Security Risk Management Masterclass 28JAN20

Julian Talbot

Agenda

- 0830 Introductions & review agenda
- 0900 SRMBOK, ISO31000 updates
- 1030 Morning tea
- 1100 Security Risk Assessments
- 1300 Lunch
- 1400 Career, leadership, promotion, income
- 1600 General discussion
- 1630 Finish

Introductions

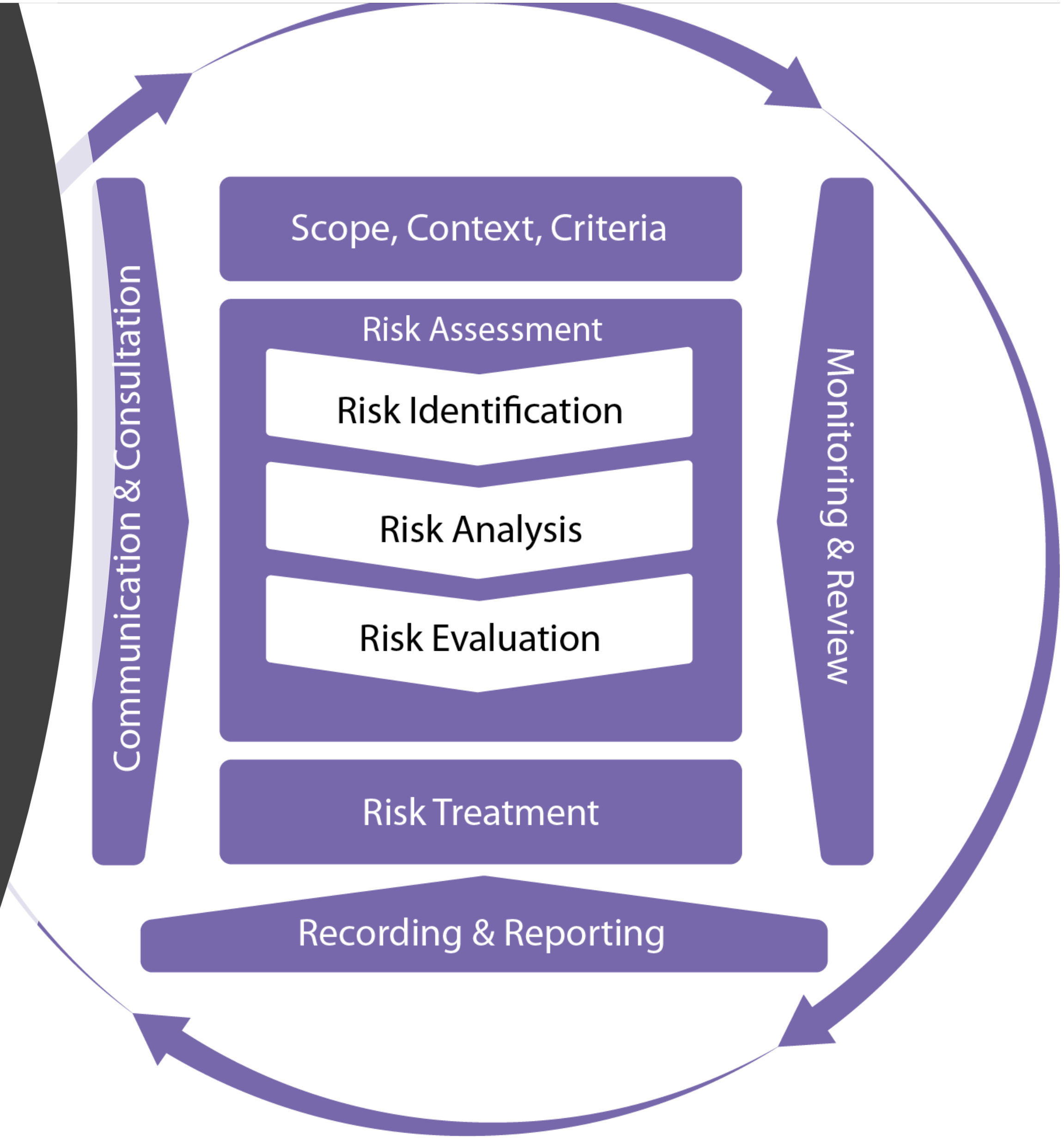
Name

Experience

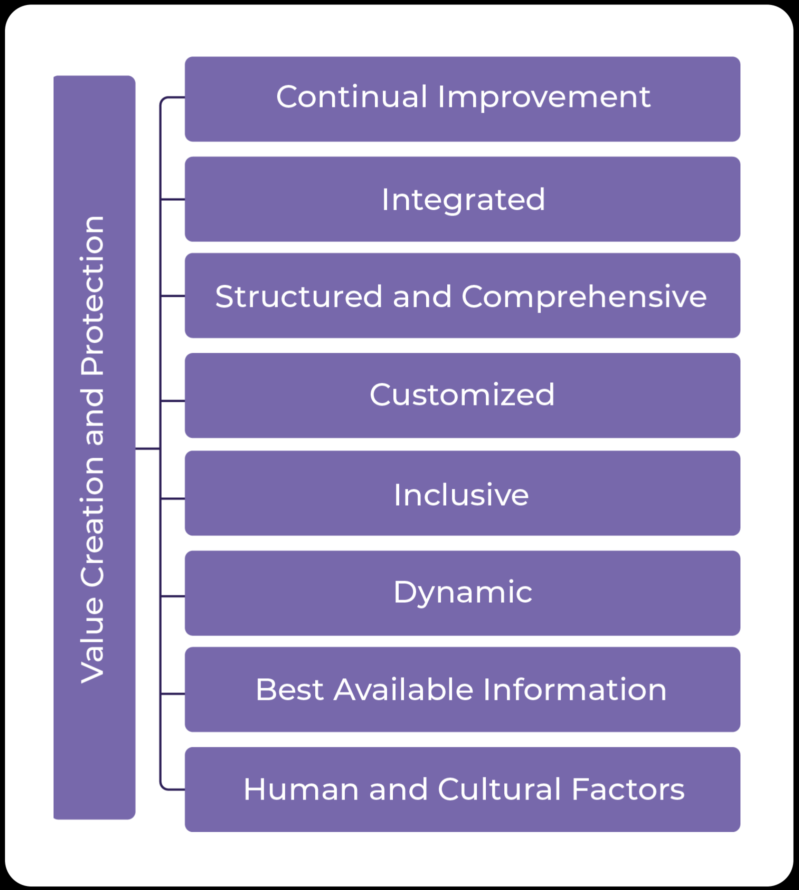
Something unusual about you

Objectives for today

ISO 31000 Process



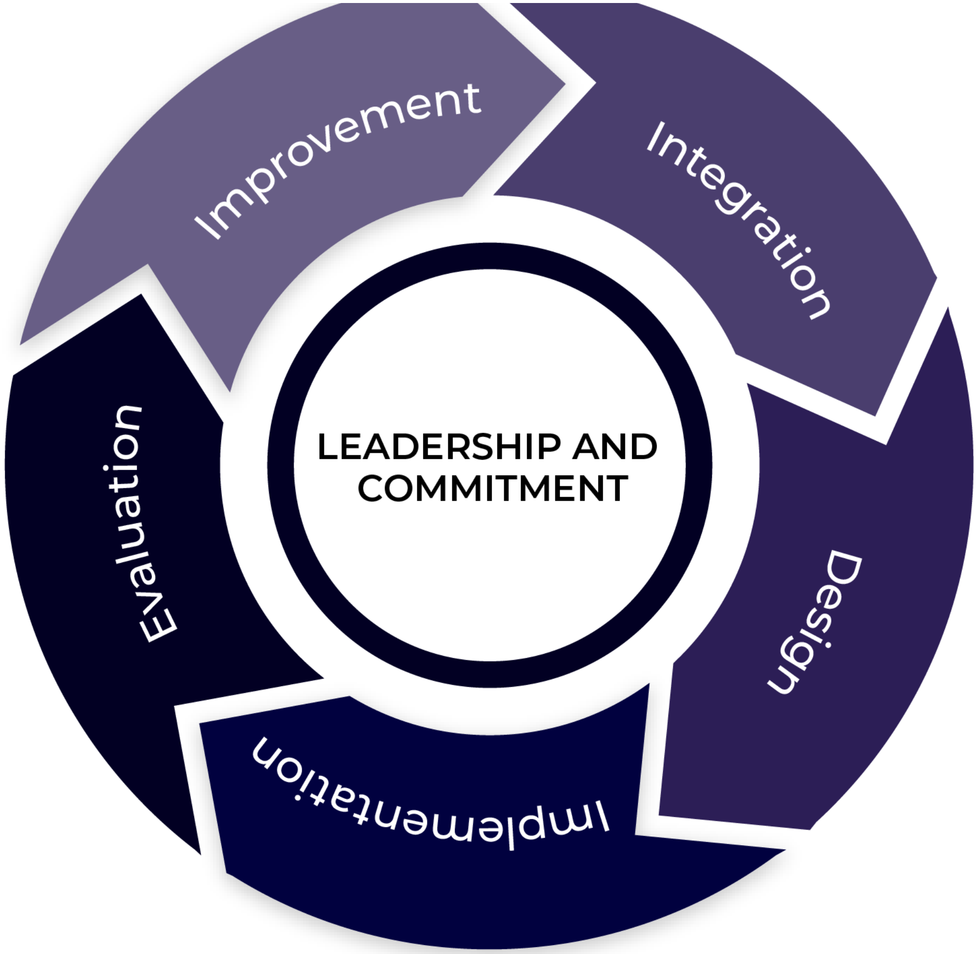
ISO31000 Principles



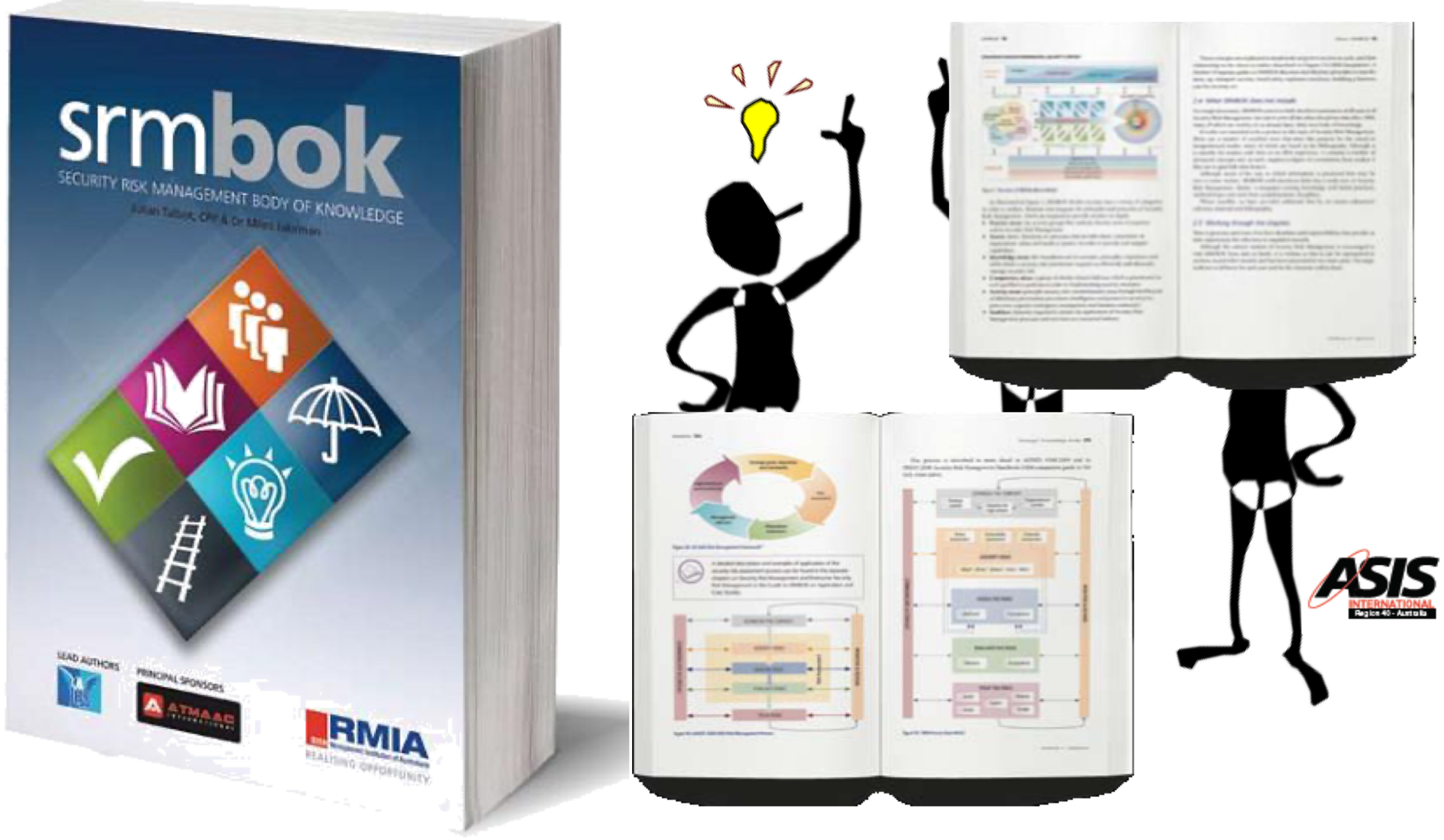
Value Creation and Protection

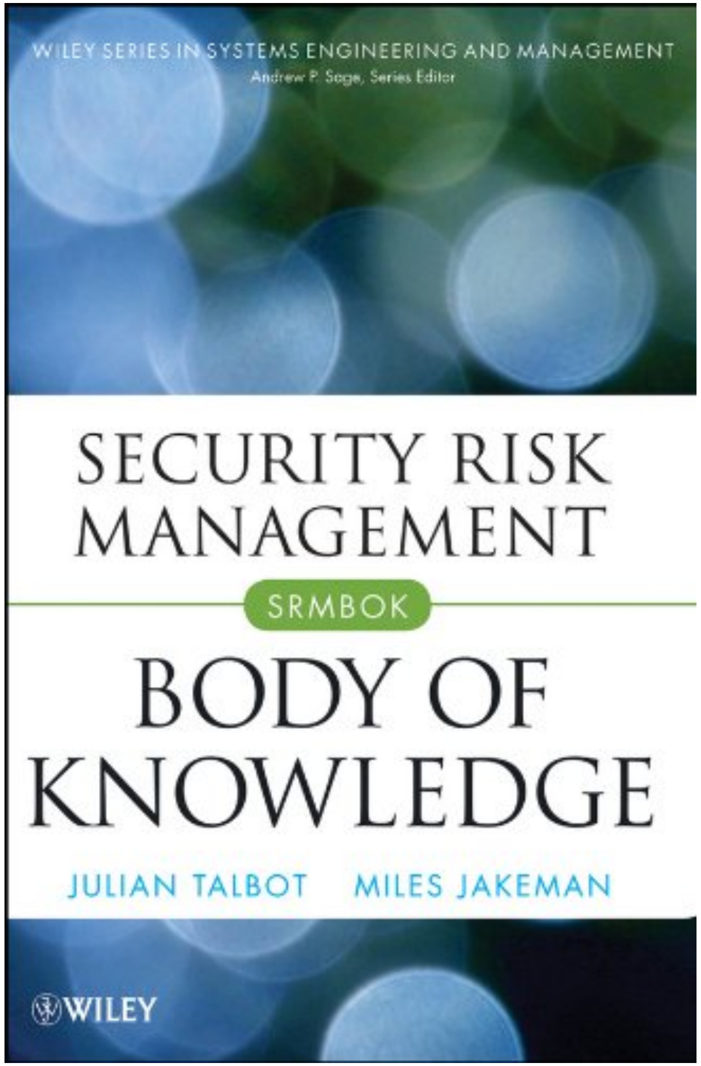
- Continual Improvement
- Integrated
- Structured and Comprehensive
- Customized
- Inclusive
- Dynamic
- Best Available Information
- Human and Cultural Factors

ISO31000 Framework



SRMBOK. In the beginning …





WILEY SERIES IN SYSTEMS ENGINEERING AND MANAGEMENT

Andrew P. Sage, Series Editor

SECURITY RISK MANAGEMENT

SRMBOK

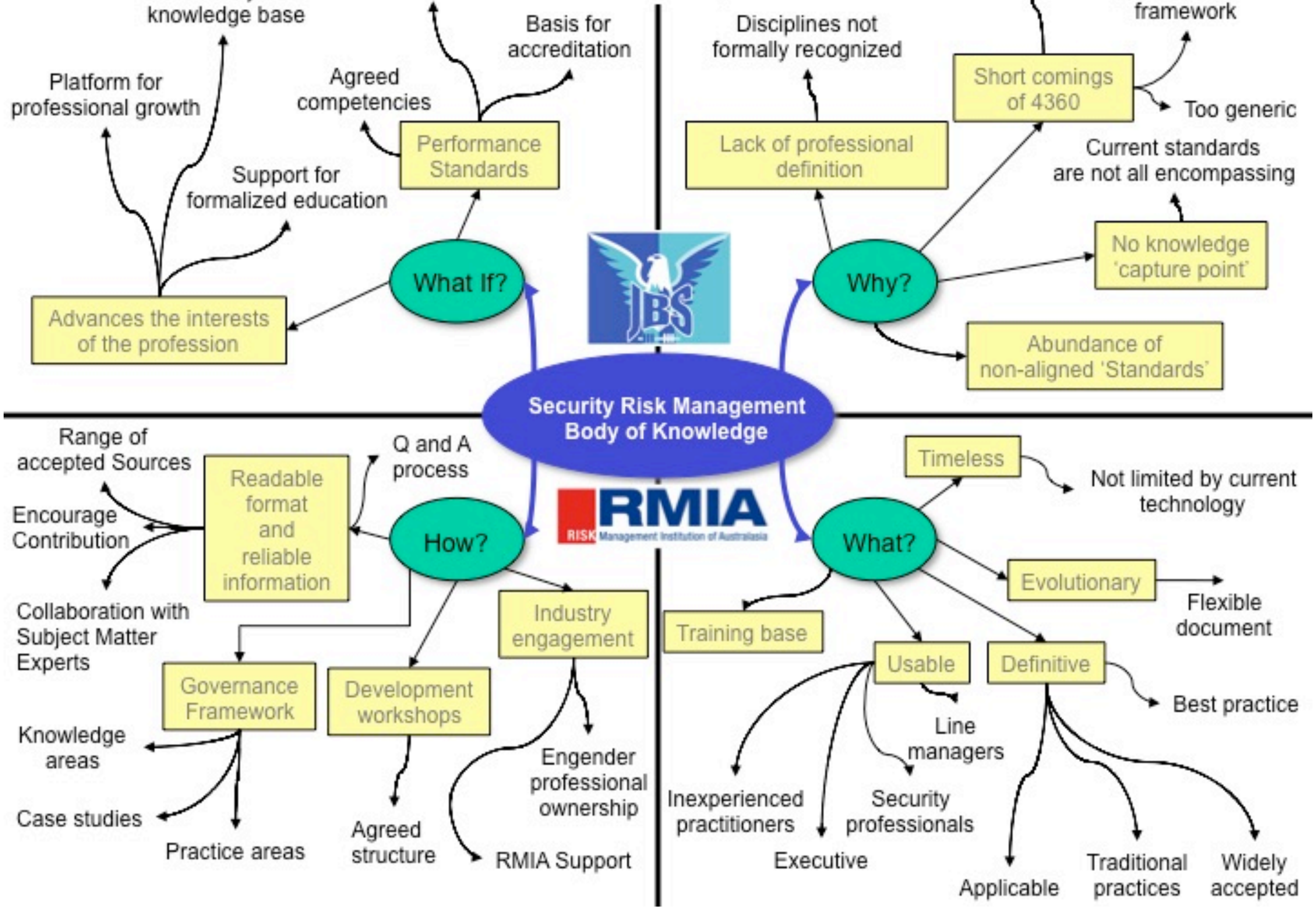
BODY OF KNOWLEDGE

JULIAN TALBOT MILES JAKEMAN

WILEY

Second Edition 2009

Mind Map



Security Risk Management Body of Knowledge

RMIA
RISK Management Institution of Australasia

What If?

