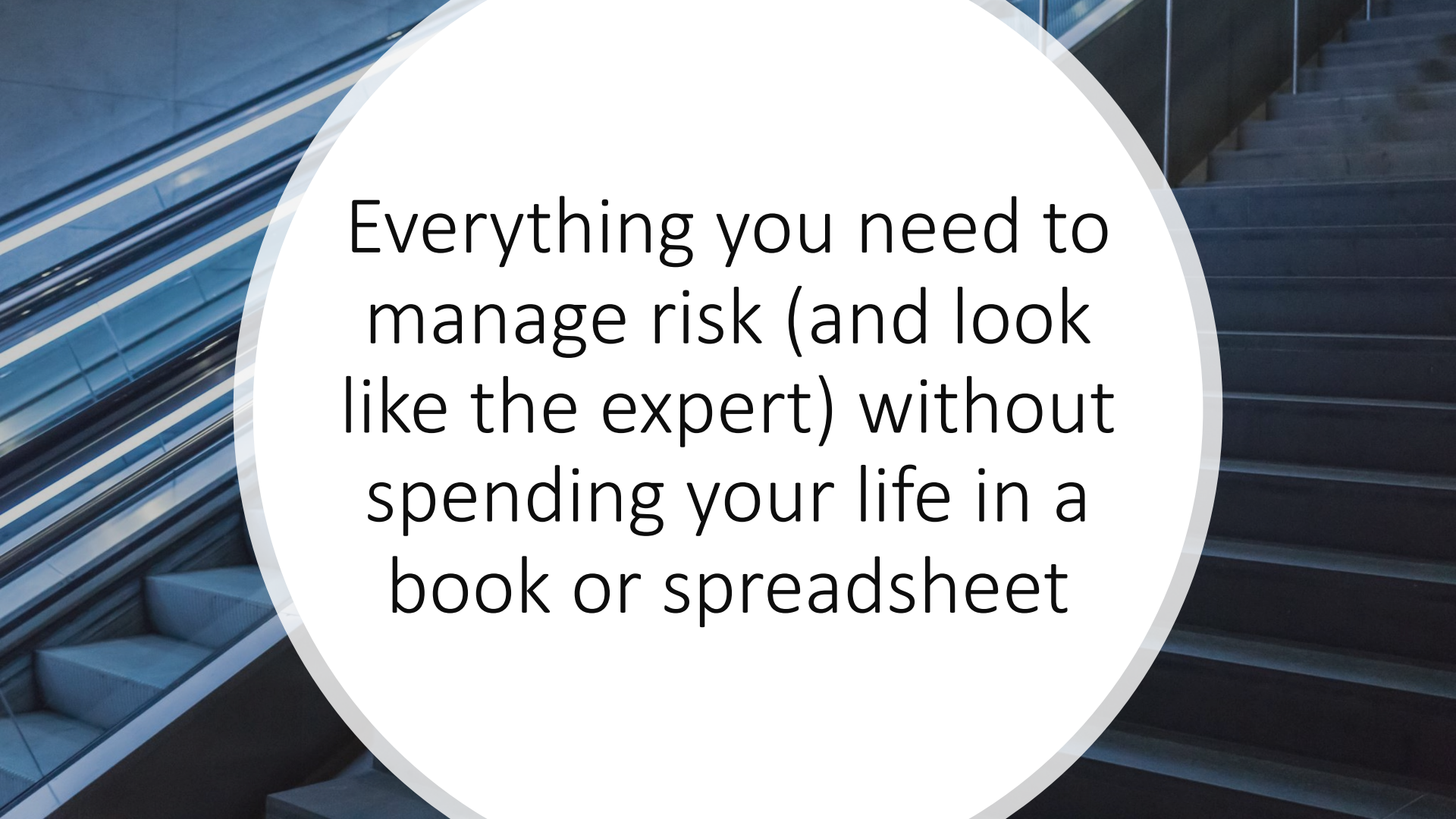
RISK MANAGEMENT 101

THE FUNDAMENTALS


Everything you need to manage risk (and look like the expert) without spending your life in a book or spreadsheet

Housekeeping

Two sessions	Screenshots & notes	Questions at the end
• 10-minute break for emails, coffee, etc • Mute microphones	• One Note, MS Word, Evernote, etc • Screen capture (Win-PrtScn, Command-Shift-3)	• Clarifications anytime • Hand up or chat box

AGENDA

- Environment and threats
- Risk fundamentals
- ISO31000 Risk Management Guideline
- Risk management strategies
- Inherent, current, residual
- Swiss Cheese and Bow Ties
- Risk identification, risk identification, risk identification
- Syndicate exercise
- Q&A Session

Training Objectives

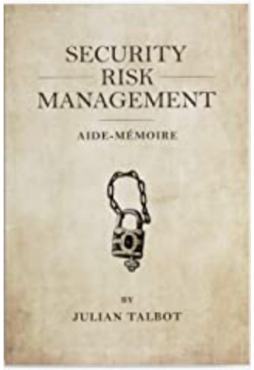
Training Objectives

- Practical & fun
- Less stress (for you)
- Better use of resources (for your organization)
- More funding (for your programs)
- Spot an ‘excellent’ vs ‘not so good’ risk assessment in under 2 minutes – and how to fix it

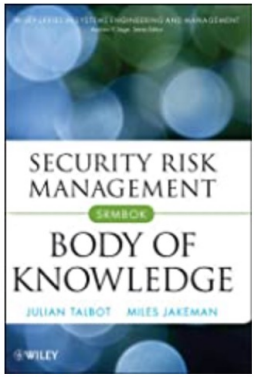
Julian Talbot

✓ Following

Follow to get new release updates and improved recommendations

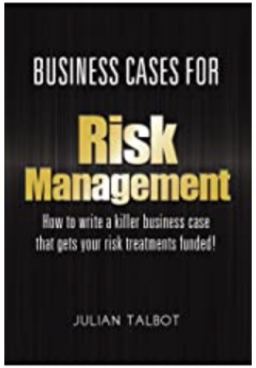


$4.69
Kindle Edition

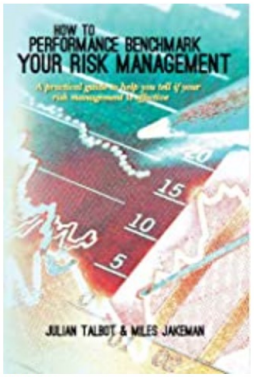


$96.00
Kindle Edition

$4.19
Kindle Edition



$9.99
Kindle Edition



$9.99
Kindle Edition

Julian Talbot CISSP F.ISRM

www.juliantalbot.com

ECTARA™

SRMBOK
Security Risk Management Body Of Knowledge

Julian Talbot

- Master of Risk Management
- Fellow of the Institute of Strategic Risk Management
- Fellow of the Risk Management Institution of Australasia
- Austrade, Manager Property & Security
- Co-founder Citadel Group
- Defence, Finance, Health, Woodside, Malaysian Smelting Corporation
- Motorcycles, adventure travel, distance hiking

"An expert is a person who has made all the mistakes that can be made in a very narrow field."
— **Niels Bohr**

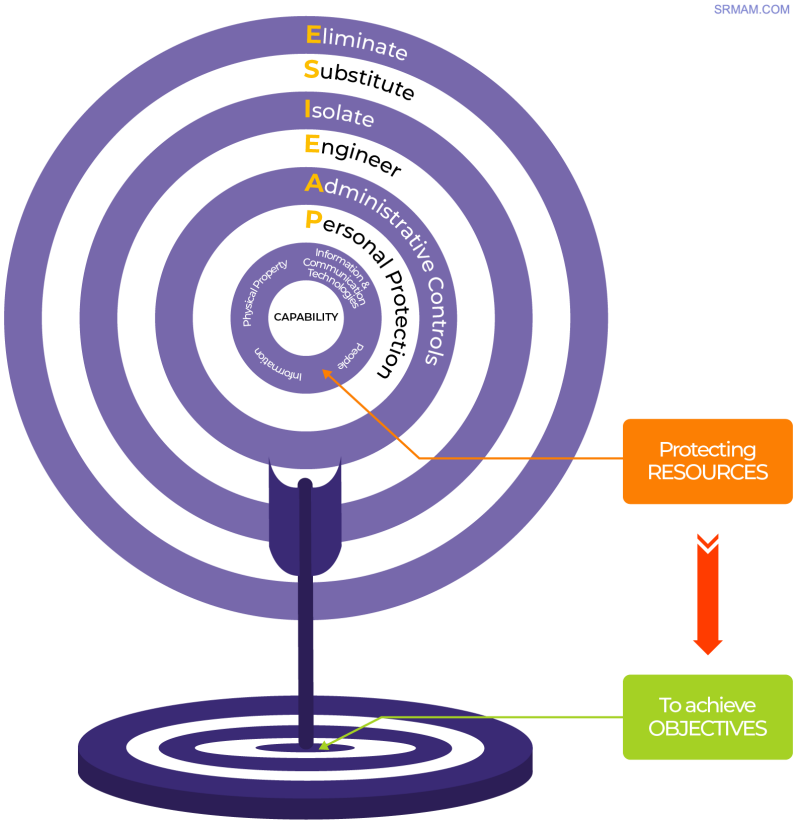
Julian talbot

- Julian has 35 years of international management and leadership experience, including over 20 years at Director and C- Suite levels in the commercial, government, and not-for-profit sectors. His credentials include a Master of Risk Management (MRiskMgt), Graduate of the Australian Institute of Company Directors (GAICD), Microsoft Certified Systems Engineer (MCSE), Professional Certificate in Property Portfolio Management, Certificate IV Workplace Trainer and Assessor, and Diplomas in Project Management, Business Management, and Security Risk Management.
- Julian is a Fellow of the Institute of Strategic Risk Management (F.ISRM), Fellow of the Risk Management Institution of Australasia (RMIA), and recipient of the Australian Security Medal (ASM). Julian co-founded the Citadel Group in 2007 and helped grow the company from a start-up to an ASX listed company with 300 employees with a market capitalization of $400 million.
- After 30 years of industry experience with the last 20 years as a director, Julian works with startups as a mentor and investor, advises large organizations, and works with a range groups including national and international standards organisations, mining and resources, Defence and intelligence, not-for-profit, and government sectors. Julian has lived and worked on five continents, in roles including CEO, consultant, company director, chairman, chief risk officer, chief security officer, operations manager, firefighter, paramedic, soldier, author, and trainer.
- Julian has started or invested in over 20 businesses, published several books, and lived on five continents. Previous roles include:
    - Divisional Manager of the $250 million ASX listed Citadel Group Ltd
    - Operations Manager for IMX Resources exploration activities in East Africa
    - Manager of Property and Security for the Australian Government's most extensive international network (Austrade)
    - Security Manager of Australia's largest resources project (the $24 billion North West Shelf Project)
    - Senior Risk Adviser for the Australian Department of Health and Ageing
    - Director and Chairman of CGL, 3 times ranked one of the 20 fastest-growing companies in Australia
    - Director of the Risk Management Institution of Australasia
    - Director of the Australian Institute of Professional Intelligence Officers
    - Director of the Washington, DC-based Security Analysis and Risk Management Association

