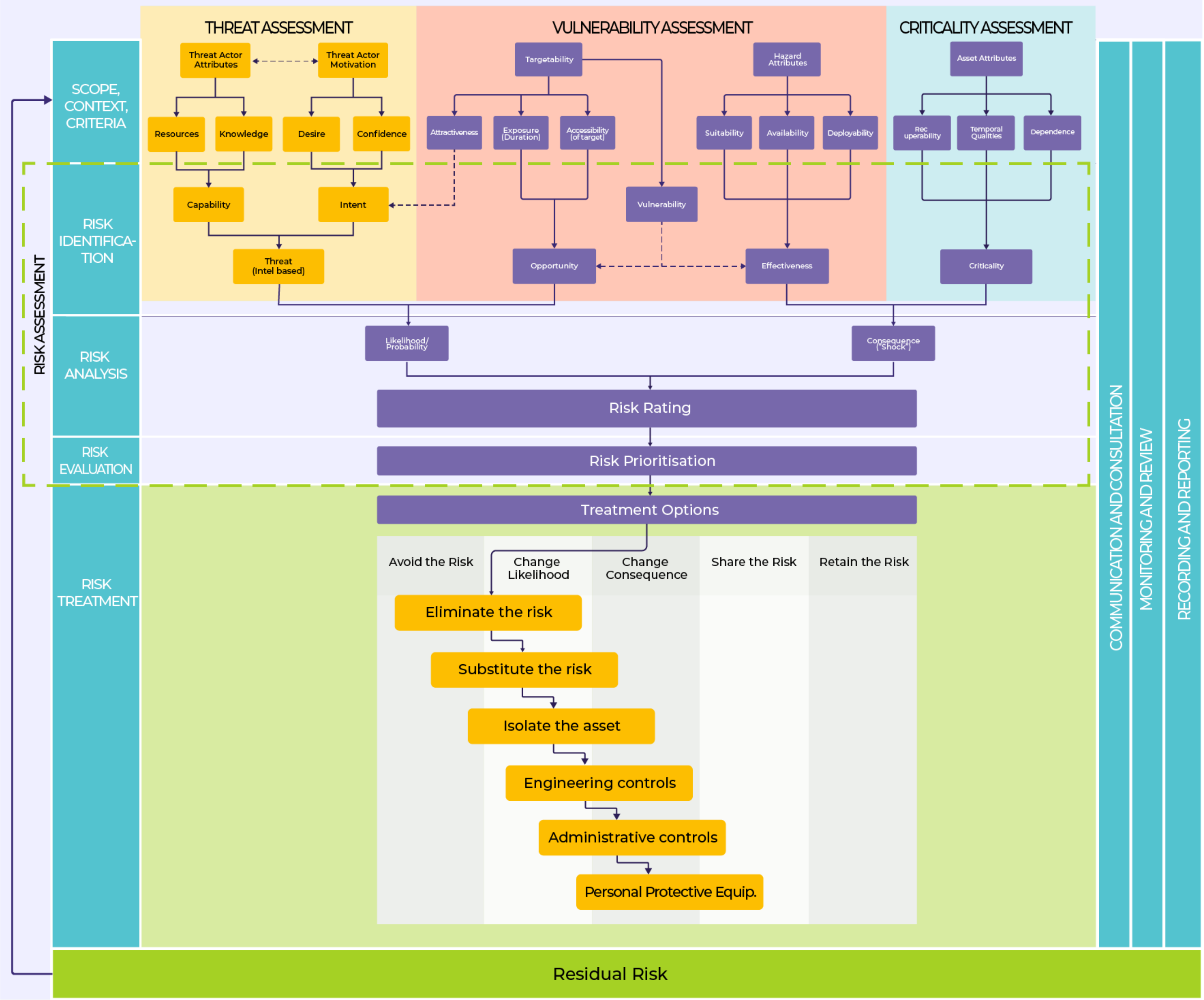
Treatment Options



SRMBOK

Security Risk Management Body Of Knowledge

SECTARA™



THREAT ASSESSMENT

VULNERABILITY ASSESSMENT

CRITICALITY ASSESSMENT

SCOPE, CONTEXT, CRITERIA

RISK IDENTIFICA-TION

RISK ANALYSIS

RISK EVALUATION

RISK TREATMENT

RISK ASSESSMENT

Threat Actor Attributes

Threat Actor Motivation

Resources

Knowledge

Desire

Confidence

Capability

Intent

Threat (Intel based)

Targetability

Attractiveness

Exposure (Duration)

Accessibility (of target)

Vulnerability

Opportunity

Hazard Attributes

Suitability

Availability

Deployability

Effectiveness

Asset Attributes

Rec uperability

Temporal Qualities

Dependence

Criticality

Likelihood/ Probability

Consequence ("Shock")

Risk Rating

Risk Prioritisation

Treatment Options

Avoid the Risk

Change Likelihood

Change Consequence

Share the Risk

Retain the Risk

Eliminate the risk

Substitute the risk

Isolate the asset

Engineering controls

Administrative controls

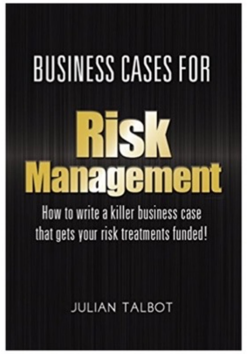
Personal Protective Equip.

COMMUNICATON AND CONSULTATION

MONITORING AND REVIEW

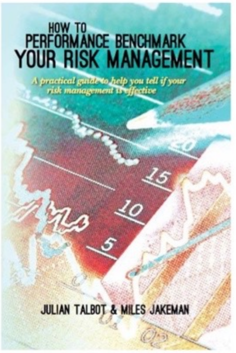
RECORDING AND REPORTING

Residual Risk


BUSINESS CASES FOR Risk Management

How to write a killer business case that gets your risk treatments funded!

JULIAN TALBOT


HOW TO PERFORMANCE BENCHMARK YOUR RISK MANAGEMENT

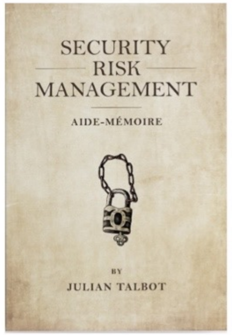
A practical guide to help you tell if your risk management is effective

JULIAN TALBOT & MILES JAKEMAN

Julian Talbot

THE NEW SUPERVISOR'S HANDBOOK

Congratulations on your promotion. now what?


SECURITY RISK MANAGEMENT

AIDE-MÉMOIRE

BY JULIAN TALBOT

SECTARA™

srmbok.fyi.to/ISC2

julian@juliantalbot.com

julian@sectara.com

julian@srmbok.com

srmbok.fyi.to/ISC2