



Information Risk Management
and Assurance Specialist Group



Business Change
Specialist Group

Measuring Control Effectiveness

25th February 2020

John Mitchell

PhD, MBA, CEng, CITP, FBSC, 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

John Mitchell

Career

- Data controller
- Operator
- Programmer
- System's analyst
- Business analyst
- Project Manager
- CIO
- Computer auditor
- IT governance specialist
- CEO own company

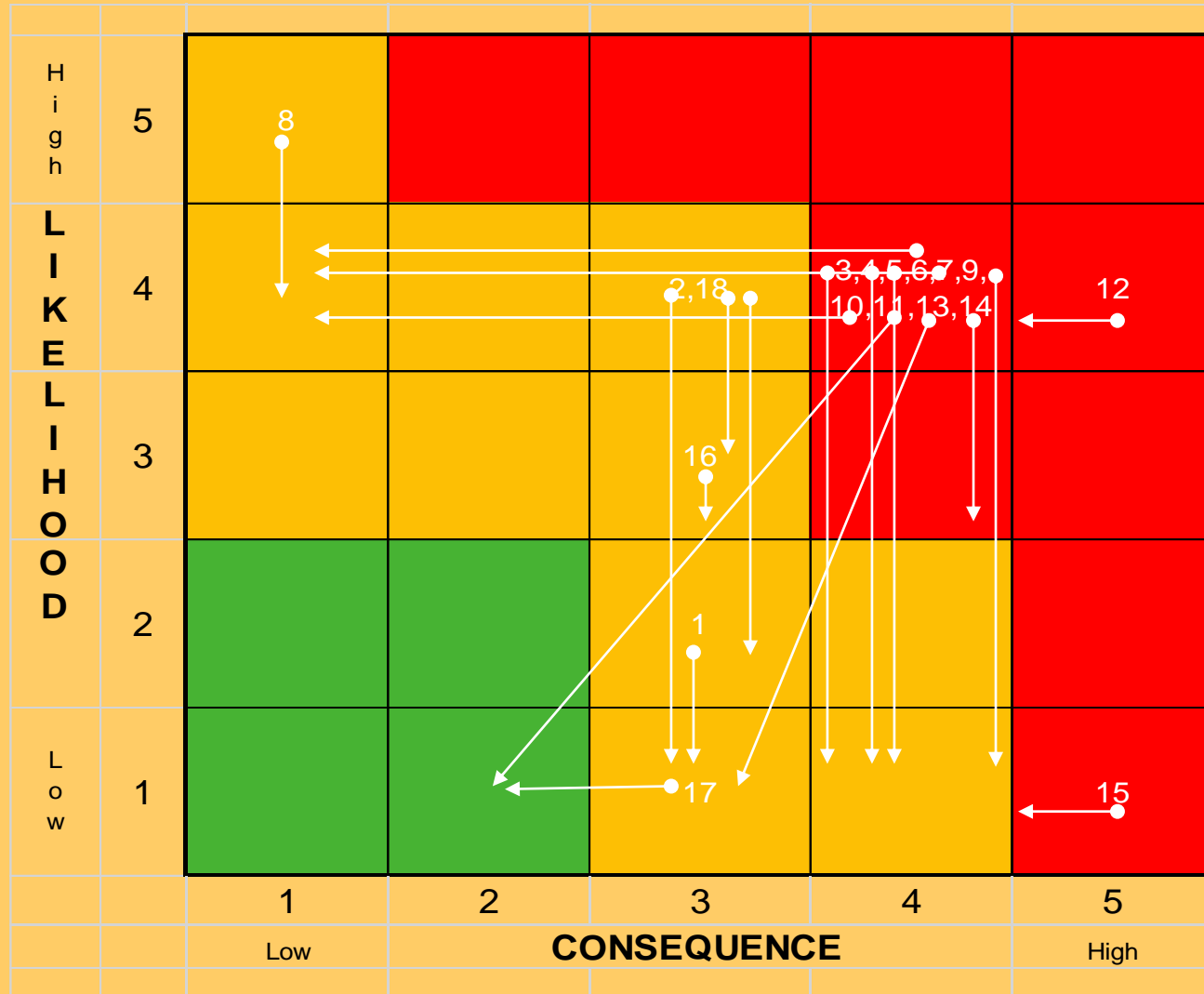
Certifications

- PhD
- MBA
- FBCS
- CITP
- CIA
- CISA
- CGEIT
- CFIIA
- QiCA
- CFE



LHS

Why Are We Here Today?



