
# Overcoming Obstacles To Implementing IT Security Governance


## John Mitchell

PhD, MBA, CEng, CITP, FBCS, MBCS, FIIA, MIIA, PIIA, CISA, QiCA, CFE

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

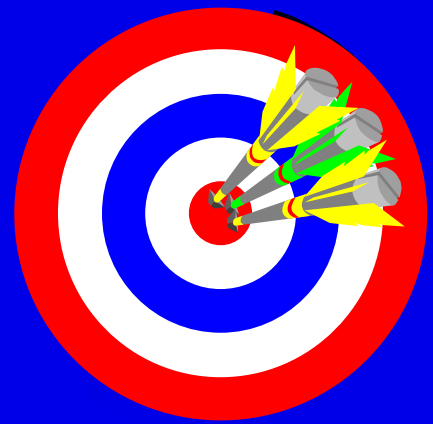
Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Mobile: + 44 (0)7774 145638
john@lhscontrol.com
www.lhscontrol.com


© John Mitchell

LHS

# Themes

- Your enterprise
- What are the obstacles?
- Overcoming resistance
- Adding value
- Who should be responsible?



© John Mitchell

# Your Enterprise

- Wants to be:
  - effective
  - efficient
  - economical
- May view security as a necessary evil because it impacts on the above

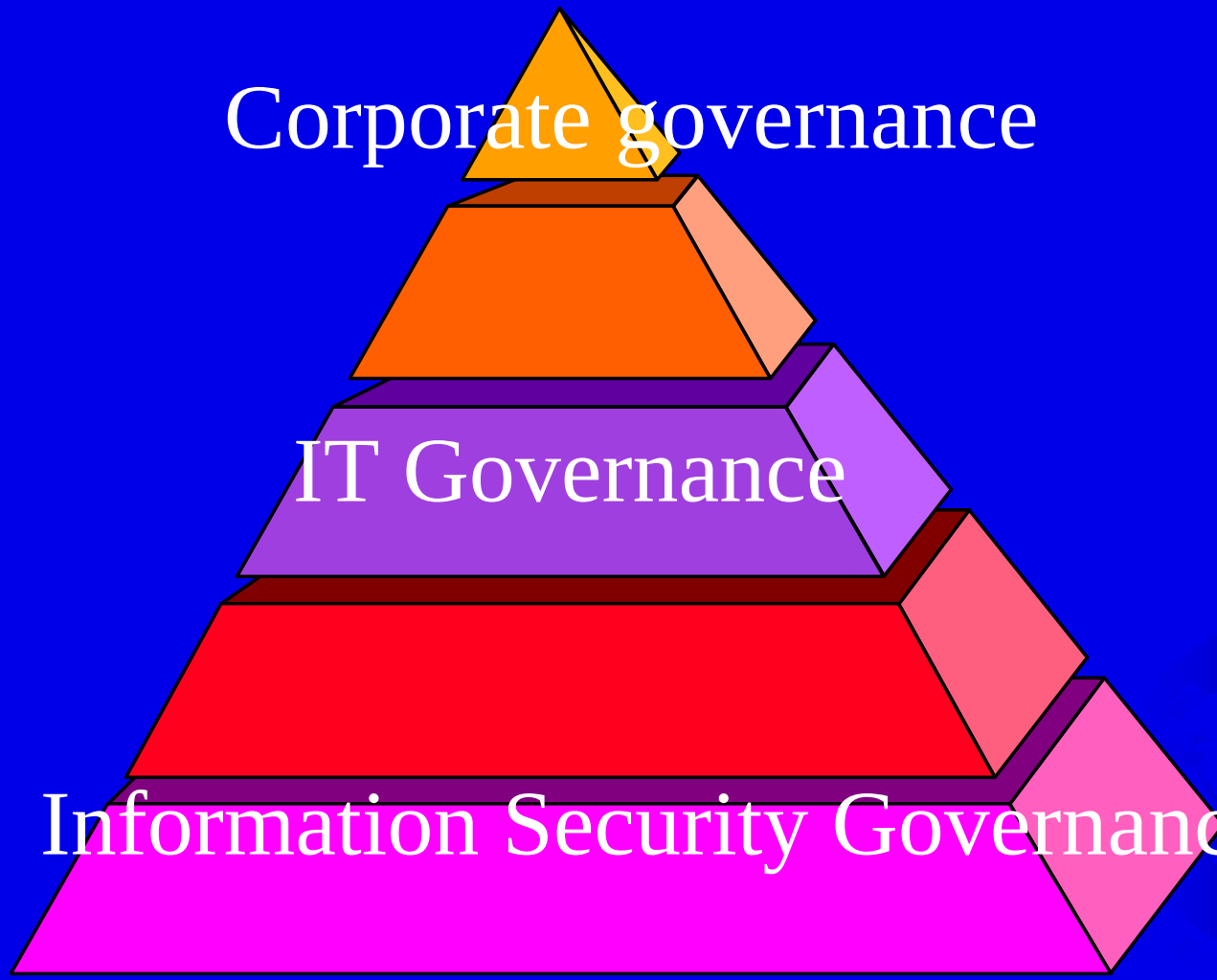
© John Mitchell

# Some Things To Think About

- If you outsource your operations or development
  - What do you know about the potential supplier?
- If you purchase a package
  - What do know about its internals?
- If you link to a third party (customer/supplier)
  - What do you know about their staff?
- If you outsource your security (MSS)
  - What accreditation do they have?

