Extending the Use of Bowties from Safety into Security

Andy Lidstone
Risktec Solutions Ltd

TÜVRheinland®
Risktec

Definitions

- Language may differ
- ….but aims are the same

….risk …. Is defined as an expression of the likelihood that a defined threat will target and successfully attack a specific security vulnerability of a particular target or combination of targets to cause a given set of consequences.

The first step in the process of managing security risks is to identify and analyze the threats and the vulnerabilities facing a facility…….

Ref. API: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

A risk assessment will help you review the threats you might be facing, including their likelihood and impact. You can then identify your vulnerabilities to these threats in a prioritised and proportionate manner and where necessary develop new mitigation strategies.

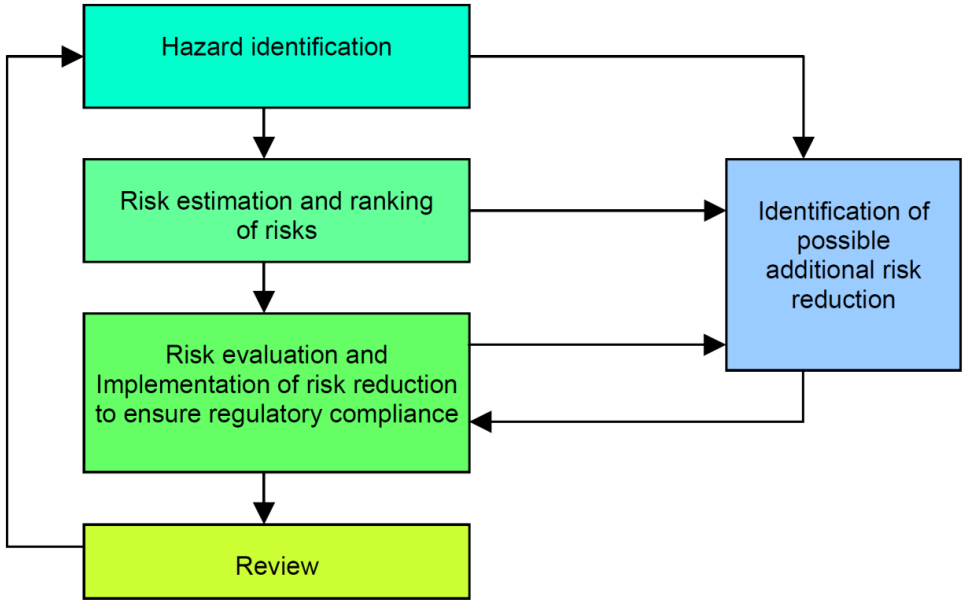
Centre for the Protection of National Infrastructure

..risk …is…combination of the probability of an event and the consequences of the event.

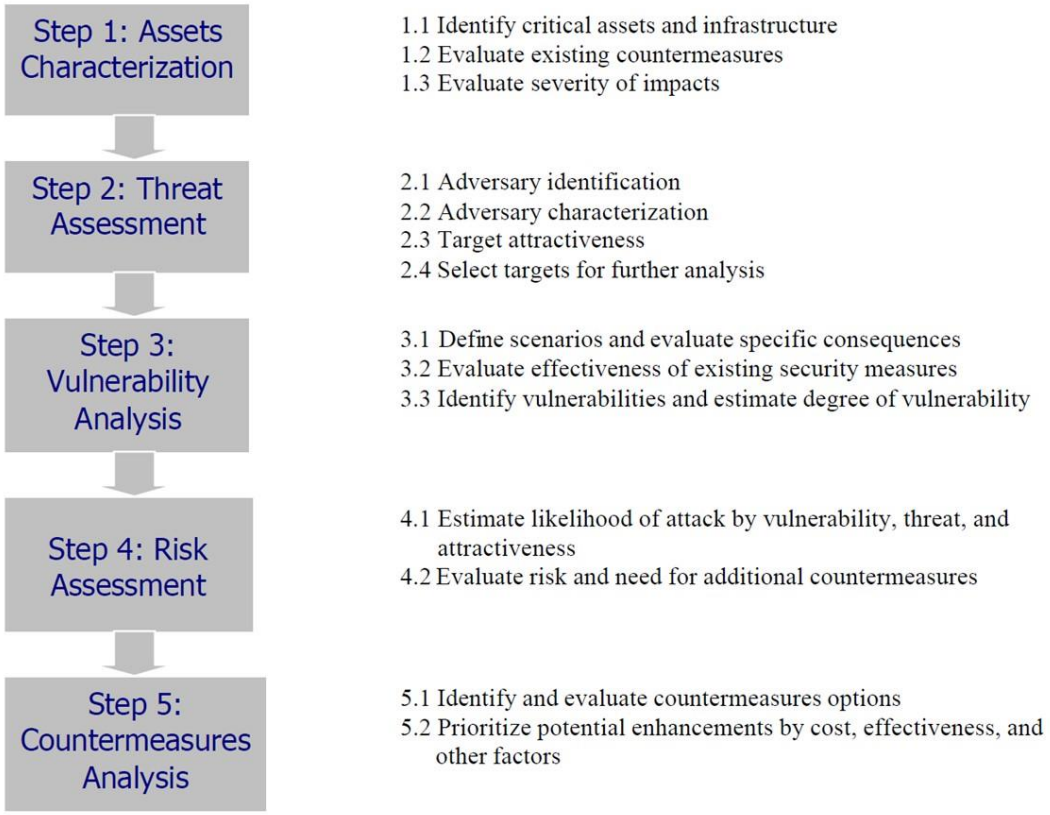
…a systematic approach to the identification of hazards and the assessment of the associated risk in order to provide information to aid decision making on the need to introduce risk reduction measures.