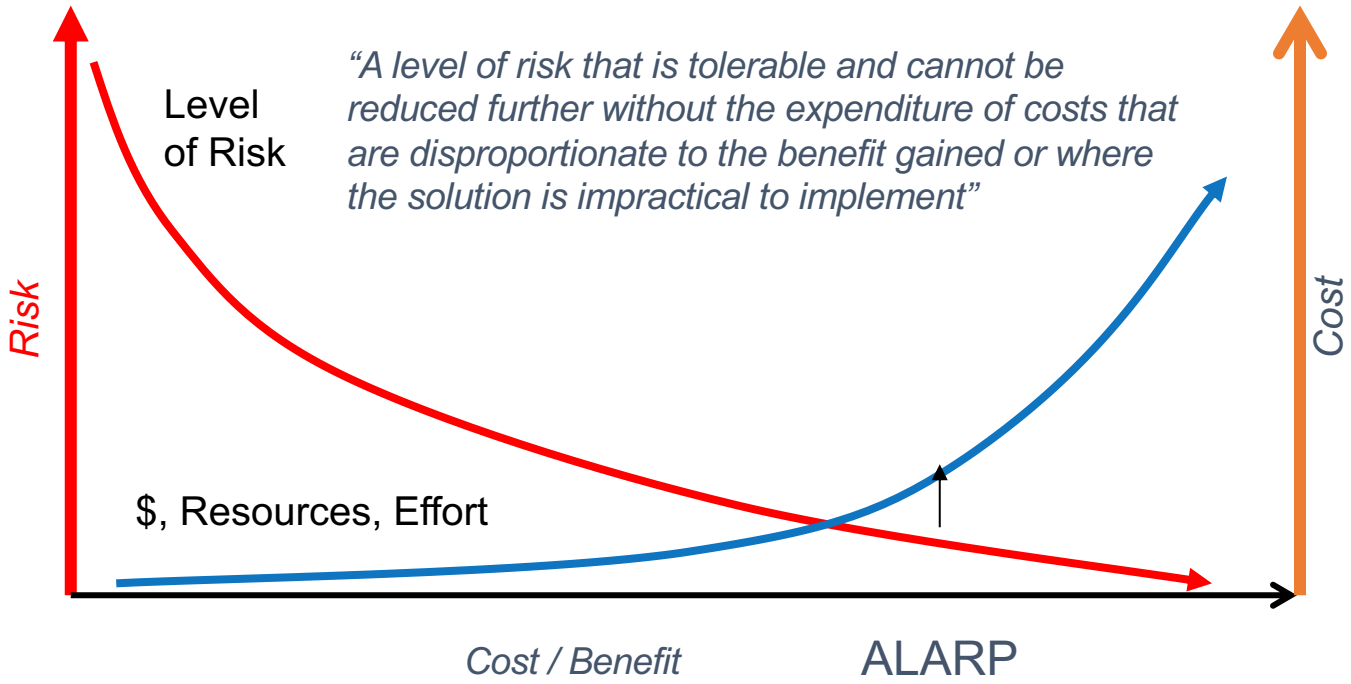
https://juliantalbot.fyi.to/julian-talbot

Risk management fundamentals

Protection in Depth



Cost/Benefit of Mitigation

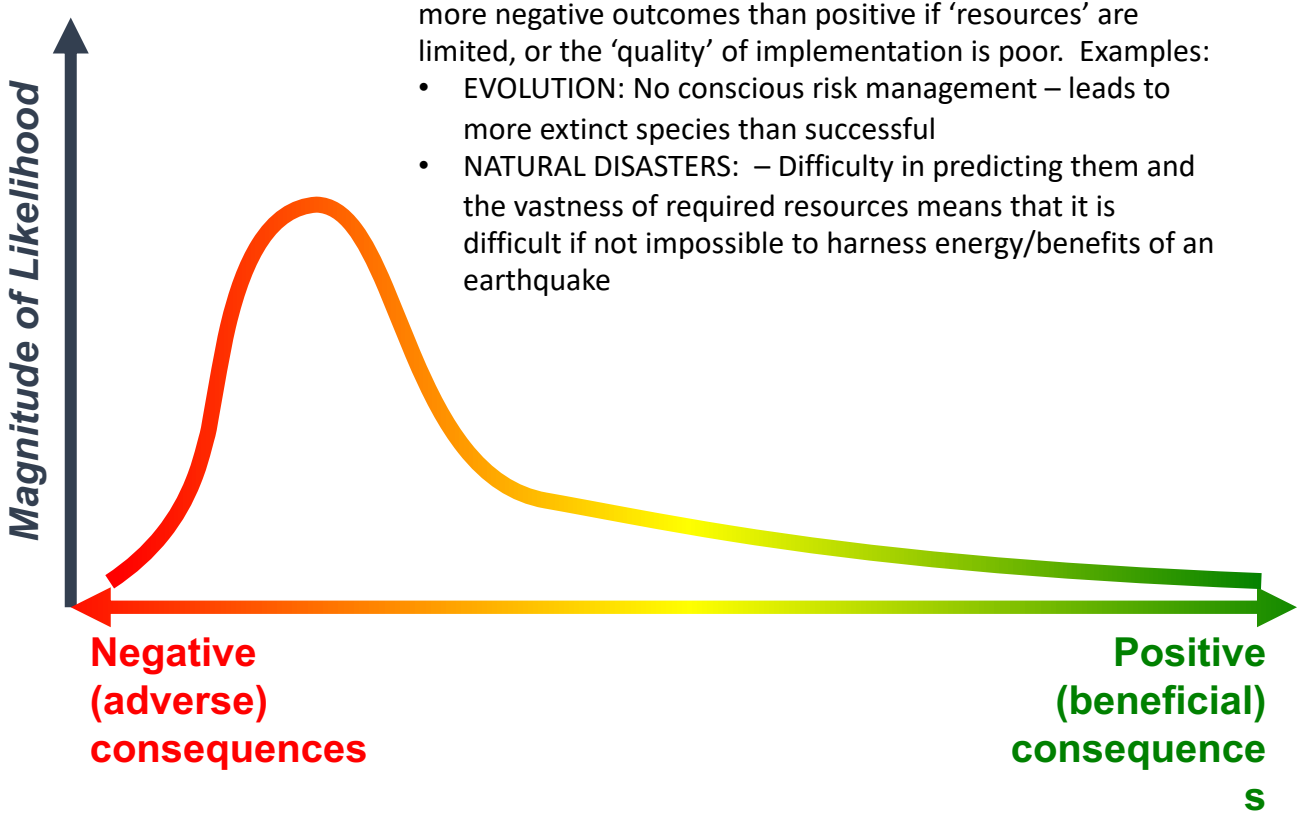


Source: Security Risk Management Body of Knowledge (SRMBOK)

POSITIVE V. NEGATIVE OUTCOMES

The "*effect of uncertainty on objectives*" is likely to produce more negative outcomes than positive if 'resources' are limited, or the 'quality' of implementation is poor. Examples:

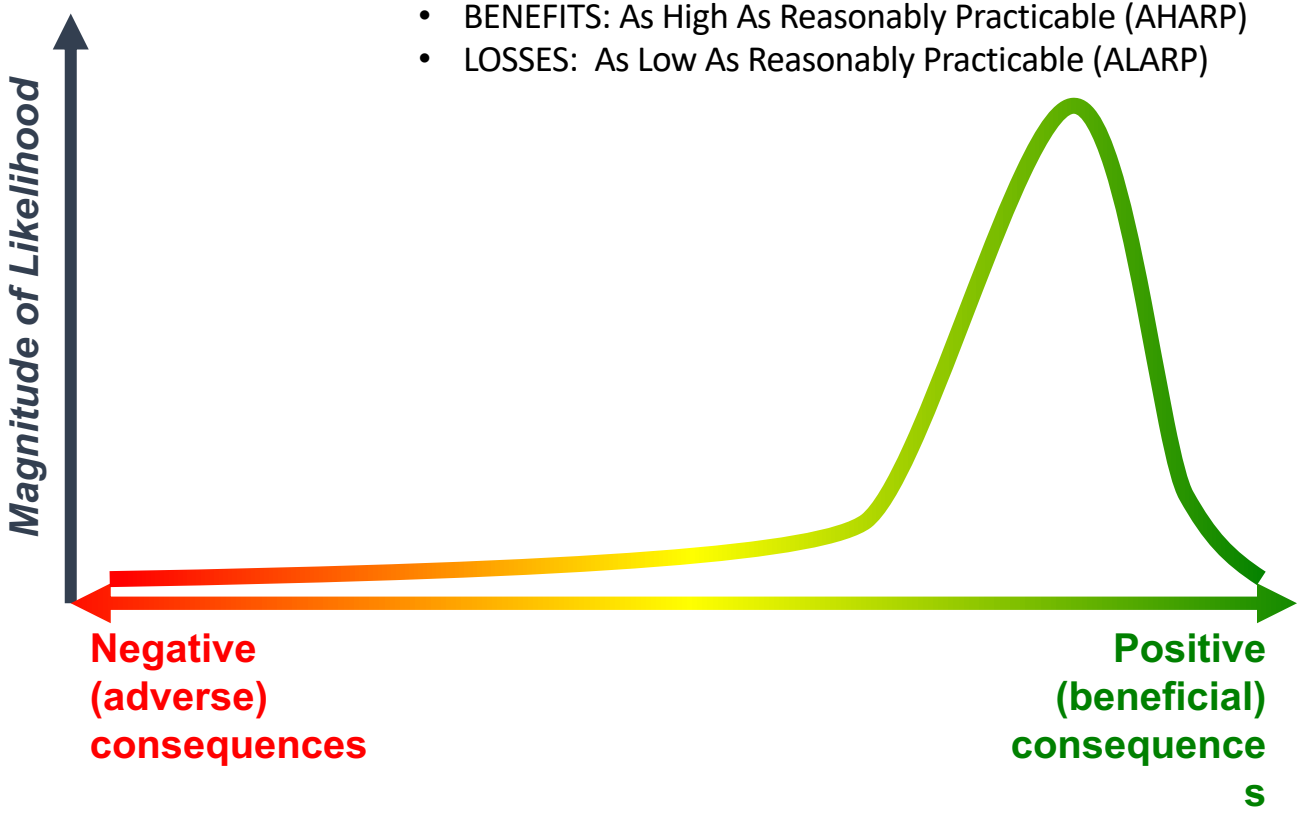
- EVOLUTION: No conscious risk management – leads to more extinct species than successful
- NATURAL DISASTERS: – Difficulty in predicting them and the vastness of required resources means that it is difficult if not impossible to harness energy/benefits of an earthquake



