SRMBOK

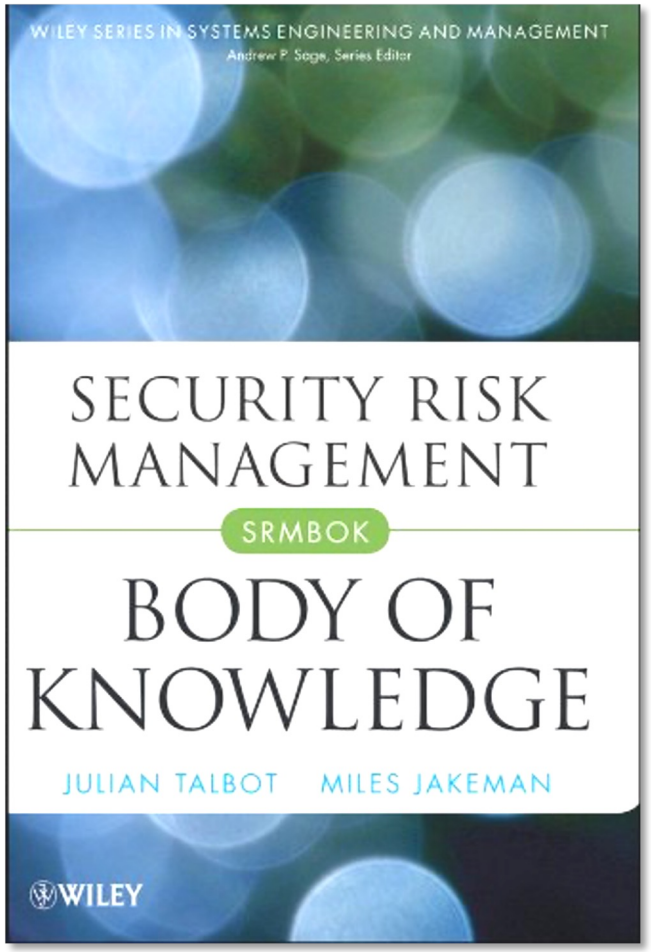
Security Risk Management Body Of Knowledge

SERT

Pty Ltd ABN76083252706

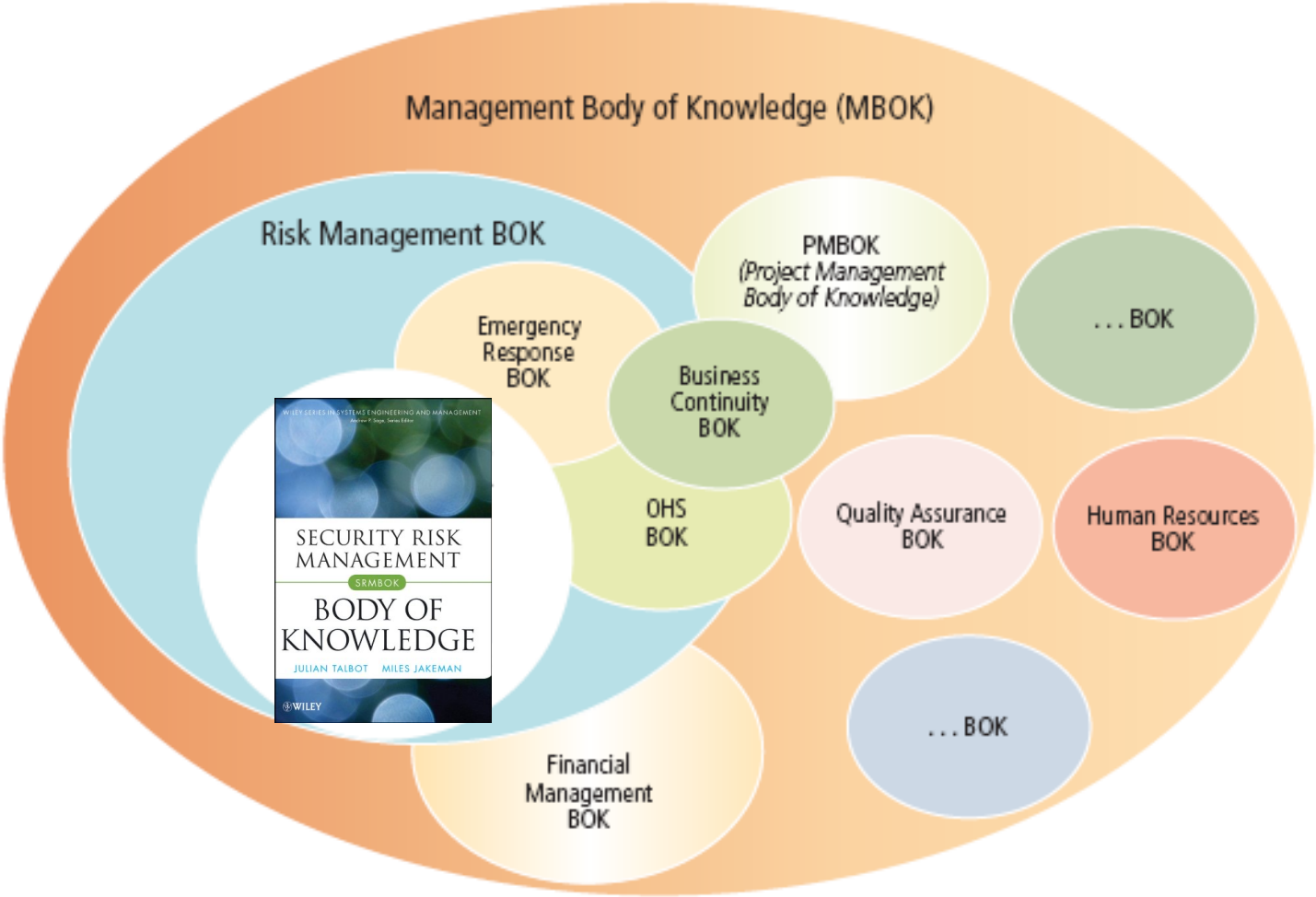
SRMBOK WEBINAR

Julian Talbot



Topics

- SRMBOK
  - What is it?
  - What does it mean for you?


Management Body of Knowledge (MBOK)
Risk Management BOK
PMBOK
(Project Management Body of Knowledge)
. . . BOK
Emergency Response BOK
Business Continuity BOK
OHS BOK
Quality Assurance BOK
Human Resources BOK
. . . BOK
Financial Management BOK
SECURITY RISK MANAGEMENT
SRMBOK
BODY OF KNOWLEDGE
JULIAN TALBOT MILES JAKEMAN
WILEY

What SRMBOK includes

- Introduction and Overview
- SRM Context
- Security Governance
- SRMBOK Framework
- Practice Areas
- Strategic Knowledge Areas
- Operational Competency Areas Activity Areas
- SRM Enablers
- Asset Areas
- SRM Integration
- SRM Lexicon
- Sample Templates
- Bibliography

Audience for SRMBOK

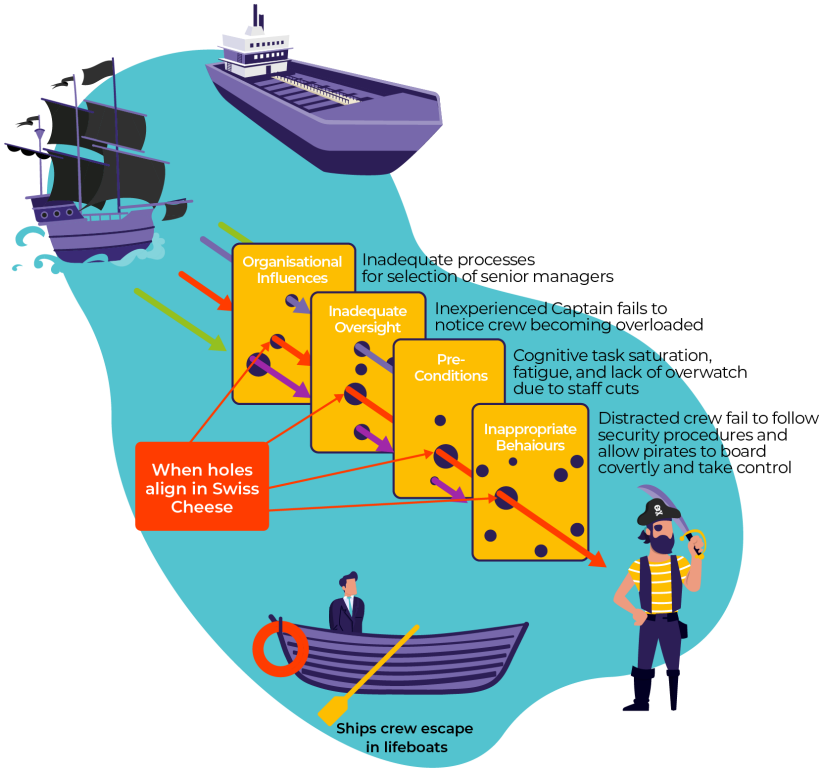

Anything that reduces my annual bonus
At least we all agree on the basics like the meaning of the word "risk"
The effect of uncertainty in our definitions?
Risk= danger!
Wait, what?
Opportunity?
Boring!

Swiss Cheese Theory

Human Factors

SRMAM.COM

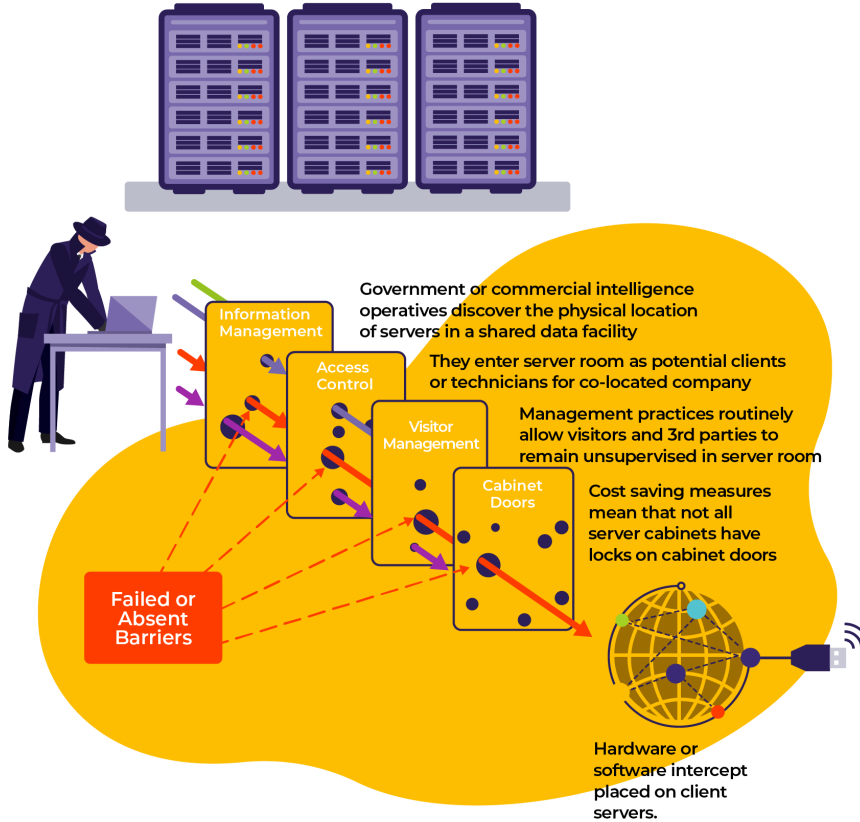
In this example, a series of Human Factors allows a boat load of pirates to gain access to an oil tanker, resulting in loss of ship



