WEBINAR ASIA PACIFIC
OSH PRACTICE

Risk Management –
Back to the basic, why we do it?

15 Aug 2020

Vincent Ho

HKARMS 香港風險管理與安全協會
Hong Kong Association of
Risk Management and Safety

"…we don't need risk management, this kind of accident never occurs here before…"

"…we don't have the money, nor the time to apply risk management…"

Case Study 1

"This is how we do our business, there is no risk…"

- Projectiles were being thrown at train windows in last few 30 months including rocks, hammer, and bricks
- Regulator viewed this as an obvious and serious safety risk and asked the rail operator to erect a fence at an approximate cost of £100k
- The duty holder employed consultants to carry out a QRA with a cost benefit analysis (CBA) with an attempt to show that the cost involved was grossly disproportionate to the improvement in risk and to justify do nothing
- What do you think? POLL-1
  - That's what I would do too, cut cost, save money
  - That is not the correct way to do a risk assessment

- A risk assessment is used to inform and support the decision maker; it should not be used to justify a decision that has already been made
- As there is a clear risk of death or serious injury, QRA/CBA is not appropriate in this case to justify no action, but can be used to select the optimal action supplementing good industry practice

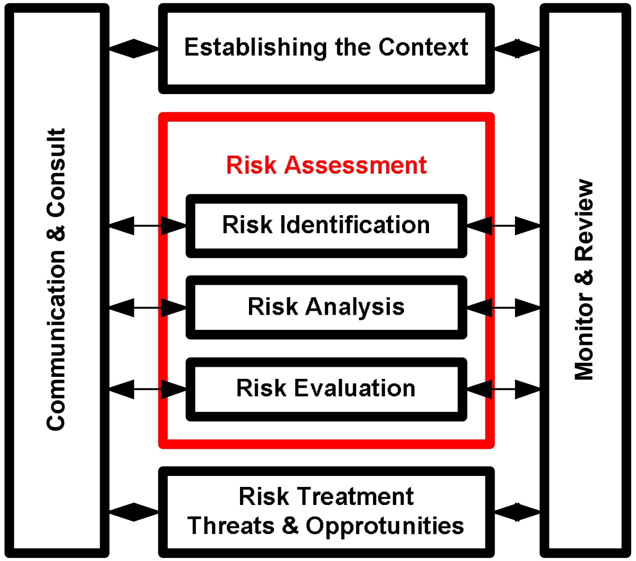
Case Study 2

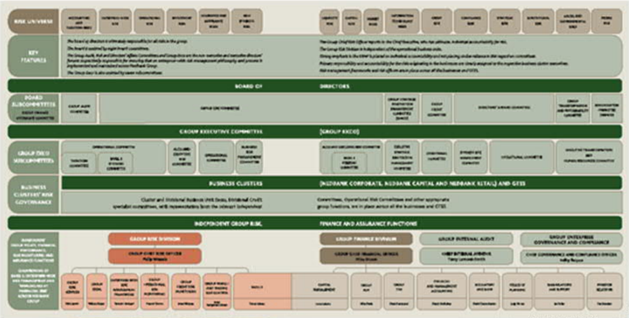
"Give me your risk report. If it works for you, it will work for us…"

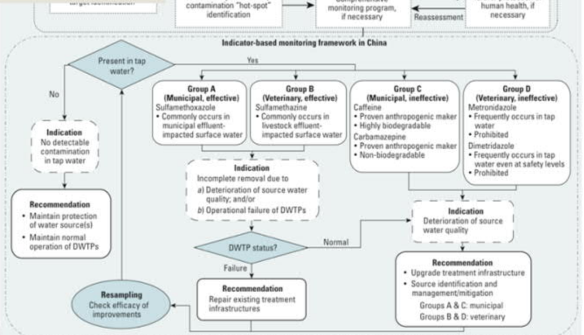
- To save efforts, a duty holder used a risk assessment prepared for work site Y, a simple work site, for its new work site X
- The duty holder wanted to show that the risks at site X were same as site Y, low
- However, there were significant differences between the two sites. For example, site X has site-specific "fall from height" risks that site Y does not have
- What do you think? POLL-2
  - o That's what I would do too, cut cost, save money, all work sites are the same
  - o That is not the correct way to do a risk assessment

