Risk Management and its application to an E-Commerce Environment

John Mitchell

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

Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Mobile: 07774 145638
john@lhscontrol.com
www.lhscontrol.com

LHS

Themes

- Risk components
- Roots causes
- Moving from inherent to retained
- Case study - e-commerce availability

LHS

Attributes of Modern Computer Systems

- Remote Access
- Logical Access Control
- Immediate update
- No human intervention
- Invisible

LHS

Risk

EVENT
leading to a
CONSEQUENCE
resulting in an
IMPACT
on a business objective

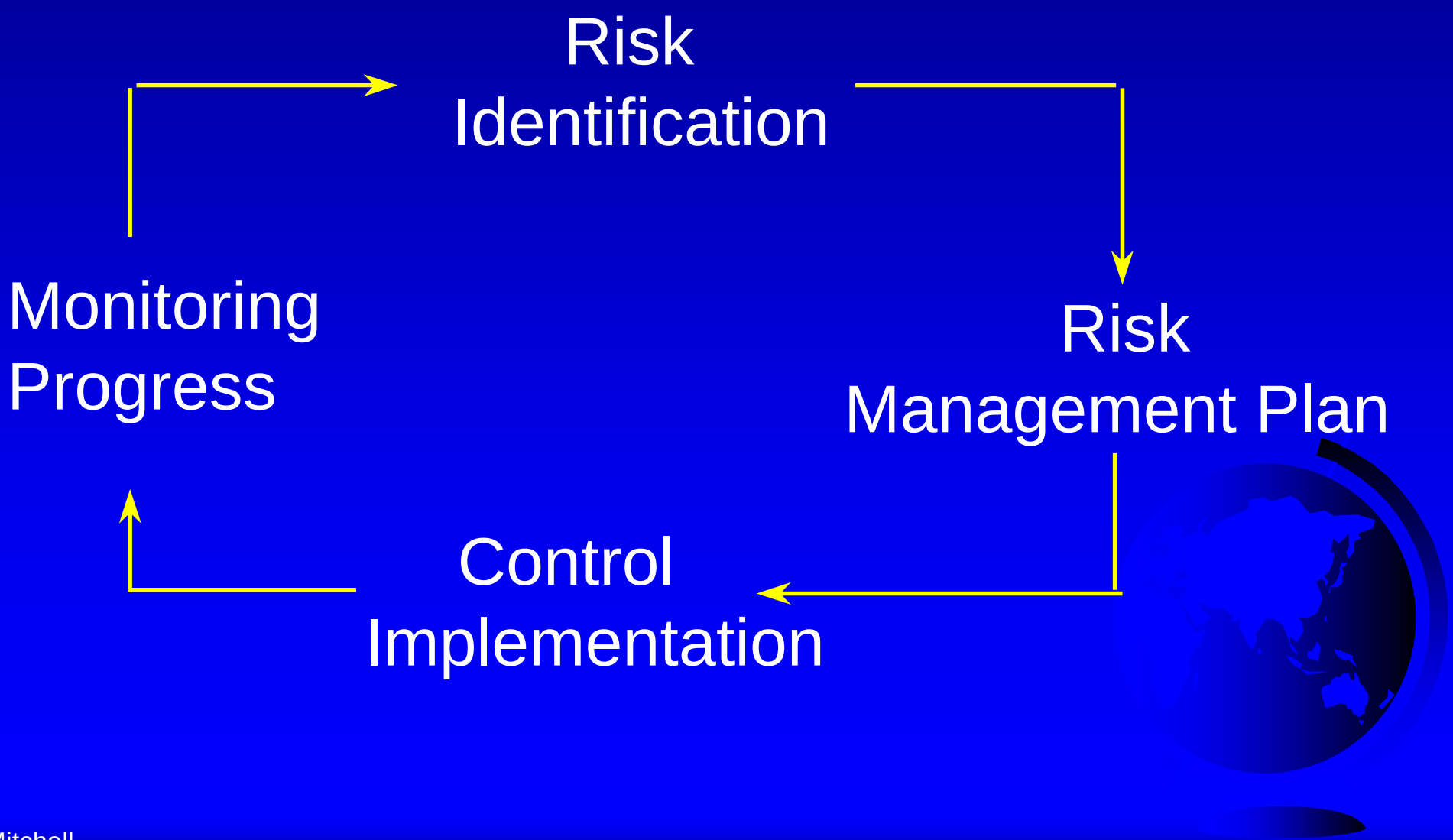
LHS

Example

EVENT (loss of power)
leading to a
CONSEQUENCE (non-availability)
resulting in an
IMPACT (loss of orders)
on a business objective (make sales)