Swiss-Cheese Example

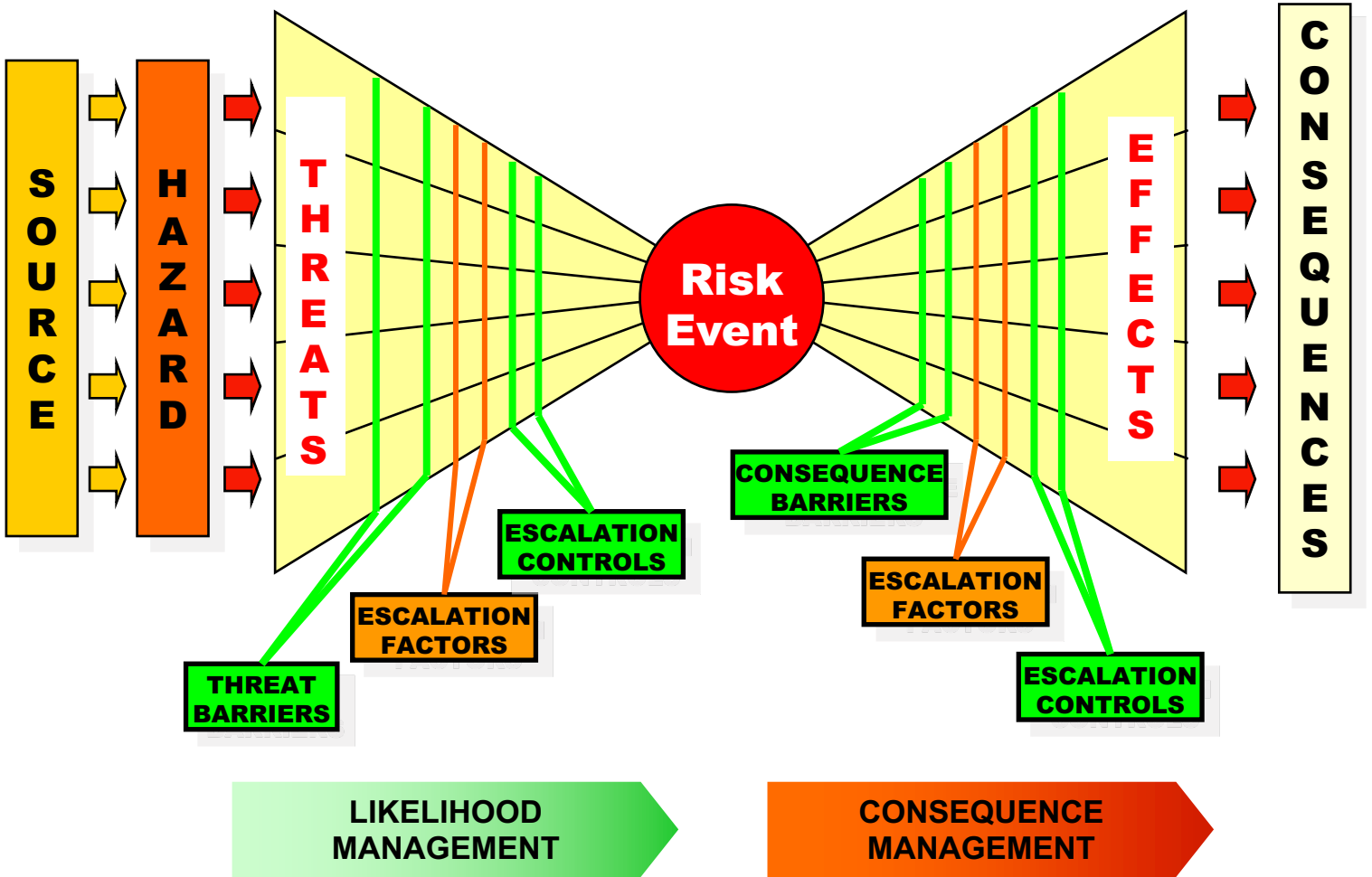
SRMAM.COM

In this example, intelligence agents gain physical access to corporate servers and steal corporate data.

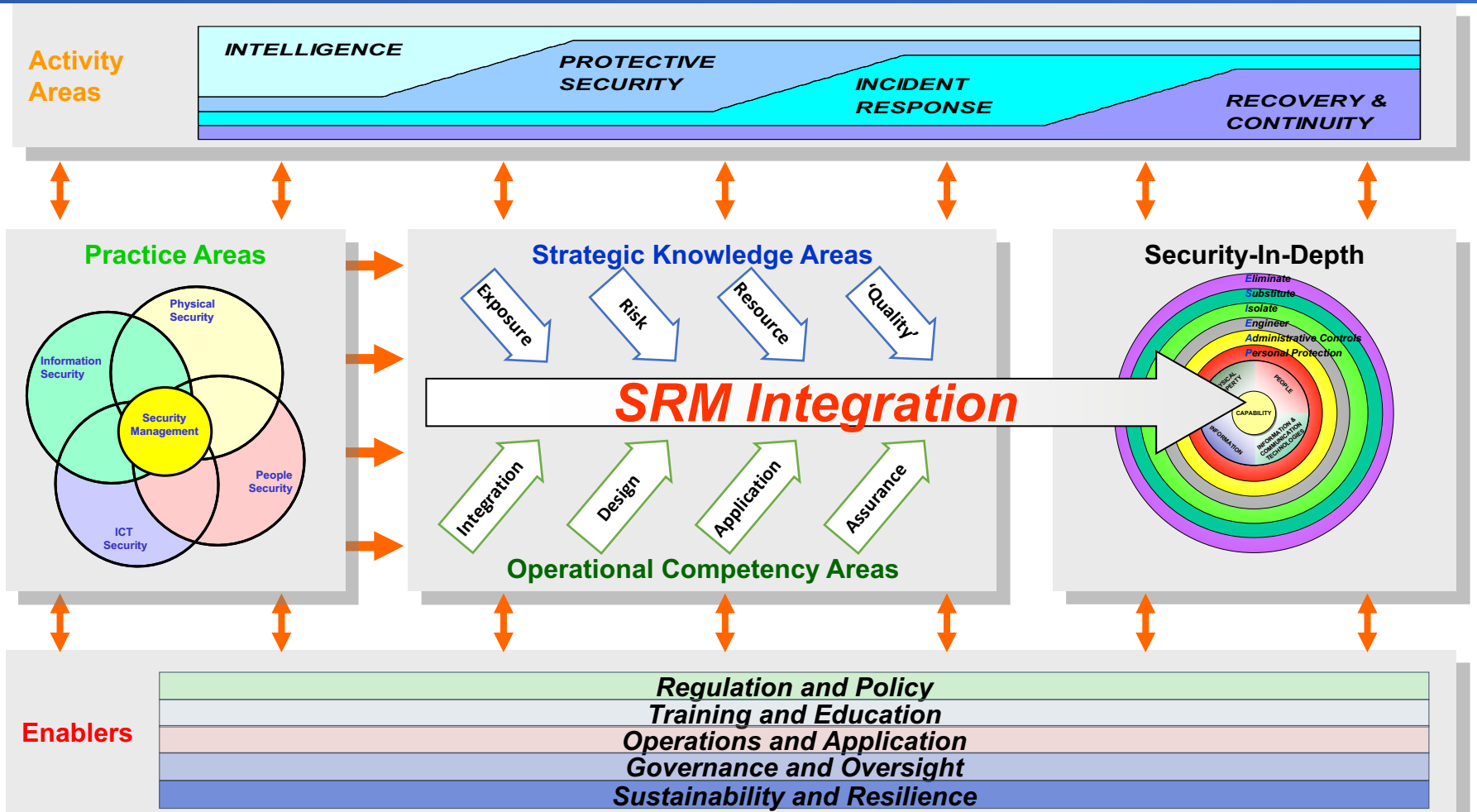


NOTE: Most data breaches occur remotely via software vulnerabilities but a) this is a lot easier example for non-IT people and b) it is (sadly) a real world example.

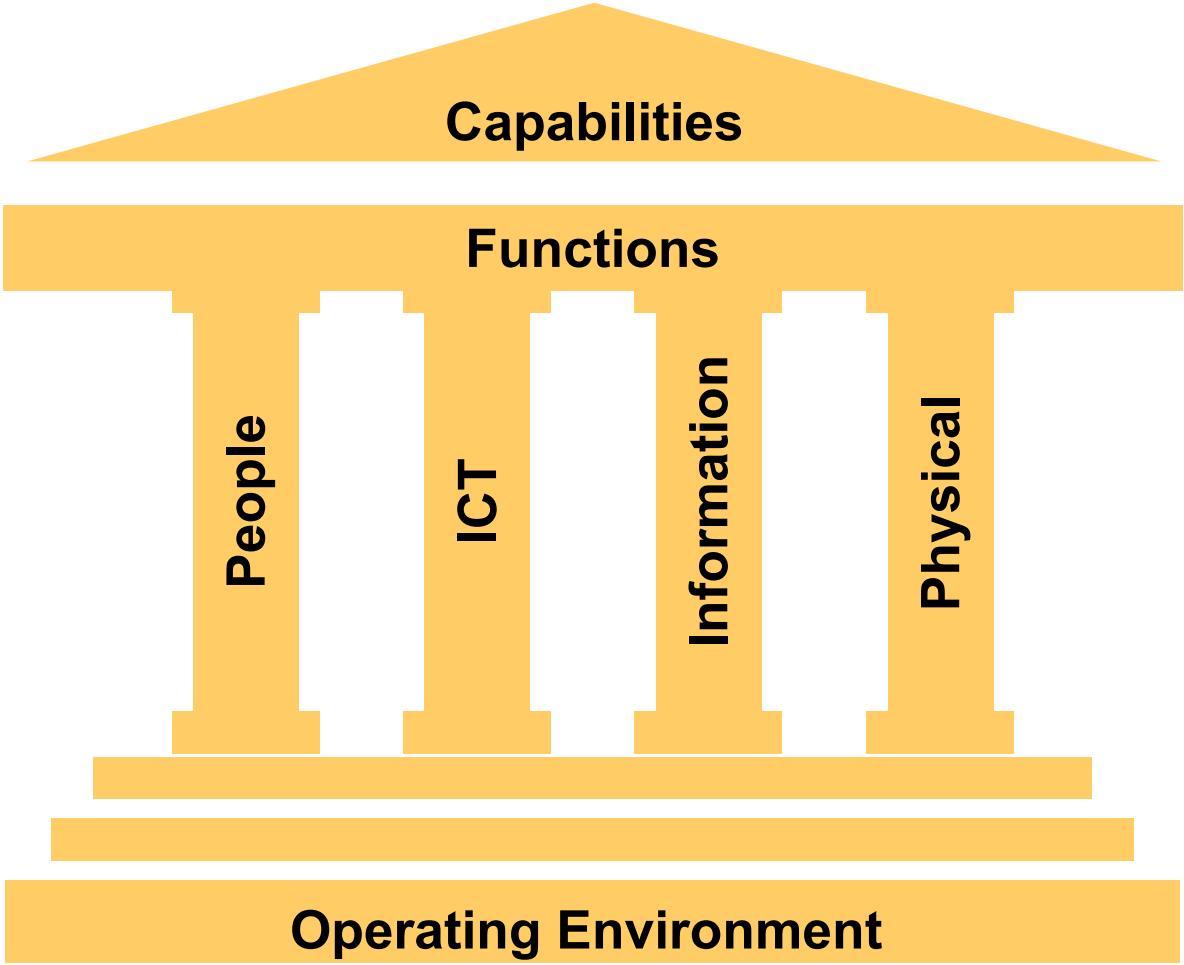
Defining Terms by Relationships



SRMBOK Framework



RESILIENCE


Capabilities
Functions
People
ICT
Information
Physical
Operating Environment

The Next Edition

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)

