Why Are We Here and Where Are We Going?

10th June 2025

John Mitchell

PhD, MBA, CEng, CITP, FBCS, CFIIA, CIA, 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

This Session

- IRMA was not always IRMA
- Advances in technology introduced new risks and opportunities
- Concept of risk management
- Development of the control environment
- Better understanding of how to control the technology
- Expert systems v AI
- What I want from AI

John Mitchell

Career

Data controller

Computer operator

Programmer

System's analyst

Business analyst

Project Manager

Computer auditor

LHS Business Control

Certifications

PhD

MBA

CEng

FBCS

CITP

CIA

CISA

CGEIT

CFIIA

QiCA

CFE

How Did We Get Here? (Professional Development)

1957	British Computer Society Established
1965	Auditing by Computer (abc) Group associates with the BCS
1981	ISACA London Chapter formed by abc members
1983	Information Security Specialist Group (ISSG) spun off from abc
1984	BCS becomes the Chartered Institute of IT
1990	abc becomes the Computer Audit Specialist Group (casg)
2001	casg becomes the Information Risk and Assurance Specialist Group (IRMA)

1965 Auditing By Computer (abc) SG

- Use of computers to aid audit work
- Use of high-level programming languages for audit purposes
  - COBOL
  - Filetab
- Development of audit programming languages
  - IDEA
  - ACL
- Data analytics
- Detecting anomalies
- Producing samples for off-line assurance

1990 Computer Audit Specialist Group (casg)

- System Development Processes
- Implementation
- Change Management
- Service Delivery
- Outsourcing
- Control Environment
- IT Governance

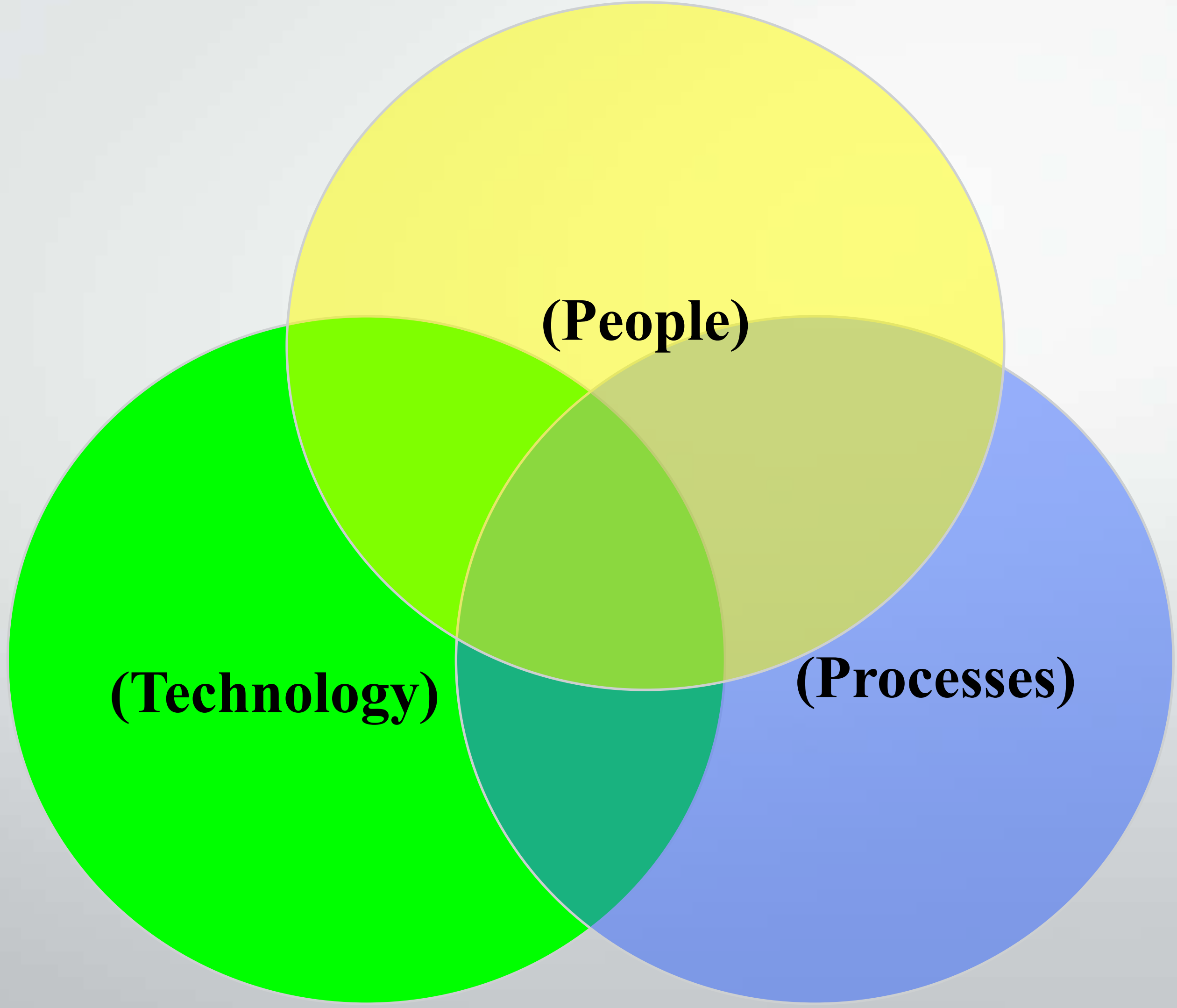
2001 Information Risk Management & Assurance (IRMA) SG

