LHS

Are We Receiving Value From Our Investment in IT Risk Management?

(1st ISACA Athens Conference)

John Mitchell

PhD, MBA, CEng, CITP, FBCS, CFIIA, CISA, CGEIT, QiCA, CFE

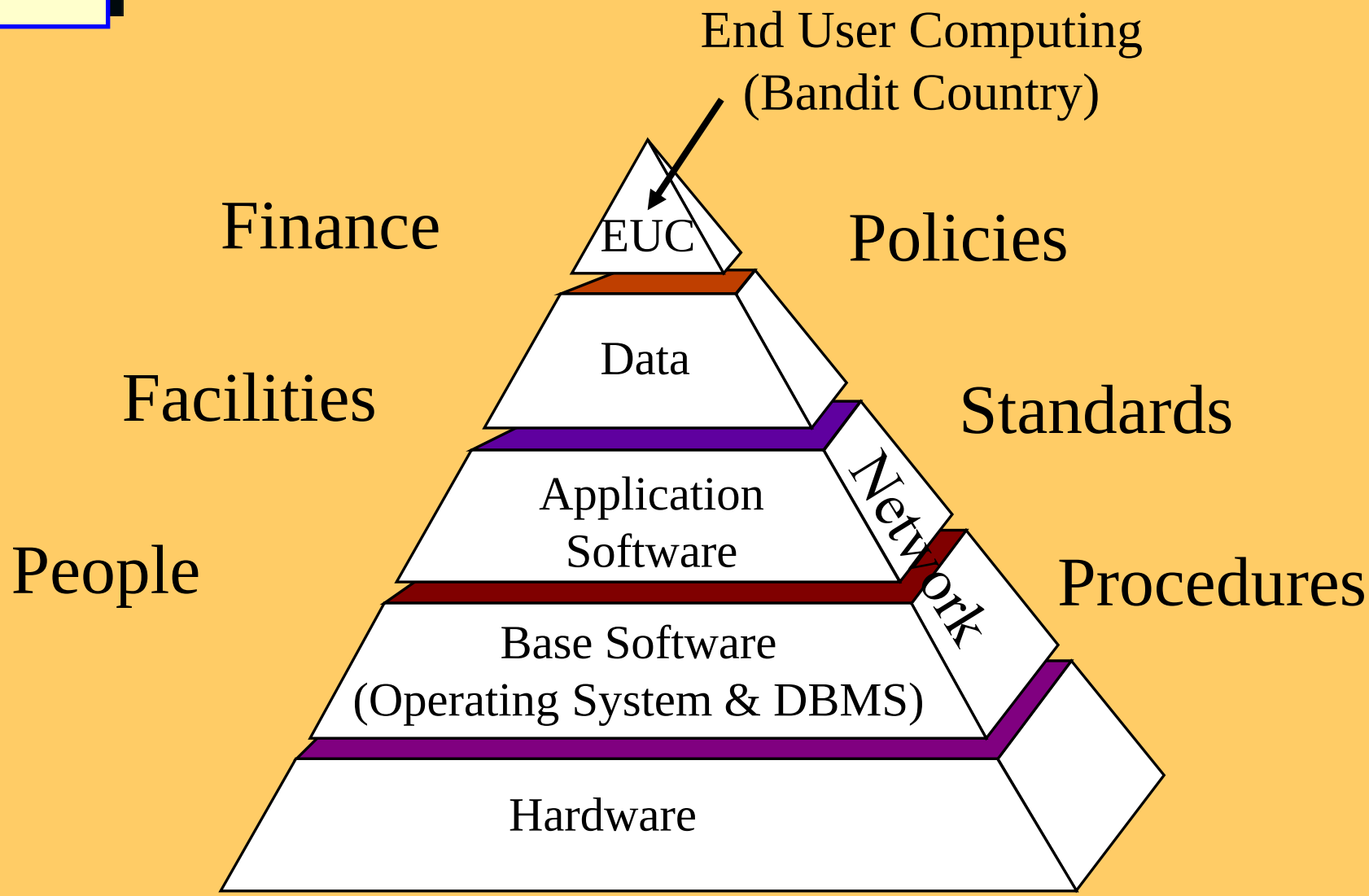
LHS Business Control
47 Grangewood
Potters Bar
Hertfordshire EN6 1SL
England