LHS

Risk Management Process

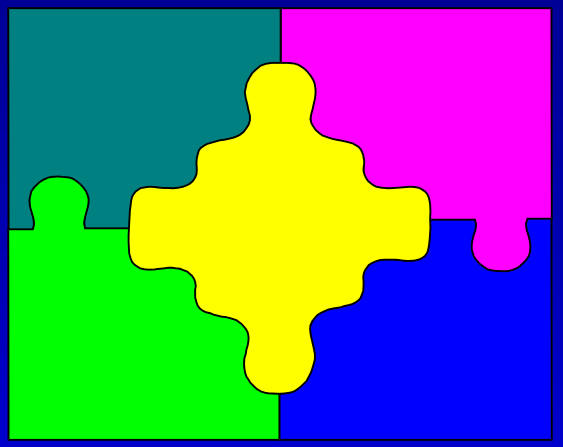


LHS

Risk Management

LHS

Components of Risk



- Inherent Risk
  - ⇨ The starting point
- Residual risk
  - ⇨ Where you end up after doing something
- Retained Risk
  - ⇨ What you formally decide to live with
  - ⇨ Often the same as the residual risk

LHS

Inherent Risk

The likelihood and consequence of risk crystallisation before mitigating actions (controls) have been put in place

LHS

Residual Risk

The likelihood and consequence of risk crystallisation after mitigating actions (controls) have been put in place

LHS

Root Causes

- Those things that may trigger an outcome (such as non-availability)
  - Server failure
  - Inadequate disk capacity
  - Network failure
  - Inadequate bandwith
  - ISP failure
  - Power failure
  - Software failure

LHS

Lesson 1

A single outcome (e.g. non-availability) may be triggered by many different root causes