- Risk identification and analysis
- Risk Management Mechanisms
- Measuring Control Effectiveness
- Risk Reporting
- Risk Visualisation

IRMA Objectives

- Encourage research into the risk management and assurance of information systems and to promote the development of information risk management and assurance techniques to reflect changes in technology, legislation, and society.
- Provide a forum for the development of awareness and competence in information systems risk management and assurance.
- Promote the efficient, effective, and economical use of risk management and assurance within information systems.

IT is Not Just the Technology



Why Did We Get Here?
(Technological changes since the 1960s)

Mainframe Computers

Single batch program

Batch multi-tasking

On-line retrieval

Stand alone PCs

Networking

Real-time update

File servers & distributed processing

Expert Systems

Internet

Palm devices

Phone devices

BYOD

Cloud computing

3D printing

Machine learning

Artificial Intelligence

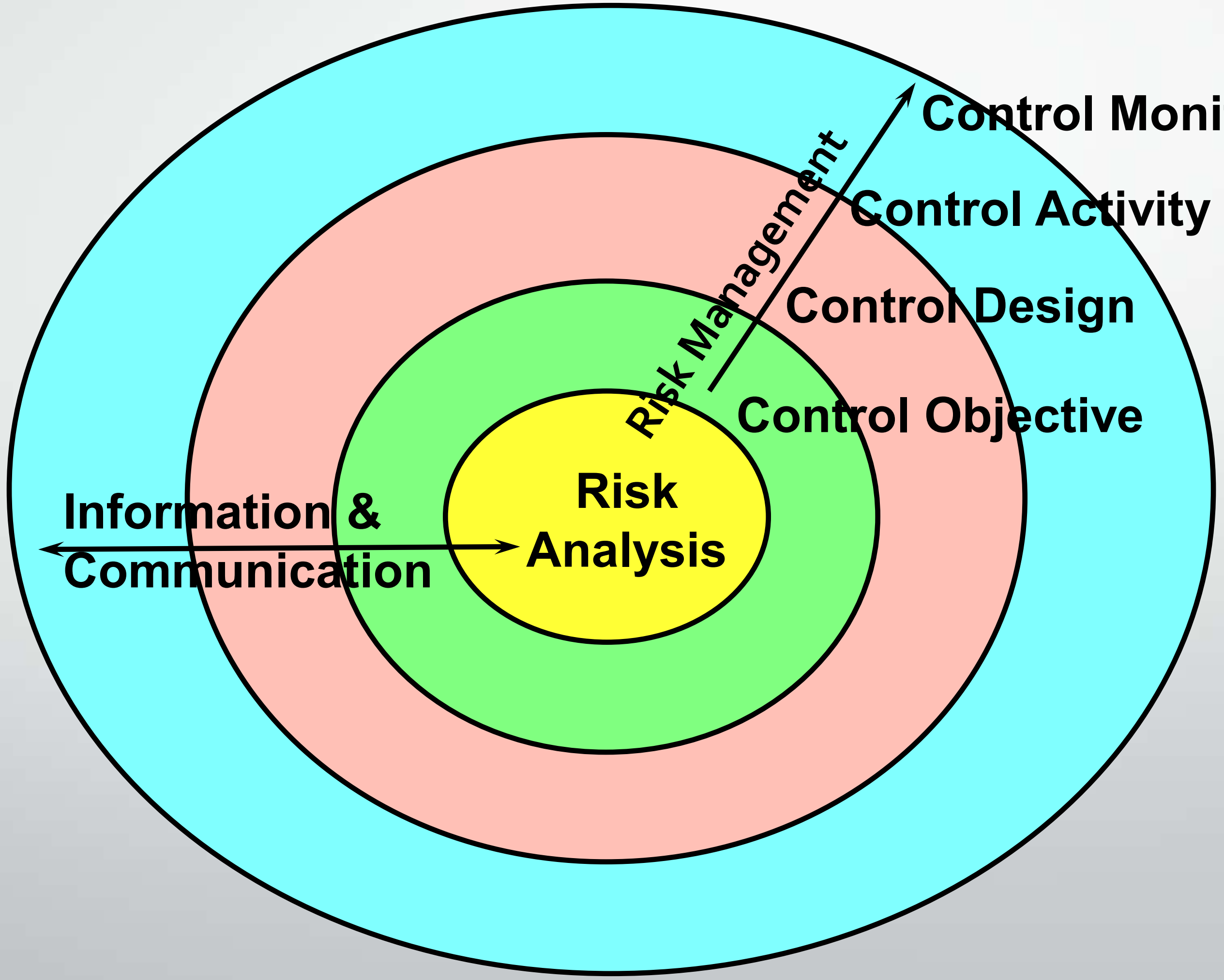
What Were Our Concerns?

