Security - Who is in charge? - The users? Or the system?

William List

www.gammassl.co.uk

w.list@ntlworld.com

Agenda

- Introduction
- Internal Control and Corporate Governance
- Time Metrics
- Risk Treatment Plans
- Overview of the 7799 Standards
- Fast Track ISMS
- Results
- An Exercise
- Summary and conclusions

GAMMA

Introduction

GAMMA

We all live in an insecure world

Nothing is really secure

GAMMA

Old Threats

- Breakdowns
- Mistakes
- Thieves
- Fraudsters
- Terrorists - bombers
- Acts of God - flood, fire, etc

GAMMA

New Threats

- Hackers - spammers
- Viruses
- Impersonation - pfishing
- Bugs and gremlins in the systems

GAMMA

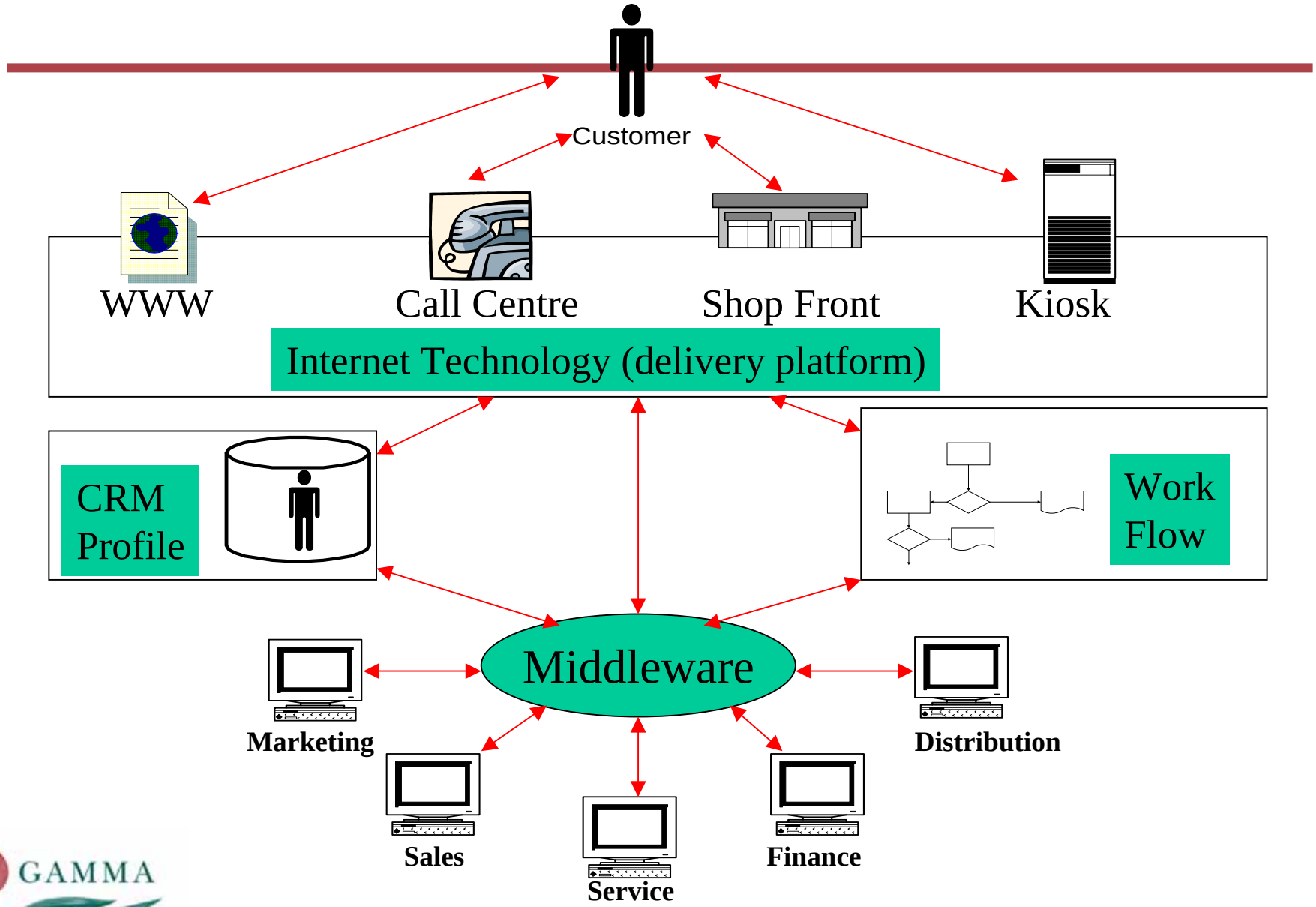
Traditional Solution

Secure the perimeter of the computer (system)