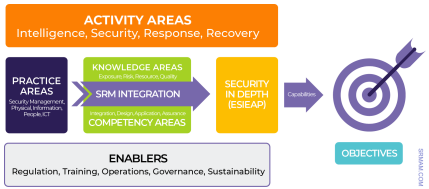
Capabilities

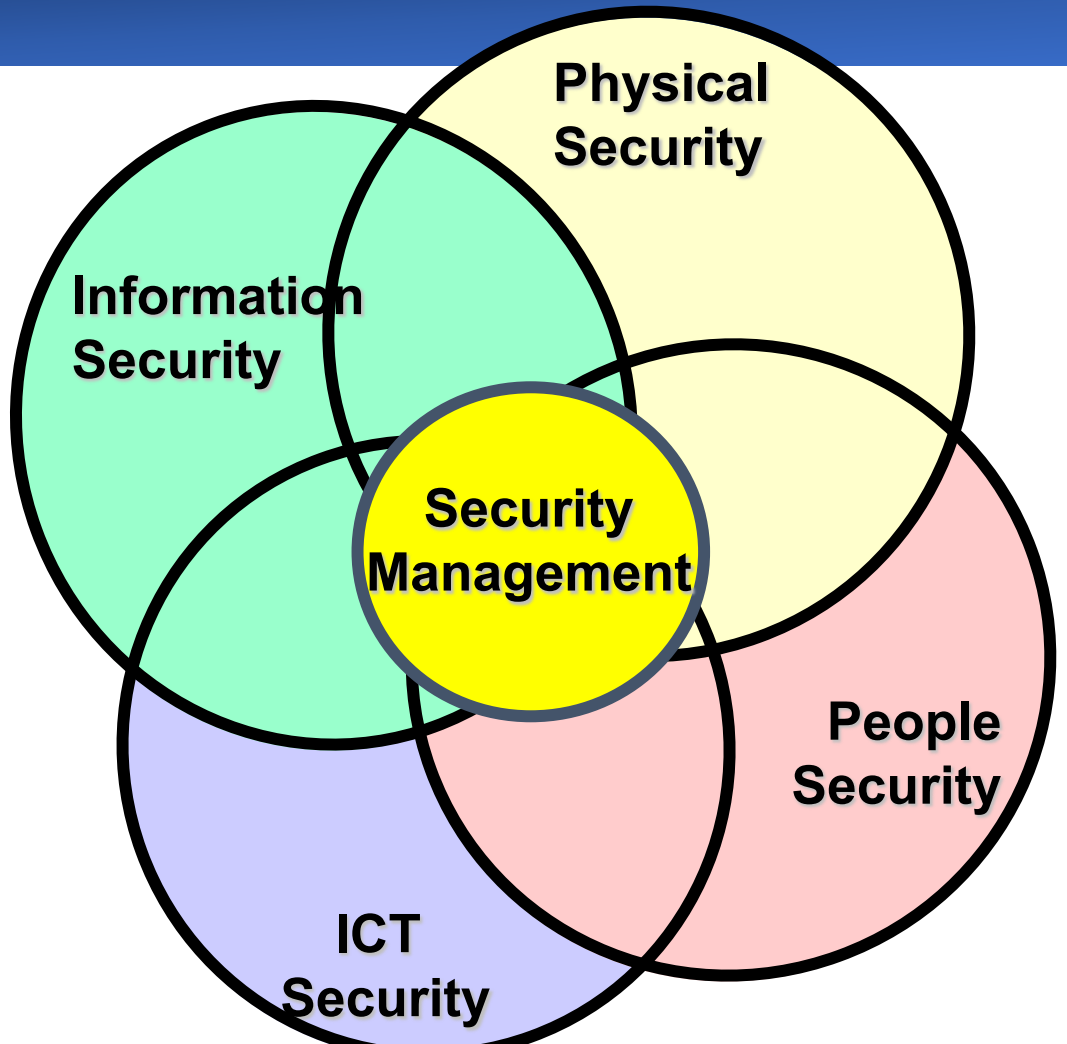
OBJECTIVES

ENABLERS
Regulation, Training, Operations, Governance, Sustainability

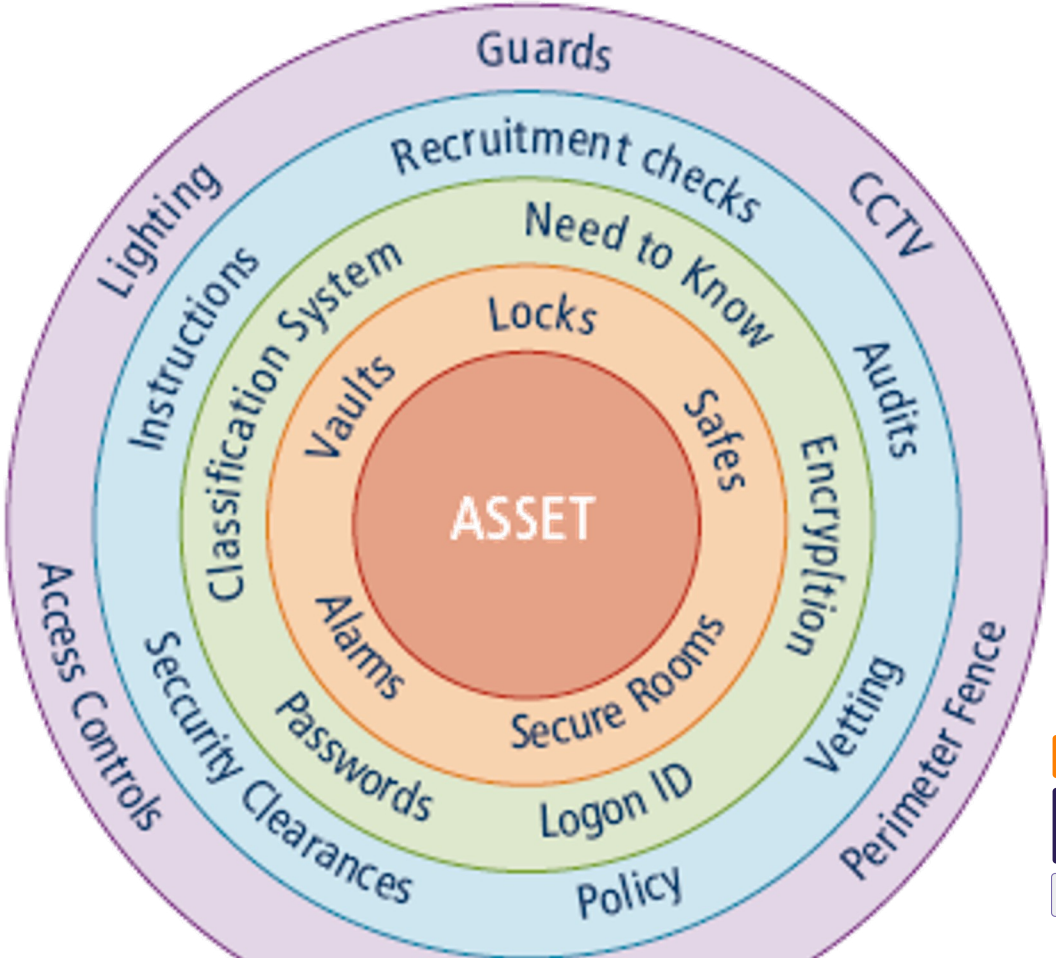
SRMAM.COM

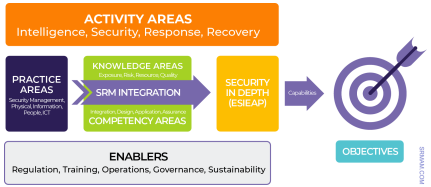
PRACTICE AREAS

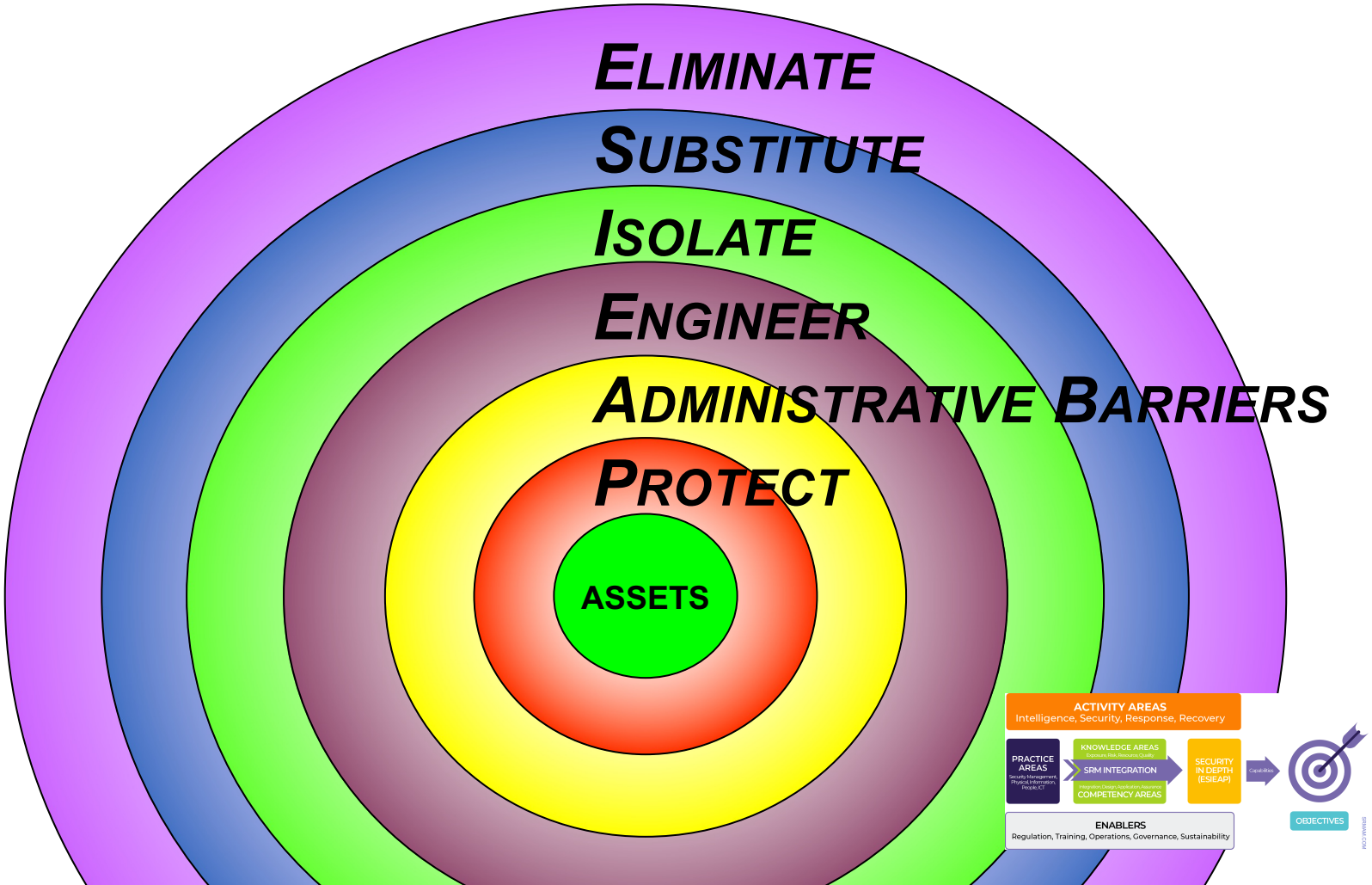




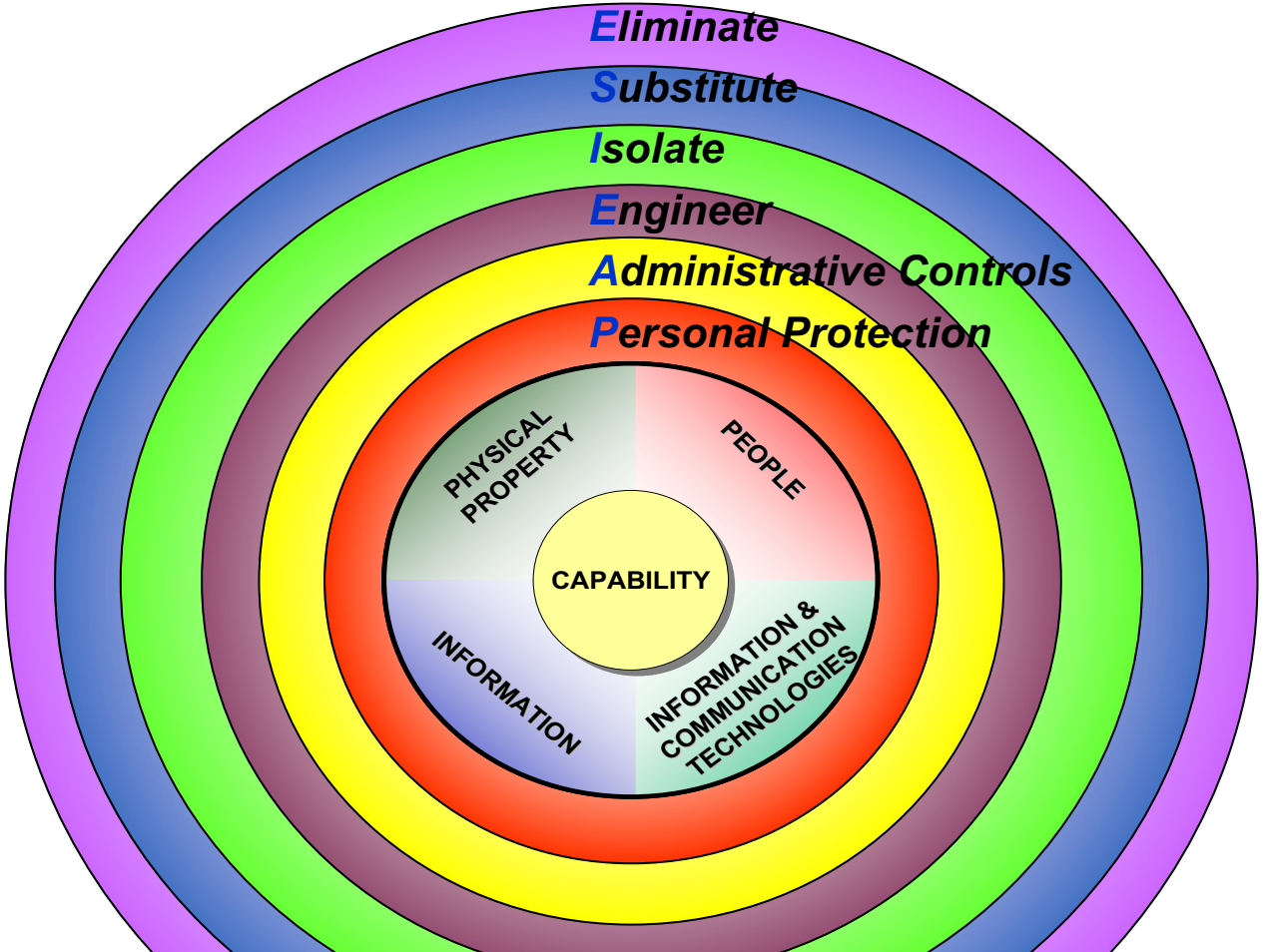
Security In Depth

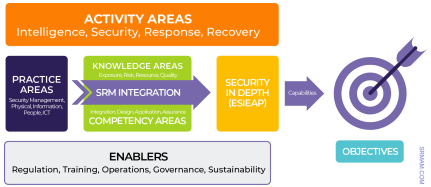





ELIMINATE
SUBSTITUTE
ISOLATE
ENGINEER
ADMINISTRATIVE BARRIERS
PROTECT
ASSETS
ACTIVITY AREAS
Intelligence, Security, Response, Recovery
PRACTICE AREAS
KNOWLEDGE AREAS
SRM INTEGRATION
COMPETENCY AREAS
SECURITY IN DEPTH (ESIEAP)
Capabilities
OBJECTIVES
ENABLERS
Regulation, Training, Operations, Governance, Sustainability

