Corporate Governance, ISO/IEC 17799 and BS 7799-2

by Dr. David Brewer

Associate Consultant

Integer Knowledge Pte Ltd (Singapore)

Director

Gamma Secure Systems Limited

Agenda

- Corporate Governance
- Internal Control
- ISO/IEC 17799 and BS 7799-2
  - *Could they serve as an adequate control framework?*
  - *Have they a wider utility?*
- Prospects and Limitations
- Summary

Corporate Governance

Why

- … a result of scandals … investing public … being "ripped off" … conduct of senior executives
  - *South Sea Bubble, Kruger, Salad Oil company, Equity funding, Polly Peck, Maxwell Pensions, Enron, WorldCom …*
- New laws/regulations … anti discrimination, privacy protection, product quality etc.
- Turnbull, OECD, Sarbanes-Oxley

Turnbull

- 100 FTSE only (Yellow Book)

The internal control requirements of the Combined Code

Principle D.2 of the Code states that 'The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets'.

Provision D.2.1 states that 'The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management'.

Provision D.2.2 states that 'Companies which do not have an internal audit function should from time to time review the need for one'.

The OECD Principles (2004)

- The rights of shareholders and key ownership functions
- The equitable treatment of shareholders
- The role of stakeholders in corporate governance
- Disclosure and transparency
- The responsibilities of the Board
  - *It is an important function of the board to establish internal control systems covering the use of corporate assets and to guard against abusive related party transactions.*

Sarbanes-Oxley/EC Directive

- An act "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes"
- Places heavy emphasis on internal control, e.g.
  - *§404 (a) (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.*

Internal Control

What is Internal Control?

- Way in which management deploys resources to achieve the organisation's objectives
- Two basic parts:
  - *Procedures to perform the work necessary to conduct the organisations business (operational procedures)*
  - *Procedures to ensure that the business is conducted as expected (controls)*
- It is this second part that concerns us today

Audit Practice Board

- This is their advice:

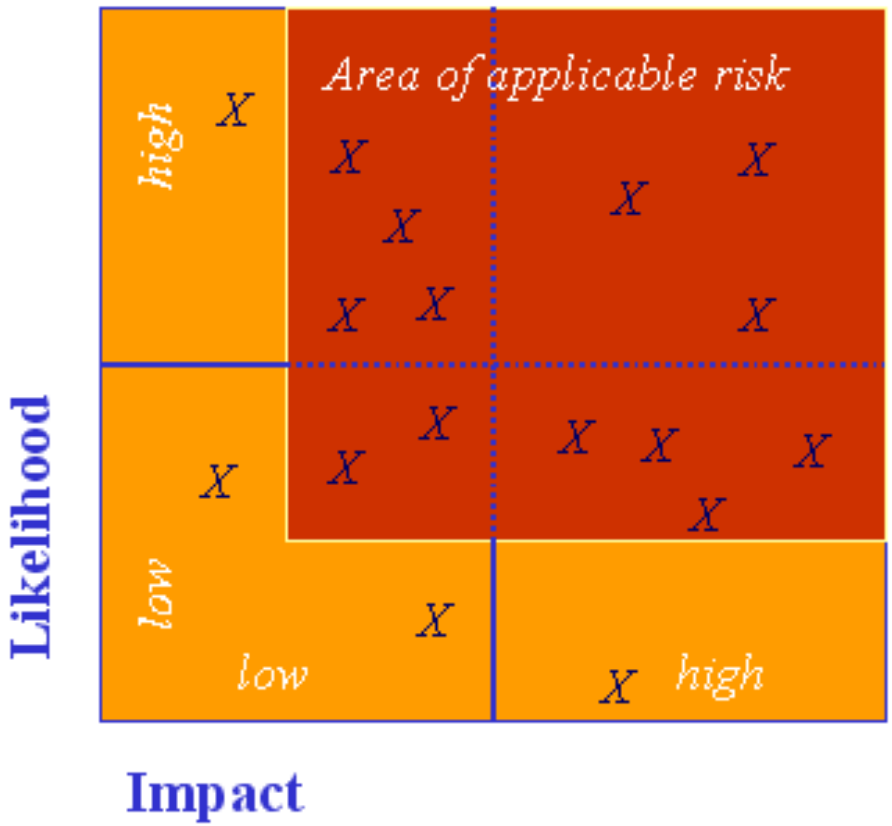
Risks – a Taxonomy

- Following Basel II

Primary Risk Category	**Definition:** the risk of loss arising from ...	**Associated Operational Risk:** the inadequacy or failure of internal processes, people and systems that results in a risk of ...
Project risk	... default by a creditor (which will usually be a customer).	... doing work and not making a profit.
Trading risk	... changes in trading positions when prices move adversely.	... our money and other assets not being worth as much as they ought.
Market risk	... the market refusing to buy what we have to offer at the price we wish to sell it.	... being unable to sell what the market wants.
Existence risk	... the fact that we exist.	... spending money unnecessarily.

Applicable Risks

- and non-applicable risks



Controls – Fundamentals

"… detect the event in sufficient time to do something positive about it… "

See http://www.gammassl.co.uk/topics/time/index.html

Types of Control

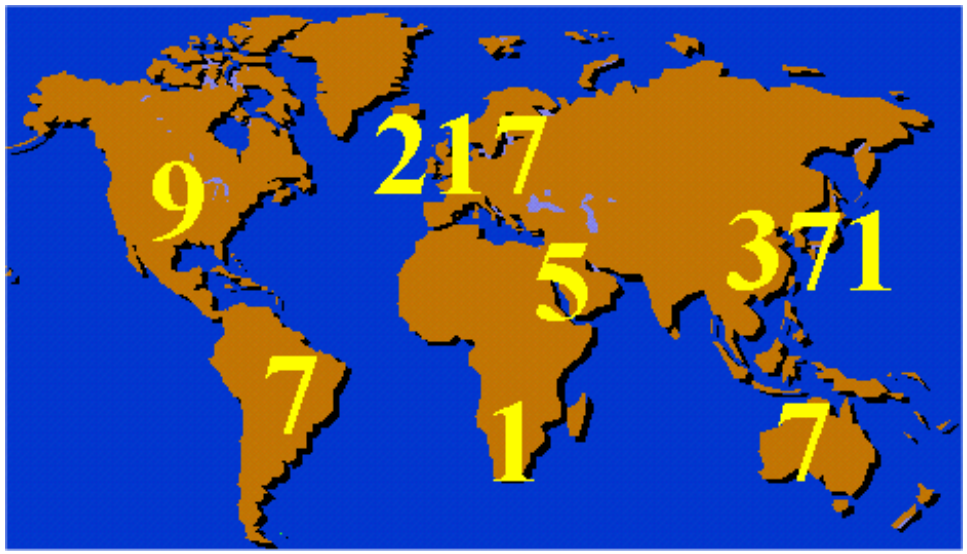
- Preventive
  - *Either prevent the event from occurring or affecting the organisation, or*
  - *Detect the event as it happens and prevent any further activity that may lead to an impact*
- Detective
  - *Identify when some event, or events have occurred … and invoke appropriate actions to arrest (or mitigate) the situation*
- Reactive
  - *Identify that the impact has occurred and invoke appropriate actions to recover (or mitigate) the situation*

