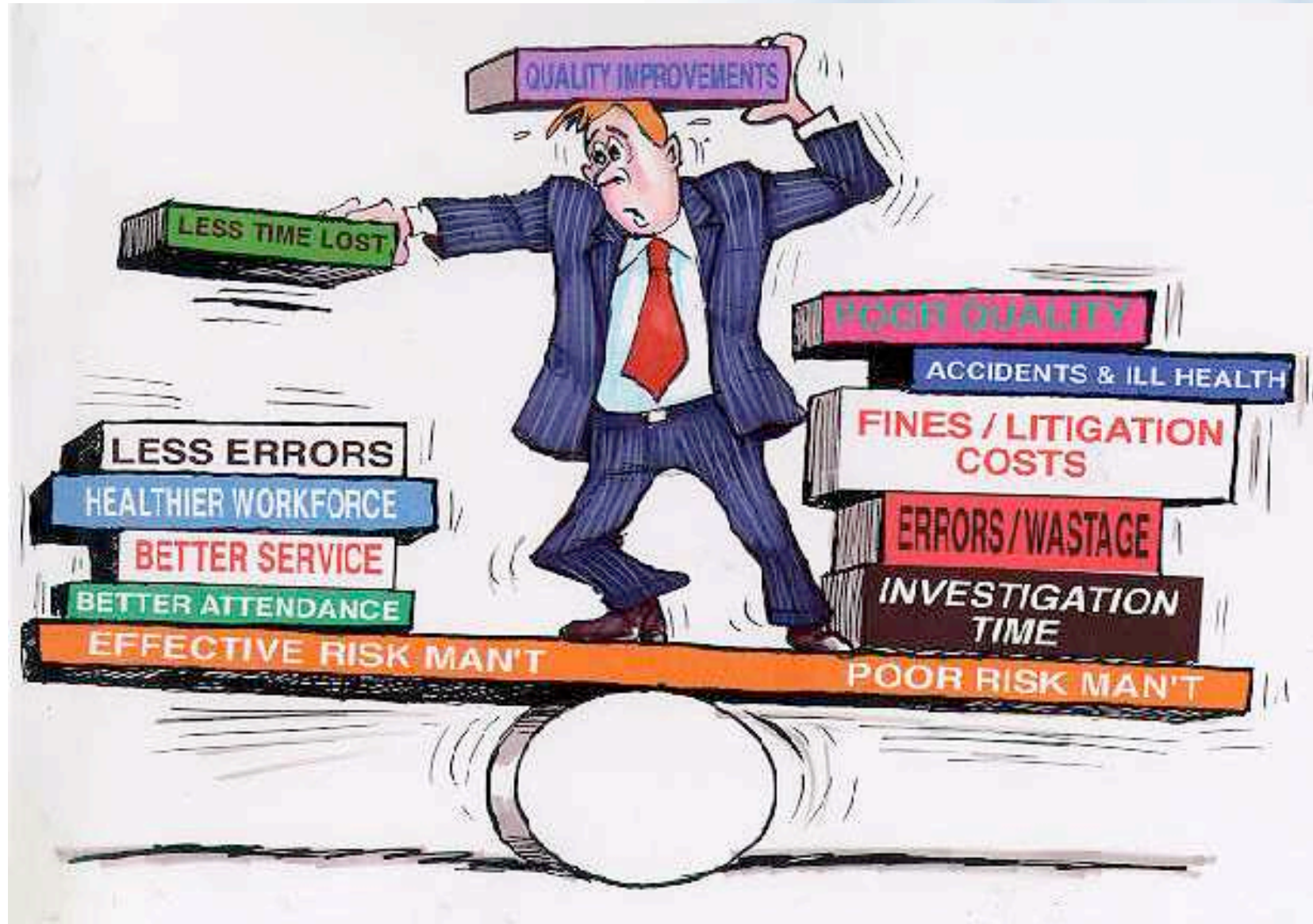# Introduction

- Occupational Safety and Health (OSH)
    - Why bother?
    - What does Cap 509 imply?
    - What about civil liability?
- Some practical guidance
    - Why not **just** behavioural safety
- Where do we go from here?

