

# Business Continuity Management

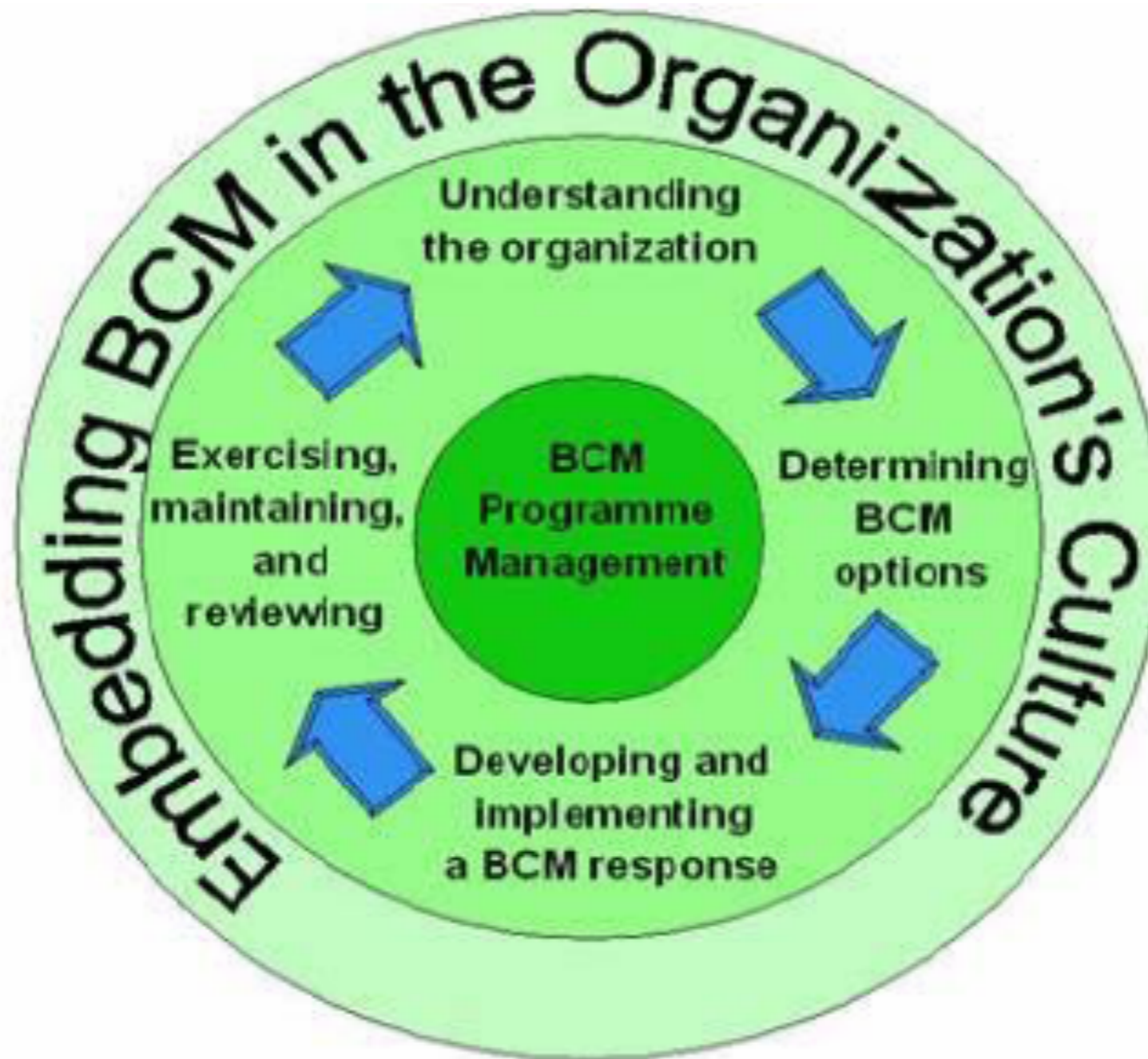
Presented by  
Clive Lunn (FBCI)  
to the  
Risk and Insurance  
Management Society,  
BC Chapter



# Agenda

- Business continuity management
  - Program not project
- Risk assessments & the business impact analysis
  - The BIA vs. the RA and risk evaluation across the enterprise
- The probability problem
  - Swans, Turkeys and Bow-Ties
- Getting executive attention
  - Getting help & burning platforms
- Planning vs. the plan
  - Keeping it simple and being proactive
- Some current threats
  - The pandemic games?
- Summary & Questions