Performance Standards

Agreed competencies

Certification

Basis for accreditation

Advances the interests of the profession

Platform for professional growth

Solidify knowledge base

Support for formalized education

Why?

Lack of professional definition

Disciplines not formally recognized

Short comings of 4360

No 'positive' risk

Requires translational framework

Too generic

No knowledge 'capture point'

Current standards are not all encompassing

Abundance of non-aligned 'Standards'

How?

Readable format and reliable information

Range of accepted Sources

Encourage Contribution

Collaboration with Subject Matter Experts

Q and A process

Governance Framework

Knowledge areas

Case studies

Practice areas

Development workshops

Agreed structure

Industry engagement

Engender professional ownership

RMIA Support

What?

Timeless

Not limited by current technology

Evolutionary

Flexible document

Training base

Usable

Line managers

Security professionals

Inexperienced practitioners

Executive

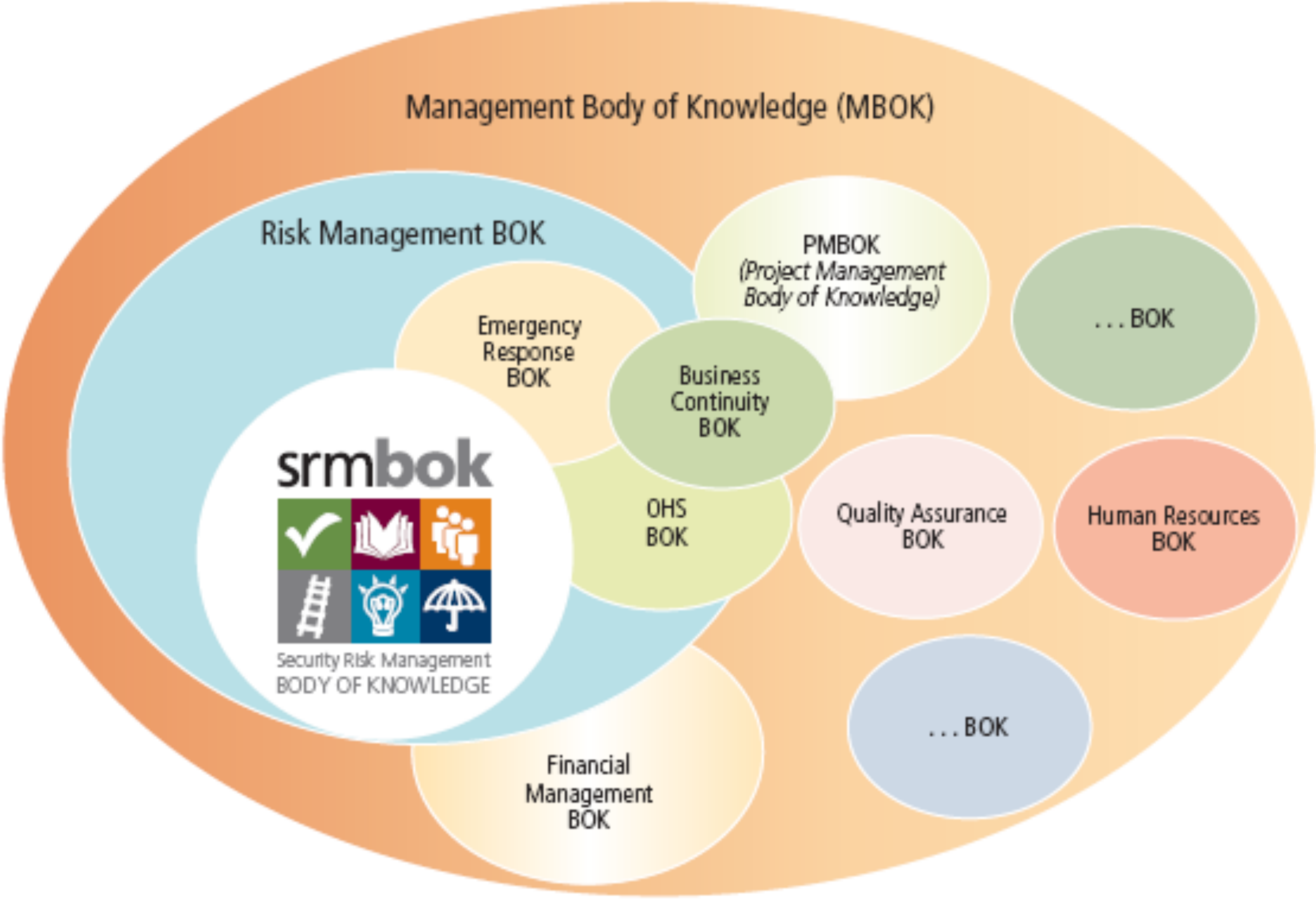
Definitive

Best practice

Applicable

Traditional practices

Widely accepted


Management Body of Knowledge (MBOK)
Risk Management BOK
Emergency Response BOK
PMBOK (Project Management Body of Knowledge)
. . . BOK
Business Continuity BOK
srmbok
Security Risk Management BODY OF KNOWLEDGE
OHS BOK
Quality Assurance BOK
Human Resources BOK
. . . BOK
Financial Management BOK

What SRMBOK includes

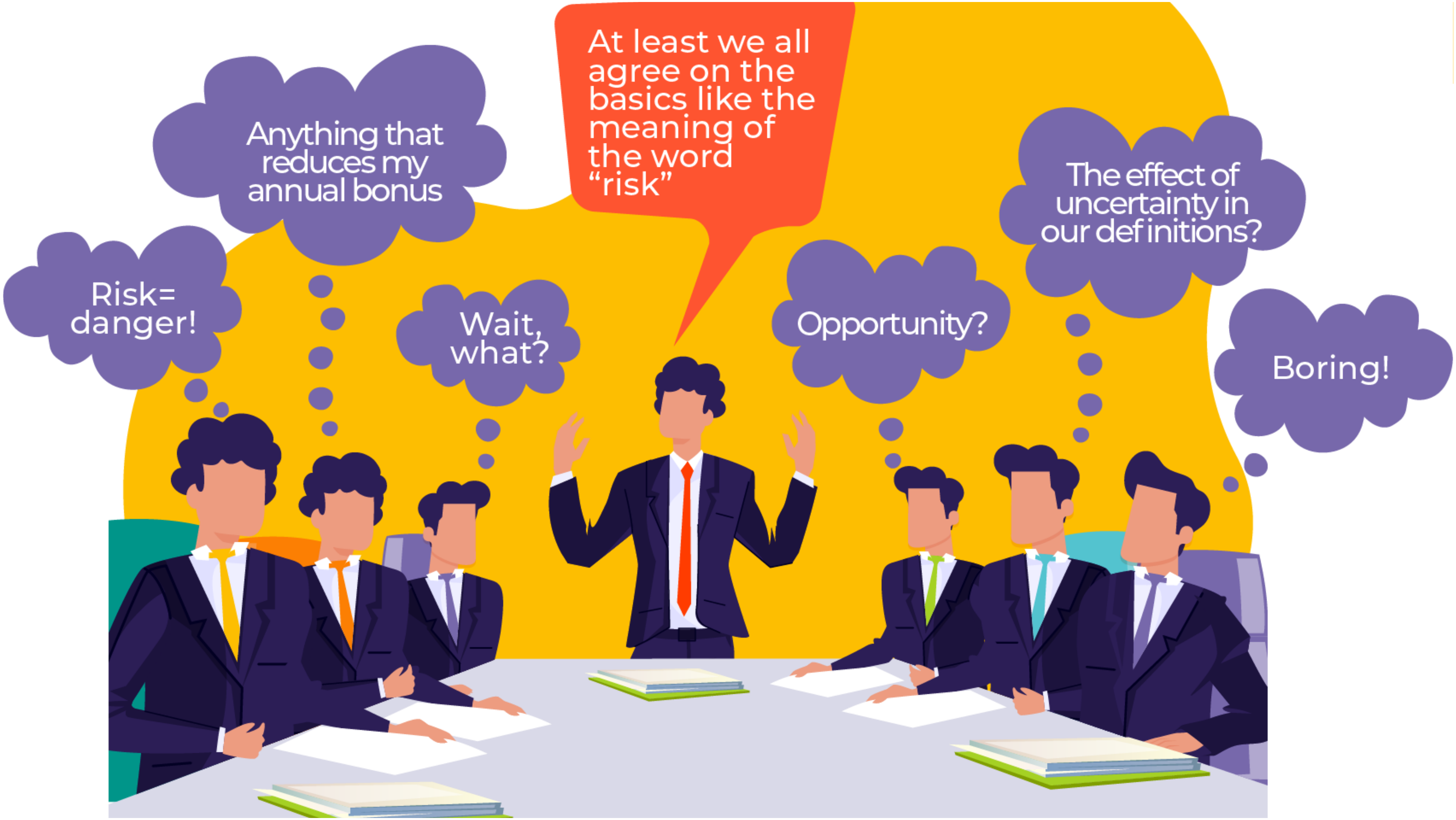
- Introduction and Overview
- SRM Context
- Security Governance
- SRMBOK Framework
- Practice Areas
- Strategic Knowledge Areas
- Operational Competency Areas
- Activity Areas
- SRM Enablers
- Asset Areas
- SRM Integration
- SRM Lexicon
- Sample Templates
- Bibliography

Audience for SRMBOK

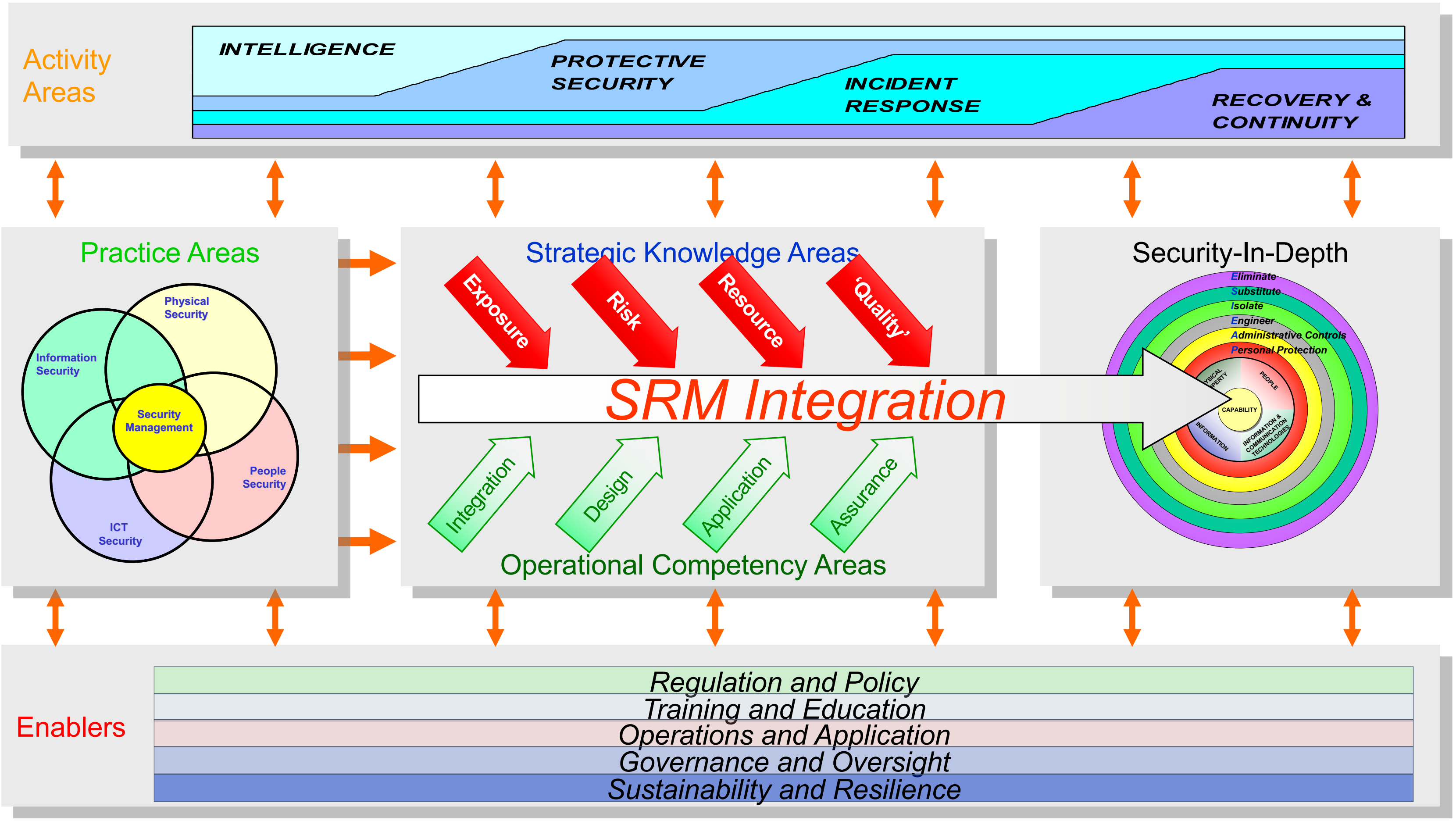
- Security Advisers
- Security Managers
- Line Managers
- Students
- Consultants
- Security professionals
- Directors
- Senior Managers
- Chief Executive Officers
- Chief Security Officers

Terminology

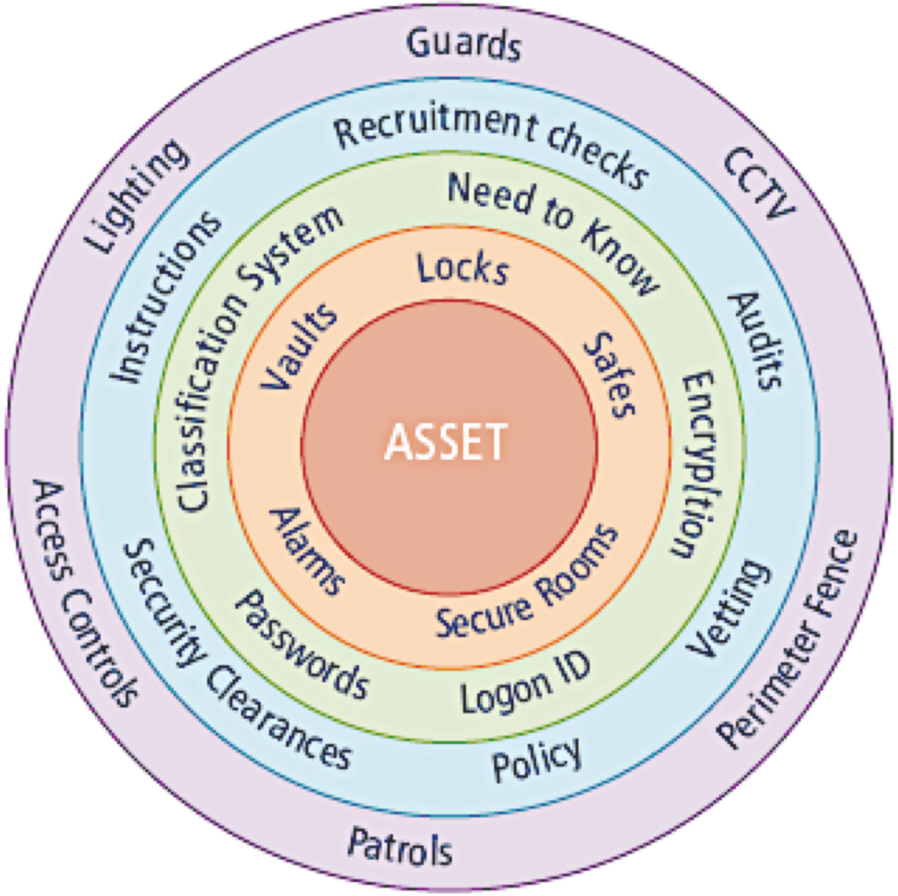
- Risk
- Threat
- Hazard
- Source
- AAAARGH!