GAMMA

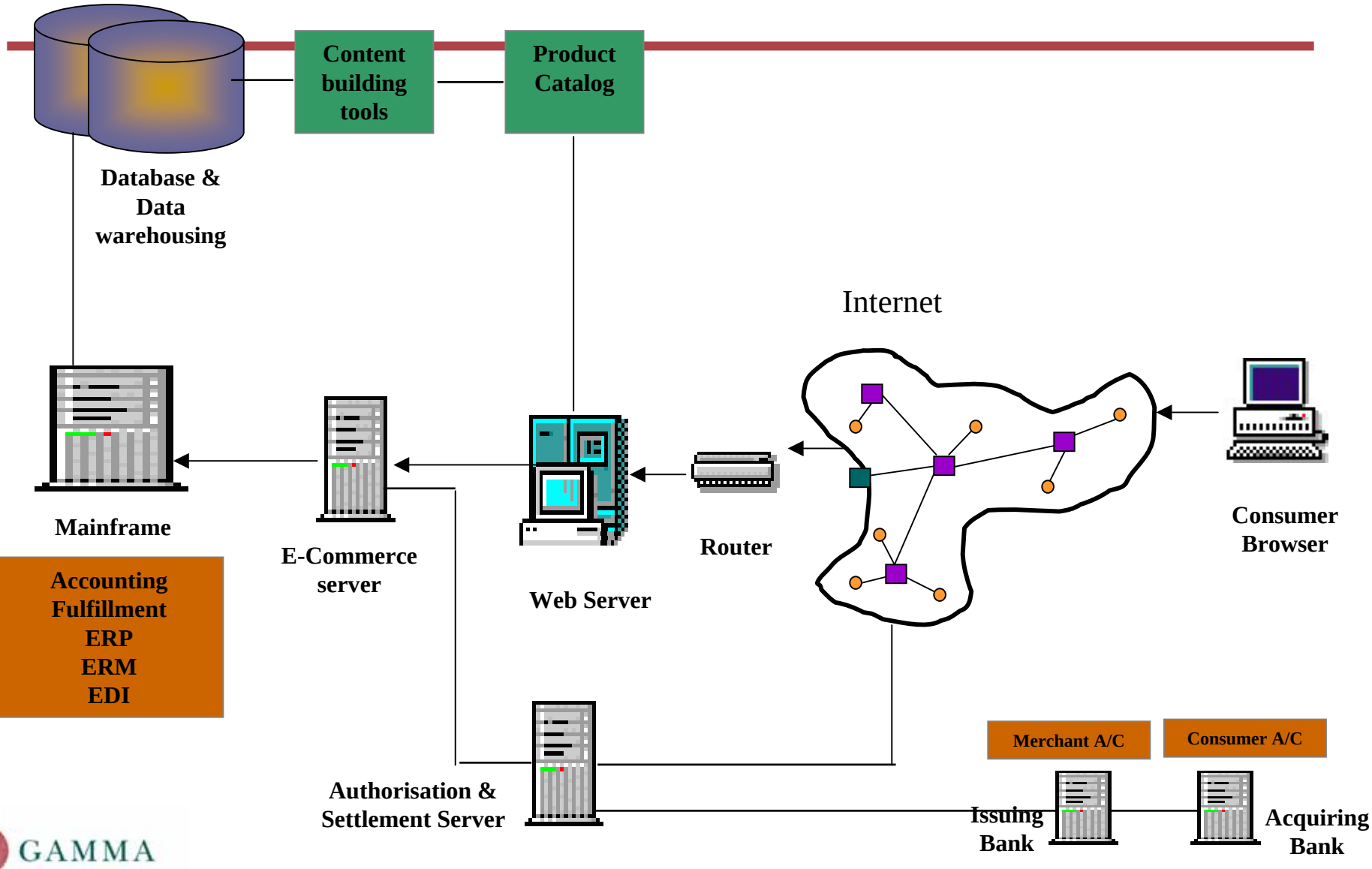
And elsewhere for E-Commerce

e-Business Structure

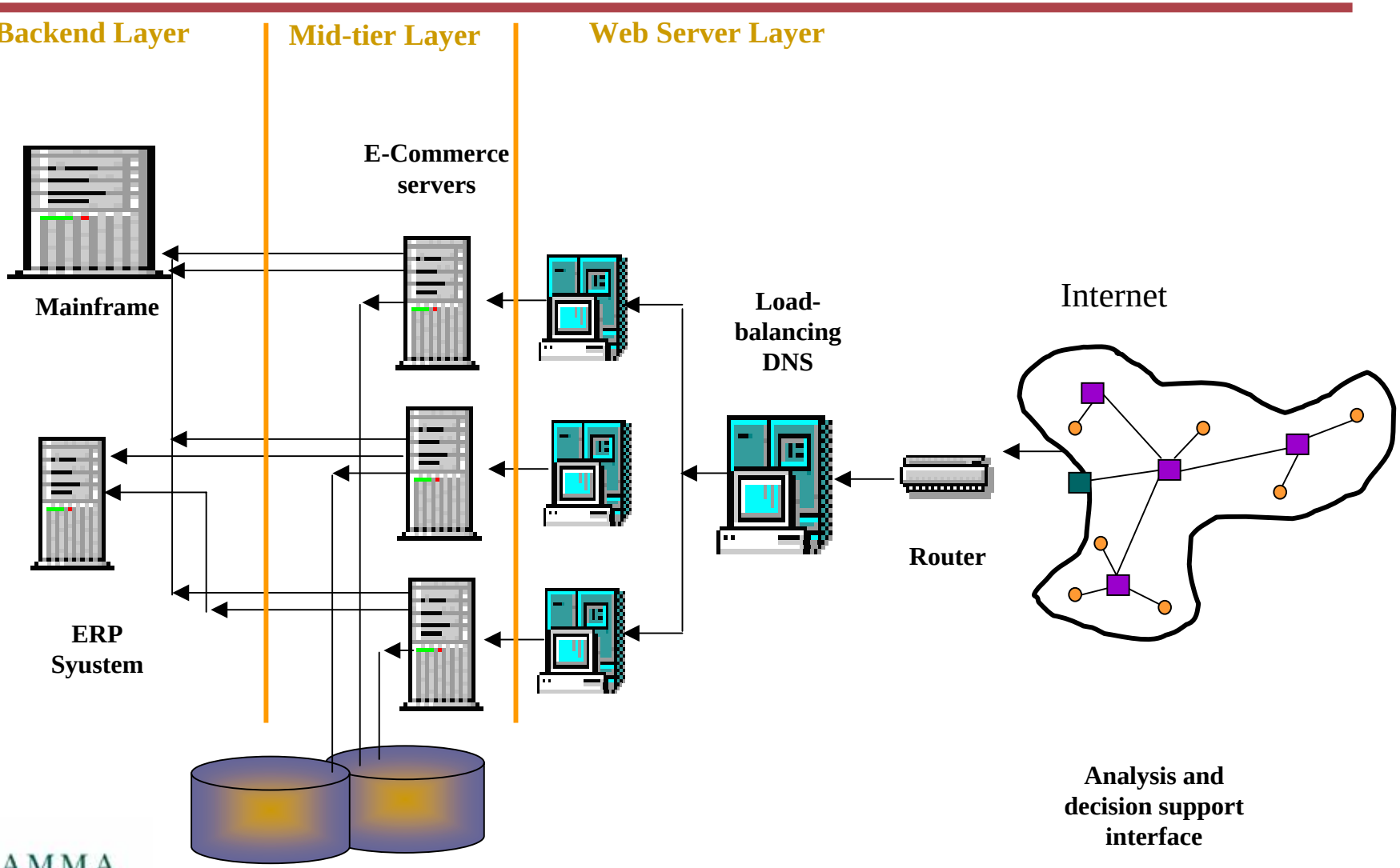


GAMMA

TYPICAL EC ARCHITECTURE



Three Tier Architectures



And we must remember that the programs are (heavily) patched and may be unstable

GAMMA

What is the system doing?

- Is it right?
- Is it authorised?
- Can I find out?

GAMMA

So what are we told?

- Rogue users compromise security
- Emails contain bad things
- Boards must be involved

GAMMA

Internal Control & Corporate Governance

GAMMA

Internal Control is an old concept

GAMMA

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

GAMMA

Audit Practice Board

- This is their advice:

GAMMA

Risks – a Taxonomy

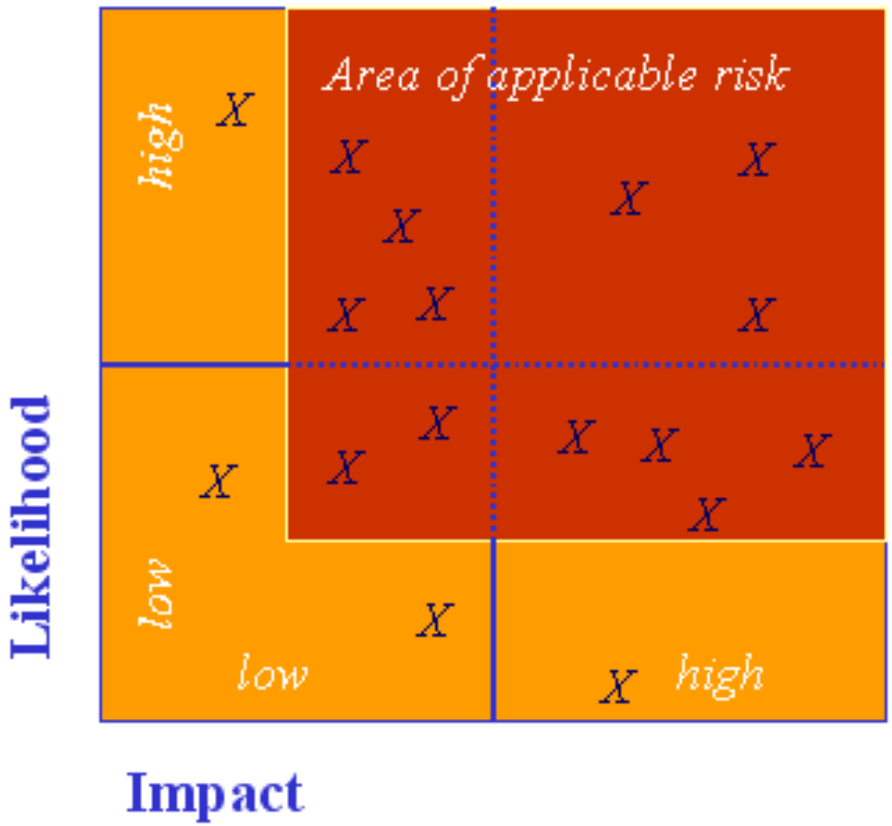
- Following Basel II

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.

GAMMA

Applicable Risks

- and non-applicable risks



Controls – Fundamentals

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

GAMMA

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

Why Corporate Governance

- ... 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, EU directive

GAMMA

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.*

GAMMA

Turnbull

- FTSE only (Yellow Book) requirement
- IC part

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'.

GAMMA

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.*

Time Metrics

GAMMA

The Fundamental Principle

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

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

GAMMA

Parameter Definition (Time)

- Time that event occurs, T_E
- Time of detection, T_D or T_M
- Time problem is fixed, T_F
- Time at which impact occurs (if not fixed), T_W

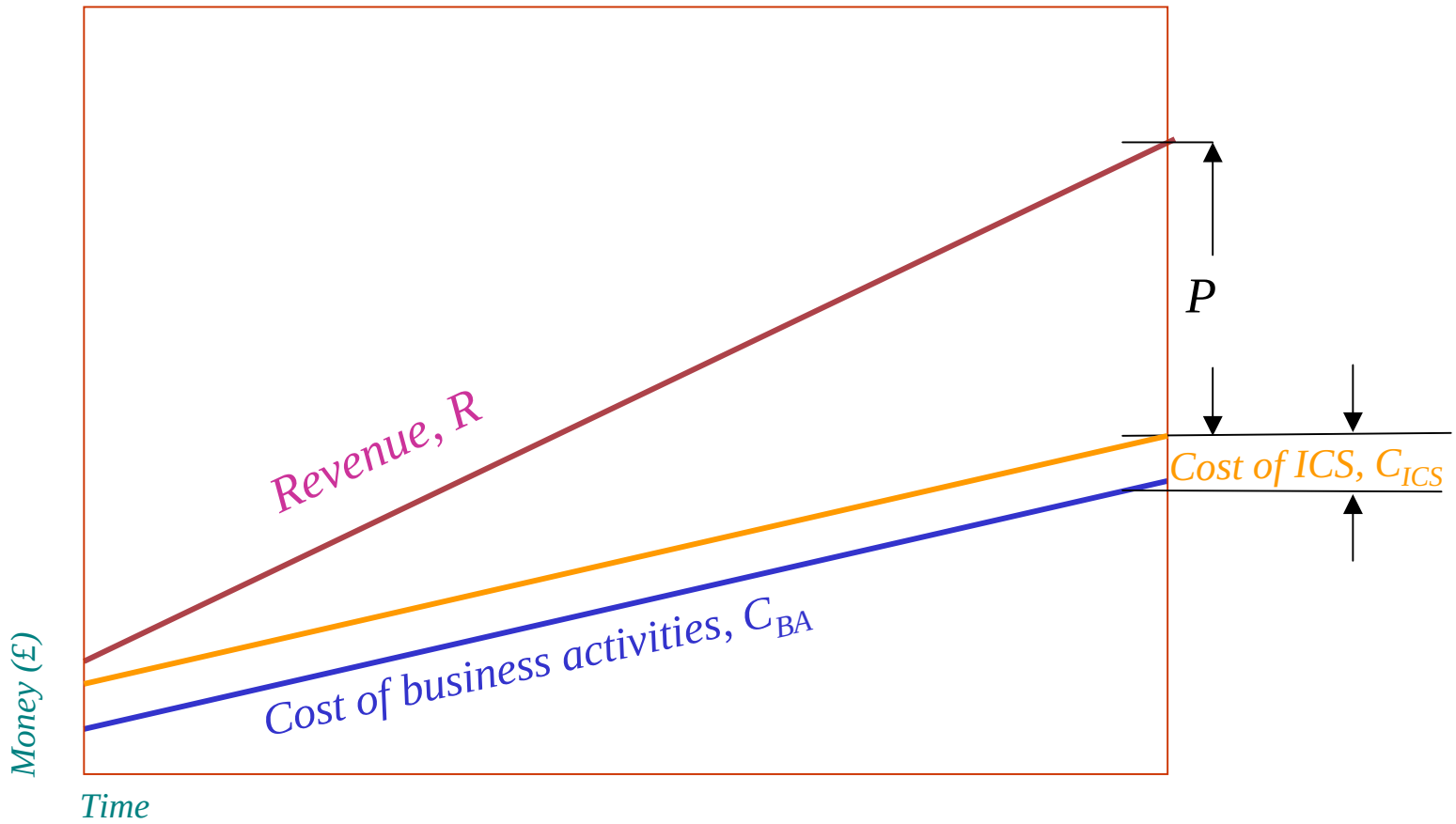
GAMMA

Parameter Definition (Money)