# Business continuity management



Understanding the Organization – BIA and RA

BCM options – Strategy, select controls

BCM response – Proactive controls, alternate sites, plans, IT recovery

Exercise, Maintenance, Review – Update plans and analysis as needed

Embedding BCM – Education, training, defined roles and responsibilities



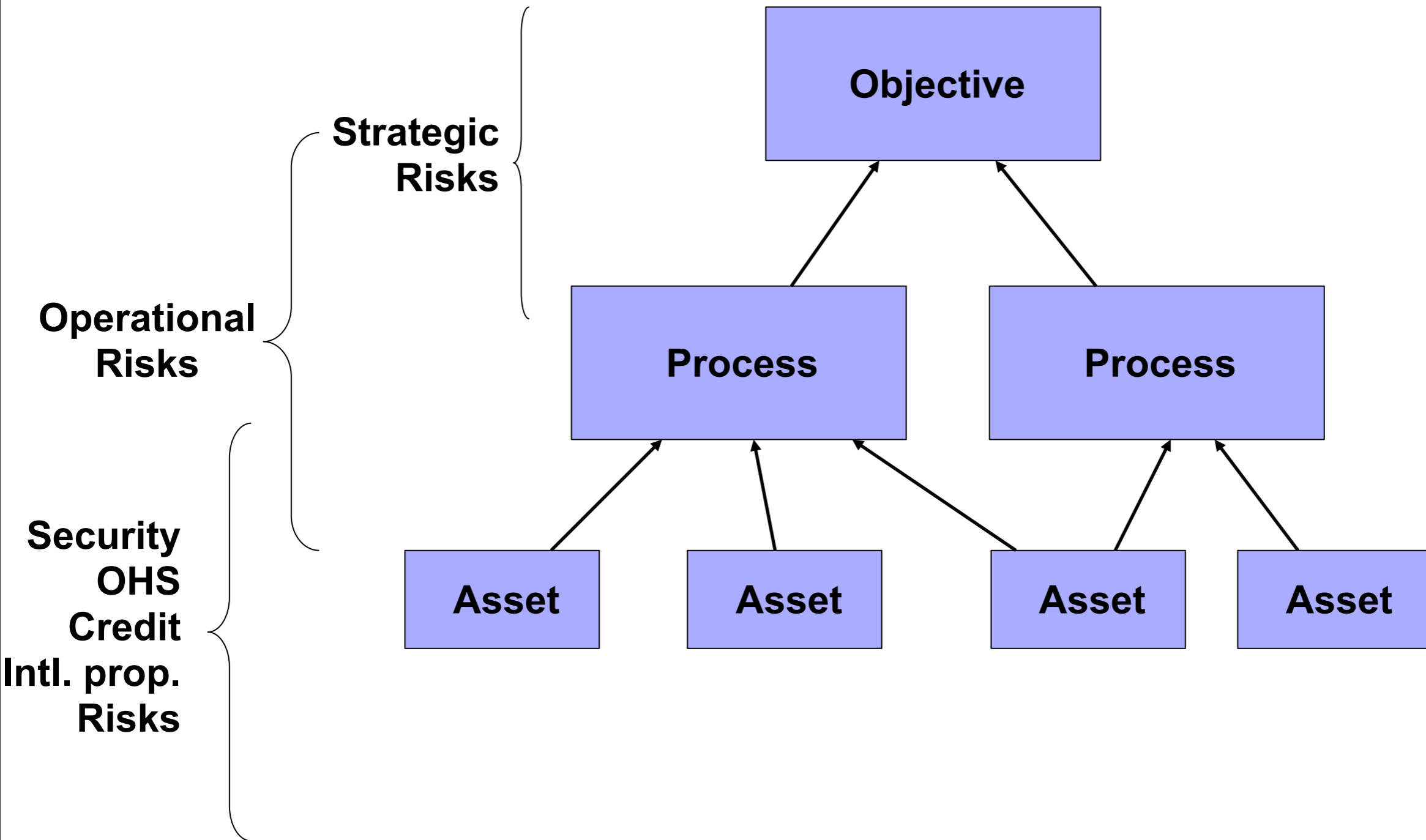
# Risk Assessments (a few common contexts)