Tel: +44 (0)1707 851454
Cell: +44 (0)7774 145638

john@lhscontrol.com
www.lhscontrol.com

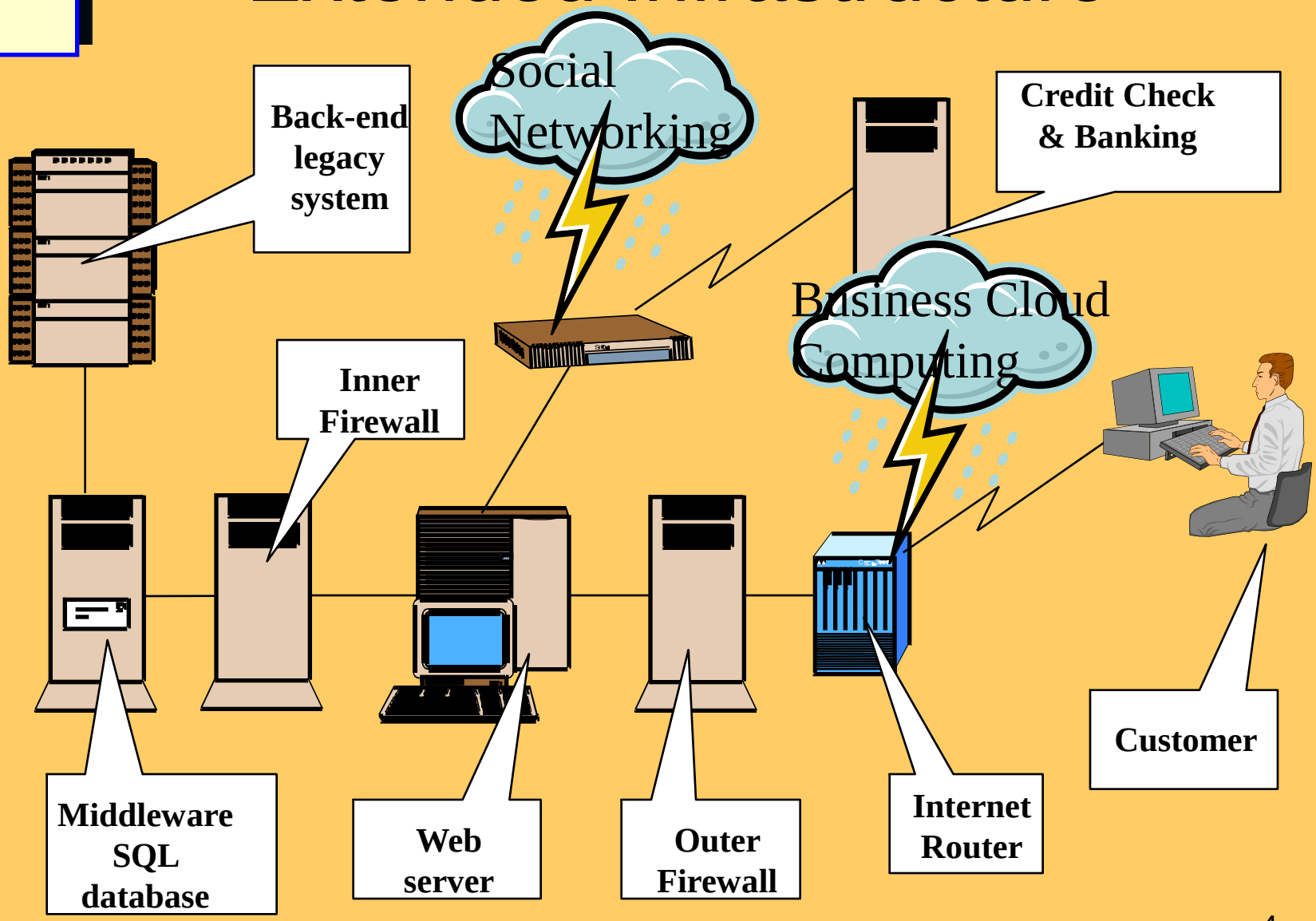
LHS

Simple IT Infrastructure

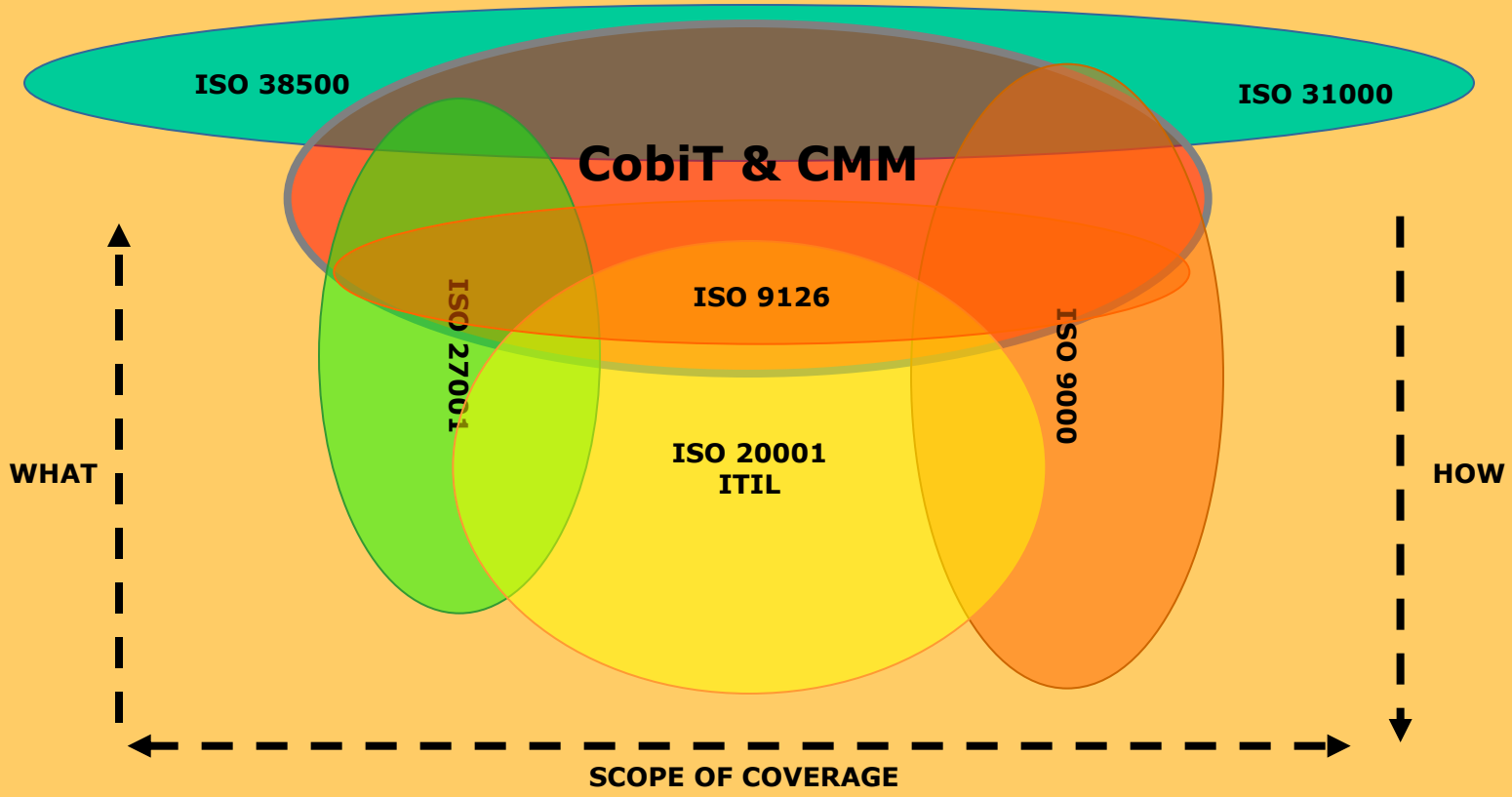


