CYBERSEC 2022 臺灣資安大會

CHANGE NOW

數位轉型 資安升級

SEP. 20-22 臺北南港展覽二館

1. 你知道公司的資安風險是『多少』嗎？
2. 你的資安『剩餘風險』是多少嗎？
3. 你的資安投資報酬(ROSI)合理嗎？
4. 你的資安專案是否用在刀口上嗎？
5. 如何有效的比較資安解決方案？
6. 你想要轉嫁資安風險，承保範圍多少才合理？

為什麼需要量化資安風險？

FAIR Risk ($) = Frequency (#%) x Magnitude ($)

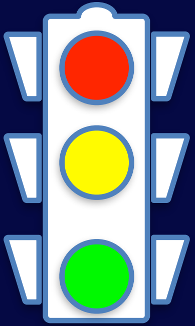
“Risk is the probable frequency and probable magnitude of future loss.”
風險是未來損失的可能頻率和可能大小。

Factor Analysis of Information Risk™

Qualitative
質化分析

BOTH

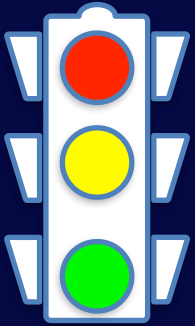
Quantitative
量化分析



High

Medium

Low



$168

$75

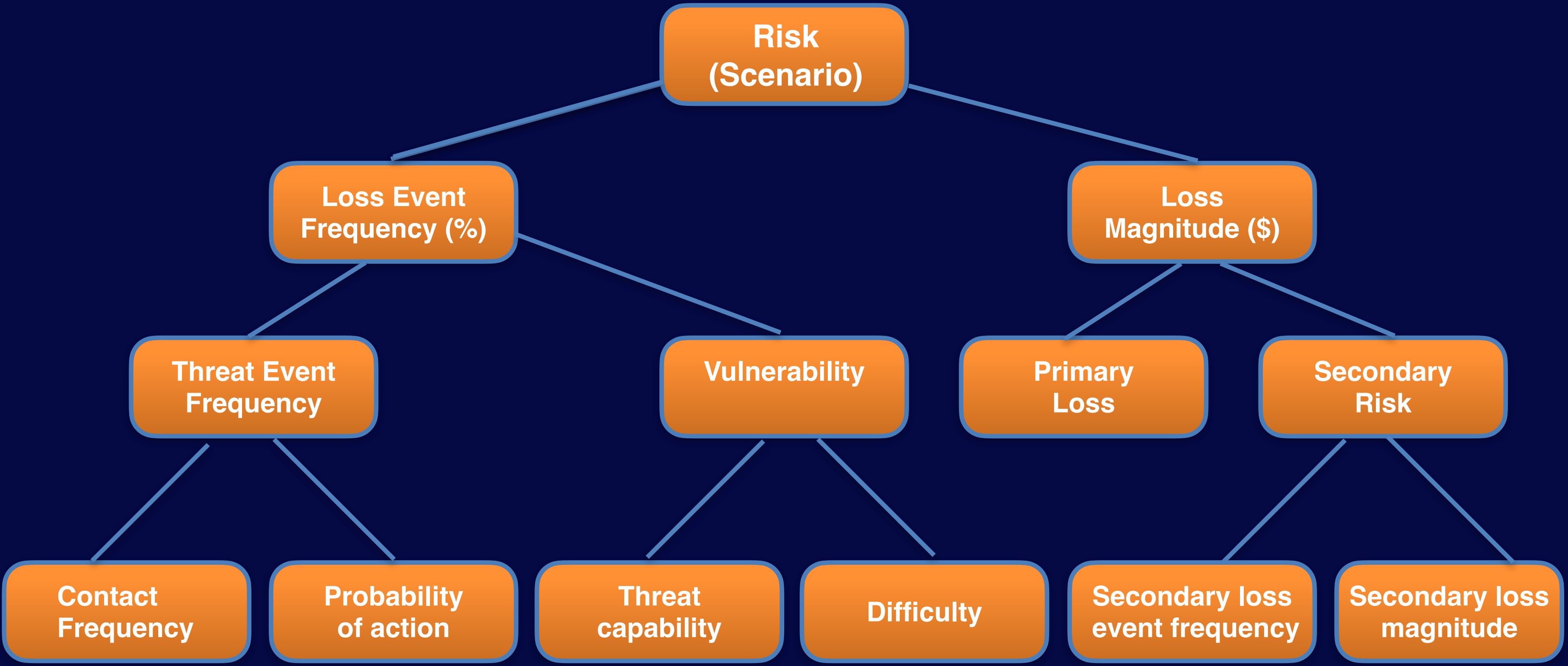
$24

1.FAIR結合質化與量化分析

Let’s play a game.....
俄羅斯輪盤賭局 - 兩把槍都只放一顆子彈

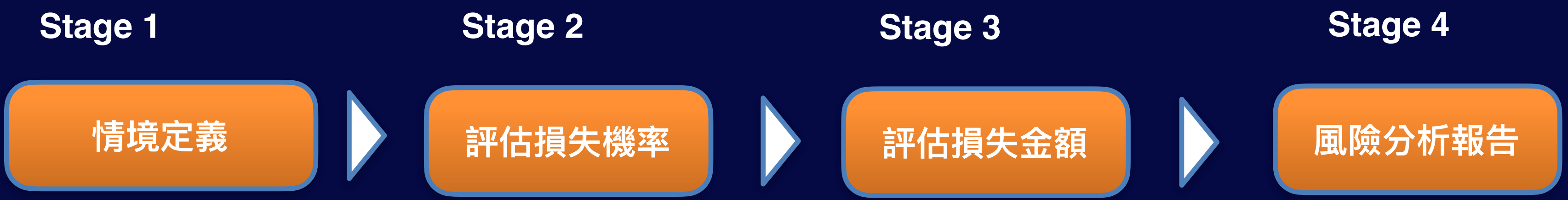
YES	Possibility	YES
16.7%	Probability	100%

2. 可能性 Possibility vs. Probability


Risk
(Scenario)
Loss Event
Frequency (%)
Loss
Magnitude ($)
Threat Event
Frequency
Vulnerability
Primary
Loss
Secondary
Risk
Contact
Frequency
Probability
of action
Threat
capability
Difficulty
Secondary loss
event frequency
Secondary loss
magnitude

3. FAIR 風險概論

FAIR 風險分析階段



Stage 1
情境定義

- Identify the asset at risk
- Identify Threat Actor

Stage 2
評估損失機率

- Evaluate the probable Threat Event Frequency (TEF)
- Estimate the Threat Capability (TCap)
- Derive Vulnerability (Vuln)
- Derive Loss Event Frequency (LEF)