Setting the context is required by standards such as AZ/NZS 4360 & ISO 31000

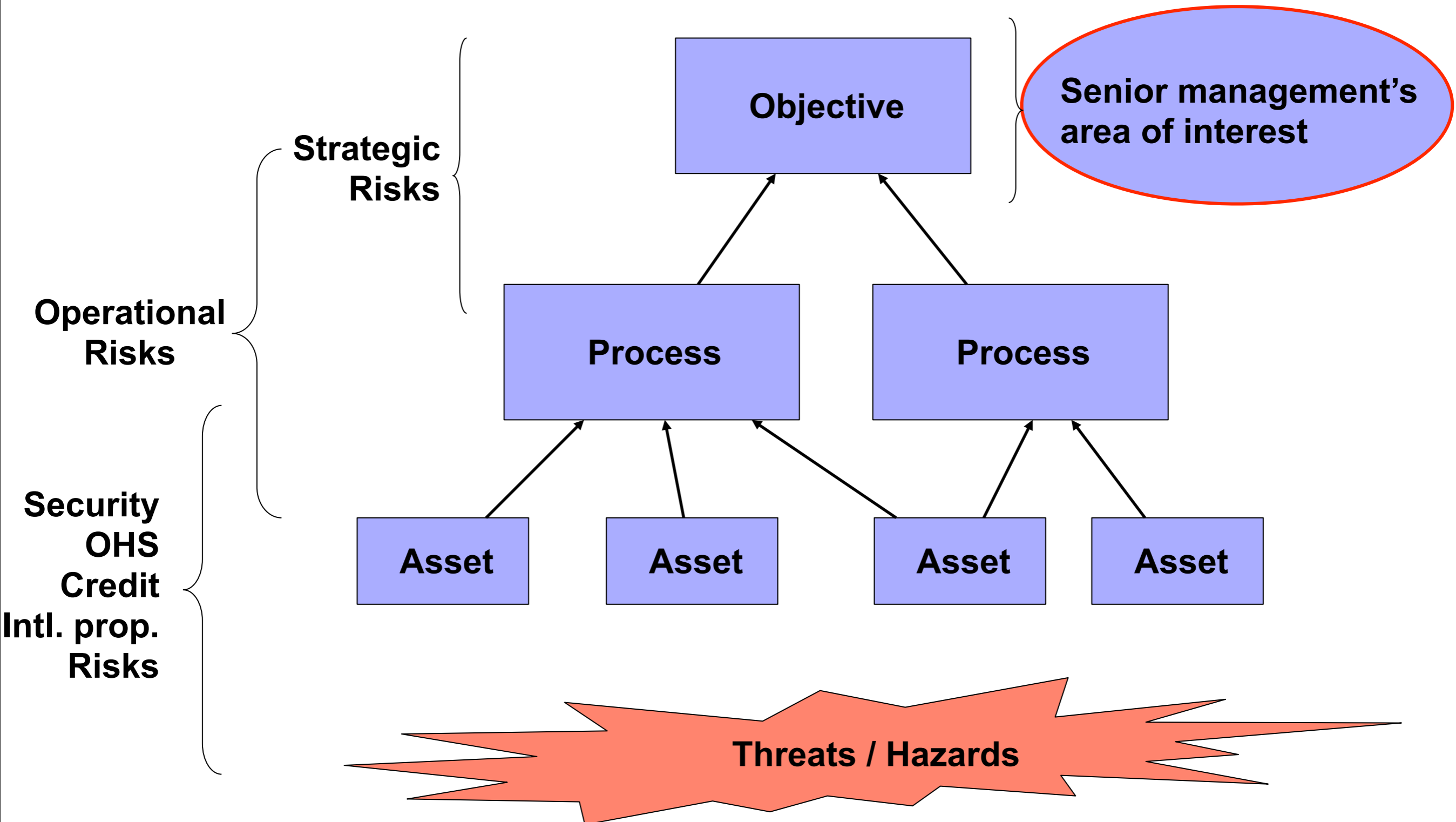
- Safety Risk Assessment
  - What can harm me (identified hazards)
- Security Threat & Risk Assessment
  - What do we have (identified assets)
- Business Impact Analysis (BIA)
  - What do we do (identified activities)
  - What do we need to do it
- Strategic Risk Assessment
  - What do we want to achieve



# BIA boundaries?



# BIA boundaries?



# Business Impact Analysis

**A BIA is just another risk assessment - with a specific context & a slightly different way to measure loss severity**

- Three fundamental questions
  - What do you DO – activities or outputs
  - What happens if you do not do these things – consequences
    - What happens if you do these things badly or incorrectly
  - What do you need to sustain these activities - resources
- Phase 1 - Loss severity
  - Consequences as a function of time (how bad, how quickly)
- Phase 2 - Loss frequency
  - Threat and vulnerability assessment for critical resources
  - Anticipated likelihood of occurrence – more on this later.....

# Risk Evaluation & Comparison

## Risk Matrix or "Heat Map"

LIKELIHOOD OF OCCURRENCE	Risk Rating					
6	3	5	7	8	9	10
5	2	4	5	7	8	9
4	2	3	5	6	7	9
3	1	3	4	5	6	8
2	1	1	3	4	5	7
1	1	1	2	3	4	6
CONSEQUENCE	A	B	C	D	E	F

- Severity of loss is measured using tailored criteria for multiple consequence categories
- Consequence types may include: Safety, Environment, Financial, Reputation and others as determined by the nature of the organization
- Likelihood of occurrence – more on this later.....
- A matrix enables easy comparison of disparate risk types (if using common evaluation criteria)