ISO 17776 Petroleum & Natural Gas industries - offshore production installations - Guidelines on tools and techniques for hazard identification and risk assessment

Risk Assessment



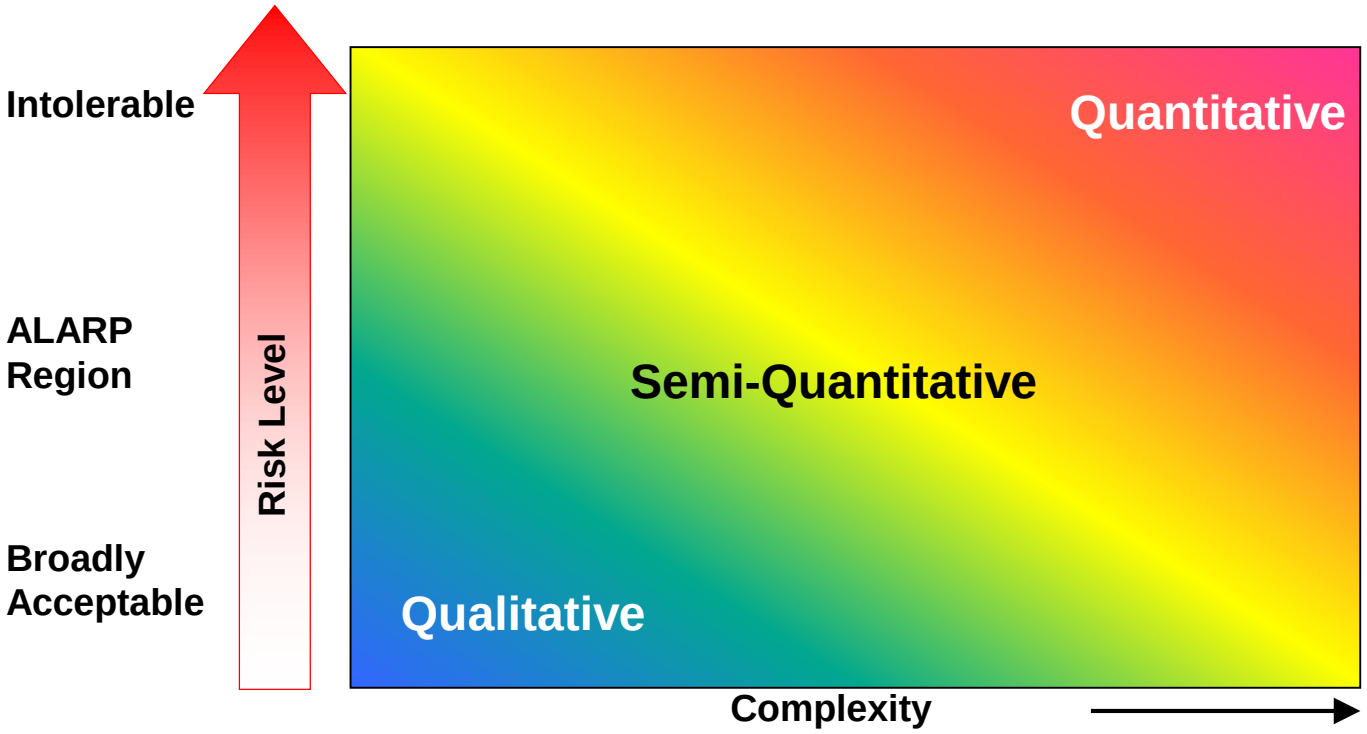
Ref. HSE's Information Sheet Guidance on Risk Assessment for Offshore Installations

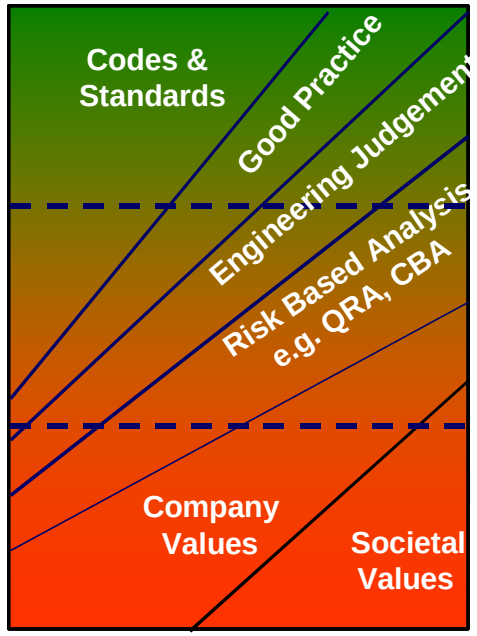


Ref. API: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

TÜVRheinland®
Risktec

Choice of approach





A
- Nothing new or unusual
- Well understood risks
- Established practice
- No major stakeholder implications

B
- Lifecycle implications
- Some risk trade offs/transfers
- Uncertainty/deviation from standard, best practic
- Significant economic implications

C
- Very novel or challenging
- Strong stakeholder views and perceptions
- Significant risk tradeoffs or risk transfers
- Large uncertainties
- Perceived lowering of safety standards

Ref: UKOOA A Framework for Risk Related Decision Support

Low complexity
Solution is obvious
Situation covered by codes and standards

High complexity
Difficult solution
One-off situation
No relevant standards/guidance