© John Mitchell

# The Hierarchy



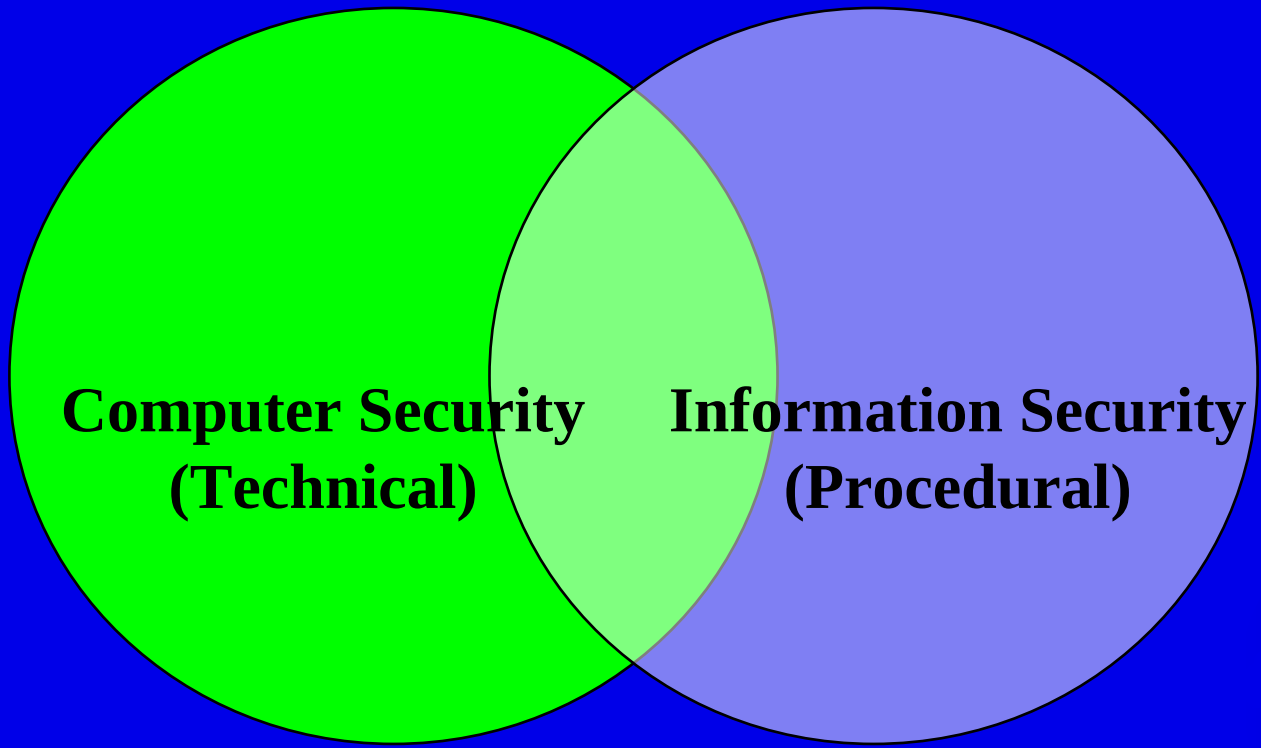

© John Mitchell

# Information Security Governance

- A structure of relationships and processes to protect the enterprise from undesirable events that will impact on its ability to deliver a service.
- This encompasses:
  - breach of confidentiality
  - Incorrect or incomplete data
  - poor processing integrity
  - non-availability of the service
  - breach of statutory regulations.

© John Mitchell

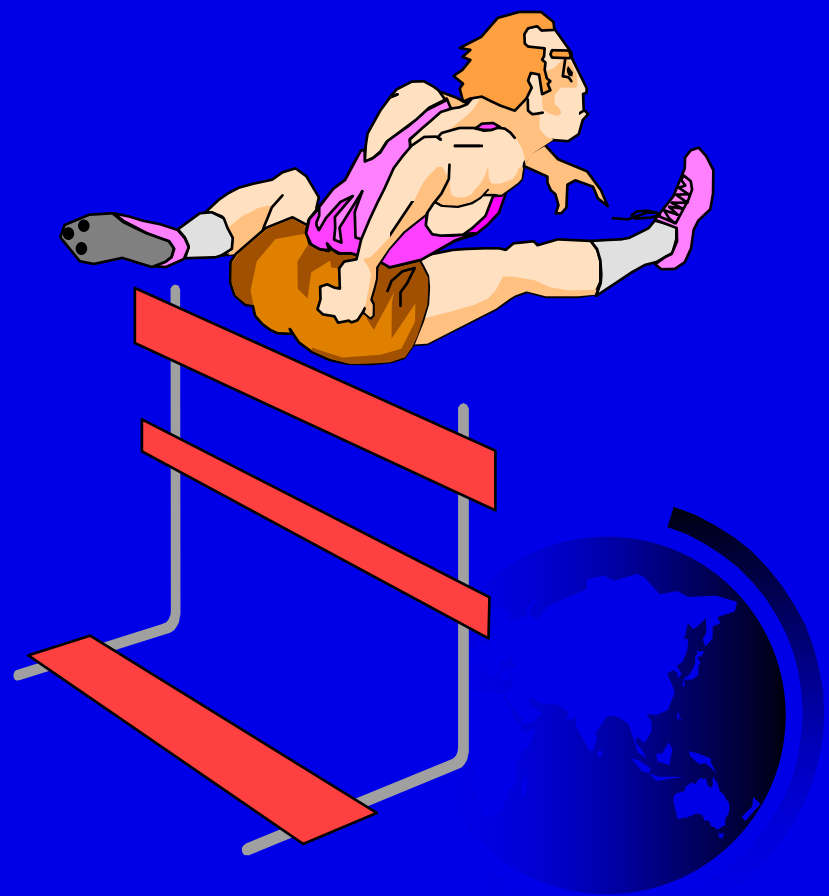
# Information Security Governance




© John Mitchell

# What are the Obstacles?

- Lack of understanding
  - By senior management
  - By local management
- Lack of resource
  - Money
  - People
  - Tools
- Lack of direction
- Corporate culture
- Other priorities
- IT is basically invisible



© John Mitchell

# Where Is The Resistance?

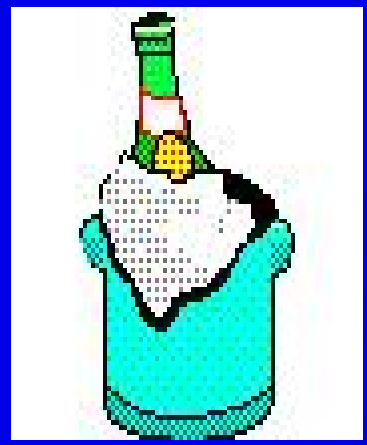
- Executive level management
- Senior management
- IT management
- Users/customers
- Workers' councils
- Trade unions
- Third parties

© John Mitchell

# Corporate Culture

- Theory X
  - Management by direction


- Theory Y
  - Management by trust



© John Mitchell

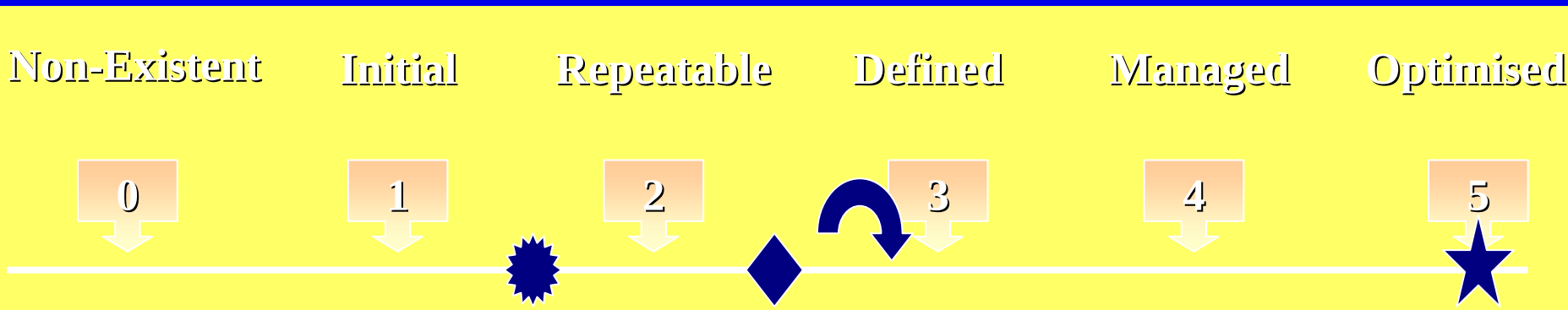
LHS

# The Drivers

- You just have to do it (e.g. SOX)
- Market forces (if you can't prove you are secure we will not deal with you)
- Your boss wants it (do it or else)
- It will be good for you (add value)