# The likelihood problem

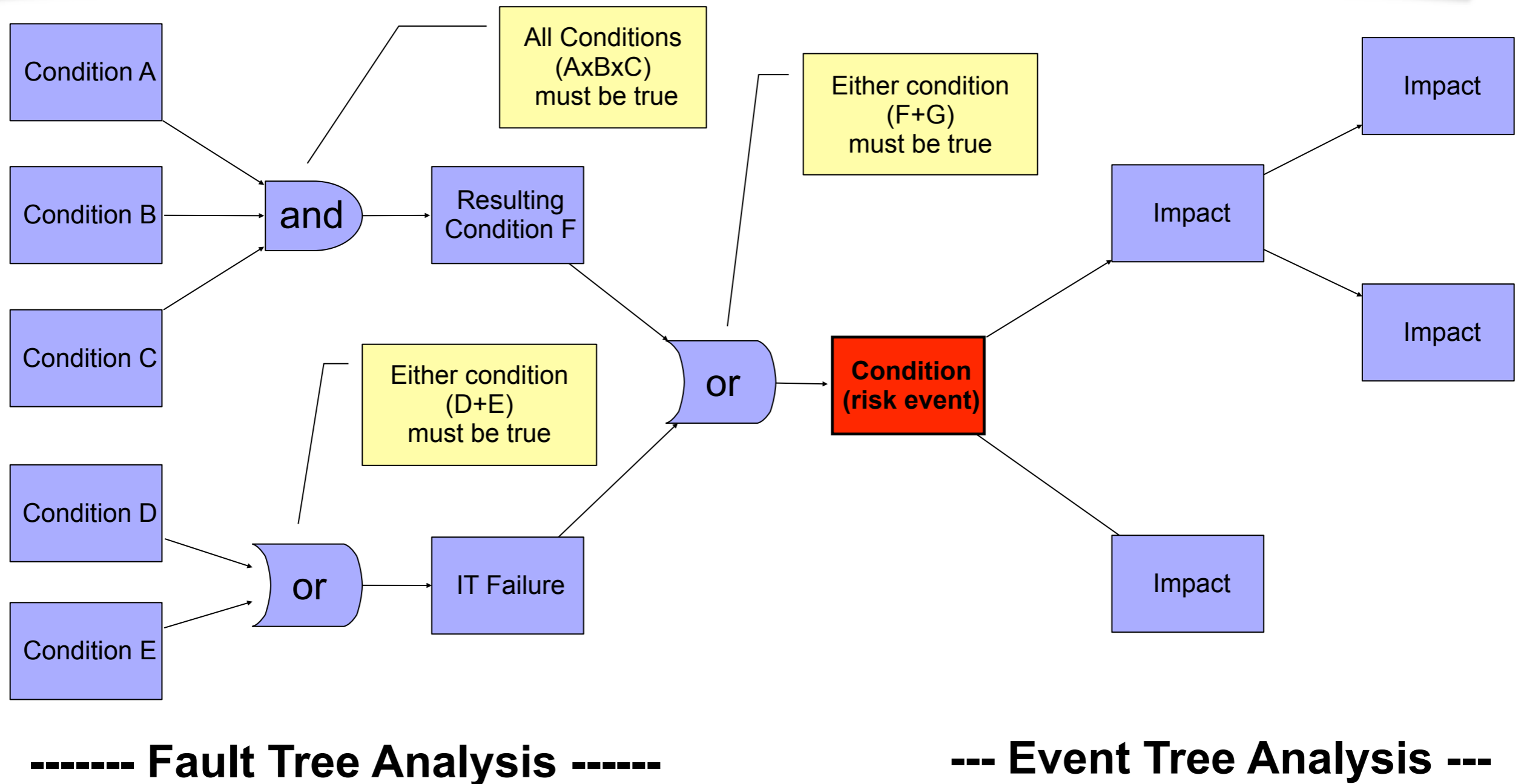
How accurately can you predict the future?

- Business Interruptions are typically low frequency high impact events
  - Often a lack of historical data
  - Multiple single points of failure – bow tie analysis?
  - The outliers will get you!
  
- Black Swans and Turkeys (with apologies to NN Taleb)\*
  - Black Swans were not thought (by Europeans) to exist until Captain Cook colonized Australia in 1770 – in fact all available historical data confirmed that black swans did not exist!
  - Consider the first 999 days of a turkey's life – fed & kept warm and dry. It cannot contemplate Thanksgiving because there is nothing in the turkey's history to suggest it even exists.
  
- Don't be a turkey – if the potential consequences are sufficiently dire then you must plan for that eventuality.