The balancing act

Signals

- How do you know that you have a good OSH risk management system?
- You know:
  - The key OSH risk issues should you be concentrating on in the coming year
  - Which risk assessments you have not yet done
  - Your top 3 OSH risk
  - You can demonstrate and justify the priority order for these OSH risks
  - You can describe control strategy for each of these risks
  - What should be done next

OSH management

- ## OSH management

  "The **process** which achieves the most efficient **combination of controls** necessary to provide **reasonable assurance** that **OSH objectives** can be achieved reliably"

Overcoming 'silo' thinking

Risk management

- Corporate Governance
- Corporate Finance
- Emergency /Contingency Planning
- Fire
- Health & Safety
- Environment

The business case

- Poor OSH risk management costs money
- Poor OSH management interferes with business effectiveness and efficiency - the hidden costs
- OSH risk can be managed
- Effective targeting of resources on *key* OSH risks
- Good OSH is *better than* 'loss control'
- Good OSH arises from good management!
- 'OSH performance' is a business advantage

Relevant OSH Law - Quick Review

The drivers for OSH risk management

- Moral

- Legal

- Business

Hong Kong Law

- Factories and Industrial Undertaking (Cap 59)
- OSHO Cap 509 (509A & 509B)
  - Immunity from prosecution for Government Bodies
  - 'Strict Liability'
- Civil law
  - Vicarious liability
  - Duty of care
  - Negligence

Civil Service Bureau
OSH management systems guidance

"In Hong Kong, the government's view on occupational health is that primary responsibility for safety & health at work rests with those who create the risks and those who work with such risks.....

...ultimate goal is self-regulation....

...purposeful creation and maintenance of specific tailor-made standards and controls commensurate with the inherent risk ...."

Interpreting Cap 509

- **Risk assessment**
  - Common sense - reasonableness
- **Employee consultation**
- **Risk reduction**
  - Proportionate response - reasonable practicability
- **Risk monitoring**
- **Information, training, instruction & supervision**
  - Competency
- **Health surveillance**

What is risk?

- Risk is:
  - An estimation of a loss event,
  - The chance of that event occurring (likelihood), and
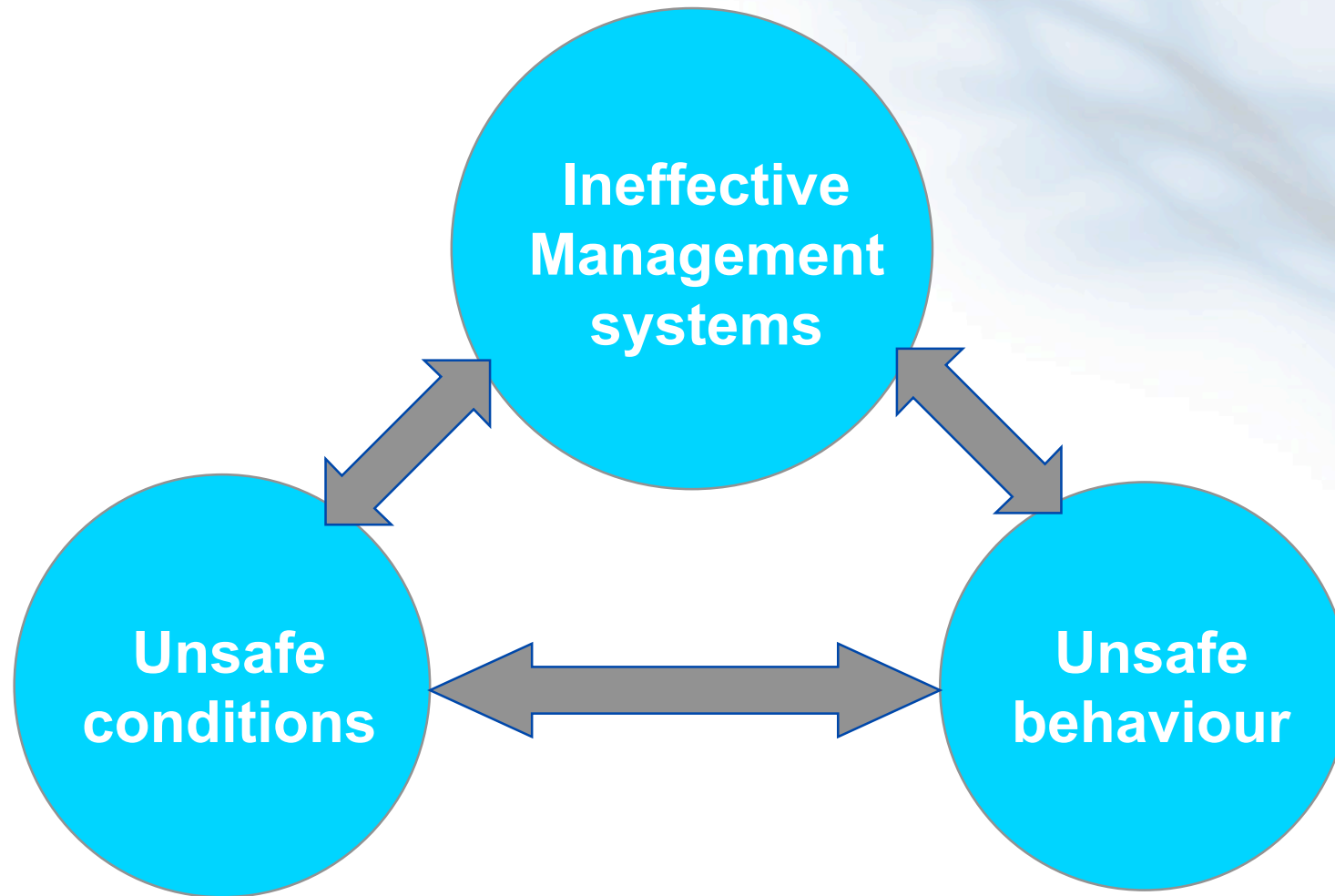 - The consequence were that event to happen (impact)