- Cost of doing business, C_{BA}
- Cost of internal control, C_{ICS}
- Impact penalty, I_P
- Cost of fix, C_F

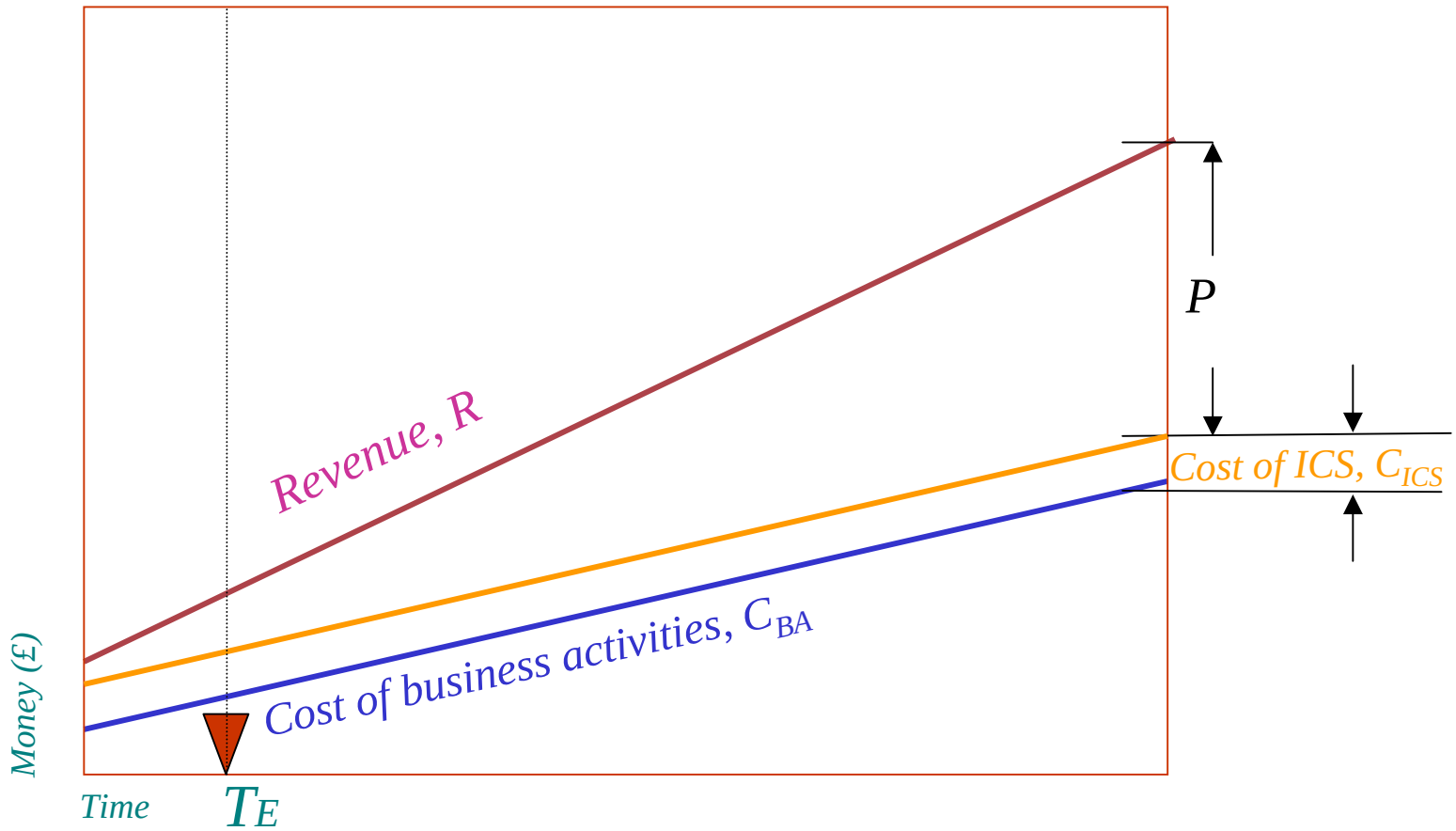
GAMMA

Fundamental Model

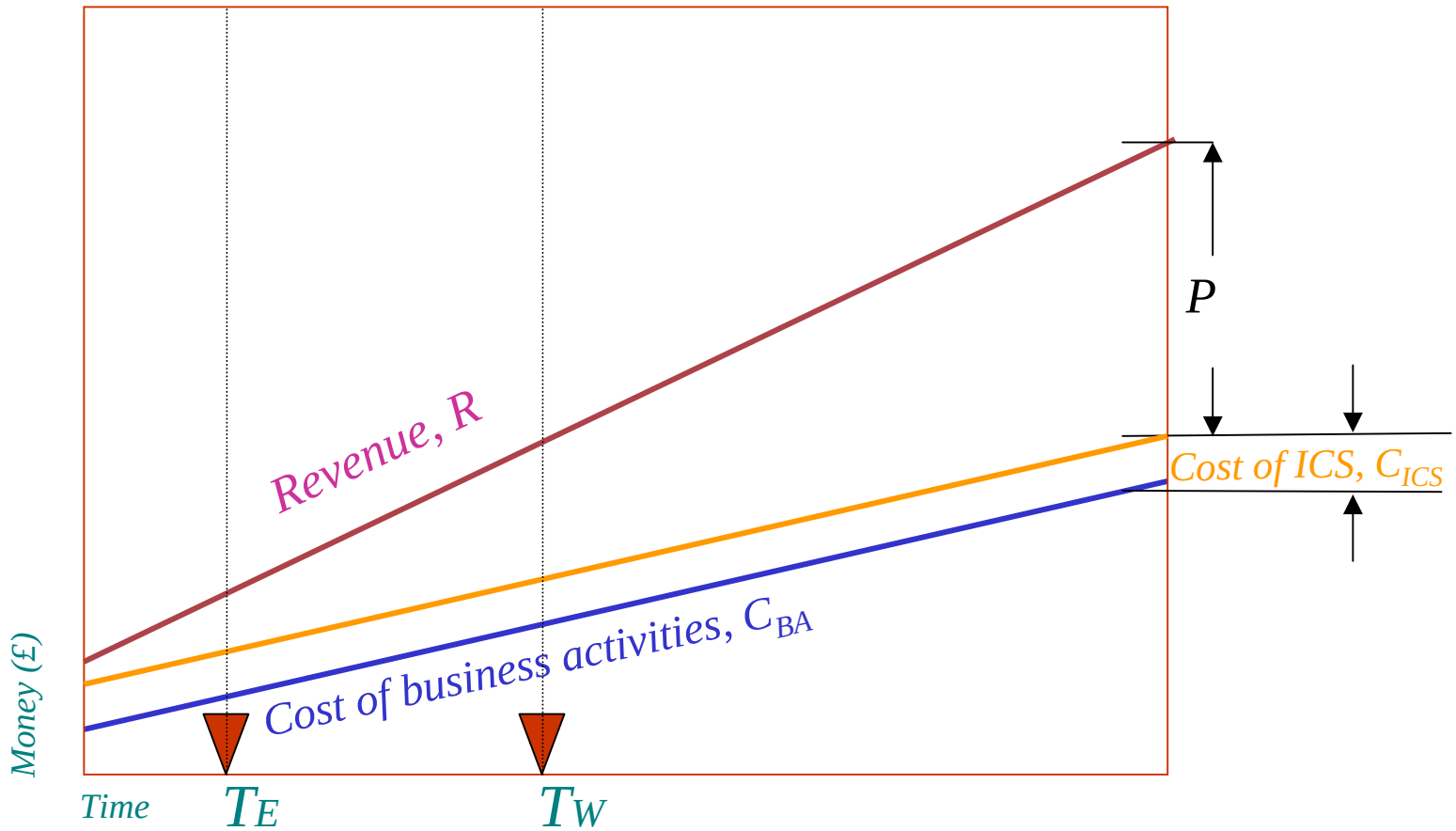


GAMMA

Fundamental Model

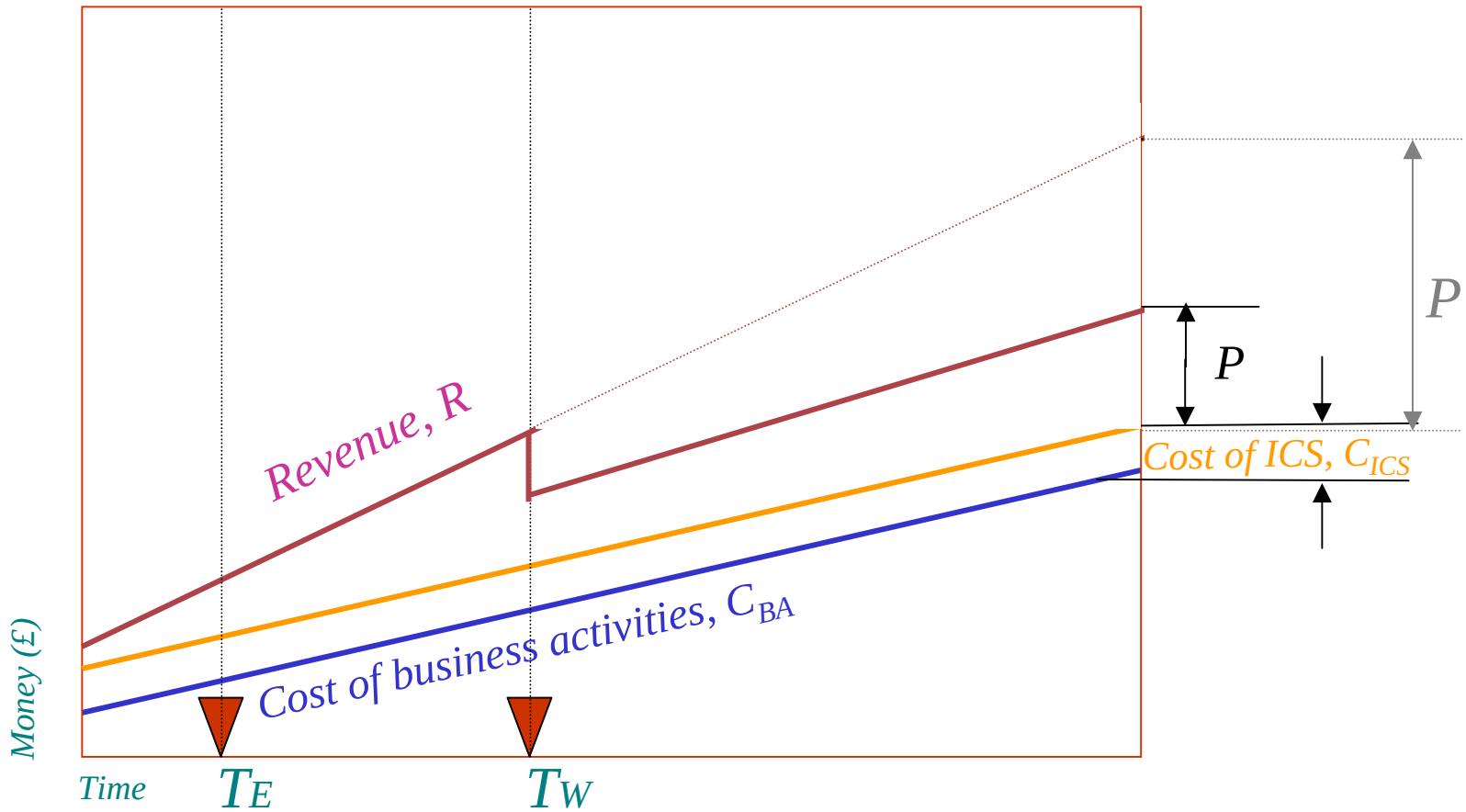


Fundamental Model

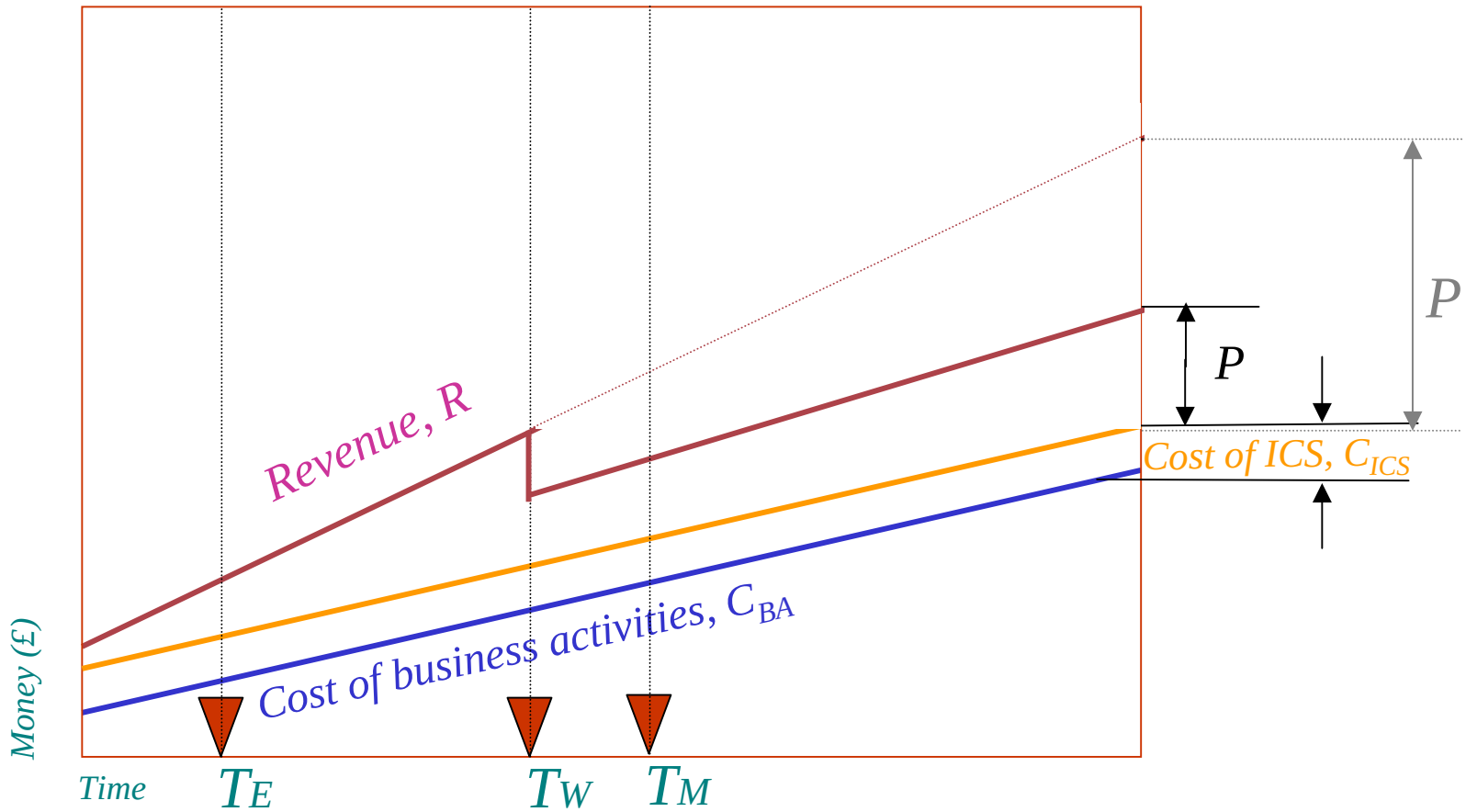


GAMMA

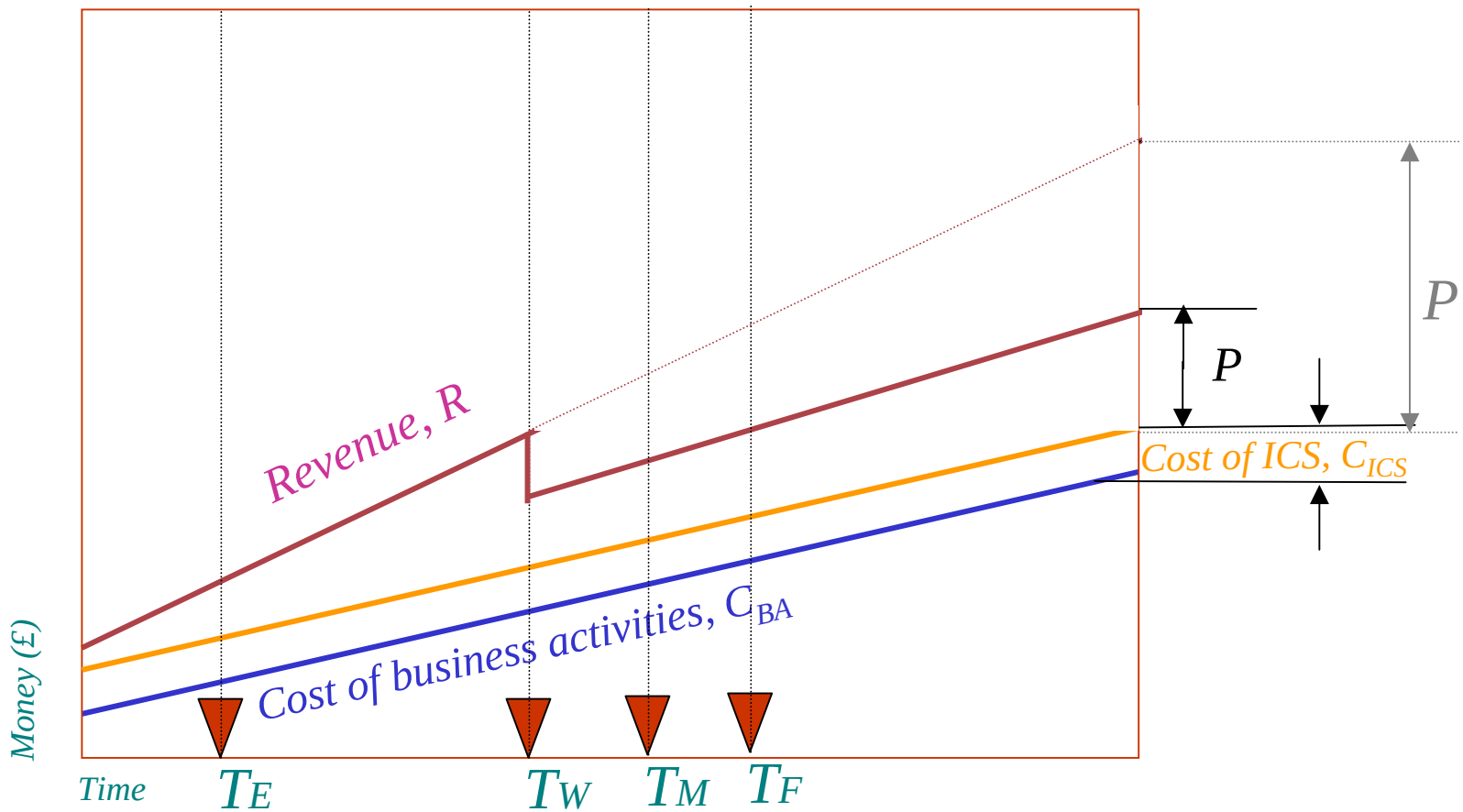
Fundamental Model



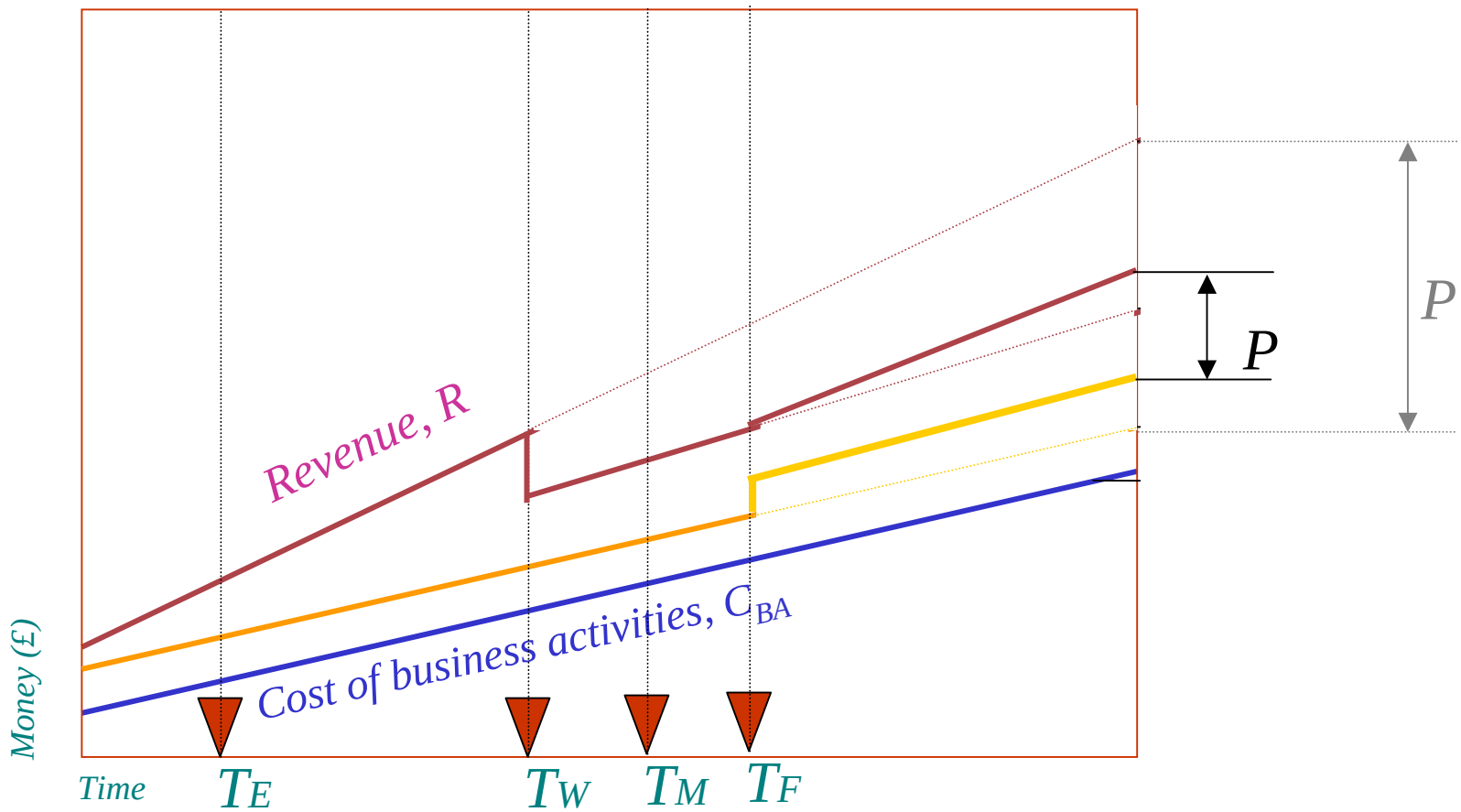
Fundamental Model



Fundamental Model

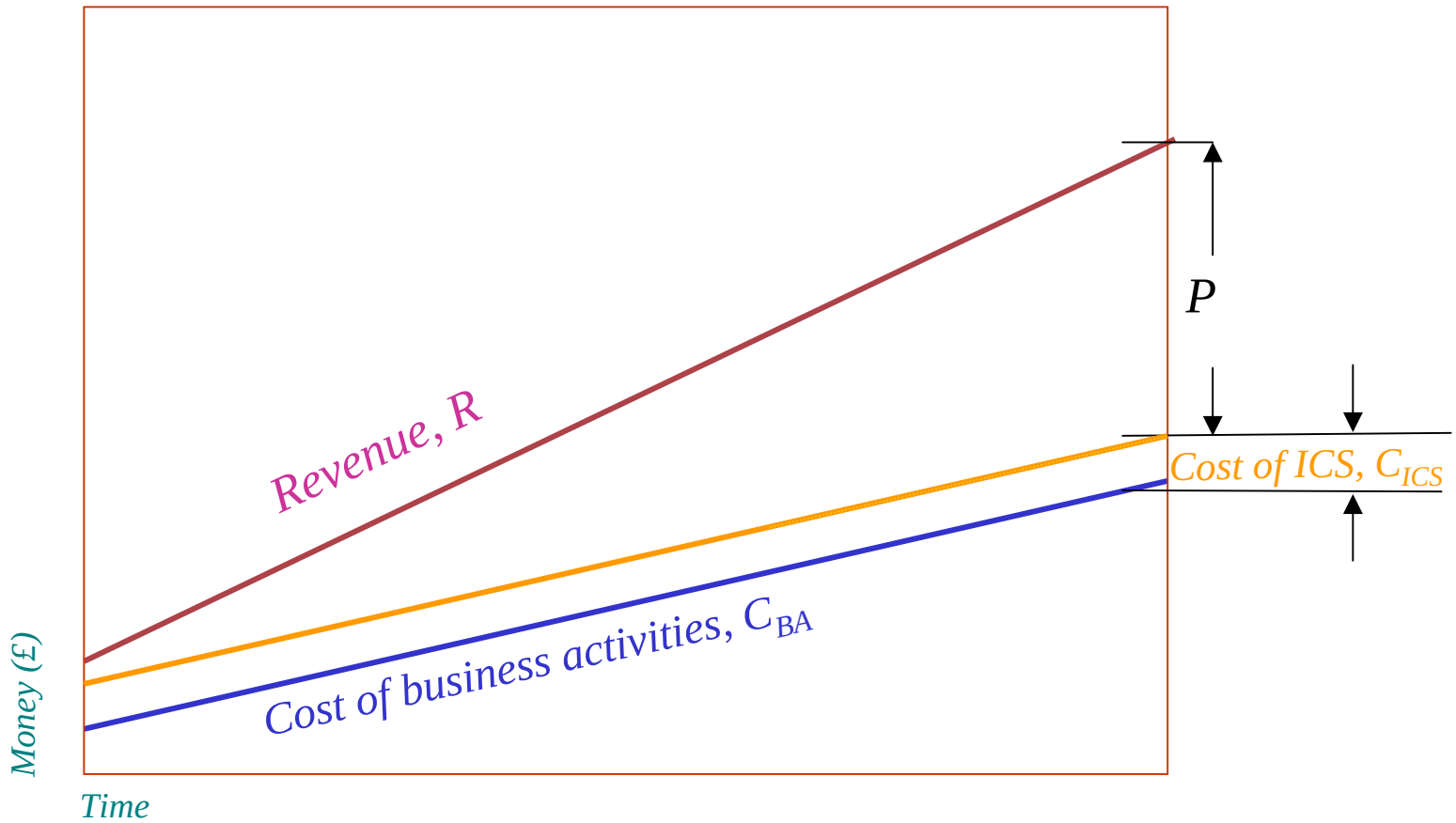


Fundamental Model



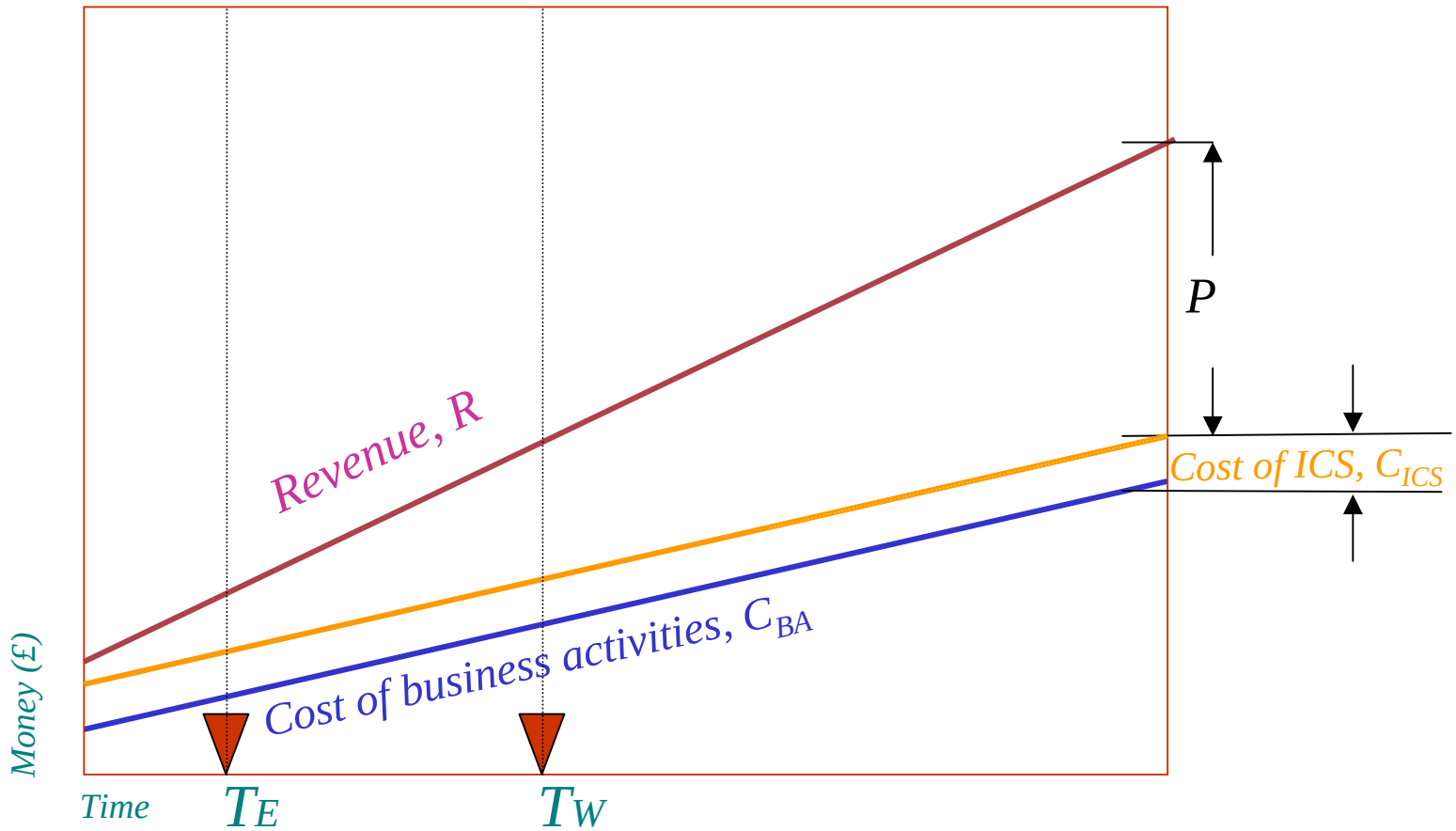
GAMMA

Fundamental Model



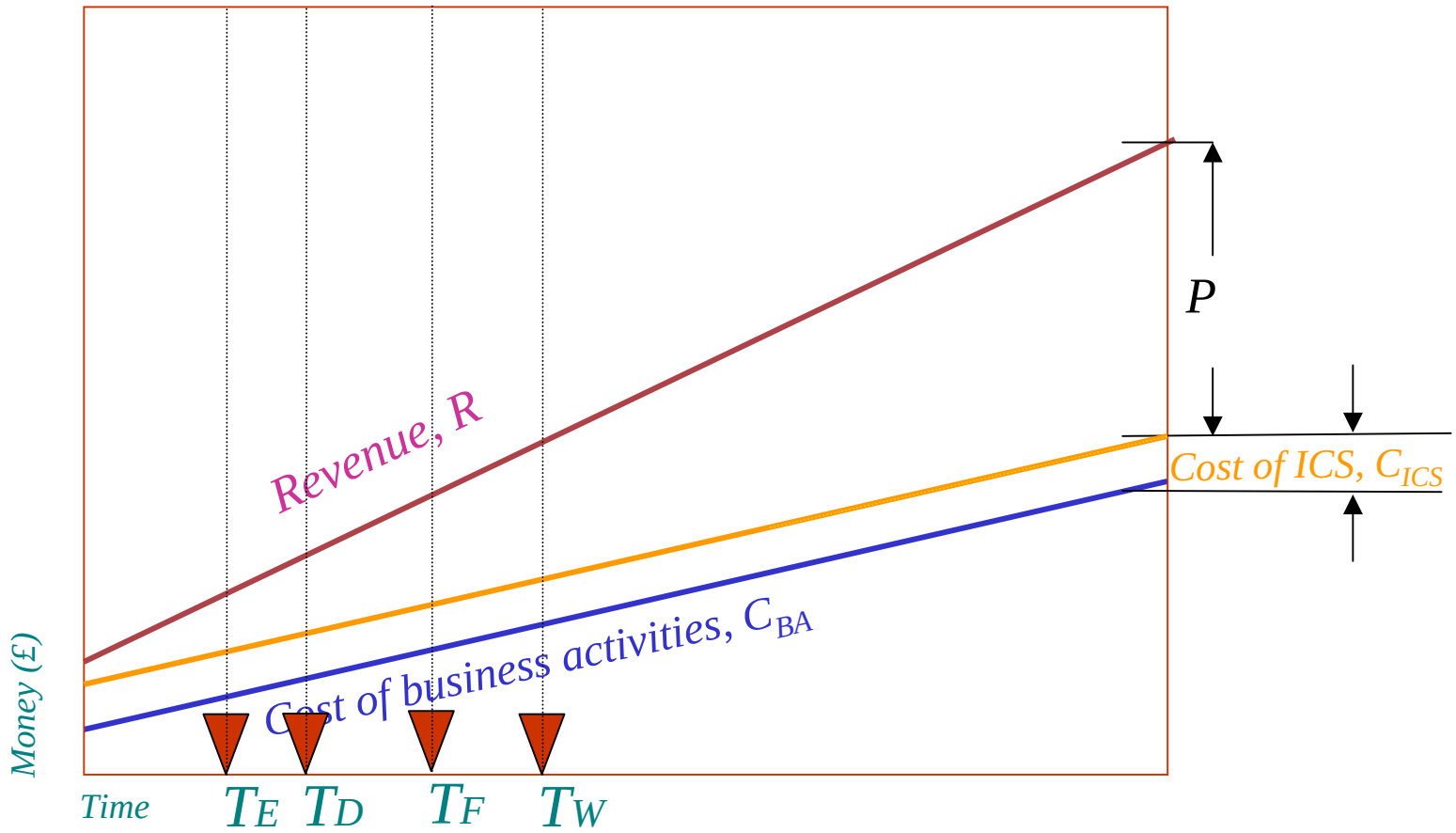
GAMMA

Fundamental Model



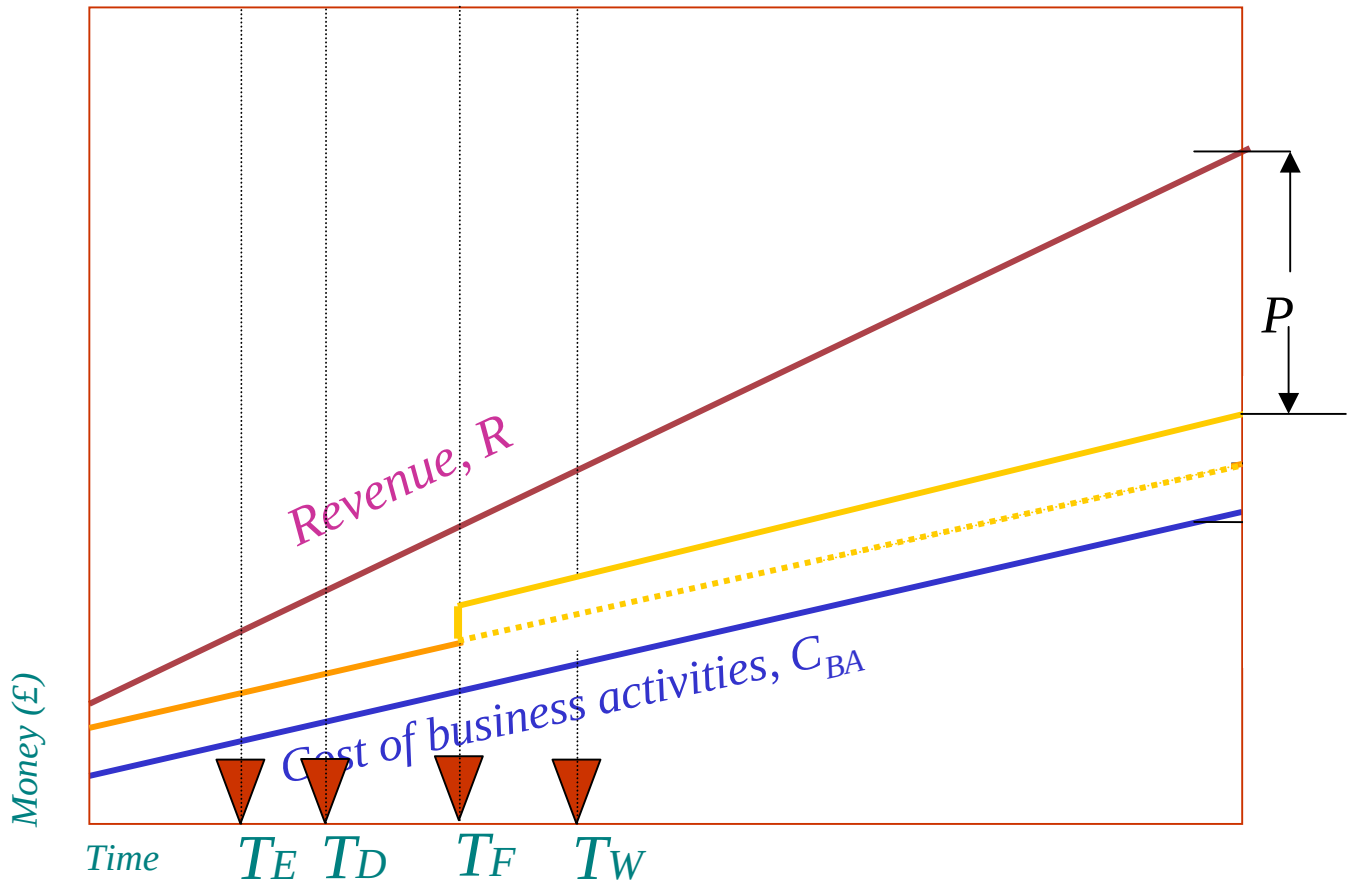
GAMMA

Fundamental Model

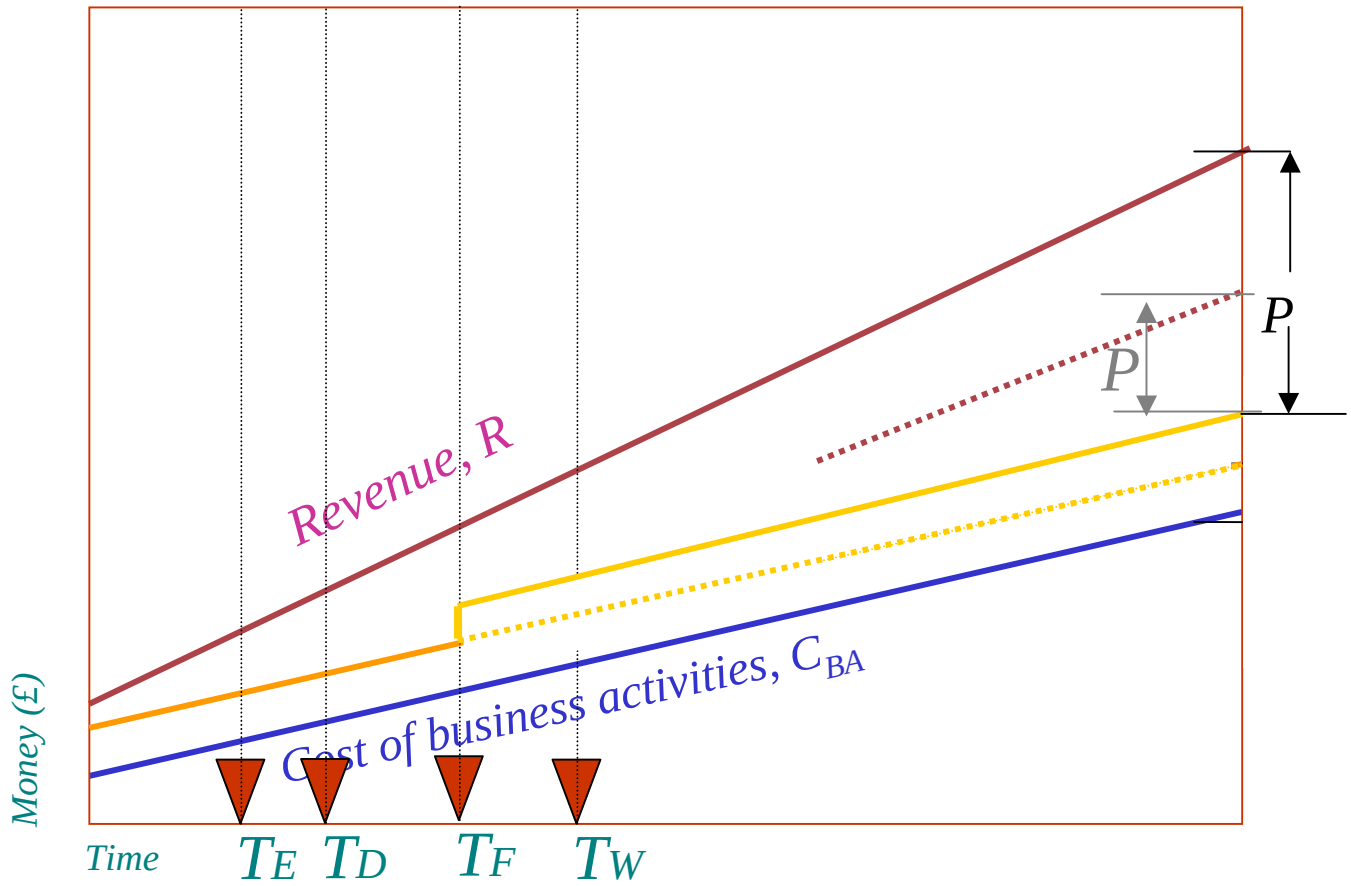


GAMMA

Fundamental Model



Fundamental Model



GAMMA

Continuum of Classes