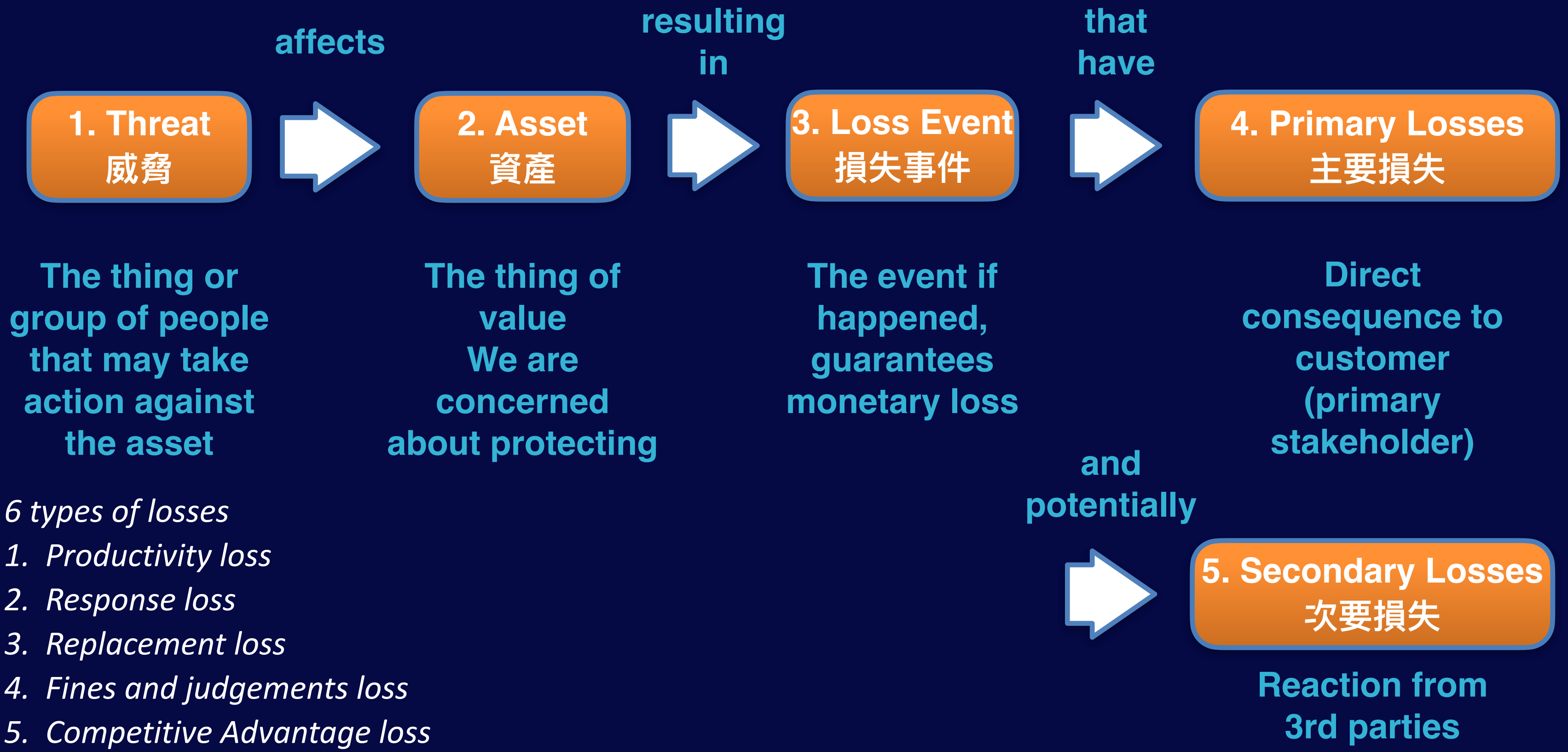
Stage 3
評估損失金額

- Estimate worst-case loss
- Estimate probable loss

Stage 4
風險分析報告

- Derive and articulate the risk

情境定義



1. Threat 威脅 → affects → 2. Asset 資產 → resulting in → 3. Loss Event 損失事件 → that have → 4. Primary Losses 主要損失