Risk management process

Challenges

- Need data
- Need context
- Need a common set of definitions

Sources of risk

What do you need?

- Not just behaviour

- Must have an effective management system

- Must design out problems

Behaviour-based or risk-based?

- Concentrating only on behaviours does not work
- "just systems" will deliver benefit only for clear accountabilities
- The OSH system must support risk management including consistent methods for:
  - Assessing,
  - Reducing, and
  - Monitoring risk

Determining core values

- Risk management won't work if the people hold the wrong values

- These values determine peoples' behaviours

- The values determine the outcome of conflict between safety and other drivers (e.g. money, business pressure, deadlines, peer pressure, etc.)

Vital role of core values

- Keep them simple
- Keep them focussed
- Make them explicit

UK Fire Service

'Aestimemur Agendo'
Let us be judged by our action

- We may risk our lives a lot, in a highly calculated manner, to protect saveable lives

- We may risk our lives a little, in a highly controlled manner, to protect saveable property

- We will not risk our lives at all for lives or property that are already lost
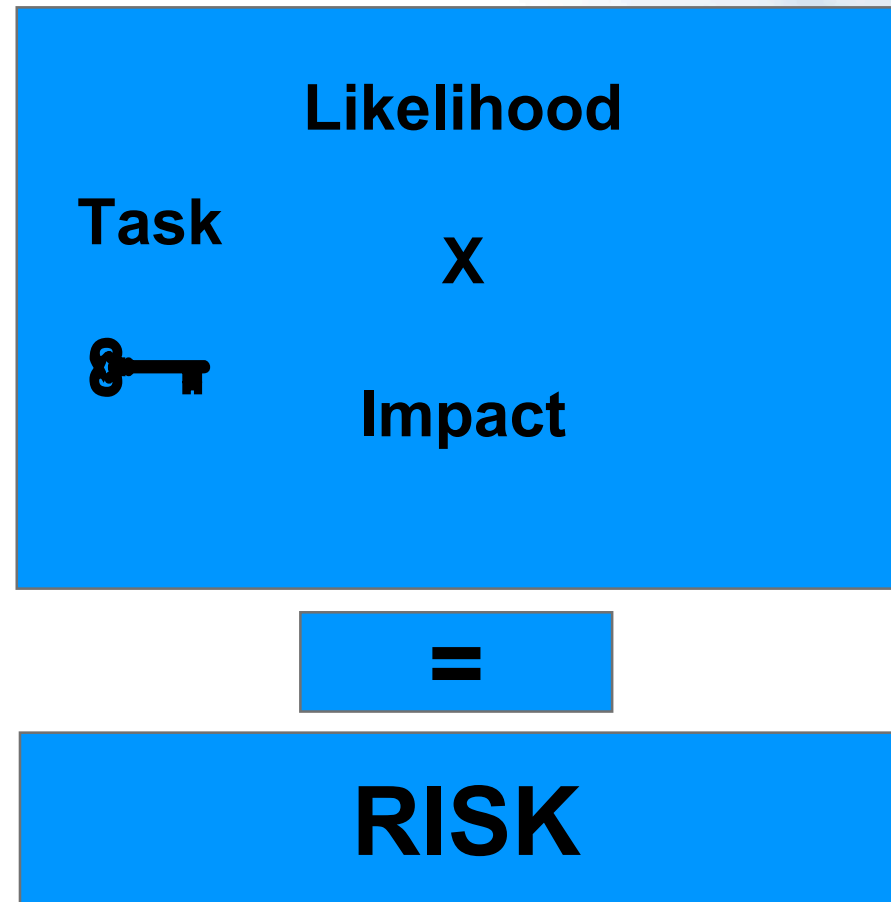
Source: Home Office Guidance

