LHS

The Role of the IT Auditor in Protecting Your Business

John Mitchell

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

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

Tel: +44 (0)7774 145638
john@lhscontrol.com
www.lhscontrol.com

LHS

Technology Developments 1970s to Present

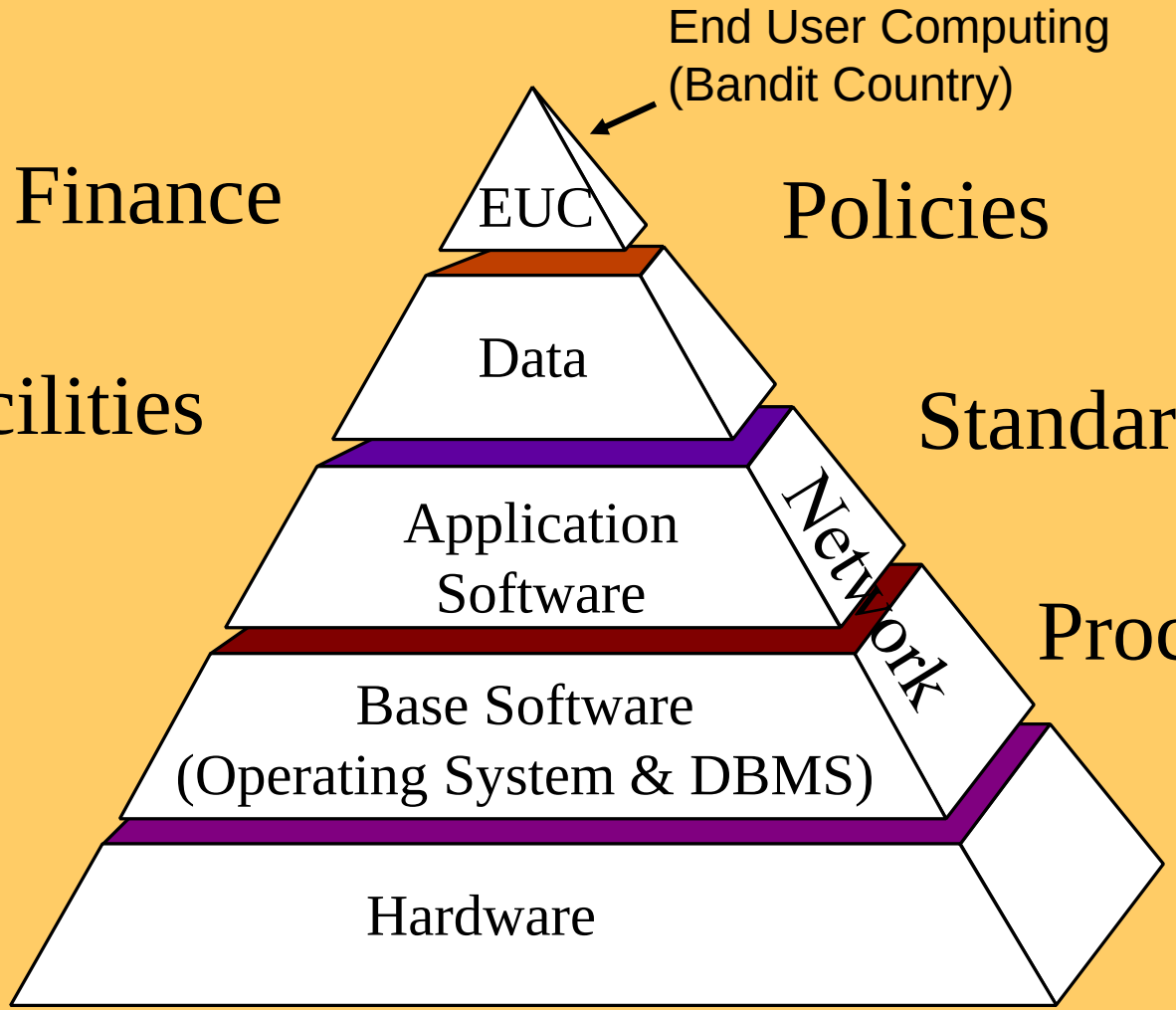
- Single batch program
- Batch multi-tasking
- On-line retrieval
- Real-time update
- Stand alone PCs
- Networking
- File servers & distributed processing
- Internet, Intranet & Extranet
- Palm devices
- Phone devices
- BYOD
- Cloud computing
- 3D printing
- Wearability