GAMMA

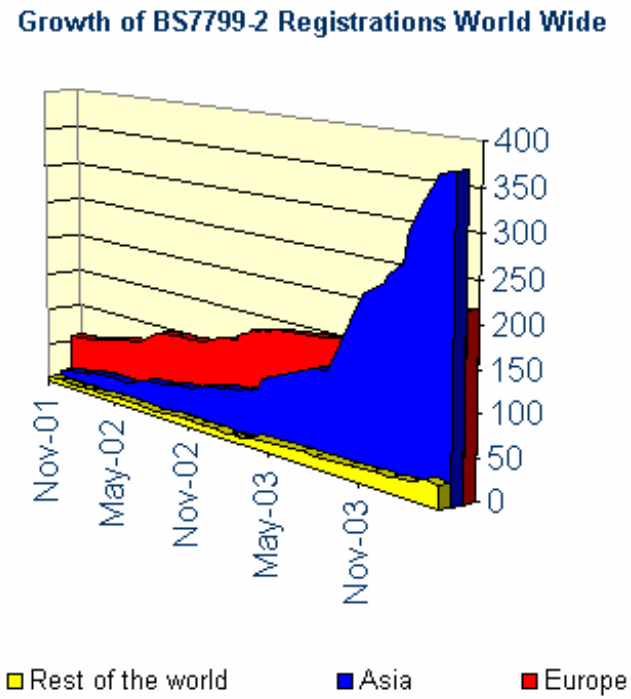
ISO/IEC 17799 and BS 7799-2

1 – What are they?

World-wide Take Up



BS 7799-2 Registrations by Continent



ISO/IEC 17799 and BS7799-2

- BS 7799 Part 2 is a *management standard – e.g. let's party.* Part 2 tells you what to do
- IS 17799 is a *super-market of good things to do*
- Certification is against Part 2 – *is the party OK?*

BS 7799-2:2002

ISO/IEC 17799:2000

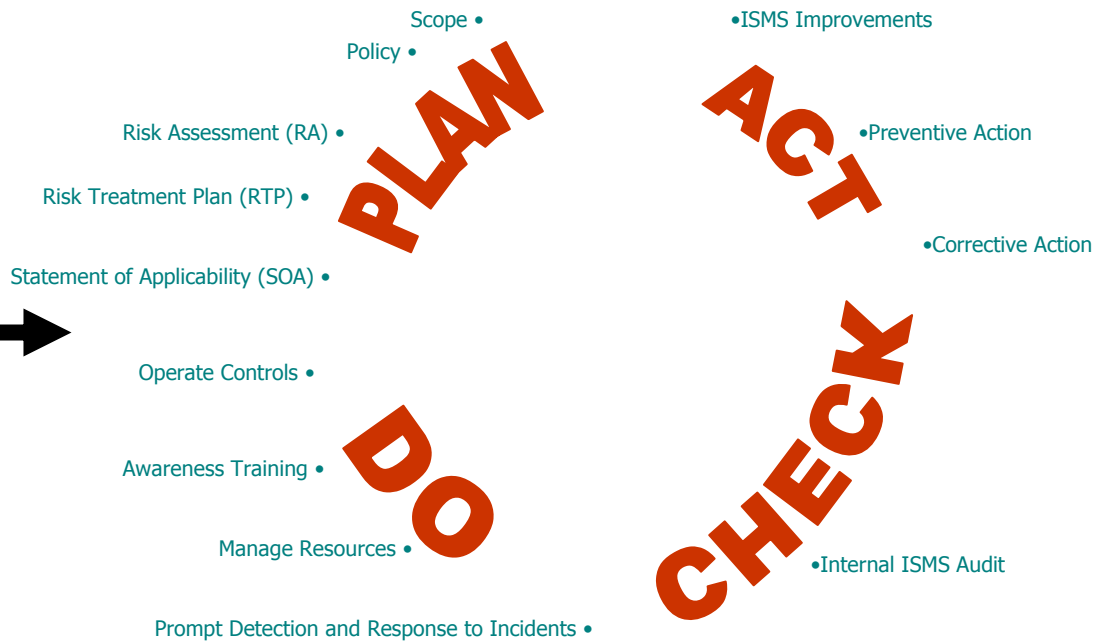
Provides guidance under 10 major headings

- Security Policy
- Security Organisation
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operational Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