LHS

Extended Infrastructure

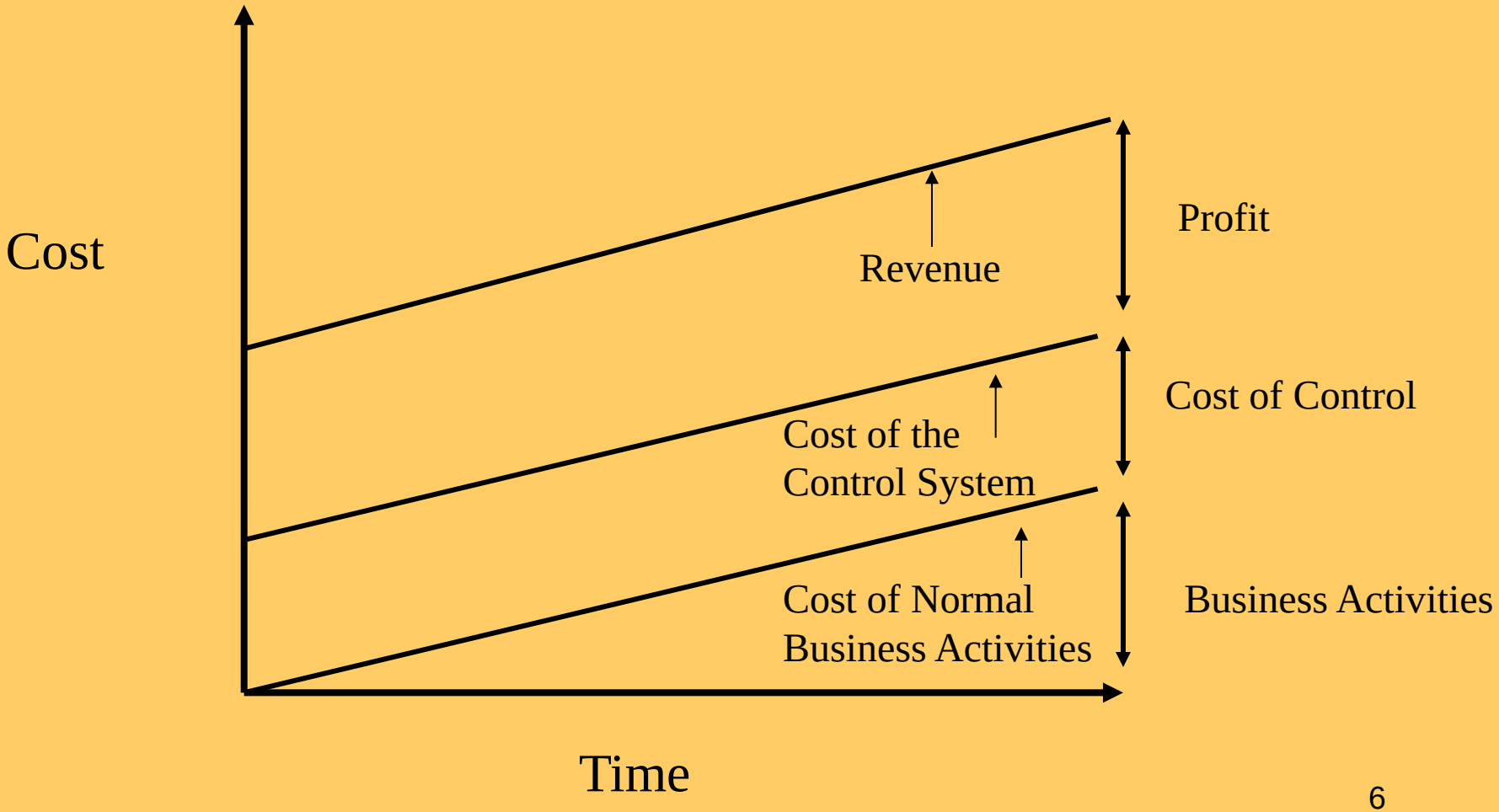


IT Assurance Frameworks

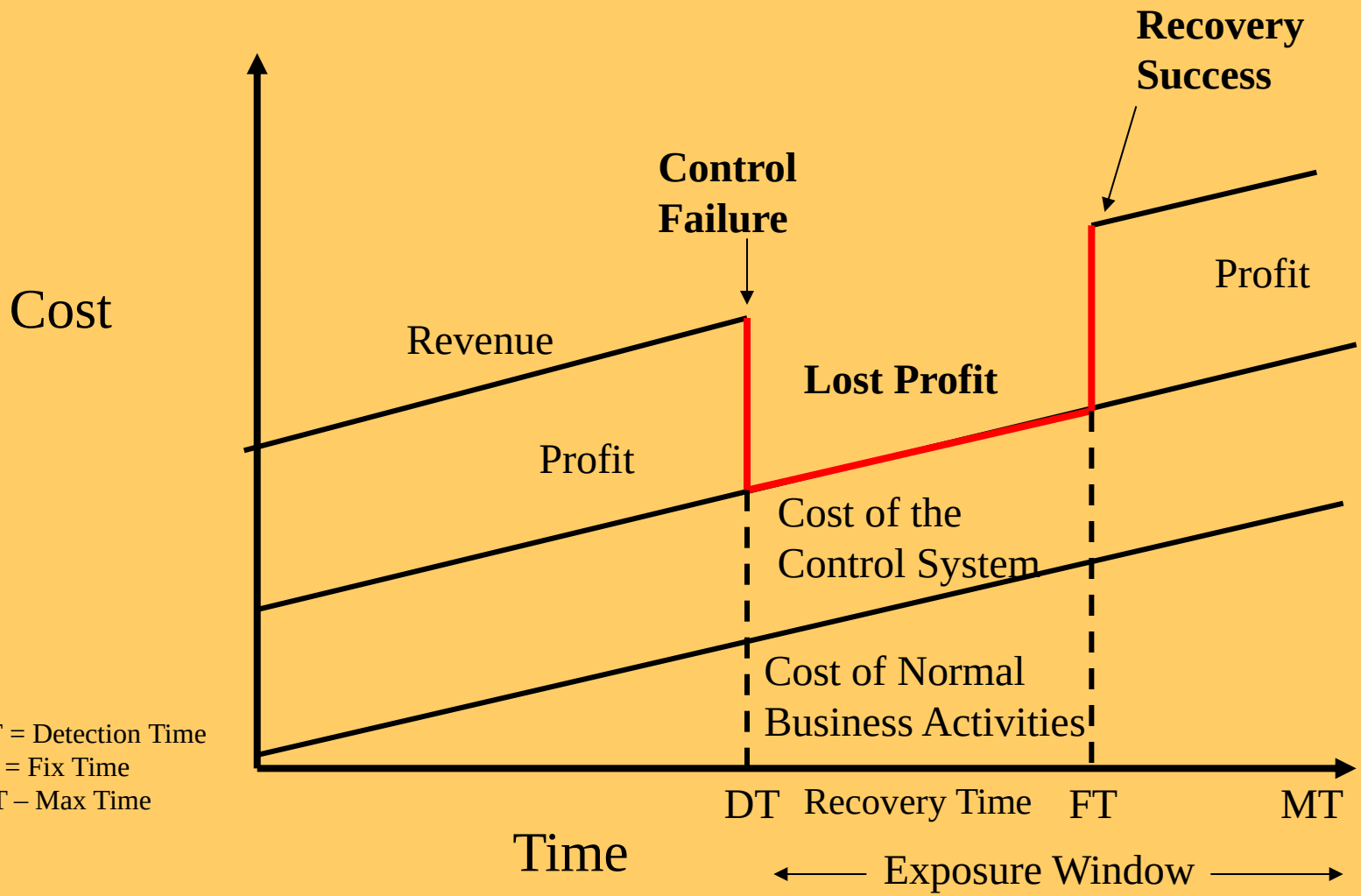


LHS

Impact of Control on Profit (Normal Operation)