© John Mitchell

# Where Are You Now? (Capability Maturity Models)

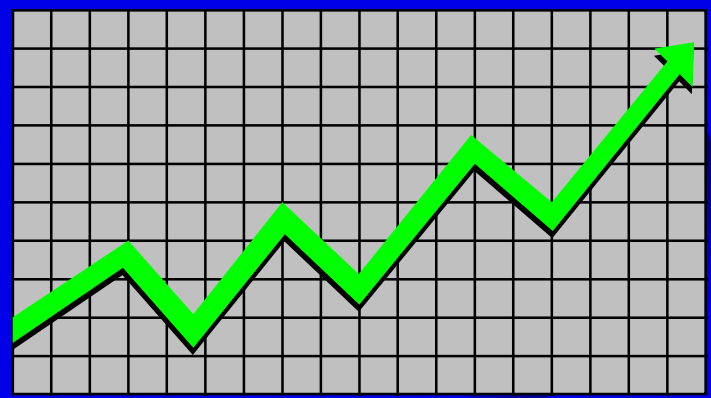



© John Mitchell

LHS

# Where Do You Want To Be?

- Key Goals
- Key Goal Indicators
- Critical Success Factors
- Key Performance Indicators
- Balanced Scorecard
- Management dashboard

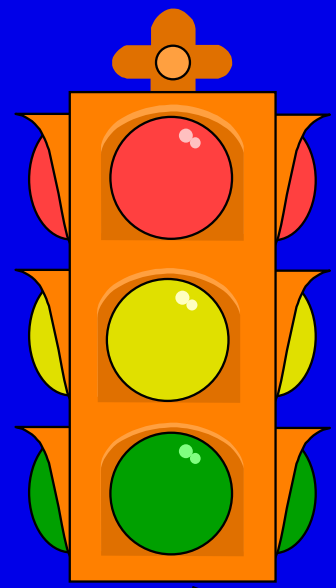


© John Mitchell

LHS

# How Well Are You Doing?

- Embedded Monitor
  - How do you know that things are okay?

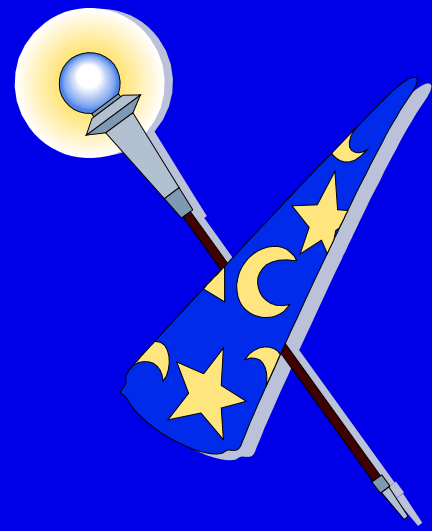


- Early Warning Indicator
  - What warning do you get that things are going wrong before they become really serious?

© John Mitchell

# Some Solutions?

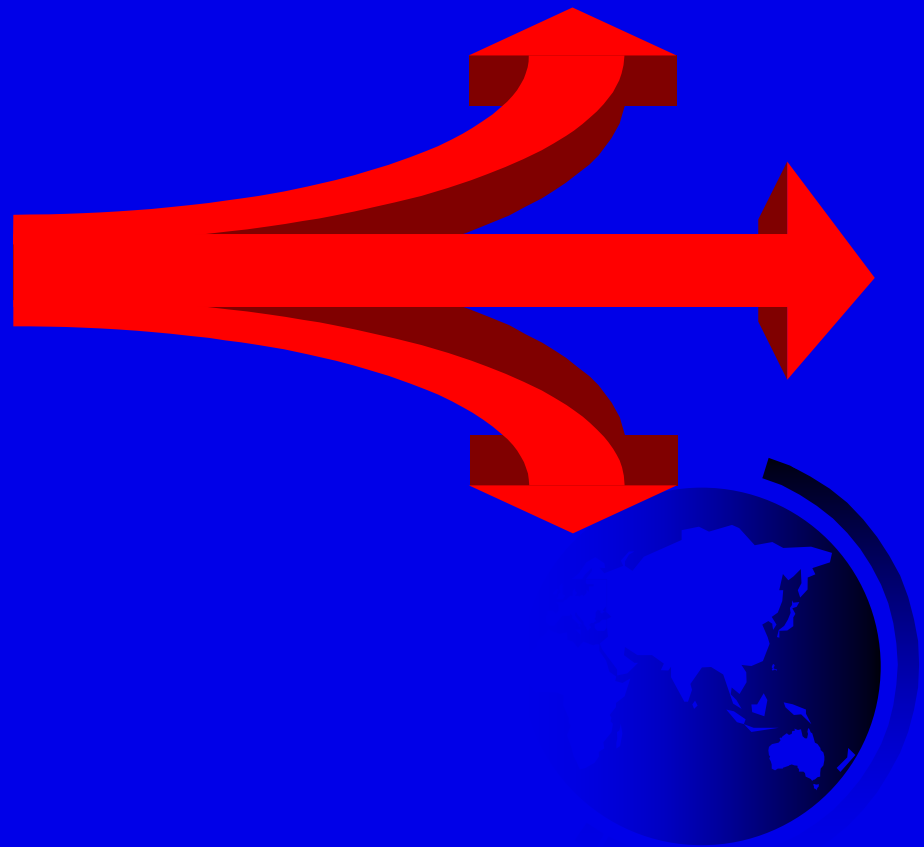
- Make it easy
- Use a risk based approach
- Provide some measures
- Introduce self assessment
- Make the assurance process transparent



© John Mitchell

# Provide A Road Map

- Identify Needs
  - Risk analysis
  - Raise awareness
- Envisage Solution
  - Where are you now?
  - Where do you want to be
  - Gap analysis
- Plan Solution
  - Identify measurement metrics
  - Develop change programme
  - Define projects
- Implement Solution
  - Generate Balanced Score Card
  - Collect metrics
  - Report



© John Mitchell

# Ask Leading Questions

| To identify IT Security Issues | To Find Out How Management Addresses IT Security Issues | To Assess IT Security Governance Practices |
|---|---|---|
| • How often is security considered at the start of an IT project?<br>• Are end users satisfied with the ease of operating IT security?<br>• Are sufficient IT security resources available to meet strategic objectives? | • How well are enterprise and IT security objectives aligned?<br>• What strategic initiatives has executive manage-ment taken to manage IT security relative to maintenance and growth of the enterprise<br>• Are they appropriate? | • Is the board regularly briefed on IT security risks to which the enterprise is exposed?<br>• Is IT security a regular item on the agenda of the board and is it addressed in a structured manner?<br>• Does the board articulate and communicate the business objectives for IT security alignment? |

© John Mitchell

# Embarrass Them!

- When was the last briefing made to the Board on IT security risks and the status of IT security improvements?
- Is the enterprise clear on its position relative to IT security risks?
- How much is currently being spent on IT security?
- What are the costs associated with a security incident?

© John Mitchell

LHS

# Embarrass Them!

- How many staff received IT security training last year?
- How many of the management team received IT security training?
- How does the organisation detect IT security incidents?
- How are they escalated and what does management do about them?
- Is management prepared to recover from a major security incident?
- Is management confident that IT security is adequately addressed in the organisation?

© John Mitchell

LHS

# Scare Them!

- What information assets are subject to laws and regulations?
- What has management implemented to assure compliance with them?
- Is there a security programme in place that covers all of the above questions?
- Is there clear accountability?