POSITIVE V. NEGATIVE OUTCOMES

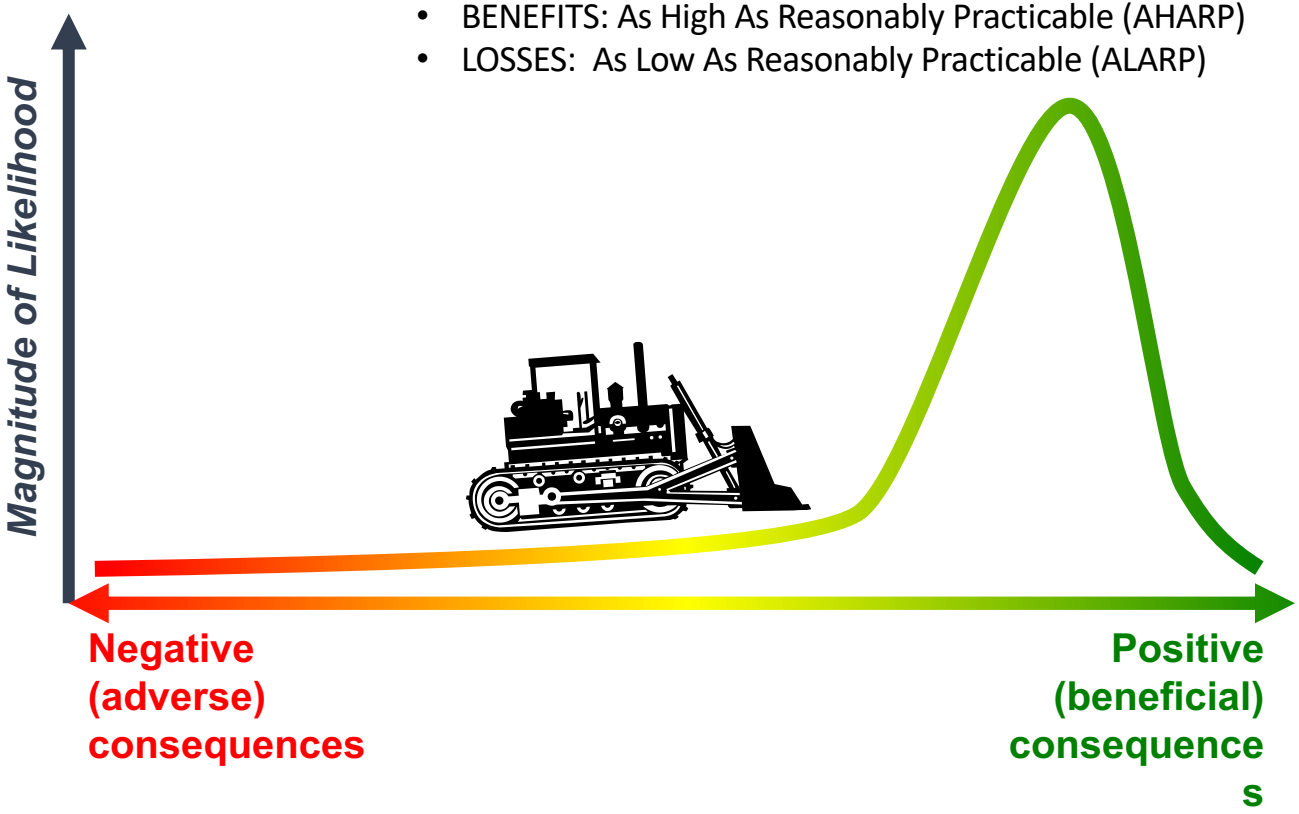
Target area for the "*effect of uncertainty on objectives*" is:

- BENEFITS: As High As Reasonably Practicable (AHARP)
- LOSSES: As Low As Reasonably Practicable (ALARP)

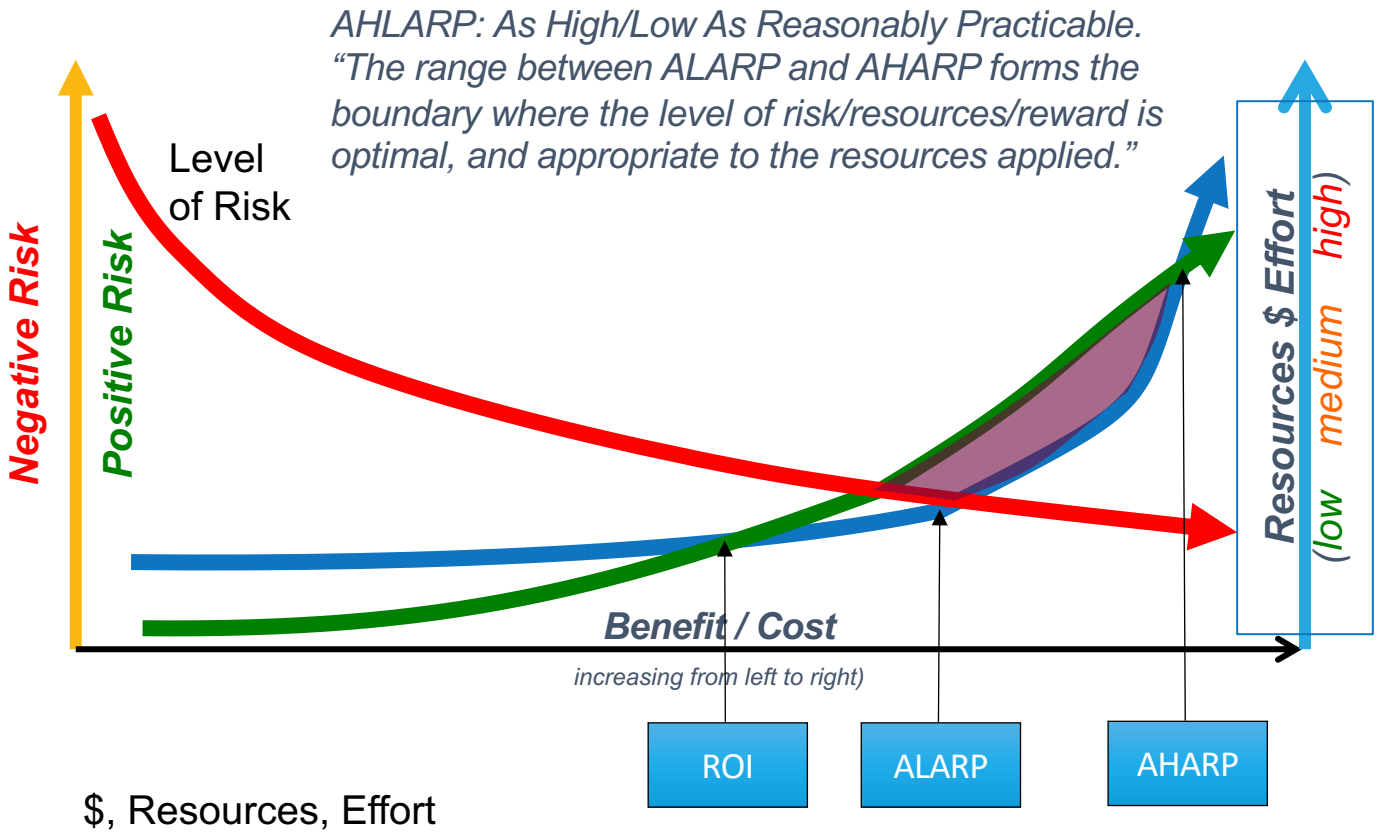


Target area for the "*effect of uncertainty on objectives*" is:

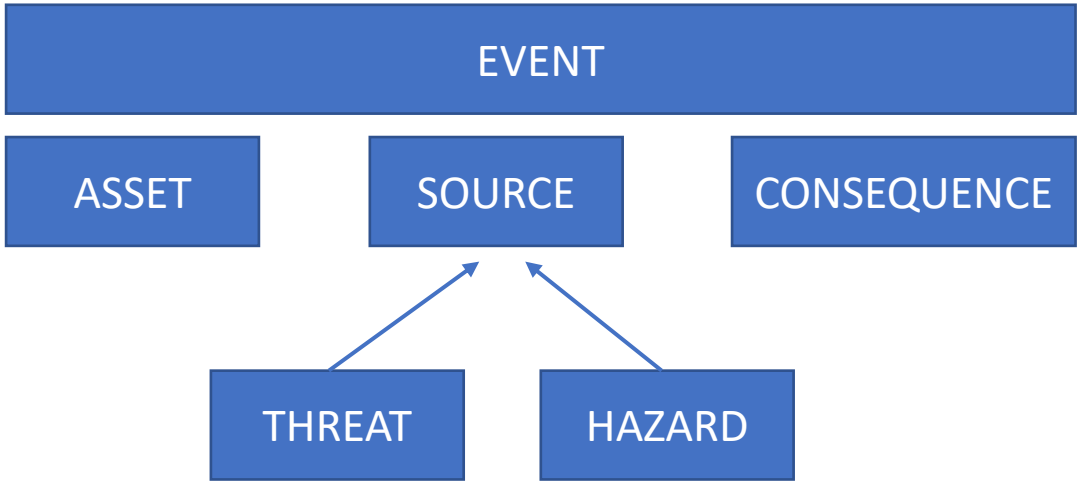
- BENEFITS: As High As Reasonably Practicable (AHARP)
- LOSSES: As Low As Reasonably Practicable (ALARP)



COST/BENEFIT OF MITIGATION



Risk = “the effect of uncertainty on objectives”