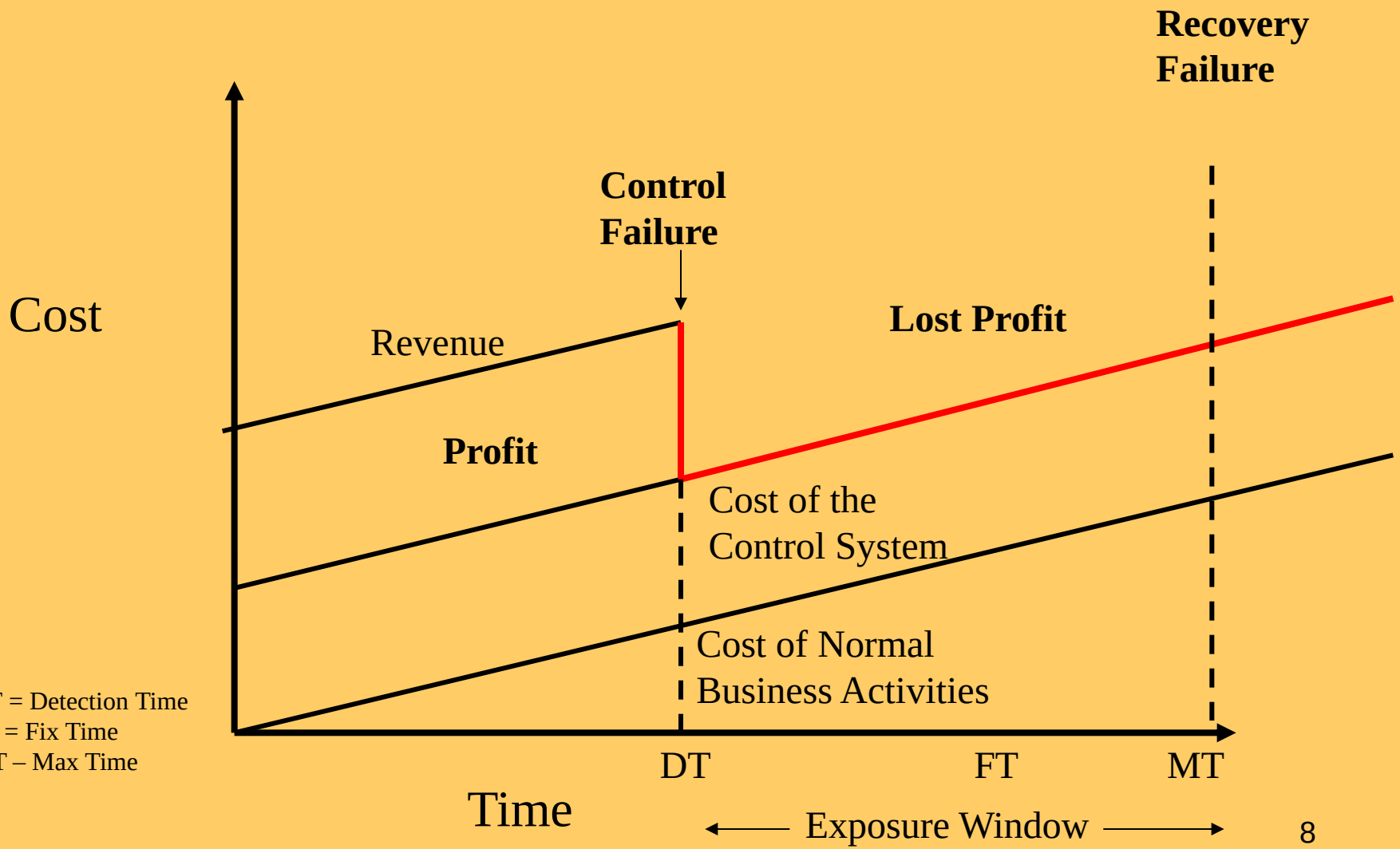


Impact of Control Failure on Profit (With Recovery)



DT = Detection Time
FT = Fix Time
MT – Max Time

Impact of Control Failure on Profit (Without Recovery)