\*The ***Black Swan***: The Impact of the Highly Improbable is a **book** about randomness and uncertainty by epistemologist Nassim Nicholas Taleb

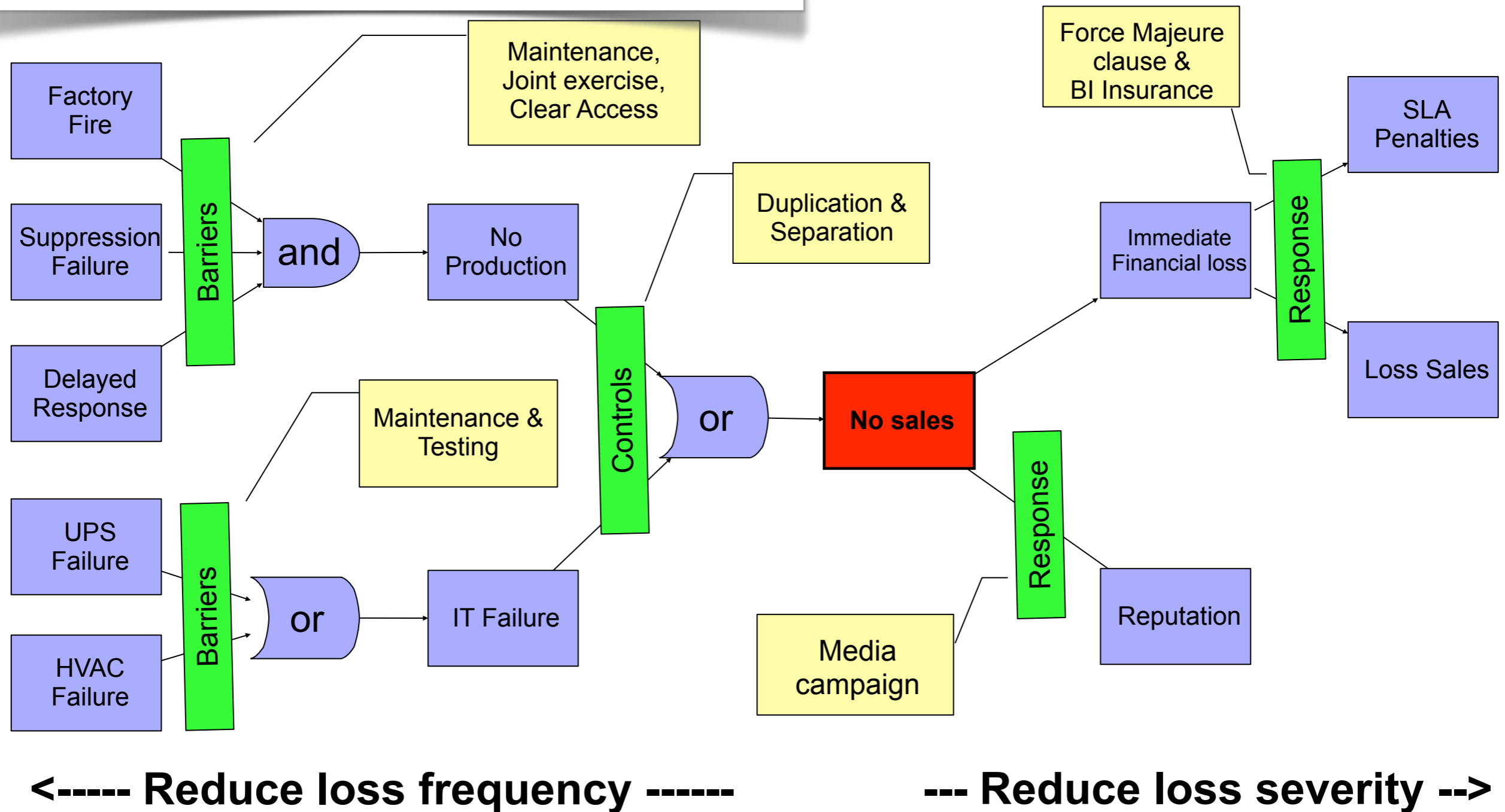
# Bow-Tie Analysis (simple example)

What can go wrong and how bad can it really get - determining the root cause



# Bow-Tie Analysis (simple example)

## Barriers, proactive and reactive controls



# Strategy and the executives

You have to have the boss on your side

- The executives must endorse the strategy for you to succeed
- They will usually only do this if:
  1. There is a damned good BIA available or;
  2. There is a “burning platform”➔ Option 1 is best, 2 leads to panic and pressure

- To attain objectives you must:
  - Ensure continuity of critical processes
  - Protect resources
  - Secure supply
  - Recover if necessary



**Bovine risk management 101**

# Planning vs. “the plan”

The “plan” is only the tip of the iceberg

## ■ Governance

- Risk management policy
- Risk management / steering committee
  - Continuity strategy decisions
- Roles - accountabilities and responsibilities (executive buy-in)

## ■ Up to date BIA

## ■ Proactive controls (a few examples)

- Security improvements (physical and logical)
- Operational resilience – Hazard & SPOF reduction
- Operational controls – reduce errors & enable recoverability
- Maintenance programs