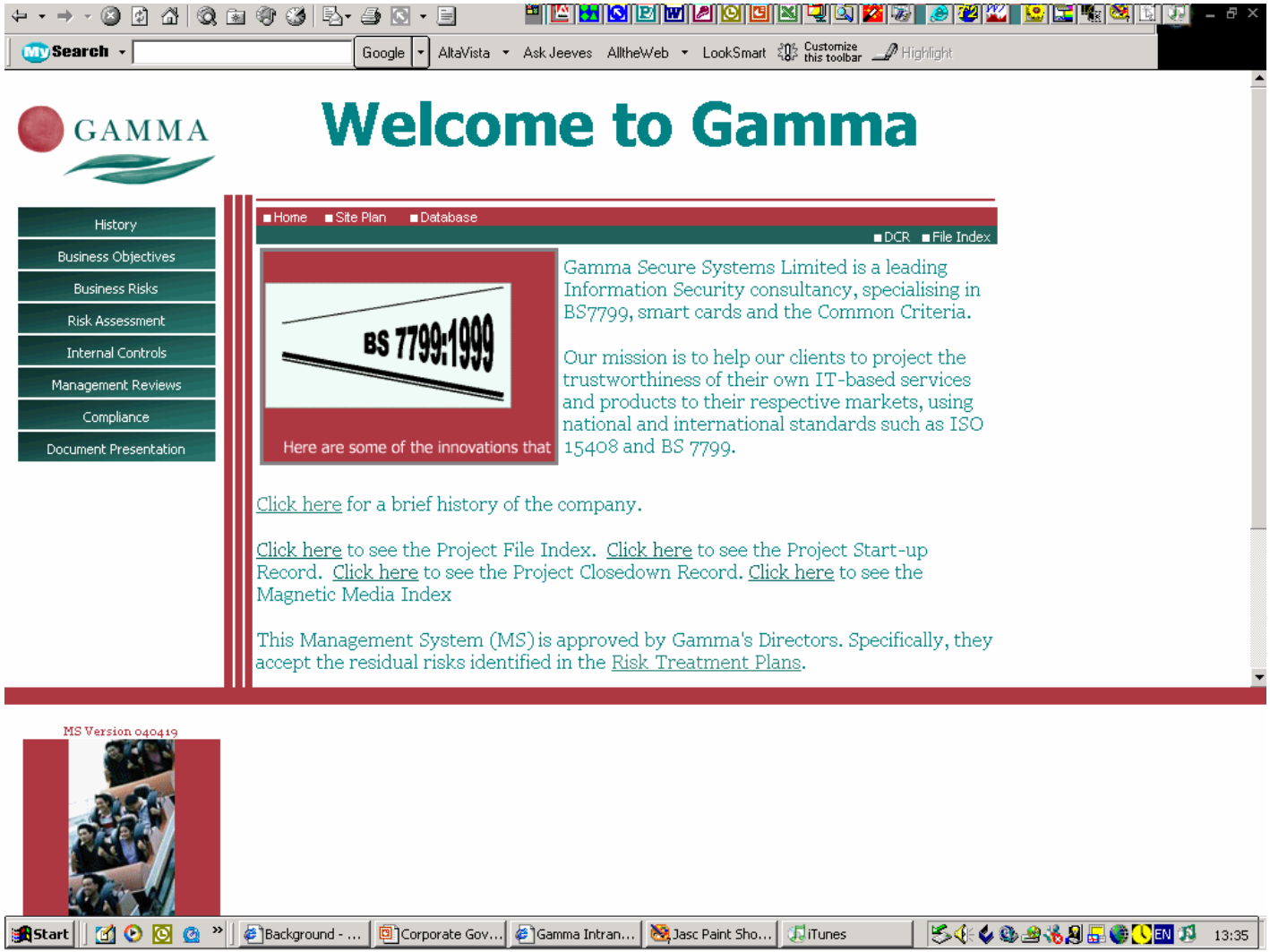
ISO/IEC 17799 and BS 7799-2

2 – Could they serve as an adequate control framework?