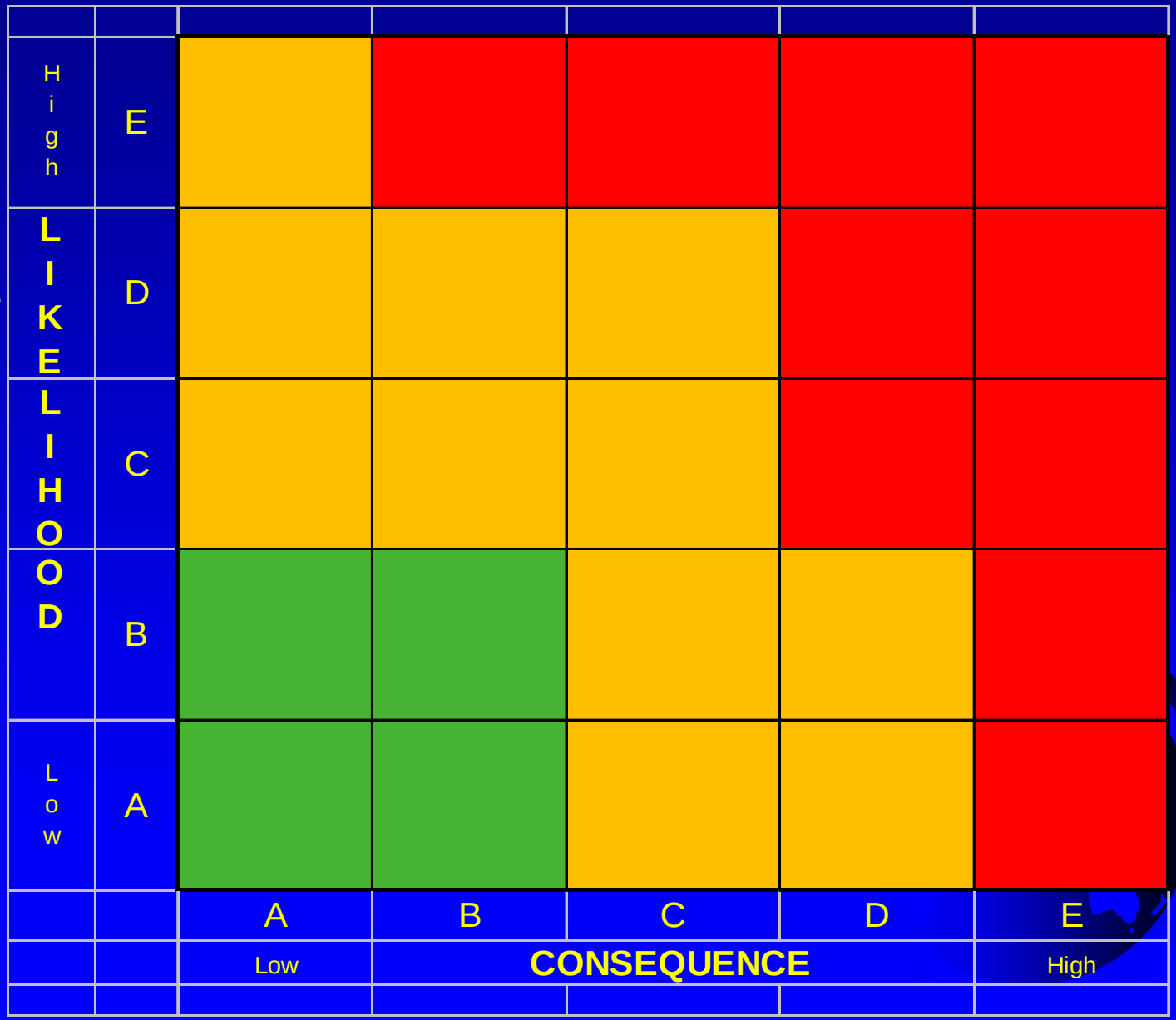
Risk Management Approach

- Determine business objectives
- Identify risks (events to impacts)
- Prioritise risks (inherent level)
- Identify event root causes (inherent lev
- Make a decision
- Identify potential controls
- Ascertain whether they are in operation
- Re-score risk (residual level)
- Agree remedial action plan (where necessary)