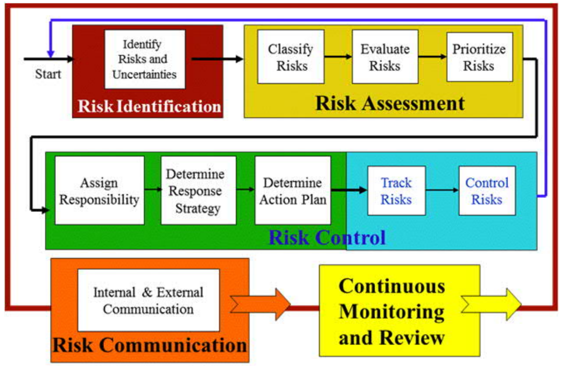
- A proper risk assessment should consider site-specific hazards, operations, locations, interfaces, maintenance regime, culture, past incidents, etc.
- Risk assessment should be specialised to a worksite or project. Generic assessment is only good for generic cases

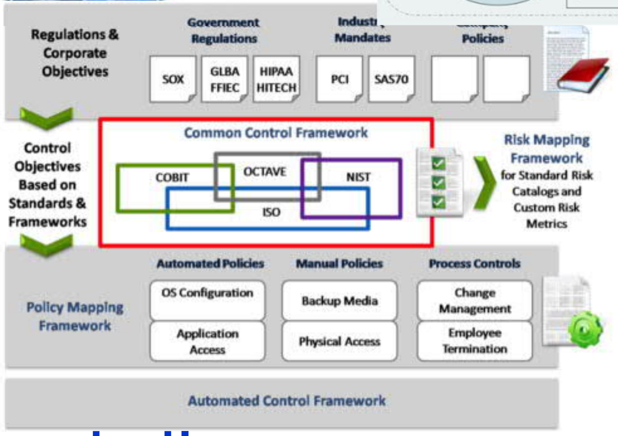
Risk management frameworks





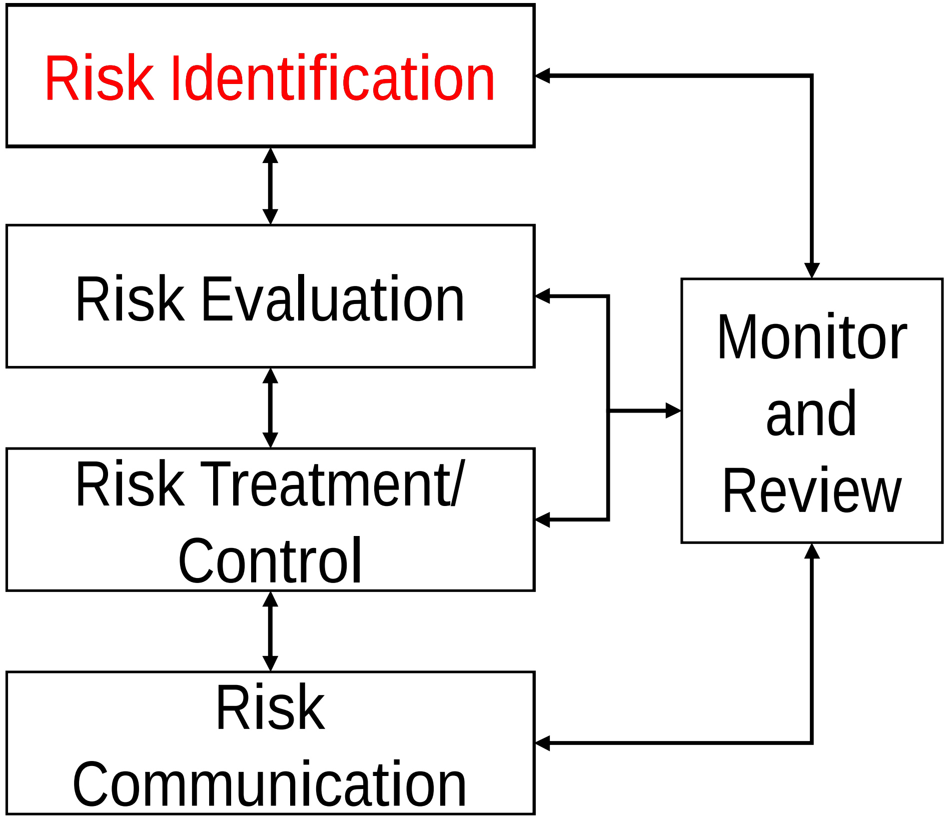

Risk management backbone of pharmaceuticals in tap water
Stage 2
Preliminary screening; risk-based prioritization; contamination "hot-spot" identification
Monitoring is unnecessary
Stage 3
Comprehensive monitoring program, if necessary
Reassessment
Stage 4
Policy/regulation for further protection of human health, if necessary
Indicator-based monitoring framework in China
Present in tap water?
Yes
No
Group A (Municipal, effective)
Sulfamethoxazole
• Commonly occurs in municipal effluent-impacted surface water
Group B (Veterinary, effective)
Sulfamethazine
• Commonly occurs in livestock effluent-impacted surface water
Group C (Municipal, ineffective)
Caffeine
• Proven anthropogenic maker
• Highly biodegradable
Carbamazepine
• Proven anthropogenic maker
• Non-biodegradable
Group D (Veterinary, ineffective)
Metronidazole
• Frequently occurs in tap water
• Prohibited
Dimetridazole
• Frequently occurs in tap water even at safety levels
• Prohibited
Indication
No detectable contamination in tap water
Recommendation
• Maintain protection of water source(s)
• Maintain normal operation of DWTPs
Indication
Incomplete removal due to
