

The Relevance of the Common Criteria to Sarbanes-Oxley and Corporate Governance

*Dr. David Brewer,
www.gammasl.co.uk &
William List, CA, Hon FBCS, CIPT
w.list@ntlworld.com*

Objective

“For many chief executives, concerned with meeting their organisation’s business objectives whilst complying with new legislation such as Sarbanes-Oxley, the utility of the Common Criteria must seem an irrelevance. Yet there is an important link.”

➤ **What is it?**

Agenda

- Overture (corporate governance ...)
- Effectiveness of internal control
- Case for the Common Criteria
- Summary and recommendations

OVERTURE

Corporate Governance

- Laws and regulations since 19th century
- Anti-discrimination, directors' conduct,...
- ... and a result of scandals
 - South Sea Bubble, Kruger, Salad Oil company, Equity Funding, Polly Peck, Maxwell Pensions, Enron, WorldCom
- Sarbanes-Oxley, EC Directive, OECD, Turnbull ...

Internal Control

- CG requirement
- Means to achieve objectives
 - Operational procedures
 - Controls
- Deming cycle (PDCA)
- Common to ISO 9001, BS7799-2 etc..



Extensiveness of Business Risk

- 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 ...
<u>Project risk</u>	... default by a creditor (which will usually be a customer).	... doing work and not making a profit.
<u>Trading risk</u>	... changes in trading positions when prices move adversely.	... our money and other assets not being worth as much as they ought.
<u>Market risk</u>	... 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.
<u>Existence risk</u>	... the fact that we exist.	... spending money unnecessarily.

How Information Security Fits

- Information security is part of internal control
 - Institute of IT Governance
 - Our experiences
- Information security is more than IT
- Exemplar - Gamma's ICS

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.

Ex	ORP	Yes	No	G1
	ORP9	The company's IT systems are ineffective in enabling us to carry out the contracted work.	Yes	If the IT isn't up to the job, or the business applications do not work as they should, the work will take longer than it ought, representing poor value for money to the customer. However, it is not judged as being significant, given the current policy for replacing and upgrading the company's IT every two years, and making special purchases when necessary.
	ORP10	We are unable to deliver our product on time.	No	Judged as being increasingly likely and potentially significant, with increased file sizes and the

RISKS CONCERNING NON-APPLICABLE RISKS

It is possible that a non-applicable risk becomes an applicable risk.

All assets could be affected, but primarily Asset Groupe Y, Z.

RISKS CONCERNING IT FAILURE

Gamma is reliant on its IT. The technology could fail for a wide variety of reasons and in a wide variety of manners. Broadly speaking, the failure will result in unavailability, loss of integrity and/or loss of confidentiality. Note that integrity also implies that information is sufficiently right for the purpose for which it is used at the time that it is used, and not just that data has been modified without authorization or in error. All IT based assets could be affected (Groups E, E, I, J, K).

The impacts of such events are:

- Possible inability to carry out some or all of Gamma's business, see S4.1a, S4.1b, S4.1c, S4.1d, S4.1e
- Possible unauthorised disclosure of information, see S4.2

The principal threats are backup failure, errors, utility failure, software failure and