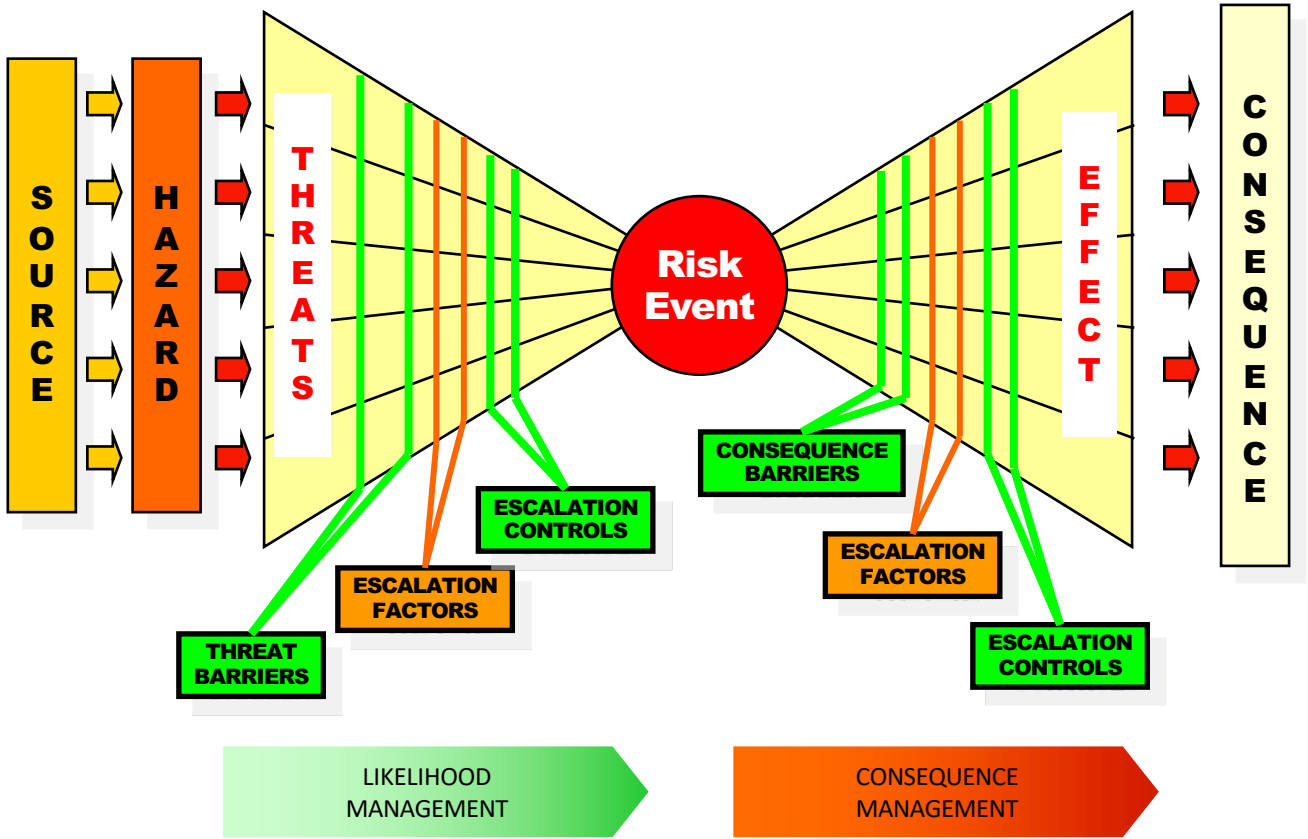


Inherent, Current, Residual


Swiss Cheese and
Bow Ties

Likelihood vs Consequence

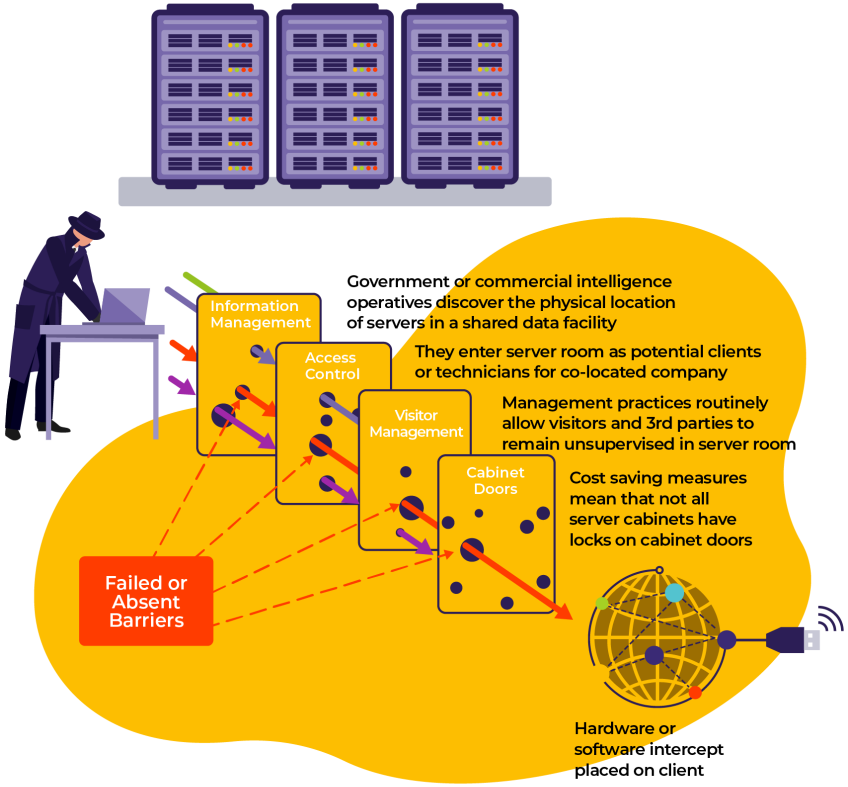
Risk Bow-Tie


SOURCE
HAZARD
THREATS
Risk Event
EFFECT
CONSEQUENCE
ESCALATION CONTROLS
ESCALATION FACTORS
THREAT BARRIERS
CONSEQUENCE BARRIERS
ESCALATION FACTORS
ESCALATION CONTROLS
LIKELIHOOD MANAGEMENT
CONSEQUENCE MANAGEMENT

Swiss Cheese Theory

Swiss-Cheese Example

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.

Swiss Cheese

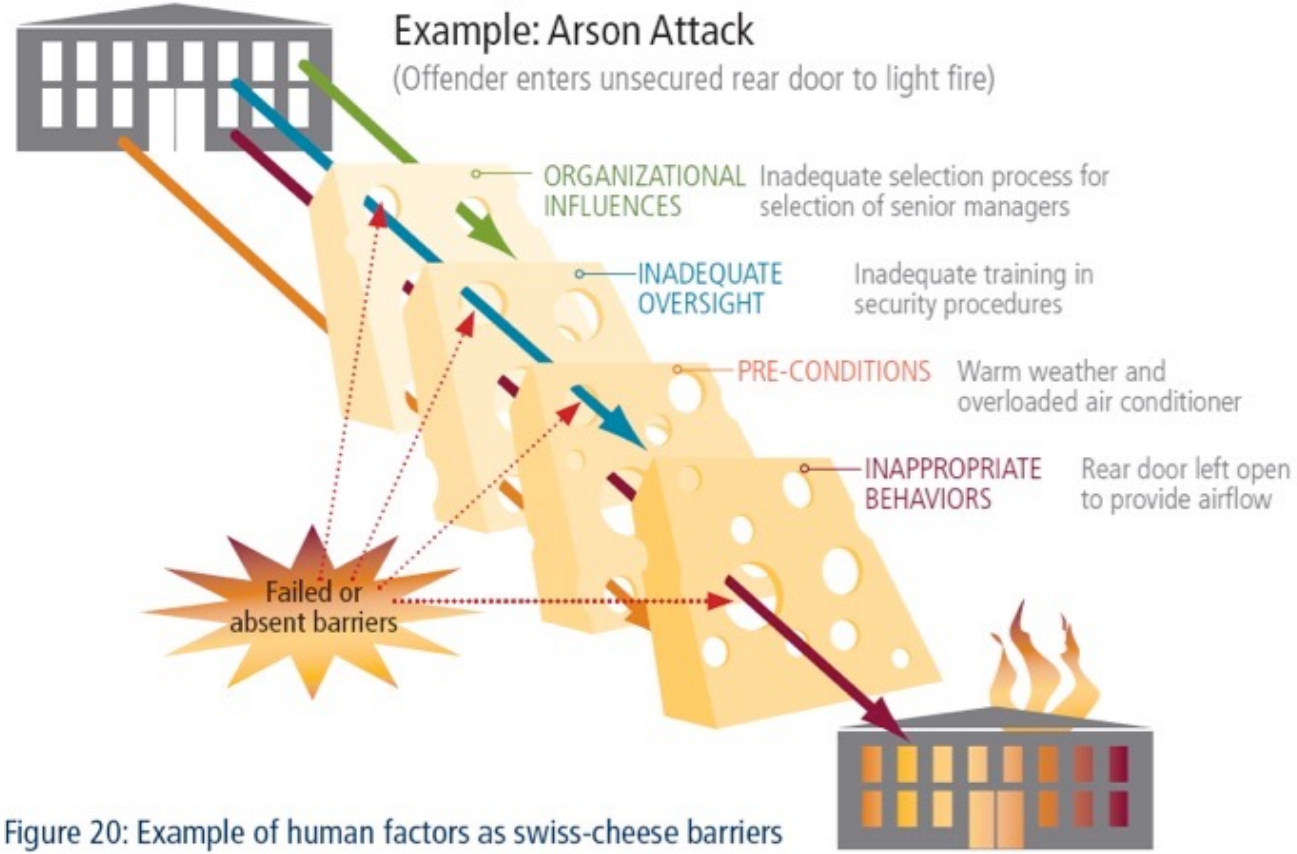
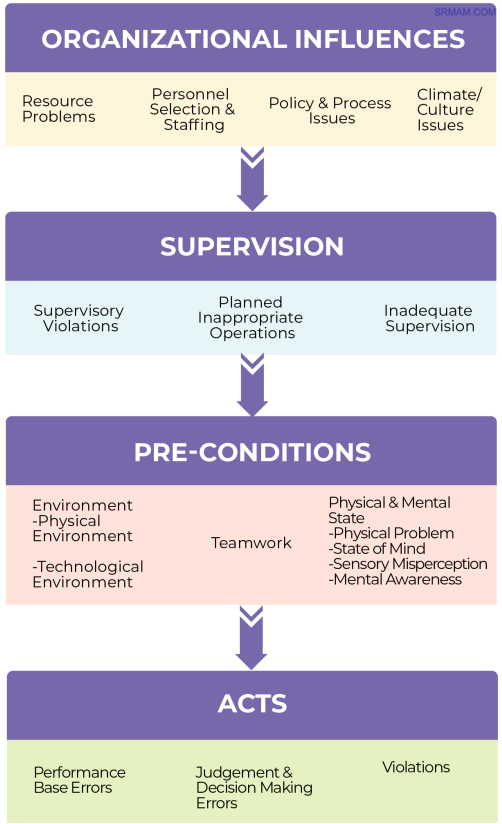


Figure 20: Example of human factors as swiss-cheese barriers

Human Factors Analysis Classification System (HFACS)