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

SRMBOK Framework

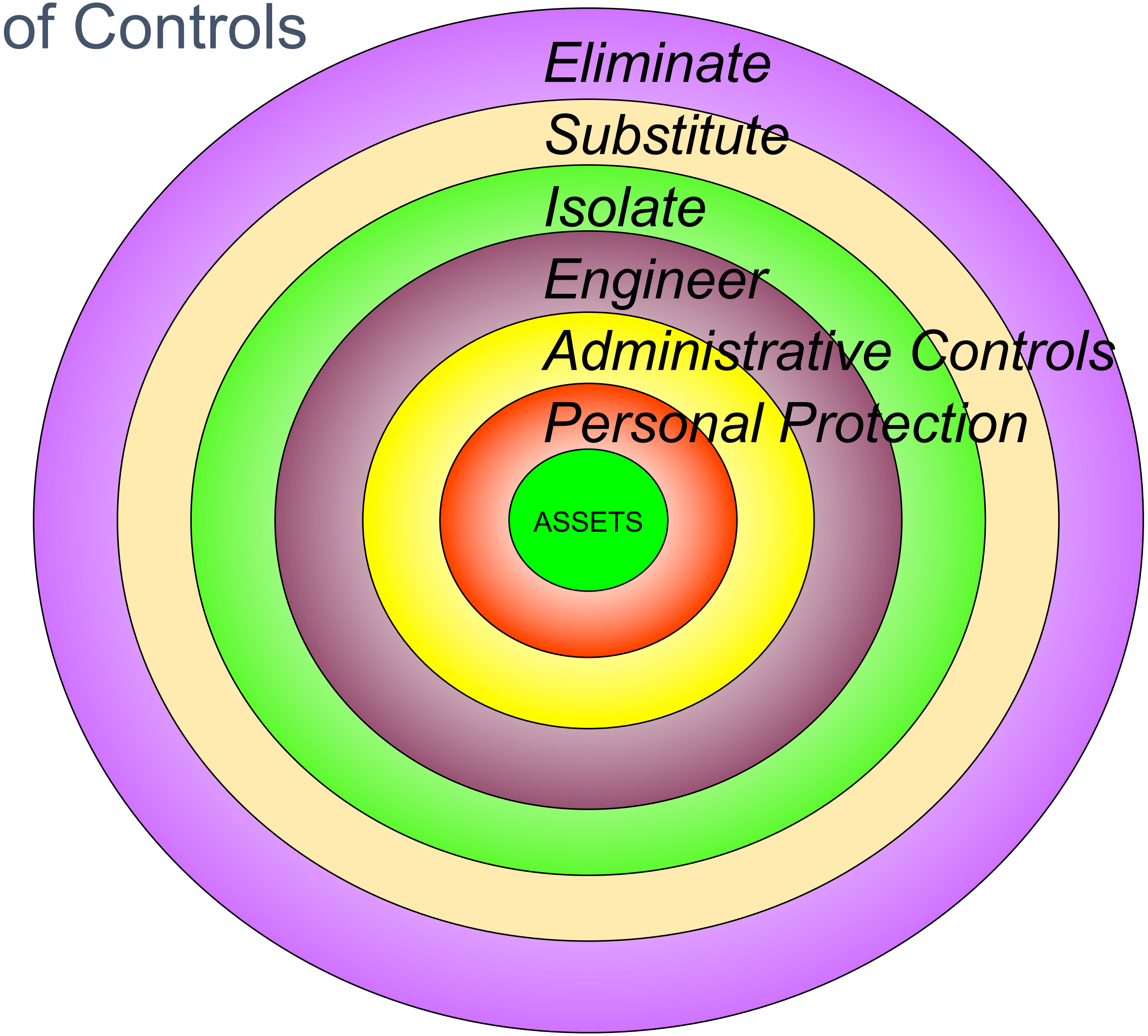


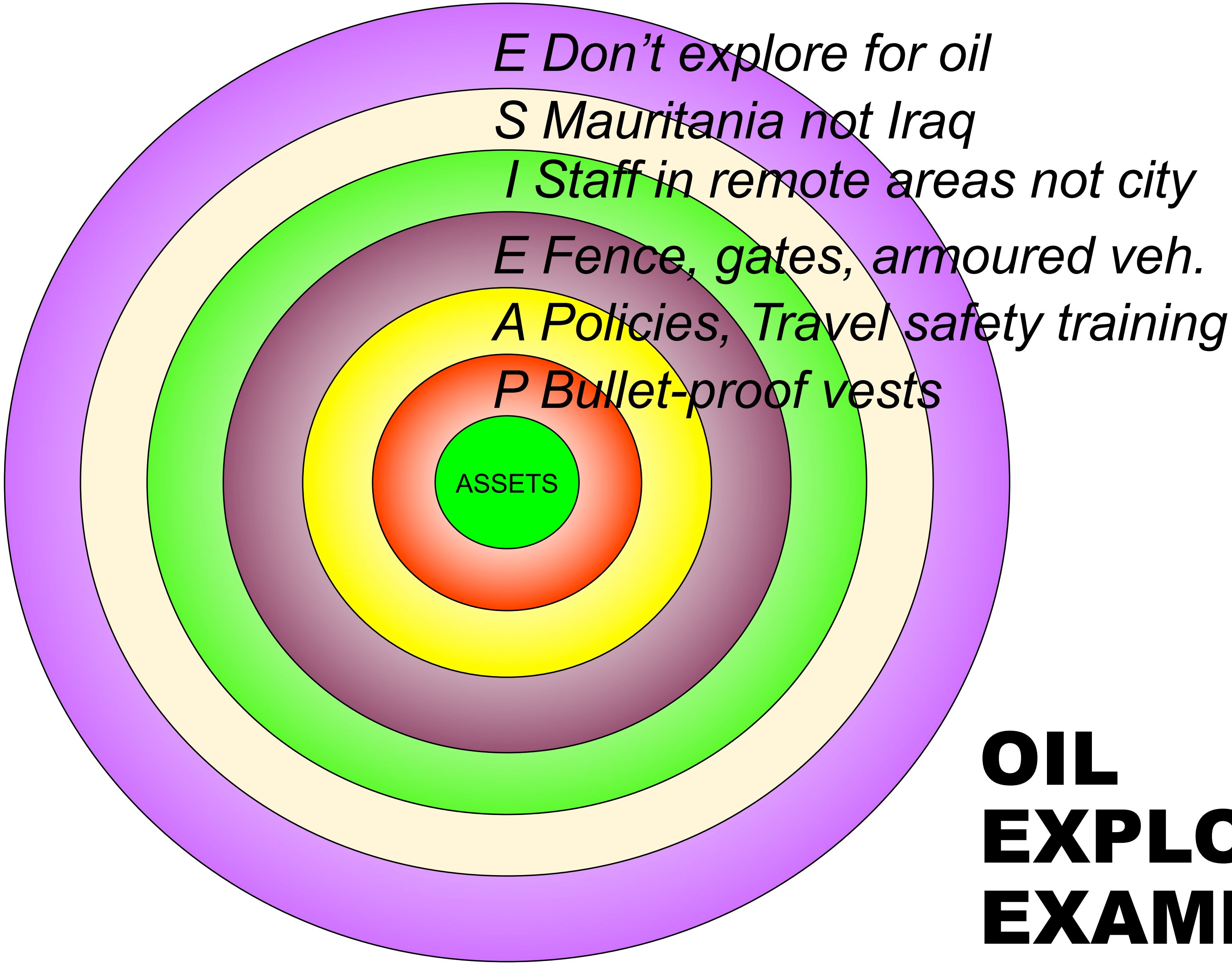
Security In Depth



Hierarchy of Controls

Source: NOHSC





E Don’t explore for oil

S Mauritania not Iraq

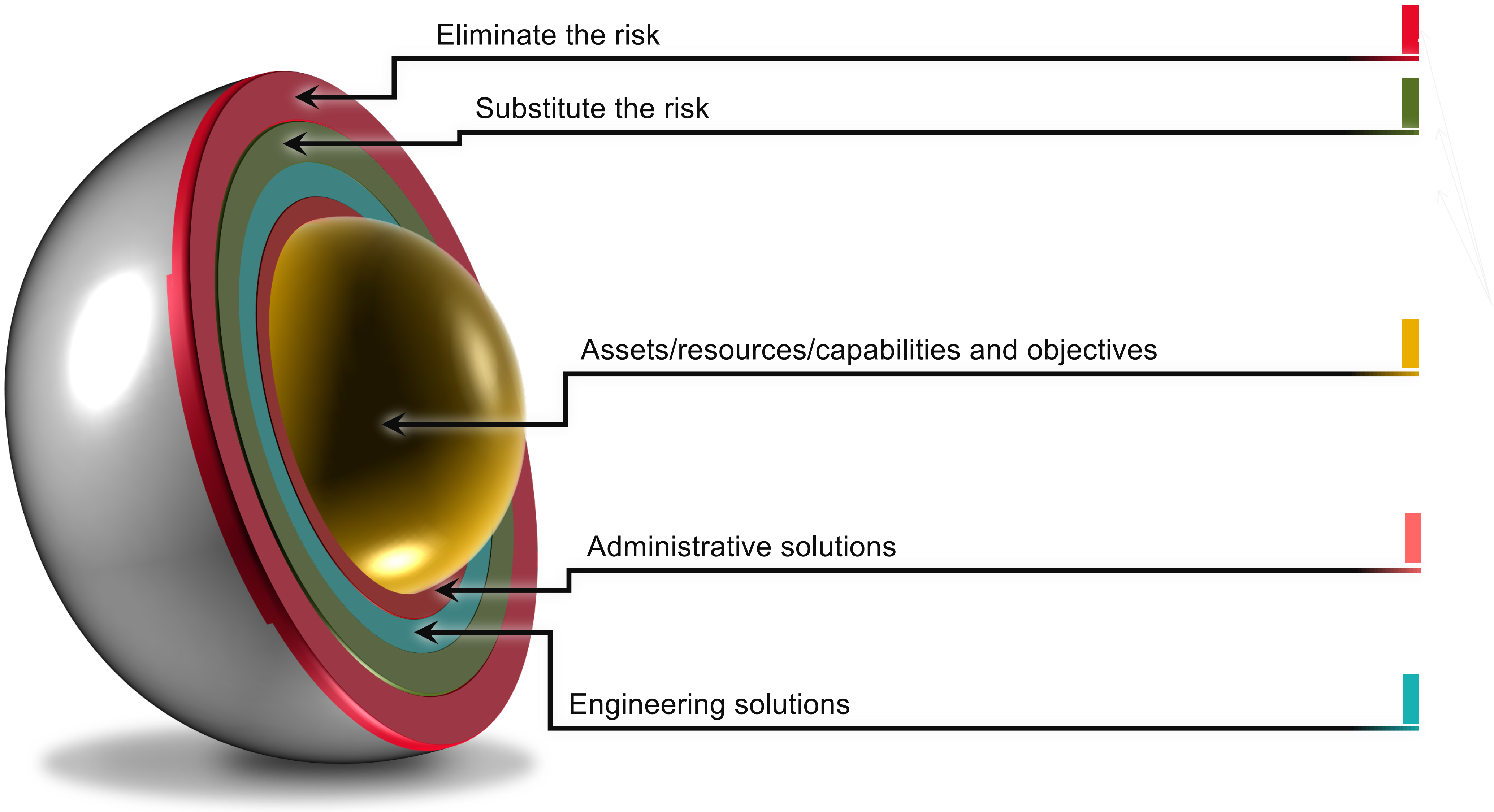
I Staff in remote areas not city

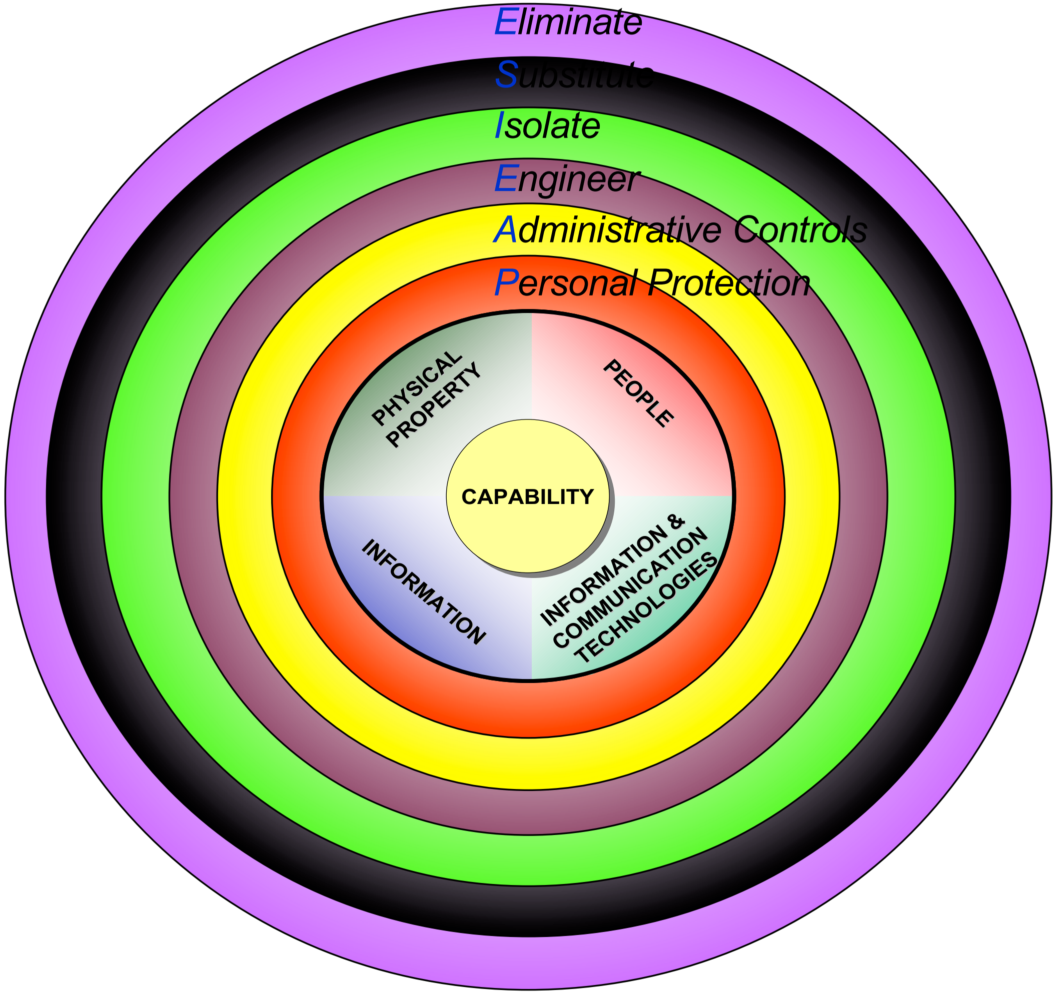
E Fence, gates, armoured veh.

A Policies, Travel safety training

P Bullet-proof vests

OIL EXPLORATION EXAMPLE

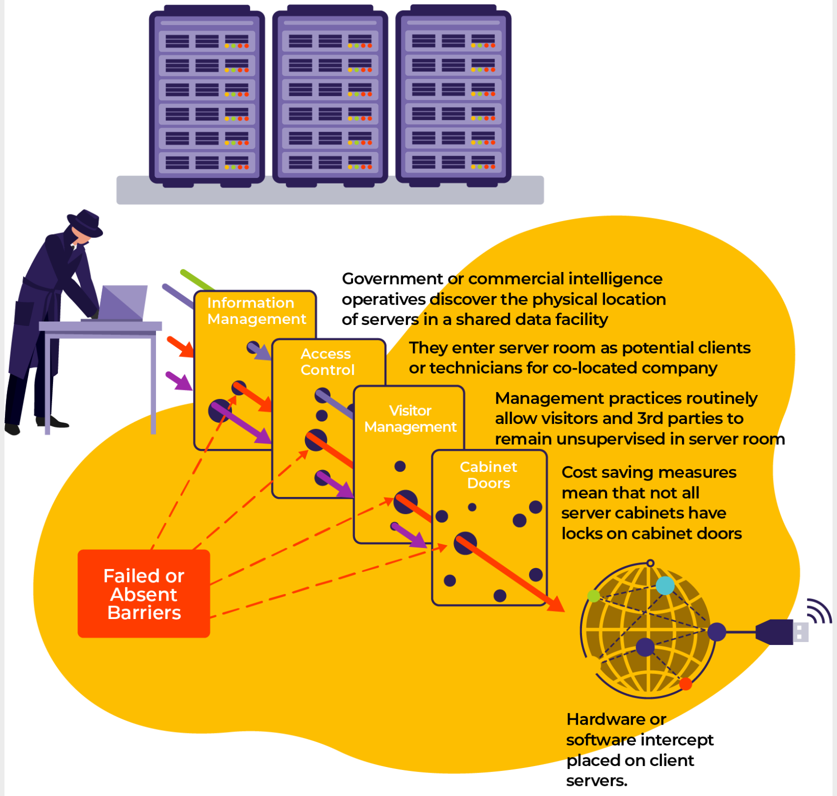

Eliminate the risk
Substitute the risk
Assets/resources/capabilities and objectives
Administrative solutions
Engineering solutions


Eliminate
Substitute
Isolate
Engineer
Administrative Controls
Personal Protection
PHYSICAL PROPERTY
PEOPLE
CAPABILITY
INFORMATION
INFORMATION & COMMUNICATION TECHNOLOGIES

SWISS CHEESE

Swiss-Cheese Example

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



Government or commercial intelligence operatives discover the physical location of servers in a shared data facility

They enter server room as potential clients or technicians for co-located company

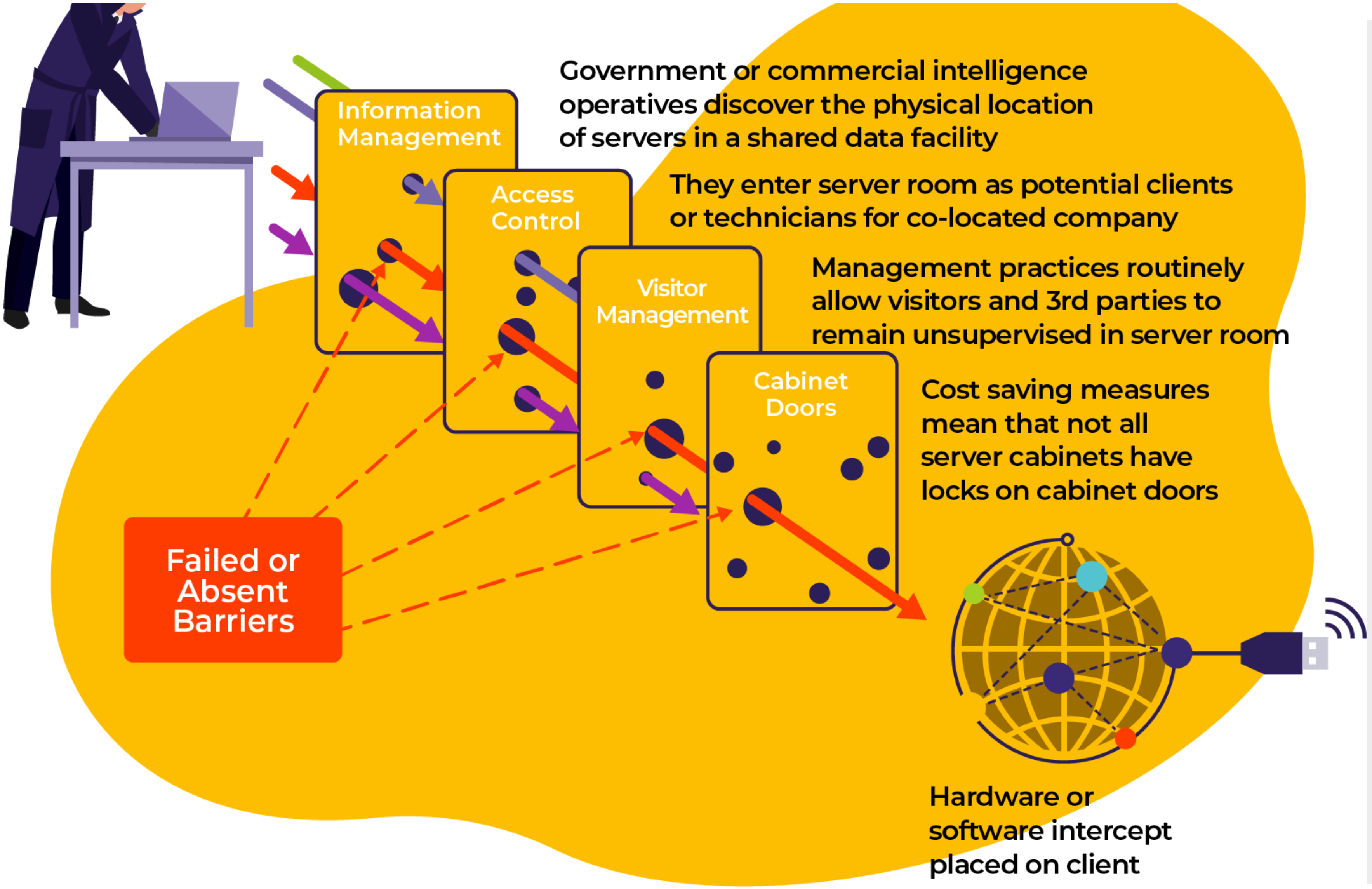
Management practices routinely allow visitors and 3rd parties to remain unsupervised in server room

Cost saving measures mean that not all server cabinets have locks on cabinet doors

Hardware or software intercept placed on client servers.

Customer and corporate records compromised.

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.