a) Deterioration of source water quality; and/or
b) Operational failure of DWTPs
DWTP status?
Normal
Failure
Indication
Deterioration of source water quality
Recommendation
Repair existing treatment infrastructures
Recommendation
• Upgrade treatment infrastructure
• Source identification and management/mitigation
Groups A & C: municipal
Groups B & D: veterinary
Resampling
Check efficacy of improvements





They all have similar steps

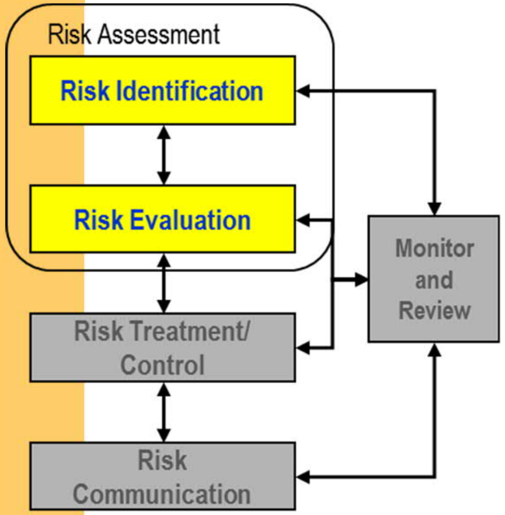
Steps in a risk management programme- simplified version



- Risk management programme is not a one-off activity
- These steps are often iteratively applied in phases, and are applicable to ALL businesses/ disciplines/ industries continually

Which one is the most important step?

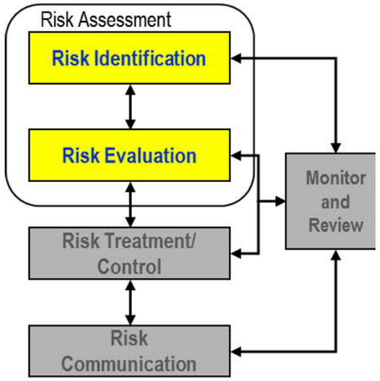
What can go wrong in these steps?



- Almost everyone under the sun is conducting a risk assessment, from spilling water to Mars landing mission
- Check the box "Hazard X present or not" → is it a risk assessment? Check-box safety
- Risk assessment methods vary widely among industries; the most popular methods are usually the least effective
- Strong "placebo effect" in analysis - a completely ineffective method would feel like it worked, particular when it is easy to master
- "Don't make this a Level-A risk, need to tell the boss" Technical risk is difficult to understand, what if you find something we cannot manage

Are we at risk? What happens if we do nothing?

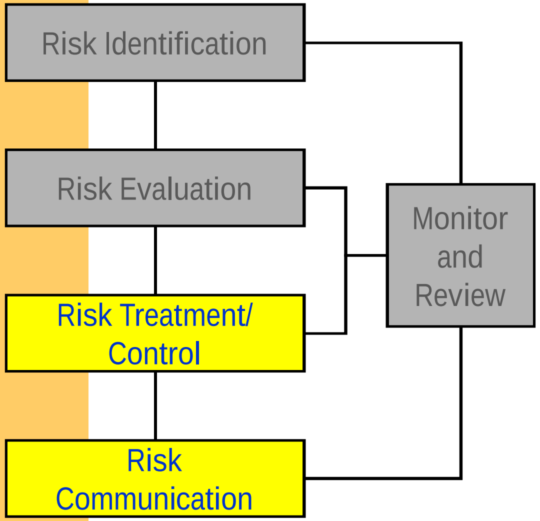
Why risk identification/ evaluation?