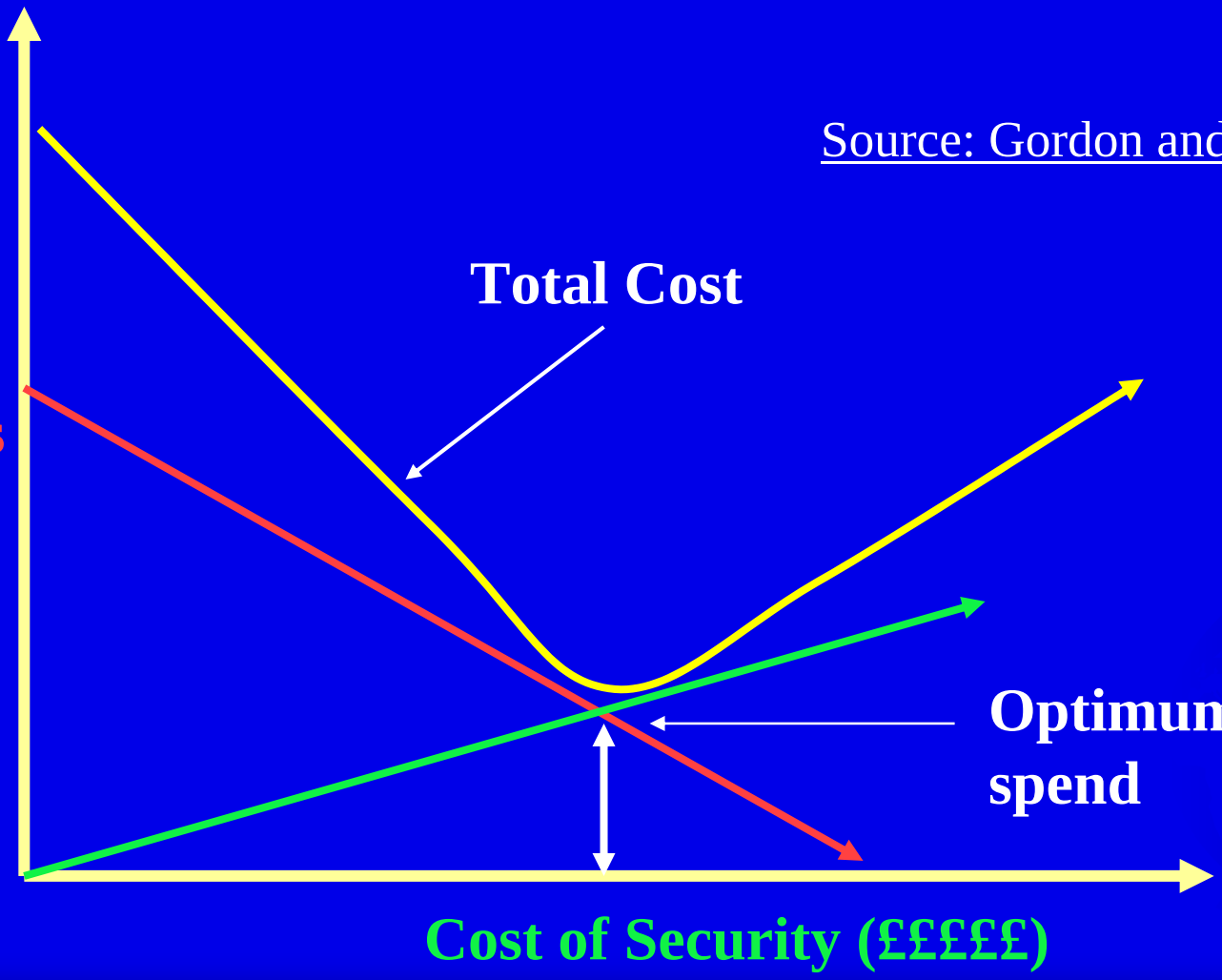
© John Mitchell

# Know the Real Cost of Security Incidents

- Competitive disadvantage
- Business loss
- Reputation loss
- Damage to morale
- Fraud
- Wrong management decisions
- Disruption
- Legal liability
- Privacy loss
- Safety risk