Information Management

Access Control

Visitor Management

Cabinet Doors

Failed or Absent Barriers

Government or commercial intelligence operatives discover the physical location of servers in a shared data facility

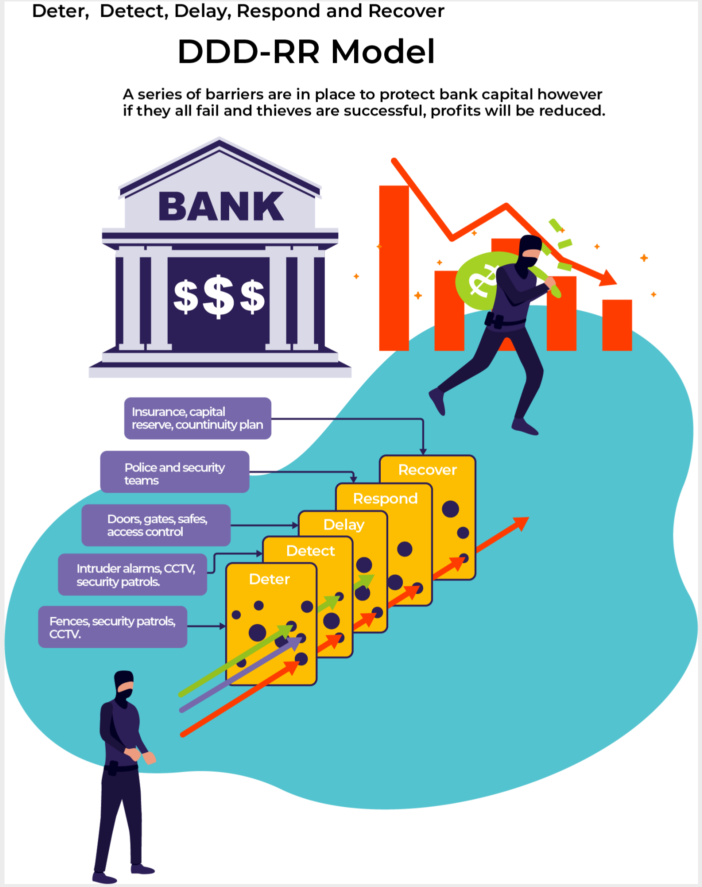
They enter server room as potential clients or technicians for co-located company

Management practices routinely allow visitors and 3rd parties to remain unsupervised in server room

Cost saving measures mean that not all server cabinets have locks on cabinet doors

Hardware or software intercept placed on client servers.

DDDRR



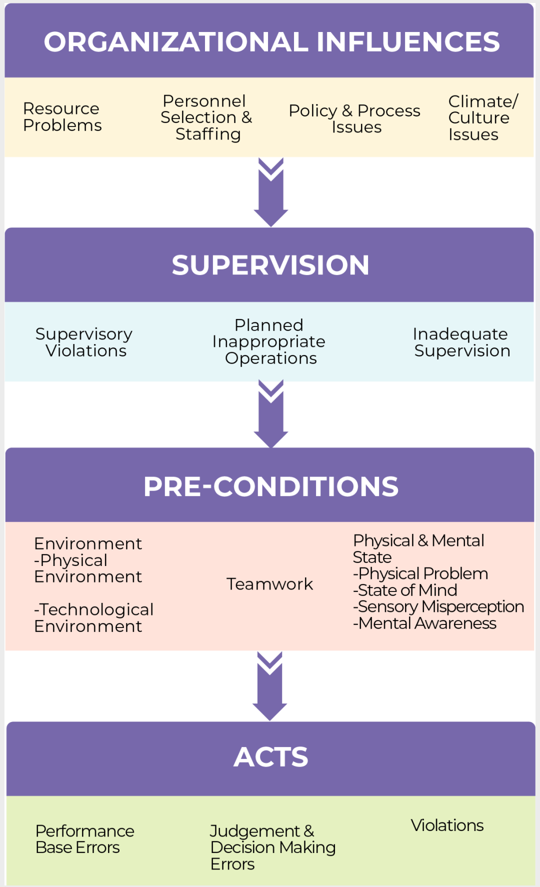
Deter, Detect, Delay, Respond and Recover

DDD-RR Model

A series of barriers are in place to protect bank capital however if they all fail and thieves are successful, profits will be reduced.

BANK
$$$
Insurance, capital reserve, countinuity plan
Police and security teams
Doors, gates, safes, access control
Intruder alarms, CCTV, security patrols.
Fences, security patrols, CCTV.
Recover
Respond
Delay
Detect
Deter

HFACS



ORGANIZATIONAL INFLUENCES

Resource Problems

Personnel Selection & Staffing

Policy & Process Issues

Climate/ Culture Issues

SUPERVISION

Supervisory Violations

Planned Inappropriate Operations

Inadequate Supervision

PRE-CONDITIONS

Environment
-Physical Environment

-Technological Environment

Teamwork

Physical & Mental State
-Physical Problem
-State of Mind
-Sensory Misperception
-Mental Awareness

ACTS

Performance Base Errors

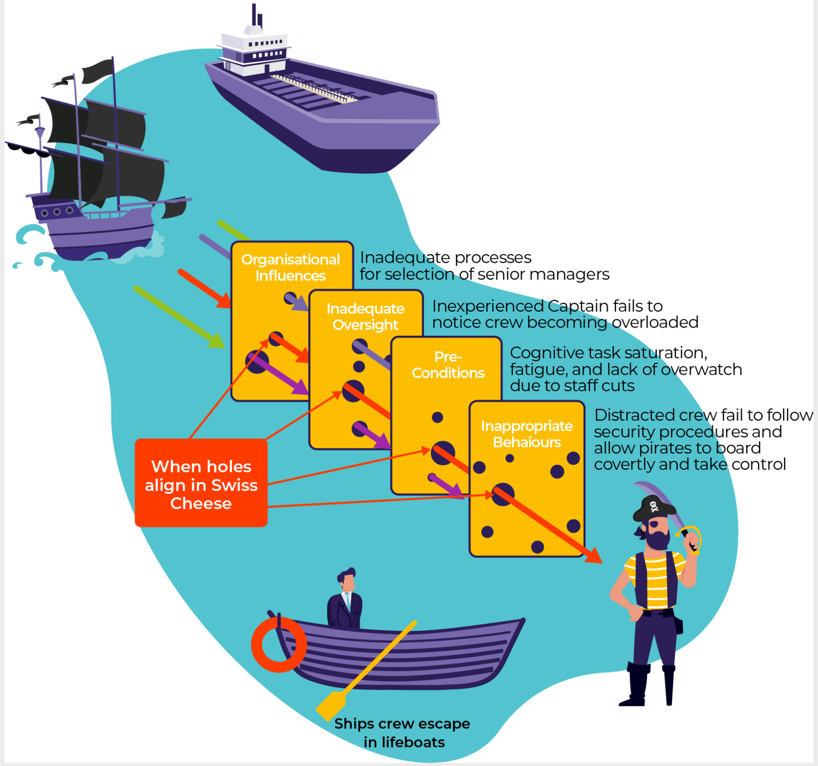
Judgement & Decision Making Errors

Violations

HUMAN FACTORS ANALYSIS CLASSIFICATION SYSTEM

Human Factors

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



Organisational Influences

Inadequate processes for selection of senior managers

Inadequate Oversight

Inexperienced Captain fails to notice crew becoming overloaded

Pre-Conditions

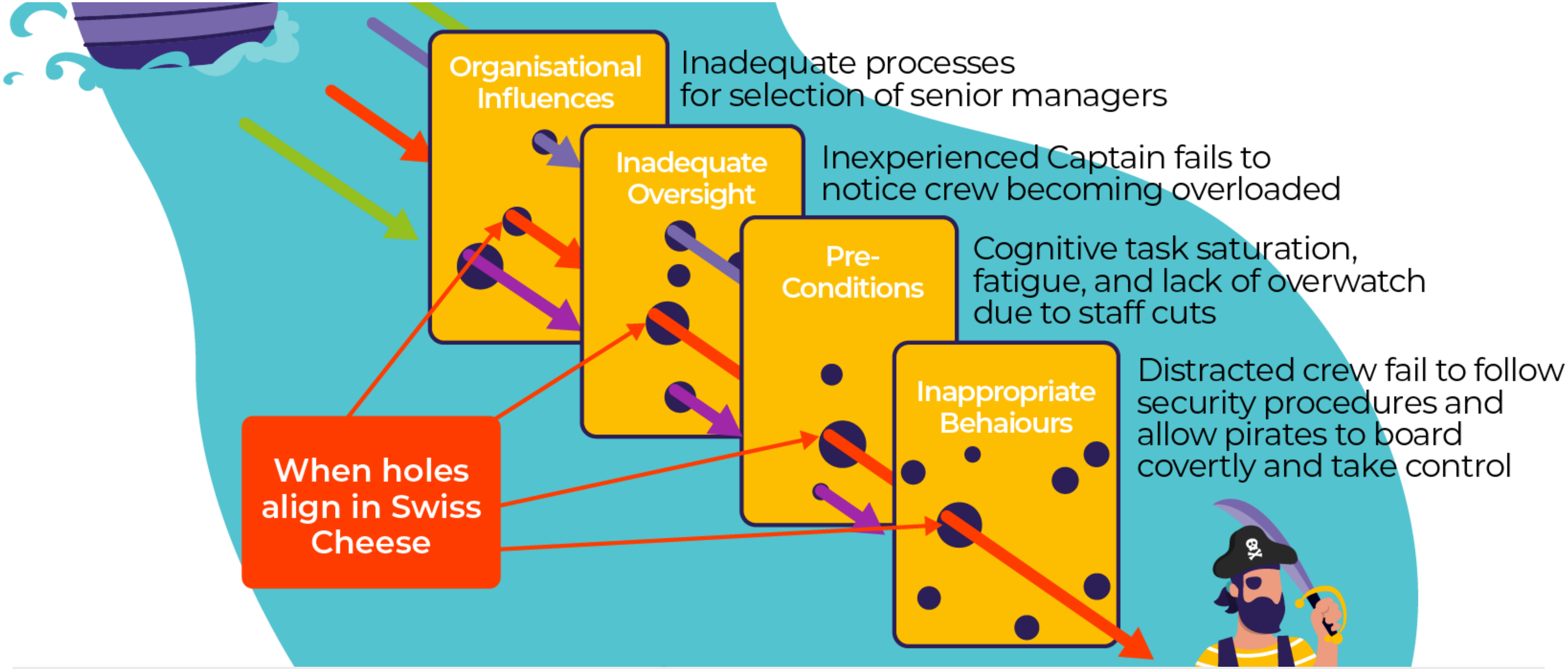
Cognitive task saturation, fatigue, and lack of overwatch due to staff cuts

Inappropriate Behaiours

Distracted crew fail to follow security procedures and allow pirates to board covertly and take control

When holes align in Swiss Cheese

Ships crew escape in lifeboats



Organisational Influences

Inadequate processes
for selection of senior managers

Inadequate Oversight

Inexperienced Captain fails to
notice crew becoming overloaded

Pre-Conditions

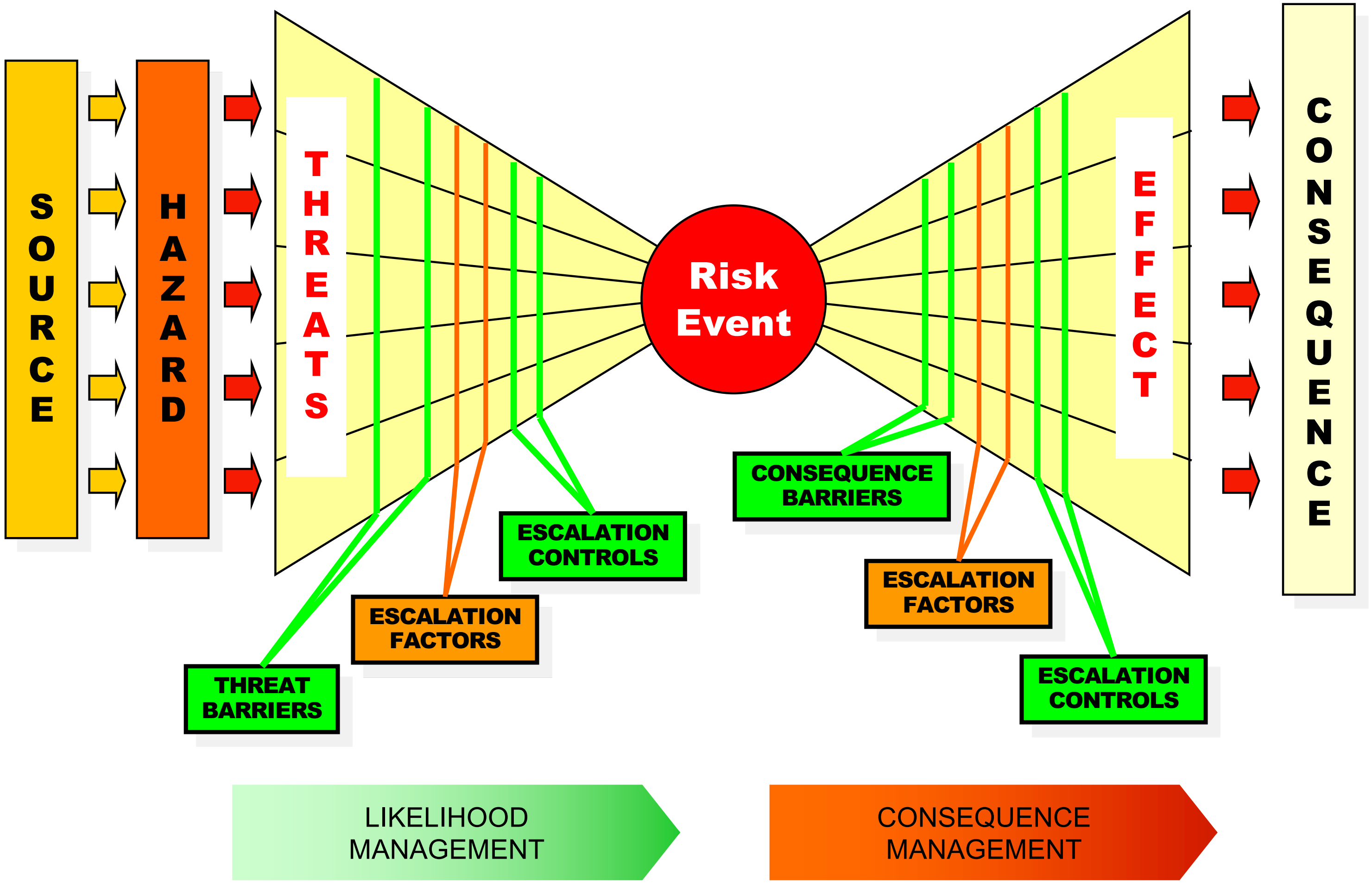
Cognitive task saturation,
fatigue, and lack of overwatch
due to staff cuts

Inappropriate Behaiours

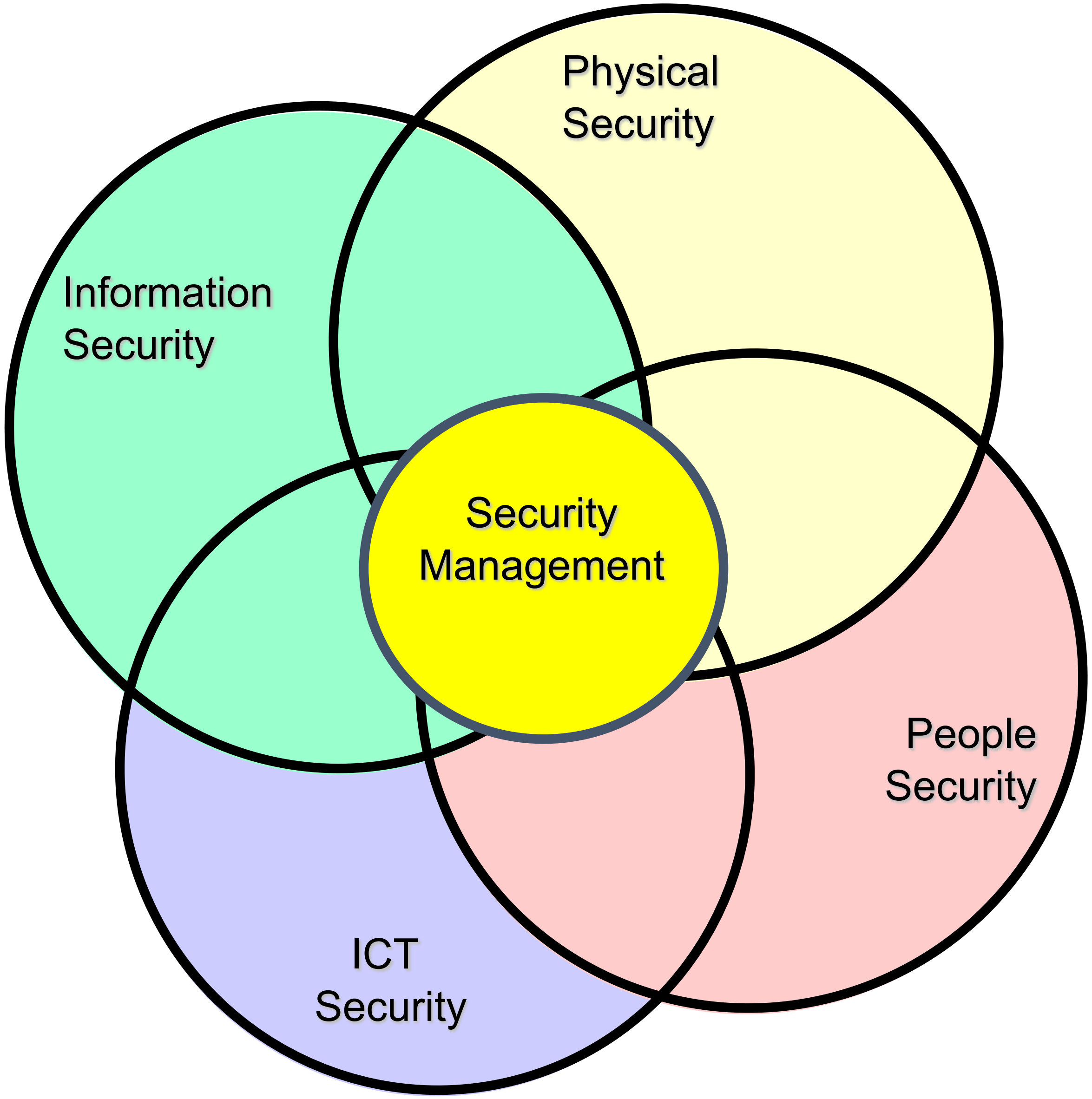
Distracted crew fail to follow
security procedures and
allow pirates to board
covertly and take control