Equivalent Structures



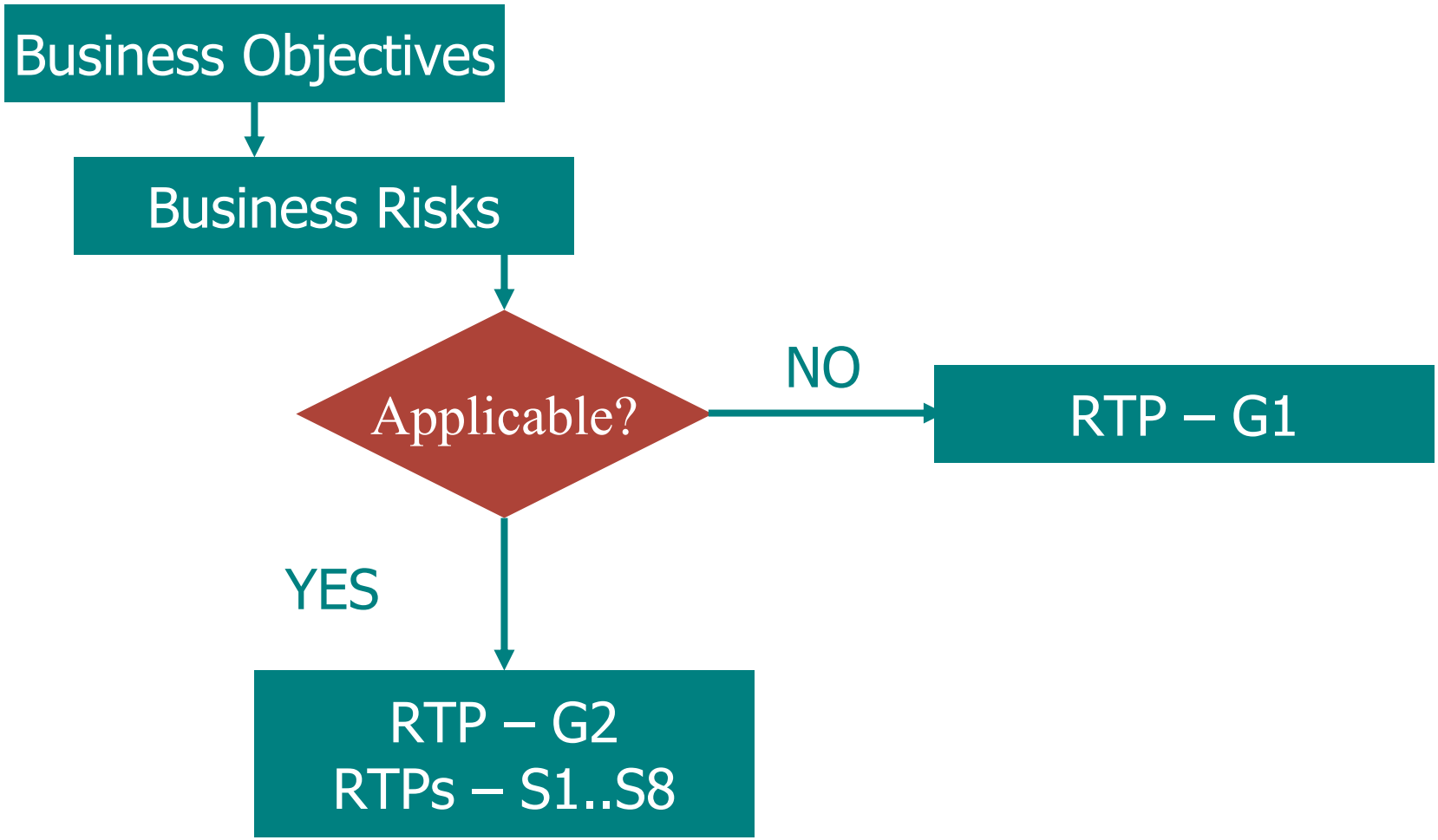
Gamma's ICS Does This (1)