- Are risk control actions needed? How safe is safe?
- Risks need to be comprehensively identified and understood so that they can be managed holistically
- Risk identification should be embedded in work process, not in isolation but an integral part of the business
- Risks related to changes should be carefully identified and assessed for an effective change management
- Risk should be systematically assessed so that they can be prioritised and their proportionate response can be measured
- A proper risk identification and assessment form the rational basis for subsequent risk control actions

Pay attention to the elephant in the room
…and the rhino in the room
…and the black swan

What to do after you have assessed the risk?

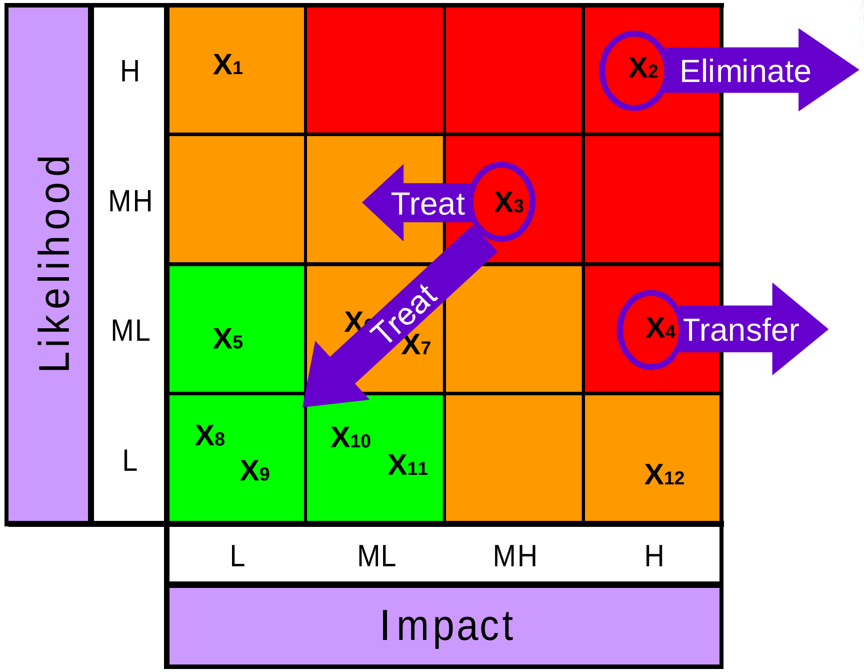


- We have the lowest accident rate, why do we do more?
- The residual risk is in the same risk class as the original risk, what is the need to do more?
- The cheapest way to reduce the risk is usually useless, but the expensive way does not mean it is useful
- So many risk control measures, which one should I use?
- Not common to see a cost/risk-benefit analysis being done
- If I have done all these steps, why do I need to tell people?