When holes align in Swiss Cheese

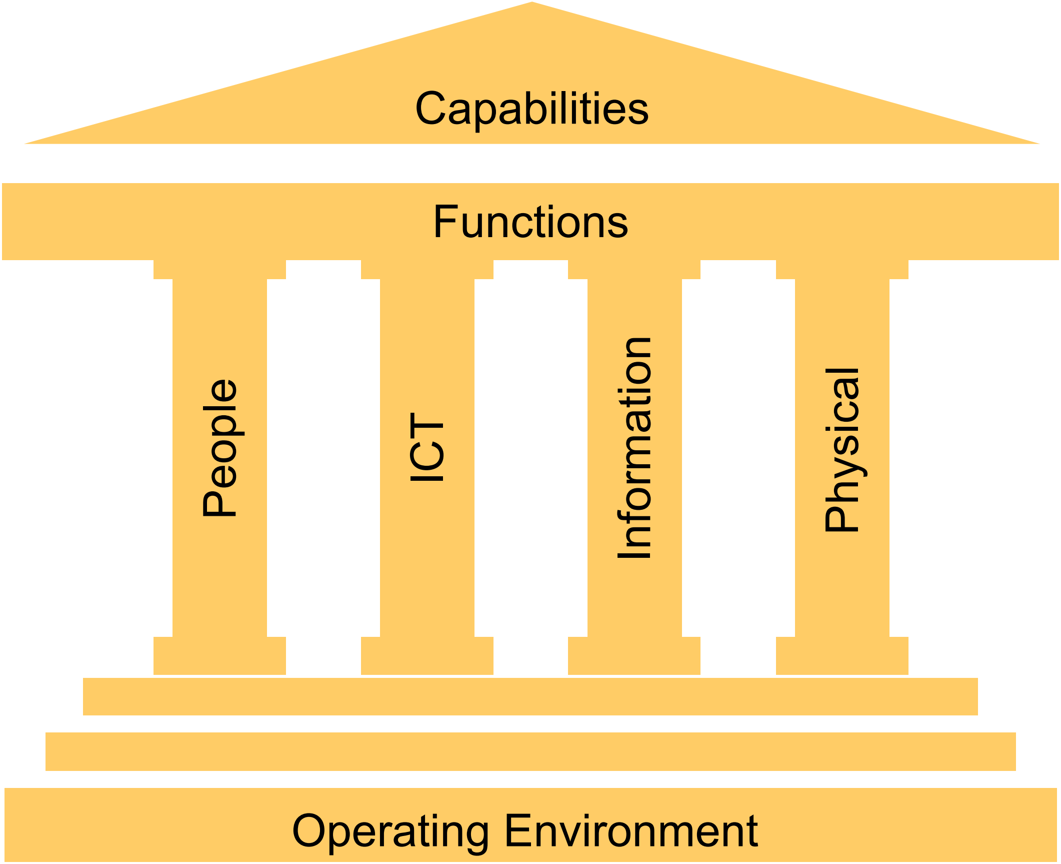
Defining Terms by Relationships



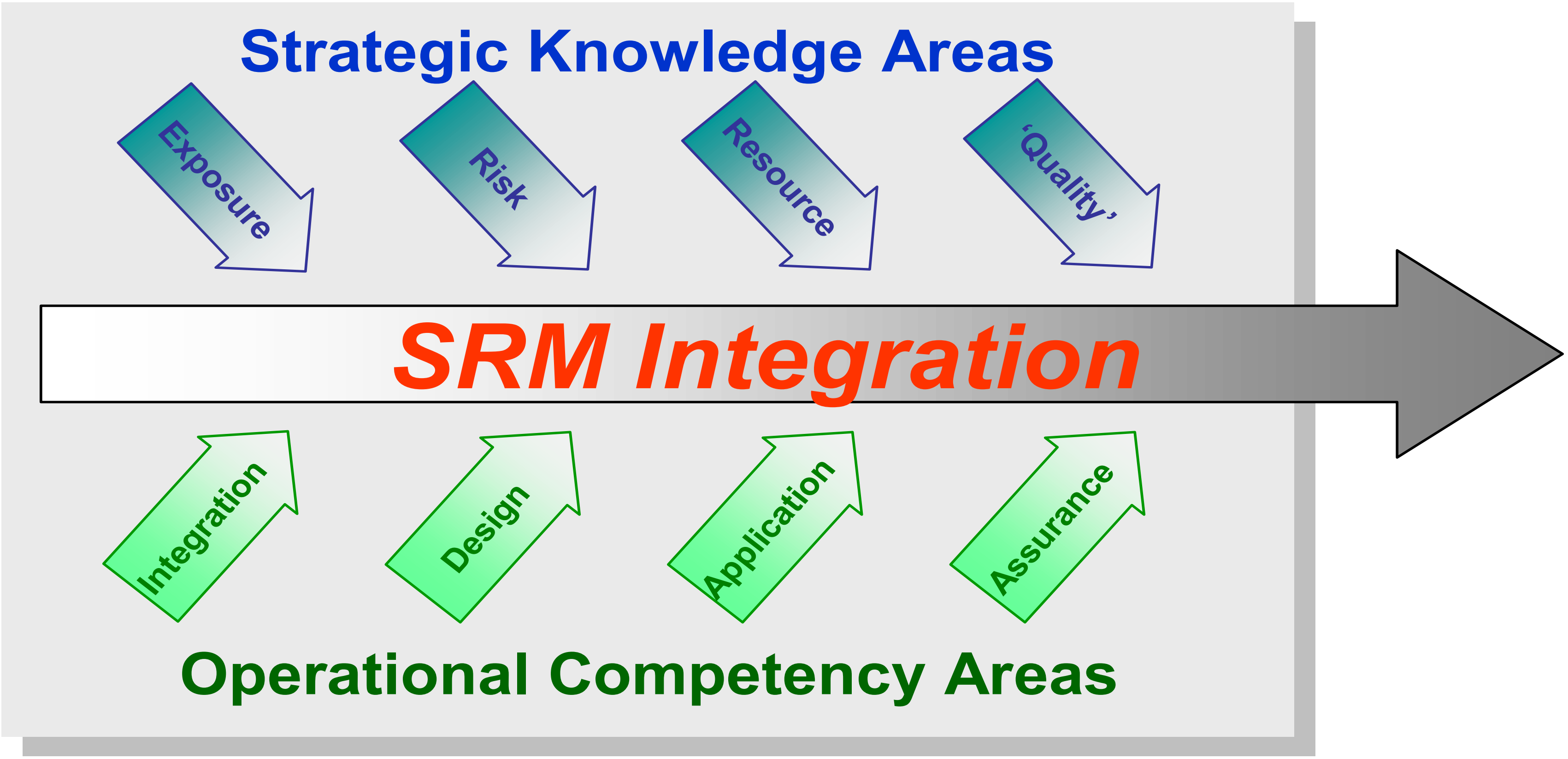
PRACTICE AREAS



RESILIENCE


Capabilities
Functions
People
ICT
Information
Physical
Operating Environment

SRM INTEGRATION



Strategic Knowledge Areas

Exposure

Risk

Resource

'Quality'

SRM Integration

Integration

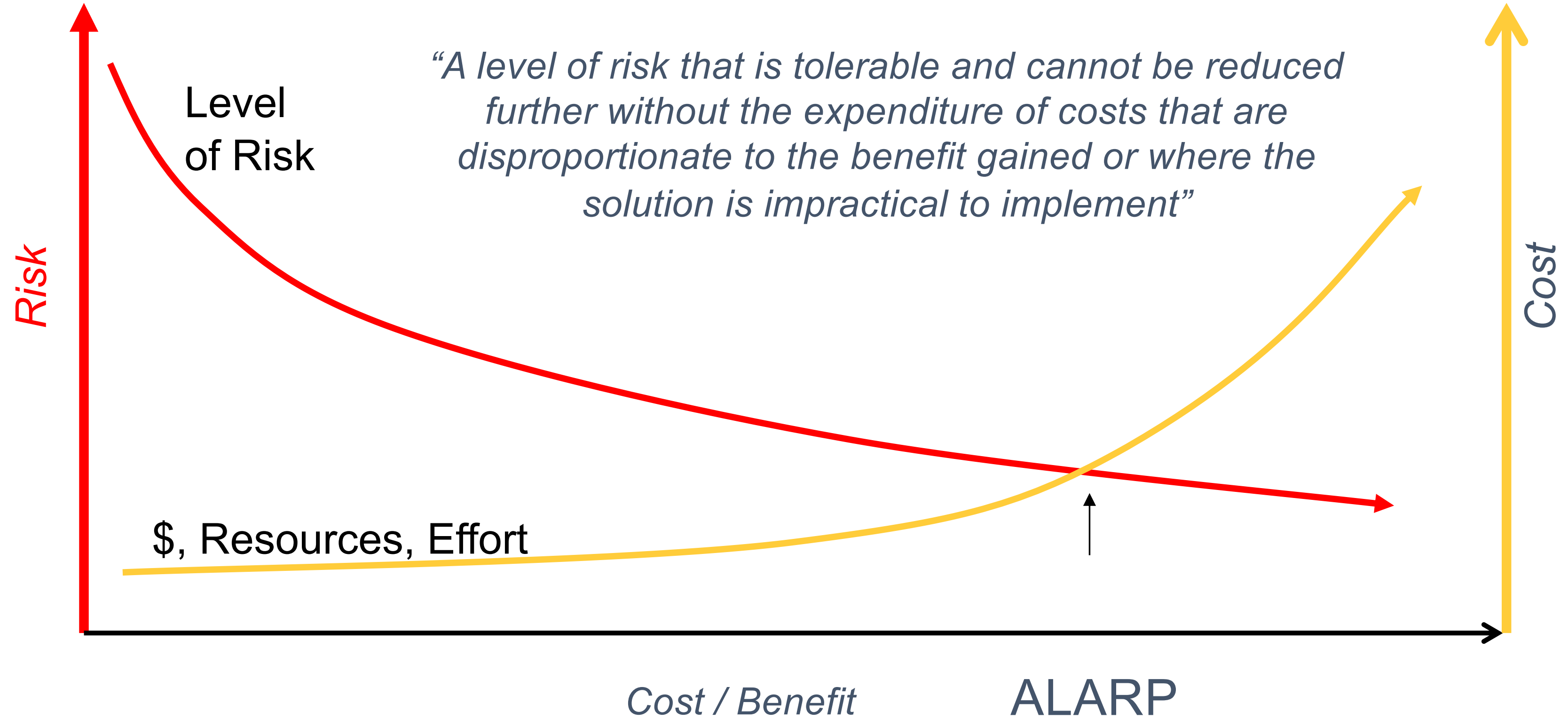
Design

Application

Assurance

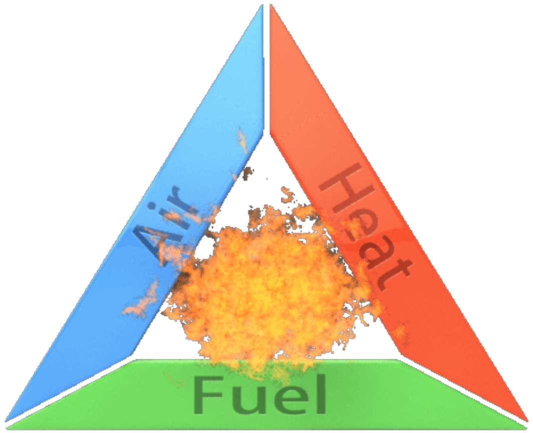
Operational Competency Areas

Cost/Benefit of Mitigation



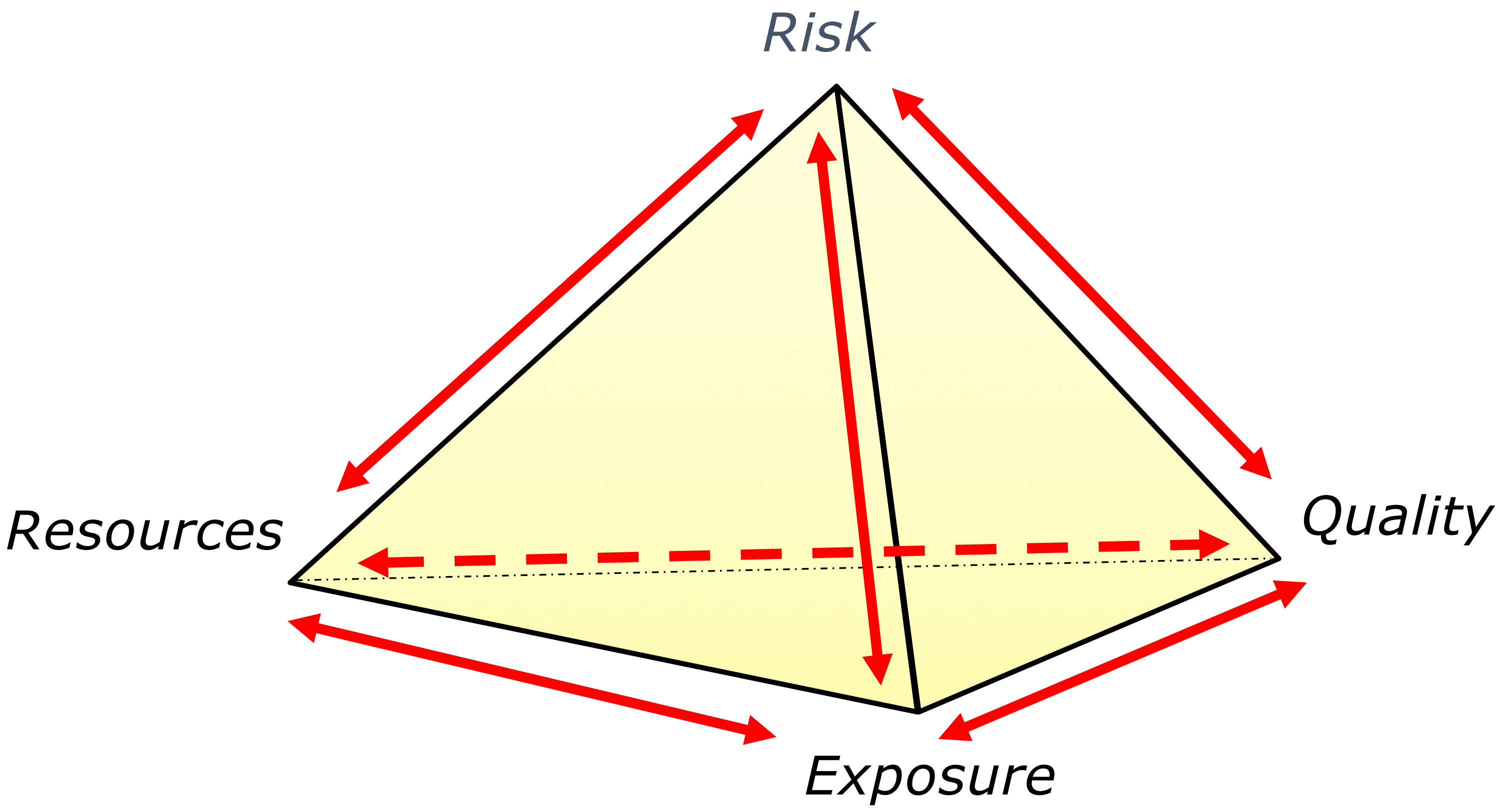
"A level of risk that is tolerable and cannot be reduced further without the expenditure of costs that are disproportionate to the benefit gained or where the solution is impractical to implement"

Light, strong, & cheap

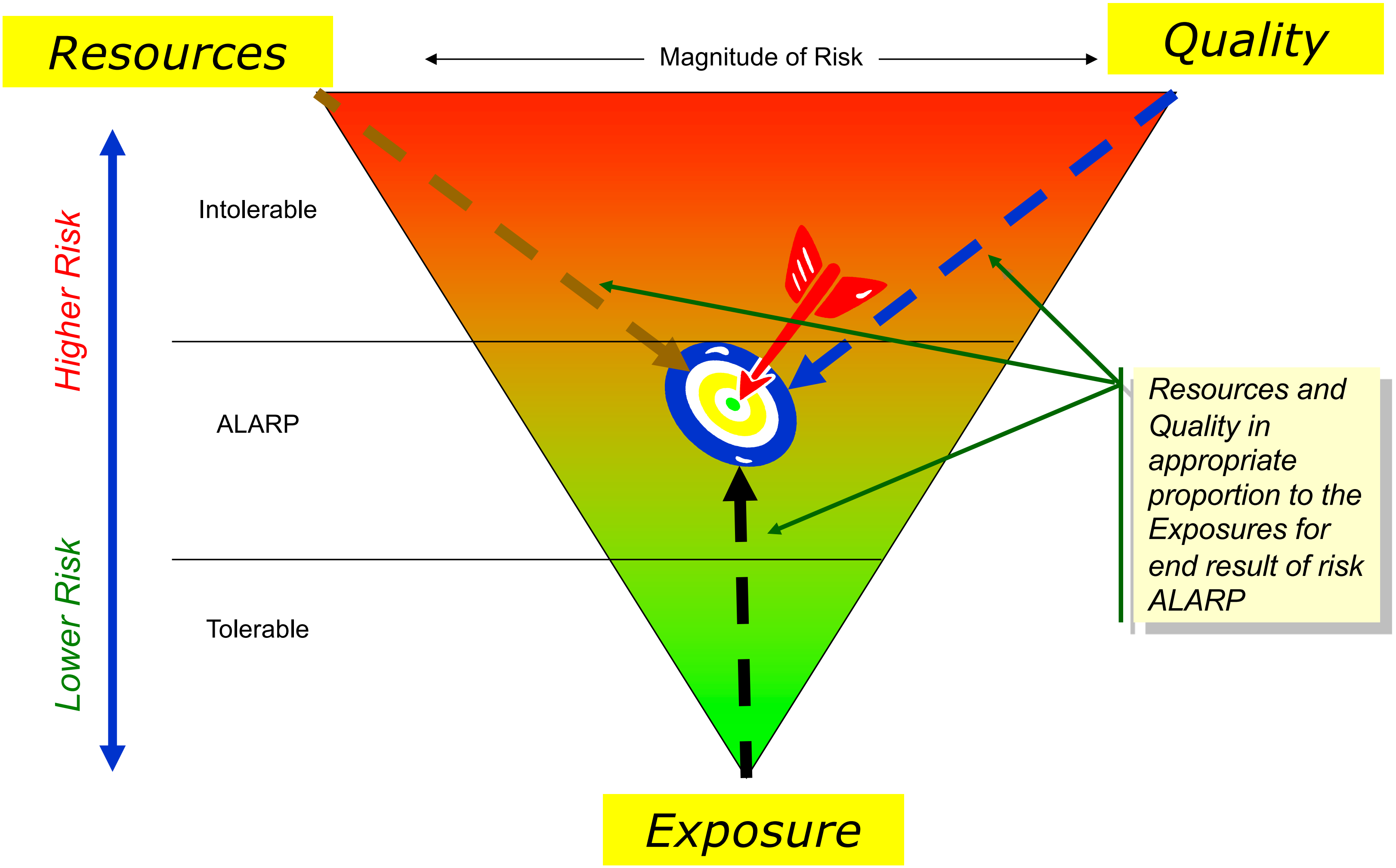


Chemical chain reaction

- Scope, Resources, Schedule (& Quality)