LHS

Before & After

LHS

Simple IT Infrastructure



Finance

Policies

Facilities

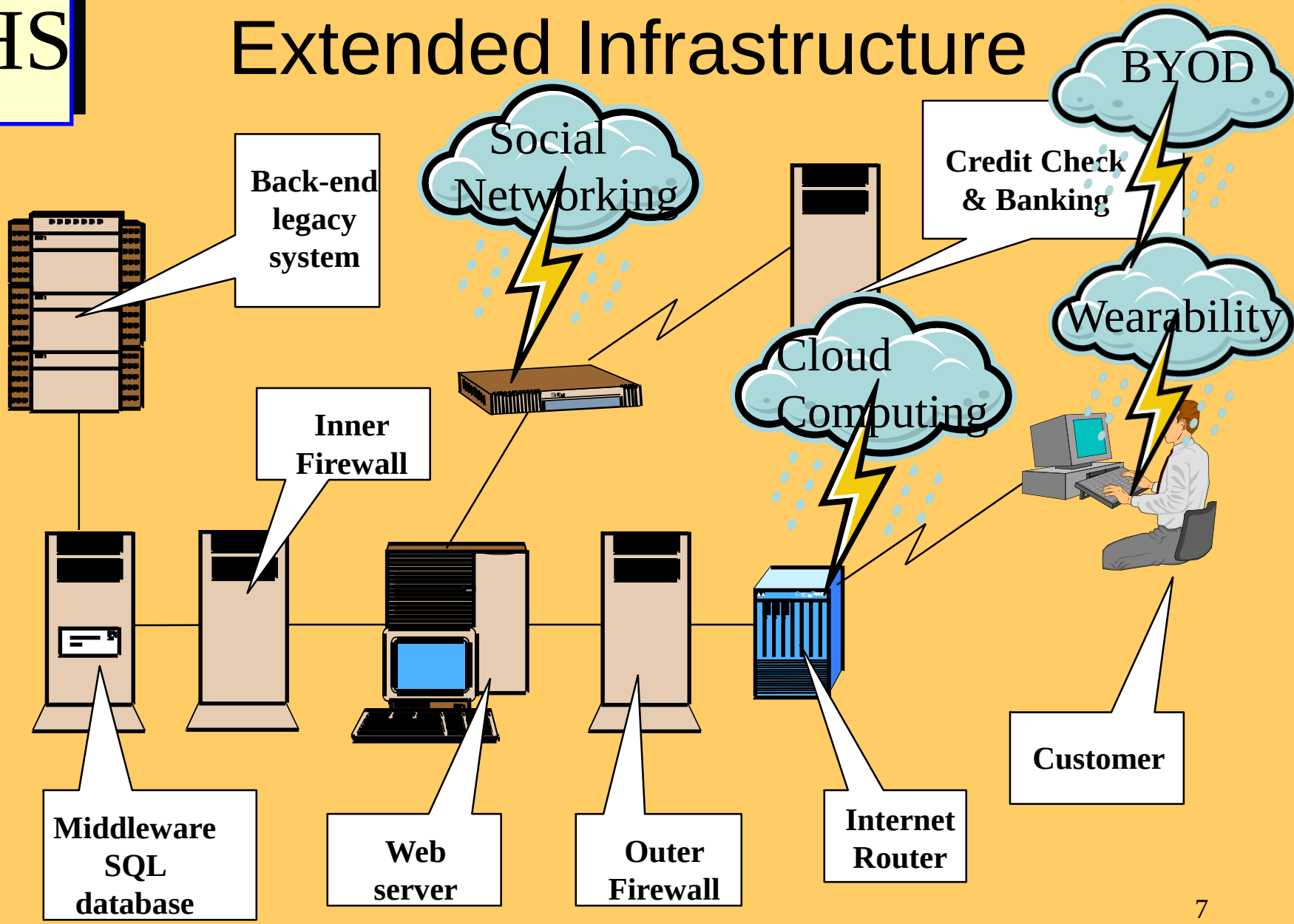
Standards

People

Procedures

LHS

Extended Infrastructure



LHS

Assurance Challenges