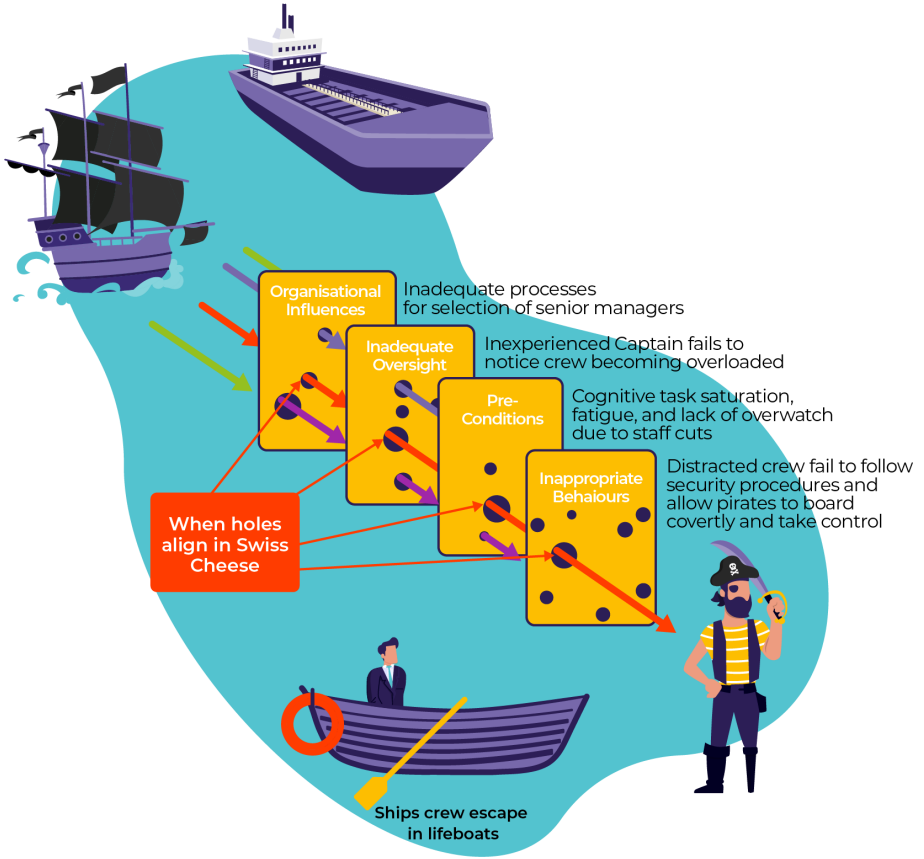


Source: US Dept of Defence

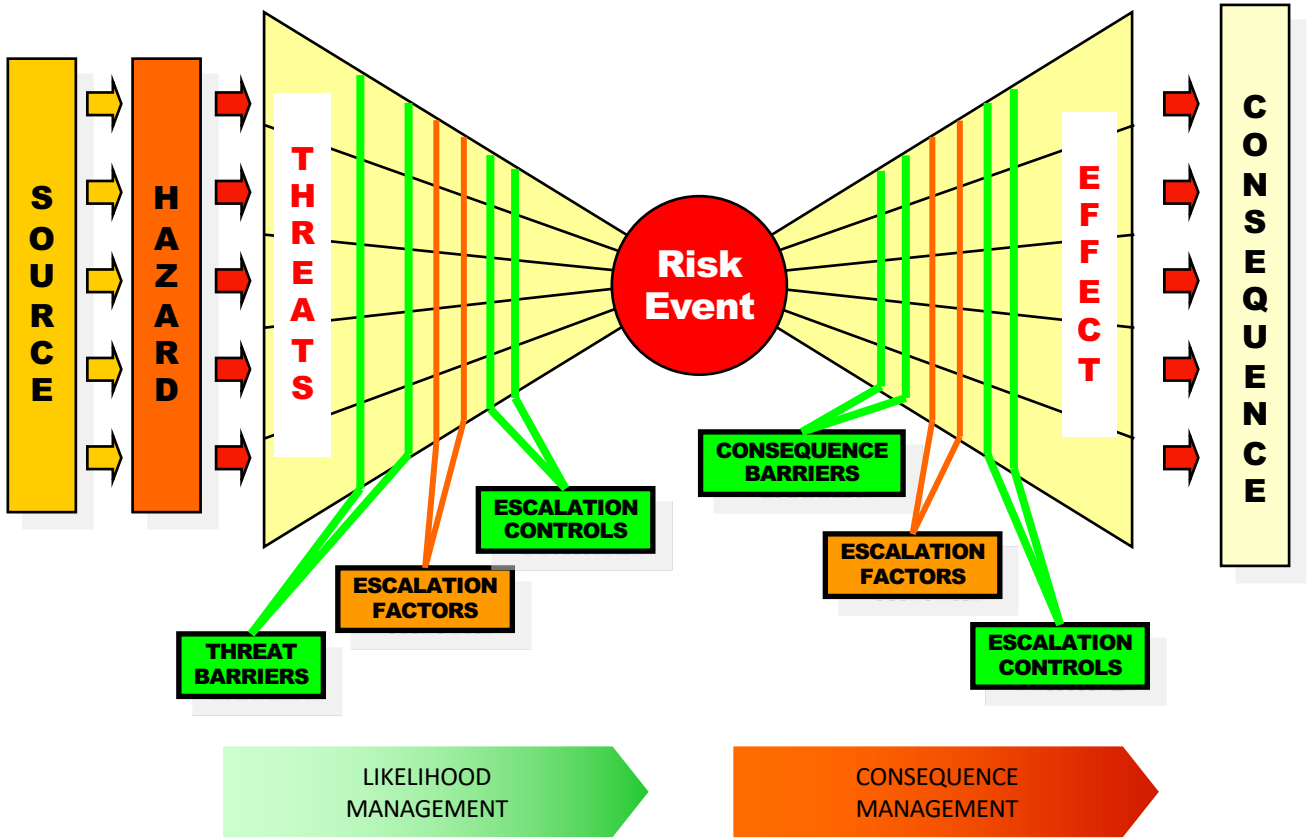
Swiss Cheese

Human Factors

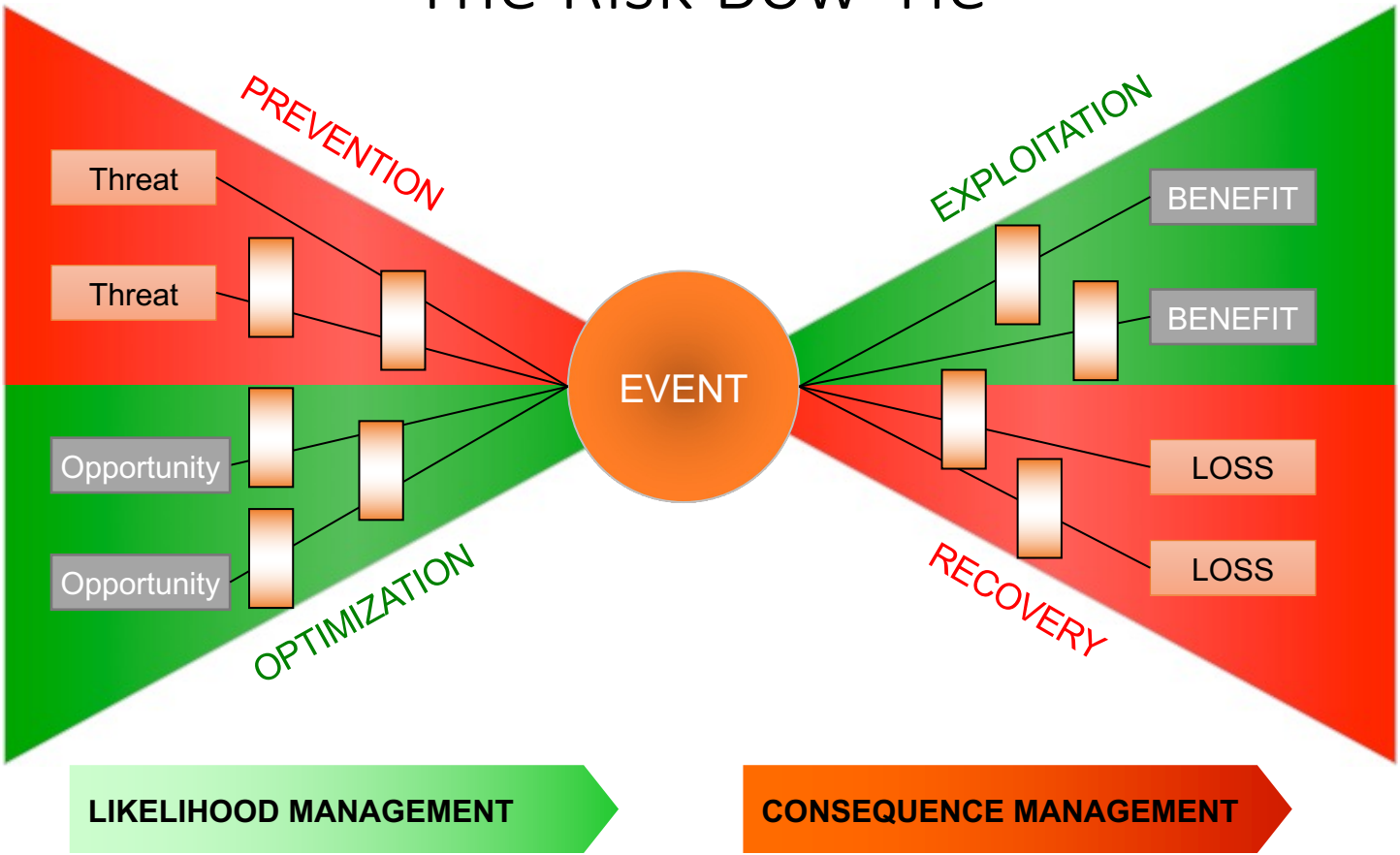
In this example, a series of Human Factors allows a boat load of pirates to gain access to an oil tanker, resulting in loss of ship