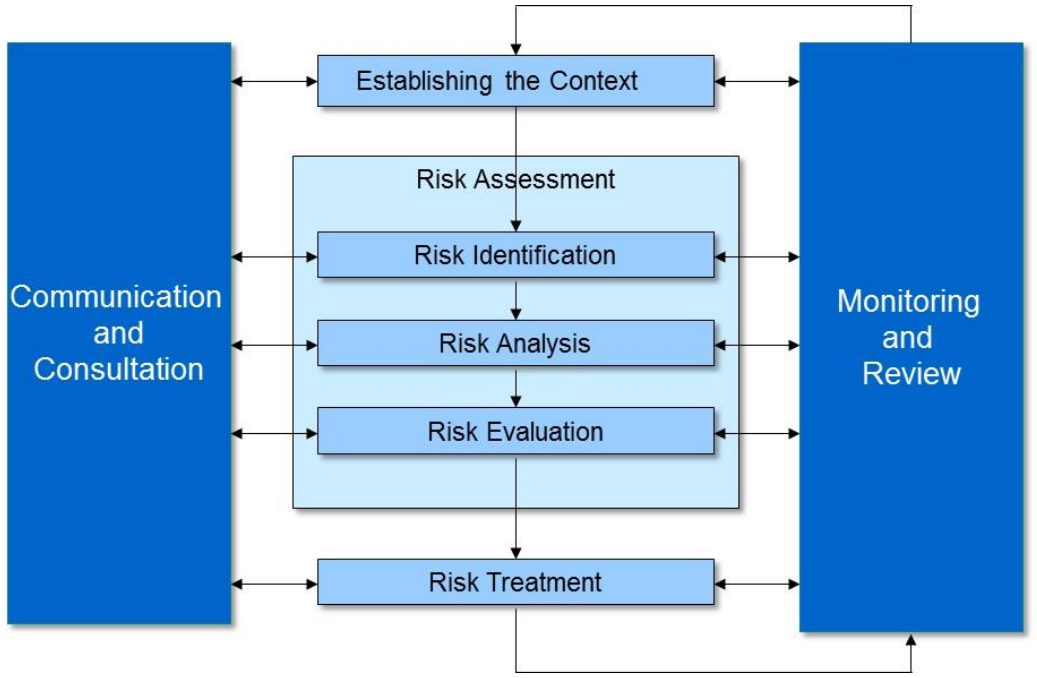
After: Guidance on Risk Assessment for Offshore Industries HSE 3/2006

TÜVRheinland®
Risktec

Basic Premise

The better we understand a risk, the better we can

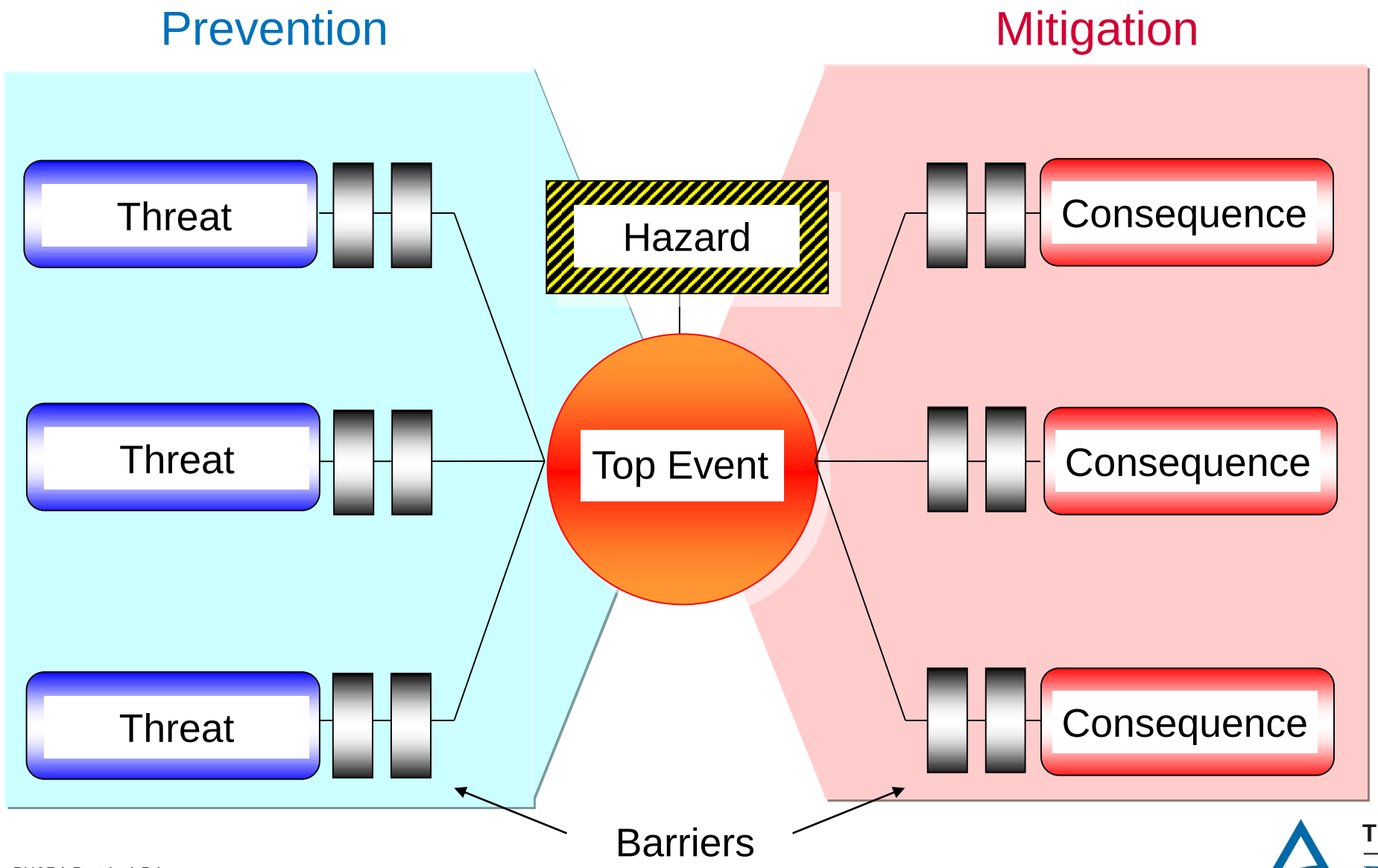
- Evaluate it
- Monitor it
- Audit it
- Communicate it
- Treat it