Mapping Likelihood & Consequence

LHS

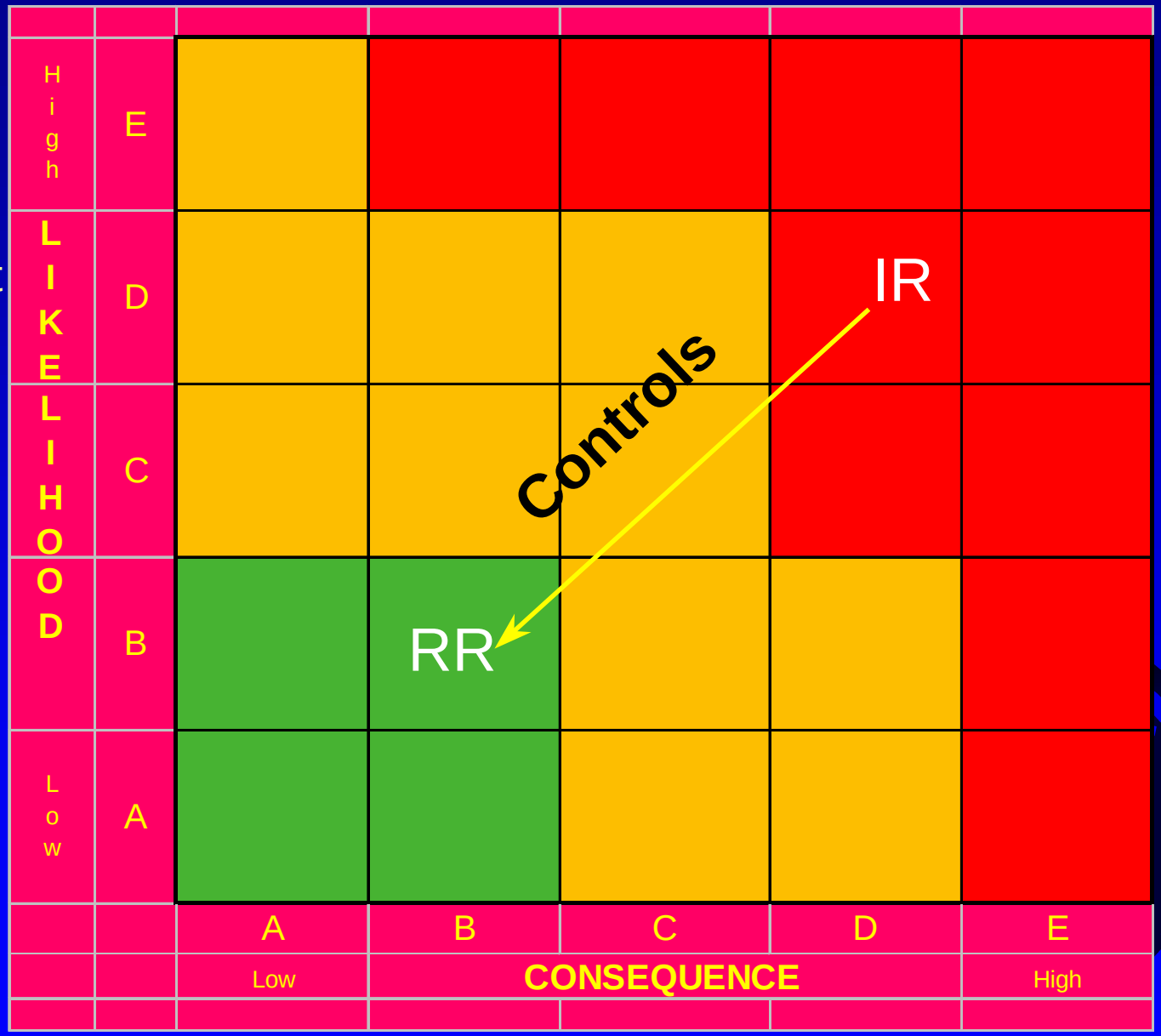
- Senior Management Attention
- Local Management Attention
- No Action