→ and potentially → 5. Secondary Losses 次要損失

1. Threat: The thing or group of people that may take action against the asset

2. Asset: The thing of value We are concerned about protecting

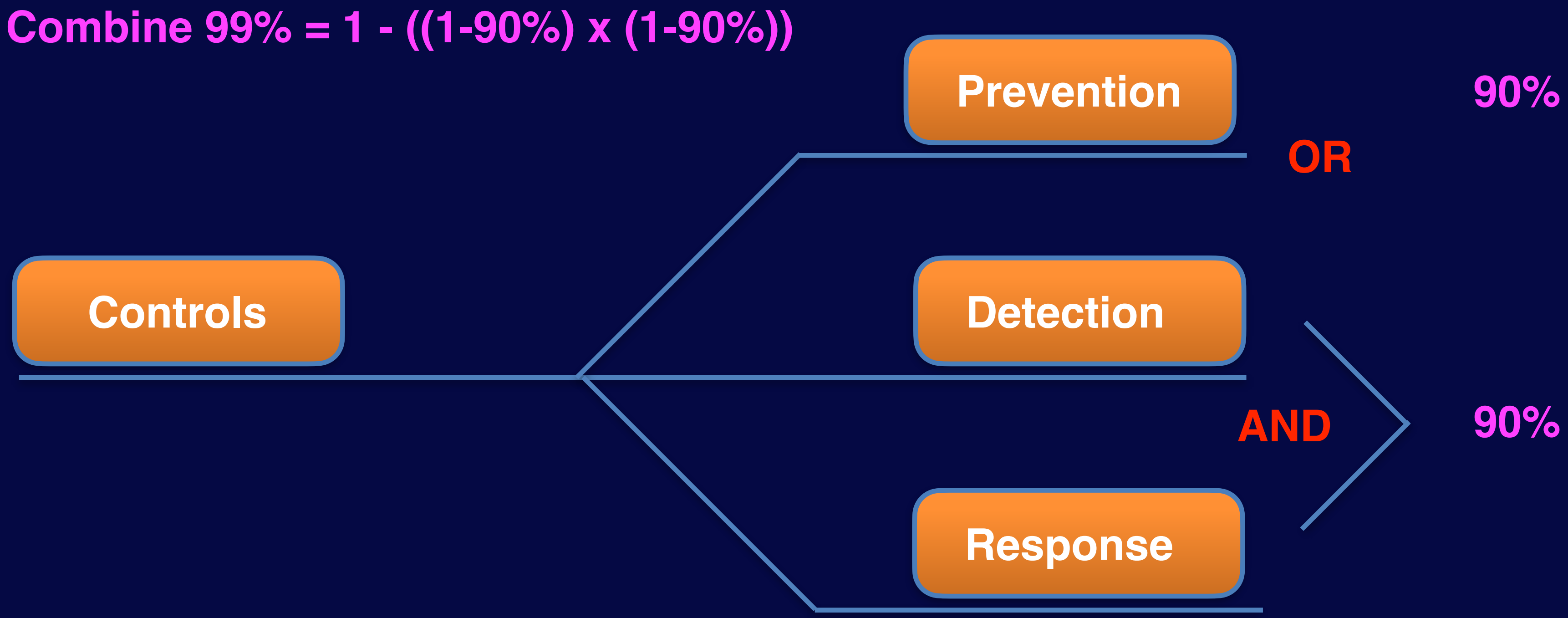
3. Loss Event: The event if happened, guarantees monetary loss