Consider

- Nothing we do is worth dying for
- We all have the right to go home at the end of work in the same condition (physical, psychological, emotional) as we started (just a bit more tired)
- We all have the right (and are expected) to challenge any unsafe acts
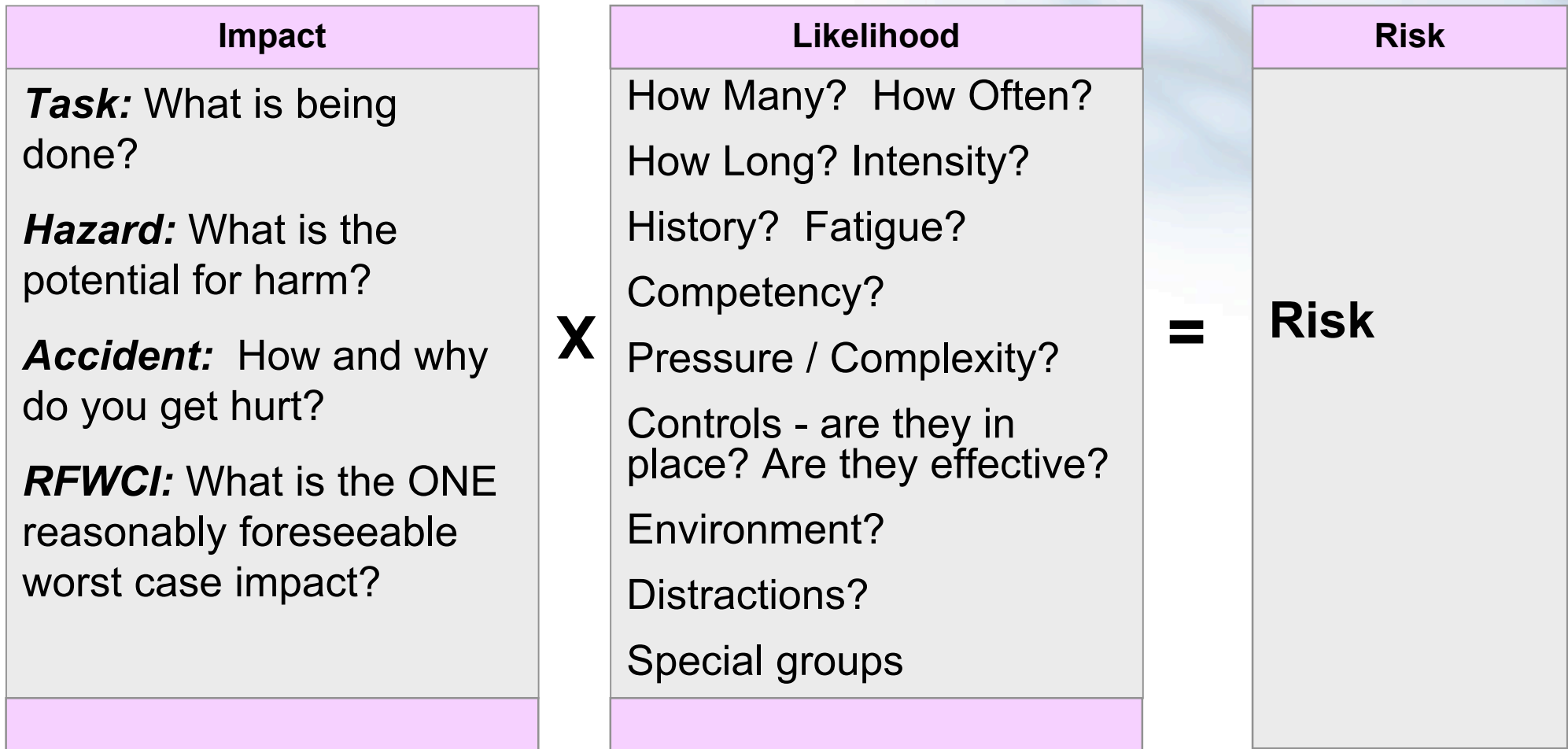- We must respond positively if we are challenged