Likelihood vs Consequence



The Risk Bow-Tie

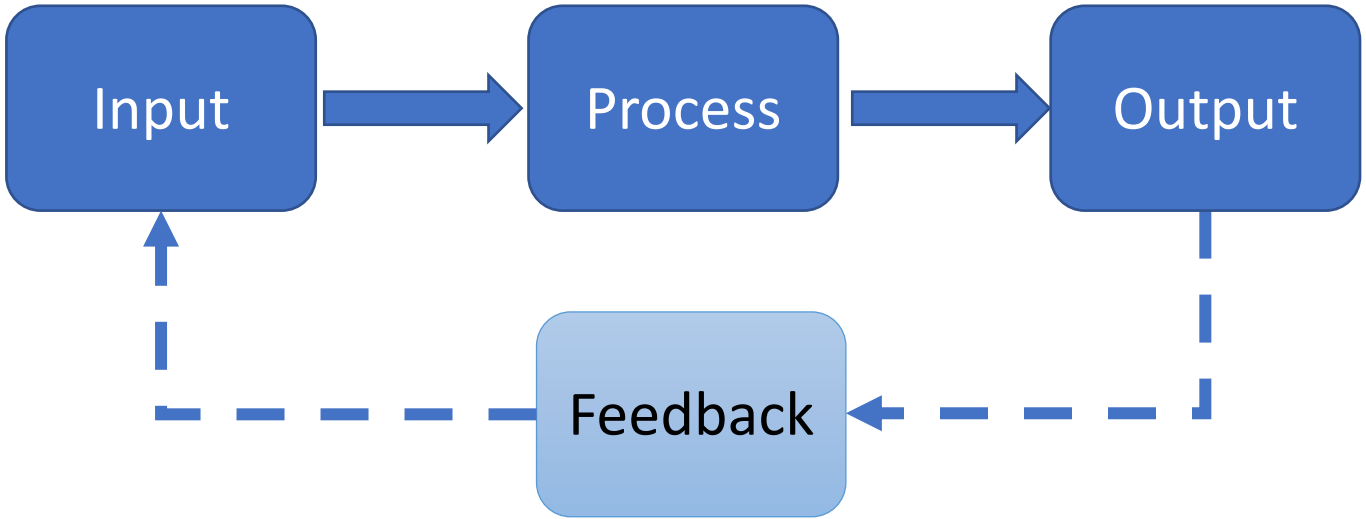


Risk management systems

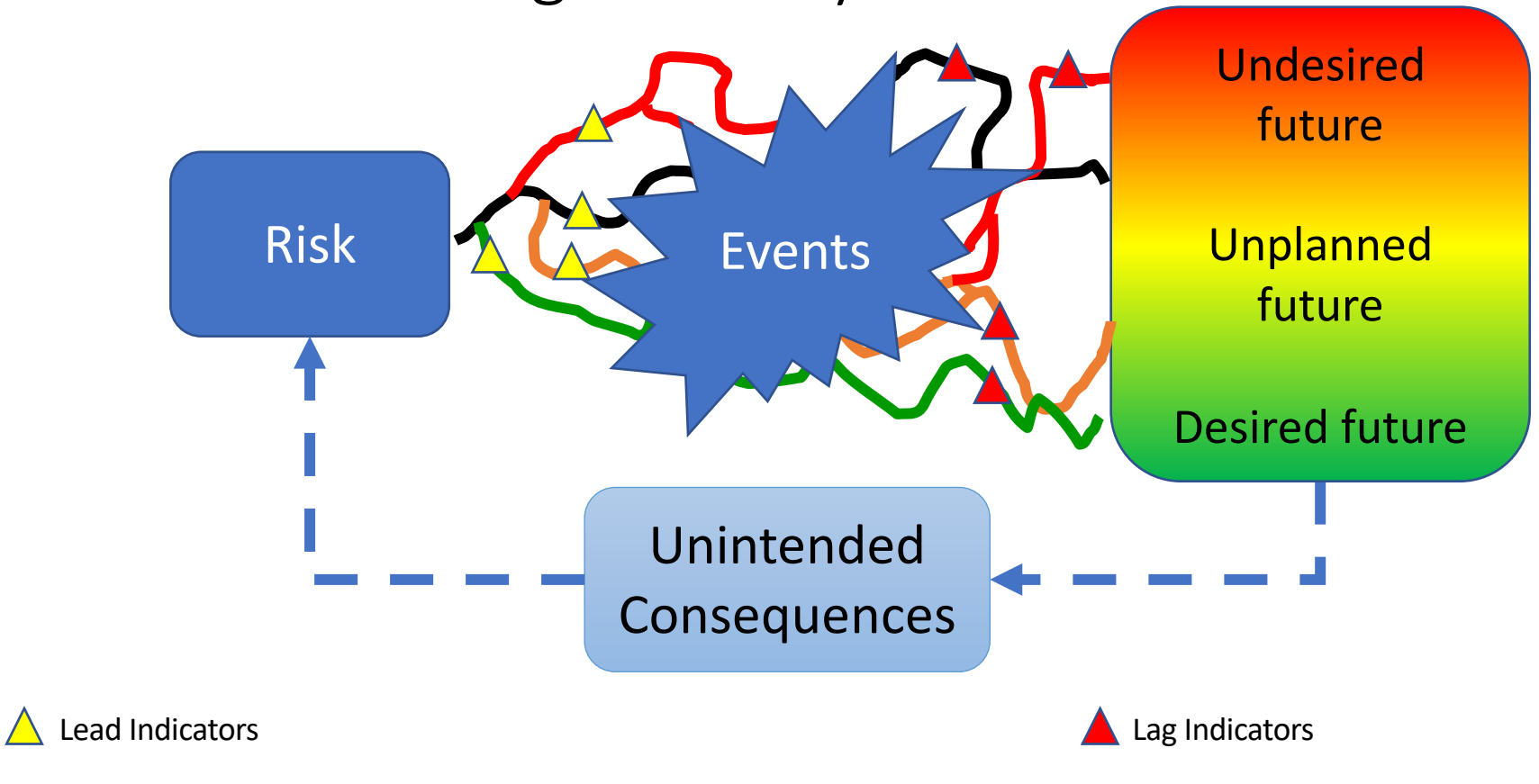
What is management?

Management is the *efficient, effective* and *economic* use of resources to achieve results with and through the efforts of other people.

How Management Systems Work



How Risk Management Systems Work



Operational Risk Management

MANAGEMENT SYSTEMS

- Policies, Procedures, Protocols, Guidance, Forms, Standards, Codes of Practice
- The why, what, when, who, where and how

ASSURANCE FRAMEWORKS

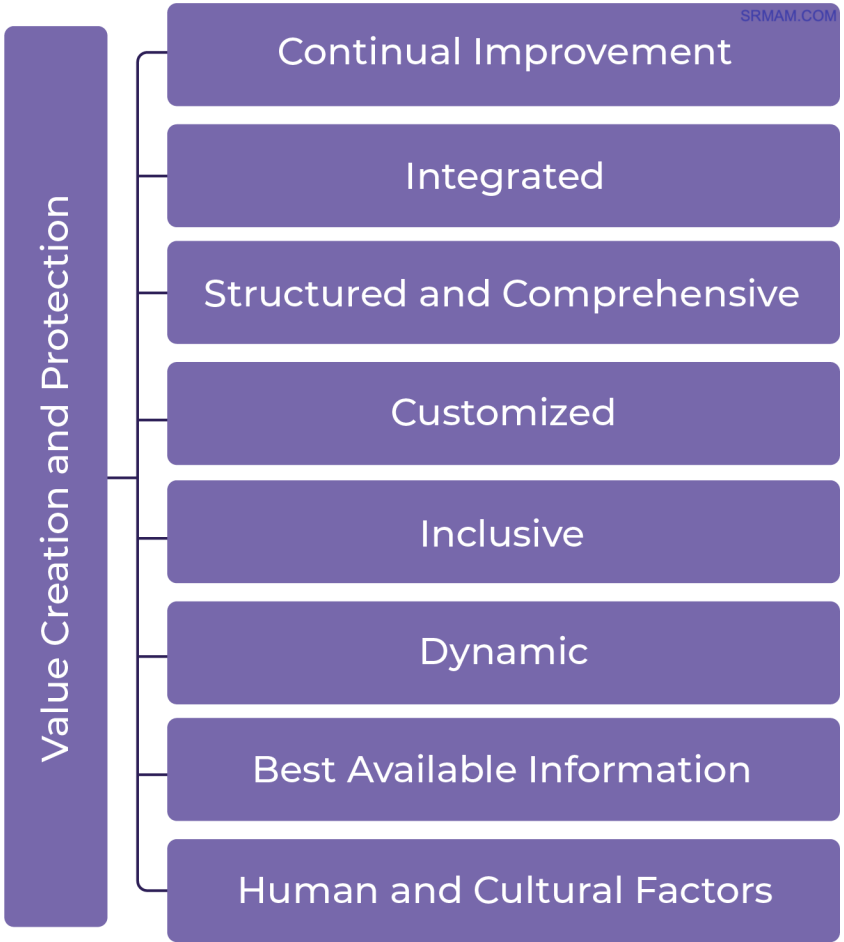
- Training, capability, competency, resources, communication,
- Ensuring there is a capability to execute

COMPLIANCE AND FEEDBACk

- Audits, Photos, Certifications, ICT logs, Incident reports
- Validation and monitoring of management and assurance

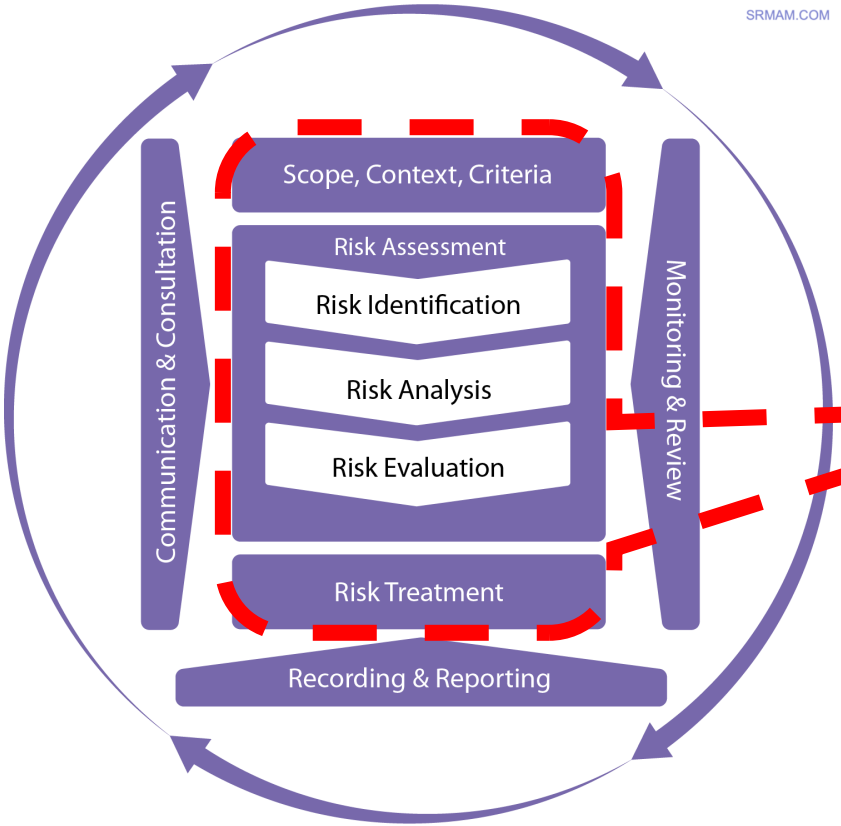

ISO31000 Principles, Framework, Process

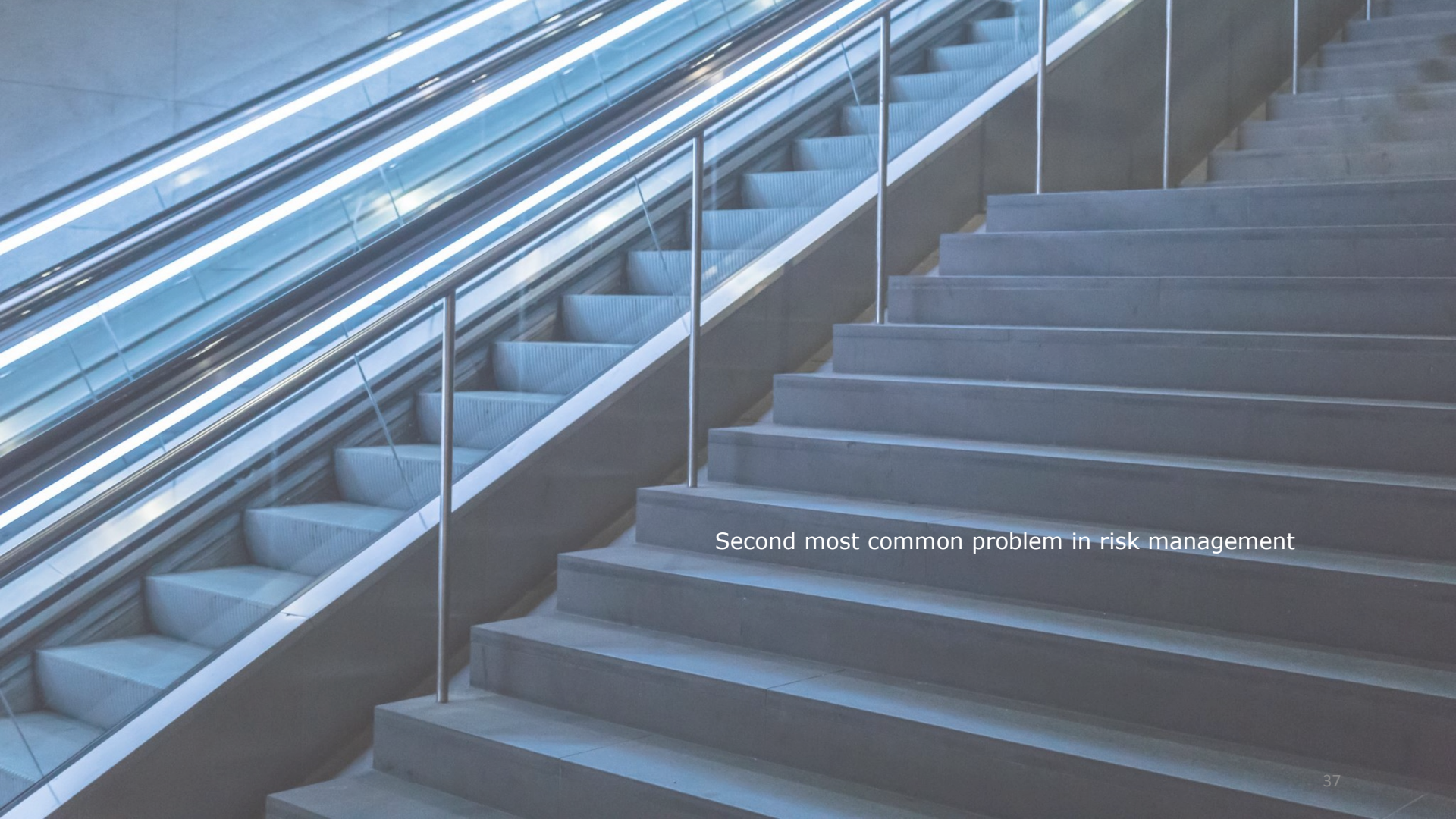
ISO31000:2018 Risk Management Guidelines - Principles