4. Primary Losses: Direct consequence to customer (primary stakeholder)

5. Secondary Losses: Reaction from 3rd parties

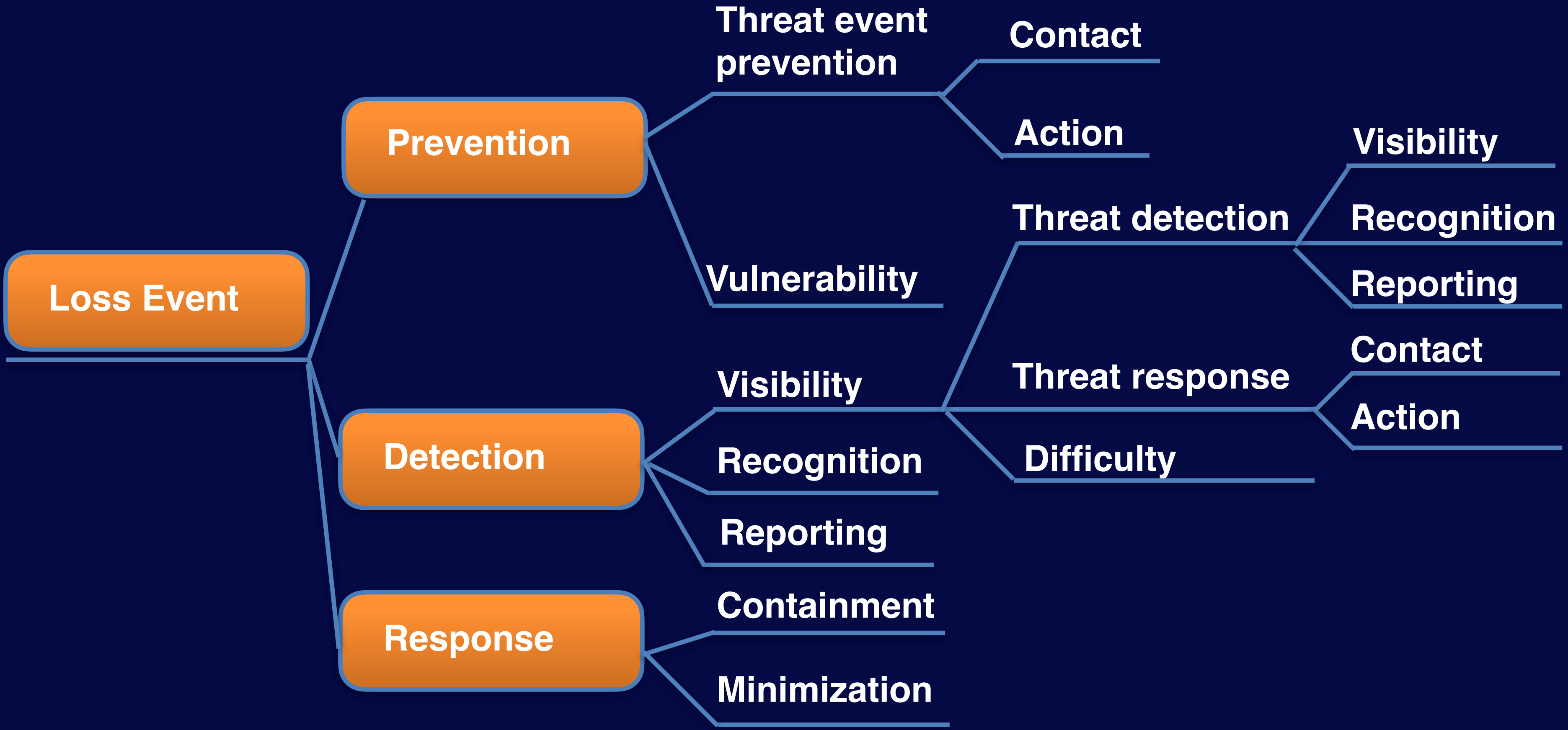
6 types of losses

1. *Productivity loss*