© John Mitchell

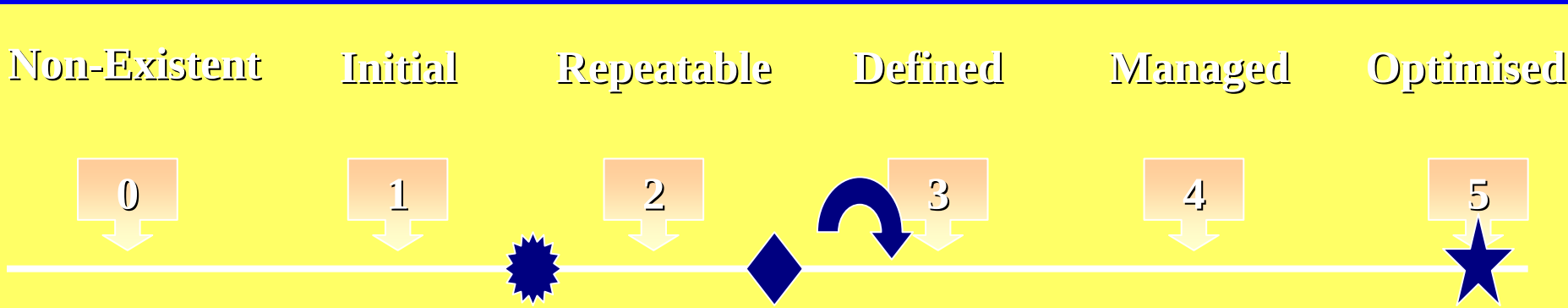
# Know How Much You Should Spend




© John Mitchell

# Ask Tough Questions

## Where Is Your Security Now?




## Where Do You Want To Be?

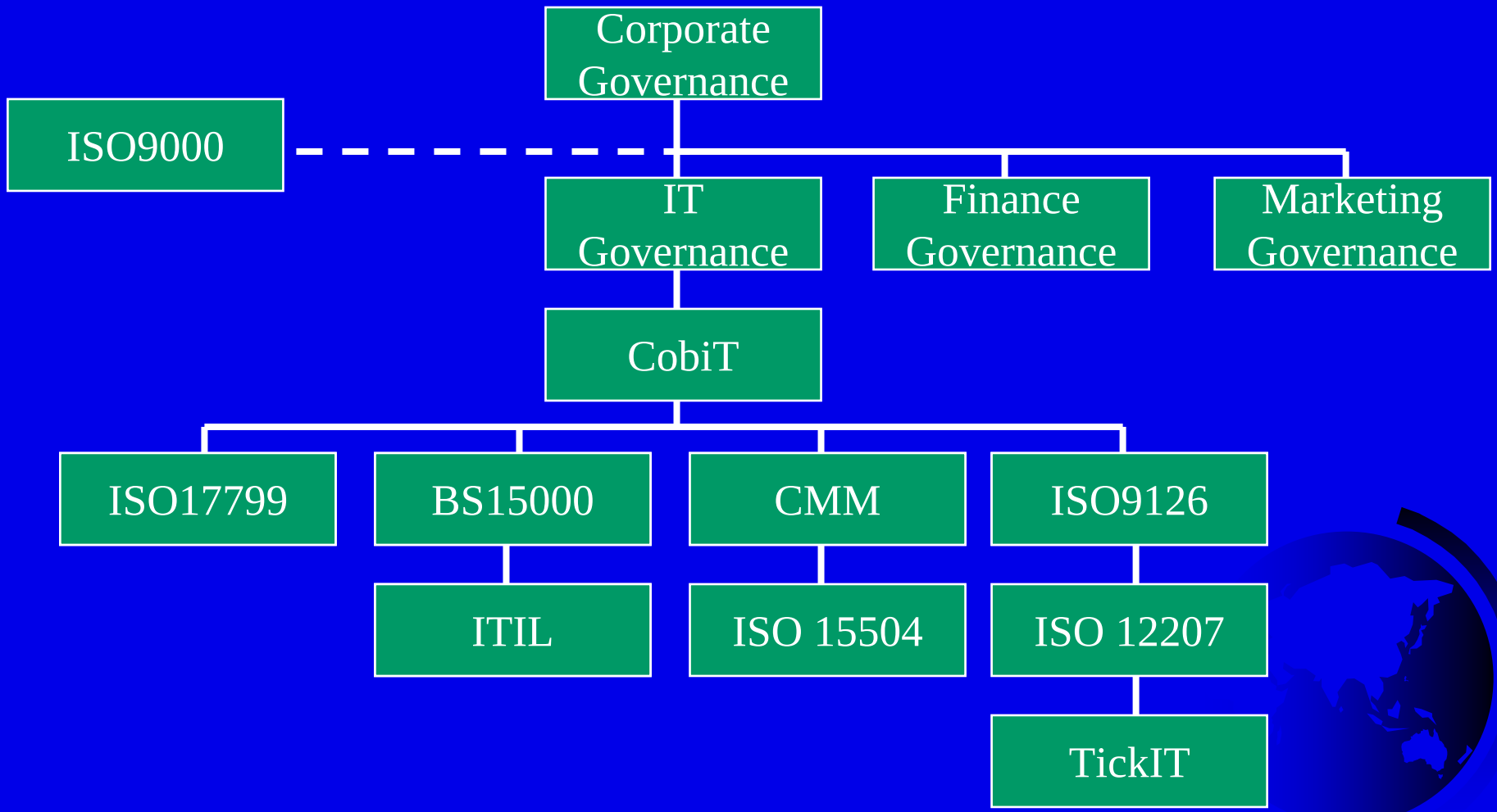
© John Mitchell

# Provide a Comprehensive Tool Kit

- Control Objectives for IT (CobiT)
- ISO 17799
- BS 15000
- ITIL
- ISO 9126
- ISO 9000