Ref. ISO 31000

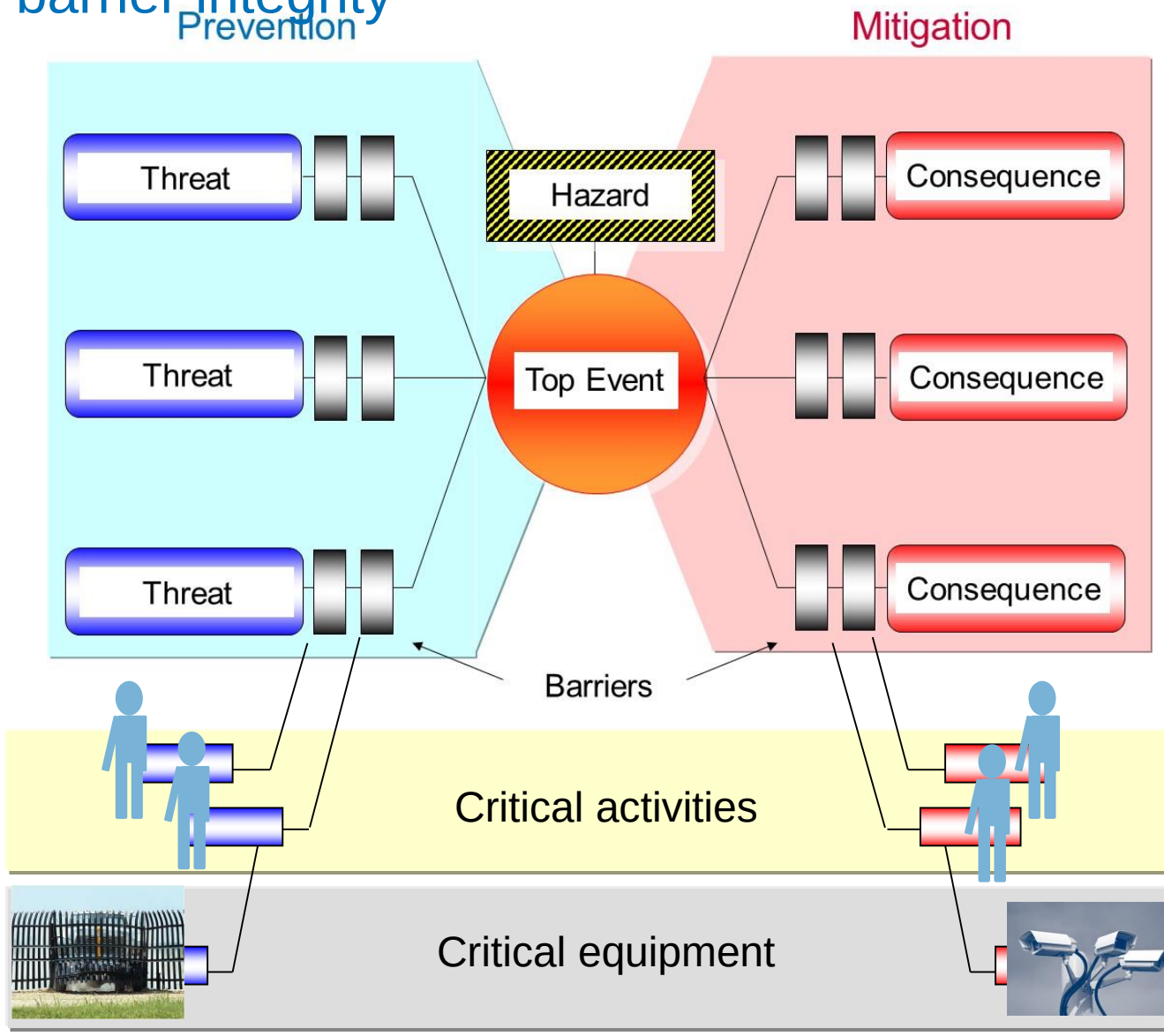
TÜVRheinland®
Risktec

Basic Bowtie diagram



TÜVRheinland®
Risktec

Assuring barrier integrity



Audit and Inspection
=========
To:

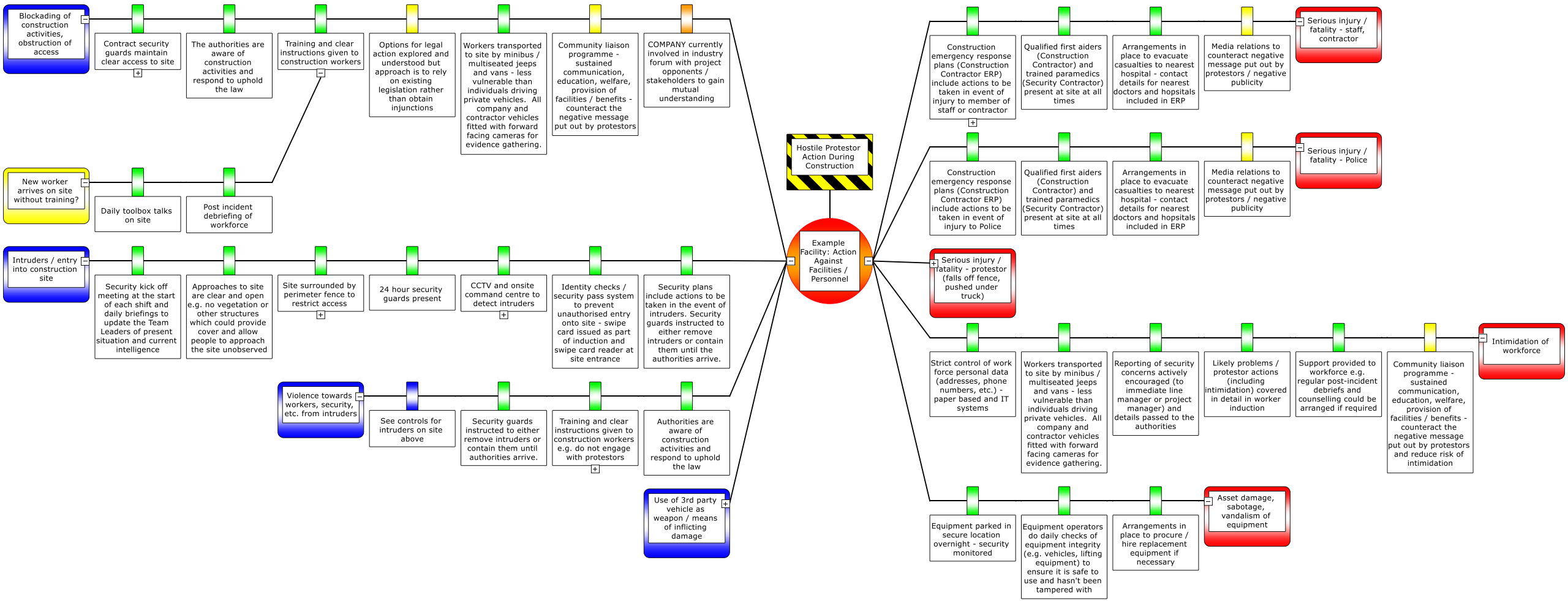
- Check accuracy and currency
- Verify performance