Assessing risk

APPLICATIONS

Defining risk

Risk assessment template

RFWCI = Reasonably Foreseeable Worst Case Impact

Impact		Likelihood		Risk
Task: What is being done? **Hazard:** What is the potential for harm? **Accident:** How and why do you get hurt? **RFWCI:** What is the ONE reasonably foreseeable worst case impact?	**X**	How Many? How Often? How Long? Intensity? History? Fatigue? Competency? Pressure / Complexity? Controls - are they in place? Are they effective? Environment? Distractions? Special groups	**=**	**Risk**

Controlling risk

Risk control

- Risk management strategies
  - Terminate
  - Reduce
  - Accept
  - Pass-on
- TRAP

ALARP

As low as is reasonably practicable

Reasonable practicability

- Risk v Cost judgements supported through evidence.

- 'Cost' implies more than just money (e.g. time, effort, resources, business interruption, technology).

  - Where the benefit is *grossly disproportionate* to the cost then we might be entitled to believe that it's not reasonably practicable.

- Act in a manner appropriate to the level *and spread* of risk faced with the resources available.

Terminate

- Why are we doing it?
- Can we do it differently?
- Is the organisation satisfied that the risk is worth taking?

Reduce

- Can we:
  - Reduce the hazard - remove it, substitute it, guard it, etc.?
  - Reduce the likelihood - reduce how often we do it, construct a safe system of work, improve the competency of our people, etc.?
  - Provide appropriate training, supervision, etc.
 - Introduce Personal Protective Equipment as a last resort (consider effect on hazard and likelihood)

Accept

- We **must** accept some risk
- The only risk free organisation is one that does nothing
- Sometimes we have to accept high risks
  - So manage them!

Pass on

- Insure high impact unlikely events
- Contract out risks that other people will manage better than us
- Remember, we might still retain some accountability