- Physical access
- Program manipulation
- Data manipulation
- Logical access
- Real-time update
- People management
- Outsourcing
- Expert systems
- The Cloud
- Artificial intelligence

- Prevention
- Detection
- Correction / Reaction

- Processes
- Management

The Control Environment

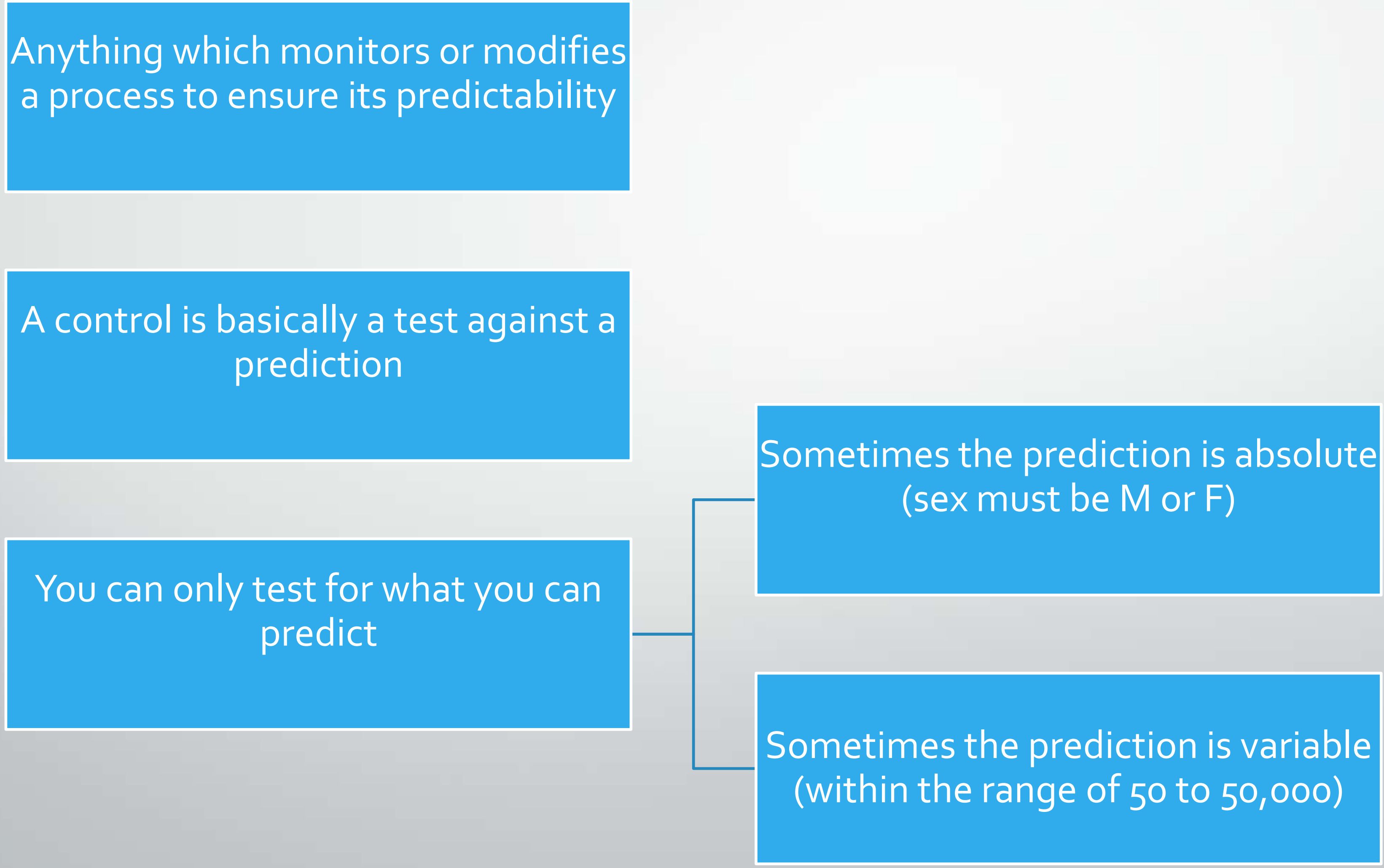


What Control(s) Should We Use?
(Control Classification)

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

What Is This Control Stuff?