Some Assumptions



YOU UNDERSTAND THE
CONTROL ENVIRONMENT



YOU UNDERSTAND RISK
MANAGEMENT



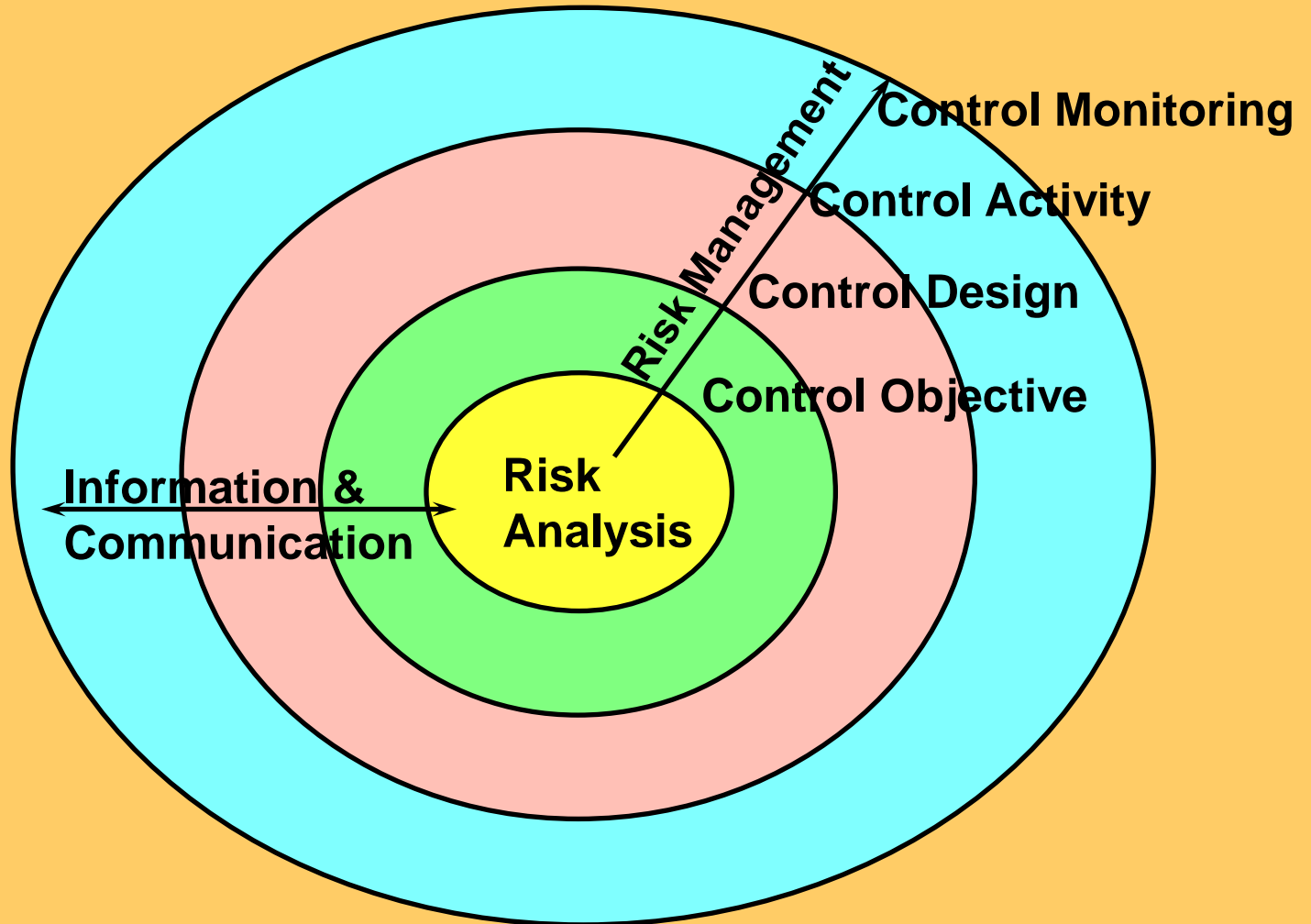
YOU CAN DEFINE WHAT A
CONTROL IS AND HOW IT
WORKS

LHS

Which Risk Should You Audit?

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

Components of the Control Environment



What Is Control?

Control Definition

- Anything which monitors, or modifies, the behaviour of a system component, to ensure its operational predictability

How Do They Work?

- They test against an expected result
 - Gender must be 'M' or 'F'
 - Range must be +1 to +999
 - Only numerics permitted

LHS

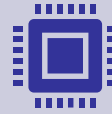
Controls Are Needed For ...