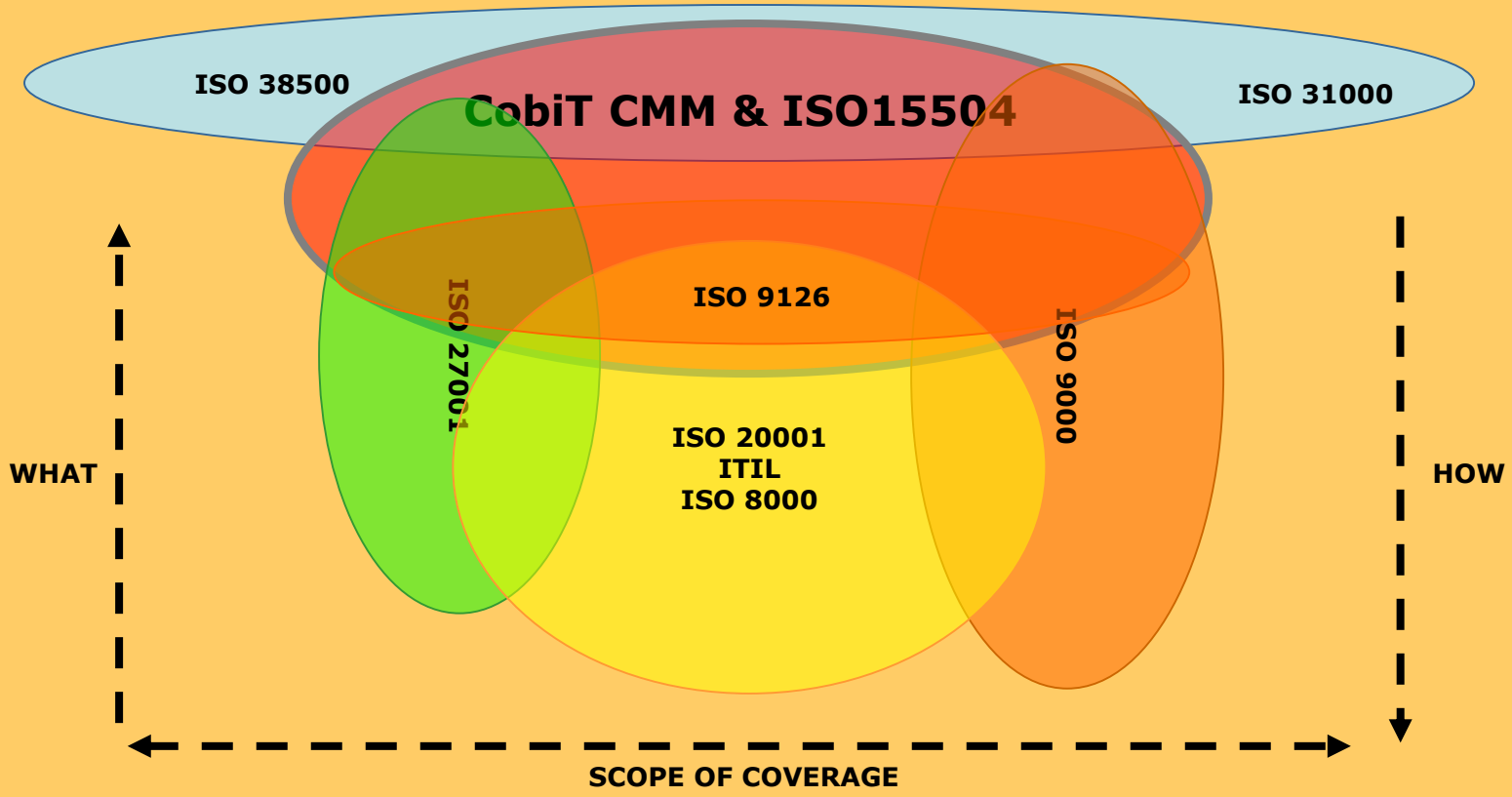
- Invisibility of the data
- Invisibility of the process
- Location of both
- Privilege allocation
- Access control
- Monitoring
- Fixing a point in time