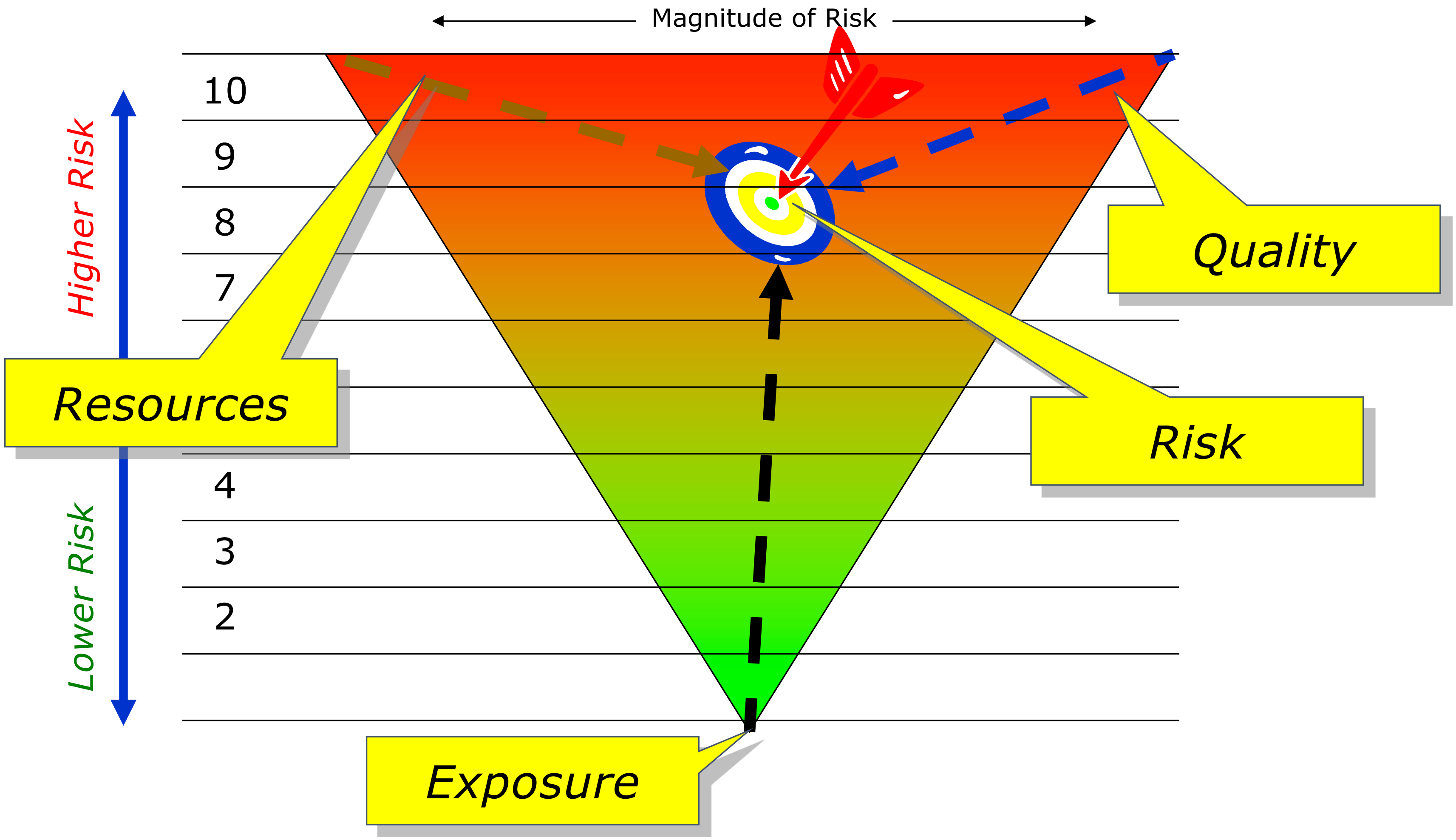

Risk
Resources
Quality
Exposure

Risk Equilibrium (Optimal Trade-Off)

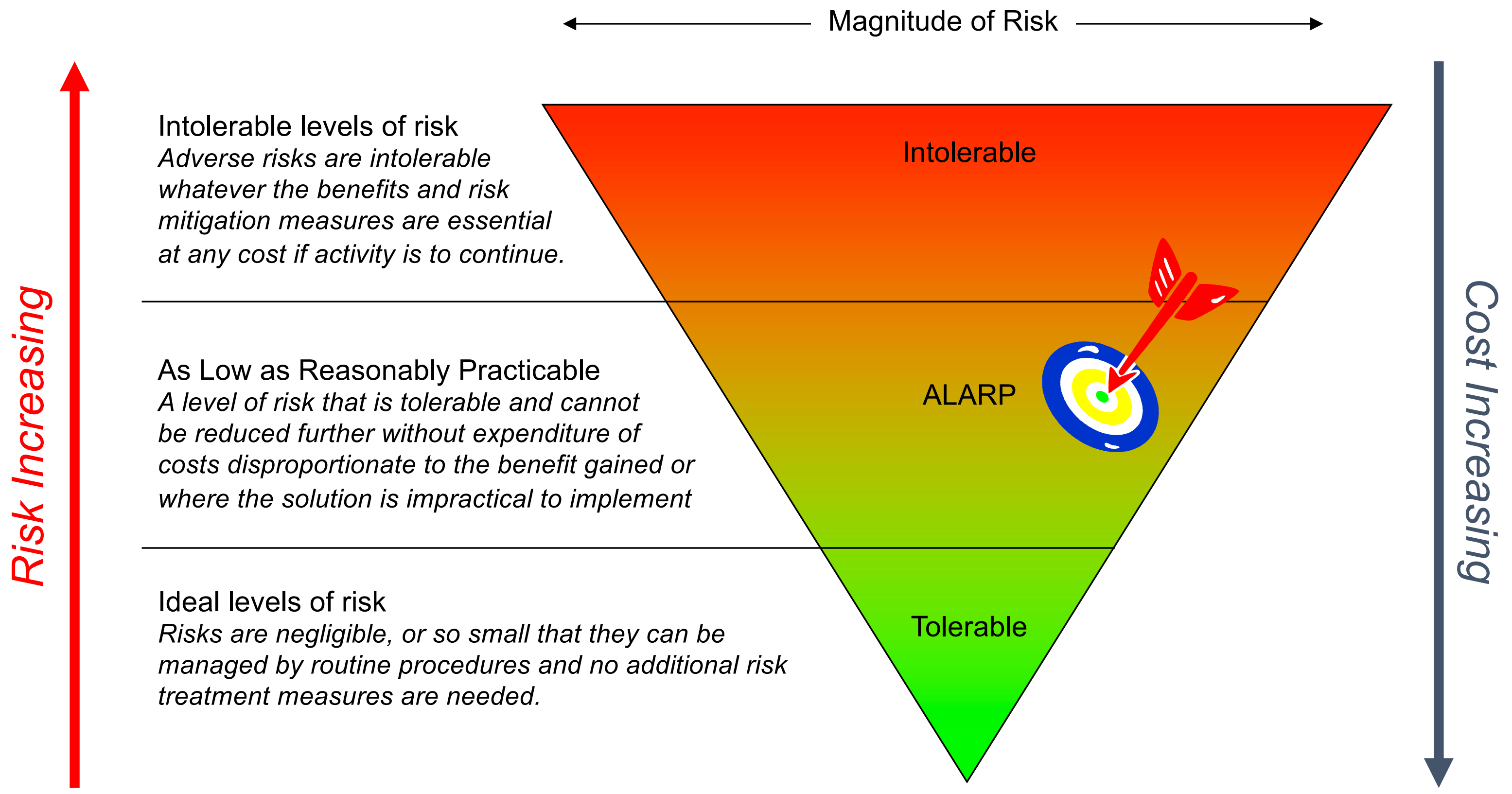


Resources and Quality in appropriate proportion to the Exposures for end result of risk ALARP

Risk High if Resources & Quality Low



As Low As Reasonably Practicable



Magnitude of Risk

Risk Increasing

Cost Increasing

Intolerable levels of risk
Adverse risks are intolerable whatever the benefits and risk mitigation measures are essential at any cost if activity is to continue.

Intolerable

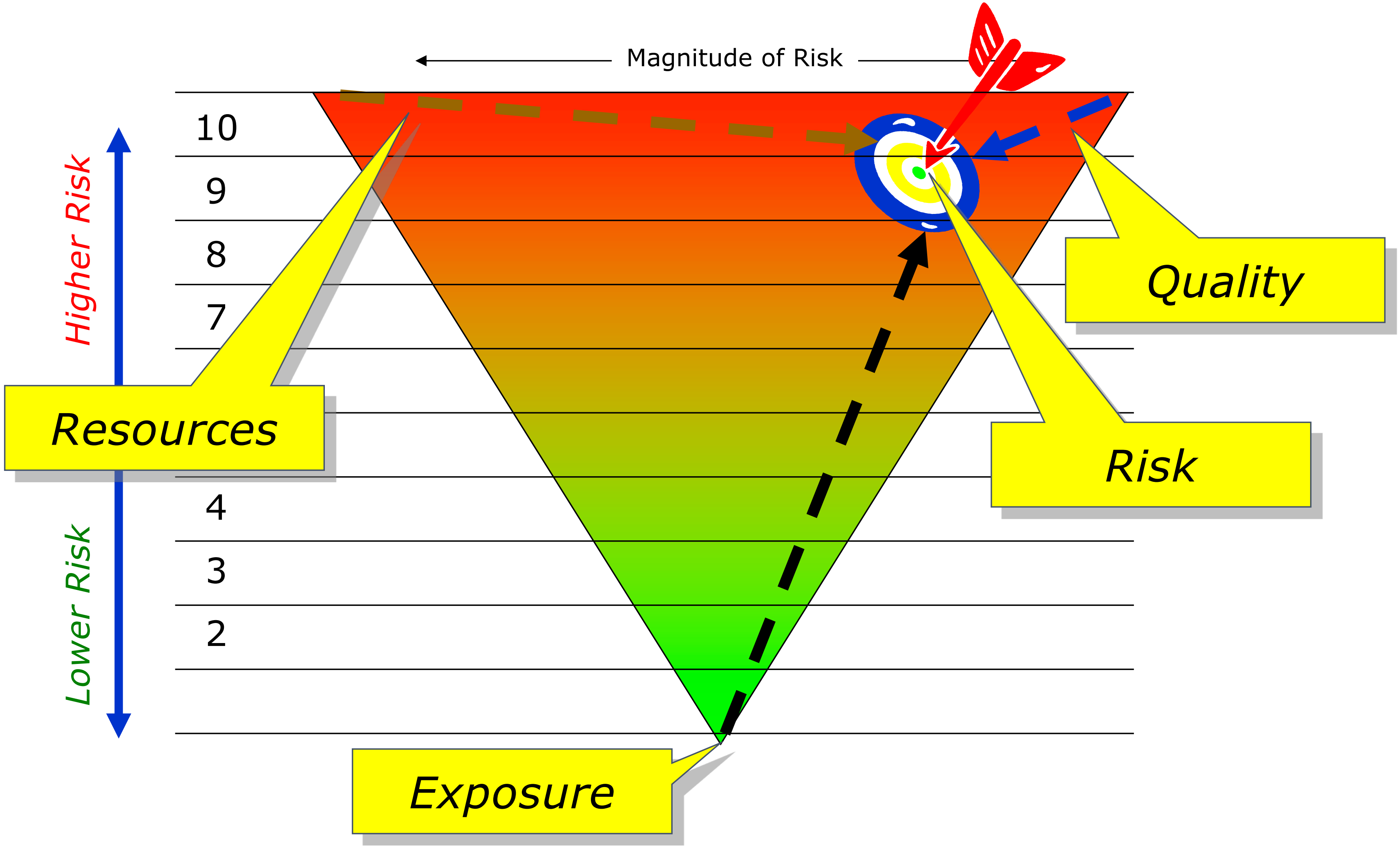
As Low as Reasonably Practicable
A level of risk that is tolerable and cannot be reduced further without expenditure of costs disproportionate to the benefit gained or where the solution is impractical to implement

ALARP

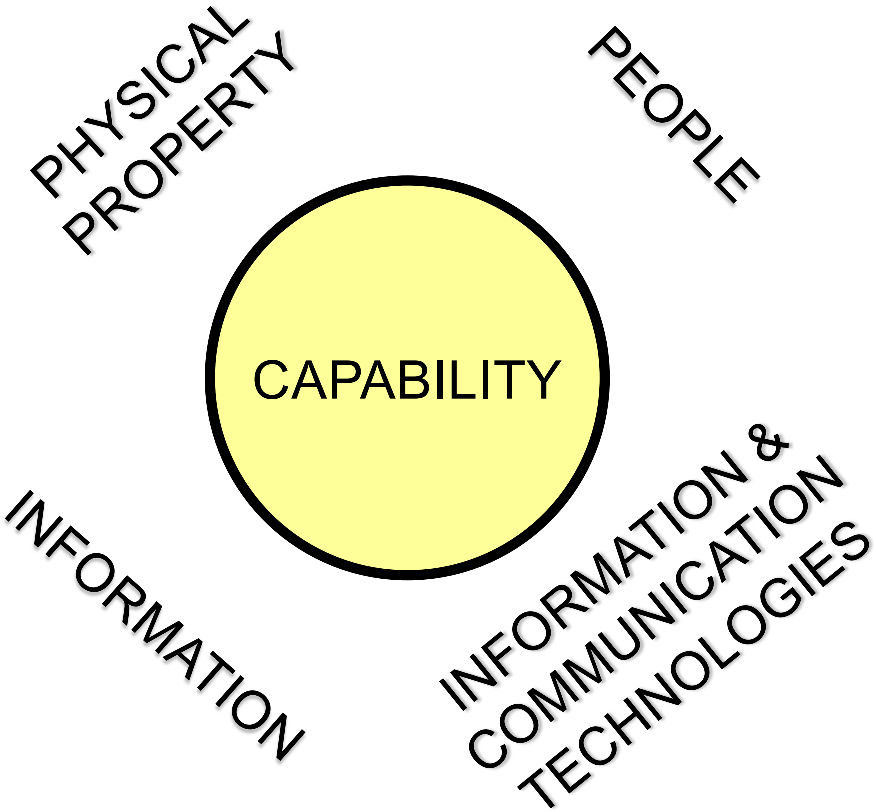
Ideal levels of risk
Risks are negligible, or so small that they can be managed by routine procedures and no additional risk treatment measures are needed.

Tolerable

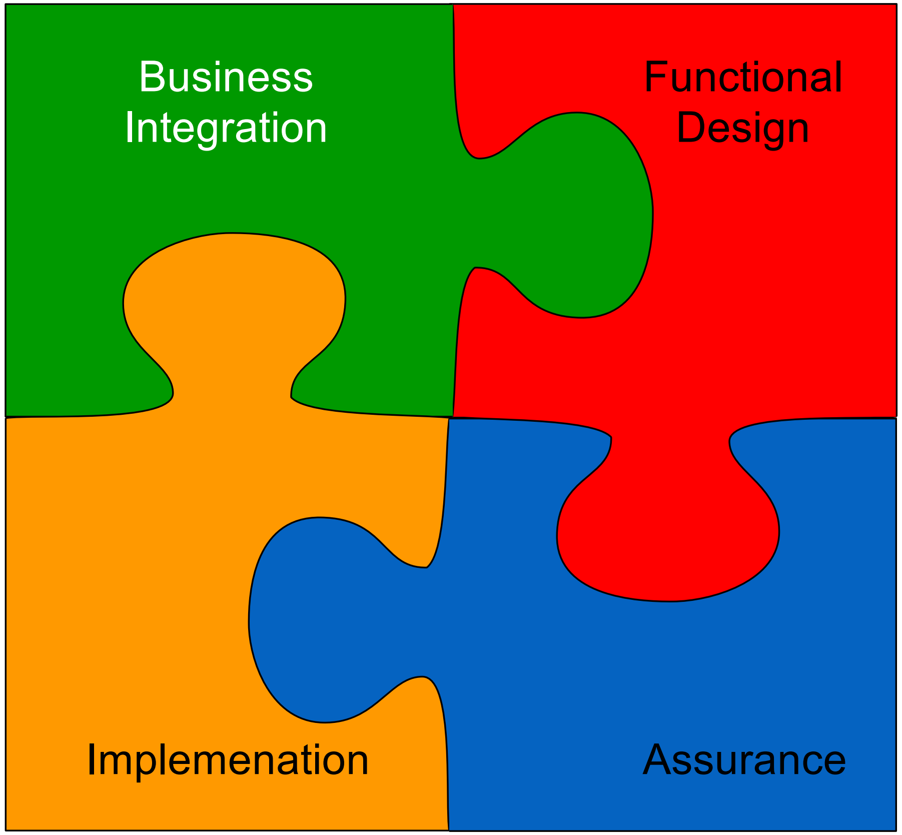
Resources High but Quality Low



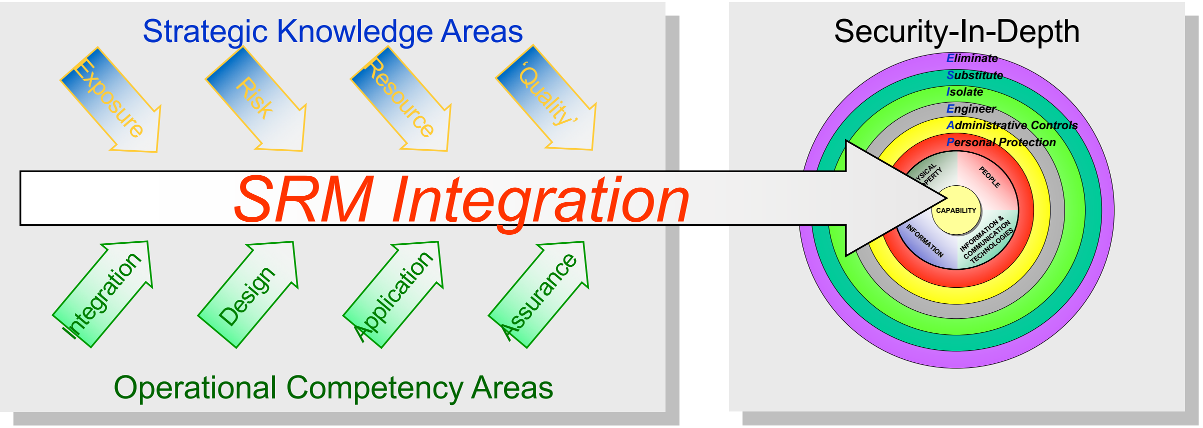
ASSETS (Resources)