Anything which monitors or modifies a process to ensure its predictability

A control is basically a test against a prediction

You can only test for what you can predict

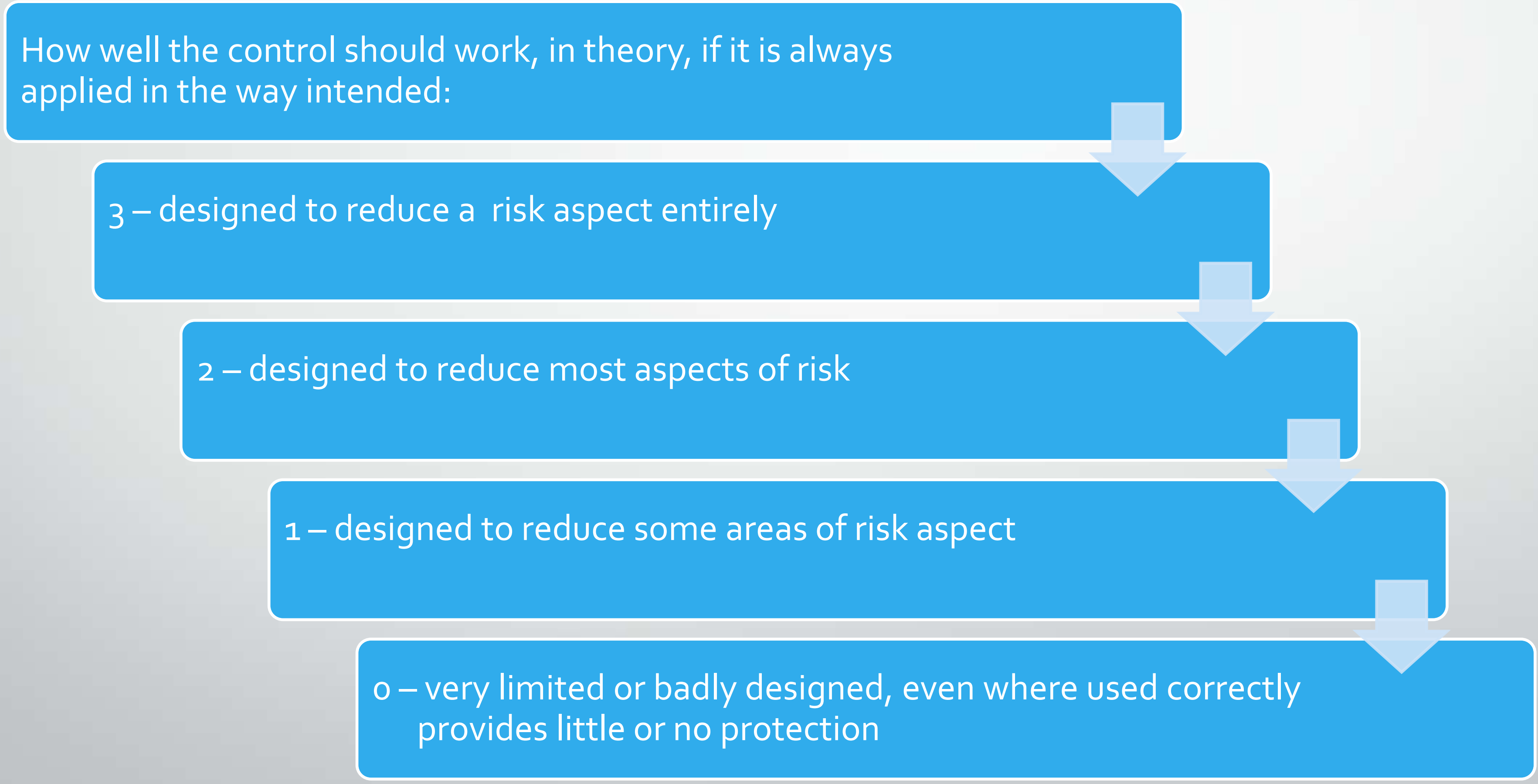
Sometimes the prediction is absolute (sex must be M or F)

Sometimes the prediction is variable (within the range of 50 to 50,000)

Anatomy of a Control (DIME)