## ■ Reactive controls

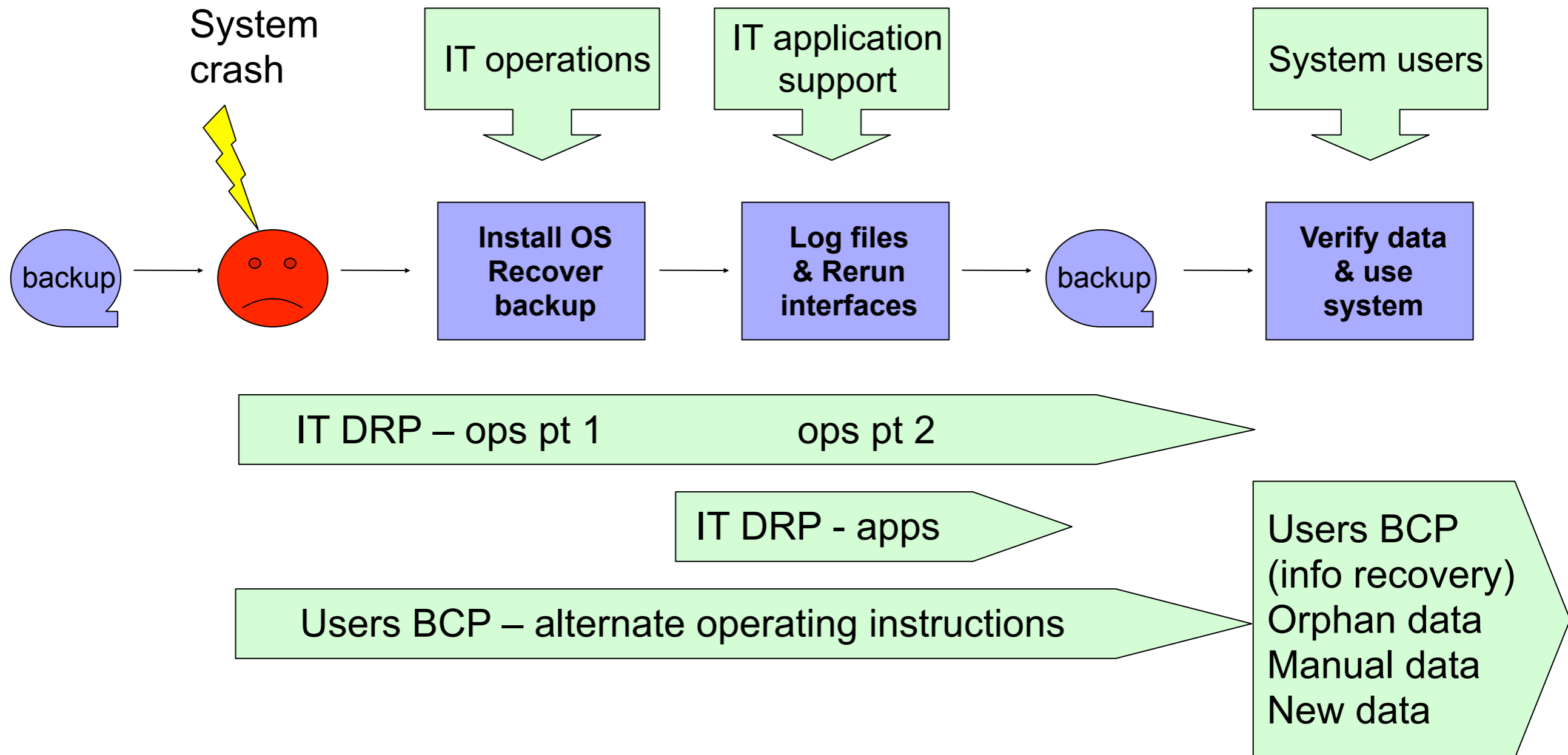
- Activity recovery - alternate workplace
- Technology recovery – alternate data centre and equipment
- Business continuity plans (including resumption plans)



left side of bow tie

BCPs are only one element

# Typical IT failure & recovery sequence



Each team – IT Operations, IT application support, Users – need a plan

# The “Plan” 101

## ■ Minimum plan requirements

- What must I do – Priorities
- What is available to me – Resources
- How do I access those resources – Contact details and/or location

## ■ Scenarios

- Workplace failure – fire, flood, denial of access, utility outage....
- Skills shortage – pandemic, strike, natural disaster, weather .....
- Information loss – IT failure, critical documents, communications ...
- Supply chain failure – business interruption, logistics, (see skills) ...
- Materials and equipment shortage – destroyed, damaged, not supplied