Gamma's ICS Does This (2)

Home		
Overall MS	ISO 9001	BS 7799-2
PLAN		
Scope	Scope	Scope
Policy	Quality Policy	Information Security Policy
Business Risks		
Risk Treatment Plan Index		Risk Assessment
		Threats
		Assets
		Vulnerabilities
		Impacts
	Exclusions	SOA
Compliance	Compliance	Compliance
DO		
Summary of Internal Controls	Control Structures	
Projects Practice		
Version Control Practice		
Media Management Practice		
Terms of Reference		
Document Review Practice		
CHECK		
Management Review (overview)		
Management System Review Practice		
Internal/External Audit and Management Review Schedule		
Management Review Index		
Management Review Checklist		
Customer Feedback (Instructions and Results)		
ACT		
To Do List		
Preventive and Corrective Action		
Improvements		

Gamma's ICS Does This (3)



Answer to the Question

- Q. Could they serve as an adequate control framework?

- A. YES

ISO/IEC 17799 and BS 7799-2

3 – Have they a wider utility?

Answer to the Question

- YES

- Gamma's ICS addresses:
  - *Credit Risk*
  - *Trading Risk*
  - *Market Risk*
  - *Quality Risk*
- As well as *Information Security Risk*

But ISO/IEC is just IT!

- No – it's information security not IT security
- IT security is just the same old problem in a different guise
- Internal control activities (including everything concerning financial reporting) predominately concerns information

Does ISO/IEC Recognise This?

- YES
  - *10.2.1 Input Validation*
  - *10.2.2 Control of Internal Processing*
  - *10.2.4 Output Validation*
- Transparency and disclosure rely on integrity, availability and confidentiality – the hallmarks of ISO/IEC 17799

GAMMA

Prospects and Limitations

Fast Track to Internal Control

- Guidance and standards exist in the public domain (although a small fee applies to some)
- A skeleton ISMS manual is available
- Standards, theory and practice of RTPs is available
- Shrink-wrapped?
  - *Almost*
  - *All ICS have to be customised to organisation*
  - *Need management involvement and resources*

Skeleton ISMS Manual

Department (Name/Logo)

ISMS Manual

Parts for you to complete

- Index
- Introduction
- Scope
- Policy
- Context
  - Assets
  - Threats
- RA
  - Impacts
  - Risks
- SOA
- To Do List
- Training/Awareness
- Int Audit
- Mgt Review
- Improvement
- Records

ISMS Version
31025

INTRODUCTION

Purpose

This document is <<State name of Department (note you
System (ISMS) Manual". The purpose of the ISMS is emp
risks.

Contents

This Manual defines the scope of the ISMS and all applicab
Assessment and Risk Treatment Plan and presents the Sta
2:2002. The SOA refers out to other relevant processes a

This manual details the processes and procedures for train
Internal ISMS Audit, Management Review and ISMS imp

Approval and Distribution Policy

This ISMS Manual was approved by the Department on <
risks identified in the Risk Treatment Plans.