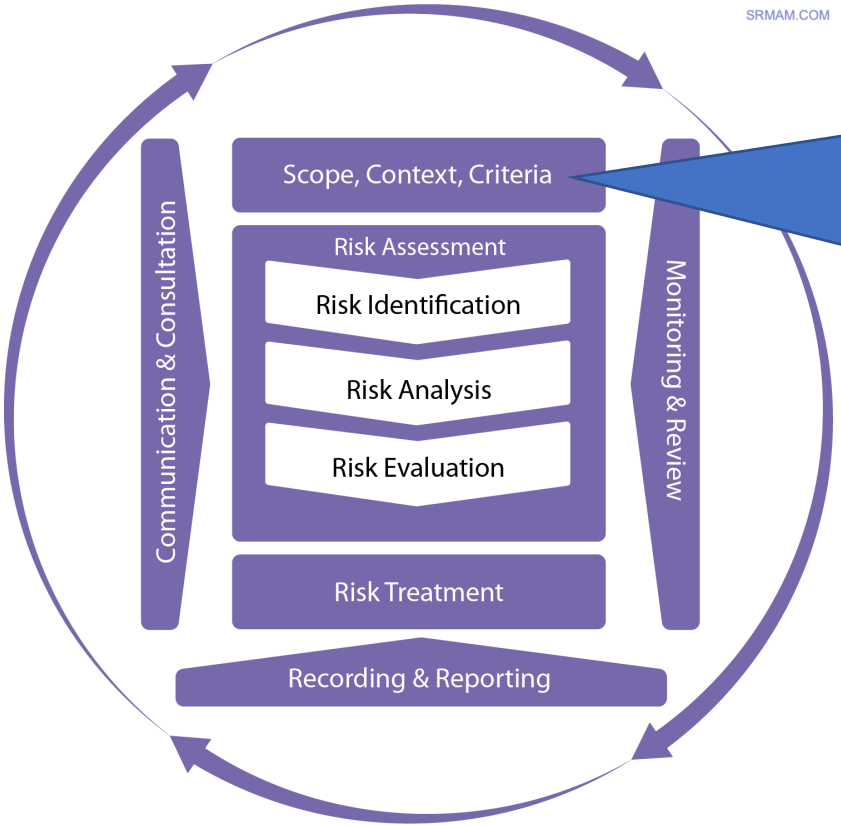
ISO31000 Framework

ISO31000 Process




Second most common problem in risk management

Scope, Context, Criteria



Second most common error in risk management

Failure to define 5W1H

- What
- When
- Who
- Where
- Why
- How

Scope

- Objectives of the assessment
- Objectives and deliverables of the risk assessment
- Timeframe for analysis
- Geographic and virtual locations
- Business unit, group or project being assessed
- Objectives of that group or project
- Constraints and assumptions
- Exclusions - disciplines, geography, demographics
- Risk analysis tools and approach
- Resources
- Responsibilities
- Records to be kept
- Relationships to other groups, projects, processes and activities

CONTEXT

External – PESTLE

- Political influences - legislation, trade tariffs, policy changes.
- Economic factors, global & local.
- Social influences, expectations, trends, and demographics.
- Technological changes and implications.
- Legal environment & compliance
- Environmental factors such as pollution, climate change, stakeholder expectations, etc.

Internal – MORTAR

- Management systems: policies, procedures, processes,
- Organization: culture, vision, objectives
- Resources: capabilities, cashflow, people, property, information, IP
- Technologies: robotics, information, communication,
- Accountability: structure, ownership, governance
- Relationships: stakeholders, interconnections, dependencies

Context - SWOT ANALYSIS

CRITERIA

Score	Rating	Description
5	Effective	Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks.
4	Limited improvement needed	Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified.
3	Significant improvement needed	Key controls and/or management activities in place, with significant opportunities for improvement identified.
2	Ineffective	Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and are somewhat ineffective in efficently mitigating risk or driving effeciency.
1	Highly ineffective	Controls and/or management activities are non-existent or have major deficiencies and do not operate as intended. Controls and/or management activities as designed are highly ineffective in efficiently mitigating risk or driving effeciency.

Score	Rating	Certainty	Frequency
5	Expected	>90 percent	At least yearly and/or multiple occurences within the year
4	Highly likely	<90 percent	Approximately every 1-3 years
3	Likely	<60 percent	Approximately every 3-7 years
2	Unlikely	<30 percent	Approximately every 7-10 years
1	Rare	<10 percent	Every 10 years and beyond or rarely

Score	Rating	Description of impact						Recovery
		Safety and security	Duration	Organizational and operational scope	Reputational impact	Impact on operations	Financial impact (measured in terms of budget)	Required action to recover
5	Critical	Loss of life (staff, partners, general population)	Potentially irrecoverable impact	**Organization-wide:** inability to continue normal business operators across the Organization.	Reports in key international media for more than one week	Inability to perform mission or operations for more than one month	>5 percent >$500 million	Requires significant attention and intervention from General Assembly and Member States
4	Significant	Loss of life due to accidents/ non-hostile activities	Recoverable in the long term (i.e., 24-36 months)	**Two (2) or more departments/offices or locations:** significant, ongoing interruptions to business operations within 2 or more departments/offices or locations	Comments in international media/forum	Discruption in operations for one week or longer	3-5 percent $300 million-$500 million	Requires attention from senior management
3	High	Injury to United Nations staff, partners and general population	Recoverable in the shortterm (i.e., 12-24 months)	**One (1) or more departments/offices or locations:** moderate impact within one or more departments/offices or locations	Several external comments within a country	Discruption in operations for less than one week	<2-3 percent $200 million-$300 million	Requires intervention from middle management
2	Moderate	Loss of insfrastructure, equipment or other assets	Temporary (i.e., less than 12 months)	**One (1) department/office or location:** limited impact within department/office or location	Isolated external comments within a country	Moderate disruption to operations	<1-2 percent $100 million-$200 million	Issues delegated to junior management and staff to resolve
1	Low	Damage to insfrastructure, equipment or other assets	Not applicable or limited impact				<1 percent <$100 million	Not applicable or limited impact

Risk identification exercise

EXERCISE

Risk or Issue?

1) Is the following a well-written risk definition?

"Fatigue cracks discovered in already delivered military vehicles may shorten service life unless remedied."

a) Yes

b) No

Answer is No: This statement describes an issue, not a risk. There is no uncertainty about the likelihood of occurrence.

Risk identification and reporting

Clarity

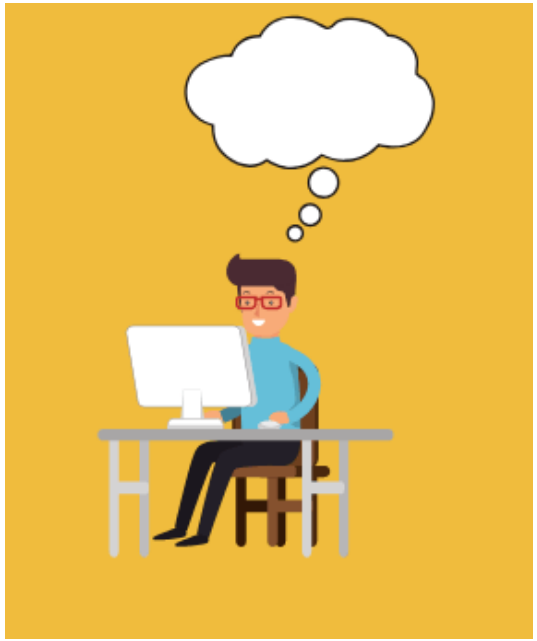

At least we all agree on the basics like the meaning of the word "risk"
Anything that reduces my annual bonus
Risk= danger!
Wait, what?
Opportunity?
The effect of uncertainty in our definitions?
Boring!

ELEMENTS OF POORLY WRITTEN RISK DEFINITIONS

Poorly written risk definitions do not promote understanding or support productive action.

They may confuse risk with cause or consequences, or they may not describe consequences accurately.

E.g., an entity may identify a risk as "**inadequate staffing**" when in fact the inadequate staffing should be considered a **cause/ driver** that may pose a variety of risks or consequences such as reduced quality, delays, or even workforce turnover.



The ‘CASE’ for identifying risks

ICT Governance & Cybersecurity

- Data breach
- Espionage
- Phishing attack

Terrorism is not a risk

- What impact/objective?
- By who/what?
- Against who/what?
- What event/act?

The CASE for Risk Identification

Consequence

- Effect on objectives

Assets at risk

- Resources impacted

Source

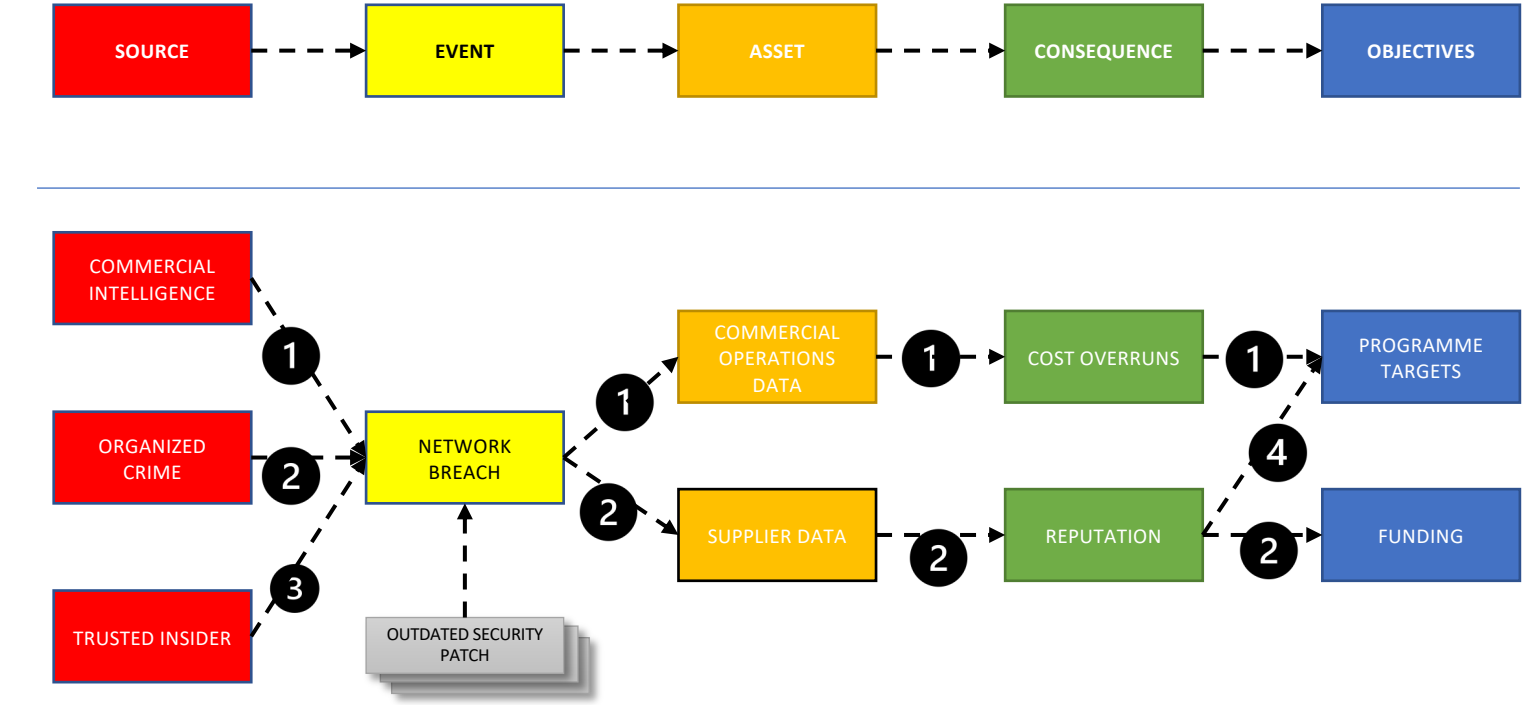
- Threat or hazard

Event

- Incident / act

Phishing – Also not a Risk

Phishing attack (EVENT) against our database of commercially sensitive budget and contract information (ASSET)
by commercial providers (SOURCE) impacts our negotiating ability, leading to cost overruns on programmes (CONSEQUENCE).