- Job descriptions
- Competency requirements
- Required documentation

- Strategic Design Requirements
- Standards of performance

TÜVRheinland®
Risktec

Example Security Bowtie



TÜVRheinland®
Risktec

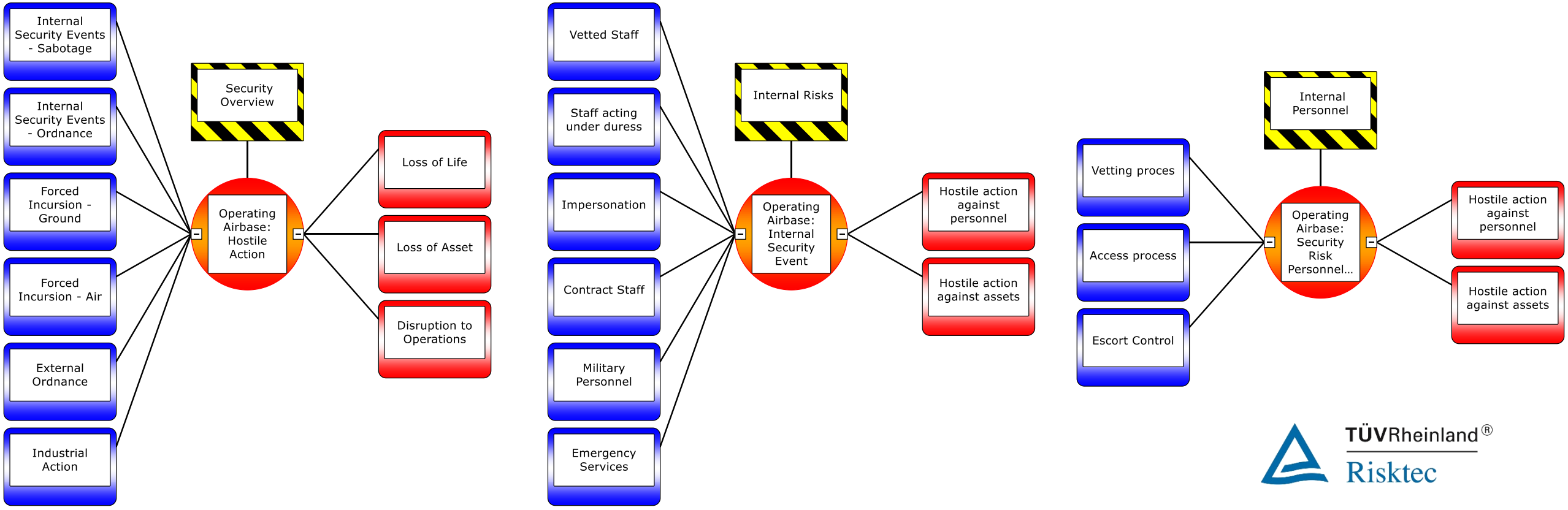
Issues for Consideration

- Level of detail
  - What do you want to find out?
- Barrier independence
  - What have we got?
- Use of Escalation Factors
  - How might it break?
- Effectiveness and acceptability
  - Is it good enough?
- Additional information
  - Data and more data
- Integration
  - Avoiding silos

TÜVRheinland®
Risktec

Level of Detail

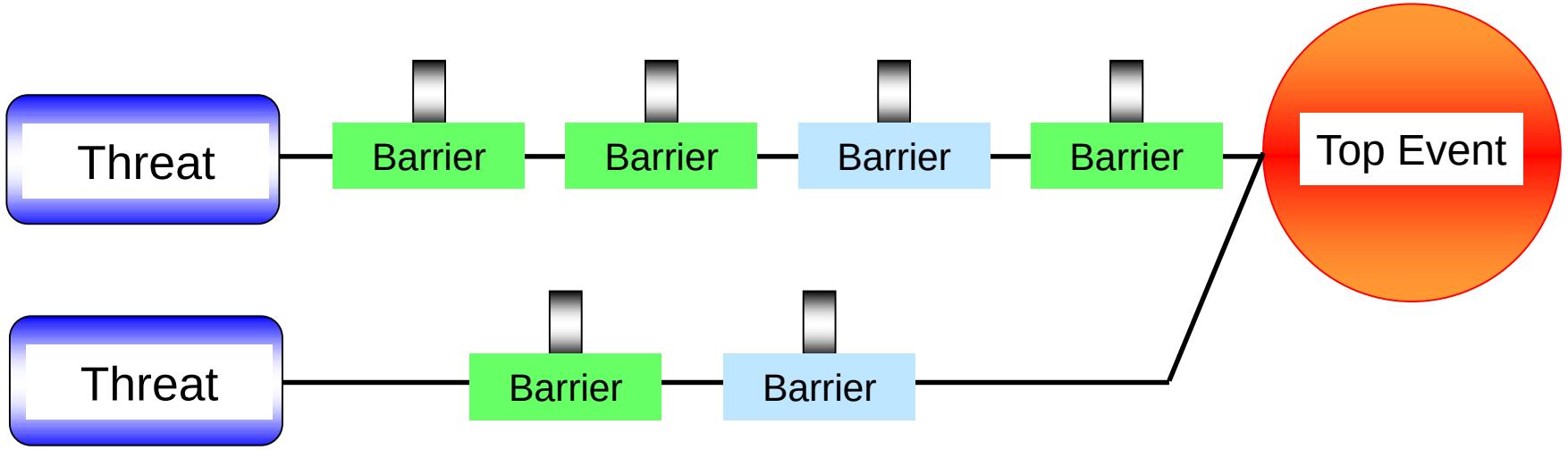
- Screening
  - What are the scenarios of concern?
- What is it that you want to understand better?
  - High level view e.g. corporate risk profile
  - Topic specific e.g. information security
  - Location/issue specific e.g. action against a site