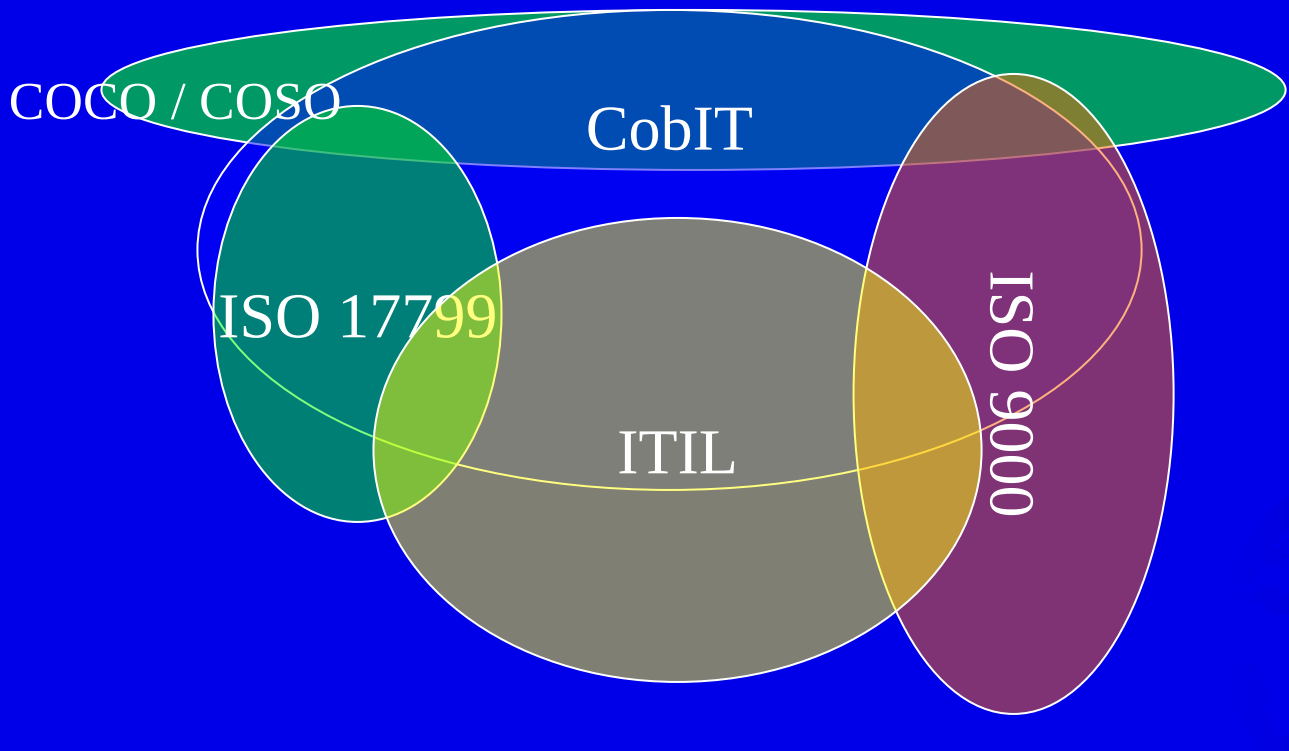
© John Mitchell

# Show How the Tools Link




© John Mitchell

# Show A Family




© John Mitchell

# Be Comprehensive

**IT SECURITY GOVERNANCE PROGRAMME**

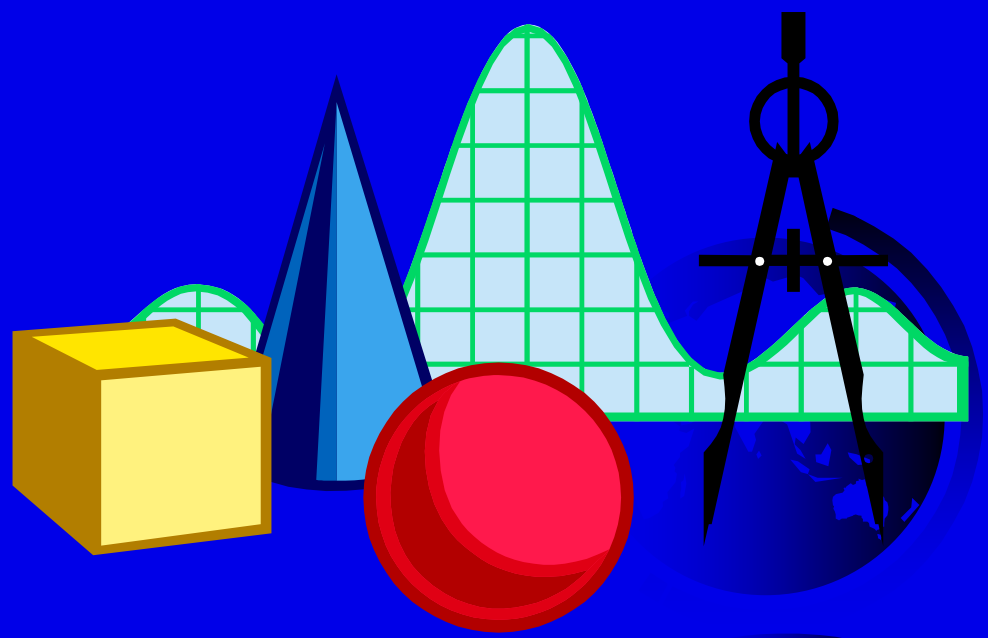
| Planning & Organisation | Acquisition & Impl. | Delivery & Support | Monitoring |
|---|---|---|---|
| - Strategic Planning<br>- Information Architecture<br>- Technological Direction<br>- IT Organisation & Relationships<br>- Manage the IT Investment<br>- Communicate Aims & Direction<br>- Manage human resources<br>- Ensure Compliance<br>- Assess Risks<br>- Manage Projects<br>- Manage Quality | - Identify Solutions<br>- Acquire & Maintain Application Software<br>- Acquire & Maintain Technology Architecture<br>- Develop & Maintain IT Procedures<br>- Install & Accredit systems<br>- Manage Changes | - Define Service Levels<br>- Manage third-party services<br>- Manage performance and capacity<br>- Ensure continuous service<br>- Ensure systems security<br>- Identify and attribute costs<br>- Educate and train users<br>- Assist & advise IT customers<br>- Manage the configuration<br>- Manage problems & incidents<br>- Manage data<br>- Manage facilities<br>- Manage operations | - Monitor the processes<br>- Assess internal control adequacy<br>- Obtain independent assurance<br>- Provide for independent audit |

© John Mitchell

LHS

# Link It To Something Else

- Risk management
- Statutory compliance (SOX, Basel II etc)
- Staff evaluation
- Self assessment



© John Mitchell

# Provide A Complete Process

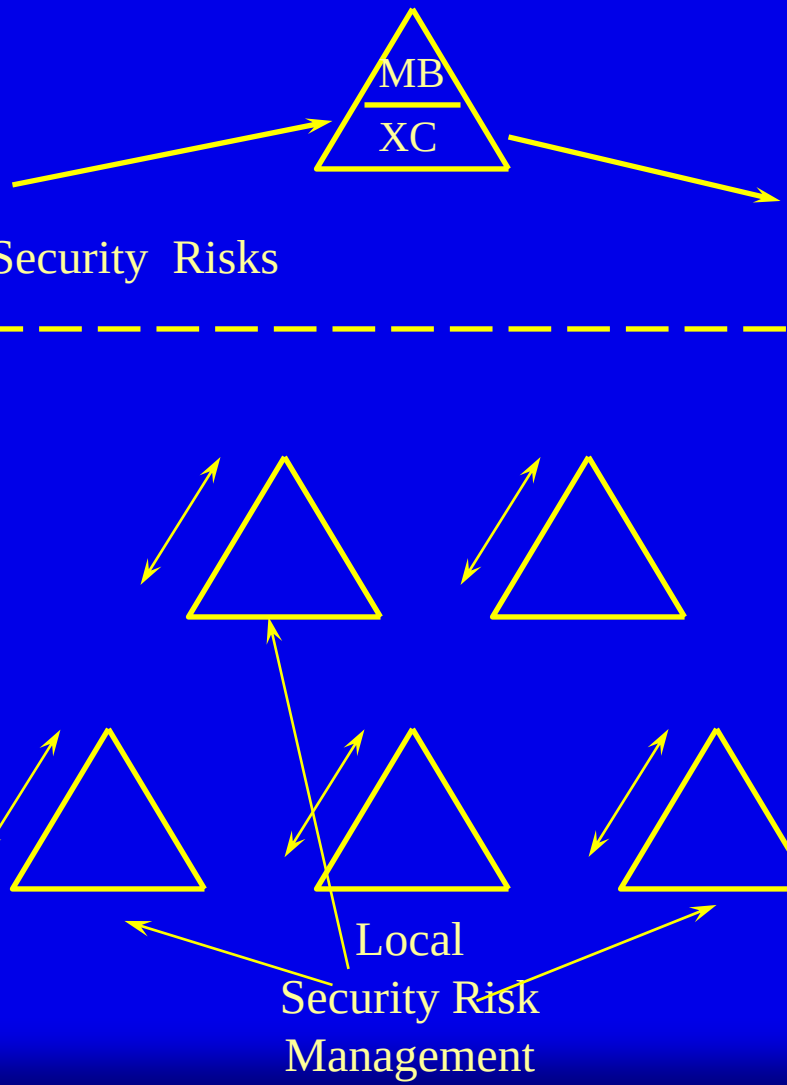

© John Mitchell

# Use Easily Recognised Risks

- Information not available when required
- Information available to unauthorised persons
- Unauthorised modifications to data, files, or programs
- Denial or delay of service
- Unauthorised use of facilities
- Damage, or theft of equipment, software or data
- Breach of statutory or regulatory requirements