PROTECTING CAPABILITY





E Don’t explore for oil

S Mauritania not Iraq

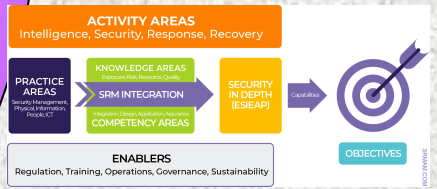
I Staff in remote areas not city

E Fence, gates, armoured veh.

A Policies, Travel safety training

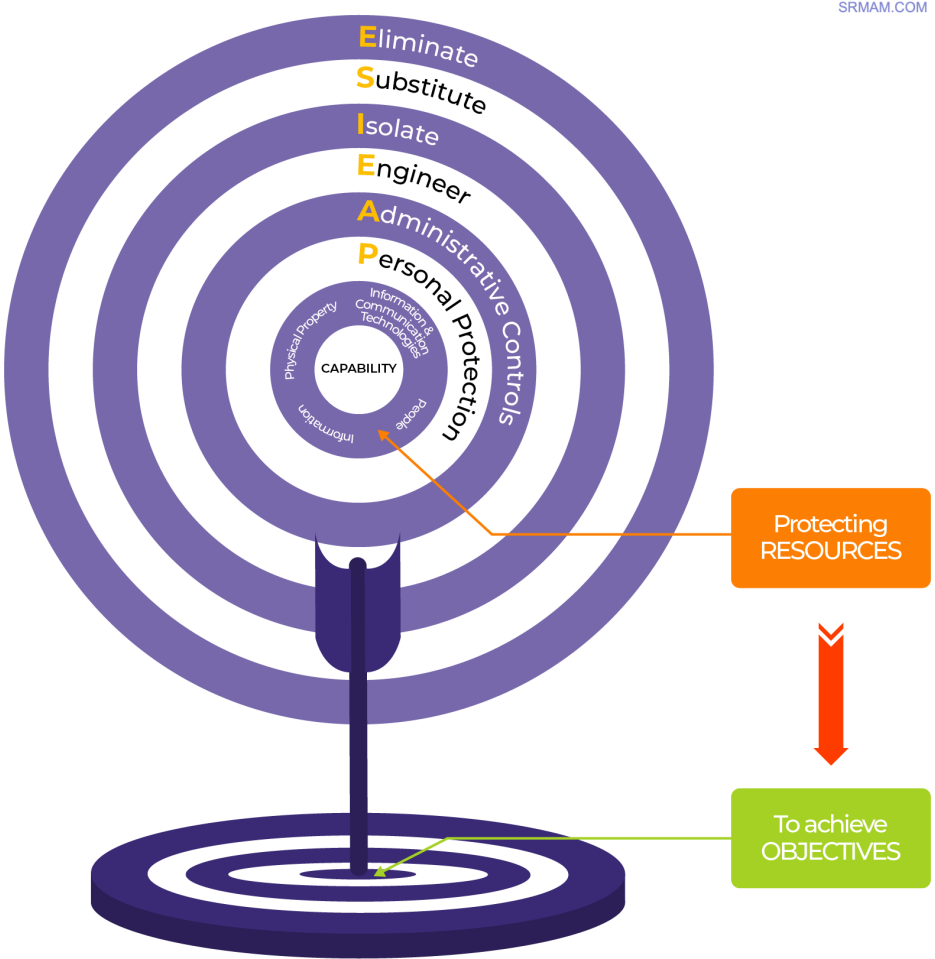
P Bullet-proof vests

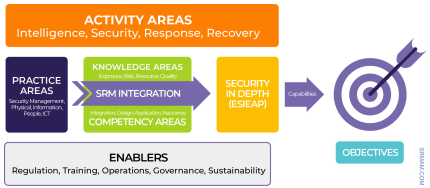
ASSETS



PROTECTING CAPABILITY

SRMAM.COM





SRM INTEGRATION

Strategic Knowledge Areas

Exposure

Risk

Resource

'Quality'