- Design
- Implementation
- Monitoring
- Evaluation

Measuring Control Design



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

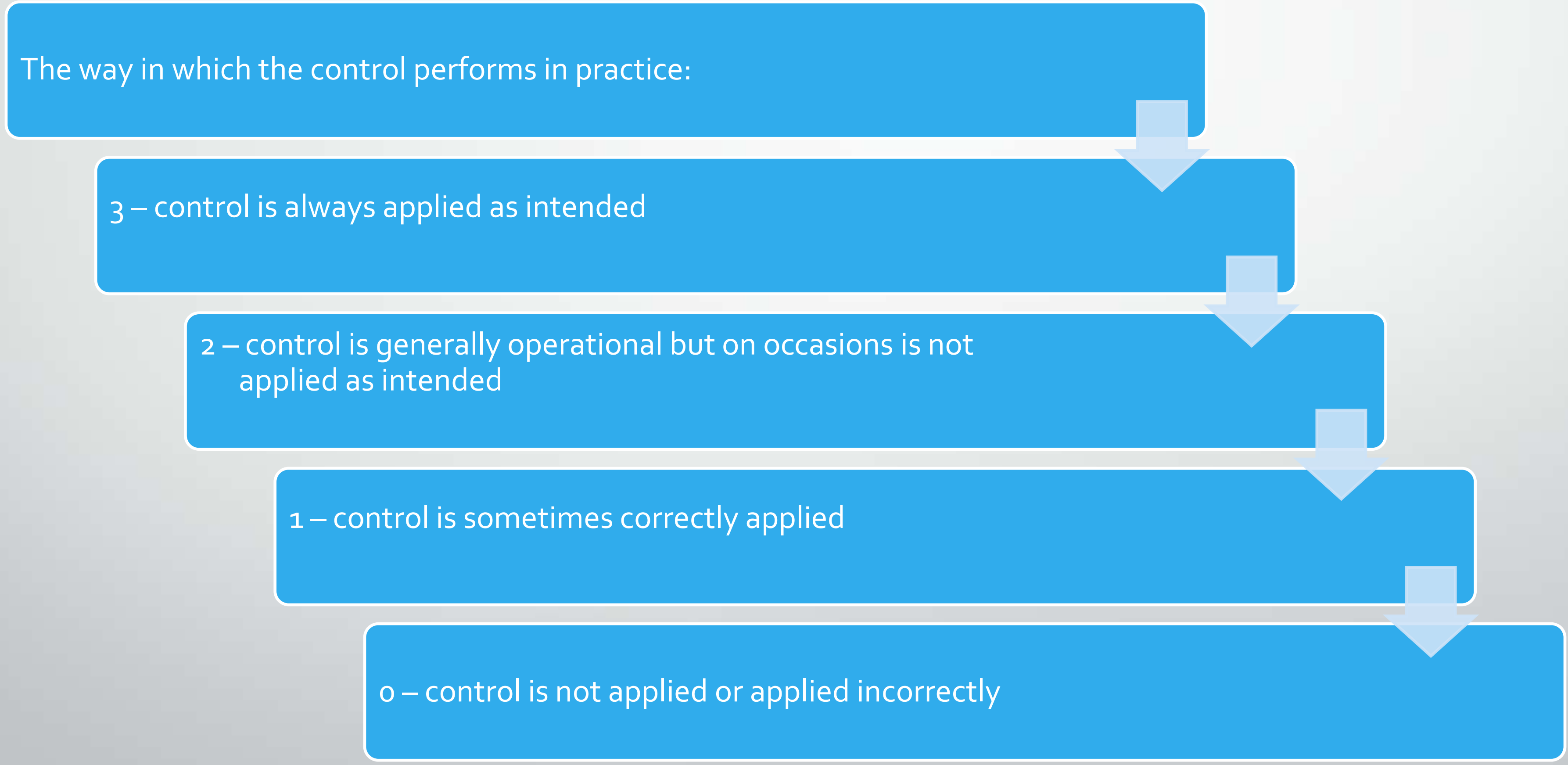
3 – designed to reduce a risk aspect entirely

2 – designed to reduce most aspects of risk

1 – designed to reduce some areas of risk aspect

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

Measuring Control Implementation



The way in which the control performs in practice:

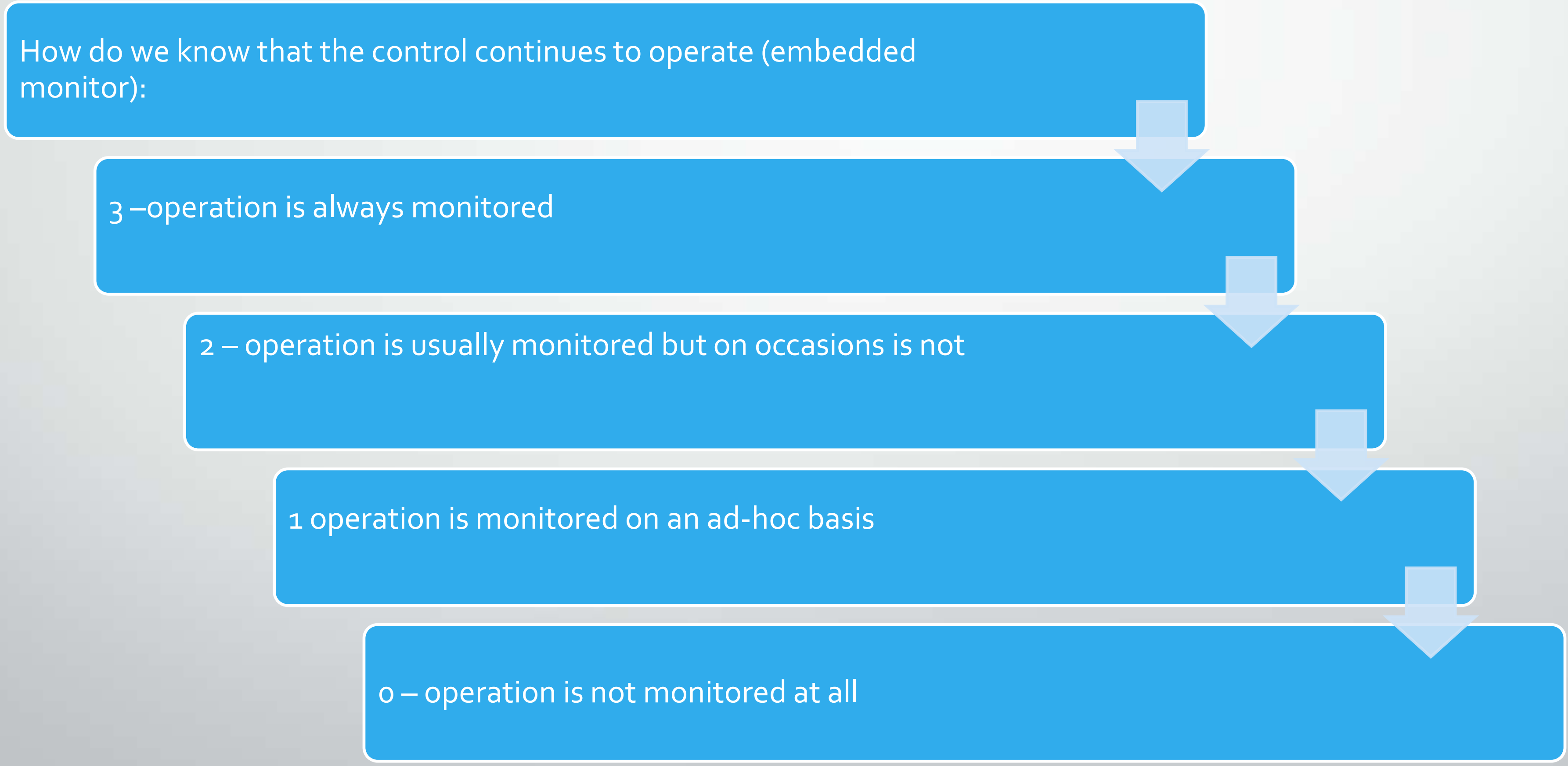
3 – control is always applied as intended

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

1 – control is sometimes correctly applied

0 – control is not applied or applied incorrectly

Measuring Control Monitoring



How do we know that the control continues to operate (embedded monitor):