LHS

The Six Big Questions

1) Are you running the correct software?
2) Do your databases have good integrity?
3) Are you correctly processing all your transactions
4) Are your operating processes robust?
5) Are you protected against unauthorised access & manipulation?
6) Can you provide consistence assurance on all of the above?

IT Assurance Frameworks



LHS

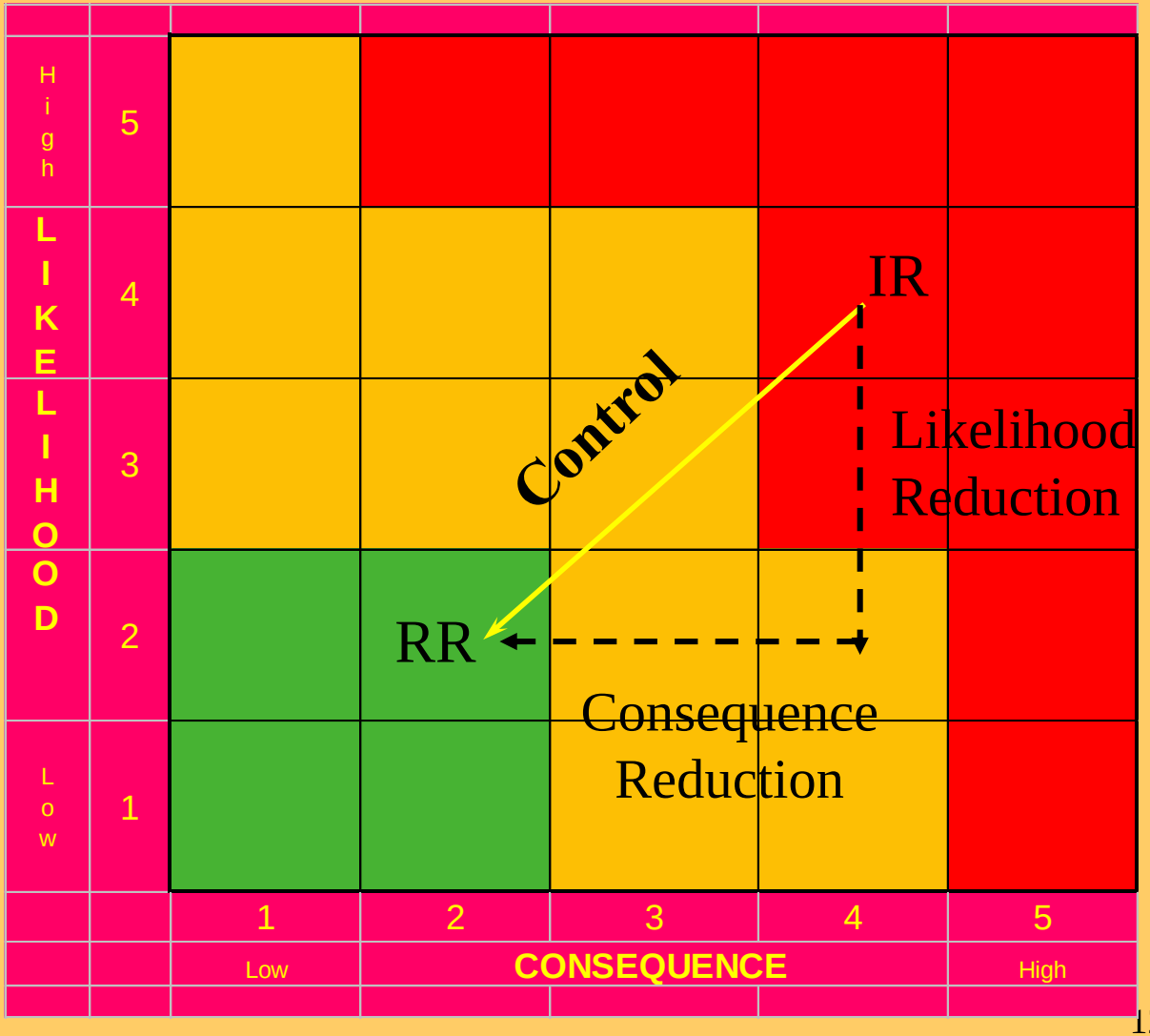
CMM & ISO 15504 Levels

CMM	ISO 15504
5 – Optimised	5 - Optimised
4 – Managed and Measurable	4 – Predictable
3 – Defined	3 – Established
2 – Repeatable	2 - Managed
1 – Ad Hoc	1 - Performed
0 – Non existent	0 - Incomplete

.

LHS Moving From Inherent To Residual

- Senior Management Attention
- Local Management Attention
- No Action



LHS

What Is This Control Stuff?

- Definition
  - Anything which modifies or monitors a process so as to ensure its predictability
- How do they work?
  - A control is simply a test (comparison) against a known (predicted) result

LHS

Control Classifications