Class	Ability to detect the event and take recovery action	Type
1	Prevents the event, or detects the event as it happens and prevents it from having any impact	Preventive
2	Detects the event and reacts fast enough to fix it well within the time window	Detective
3	Detects the event and just reacts fast enough to fix it within the time window	
4	Detects the event but cannot react fast enough to fix it within the time window	
5	Fails to detect the event but has a partially deployed BCP	Reactive
6	Fails to detect the event but does have a BCP	
7	Fails to detect the event and does not have a BCP	

GAMMA

Risk Treatment Plans

What is a Risk Treatment Plan?

- **Risk Treatment**: *treatment process of selection and implementation of measures to modify risk [ISO Guide 73]*
- Identification of risk
- Prevention of occurrence
- Detection of occurrence
- Limitation of Impact
- Recovery

GAMMA

What is a Good Risk Analysis?

- The senior management, as a whole can
  - *understand the risks*
  - *together participate in determining optimum countermeasures to risk*
  - *allocate the overall 'control' spend to various risks across the whole business*
- All staff concerned with design, implementation or performance of controls
  - *to understand why the control is necessary*
  - *to determine when an implementation of a control fails to meet its objective*
  - *to understand how failures in a control are detected*
- Enables prompt revisions to be undertaken as circumstances change or incidents occur
- NOTE The risk analysis can be in tiers if complex

GAMMA

Traditional risk analysis

- Identify
  - *Assets*
  - *Threats*
  - *Vulnerabilities*
  - *Probability of incident occurring*
- Estimate risk factor
  - *Value of loss if risk occurs*