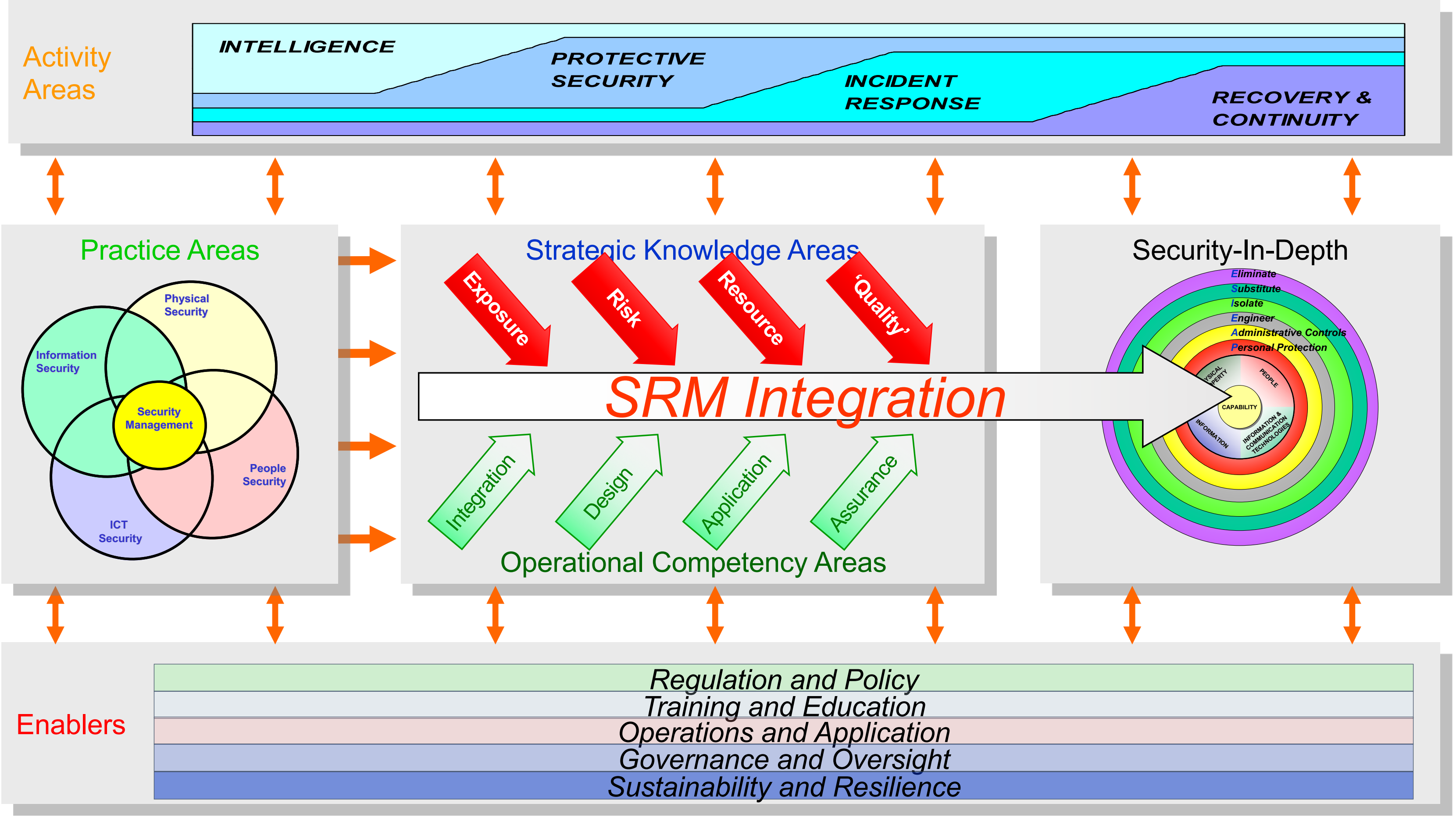
COMPETENCY AREAS



SRMBOK FRAMEWORK



SRMBOK Framework



Activity Areas

INTELLIGENCE

PROTECTIVE SECURITY

INCIDENT RESPONSE

RECOVERY & CONTINUITY

Practice Areas

Physical Security

Information Security

Security Management

People Security

ICT Security

Strategic Knowledge Areas

Exposure

Risk

Resource

'Quality'

SRM Integration

Integration

Design

Application

Assurance

Operational Competency Areas

Security-In-Depth

Eliminate

Substitute

Isolate

Engineer

Administrative Controls

Personal Protection

YSICAL PERTY

PEOPLE

CAPABILITY

INFORMATION

INFORMATION & COMMUNICATION TECHNOLOGIES

Enablers

Regulation and Policy

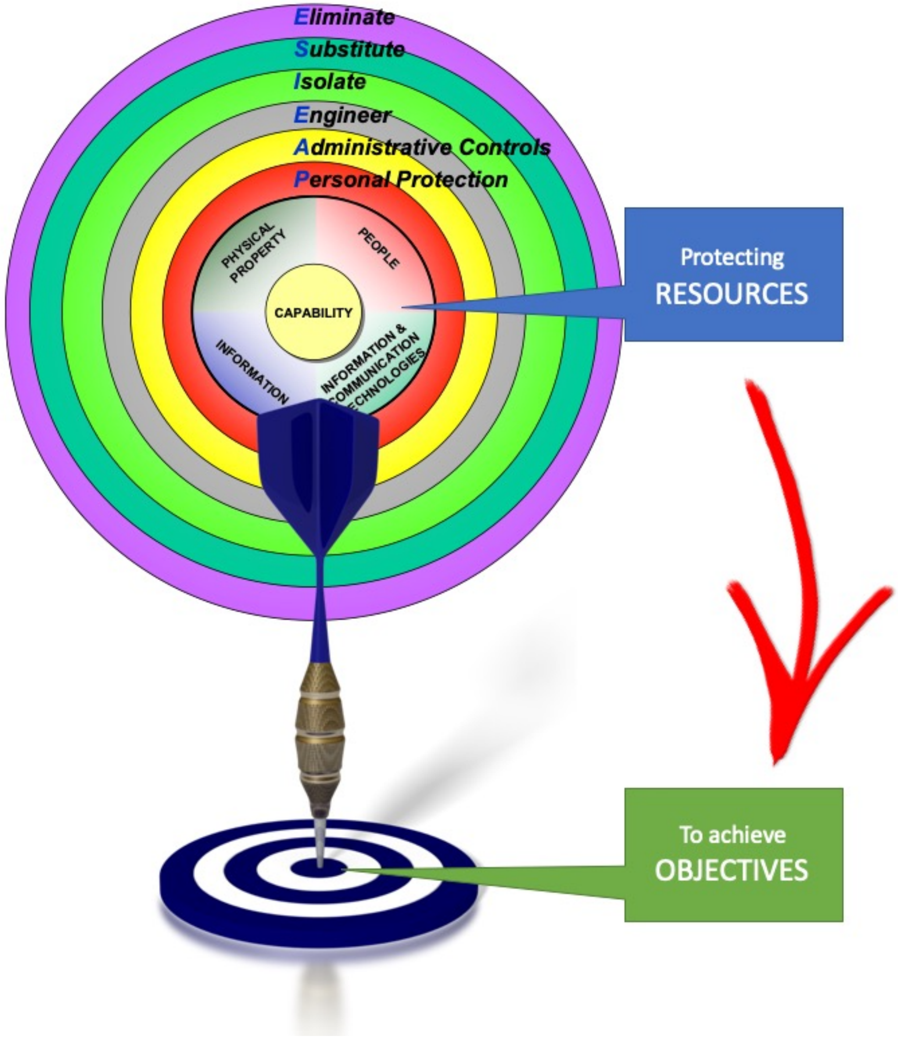
Training and Education

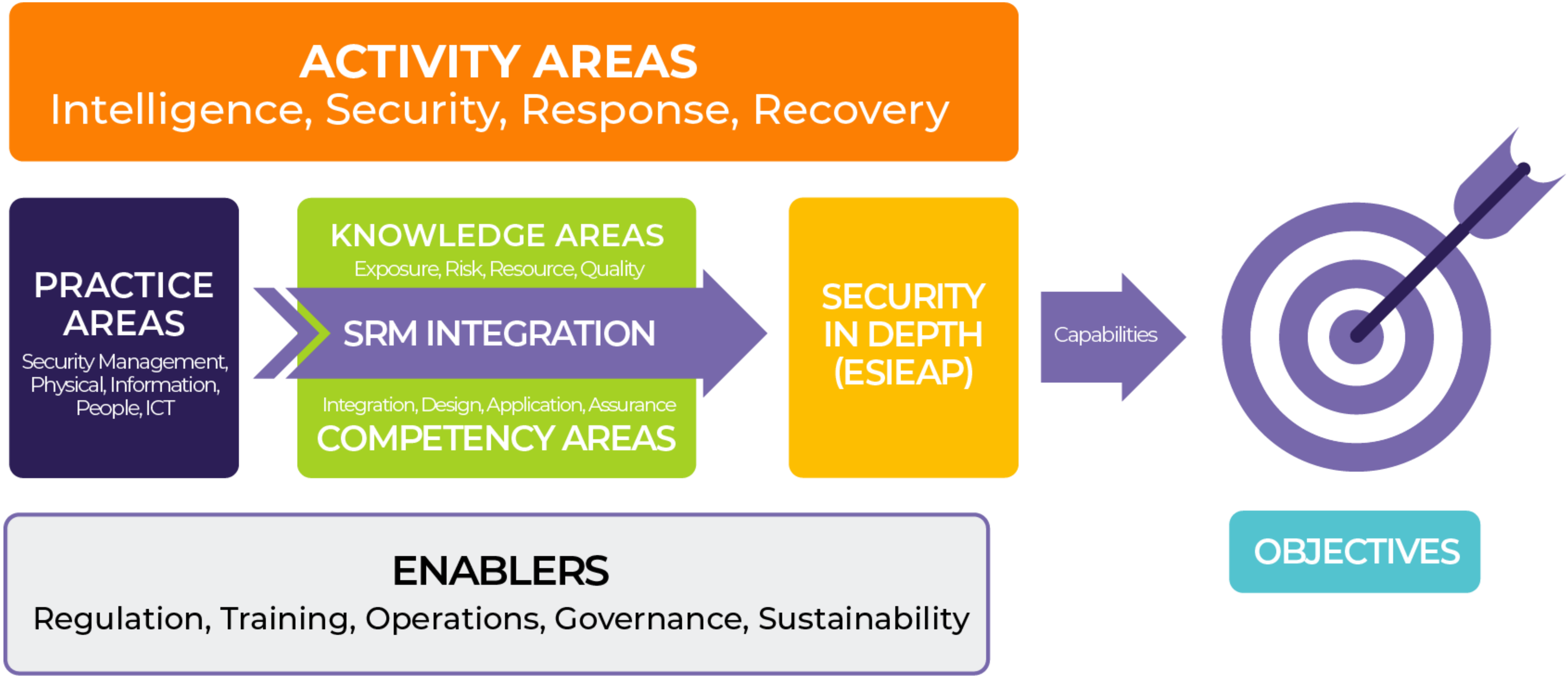
Operations and Application

Governance and Oversight

Sustainability and Resilience

Security-In-Depth





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

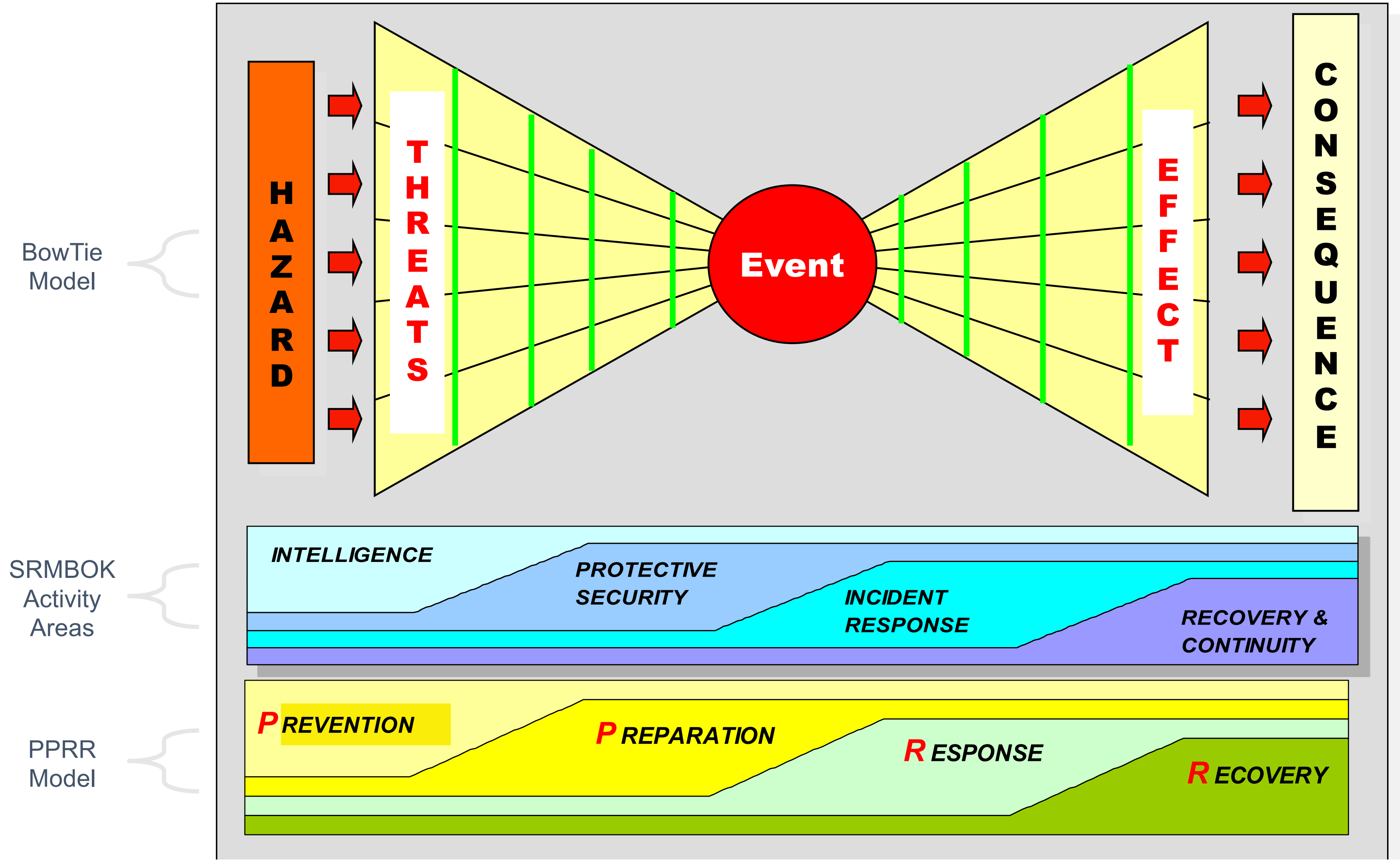
OBJECTIVES

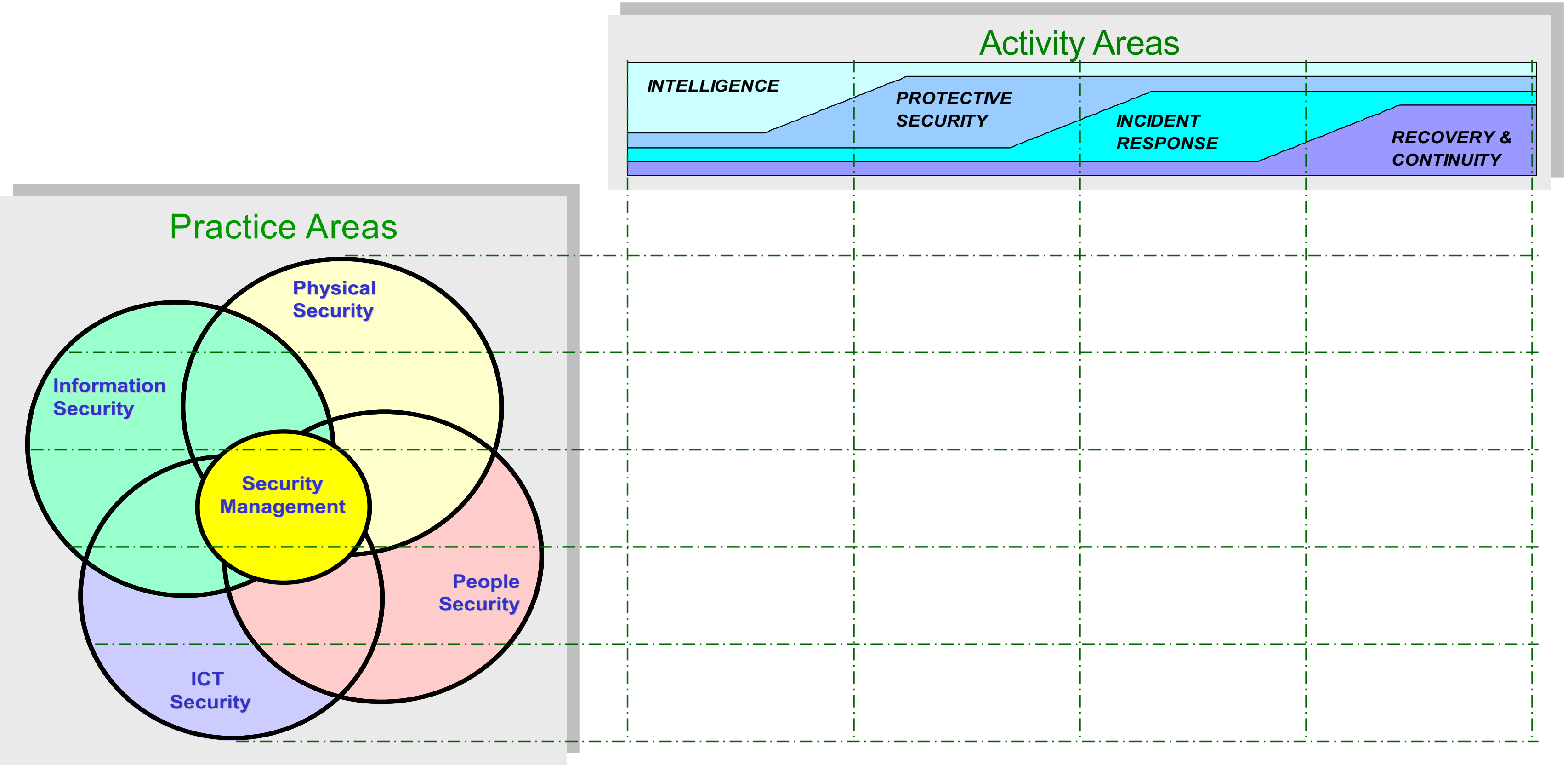
ENABLERS

Regulation, Training, Operations, Governance, Sustainability

- *Security Governance* refers to the processes by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised in the organisation. Generally focuses on two main requirements:
  - *Performance:* whereby the organisation uses its security governance arrangements to contribute to its overall performance, the delivery of its products/services, and general resilience; and
  - *Conformance:* whereby the organisation uses its security arrangements to ensure it meets the requirements of the law, regulations, published standards and community expectations.