Moving from Inherent to Residual/Retained Risk

LHS

- Senior Management Attention
- Local Management Attention
- No Action

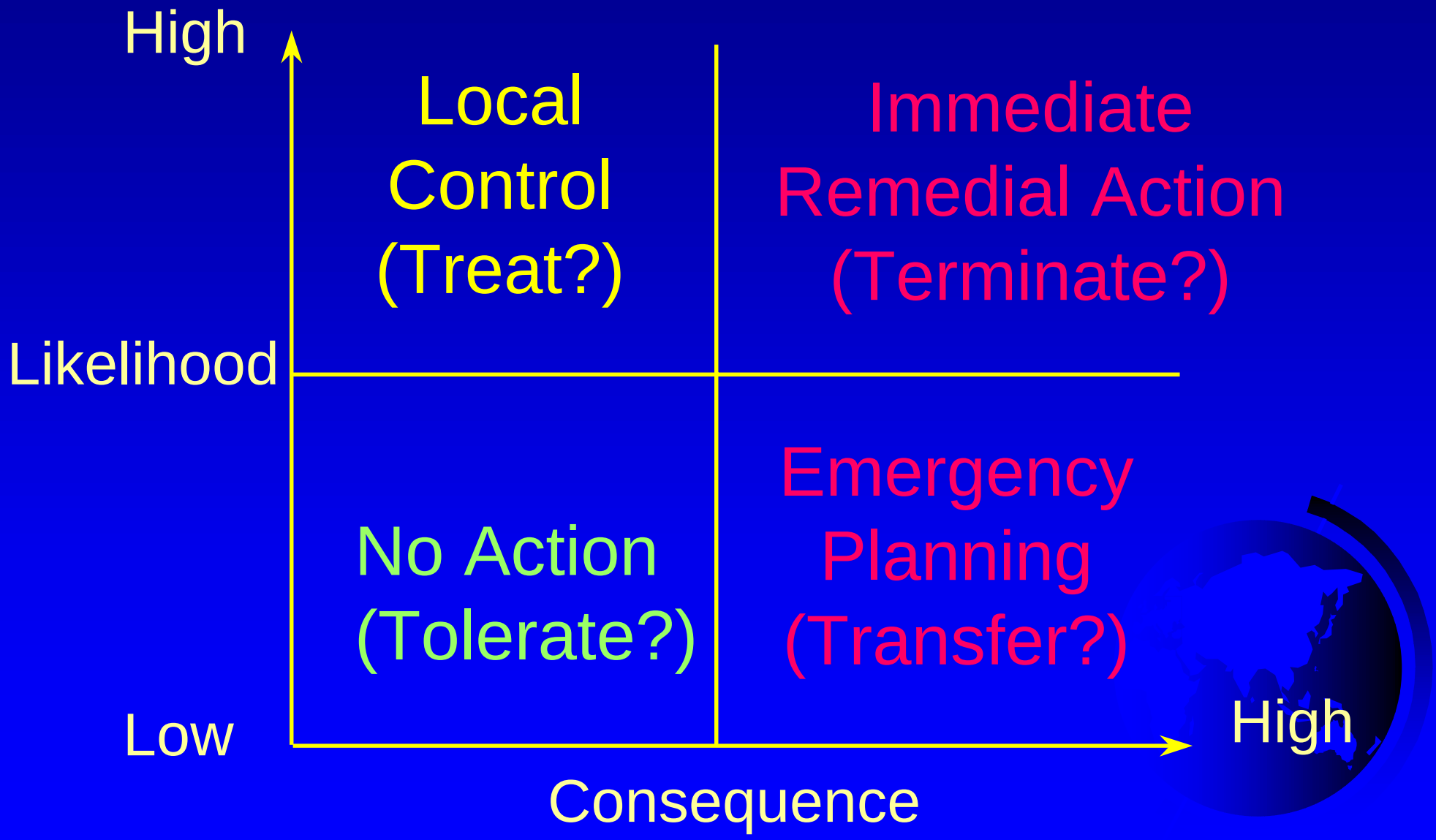


LHS

Handling Risk

LHS

Decision Matrix



LHS

Retained Risk

- The level of risk formally accepted by the organisation
- Usually the same as the residual risk
- Sometimes reduced (transferred) by insurance (but only the consequence)

LHS

Root Cause

- What really caused the problem?
  - Not, what is the symptom that I see
- Will this mitigating action reduce the likelihood, or the consequence?
  - It will only do one, or the other

A Case Study Based on E-Commerce Availability

LHS

The Problem

- Moving from an inward focussed to a customer facing outlook
- 600,000 customers world-wide
- Need for a high integrity, high availability system

LHS

Critical Success Factors

- Confidentiality of customer data
- Integrity of content presented to the customer
- Availability of system to the customer
- Compliance with statutory obligations

LHS

Availability CSF

Availability of the service to the customers when they require it

LHS

Key Goal Indicator

Availability never drops below 100% (unless planned)

LHS

Key Performance Indicators

- Available bandwidth
- Server availability
- Software integrity

LHS

Non-Availability Risks

- Customers are unable to access the system leading to them being unable to place orders resulting in loss of income
- Customers are unable to obtain help with non-availability problems leading to dissatisfaction with the company resulting in loss of customers

LHS

Non-Availability Root Causes

1) Failure of connectivity as a result of loading company recommended third-party software onto customer computers
2) Failure of connectivity as a result of loading company produced software onto customer computers
3) Failure of the company's internet connection
4) Company firewall prevents legitimate access
5) Company internal network failure
6) Key hardware failure
7) Key software failure

LHS

Non-Availability Root Causes

8) Customer forgets access information
9) Inadequate capacity
10) Hacking attack:
    a) Halts servers
    b) Halts network
11) Virus/worm infestation disrupts the system
12) Power loss
13) Failure of the back-up/restore process
14) Ineffective third-party support for critical software
15) Complete destruction of computer facilities

LHS

Inadequate Support Root Causes

16) Support staff not available when required
17) Support staff unresponsive to requests for help
18) Support staff have inadequate knowledge to deal with the problem