© John Mitchell

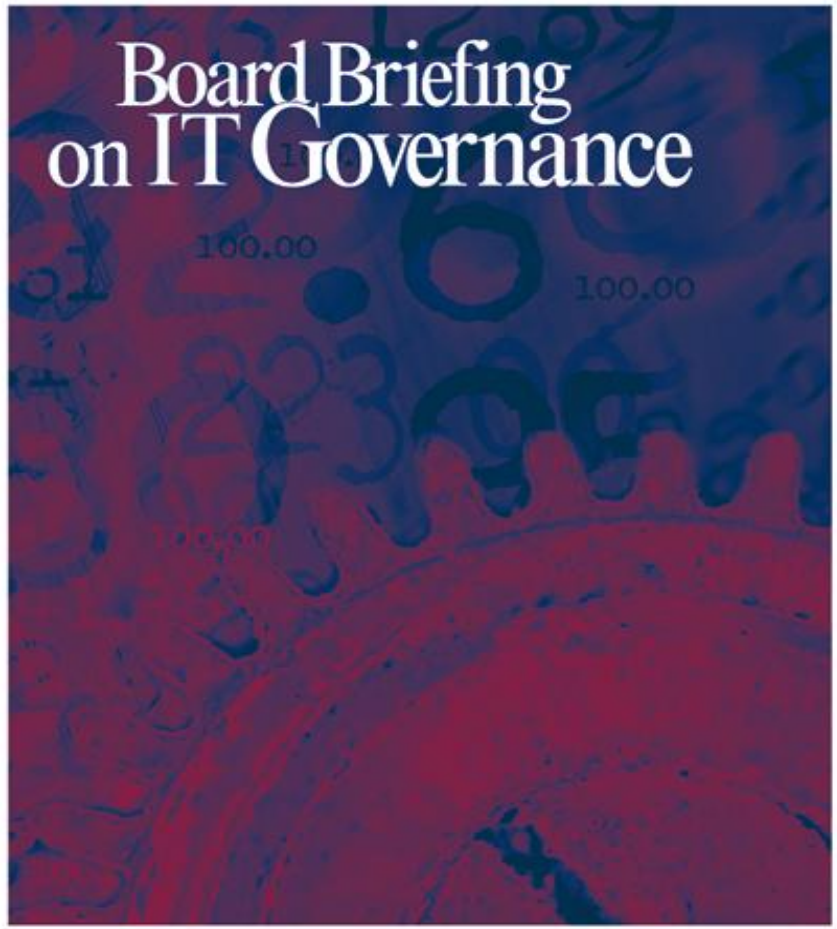
# Show the Big Picture




© John Mitchell

LHS

# Provide free information




Download from www.itgi.org

© John Mitchell

LHS

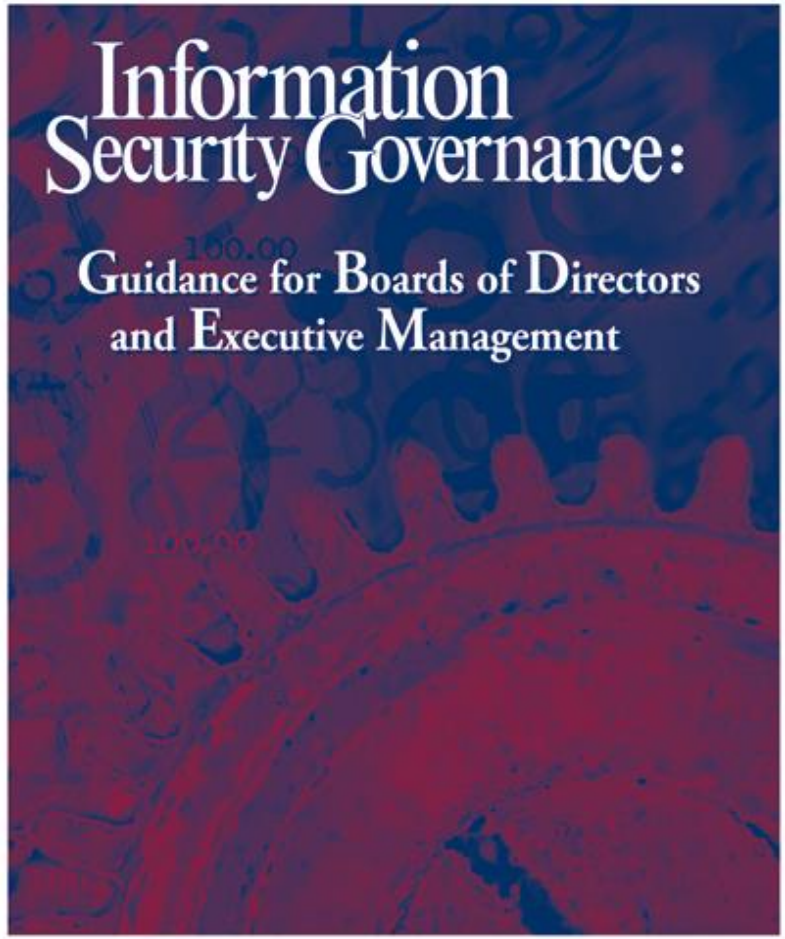
# Introduce ideas


Download from www.itgi.org

© John Mitchell

LHS

# Provide some guidance & show international support

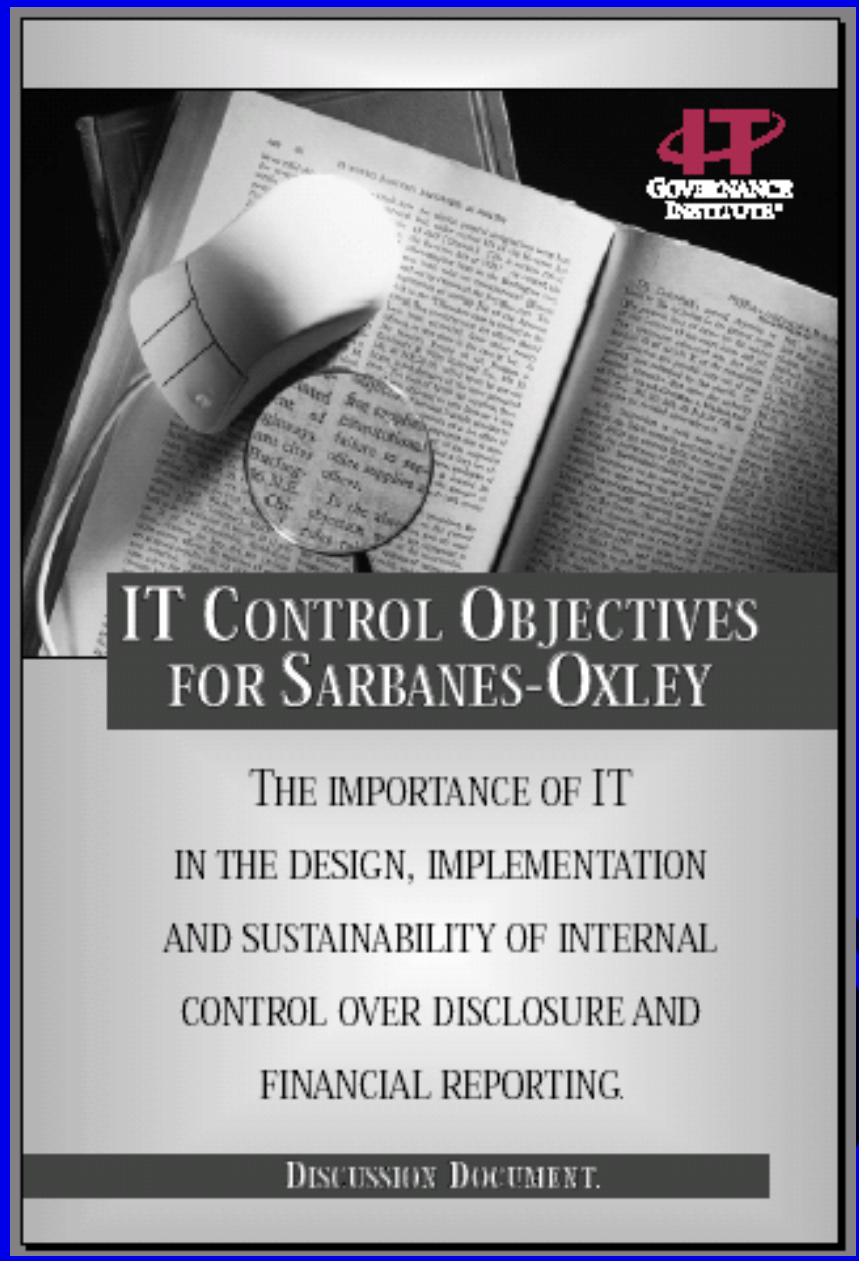



Download from www.itgi.org

© John Mitchell

LHS

# SOX is big - so provide a solution




Download from www.itgi.org

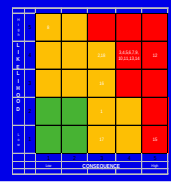
© John Mitchell

# Add Real Value

Risk Description

Root Cause

Inherent Risk Scores



Movement is plotted on a heat diagram

Residual Scores

| Ref. | Risk | Root causes | Owner | INHERENT | | Mitigating Actions | Embedded Monitors/Early Warning Indicators | RESIDUAL | |
|---|---|---|---|---|---|---|---|---|---|
| | (Threat to achievement of business objective) | (How the threat could arise) | | | | (What we are doing to manage the threat) | (How we know if we are succeeding) | | |
| | Format: EVENT leading to CONSEQUENCE resulting in EFFECT ON BUSINESS OBJECTIVE | | | Probability | Impact | Format: Who, What action, How frequent, How evidenced | Format: include comment on effectiveness. | Probability | Impact |
| | | | | | | | | | |
| 12 | Non-availability of the HRIT service leads to users not being able to retrieve HR information resulting in regulatory failure | Loss of power to key server | Ops&IT | 4 | 4 | UPS and standby generator | Regular successful tests of power interruption | 1 | 4 |