## ■ Communication

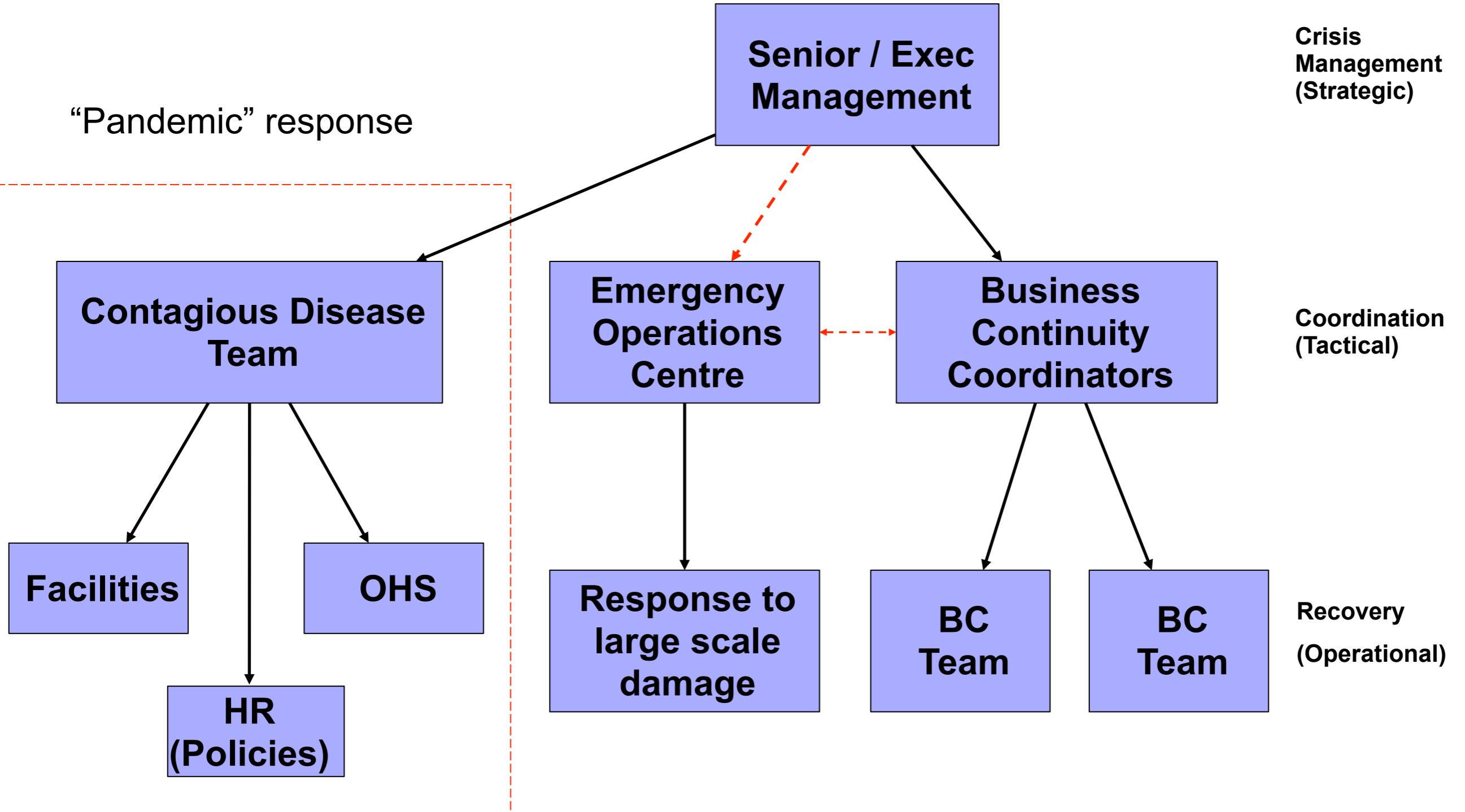
- Chain of command & authority levels
- Problem escalation criteria
- Communication plan (incl. alternatives to corporate email / intranet)

➡ The simpler the plan, the more likely it is to be up to date.

➡ The simpler the plan, the more time you will have to spend on exercises.

# A response structure

“Pandemic” response



The EOC may be opened for large infrastructure damage e.g. loss of major building

# Some current threats

## ■ Pandemic influenza - its all about the people

- Proactive HR policy revisions
  - telecommuting, time off
- Proactive transmission mitigation
  - (personal hygiene, social distancing, cleaning)
- Departmental business continuity plans that include:
  - Identified priorities (what do we do now, what do we leave for later)
  - Alternative staff (identified alternatives with experience and/or X-trained)