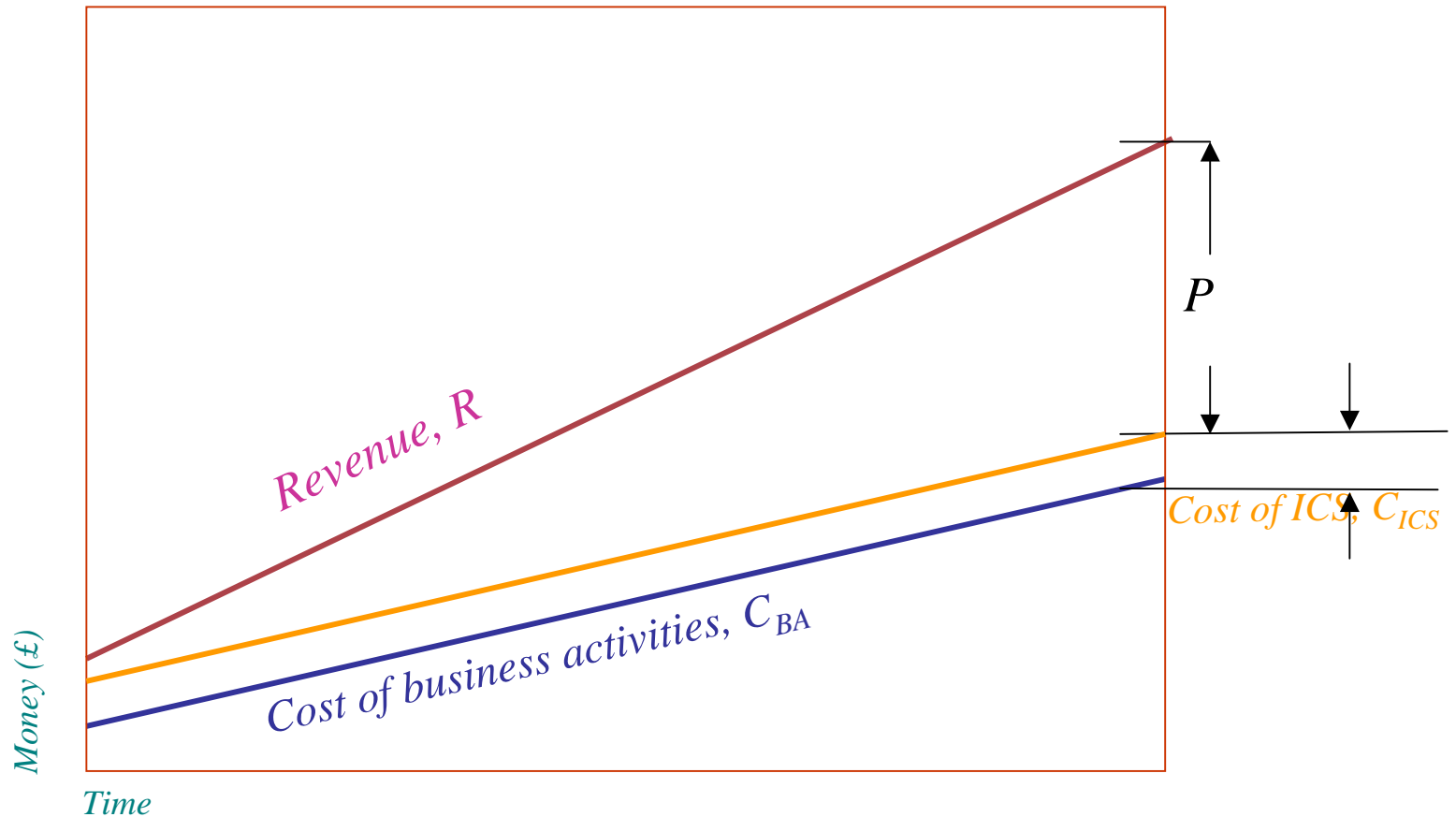
EFFECTIVENESS OF INTERNAL CONTROL

Time Metrics

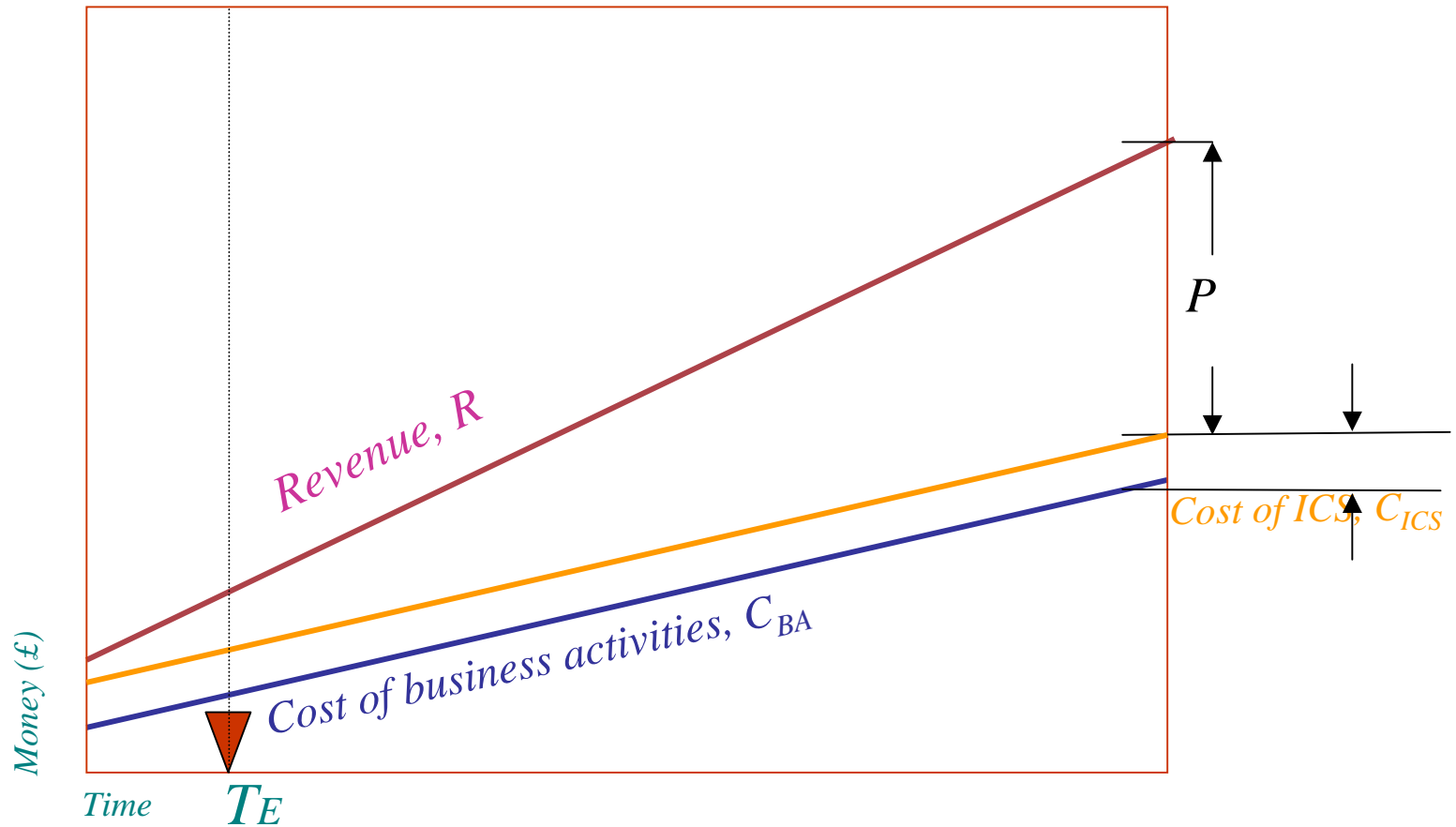
“... detect the event in sufficient time to do something positive about it...”