  - *Probability of risk occurring*
  - *Complex mathematics*

GAMMA

Who knows

- All the threats - or their urgency
- All the vulnerabilities - in purchased software
- What are probabilities of occurrence

- So 9/11

GAMMA

DO THE BOARD UNDERSTAND THE RESULTS?

GAMMA

There must be
a better way to
explain the
risk treatment plan

GAMMA

Suppose we start with what worries people

GAMMA

Worries

- No Sales → Wrong product
- No Money → Competitors
- IT failed → Too expensive
- Fraud → No bribes
- Regulators
- Bad press
- Info all to pot

GAMMA

My Customers have not paid me

Bad work

Did not deliver

Did not Invoice

Customer broke

GAMMA

How to address worries

- Identify what they are
- Try to prevent
- Detect if materialised
- Limit impacts
- Recover

GAMMA

Recording the RTP

- Tell the story:
  - *How I planned to save the business*
- For example:
  - *My airplane is broken - far away*
  - *Impacts*
    - *Safety for crew and passengers*
    - *Customer satisfaction*
    - *Additional costs*

- This happen to us on BA 122 on 22nd November 2003 – read the Time Paper

GAMMA

Stylised RTPs

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

Organisation Specific

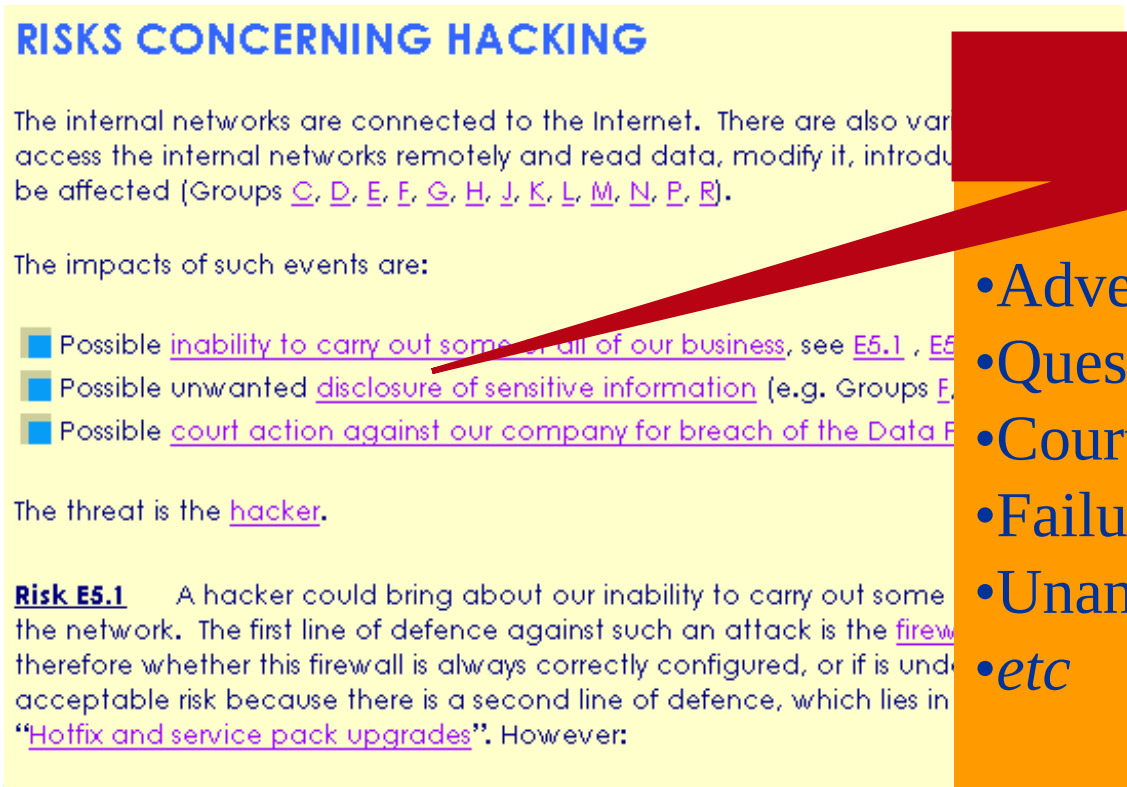
Common (but treatment might be different!)

Event

- Aircraft broken down
- Bagage handler strike
- Theft
- Acts of God
- Regular Fraud
- IT failure
- Hacking
- *etc*

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 var
access the internal networks remotely and read data, modify it, introdu
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 or all of our business, see E5.1 , E5
- Possible unwanted disclosure of sensitive information (e.g. Groups F,
- Possible court action against our company for breach of the Data P

The threat is the hacker.