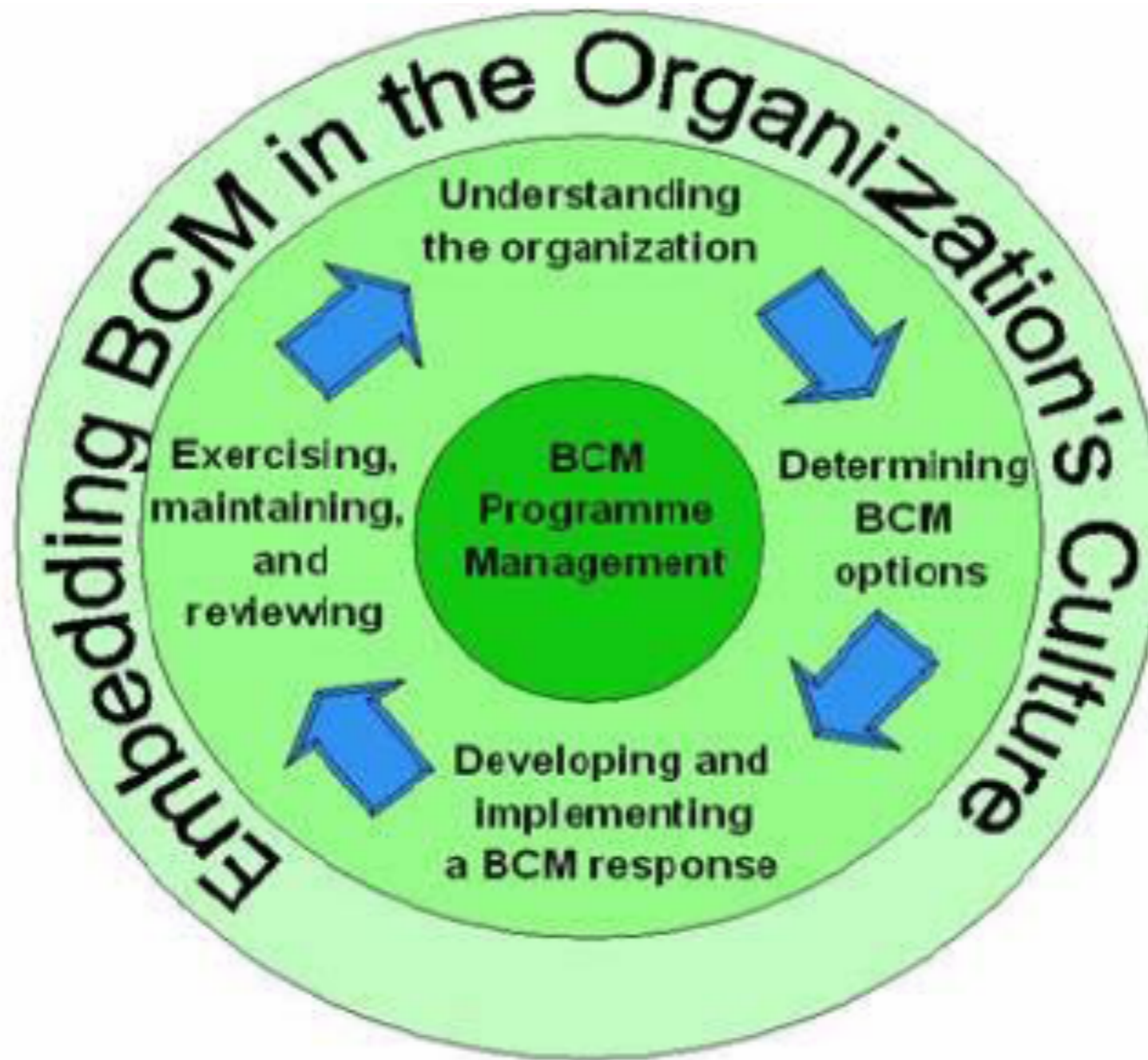
## ■ 2010 Winter Games - its all about the people

- Proactive HR policy revisions - flexible work arrangements
  - telecommuting, alternate work locations, alternate hours of work, time off
- Proactive planning for alternate work locations
  - (Other offices close to home and/or telecommute)
- Departmental Business continuity plans that include:
  - Identified priorities (what do we do now, what do we leave for later)
  - Alternative staff (identified alternatives with experience and/or X-trained)

# Summary

- BCM is a program, not a project
- BCM is risk management
- BCM is not “just about the plan”
- Governance process is critical to ensure success
- Plan for a few basic situations
  - Loss of: Workplace, People, IT & Information, Supply chain, Critical resources
- Tests and exercises are critical
- Be proactive, address the hazards to reduce loss frequency
- Simple plans are better than no plan or an out of date plan

# Where are you ?



# Are you prepared ?



# Thank You

- Questions?



# Leading Practices & Standards

- Business Continuity Institute ([www.thebci.org](http://www.thebci.org))
  - Good practice guide (FREE!)
  - Aligns with BS 25999 - probably future ISO standard
- Disaster Recovery Institute ([www.drii.org](http://www.drii.org))
- ASIS ([www.asisonline.org/guidelines](http://www.asisonline.org/guidelines))
- ISO/IEC 27002 (Information security)
- NFPA 1600 / CSA-Z1600