ACCESS



DATA
QUALITY



PROCESSING



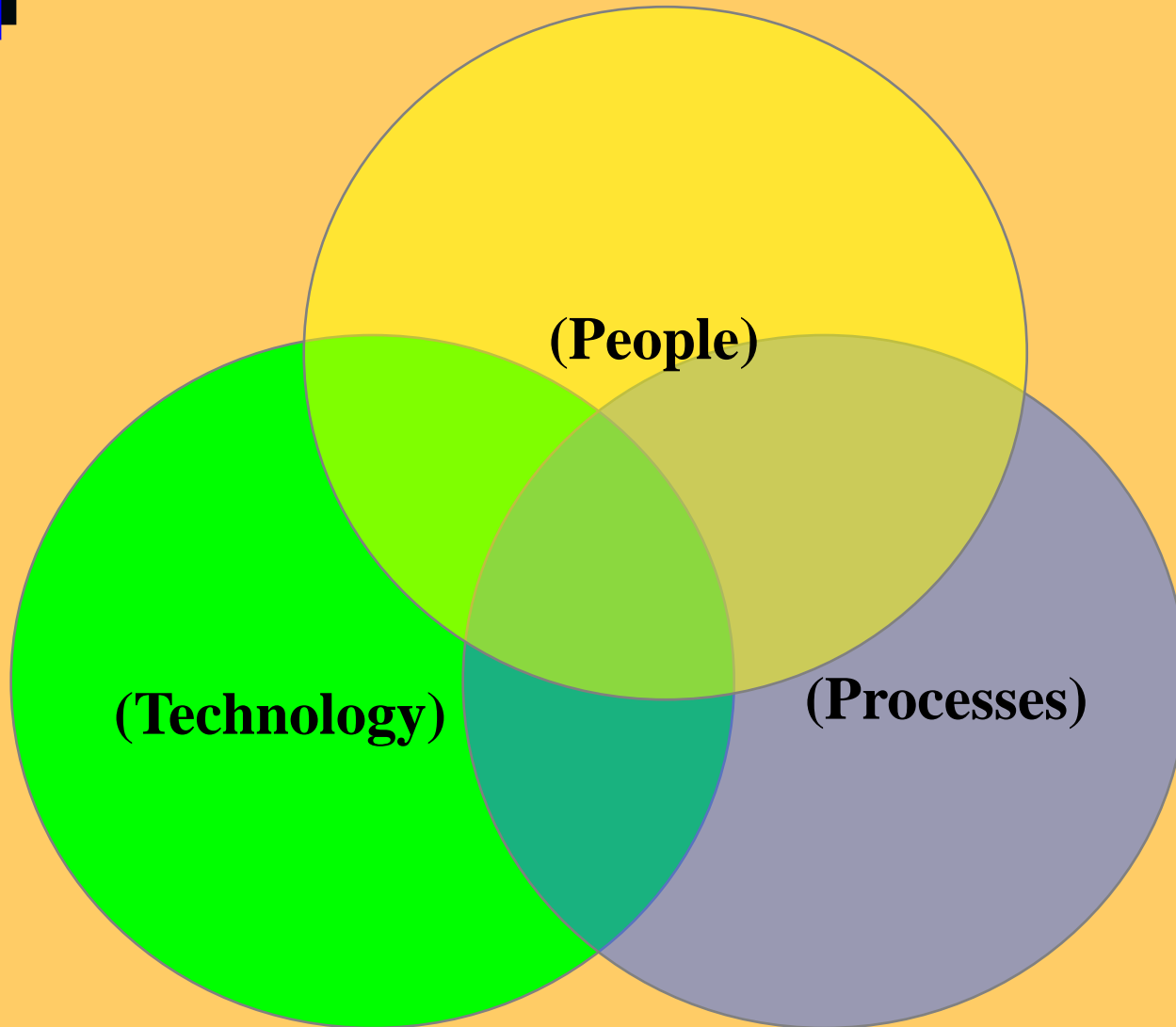
AVAILABILITY



COMPLIANCE

LHS

Control May Exist In



Basic Control Types

Preventive

- Stops the bad thing happening

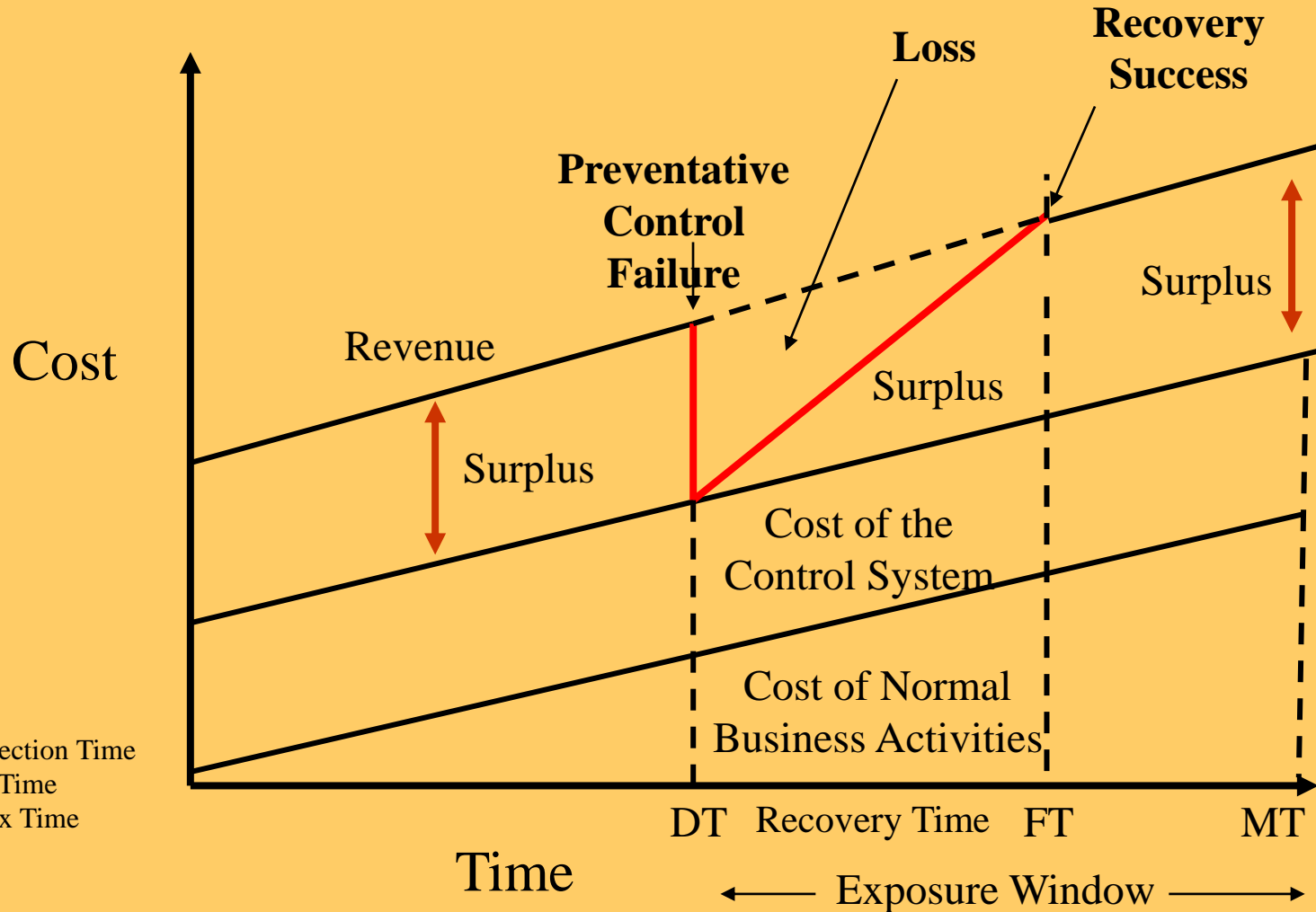
Detective

- Identifies that a bad thing has happened

Reactive (Corrective)

- Fixes the damage caused by the bad thing

Impact of Preventative Control Failure



Control Types - Classified

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	
3	Detects the event and reacts just fast enough to fix it within the specified time window	Detective
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

Control Hierarchy

Control objective

- What the control is meant to achieve

Control design

- How the control will work

Control activity

- The control in operation

Control monitoring

- How do we know that the control is (still) effectively working?

Example

Control objective

- Only 'correct gender is accepted

Control design

- Incoming transaction field is compared against a table

Control activity

- Only transactions containing 'M' or 'F' allowed to next stage

Control monitoring

- Run a CAAT to detect any non 'M' or 'F'

LHS

Anatomy of a Control

- Design
- Implementation
- Monitoring
- Evaluation

(DIME)



Control Design

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

4) – designed to reduce a risk aspect entirely
(either likelihood and/or impact)

3) – designed to reduce most of a risk aspect

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

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

Control Implementation

- The way in which the control is implemented and performs in practice:

4) – the control is always applied as intended

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

2) – the control is sometimes correctly applied

1) – the control is not applied or is applied incorrectly

Control Monitoring

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

4) – operation is always monitored