Need a robust risk control strategy and proper risk communication framework

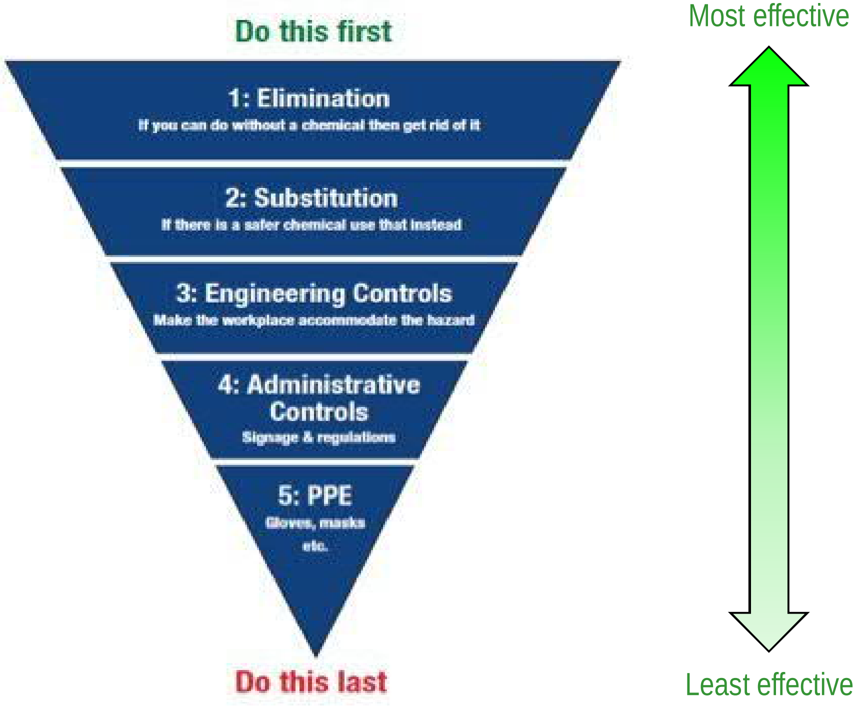
Principles of risk control

- Risk Elimination
- Risk Avoidance
- Risk Transfer
- Risk Reduction
- Risk Absorption



Likelihood	L	ML	MH	H
H	X_1			X_2
MH			X_3	
ML	X_5	X_6 X_7		X_4
L	X_8 X_9	X_{10} X_{11}		X_{12}

Hierarchy of risk control



Do this first

1: Elimination
If you can do without a chemical then get rid of it

2: Substitution
If there is a safer chemical use that instead

3: Engineering Controls
Make the workplace accommodate the hazard

4: Administrative Controls
Signage & regulations

5: PPE
Gloves, masks etc.

Do this last

Why risk communication?

- “An interactive process among scientists and non-scientists about risk assessment., risk characterization, risk management and risk policy.” (McComas, 2005)
- Use the right language to address the stakeholders and audience – Bring audience to the same page to understand the risk envelop they are exposing to
- Gain buy-in to your recommendations
- To document your findings and address your accountability/ liability
- Pay attention to risk perception, risk projection, risk extrapolation, statement taken out of context,

Be professional, responsible, truthful, sensitive, understanding

Ethics, ethics, ethics

Barriers to effective risk communication

- ➢ Lack of ownership
- ➢ "Bring me the solution, never the problem"
- ➢ Every business unit (silo) wants to do it their own way
- ➢ Lack of a common, agreed language or terminology
- ➢ Lack of a clear and consistent Risk Management champion
- ➢ Unclear or non-existent decision authority structure
- ➢ Silos of analyses and reporting of different risk types
- ➢ Maturity, governance, technology, process and people
- ➢ Inadequate resource allocation, ambiguous inputs and outputs
- ➢ Perception of a risk manager and roles/responsibilities
- ➢ Immature safety culture (How does the organisation operate?)
- ➢ Lack of effective internal and external communication to stakeholders

"…our business partner does not believe in risk management..." ☹

What works for risk communication?

- Have a clear and consistent organisation-wide approach supported by leadership and stakeholders in managing and communicating risks across business units
- Tackle the most important risks first, and that the safety budgets will be spent in the most effective way
- Give risk management appropriate visibility in organisations with open communication engaging users and stakeholders
- Communicate lessons learnt between business units
- Document risk management process with maturity tracking
- Involve the front line staff in the risk control process
- Provide training to all involved in the risk management process
- Report incidents and near-misses timely and accurately

Risk Management –
Back to the basic, why we do it?

- Identify risk exposure/ levels/ profile
  - to see how deep the hole you are in
- Rank hazards and risk control measures
  - to optimise resources by balancing costs, risks and benefits
- Provide information to decision-maker
  - to decide what to do
- Document decisions and actions
  - to address liability, document what you have done to prevent the accident, have you done enough to avoid the accident?
- And do the above systematically, iteratively, continually
  - to minimise uncertainty and surprises

Making the right decision can reduce harm to individuals,
risk management helps you to choose the optimal decision

What do you want to know from a risk assessment?

	Knowns	Unknowns
Known	Things we are aware of and understand	Things we are aware of but don't understand
Unknown	Things we understand but are not aware of	Things we are neither aware of nor understand

Source: US Secretary of Defense Donald Rumsfeld during a Pentagon news briefing in February 2002

Which one worries you the most?