Managing risk in practice

33
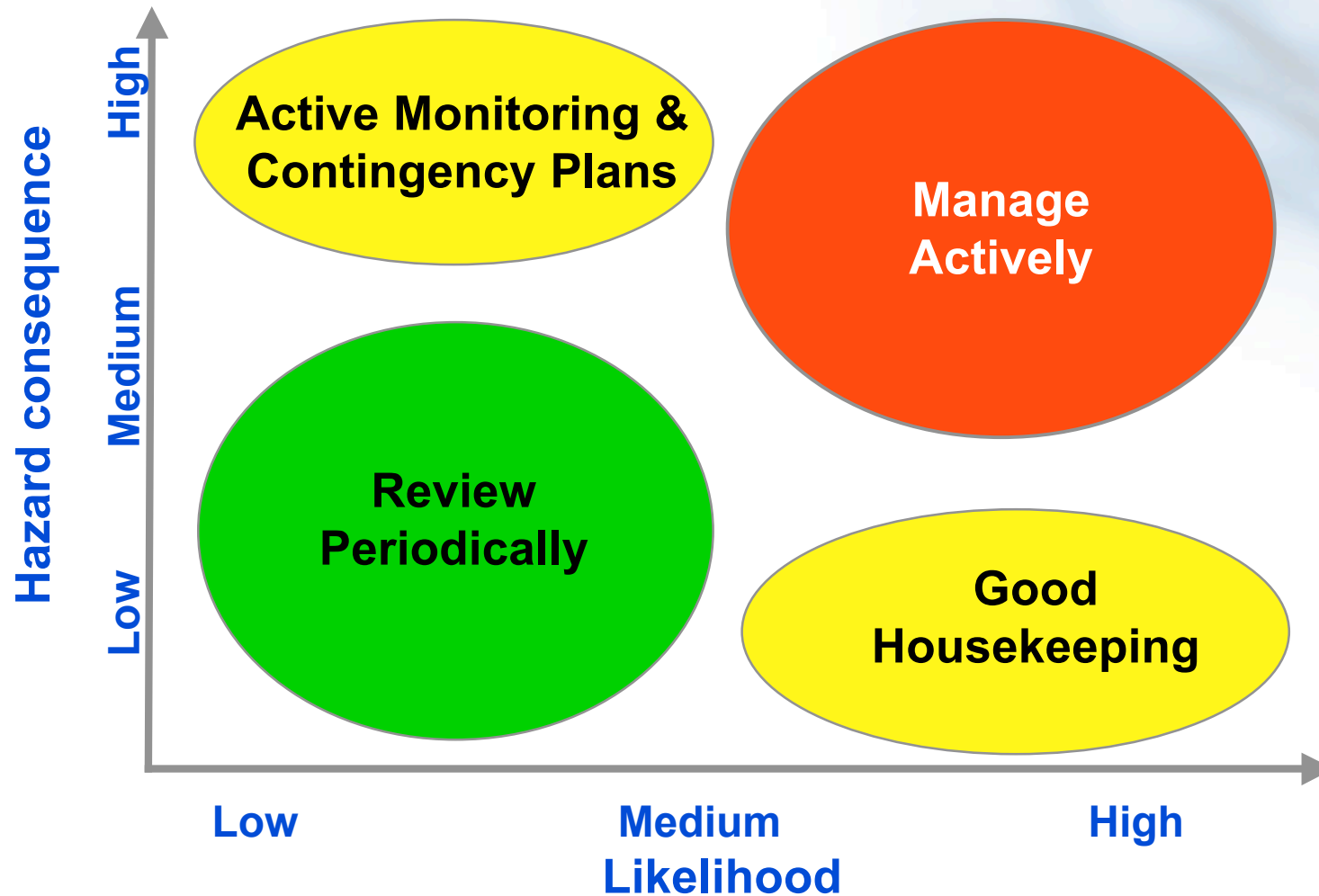
Risk review and monitoring

Risk review

- What's the difference between risk review and risk monitoring?

- What's the difference between risk monitoring and audit?

- When should an assessment be reviewed?

  - After a significant change

  - After an incident (accident or near miss)

  - Periodically and appropriately to the level of risk

Risk monitoring

- An on-going 'regular' activity
  - The nature and extent of risk can change
  - The effectiveness of controls can change over time

- Monitoring must
  - Be appropriate to the level of residual risk
  - Be tempered through arguments of reasonable practicability
  - Take into account the numbers of existing risks

- Reducing one risk might occasionally create new ones - monitoring must identify this

Discussion: risk records

- Defining, creating and maintaining audit trails of what we did (and didn't) do will be a vital part of effective risk management.
- Know which are live, completed or dead assessments.

- Which records must we have?
- Who should be/will be responsible for creating and updating them and who is accountable for them?

Organising for OSH Risk Management

Human

The 'Top X' principle

- An effective risk management system demonstrates:
  - You report, regularly, on your Top 'X' risks
    - In this operational period; you've looked wider than just these
  - There's quality to the list
    - It's the 'right' list; demonstrate competence and quality control
  - You have a management action plan for dealing with your Top X risks
  - The action plan has changed for the better over time
    - show that you continue to act
  - This process takes place throughout your part of the organization
  - You have both pro-active and re-active systems in place

Human Applications

The Elms

Elms Grove

Loughborough

Leicestershire

LE11 1RG

UK

+44 (0) 1509 211866

e-mail: enquiries@humanapps.co.uk
web: www.humanapps.co.uk

The Elms