Risk E5.1 A hacker could bring about our inability to carry out some
the network. The first line of defence against such an attack is the firew
therefore whether this firewall is always correctly configured, or if is und
acceptable risk because there is a second line of defence, which lies in
"Hotfix and service pack upgrades". However:

Impacts

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

Method

- One RTP per event
- Describe event
- List assets that might be affected
- Document, order applicable impacts
- List applicable threats
- Repeat until all impacts dealt with, and residual risk is acceptable:
  - *How can it happen?*
  - *Do I prevent it?*
  - *How do I detect it?*
    - *No preventive measure or*
    - *Preventive measure fails or*
    - *Didn't know it could happen that way*
  - *How do I fix/recover?*

GAMMA

Overview of the 7799 Standards

GAMMA

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

GAMMA

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

Linking the Two Standards

- The Statement of Applicability (SOA):

  "a document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes"

- It is a certification requirement (EA7/03)

GAMMA

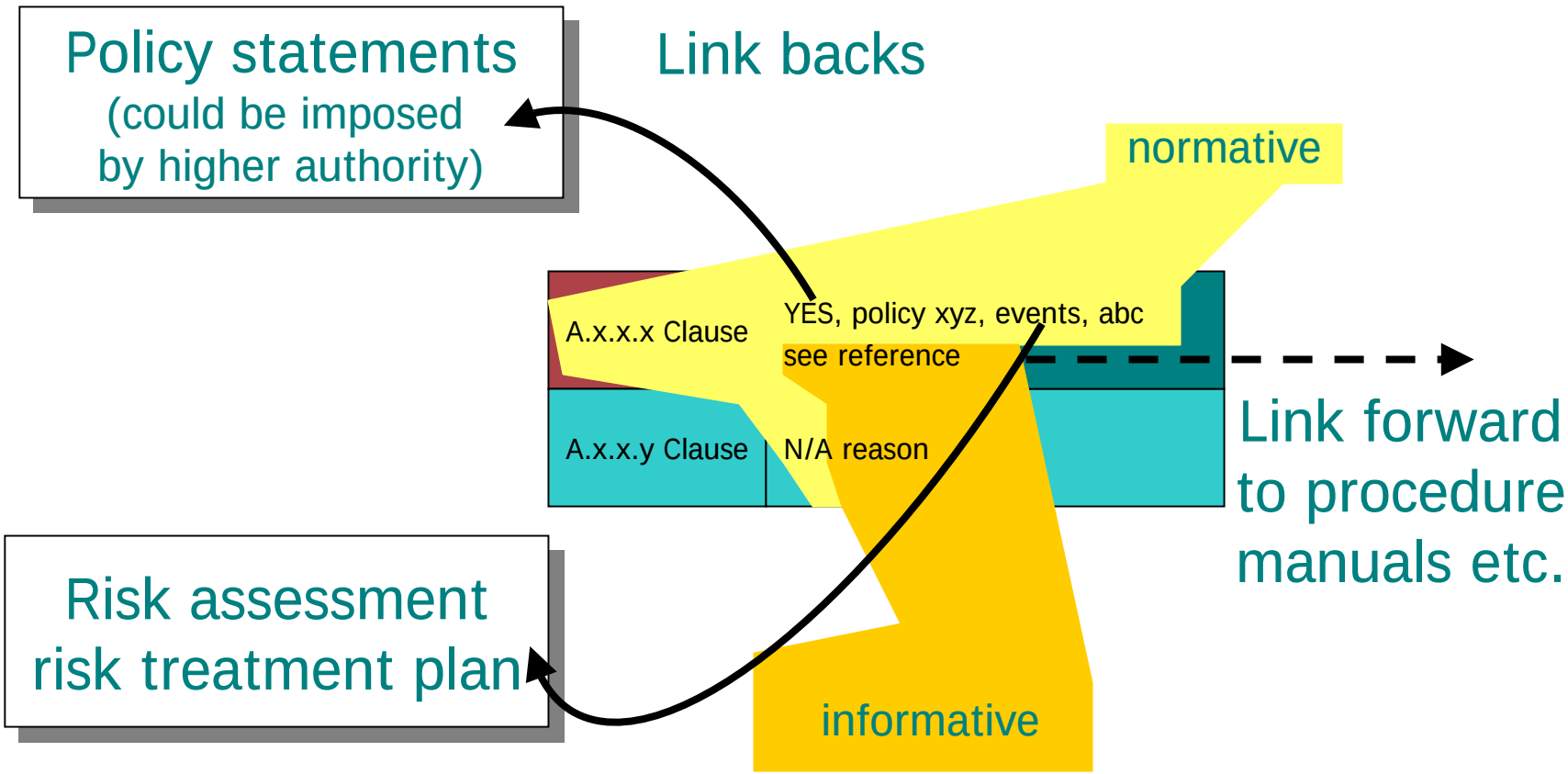
Why is it Important?

			BS ISO/IEC 17799:2000 numbering
A.3.1 *Information security policy* *Control objective*: To provide management direction and support for information security.			3.1
Controls			
A.3.1.1	*Information security policy document*	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.	3.1.1
A.3.1.2	*Review and evaluation*	The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate	3.1.2

- You have to say, for all 127 ISO/IEC 17799 controls, whether they are applicable or not
- If YES, why (with reference to risk assessment)
- Important because everyone uses the same laundry list

GAMMA

A Practical Implementation



Fast Track ISMS

GAMMA

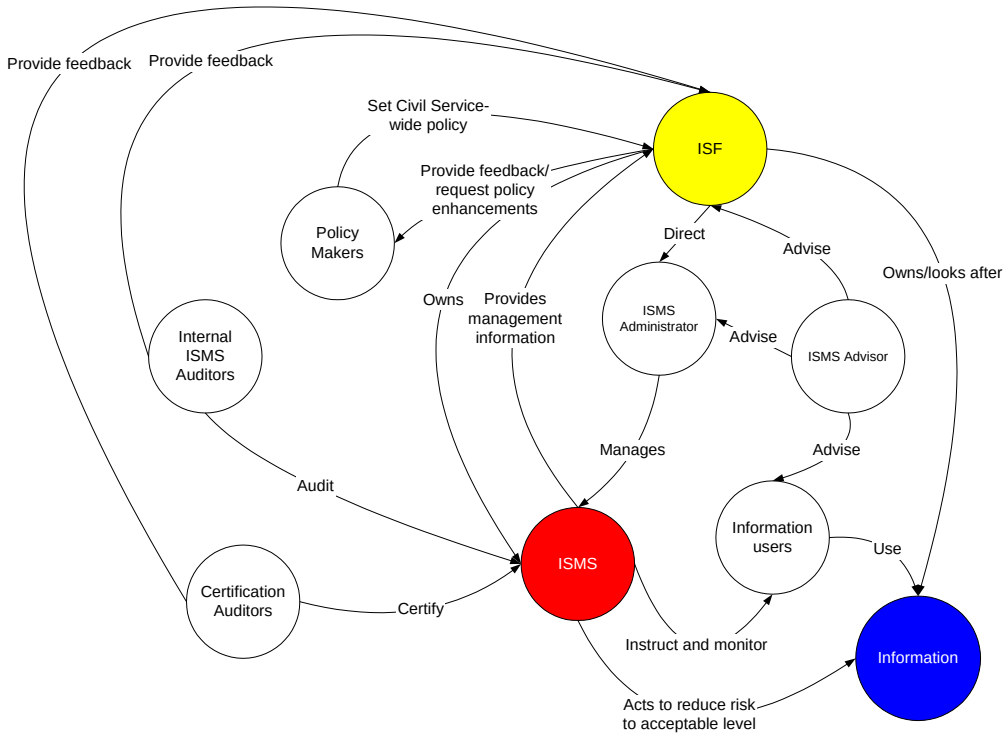
The Vital Ingredients

- Role Model
- Skeleton ISMS Manual
- The event-impact driven RTPs (as previously discussed)
- Classroom and on-the-job training
- Various quality assurance activities

GAMMA

Role Model

- Information Security Forum (ISF)
- ISMS Administrator
- Internal ISMS Auditor
- ISMS Trainer
- ISMS Advisor
- Certification Auditor
- Policy Maker



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
031025

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

Contents

- Pages associated with the whole PDCA cycle
- Built-in facility for document control
- Space to define ISMS scope and context
- Prototype ISMS policy
- Provision for RTPs
- Virtually complete SOA (with built-in hyperlinks to policy statements and standard events)
- Facility for including training and awareness
- Internal ISMS audit proforma and checklist
- Management system review checklist
- Procedures for corrective action etc.
- To-Do-List and associated procedures
- Compliance index

GAMMA

The "To-Do-List"

- BS 7799-2 is a management standard – so is internal control
- Management processes must be in place, but new security processes may be required because risks change
- At any point in time:
  - *Existing security procedures in place*
  - *Newly identified ones still-to-do*
- Managed using a "To-Do-List"

GAMMA

The "To-Do-List"

- BS 7799-2 is a management standard – so is managed using a "To-Do-List"

The To-Do-List

Reference	Action	Target Date	Comment/ Completion Date
Extend scope of MS to include BS7799-2	Produce SOA	040402	040331
	Produce scope statement	040402	040331
	Produce context (i.e. information architecture)	040402	040331
	Integrate checklists into current MS, modify existing MS Review practice accordingly	040402	040331
	Produce RTPs (just the standard 8) and link with business risk analysis	040402	040331
	Insert compliance statement from Skeleton and check all cross refs	040402	040331

GAMMA

Results

Some Results

- UK Logistics Company
  - *Initial development of Skeleton*
  - *First application of event-impact driven RA/RTPs*
  - *Engaged Board*
  - *MD in control*
- Government of Mauritius
  - *4 sites "attested" by MSB*
  - *Chiefs empowered*
  - *Rollout to all other departments*
- UK start-up
  - *Up to speed in a day*
  - *2 day brainstorm for RTPs*
  - *First BSI visit in September*

GAMMA

Principle can be extended

- Overall ICS
- Including
  - *ISO 9000*
  - *Financials*
  - *General management issues*

GAMMA

Now an audience participation exercise

Identity Cards

Summary and Conclusions

GAMMA

Computers help people

- PCs, mobile phones, mainframes, servers etc
- Could we do without them?
  - *Volume of transactions*
  - *Speed of communications*
- Criminals are businesses too

GAMMA

Summary

- Information security part of internal control
- Time metrics key to effectiveness
- Event-impact driven RA/RTPs key to Board engagement
- Hypertext, web-technology Skeleton key to rapid development
- Certification successes bear this out

GAMMA

Security - Who is in charge? - The users? Or the system?

William List

www.gammassl.co.uk

w.list@ntlworld.com