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

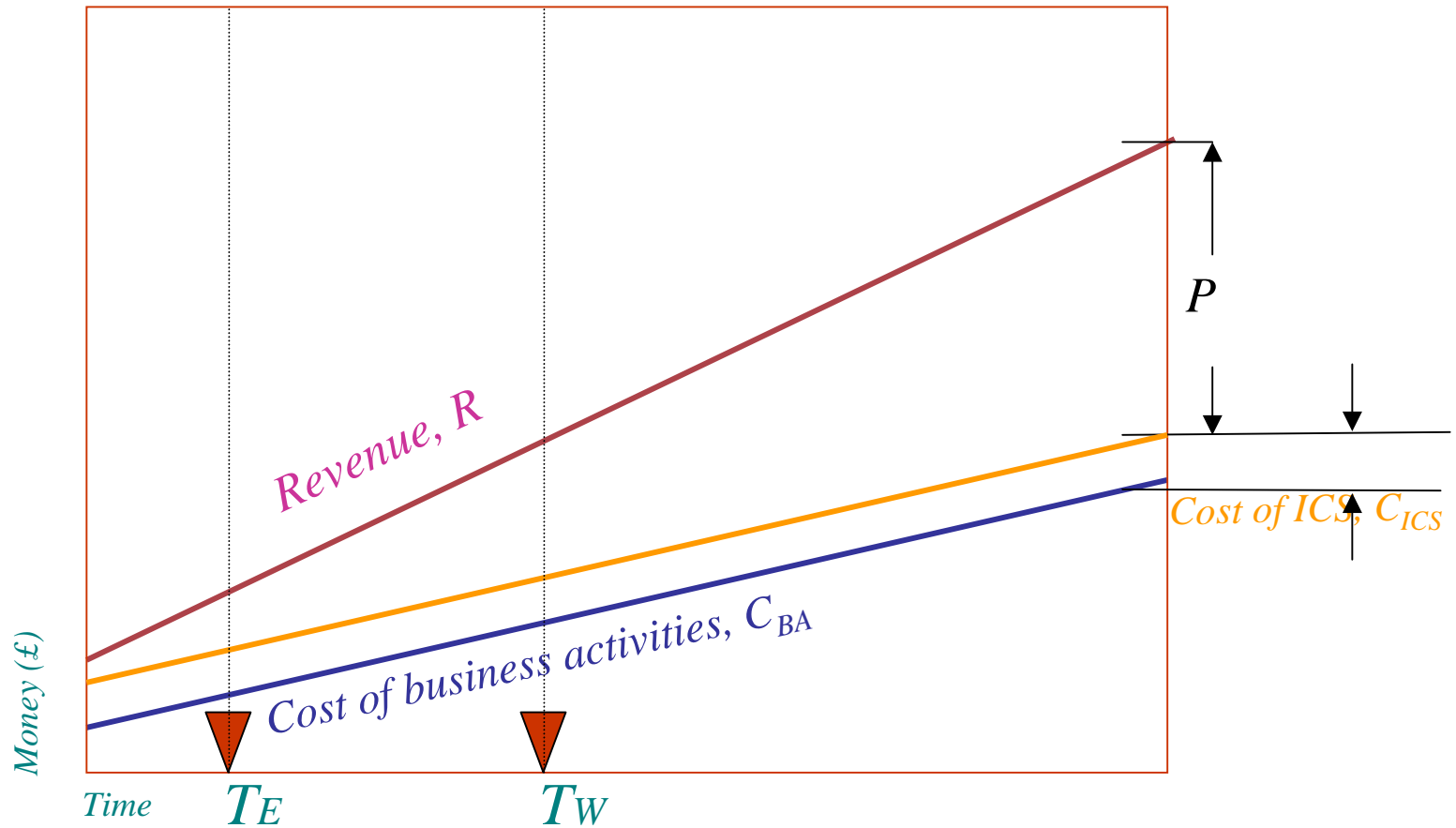
Fundamental Model (too late)