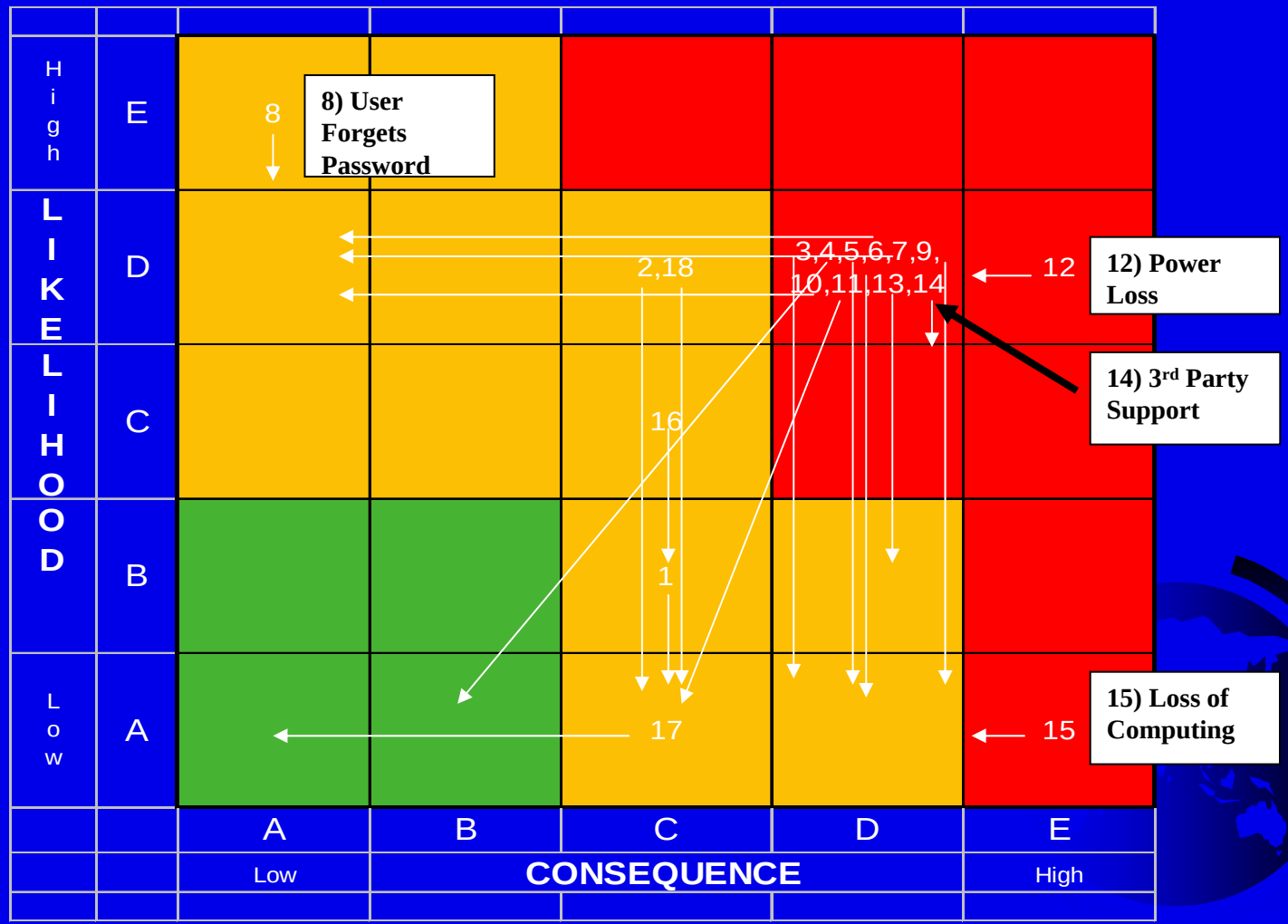
Owner

Mitigating Actions

Embedded Monitors

© John Mitchell

# Make It Interesting




© John Mitchell

LHS

# Responsibilities?

- Executive management for direction
- HR for setting the employment conditions, the disciplinary processes and the training
- Legal for providing guidance on what can and should not be allowed
- IT for providing the technical capability
- Audit for providing assurance

© John Mitchell

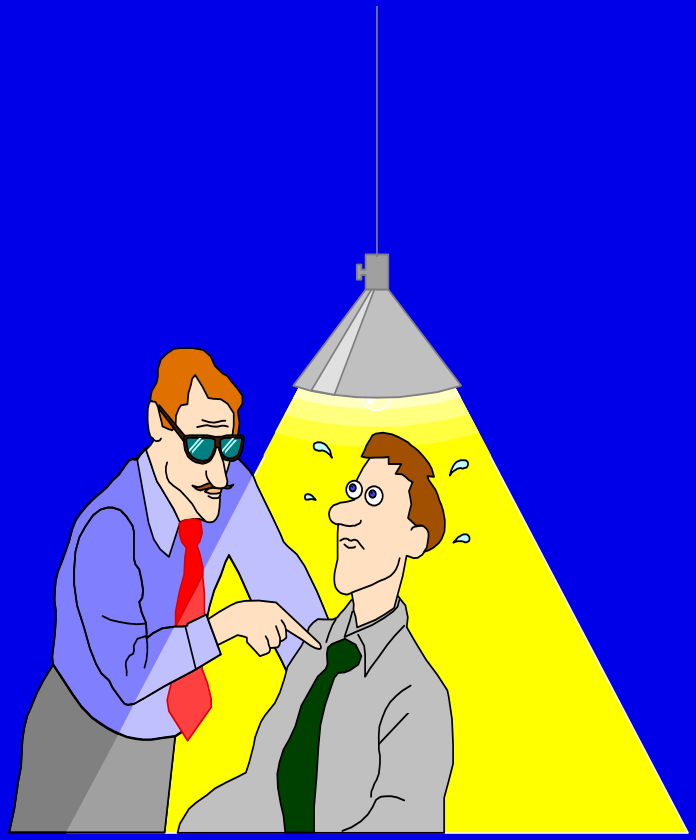
LHS

# Summary

- Overcoming obstacles to IT security governance requires an understanding of company dynamics, psychology & perseverance!
- CobiT, ISO 17799, BS 15000 & ITIL (amongst others) provide a useful framework
- Human Resources (Personnel), Legal, IT and audit have a role to play, but HR is the key player
- Provide a process that adds value whilst minimising risk

© John Mitchell

# Questions?



John Mitchell

PhD, MBA, CEng, CITP, FBCS, MBCS, FIIA, MIIA, PIIA, CISA, QiCA, CFE

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

Tel:  +44 (0)1707 851454
Fax:  +44 (0)1707 851455
Mobile +44 (0)7774 145638

john@lhscontrol.com
www.lhscontrol.com

© John Mitchell