Last Words

- The biggest single risk for any organization may be the risk that their approach in applying risk management doesn't really work for them - it is the ultimate "common mode failure"
- Risk management methods vary widely among industries and the most popular are usually the least effective
- There is a strong "placebo effect" in analysis - even a completely ineffective method would feel like it worked
- Your perception of risks and your risk aversion changes daily due to irrelevant, random external influences
- Risks ultimately should be filtered to the lowest level possible in a business for ownership and mitigation

Risk is the effect of uncertainty on objectives, whether positive or negative

Thank You

End

Safety Corner: What are the Criteria for an "Acceptable" Risk Assessment?

(as appeared in Hong Kong Engineers, July 2010)

The objective of a risk assessment for a system is to find out what can go wrong (the scenarios) so that their impact can be prioritized (typically, by their likelihood and consequence). Effective measures can then be implemented to control the risks; thus, rendering the system safer to operate. Because the "true" total risk of a system will never be known without accepting a certain level of uncertainties, philosophically, there is no such thing as a "perfect" risk assessment. To make a risk assessment acceptable or being a "good" risk assessment, care must be taken in every step to ensure the process is done according to criteria. The following list of criteria or factors that lead to a "good" risk assessment is by no mean exhaustive but forms the general characteristics that you would expect to find in a "good" risk assessment:

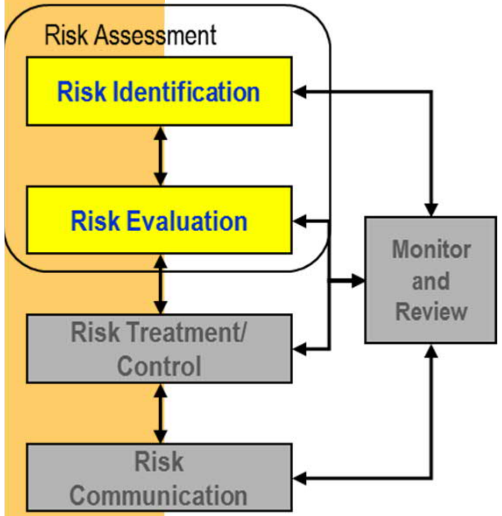
1. Comprehensive to include all reasonably foreseeable scenarios
2. Adherent to evidence
3. Logical and technically sound
4. Practical and reasonable
5. Open to evaluation through peer professional review
6. Based on explicit assumptions and premises
7. Compatible and specialised to the system being analysed
8. Conducive to learning as a living document
9. Attuned to risk communication to stakeholders
10. Innovative but does not reinvent the wheel

So, what are the characteristics of a "bad" risk assessment? These are the common symptoms:

1. Narrowly focused with unclear scope
2. Unsystematic and unclear scenario generation
3. Underestimate of the complexity of the system and data available
4. Overly subjective with no supporting evidence
5. Only generic data used without system-specific input
6. Difficult to understand with no open review
7. Incorrect application of tools and techniques
8. Inconclusive outcome
9. Too deterministic with no account for uncertainties
10. Overconfidence in applying expert judgment without any calibration

==

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho@UCLA.edu



Risk Assessment

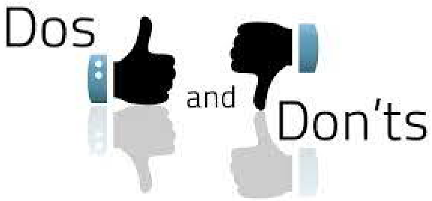
Risk Identification

Risk Evaluation

Risk Treatment/ Control

Risk Communication

Monitor and Review



Do's

☺ Comprehensively include all reasonably foreseeable scenarios
☺ Adhere to evidence
☺ Apply logical and technically sound methods
☺ Be practical and reasonable
☺ Open to evaluation through peer professional review
☺ Base on explicit assumptions and premises
☺ Specialise to the system being analysed
☺ Conducive to learning as a living document
☺ Attune to risk communication to stakeholders

Don'ts

☹ Focus narrowly with unclear scope
☹ Conduct unsystematic and unclear scenario generation
☹ Underestimate the complexity of the system and data available
☹ Be overly subjective with no supporting evidence
☹ Apply only generic data without system-specific input
☹ Apply process that is difficult to understand with no open review
☹ Apply incorrect tools and techniques
☹ Present inconclusive outcome
☹ Be too deterministic with no account for uncertainties
☹ Be overconfident in applying expert judgment without any calibration