<<State here the distribution policy for this ISMS Manual>>

Checklists

Internal ISMS Audit Report and Checklist

INTERNAL ISMS AUDIT REPORT and CHECKLIST

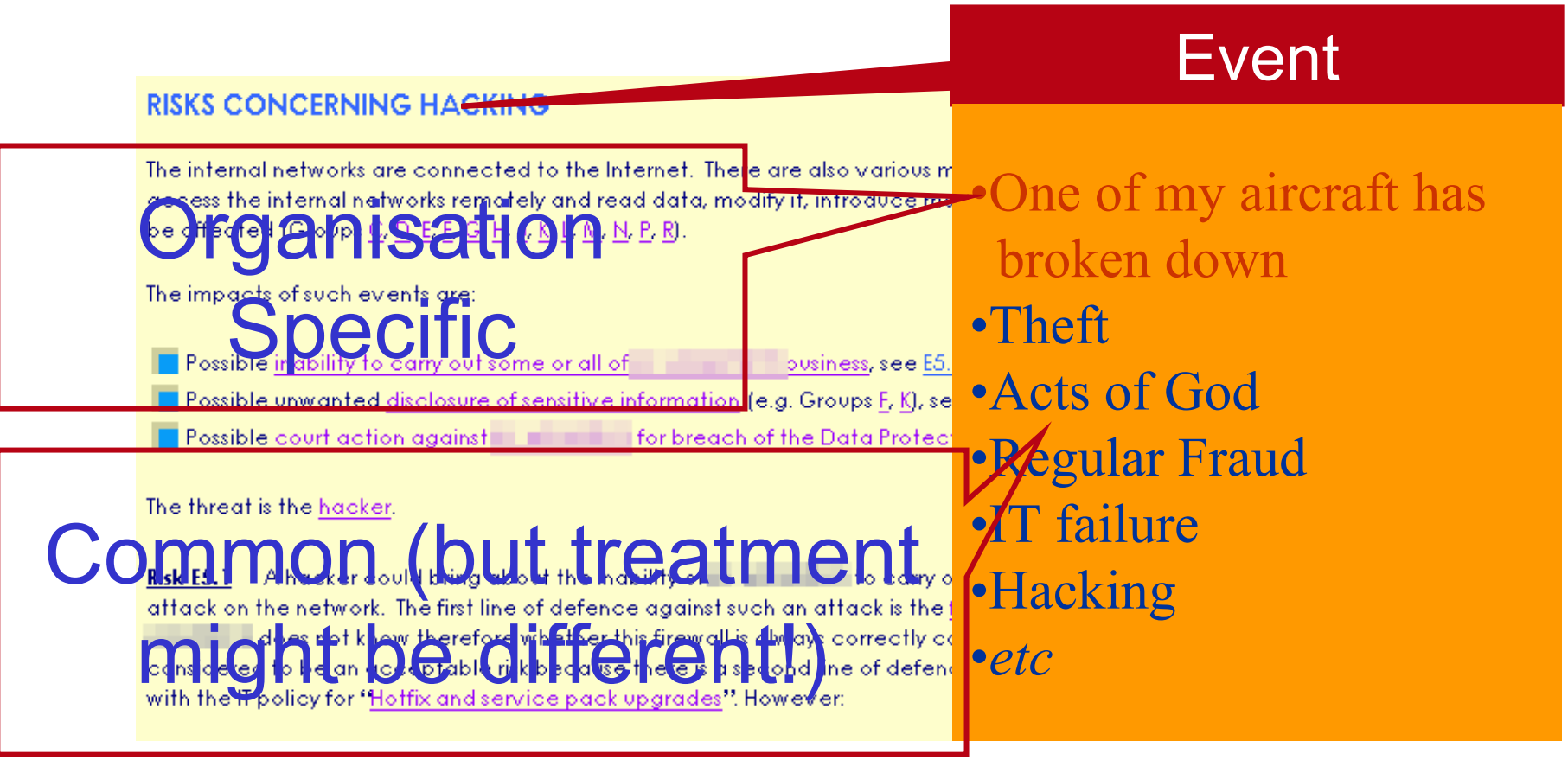
Department:

Completed by:

Covers every requirement of BS7799-2:2002

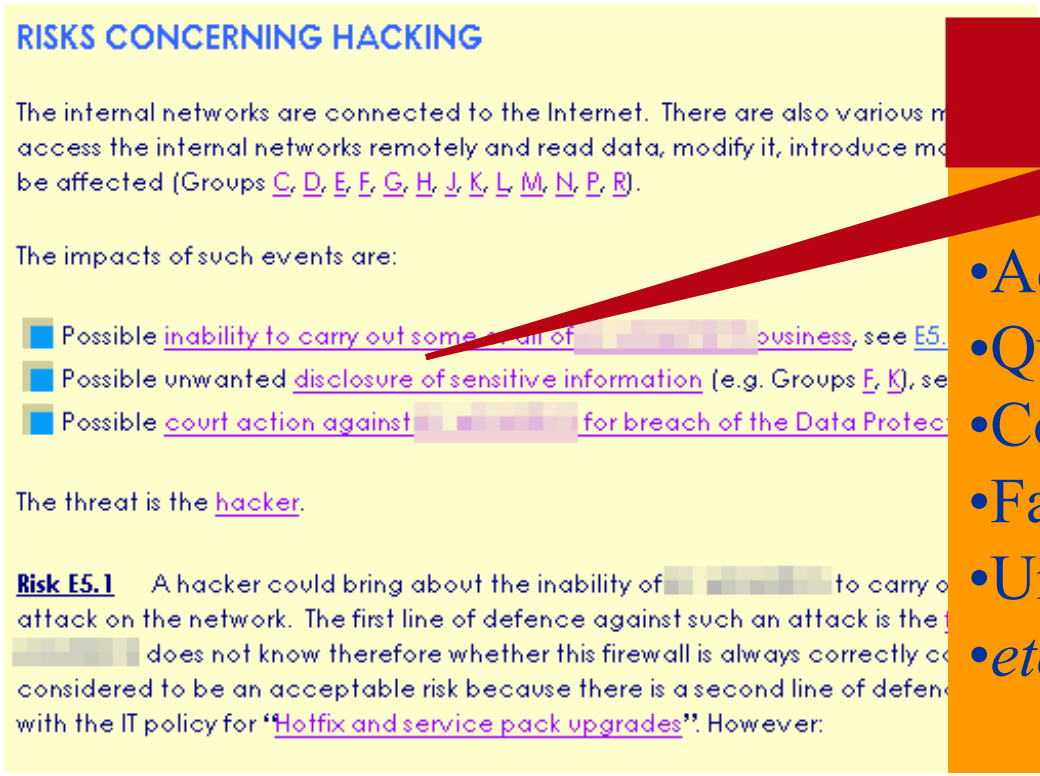
Stylised RTPs

- Business driven risk assessment/ treatment using events and impacts → making it all worthwhile



Stylised RTPs

- Business driven risk assessment/ treatment using events and impacts → making it all worthwhile



RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various m
access the internal networks remotely and read data, modify it, introduce mo
be affected (Groups C, D, E, F, G, H, J, K, L, M, N, P, R).

The impacts of such events are:

- Possible inability to carry out some [illegible] of [illegible] business, see E5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), se
- Possible court action against [illegible] for breach of the Data Protec

The threat is the hacker.

Risk E5.1 A hacker could bring about the inability of [illegible] to carry o
attack on the network. The first line of defence against such an attack is the
[illegible] does not know therefore whether this firewall is always correctly co
considered to be an acceptable risk because there is a second line of defen
with the IT policy for "Hotfix and service pack upgrades". However:

Impacts

- Adverse press coverage
- Questions in parliament
- Court action against dep
- Failure to prosecute
- Unanticipated costs
- *etc*

Limitations

- Buy and forget?
  - *NO*
  - *Risks may be common but treatment is not*
  - *PDCA cycle requires requires continuous resource*
  - *Fast track requires senior management involvement*
- Extension to other standards
  - *Not a problem*
  - *Conceived as part of a whole*
- Conclusion
  - *The "Sky" is the limit*

Summary

Summary

- Corporate governance is a modern day imperative
- Demands an effective internal control system
- BS 7799-2 provides a coherent framework
- Information risk is more than just IT (and is captured by ISO/IEC 17799)
- Fast track methods are available, but management involvement is imperative

Thank you

I will take questions in the panel later