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

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

1) – operation is not monitored at all

Control Evaluation

- How frequently the control effectiveness & efficiency is re-evaluated:

4) – control is regularly re-evaluated for effectiveness/efficiency

3) – control is occasionally re-evaluated for effectiveness/efficiency

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

1) – control is never re-evaluated

Control Design Example

- Control Objective
 - Only the correct gender is accepted
- Risk
 - Incorrect gender is accepted into the system
- Control Type
 - Preventive
- Control Implementation
 - The entered gender is validated by program logic
 - Only 'M' or 'F' is accepted
 - Incorrect entry results in an error message & the input is not further processed

Scoring Control Effectiveness (Simple Model – No Weights)

- Apply DIME:

- Design = 3 (4)

- Implementation = 4 (4)

- Monitoring = 2 (4)

- Evaluation = 1 (4)

- TOTAL SCORE = 10 (16) = 62.50%

- or **62% total effectiveness**

Scoring Control Effectiveness (Weighted Model)

- Apply DIME:
 - Design (x3) = 9 (12)
 - Implementation (x3) = 12 (12)
 - Monitoring (x2) = 4 (8)
 - Evaluation (x1) = 1 (4)

 - TOTAL SCORE = 26 (36) = 72.22%
 - or **72% total effectiveness**

LHS

Weighted v Unweighted Model



Unweighted

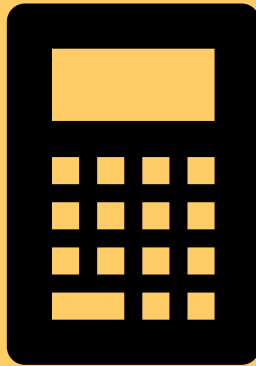
62% effective in managing risk of incorrect input



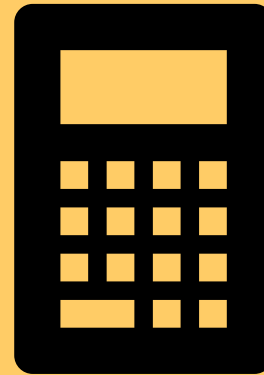
Weighted

72% effective in managing risk of incorrect input

Control Effectiveness Calculation Examples



Key Logger Detection



Ghost Employee Prevention

Control Documentation Hierarchy



Risk & Control Documentation

Company: _____
 Division: _____
 Location: _____

Business Area/Activity: _____

A		Score the Effectiveness of the Controls in Mitigating the Risk					
		N/A	1	2	3	4	5
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	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?