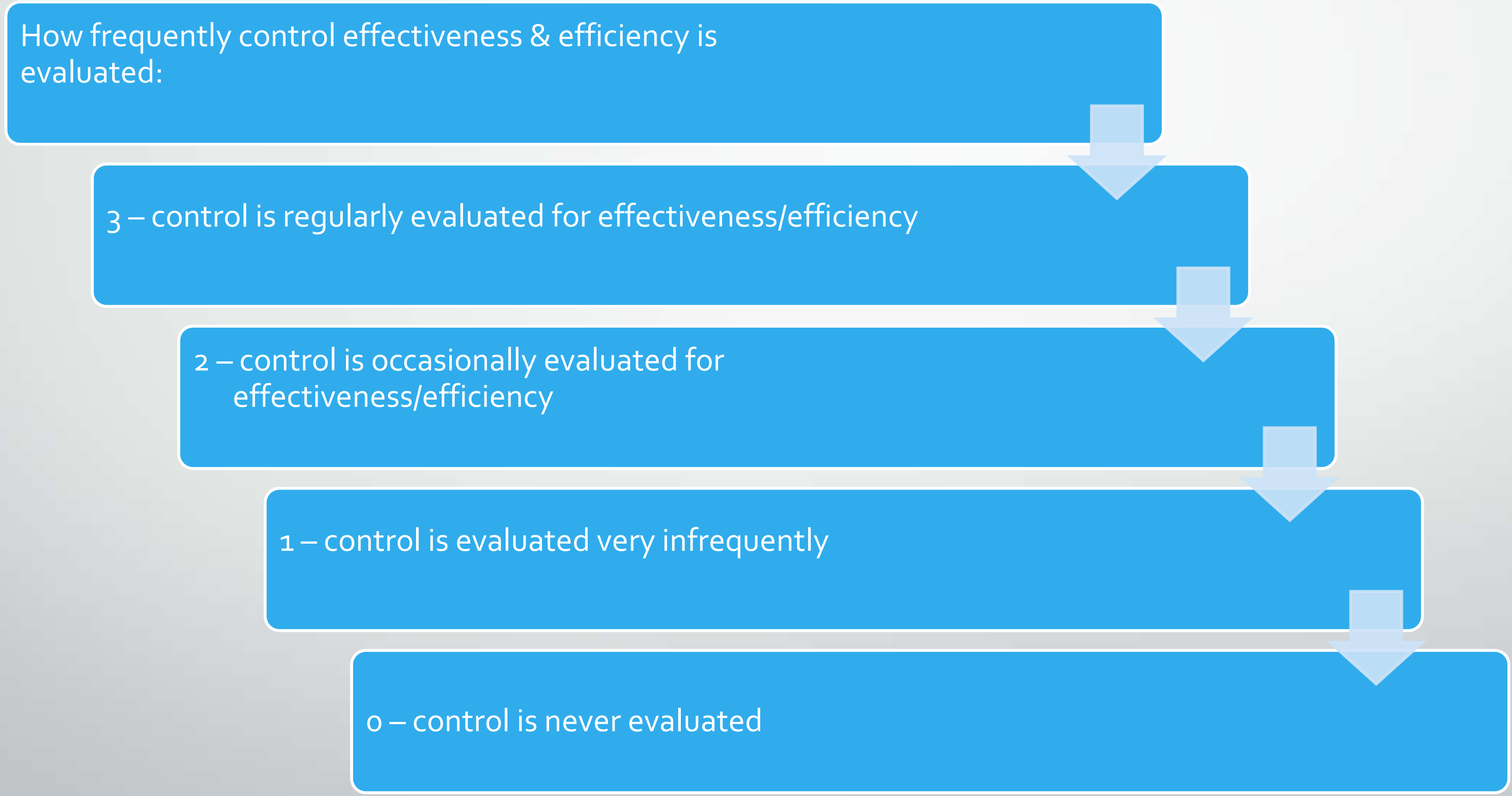
3 –operation is always monitored

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

Measuring Control Evaluation



How frequently 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 very infrequently

0 – control is never evaluated

Scoring Control Effectiveness Example (No Weighting of Elements)

- Apply DIME:
  - Design = 2 (3)
  - Implementation = 3 (3)
  - Monitoring = 2 (3)
  - Evaluation = 1 (3)

TOTAL = 8 (12) = 0.75 (75% total effectiveness)

NOTE: If either Design, or Implementation is zero then total score becomes zero

Expert Systems v Artificial Intelligence

Expert Systems (1990)

Captures expert knowledge

Takes a long time

May be no expert consensus

Power efficient

Artificial Intelligence

Neither artificial nor intelligent

General/Specific/Generative

Mines the internet

Machine learning

Answer limited to what is available

Power hungry

What Do I Want From AI?

Risk Selection
(Which Risk Should We Review?

Inherent Risk	Controls In Operation	Residual Risk
Risk 1	None	🟥
Risk 2	Some	🟨
Risk 3	Lots	🟩

Company:

Division:

Location:

RISK & CONTROL RECORDING

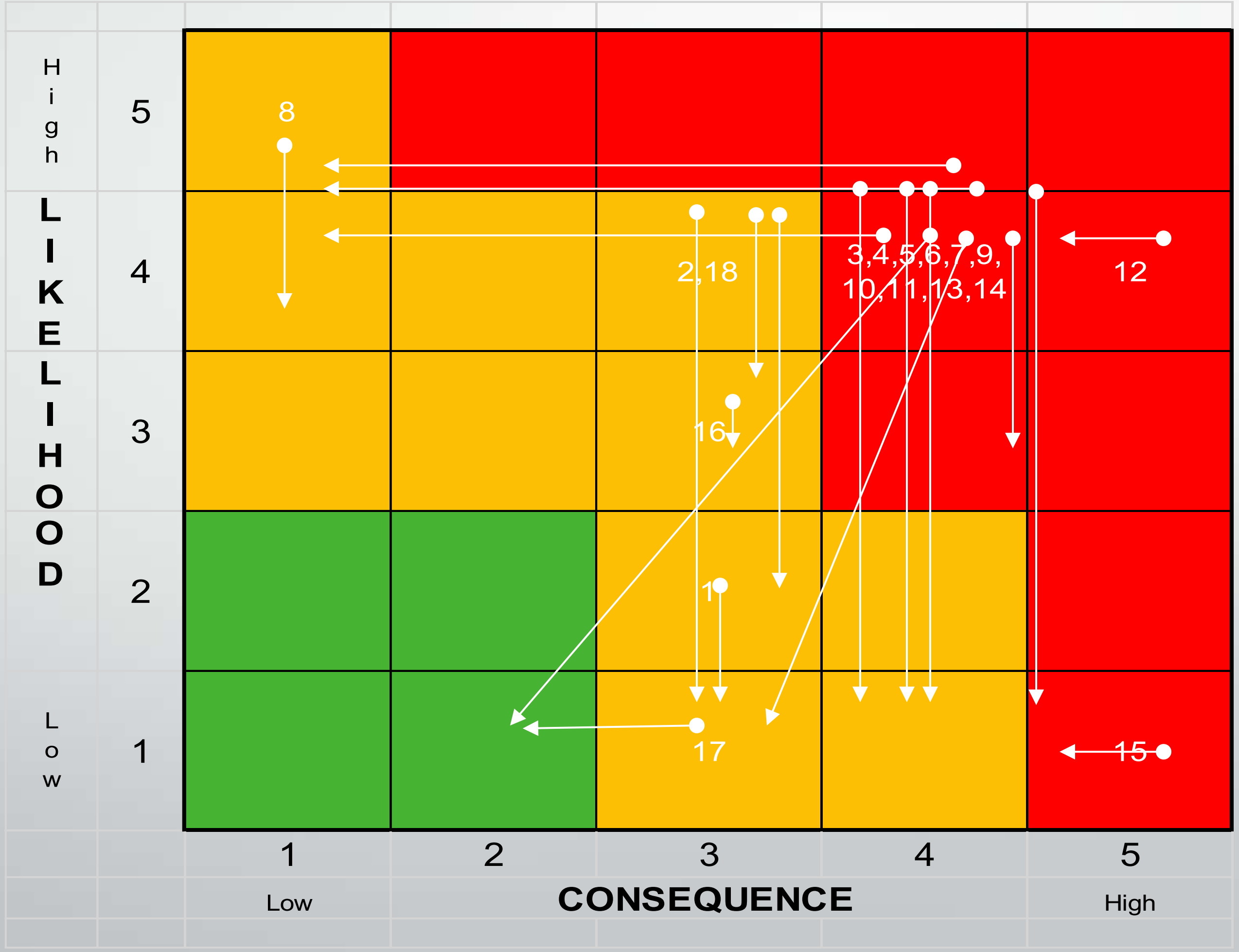
Business Area/Activity:		Score the Effectiveness of the Controls in Mitigating the Risk					
		N/A	1	2	3	4	5
A	Controls for managing the risk of						

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				
	1) Control 1								
	2) Control 2								
	3) Control 3								
	4) Control 4								

C	<u>Where the answer to a minimum requirement is NO:</u> 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	<u>Where the score for control effectiveness is < 3</u> Please detail the control which is to be implemented to improve the result	Class	Proposed Implementation Date	Pot. Score	Who/what will perform it?	How Often?	How will it be evidenced?

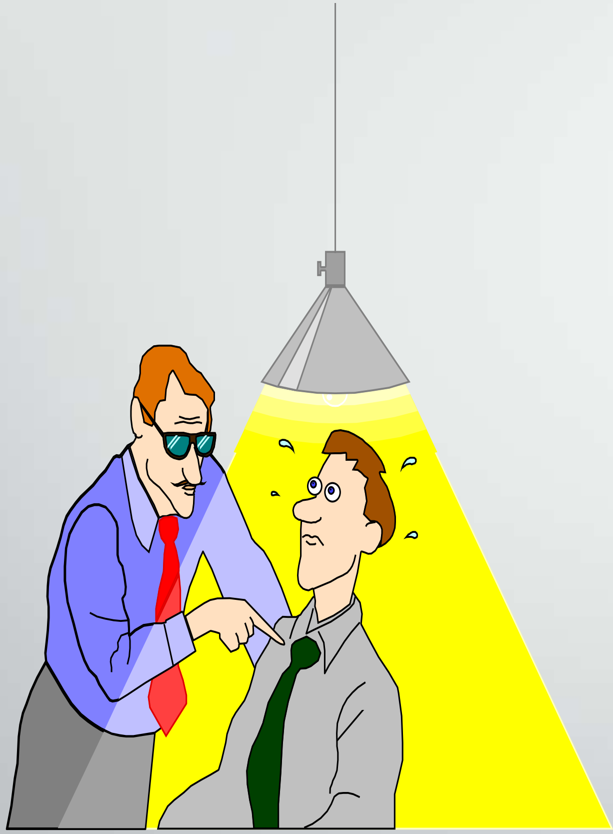
Risk Visualisation



Summary
(What I Want From AI)

- ⚠ Inherent Risk Identification
- Control Identification
- Control Measurement
- ✓ Residual Risk Scoring
- Evidence Recording
- Opinion
- Visualisation

Satisfactory, because ………
Satisfactory, except for ……..
Unsatisfactory, because ……



John Mitchell
PhD, MBA, CEng, CITP, FBCS, CFIIA, CIA, 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