TÜVRheinland®
Risktec

Dependency

If controls are dependent, there is less defence

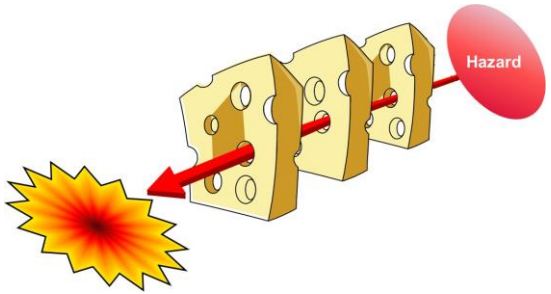


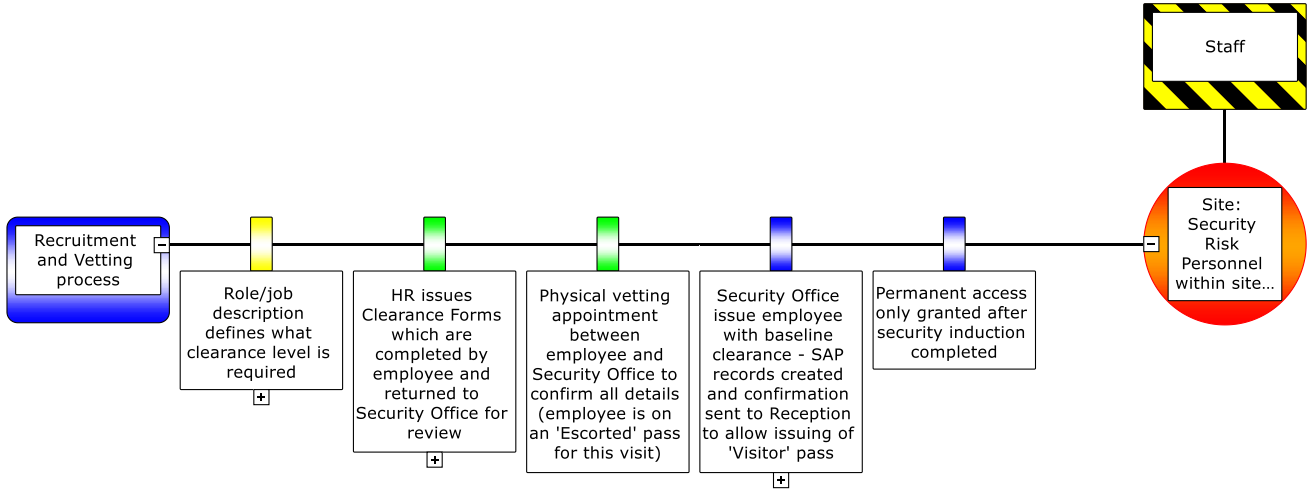
- What counts as dependency?
  - Same person?
  - Same systems?
  - Common services, contractors?
- Separate bowtie for common areas?