2. *Response loss*
3. *Replacement loss*
4. *Fines and judgements loss*
5. *Competitive Advantage loss*
6. *Reputation loss*

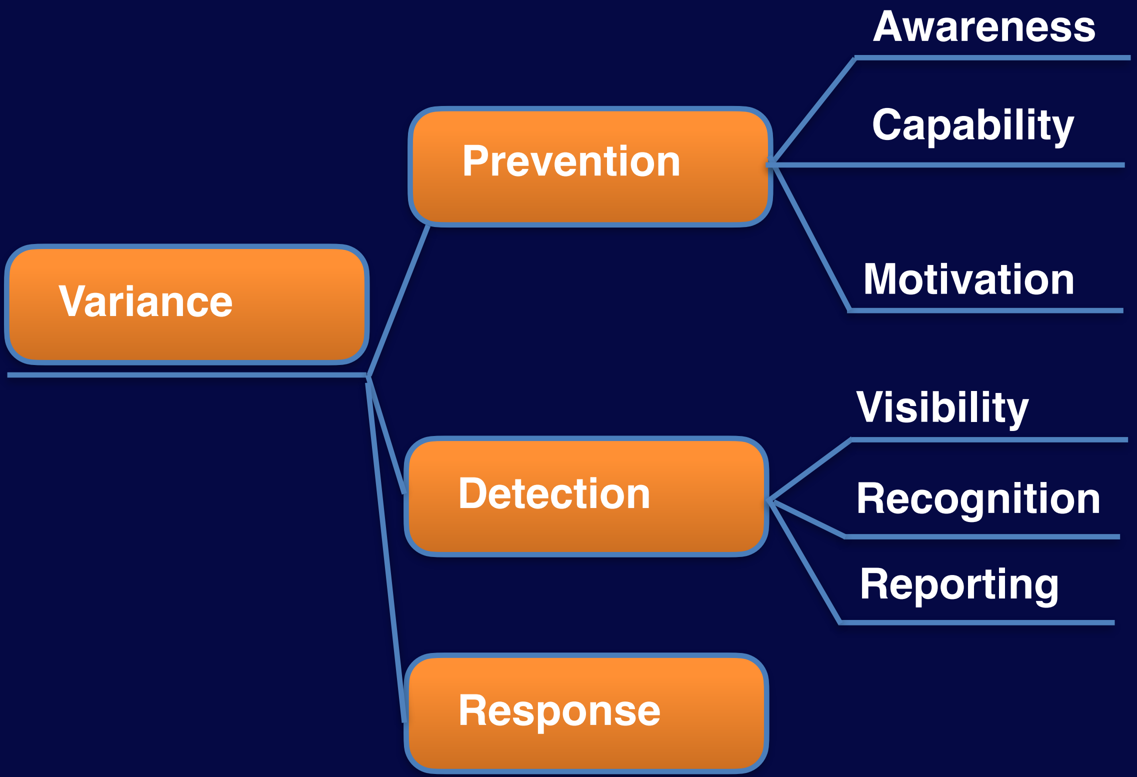


Combine 99% = 1 - ((1-90%) x (1-90%))