SRM Integration

Integration

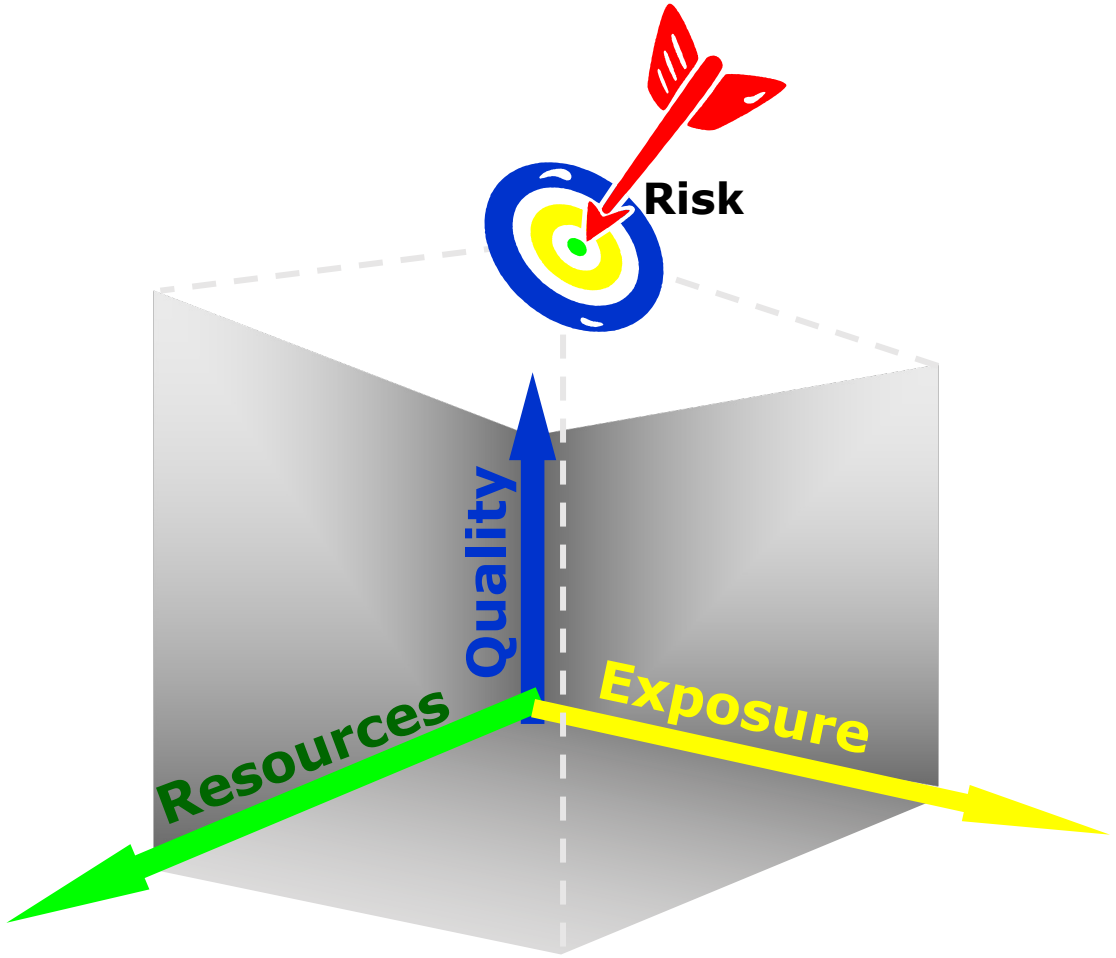
Design

Application

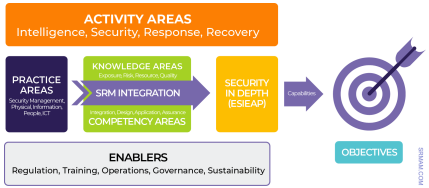
Assurance

Operational Competency Areas

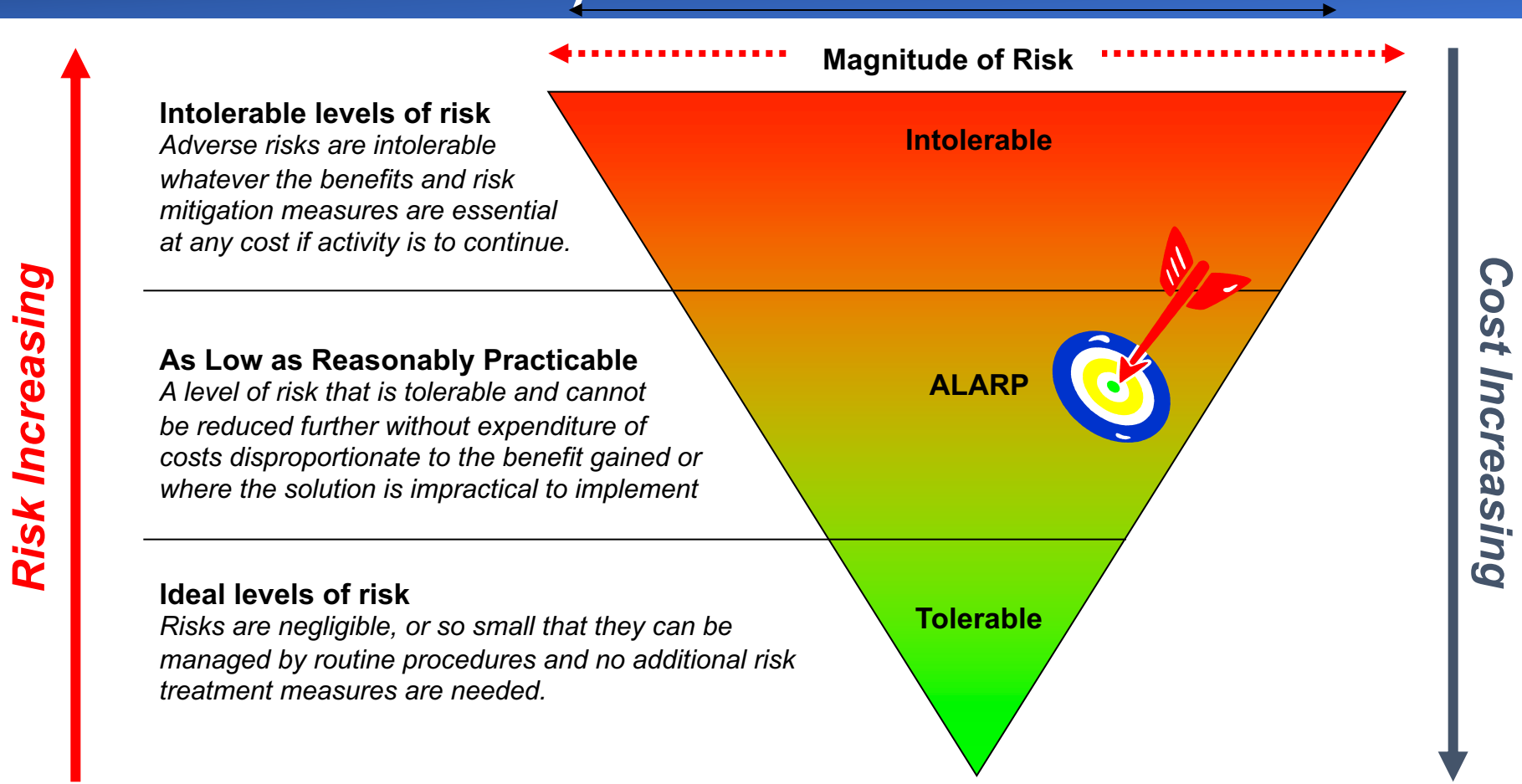
SRM QUADRUPLE CONSTRAINTS



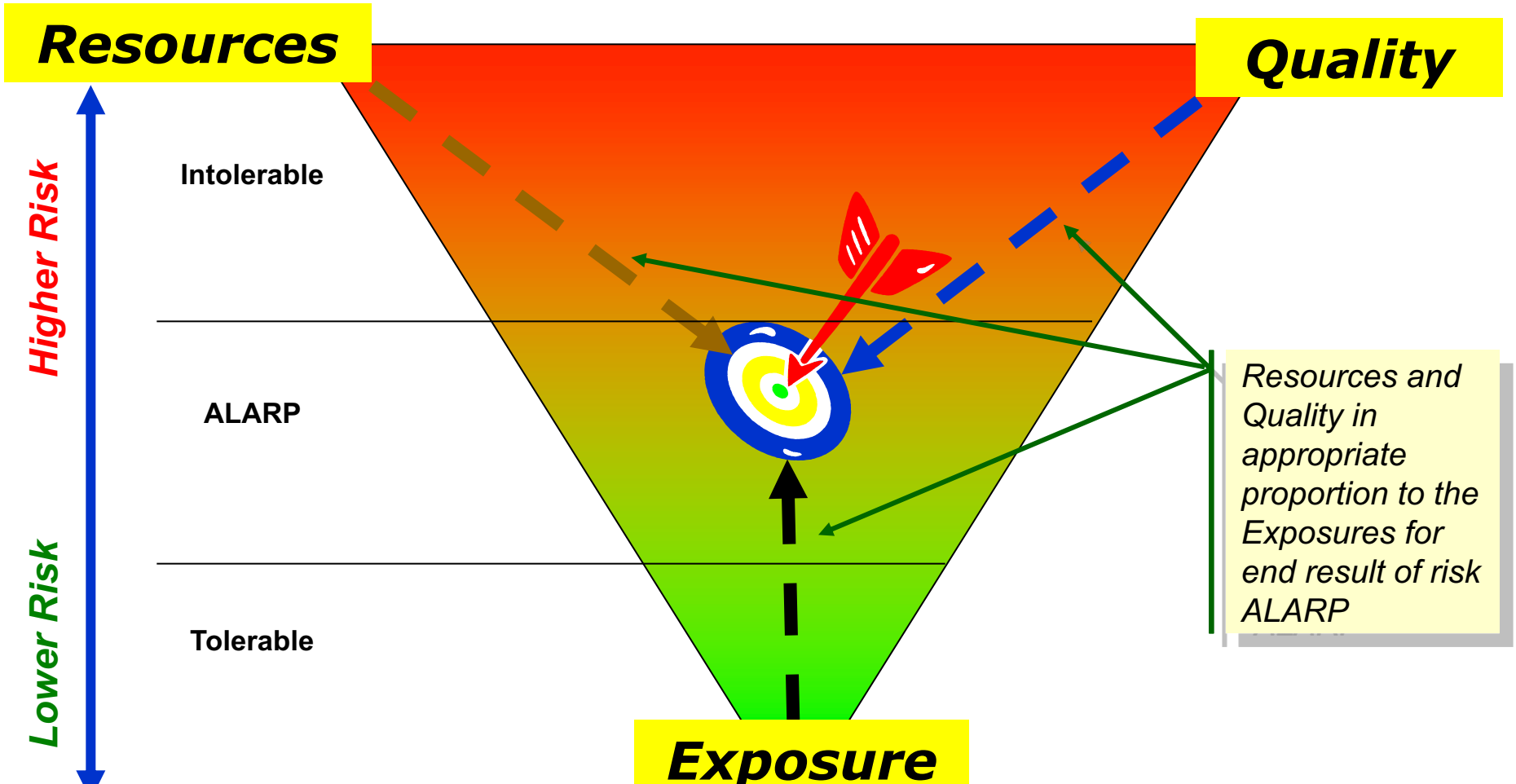
KNOWLEDGE AREAS



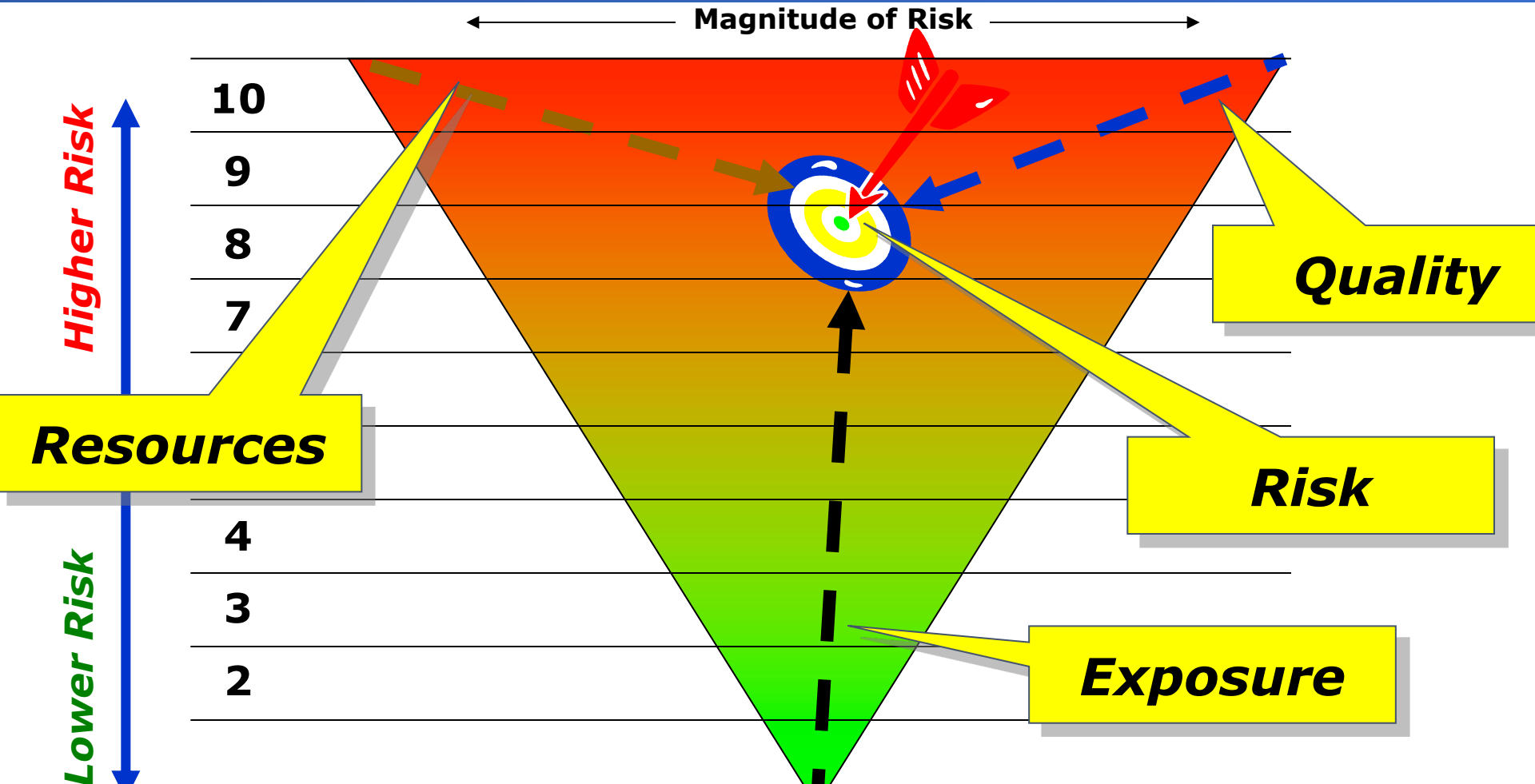
As Low As Reasonably Practicable



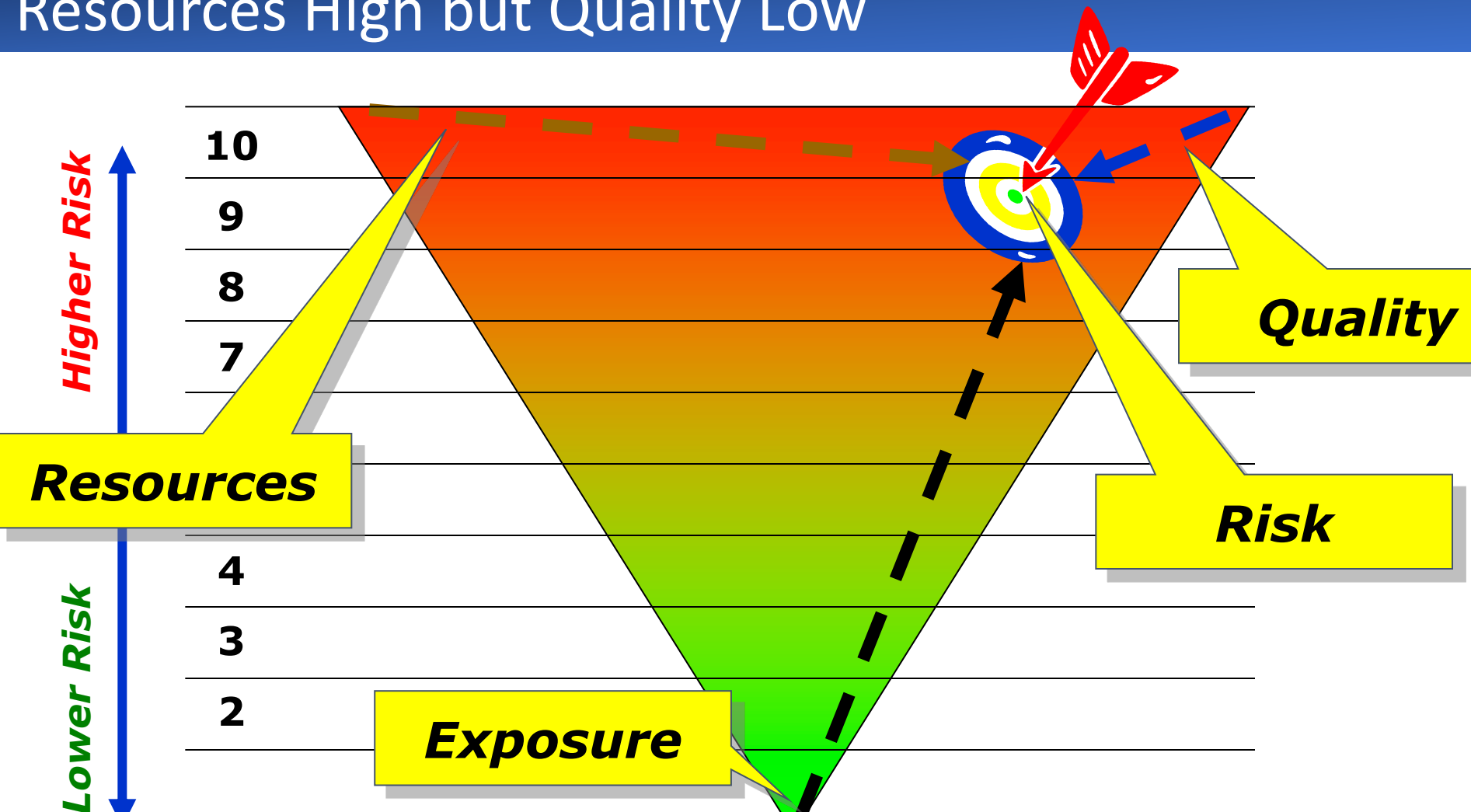
Risk Equilibrium (Optimal Trade-Off)