DT = Detection Time
FT = Fix Time
MT – Max Time

LHS

Control Classification

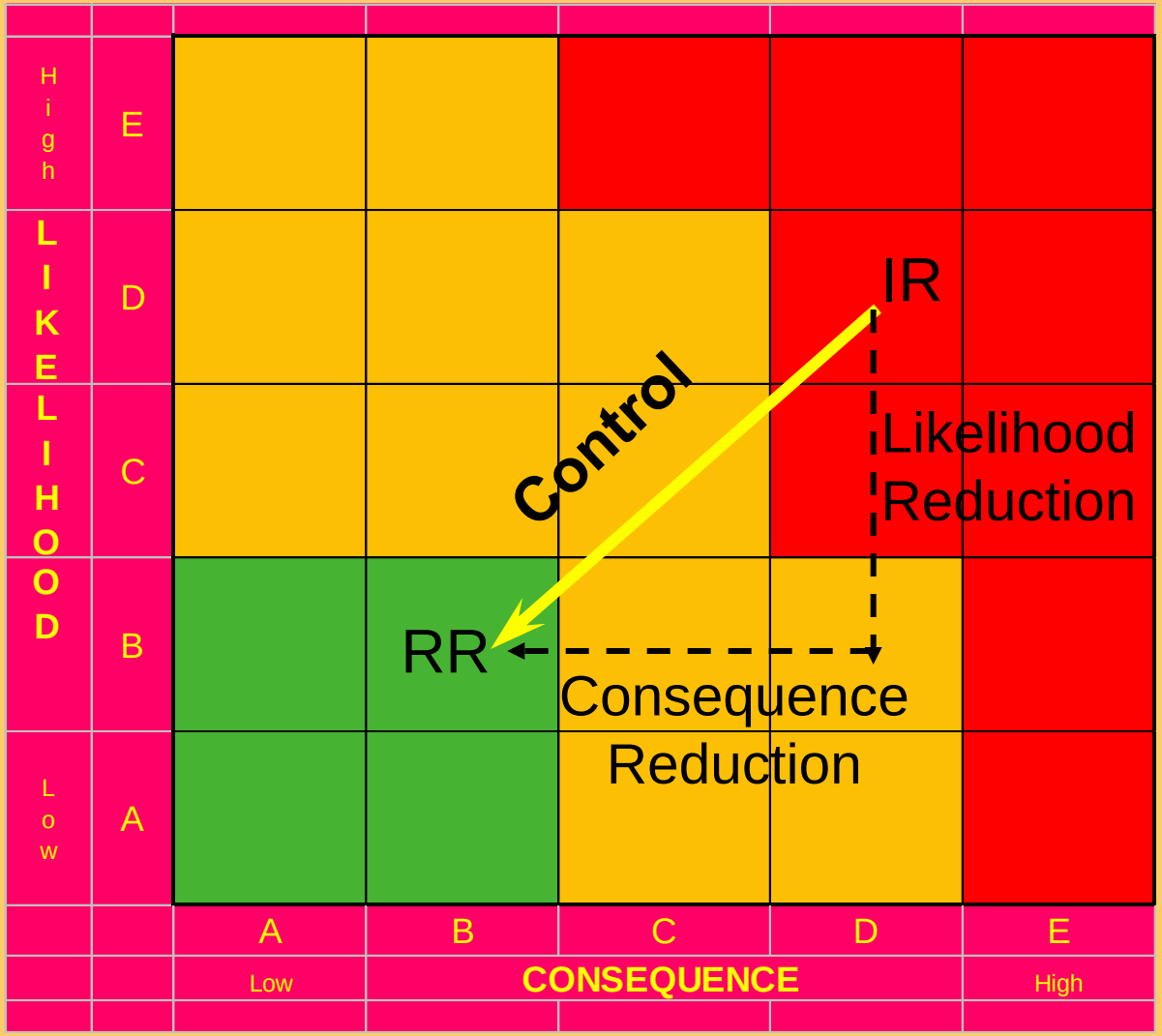
Class	Ability to detect the event and take recovery action	Type
1	Prevents the event, or detects it as it happens and prevents further impact	Preventive
2	Detects the event and reacts fast enough to fix it well within the specified time window	Detective
3	Detects the event and reacts just fast enough to fix it within the specified time window	
4	Detects the event but cannot react fast enough to fix it within the specified time window	
5	Fails to detect the event but has a partially deployed business continuity plan	Reactive
6	Fails to detect the event but does have a business continuity plan	
7	Fails to detect the event and does not have a business continuity plan	