ACTIVITY AREAS





Activity Areas

INTELLIGENCE

PROTECTIVE SECURITY

INCIDENT RESPONSE

RECOVERY & CONTINUITY

Practice Areas

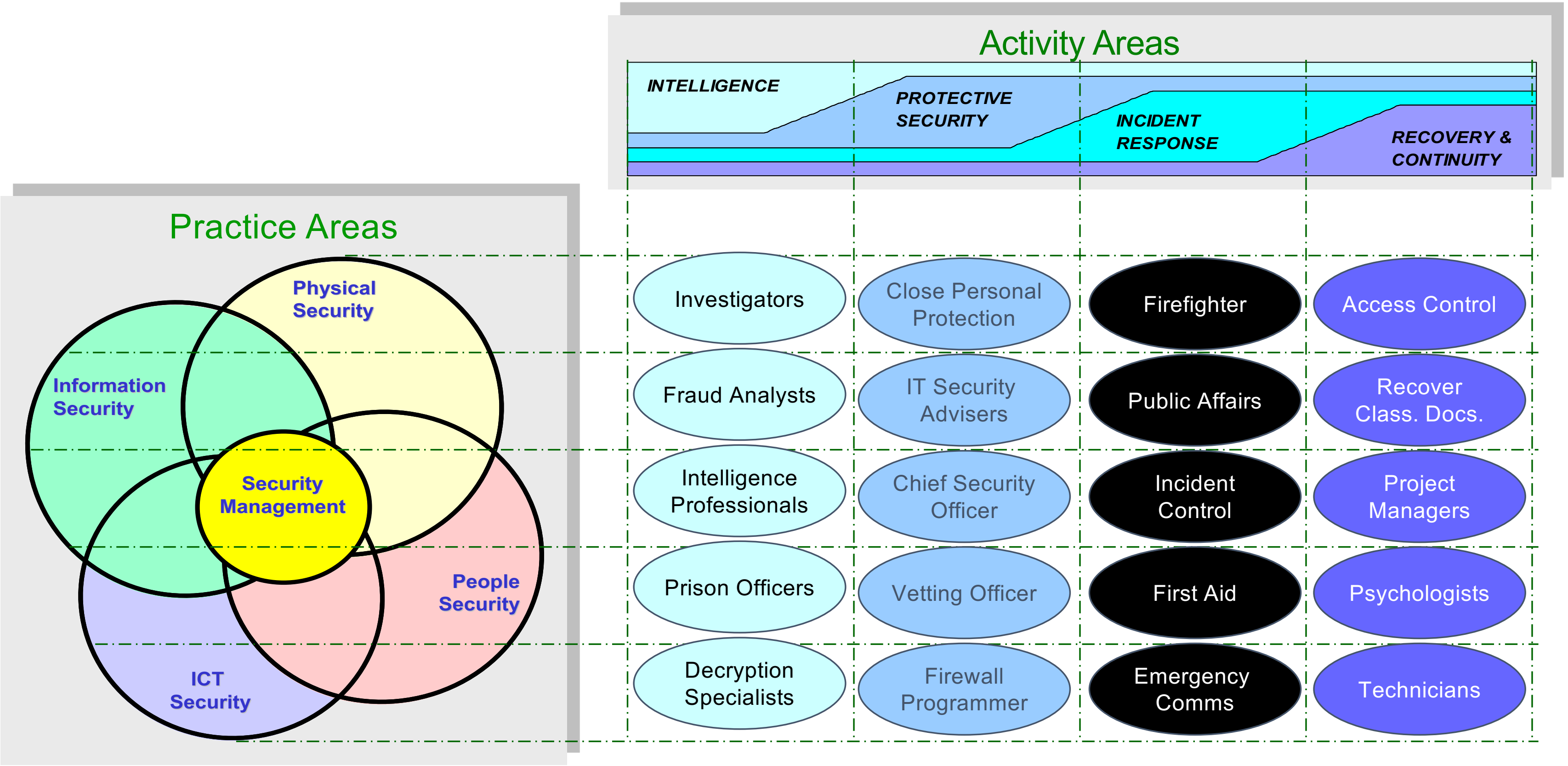
Physical Security

Information Security

Security Management

People Security

ICT Security



Activity Areas

INTELLIGENCE	PROTECTIVE SECURITY	INCIDENT RESPONSE	RECOVERY & CONTINUITY
Investigators	Close Personal Protection	Firefighter	Access Control
Fraud Analysts	IT Security Advisers	Public Affairs	Recover Class. Docs.
Intelligence Professionals	Chief Security Officer	Incident Control	Project Managers
Prison Officers	Vetting Officer	First Aid	Psychologists
Decryption Specialists	Firewall Programmer	Emergency Comms	Technicians

Practice Areas

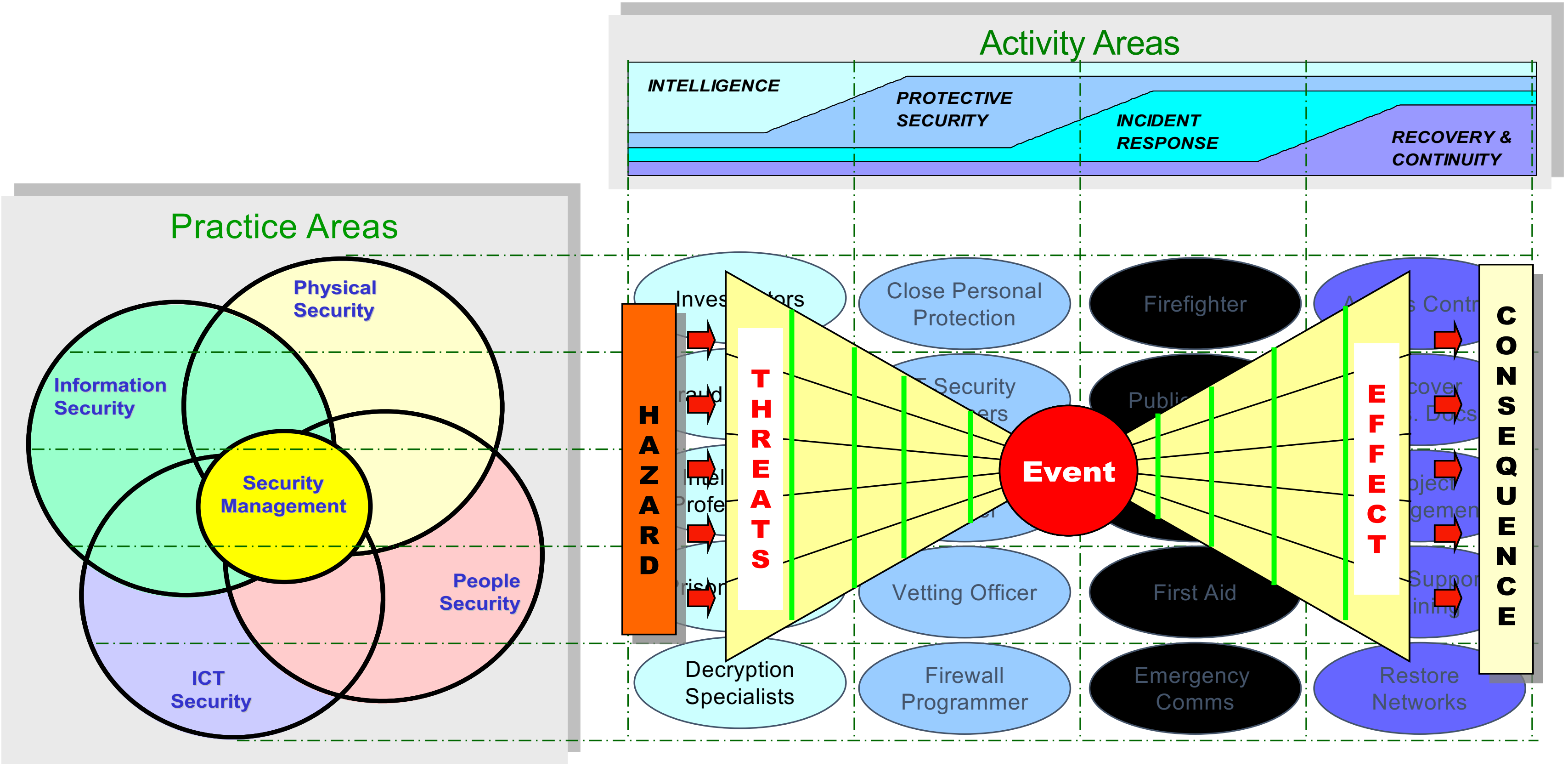
Physical Security

Information Security

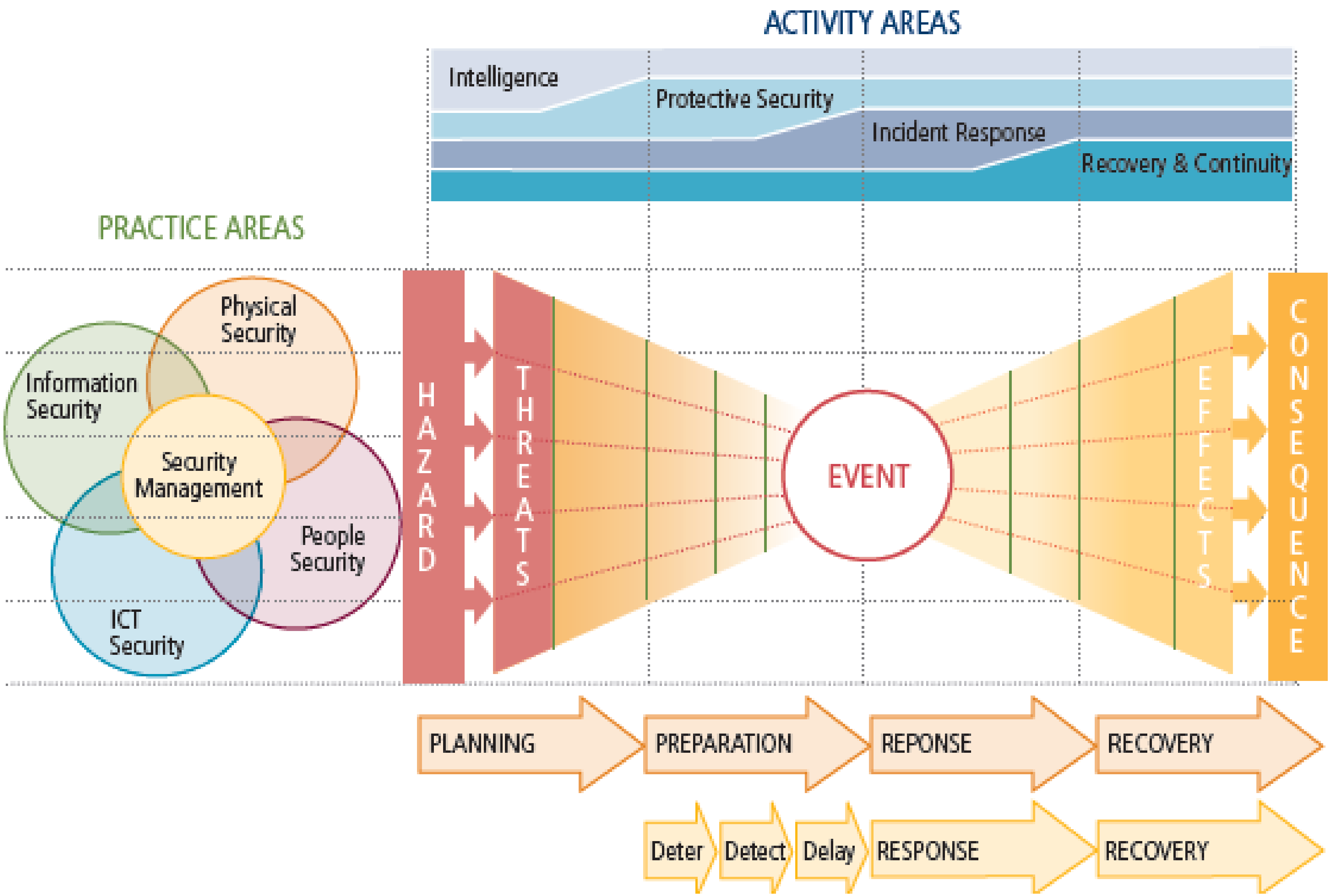
Security Management

People Security

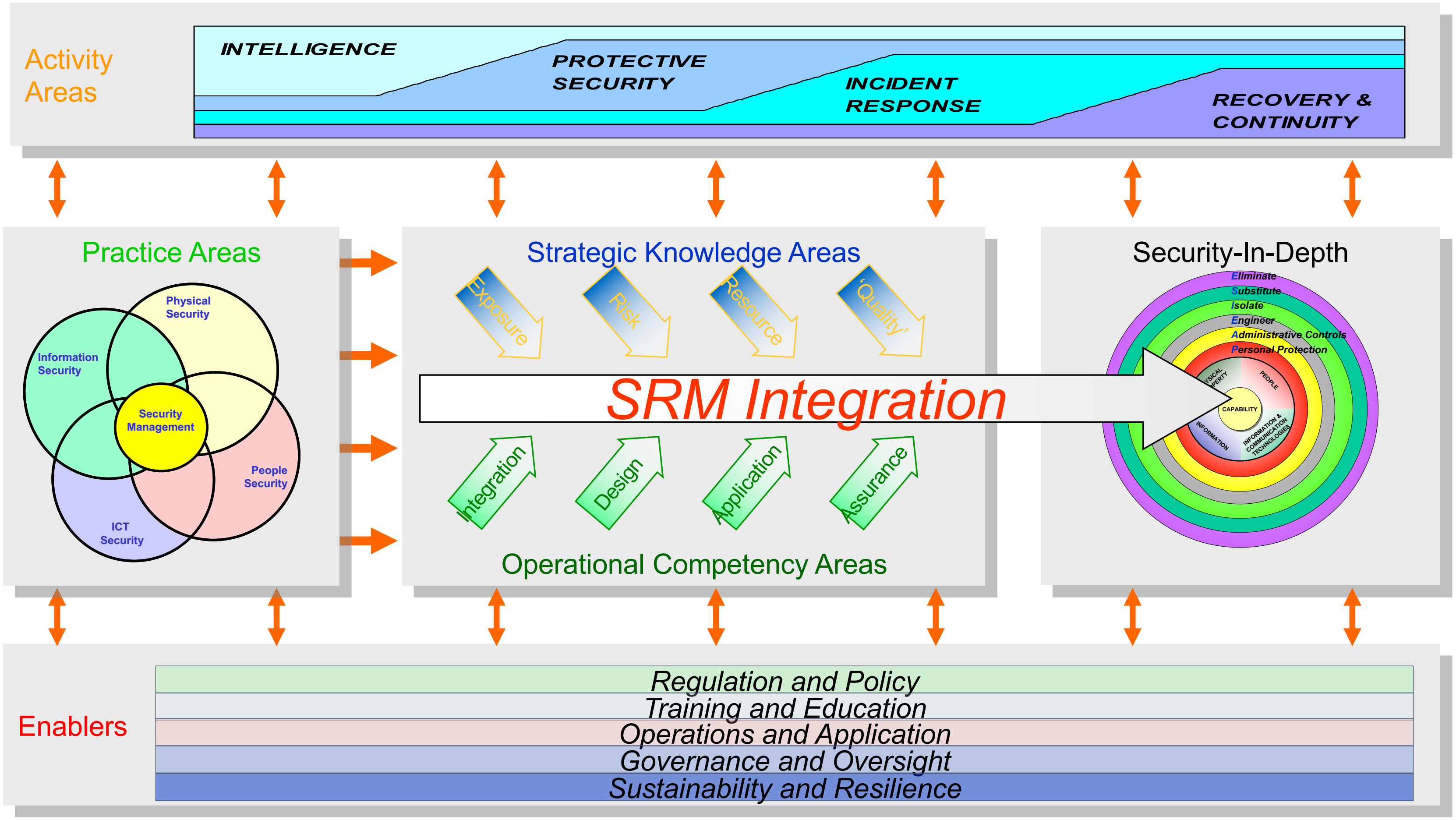
ICT Security

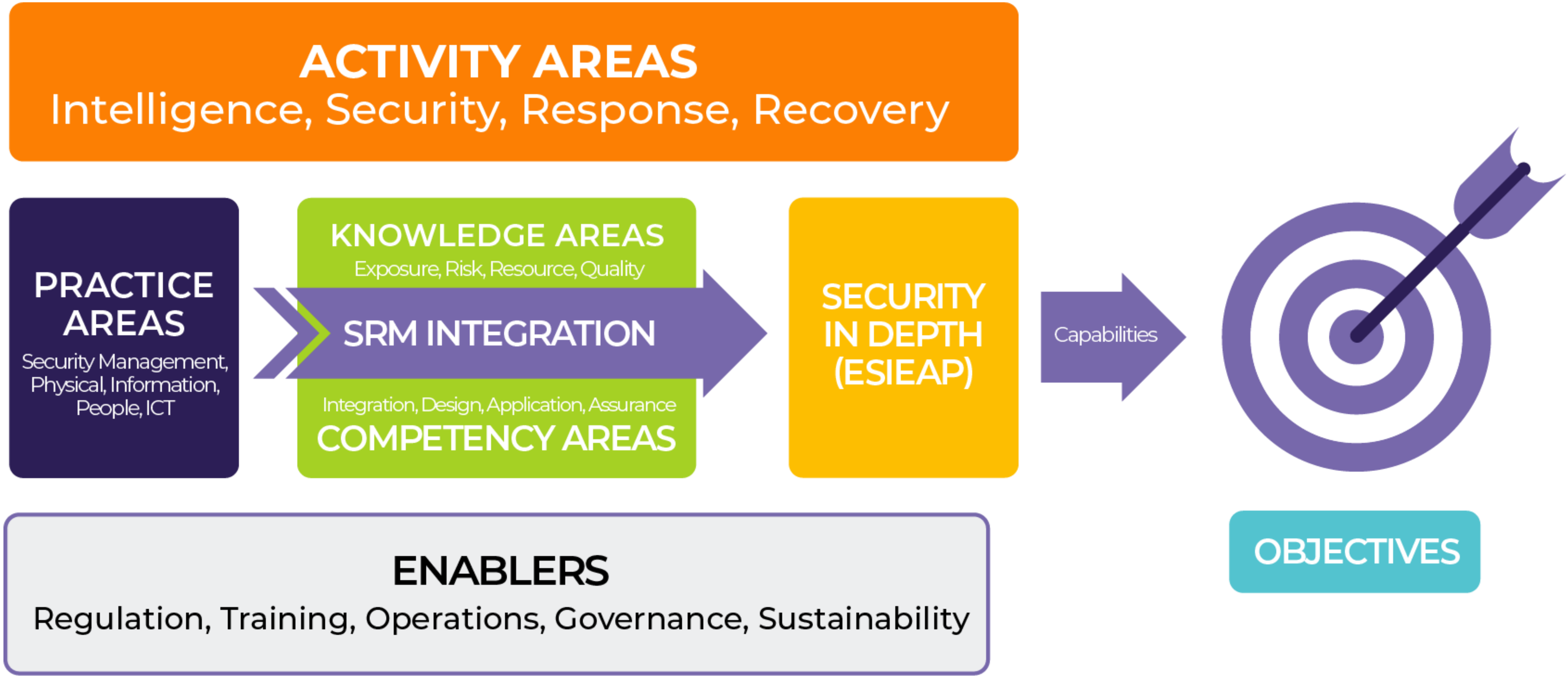


Practice Areas
Physical Security
Information Security
Security Management
People Security
ICT Security
Activity Areas
INTELLIGENCE
PROTECTIVE SECURITY
INCIDENT RESPONSE
RECOVERY & CONTINUITY
HAZARD
THREATS
Event
EFFECT
CONSEQUENCE
Inves tors
raud
Intel
Profe
Prison
Decryption Specialists
Close Personal Protection
T Security ers
Vetting Officer
Firewall Programmer
Firefighter
Publi
First Aid
Emergency Comms
A s Contr
cover . Docs
oject gemen
Suppor ining
Restore Networks


ACTIVITY AREAS
Intelligence
Protective Security
Incident Response
Recovery & Continuity
PRACTICE AREAS
Physical Security
Information Security
Security Management
People Security
ICT Security
HAZARD
THREATS
EVENT
EFFECTS
CONSEQUENCE
PLANNING
PREPARATION
REPONSE
RECOVERY
Deter
Detect
Delay
RESPONSE
RECOVERY

SRM INTEGRATION





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

Morning Tea

- 1030 to 1100