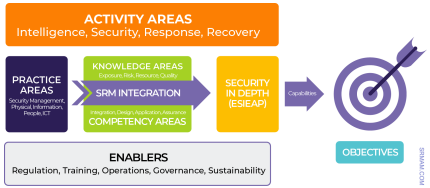
Risk High if Resources & Quality Low

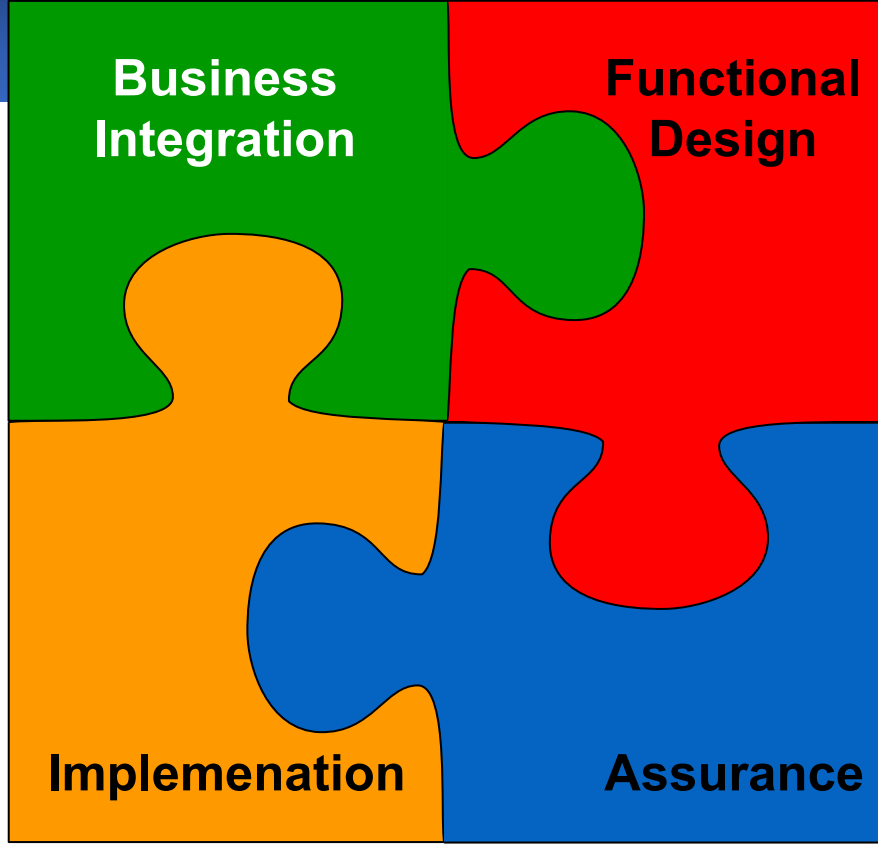


Resources High but Quality Low

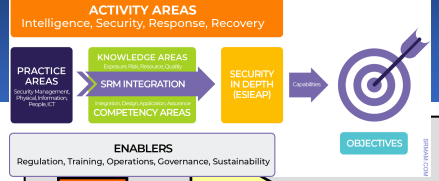


COMPETENCY AREAS





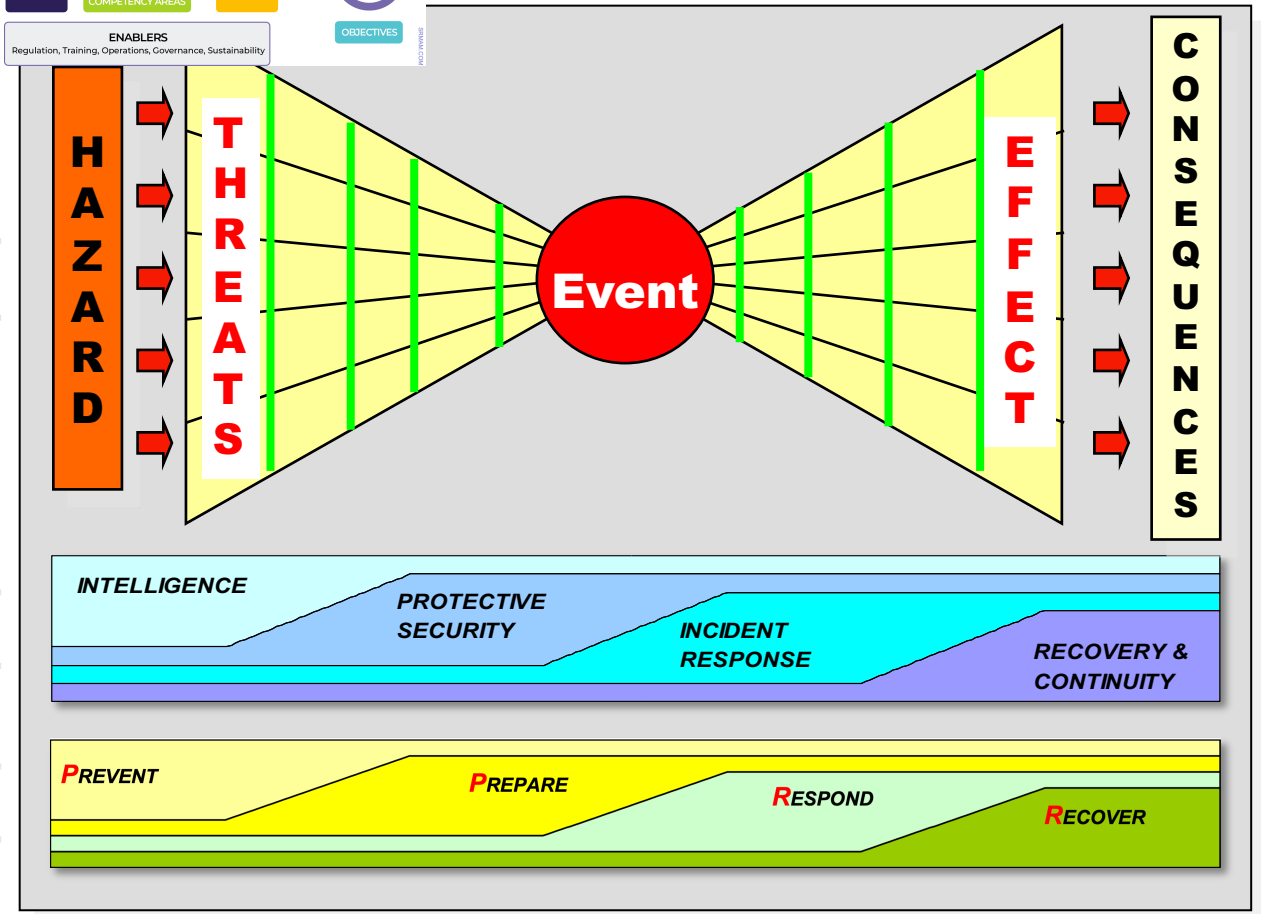
ACTIVITY AREAS

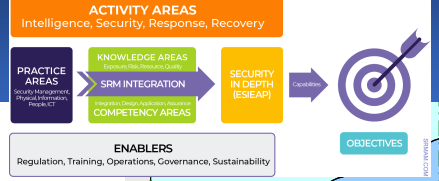


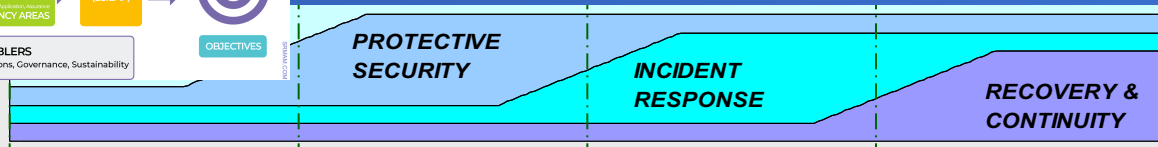
BowTie Model

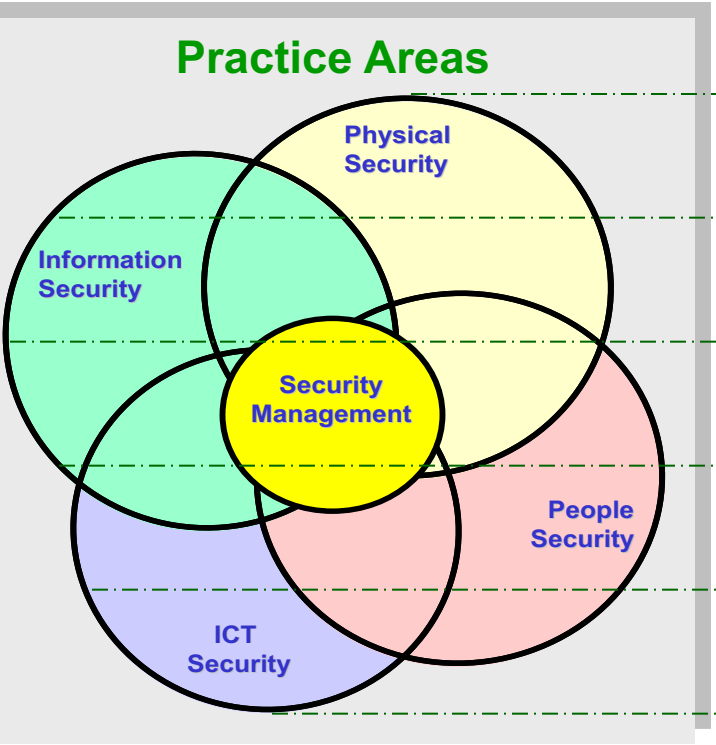
SRMBOK Activity Areas

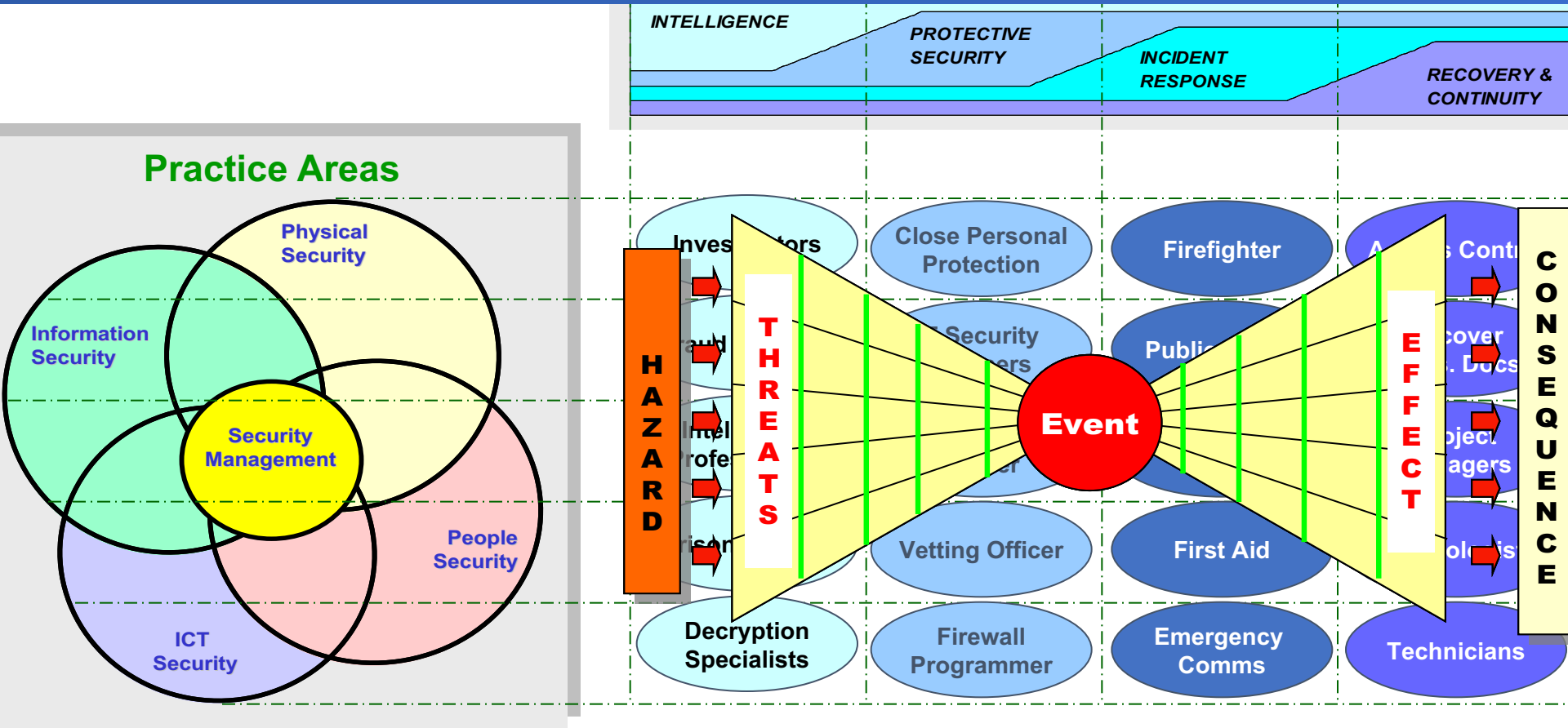
PPRR Model



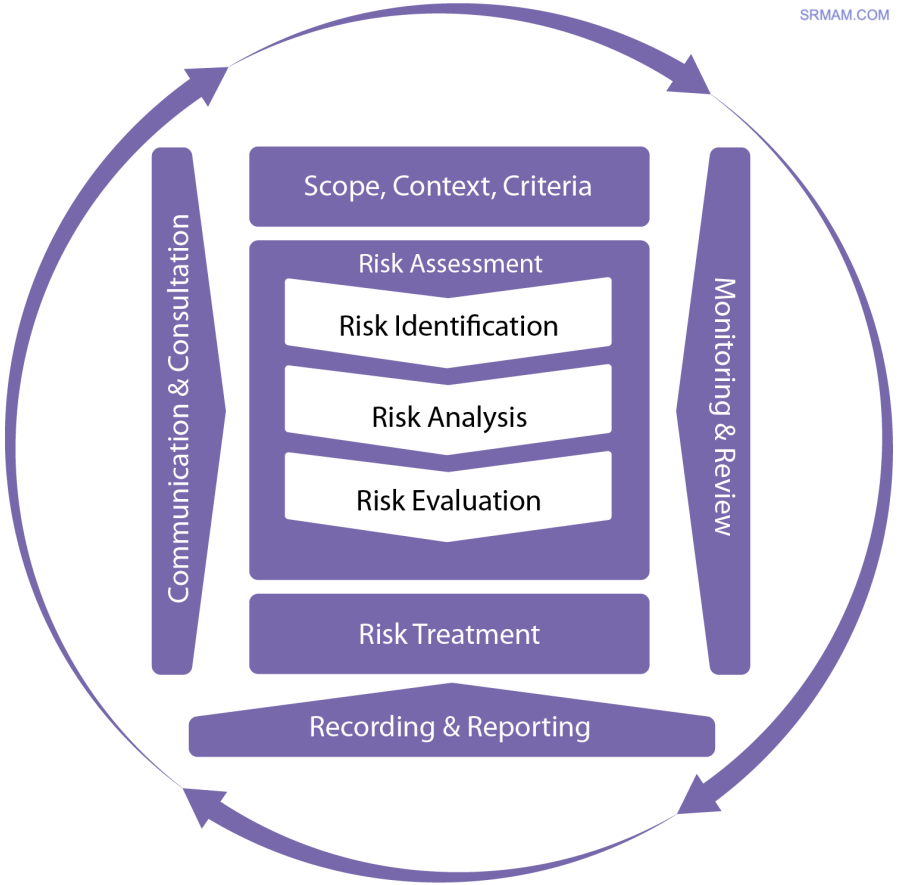

ACTIVITY AREAS
Intelligence, Security, Response, Recovery
PRACTICE AREAS
Security Management, Physical, Information, People, ICT
KNOWLEDGE AREAS
Assets, Risk, Resilience, Quality
SRM INTEGRATION
Integration, Design, Application, Assurance
COMPETENCY AREAS
SECURITY IN DEPTH (ESEAP)