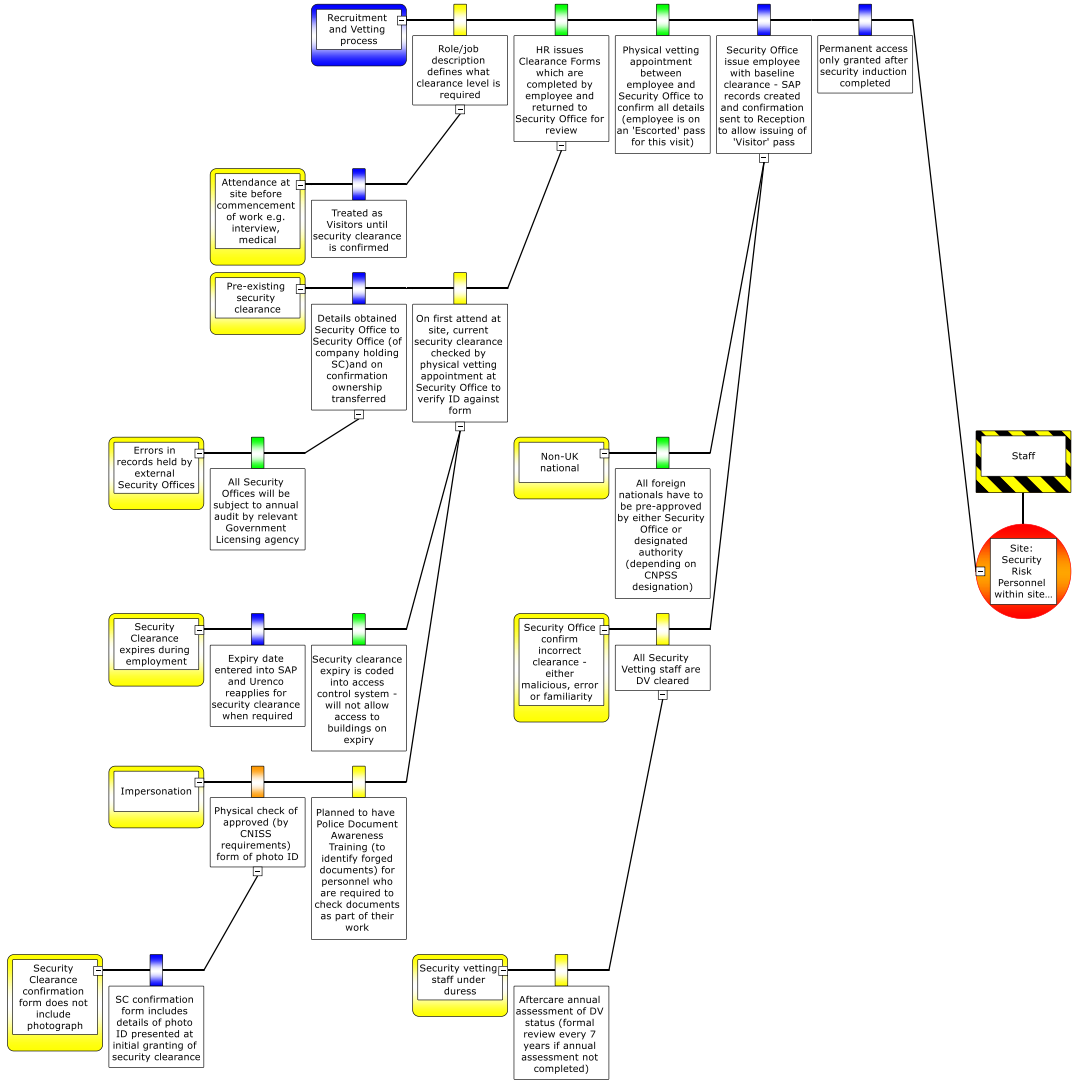
TÜVRheinland®
Risktec

Escalation Factors

- Allows for local failure cases
  - By time…
  - By location…..
  - By activity……
- Contain a lot of information
  - but can get very repetitive or obstructive







TÜVRheinland®
Risktec

Effectiveness and Acceptability

- Estimation of control effectiveness allows for assessment of acceptability
- Bowties allow decision making, not a decision maker
- Controls may be graded by
  - Gut feel
  - Scaling, 1-3, 1-5
  - Numerical
  - SIL/LOPA pfd
- Effectiveness influenced by e.g.
  - Robustness
  - Reliability
  - Human involvement
  - Ease of defeating etc.
- Not all threats are equal

Rating	Is it used? Is it in place?	Does it work/is it effective/human dependency?	Bowtie code
Very Reliable	Always	Control has more than a 99.5 % of working when required, no human involvement	
Reliable	Frequently	Control has a > 90 % chance of working when required, little human involvement	
Fairly Reliable	Mainly	Control has a < 90 % > 60 % chance of working when required, active human involvement	
Unreliable	Occasionally	Control has a < 60 % > 30 % chance of working when required, very active human involvement, complex and stressful to operate	
Very Unreliable	Rarely	Control has less than a 30 % chance of working when required, continuous human involvement, very complex	
-	-	Additional risk reduction measure (as part of ALARP demonstration)	

Effectiveness	Source	Criteria
Effective	Field Experience	Hardware: Inspections/tests conducted as per Performance Standard; Functions properly when tested Processes: Audits conducted, corrective actions resolved or planned Personnel: HSE training up-to-date, Personal Job Profile accurate; Competence assured; Contractor HSEMS meets standards
	Internal or Asset Integrity Audit	No or Low audit finding
	Incident Investigation	Control is in place
Partially Effective	Field Experience	Hardware: Inspections/tests conducted but hardware needs frequent adjustment to pass function test; some backlog of preventive maintenance activities that could impair performance Processes: Not applied consistently but still considered functional by each crew Personnel: HSE training only partially up-to-date, all Personal Job Profile not completed; Contractor HSEMS has some deficiencies
	Internal or Asset Integrity Audit	Medium audit finding
	Incident Investigation	Investigation determines Human Element is at fault
Ineffective	Field Experience	Control is Missing, Failed, or does not meet mandatory aspects of performance standard.
	Internal or Asset Integrity Audit	High or Serious audit finding
	Incident Investigation	Control found to be Missing or Failed

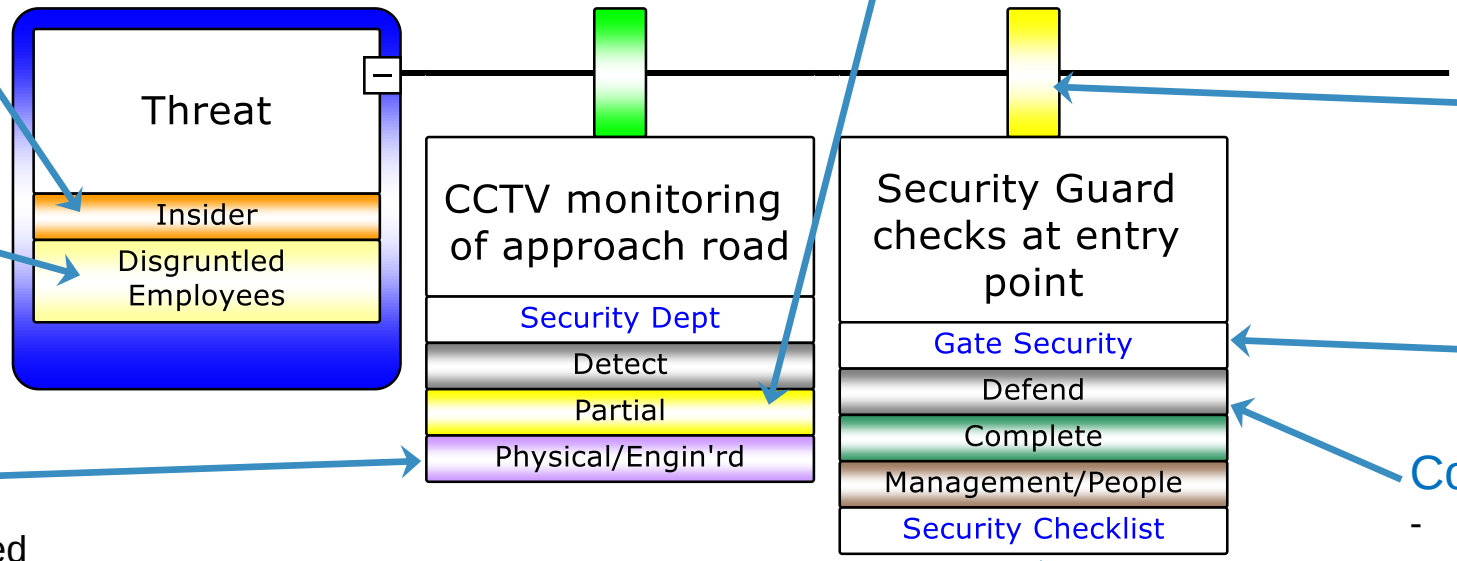
		Barrier Operating Effectiveness Level			
		Industry best practice / world class	Industry standard	Minor degradation	Major degradation
Barrier Design Effectiveness Level	Industry best practice / world class	6	5	4	3
	Industry standard	5	4	3	2
	Sub-standard	4	3	2	1
	Ineffective or unknown	3	2	1	0