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	

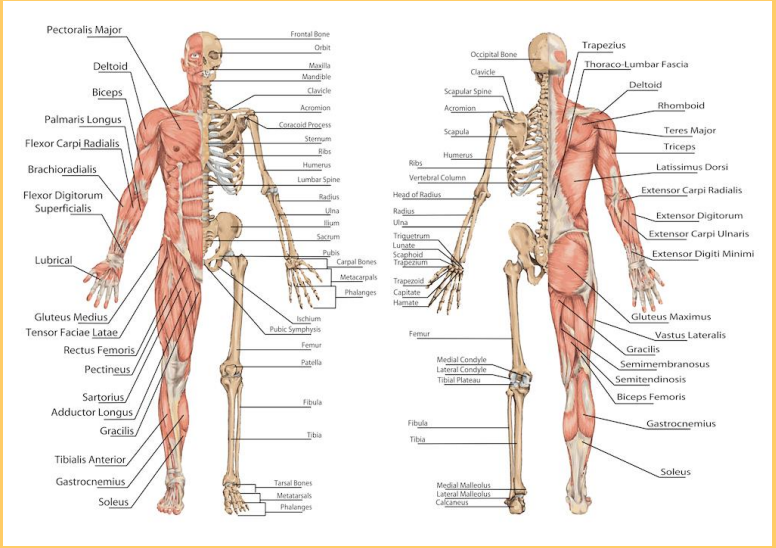
Source: D Brewer & W List

© John Mitchell

LHS

Anatomy of a Control

- Design
- Implementation
- Monitoring
- Evaluation



LHS

Control 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 impact)

  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

Control Implementation

- The way in which the control performs 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

Control 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

Control Evaluation

- How frequently the control effectiveness & efficiency is evaluated:

  3) – control is regularly evaluated for effectiveness/efficiency

  2) – control is occasionally evaluated for effectiveness/efficiency

  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 – Not Weighted)

- Apply DIME:
  - Design = 2 (3)
  - Implementation = 2 (3)
  - Monitoring = 1 (3)
  - Evaluation = 1 (3)
  - **INITIAL SCORE = 6 (12) = 50%**