Capabilities
OBJECTIVES
ENABLERS
Regulation, Training, Operations, Governance, Sustainability


PROTECTIVE SECURITY
INCIDENT RESPONSE
RECOVERY & CONTINUITY


Practice Areas
Physical Security
Information Security
Security Management
People Security
ICT Security


INTELLIGENCE
PROTECTIVE SECURITY
INCIDENT RESPONSE
RECOVERY & CONTINUITY
Practice Areas
Physical Security
Information Security
Security Management
People Security
ICT Security
HAZARD
THREATS
Event
EFFECT
CONSEQUENCE
Close Personal Protection
Firefighter
Vetting Officer
First Aid
Decryption Specialists
Firewall Programmer
Emergency Comms
Technicians

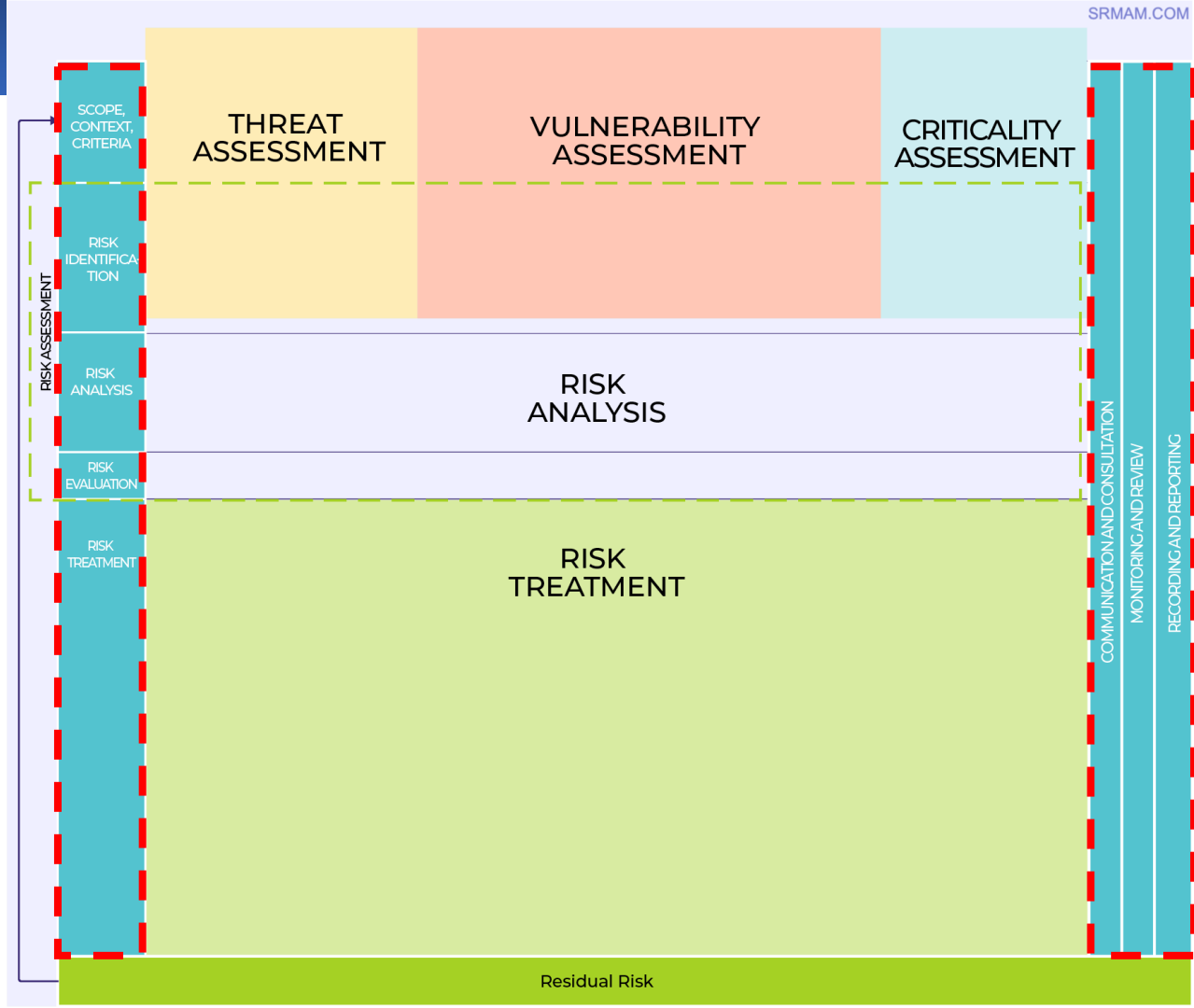
ISO31000:2018 Risk Management Guidelines



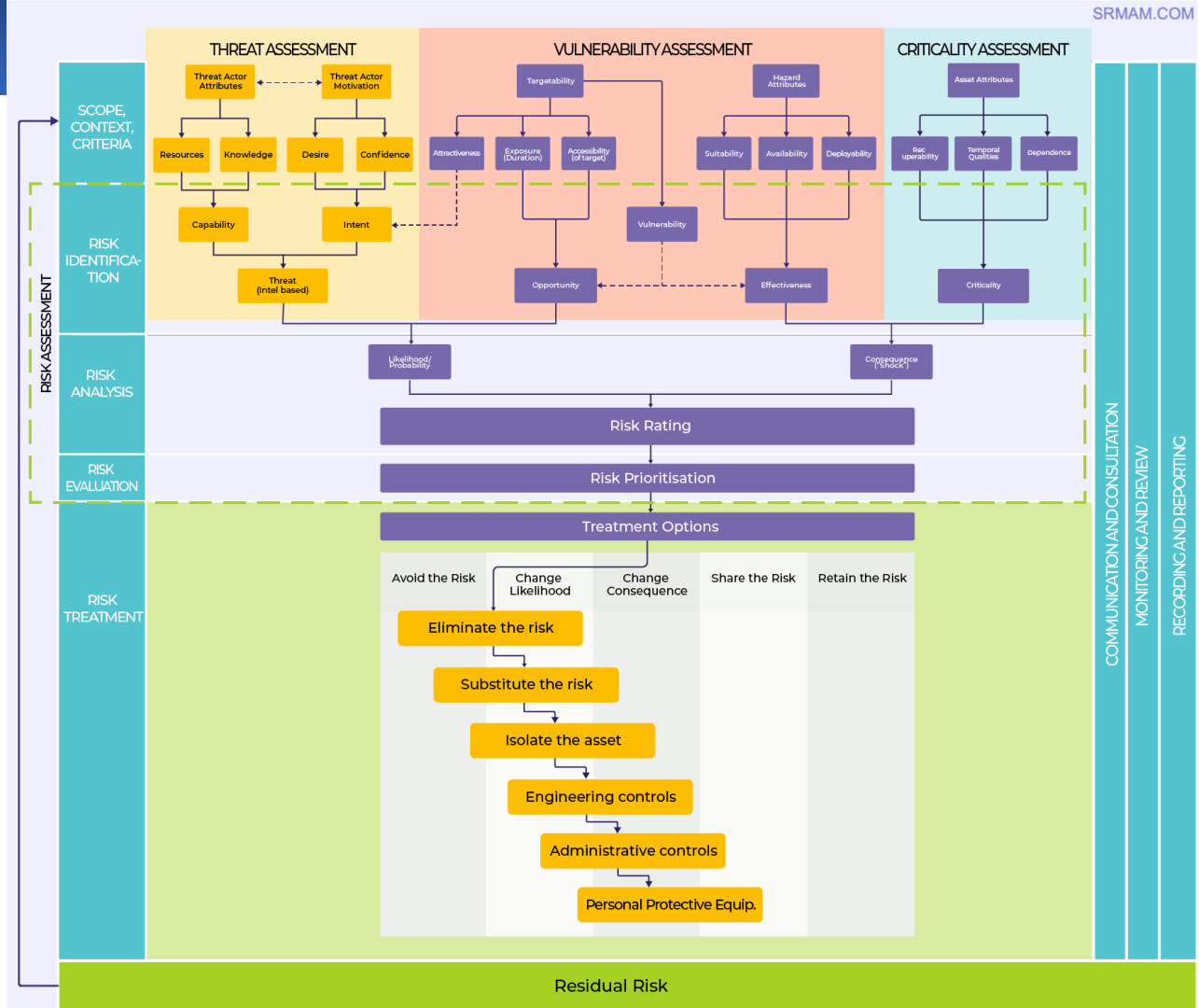
SRM INTEGRATION

Updated from SRMBOK

Security Risk Management Aide-Mémoire (SRMAM)