4. Control Relationships 控制措施關係圖



Asset-Level Control 資產心智圖



Variance

Prevention

Awareness

Capability

Motivation

Detection

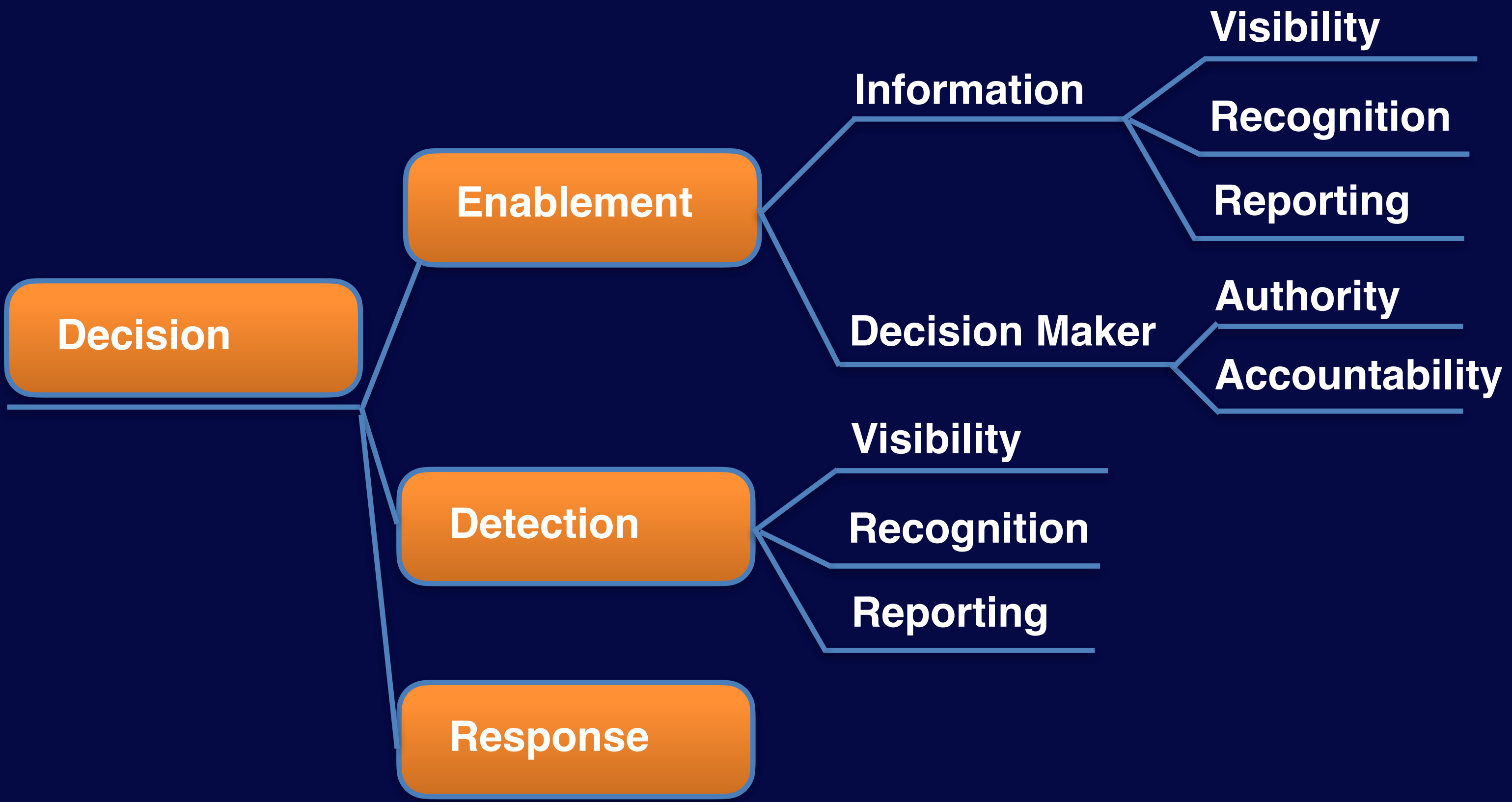
Visibility

Recognition

Reporting

Response

Variance Control 「變動」心智圖



Decision Control 治理決策心智圖

Anthony Lee

@anthony3000

LinkedIn

Medium