Source: D Brewer & W List

LHS

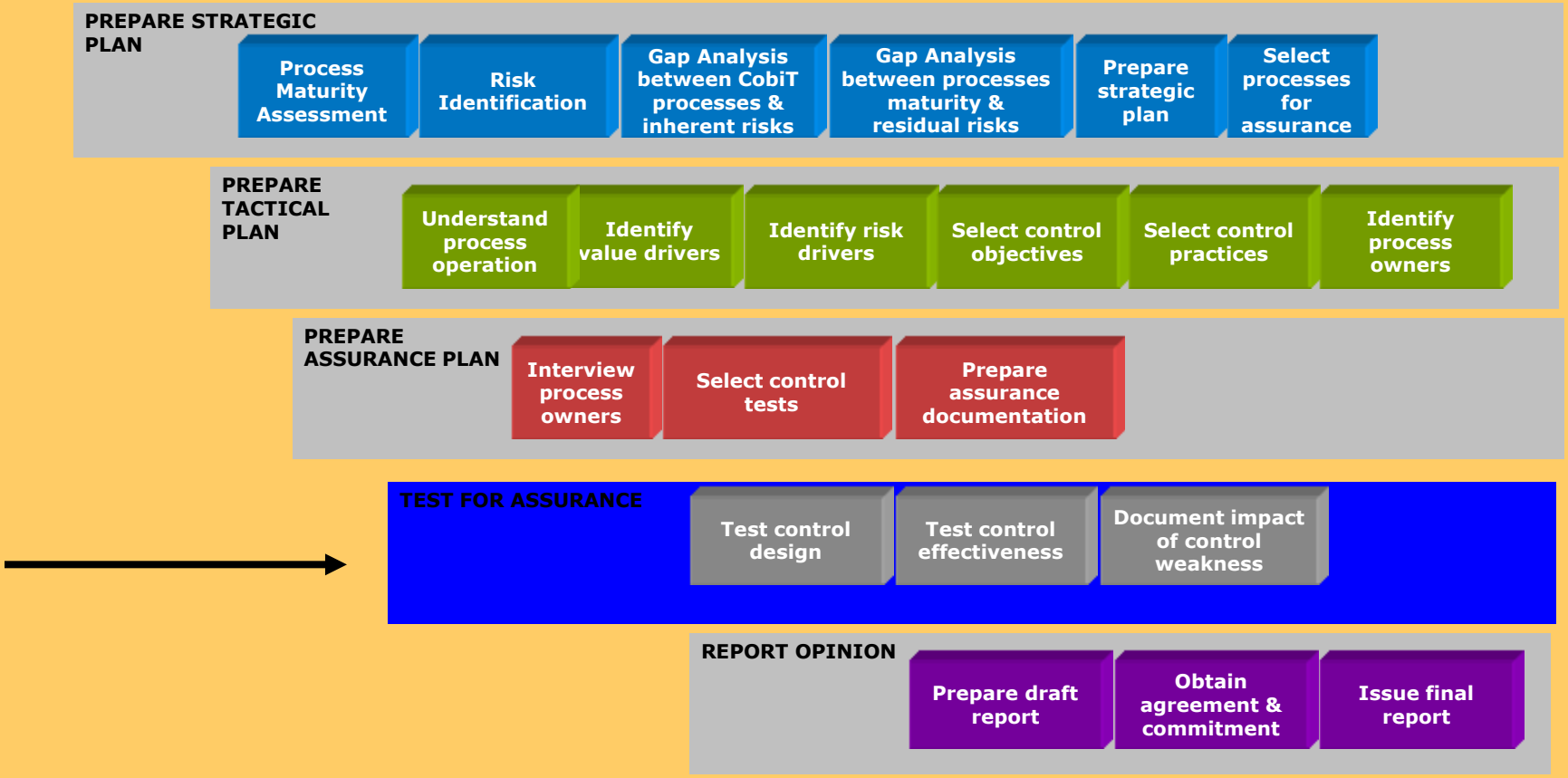
Risk & Control

- Senior Management Attention
- Local Management Attention
- No Action



LHS

IT Assurance Roadmap



LHS

What Is This Control Stuff?

- Definition
  - Anything which monitors or modifies the behaviour of a process so as to make the process predictable
- How Does It Work?
  - A control is simply a test against a known answer

LHS

Effective Risk Management is a journey

LHS

Which One Would You Audit?

Inherent Risk	Controls	Residual Risk
Risk 1	None	High
Risk 2	Some	Medium
Risk 3	Lots	Low

LHS

Anatomy of a Control

- Design
- Implementation
- Monitoring
- Evaluation

LHS

Design

- How well the control should work, in theory, if it is always applied in the way intended:

3) – designed to reduce a risk aspect entirely (either likelihood or consequence)

2) – designed to reduce most of a risk aspect

1) – designed to reduce some parts of a risk aspect

0) – very limited or badly designed, even where used correctly provides little or no protection

LHS

Implementation

- The way in which the control operates in practice:

  3) – the control is always applied as intended

  2) – the control is generally operational, but on occasions is not applied as intended

  1) – the control is sometimes correctly applied

  0) – the control is not applied, or is applied incorrectly

LHS

Monitoring

- How we know that the the control is continuing to operate (embedded monitor):

  3) – operation is always monitored

  2) – operation is usually monitored, but on occasions is not

  1) – operation is monitored on an ad-hoc basis

  0) – operation is not monitored at all

LHS

Evaluation

- How frequently the control effectiveness is evaluated:

  3) – control is regularly evaluated for effectiveness

  2) – control is occasionally evaluated for effectiveness

  1) – control is evaluated on an ad-hoc basis (usually when something goes wrong)

  0) – control is never evaluated

LHS

Scoring Control Effectiveness (Simple Model)

- Design = 3 (3)
- Implementation = 3 (3)
- Monitoring = 2 (3)
- Evaluation = 1 (3)