Additional Information

- Once basic bowtie established, each barrier is an opportunity to ask questions
- Additional information can be displayed
- Easy to get carried away

Adversary Type
- Insider threats
- External threats
- Insiders/Colluders

Source
- Terrorists
- Activists
- Employees
- Criminals



Barrier Type
- Physical/Engineered
  - Fences, Plant Layout, Buildings
- Procedural
  - Access, Document Control, Maintenance, Emergency response
- Management/People
  - Vetting, Responsibilities, Competence Assurance
- IT/Computer
  - Software based

Quality
- Complete (not dependent on other countermeasures)
- Partial (is dependent on other countermeasures)

Effectiveness
- Very Poor
- Poor
- Good
- Very Good

Responsible/ Accountable

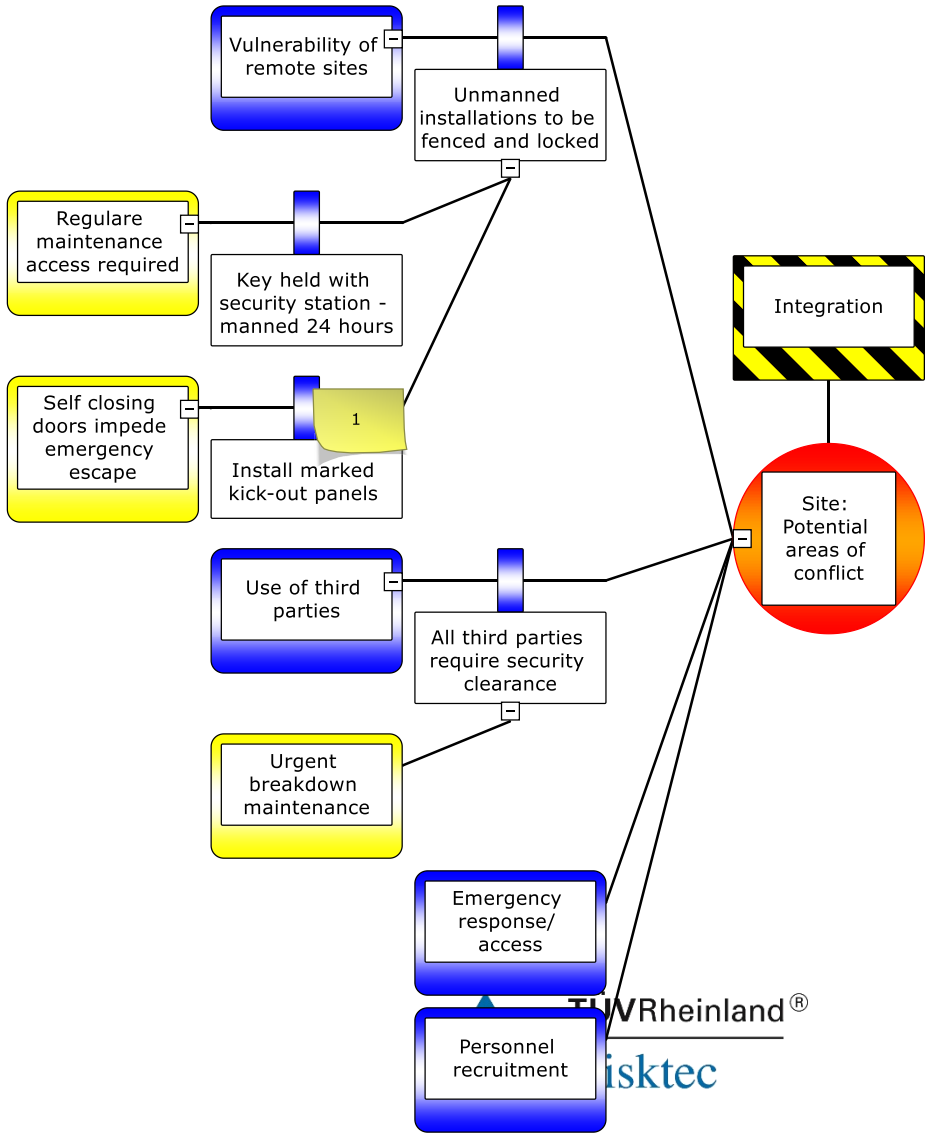
Countermeasure Type
- Detect
- Deter
- Defend
- Delay
- Deploy
- Detain

Documentation

TÜVRheinland®
Risktec

Integration

- Same basic objective of preventing harm to people and assets
- Conflicting approaches?
  - Prescriptive vs Risk Based
  - Need-to-Know vs Open Communication
- Differing needs? e.g.
  - Restricted access to remote facilities
  - Access for emergency services
  - Bottlenecking of escape routes
  - Dissemination of information
- Some involvement of security in safety analysis. Vice versa?
- Use of a targeted bowtie involving all parties



Lessons Learnt

- Screening
- Involve people with knowledge of the subject
  - What is actually present, rather than what we wish for
  - Create ownership
  - Obtain practical solutions
- Define the scope
- Check the logic
  - This causes this results in this
- Define controls explicitly
  - Check that they protect against a threat or minimise a consequence
  - Procedures are rarely barriers
- Remember Zymurgy's First Law

TÜVRheinland®
Risktec

Summary

- Widely accepted method within the HSE field
- Graphical format allows for
  - Clear communication and understanding
  - Encouraging use
- Can be used for assessing current controls, auditing and investigations
- Easily scalable
- Predominantly qualitative
- Can appear deceptively simple
- Needs rules – to guide rather than mandate

TÜVRheinland®
Risktec

Thank you for your attention

Any Questions?

Andy Lidstone – Principal Consultant
andy.lidstone@Risktec.tuv.com

TÜVRheinland®
Risktec