From RR

From Control Classification

From Control Spreadsheet

Determines Length of Control Line

Based on Control Scores

From Control Specification

Risk Register

Development Risk Register.xls - Compatibility Mode - 21/05/2019

File Home Insert Page Layout Formulas Data Review View Help Search

Clipboard Font Alignment Number Styles Cells Editing Ideas




R5

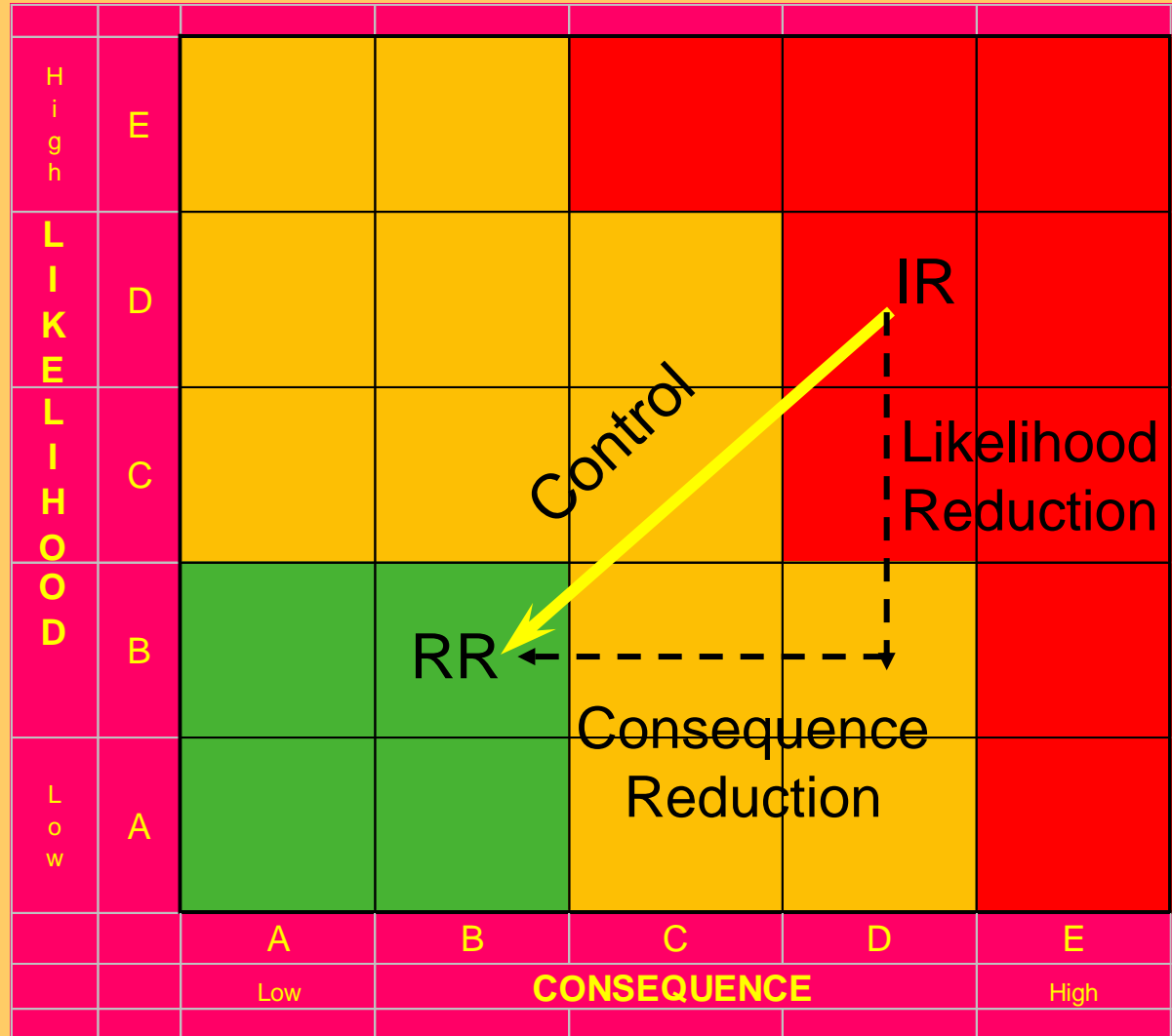
RISK REFERENCE	RISK DESCRIPTION	Risk Cause Ref.	RISK CAUSE DESCRIPTION (How the risk could arise - the event)	RISK CAUSE OWNER	INHERENT RISK SCORE (No Control)			ACTION DECISION Control, Mitigate, Transfer, Avoid, Exploit, Tolerate	CURRENT ACTIONS (What we are currently doing to manage the risk - required for every decision other than tolerate) Format: Who, What action, How frequent, How evidenced	Control Effectiveness		RESIDUAL RISK SCORE (With Control)		EMBEDDED MONITOR (How we know that we are successfully managing the risk) Format: Describe what is being measured or tracked.
					Impact	Probability	Matrix Zone			Design	Performance	Impact	Probability	
		DV-1	Business processes not aligned with divisions	Business	B	4	O	Control	Business			B	4	O
DV-1	Inappropriate business solution provided	DV-2	Incorrect or unclear specifications	GC	B	4	O	Control	The Change Control standards in force will ensure that all user requirements are thoroughly discussed, agreed and signed off before development commences. There are three levels of testing are conducted, the last by the end user before the system is made live. A comprehensive Change Control system that ensure all changes are migrated correctly. A Change control facility			A	1	G
		DV-3	Use of leading edge technology	RAA	C	4	R	Control	Refer to IT Strategy Paper			A	1	G
		DV-4	Scope creep	GC	B	4	O	Control	Walkthrough / Impact analysis / Change Control, Project Procedures.			A	1	G
		DV-5	Time overruns	GC	B	4	O	Control	Walkthrough / Impact analysis / Change Control, Project Procedures.			A	2	G
		DV-6	Budget overruns - Projects only	RAA	B	4	O	Control	Project Manager control			A	1	G
		Business solution not provided within												