LHS

Scoring Control Effectiveness (Weighted Model)

- Apply DIME:
  - Design (x3) 2 = 6 (9)
  - Implementation (x3) 2 = 6 (9)
  - Monitoring (x2) 1 = 2 (6)
  - Evaluation (x1) 1 = 1 (3)
  - **INITIAL SCORE = 15 (27) = 55%**

LHS

Risk & Control Documentation

Company:

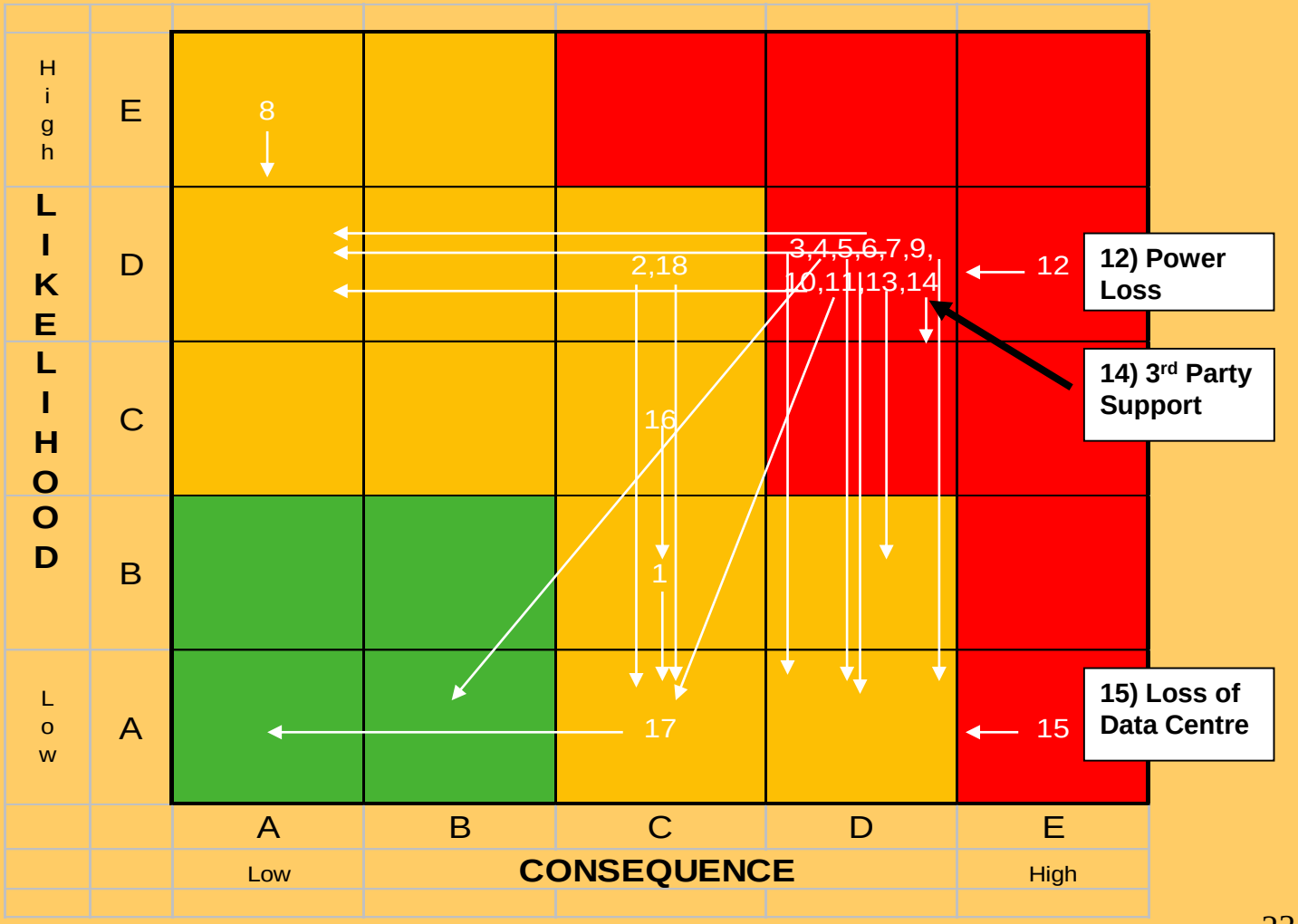
Division:

Location:

Business Area/Activity:									Score the Effectiveness of the Controls in Mitigating the Risk					
									N/A	1	2	3	4	5
A	**Controls for managing the risk of (Risk Description)**													
B	**As a minimum these should include the following standard controls**	**Contr. Class**	**Is it performed?**			**Contr. Score**	**Who/what performs it?**	**How Often?**	**How is it evidenced?**					
			N/A	**Yes**	**No**									
	Control 1 Description													
	Control 2 Description													
	Control 3 Description													
	Control 4 Description													
	Control 5 Description													
	Control 6 Description													
C	**Where the answer to a minimum requirement is NO:** **Please give details of any alternative controls providing assurance**	**Contr. Class**	**Is it performed?**			**Contr. Score**	**Who/what performs it?**	**How Often?**	**How is it evidenced?**					
			N/A	**Yes**	**No**									
D	**Where the score for control effectiveness is < 3** **Please detail the control which is to be implemented to improve the result**	**Contr. Class**	**Proposed Implementation Date**			**Pot. Score**	**Who/what will perform it?**	**How Often?**	**How will it be evidenced?**					

LHS

Risk Reporting



LHS

Things to Ponder

- “If the only tool you have is a hammer, you tend to see every problem as a nail”

  Abraham Maslow
- “It's so much easier to suggest solutions when you don't know too much about the problem”

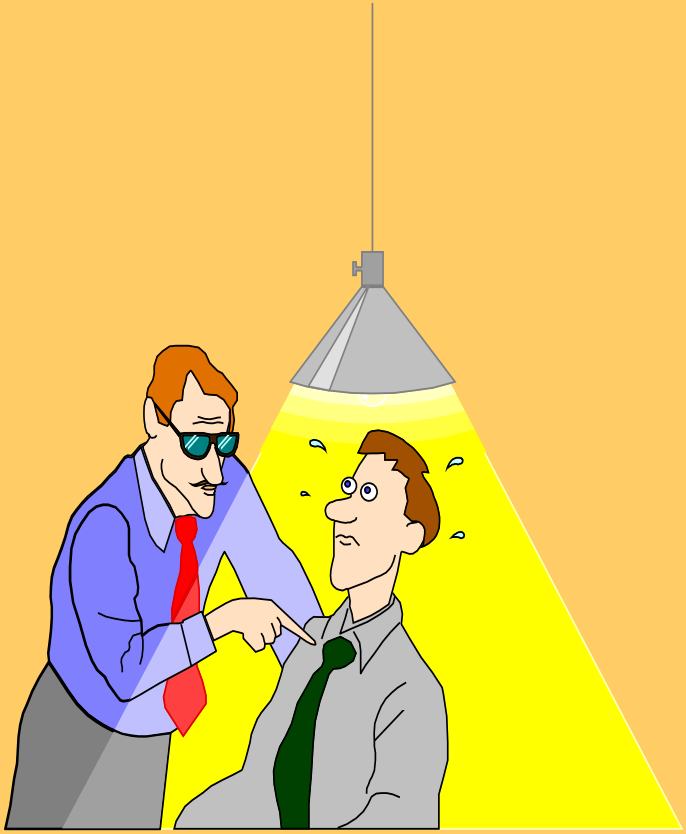
  Malcolm Forbes
- “For every complex problem there is a solution which is simple, clean and wrong”

  Henry Louis Mencken
- “We don’t know what we don’t know, until we know it”

  Karl Popper

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)7774 145638

john@lhscontrol.com
www.lhscontrol.com