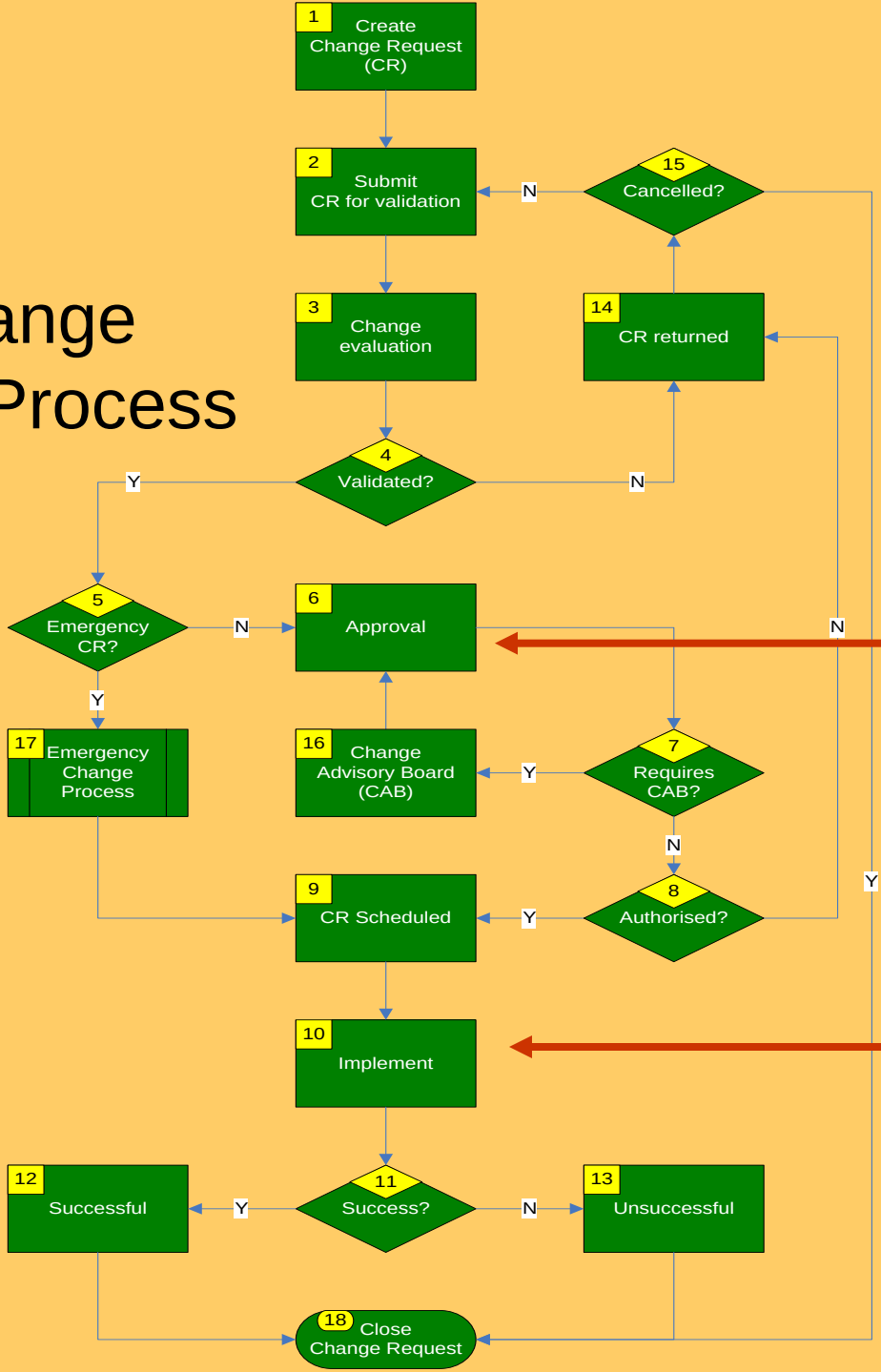
TOTAL SCORE = 9 (12) = 75%

or 75% total effectiveness

$$\sum_{\forall i} x_i = 0$$

LHS

Typical Change Management Process

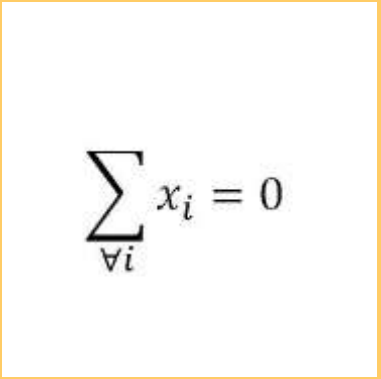


LHS

Prevention Control?

- A signature on a change request will PREVENT an unauthorised change being made

  - Design = 0 (3)
  - Implementation = 3 (3)
  - Monitoring = 3 (3)
  - Evaluation = 3 (3)



SCORE = 9 (12) = 75%

However, as Design scores 0, then total score becomes zero.

LHS

Trust
(A Misconceived Control Mechanism)

- Trust is an action that involves a voluntary transfer of resources (physical, financial, intellectual, or temporal) from the truster to the trustee with no real commitment from the trustee
- A time lag exists between the extension of trust and the result of the trusting behaviour

LHS

Detection Control? (Trust Model)

- Unauthorised changes inserted during an authorised change will be DETECTED by testing

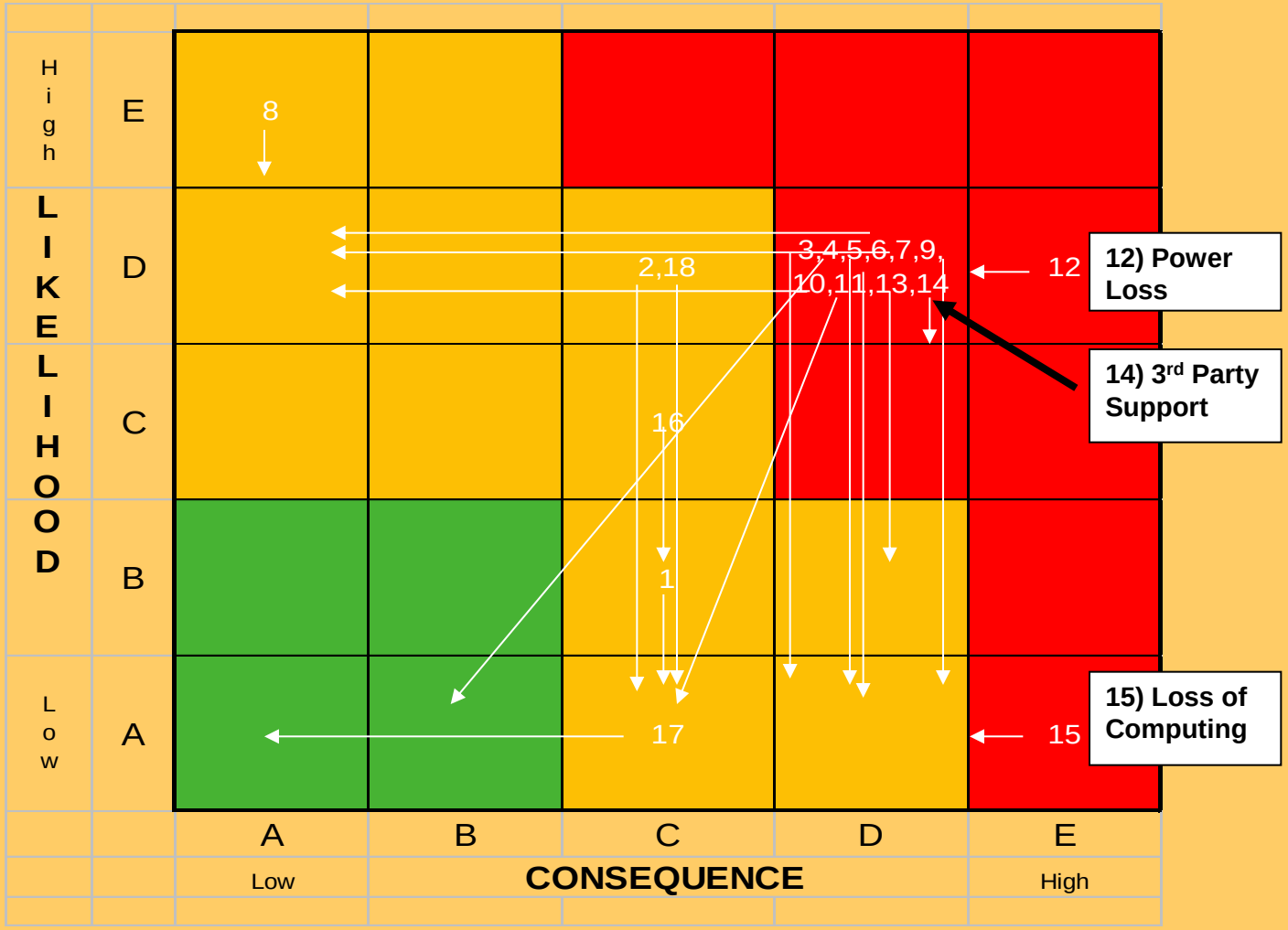
  - Design = 1 (3)
  - Implementation = 3 (3)
  - Monitoring = 3 (3)
  - Evaluation = 1 (3)