LHS

Likelihood

Probability of event occurring within 3 years:

A = Improbable

B = Unlikely

C = Reasonably possible

D = Likely

E = Highly probable

LHS

Consequence to the Business

A = No consequence

B = Operational/administrative issue which merits attention at local level

C = Important but, if came about, may only affect part(s) of the the company

D = Important to the whole company and, if it came about, would affect the whole company

E = Critical to the whole company and, if it came about would affect the whole company

E-Commerce Availability Inherent Risk Mapping

Microsoft Word Document

E-Commerce Availability Residual Risk Mapping

Microsoft Word Document

LHS

Embedded Monitors

- Tell you that your mitigating actions are succeeding
  - Green light indicates that the power is on
  - 20% spare disk capacity means that you will not immediately run out of disk space

LHS

Early Warning Indicators

- Tells you that things are going wrong, but are not yet critical
  - Amber light shows that the UPS has kicked in
  - < 20% of spare disk capacity indicates the need to free up space

The Holistic Risk Process

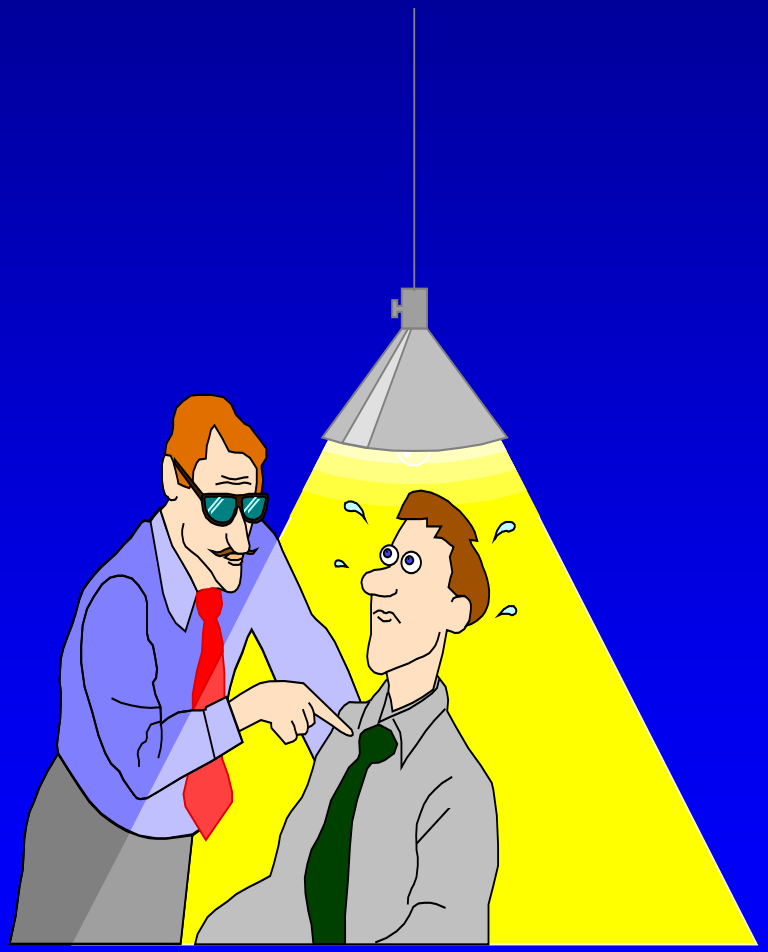
- Identify business objective
- Identify potential undesirable outcomes
- Identify root causes (event triggers)
- Map at the inherent level
- Make key decision (tolerate, terminate, transfer, treat)
- Identify mitigating actions
- Map at the residual level
- Provide objective assurance that the residual level is achievable and appropriate

LHS

Conclusions

- Managing risk requires the identification of the root cause of an event as well as its outcomr
- Managing risk does not mean eliminating it
- Implementing embedded monitors and early warning indicators ensures that risk management becomes an integral part of the business process
- Using a risk based approach makes auditing complex processes easier

Questions?



John Mitchell

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

Tel: +44 (0)1707 851454
Fax: + 44 (0)1707 851455

john@lhscontrol.com
www.lhscontrol.com