Header Sheet | Change History | **Development Risk Register** | Risk Matrix | Documentation

13:54 21/05/2019

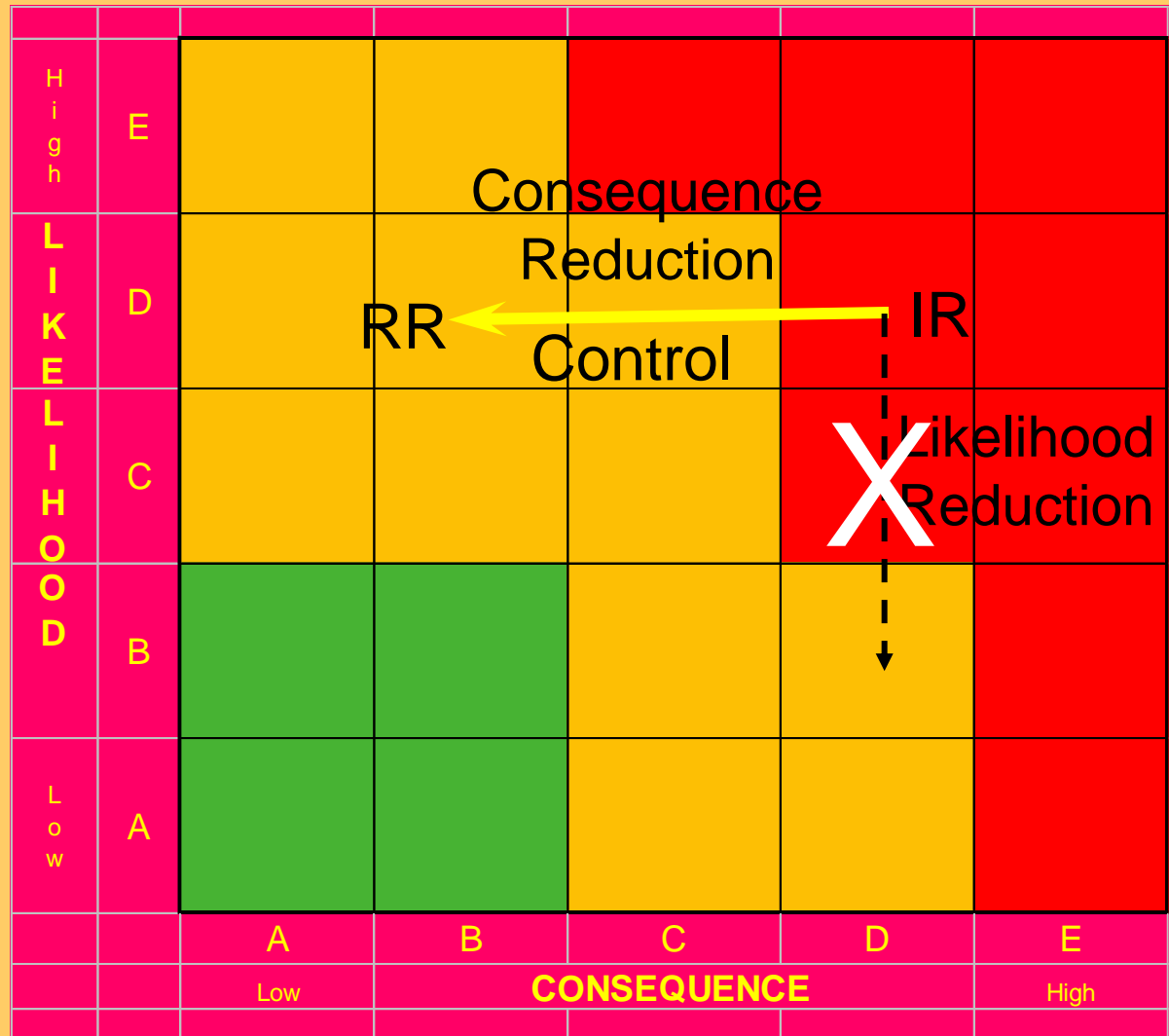
Theoretical Risk Management Model

-  Senior Management Attention