$$\sum_{\forall i} x_i = 0$$

SCORE = 8 (12) = 67%

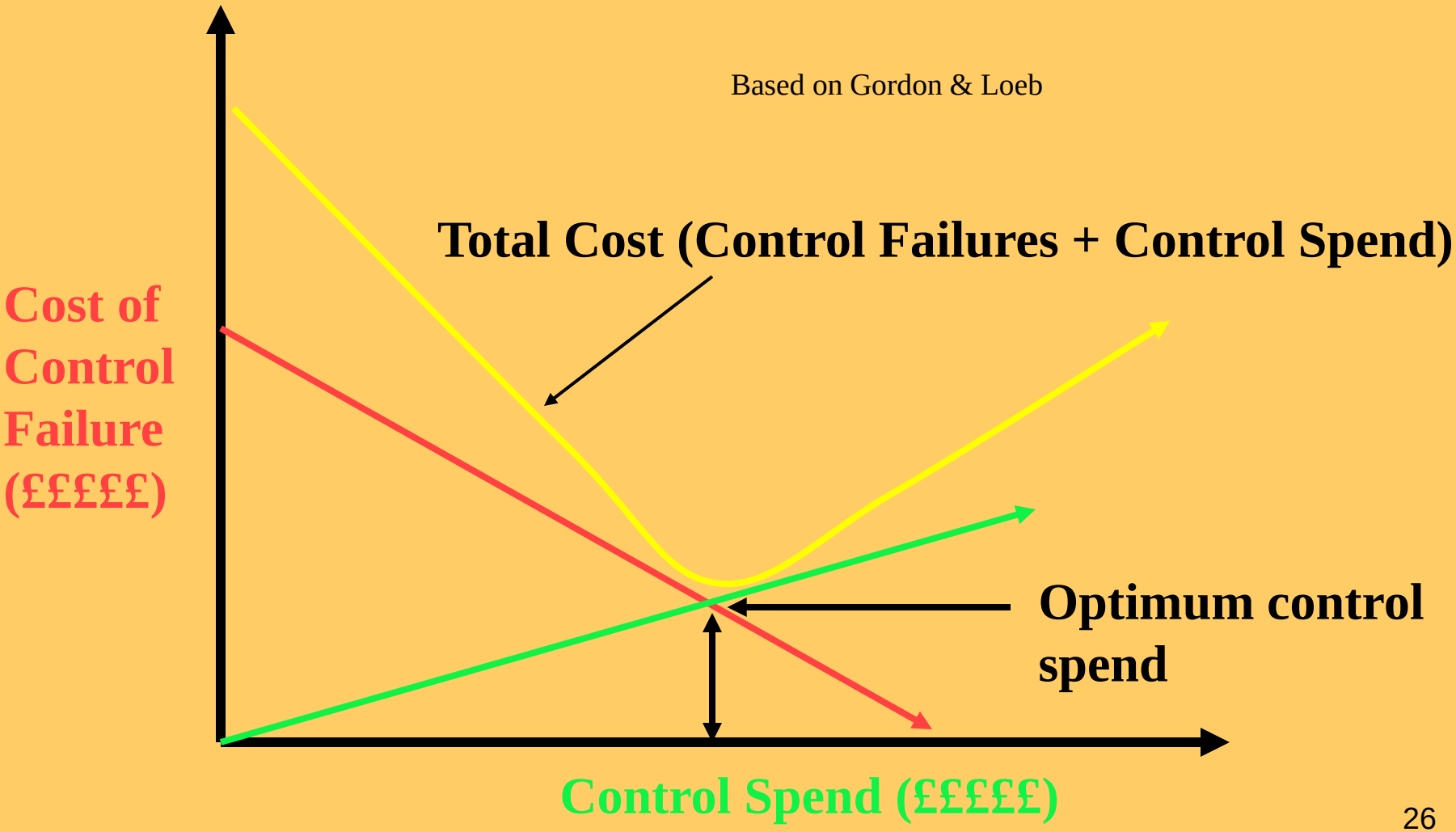
LHS

Importance of Control Effectiveness Measurement



LHS

How Much Should We Spend?



LHS

Things To Think about

- A single control only manages one aspect of the risk equation (either likelihood or consequence)
- Many control processes are based around pre-approvals
- Pre-approvals rely on trust
- Trust is not a control mechanism
- Most of our controls are less than 100% effective

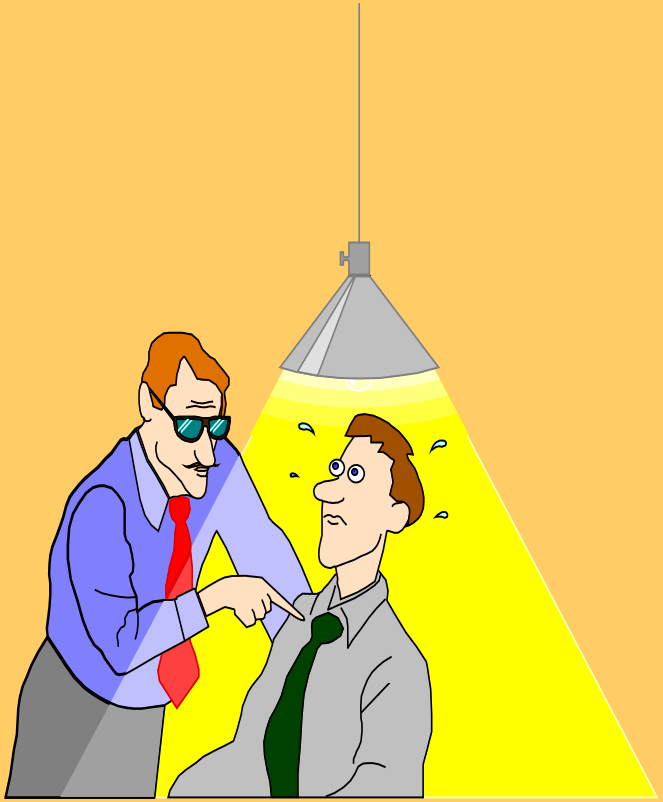
LHS

Summary

- Risk is managed by controls
- Evaluating control effectiveness is the key to risk management
- The value we are getting from our control investment is much less than we think, because most of our controls are not effectively managing our risks

LHS

Questions?



John Mitchell
PhD, MBA, CEng, CITP, FBCS, CFIIA, CISA, CGEIT, QiCA, CFE

LHS Business Control
47 Grangewood
Potters Bar
Hertfordshire EN6 1SL
England

Tel: +44 (0)1707 851454
Cell: +44 (0)7774 145638

john@lhscontrol.com
www.lhscontrol.com