1 *Failure to achieve objectives within budget due to commercial intelligence operators breaching network and providing sensitive supplier cost information to their clients (our suppliers).*

Identifying Risks from First Principles

Consequence	Asset	Source	Event	Objectives
Harm	People	Inadequate maintenance	Slips, trips, falls	Safety
Loss	Information	State sponsored hackers	Ransomware	Customer satisfaction
Theft	Property	Competitors	Petty theft	Compliance
Product quality	Economic	Religious fundamentalists	Improvised explosive device	Capability
Staff turnover	Reputation	Pandemic	Illness	Profit
Reputation	Inventory	Wholesalers	Trade Fair	Revenue Growth
Sales	Equipment	International markets	Webinars	Health

EXERCISE

Risk Definitions

2) Which of the following is a well-written risk definition?

a) Shortage of competent staff to complete program on time.

b) Failure to achieve project deliverables due to financial overruns as a result of inadequate staffing due to high demand for the required skillset.

Answer is b: The focus of the risk statement should be poor performance/failure to deliver results: Failure to achieve project deliverables (CONSEQUENCE) due to financial (ASSET) overruns as a result of inadequate staffing (EVENT) due to high demand for the required skillset (SOURCE)**.**

Example

- Risk: Loss of operational capability due to the mzungu failing to anticipate the difficulty of finding qualified drivers in a region where most people walk everywhere and live in grass huts.
- Treatment: Bring in a qualified mechanic and some army mates to help develop and deliver a driver training program so that the vehicles will last (a little bit) longer.

Your Risks

- Think about one of your risks (or make one up).
- Write it in a sentence using CASE
  - Consequence
  - Asset
  - Source
  - Event
- Copy and paste it into the chat box
- We will vote on the best one
- Bonus points for humour or improbable risks

CASE OF RISK IDENTIFICATION

CONSEQUENCE

- What is the impact?
- The effect on objectives.

ASSET

- Which assets are involved?
- The resources, entity, or capabilities.

SOURCE

- What is the source of the risk?
- The threat(s) or hazard(s).

EVENT

- How is the risk likely to manifest?
- The incident, act, or mishap.

RISK MANAGEMENT CONTROLS

MANAGEMENT SYSTEMS

- Policies, Procedures, Protocols, Guidance, Forms, Standards, Codes of Practice
- The why, what, when, who, where and how

ASSURANCE FRAMEWORKS

- Training, capability, competency, resources, communication,
- Ensuring there is a capability to execute

COMPLIANCE AND FEEDBACk

- Audits, Photos, Certifications, ICT logs, Incident reports
- Validation and monitoring of management and assurance

4C'S OF RISK FINDINGS & OBSERVATIONS

CONDITION

- What is happening?
- Observable artefacts.

CRITERIA

- What should be happening?
- The policy, procedure, requirement or best practice.

CONSEQUENCE

- What is, or will be, the outcome?
- The impact on objectives

CAUSE

- What is the cause of this situation?
- The underlying systemic root cause.

4AS OF RISK TREATMENTS

ACTIONABLE

- Is it clear what to do?
- Specific, measurable and time bound.

ACHIEVABLE

- How will you know when you have done it?
- Metrics for success, ideally binary with a yes/no gate.

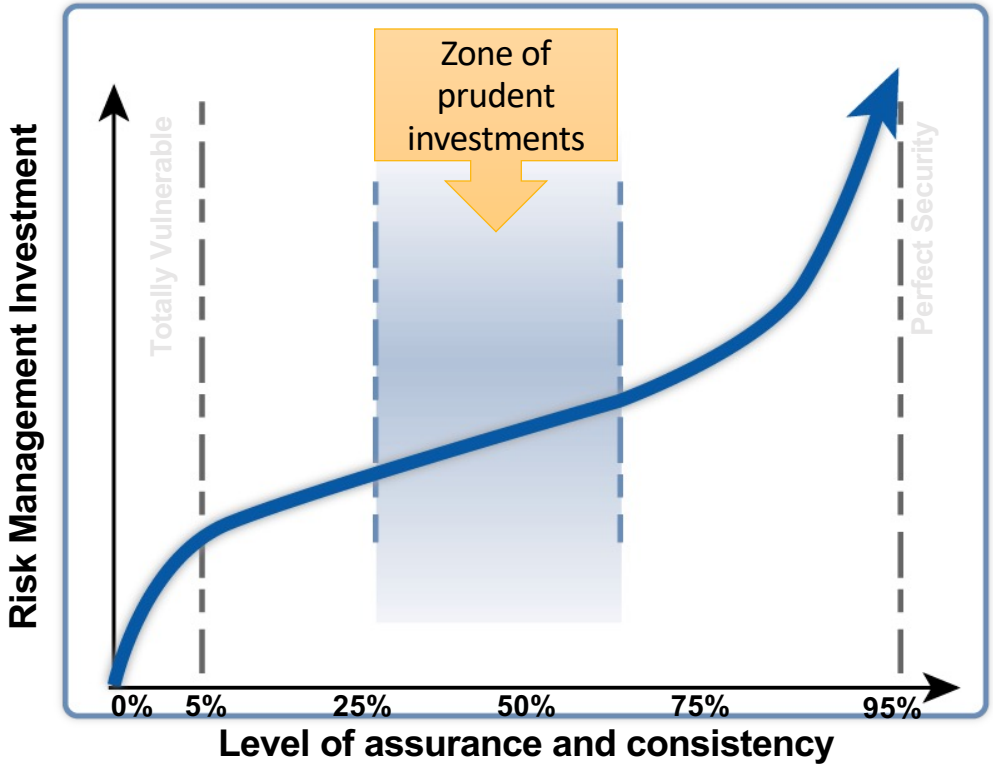
APPROPRIATE

- Does it address the root cause?
- Address underlying cause, not the immediate issue.

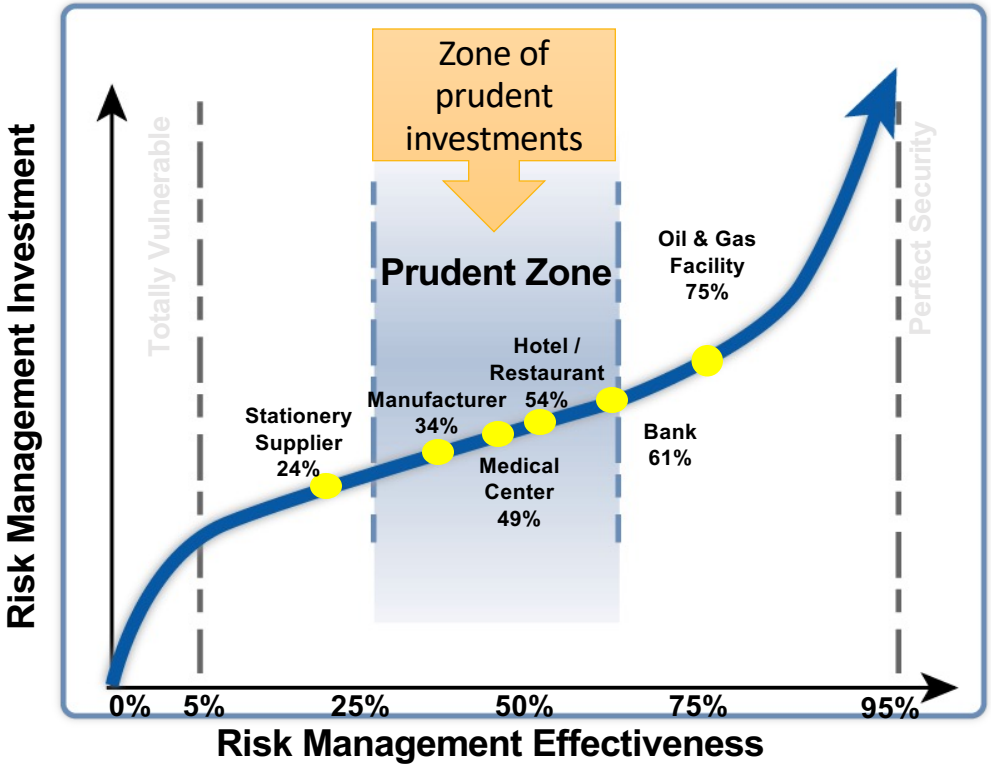
AGREED

- Do the review team and risk owner support this?
- Supported by management and adequate resources.

Investment vs. Effectiveness of risk treatments



Investment vs. Effectiveness of risk treatments




Q&A

Other Training

1 Hour

1 Day

3 Days

5 Days

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

www.juliantalbot.com

www.srmbok.com

www.sectara.com

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)

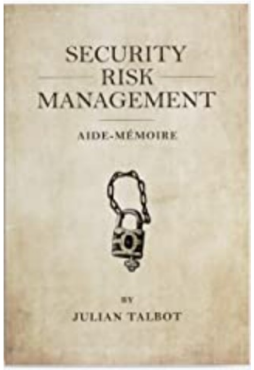
Wed, Sep 28, 2022 9:00 AM AEST

Starts at A$100.00

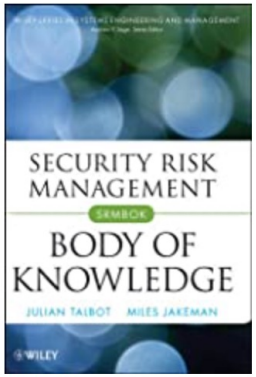
Julian Talbot

✓ Following

Follow to get new release updates and improved recommendations

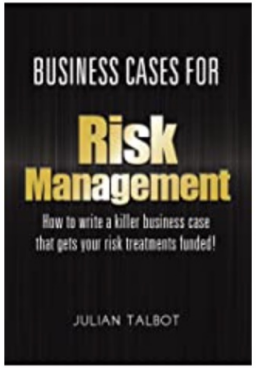


$4.69
Kindle Edition

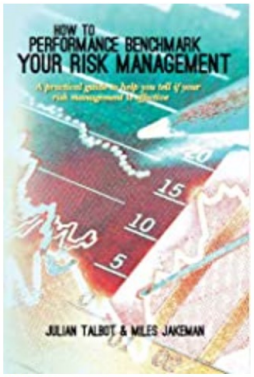


$96.00
Kindle Edition

$4.19
Kindle Edition



$9.99
Kindle Edition



$9.99
Kindle Edition

Julian Talbot CISSP F.ISRM

www.juliantalbot.com

ECTARA™

SRMBOK
Security Risk Management Body Of Knowledge