-  Local Management Attention
-  No Action



Risk Model Without Likelihood Mitigation

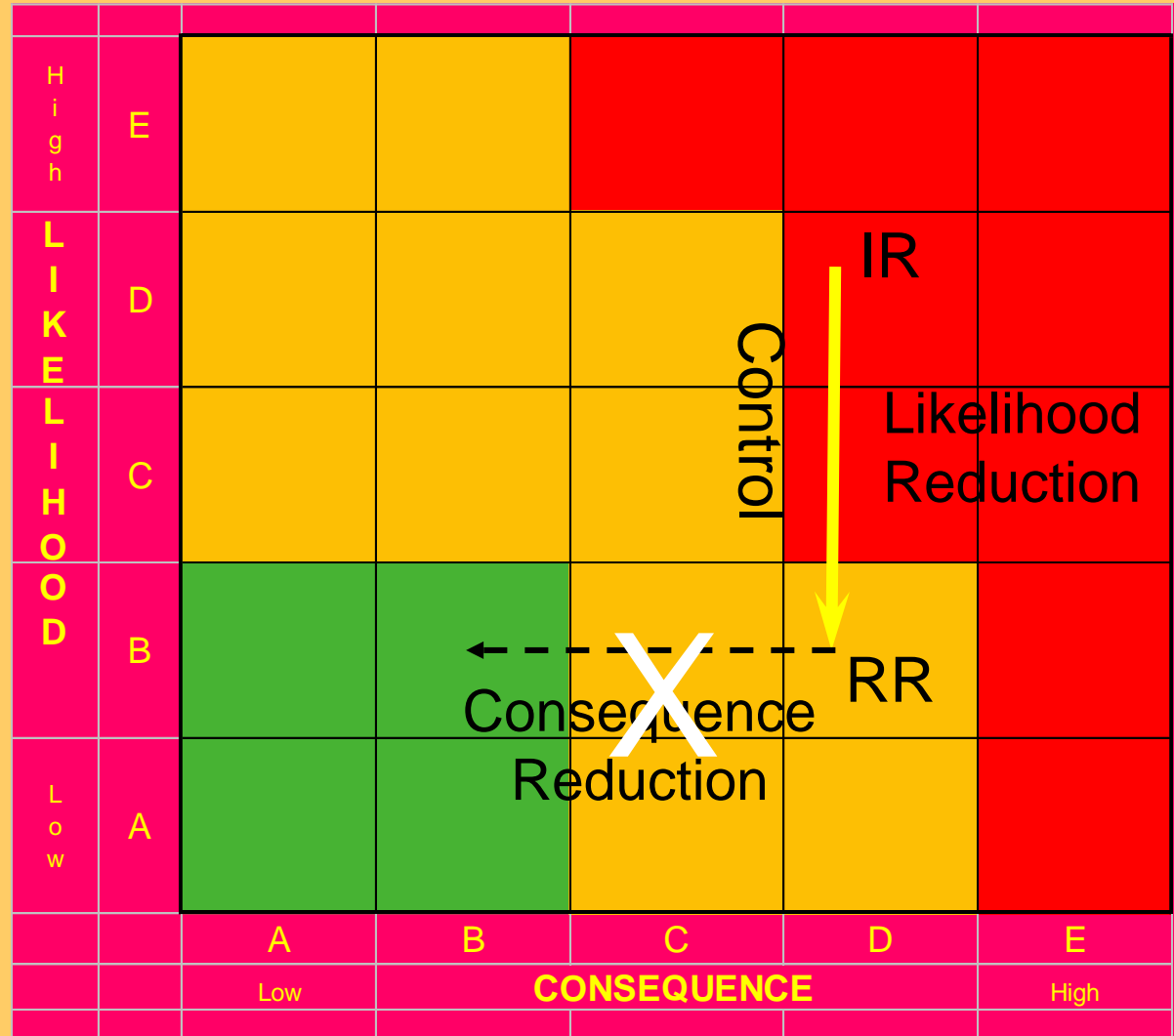
- Senior Management Attention
- Local Management Attention
- No Action