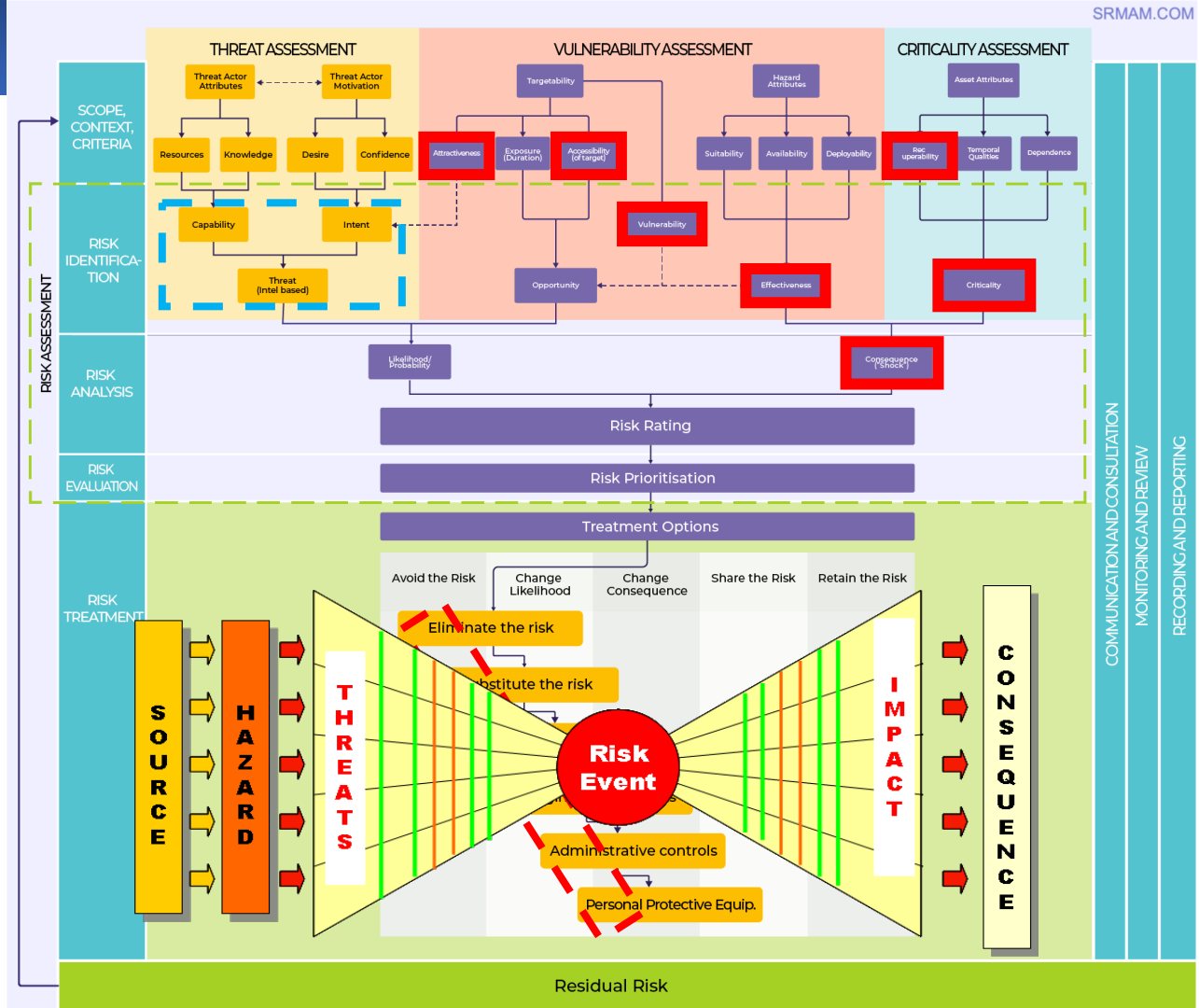


SRM INTEGRATION

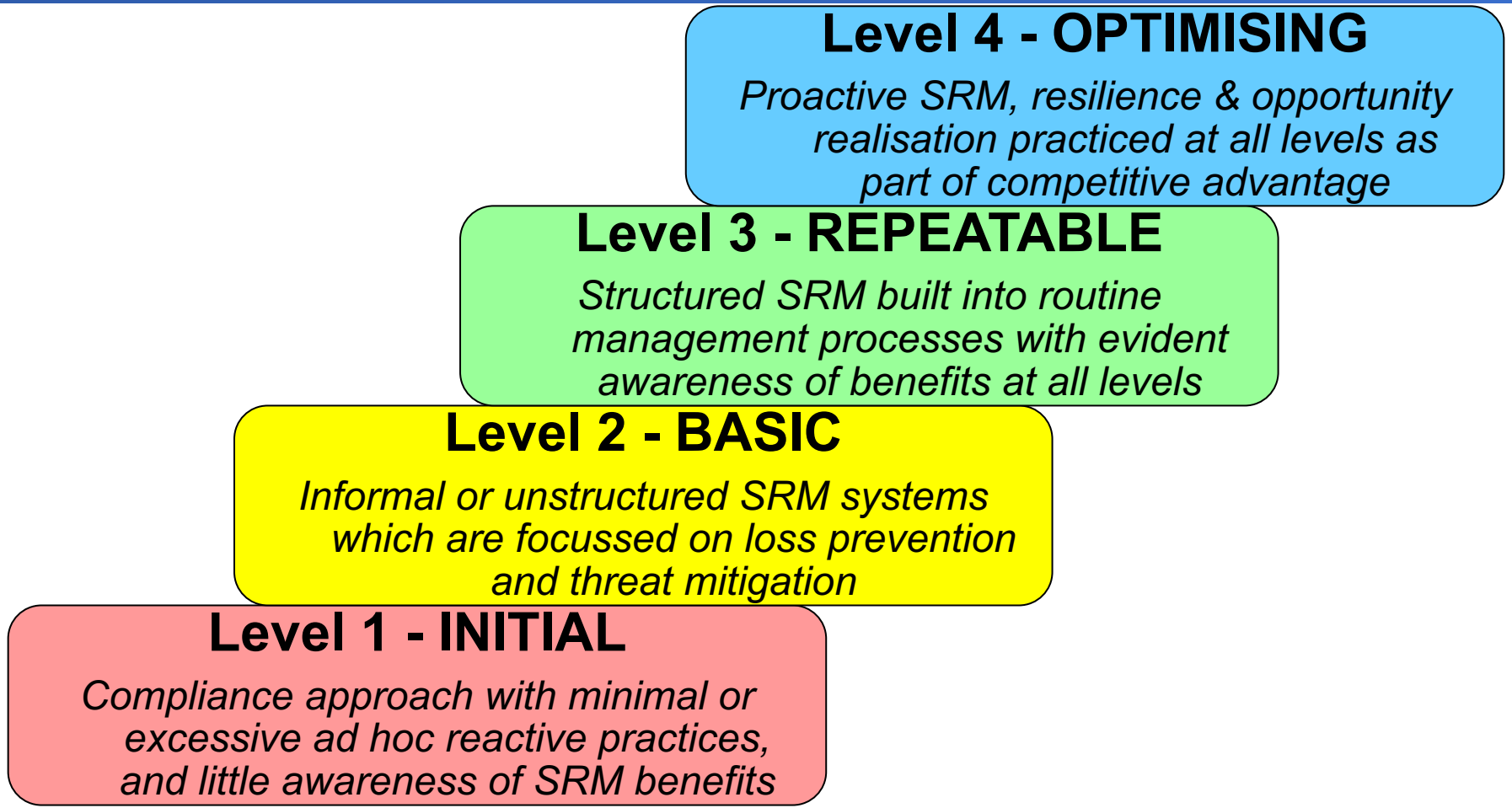


SRM INTEGRATION

- *ISO31000*
- *CARVER*
- *ESIEAP*
- *BOW=TIE*
- *SWISS-CHEESE*
- *THREAT*



SRM Maturity Model



Enterprise Security Specifications

Security Measure / Area Type	Threat Level				
	Low	**Moderate**	**Medium**	**High**	**Extreme**
Building Protection *	**Commercial Grade with back-to-base monitoring**	**Commercial Grade with back-to-base monitoring**	**Type 2**	**Type 2**	**Type 1****
Intruder Resistant Area	Type 2 Alarm system & peripherals				
Secure Room	Type 1 Alarm system & peripherals **NOTES:** * Sensor-activated halogen flood lighting should be installed at both the front and rear of the office/residence to illuminate the immediate grounds area. A command switch for the lighting shall be installed within the house for manual override or for manual use of the lighting. ** For all Type 1 security alarm systems (SAS): ➢Detectors should cover all entrance and exit points. All perimeter doors should be protected with balanced magnetic reed switches. All SAS hardware is to be located in the controlled perimeter ➢A Man-Machine Interface, (keypad), should be located within the residence in close proximity to the main entry door, and should provide for a 30-second delay on entry/exit. If power is lost to the residence, an uninterrupted power supply (UPS) or battery back up system should be used to provide power to the SAS for a minimum of four (4) hours ➢The SAS should be monitored by a host country accredited monitoring station, in accordance with Australian Standard (AS) 2201 or an equivalent specification ➢There should be written procedures in place in the event of an alarm. These may vary in accordance with operational requirements, but they must encompass instructions on contacting the staff and families, and a suitable response. Contingency plans should be put in place in the event of failure of the Type 1 SAS				

Enterprise Security Specifications

		THREAT LEVELS				
		1	2	3	4	5
Intruder Alarm System	VC	S	M	M	M	M-Crypt
	IMG		S	M	M	M-Crypt
	PMV		S	M	M	M-Crypt
	Esp.	S	M	M-Crypt	M-Crypt	M-Crypt

Enterprise Security Postures

SAFETY MEASURE	1	2	3	4	5
Briefings	Upon induction/ recruitment plus on an annual basis, all staff are to be briefed on local security plans and on protective security measures/ practices. Intelligence & Staff Safety summaries provided on each country as required, but no less than quarterly.	All staff to be briefed on change of Alert Level and threat where known. All staff to be reminded to be vigilant/ inquisitive about strangers, to watch out for unidentified or unattended packages and vehicles. Monthly Intelligence & Staff Safety summaries provided on each country.	All staff to be briefed on change of Alert Level and threat where known. All staff to be advised of contingency and emergency response plans, and reminded to be particularly vigilant. Intelligence & Staff Safety summaries provided on each country as required but not less than weekly.	All staff to be briefed on change of Alert Level and specific threat. Intelligence & Staff Safety summaries provided on each country as required but not less than bi-weekly.	All staff to be briefed on change of Alert Level and specific threat. Intelligence & Staff Safety summaries provided on each country as required but not less than daily.
Uniform	No restrictions on the wearing of uniform except that security passes are not to be worn outside of airports.	No restrictions on the wearing of uniform except that security passes are not to be worn outside of airports	No security restrictions on the wearing of uniform, unless the cabin crew manager imposes local restrictions.	No uniforms to be worn outside of airport precincts. Staff are to change within designated lounges.	Consider cancelling flights until Alert Level lowers. Otherwise as per Alert Level 4.

Other Training

- 1 Hour
- 1 Day
- 3 Days
- 5 Days

- Risk Assessment
- Risk Treatment
- Risk Management
- Enterprise Risk Management

ISO31000 Risk Management Standard (Webinar)

Tue, Sep 13, 2022 5:15 PM AEST

Save time and improve profits with risk management software (Webinar)

Wed, Sep 14, 2022 5:15 PM AEST

An Introduction to SRMBOK (Webinar)

Mon, Sep 19, 2022 5:10 PM AEST

ISO31000 Risk Management Standard (Webinar)

Tue, Sep 20, 2022 5:15 PM AEST

Risk Management 101 - The Fundamentals

Fri, Sep 23, 2022 8:30 PM AEST

Risk Management Coaching and Mentoring

Mon, Sep 26, 2022 12:30 PM AEST

Risk Management 101 - The Fundamentals

Mon, Sep 26, 2022 3:00 PM AEST

SRMBOK Security Risk Assessment (Virtual Training)

Tue, Sep 27, 2022 9:00 AM AEST

Starts at A$150.00

ISO31000 Risk Management (Virtual Interactive Training)

Wed, Sep 28, 2022 9:00 AM AEST

Starts at A$100.00

www.juliantalbot.com

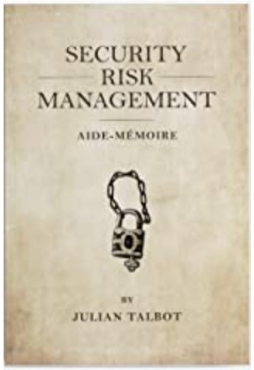
www.srmbok.com

www.sectara.com

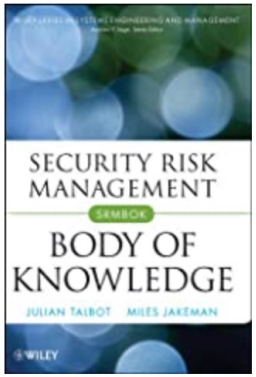
✓ Following

Follow to get new release updates and improved recommendations

Julian Talbot

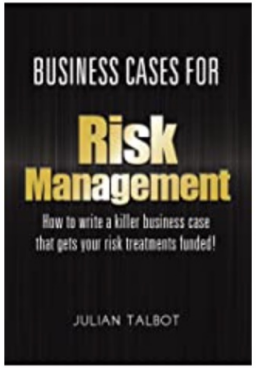


$4.69
Kindle Edition

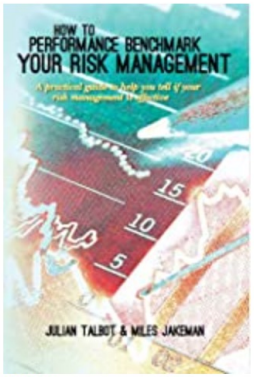


$96.00
Kindle Edition

$4.19
Kindle Edition



$9.99
Kindle Edition



$9.99
Kindle Edition

Julian Talbot CISSP F.ISRM

www.juliantalbot.com