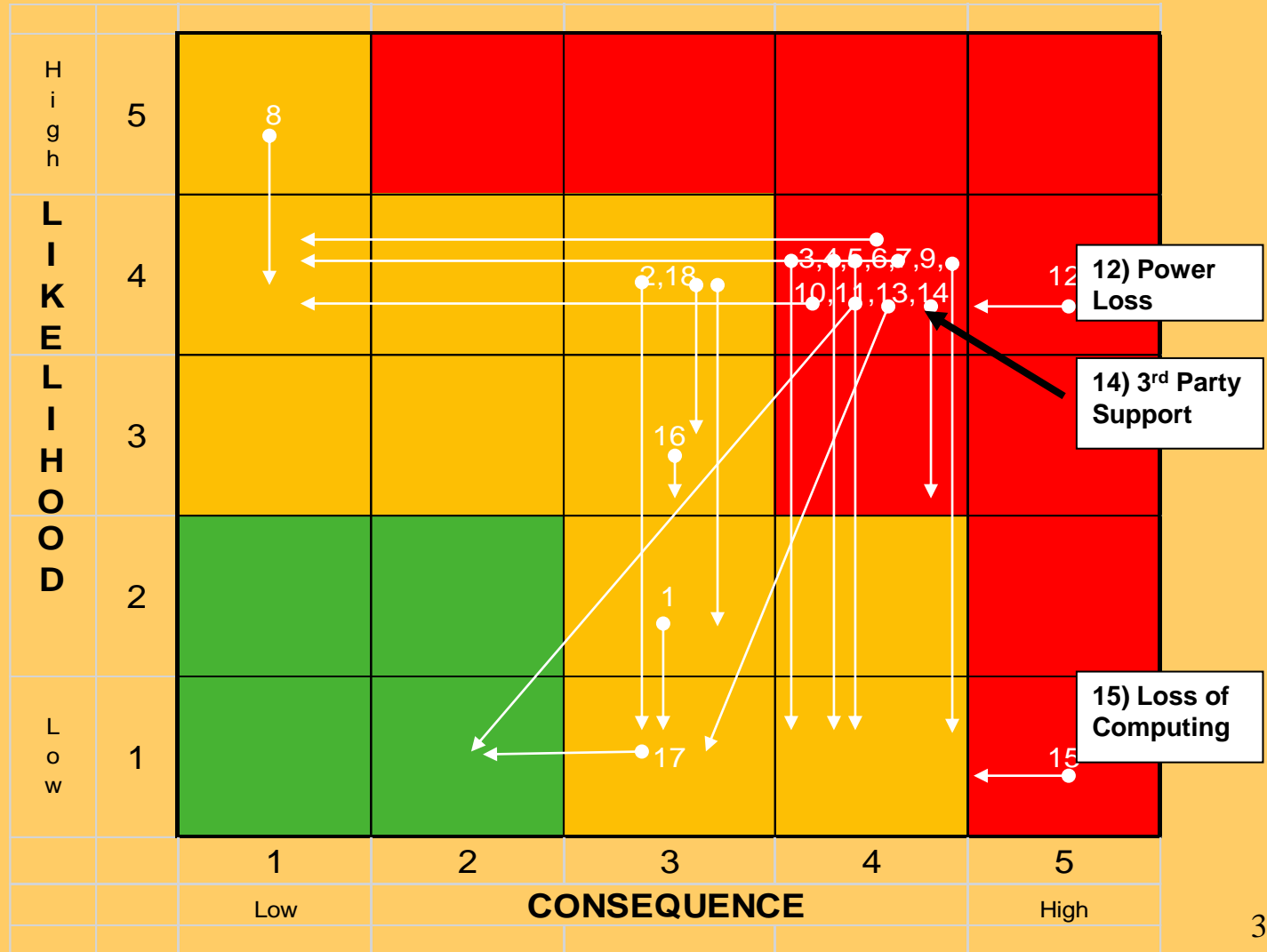
LHS

Risk Model Without Consequence Mitigation

- Senior Management Attention
- Local Management Attention
- No Action



Risk/Control Visualisation



Where Should Controls Be Referenced?

Requirements specification

- Statement – “The app/system/process must be suitably controlled to ensure predictability”

Design specification

- Data quality rules
- Confidentiality rules
- Integrity rules
- Availability rules
- Compliance rules

Testing specification

- How each control will be tested

Significant Changes In The Control Paradigm (1960s to date)

- **Single batch program**

- Batch multi-tasking
- On-line retrieval

- **Networking**

- Stand alone PCs

- **Real-time update**

- File servers & distributed processing

- **Internet**

- Palm devices
- Phone devices
- BYOD

- **Cloud computing**

- 3D printing
- Specific Artificial Intelligence

- **Expert Systems (AI)**

LHS

Which Would You Choose?



One Engine – Can Fly On One



Two Engines – Can Fly On One



Four Engines – Can Fly On One



Eight Engines – Can Fly On Two

Summary



Data quality rules and other control requirements should form a separate section of the requirements, design & testing specifications



Controls should be specified/documented using DIME:

Control objective

Control design

Control implementation

Control monitoring

Control evaluation



Most single controls are less than 75% effective in completely managing either likelihood, or consequence

The logo consists of the letters 'LHS' in a bold, black, serif font, enclosed within a white square with a blue border.

Questions?

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