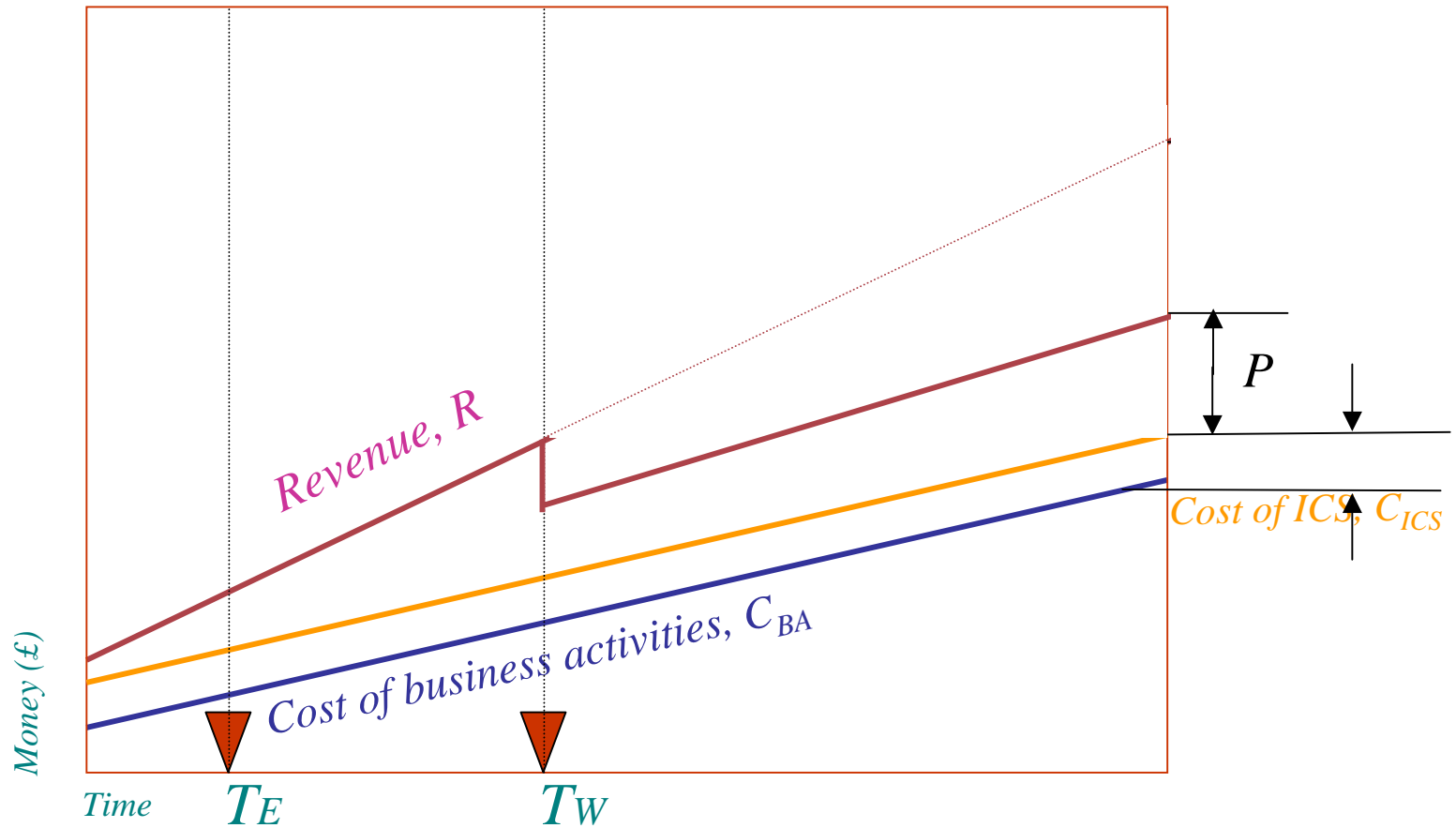
Fundamental Model (too late)



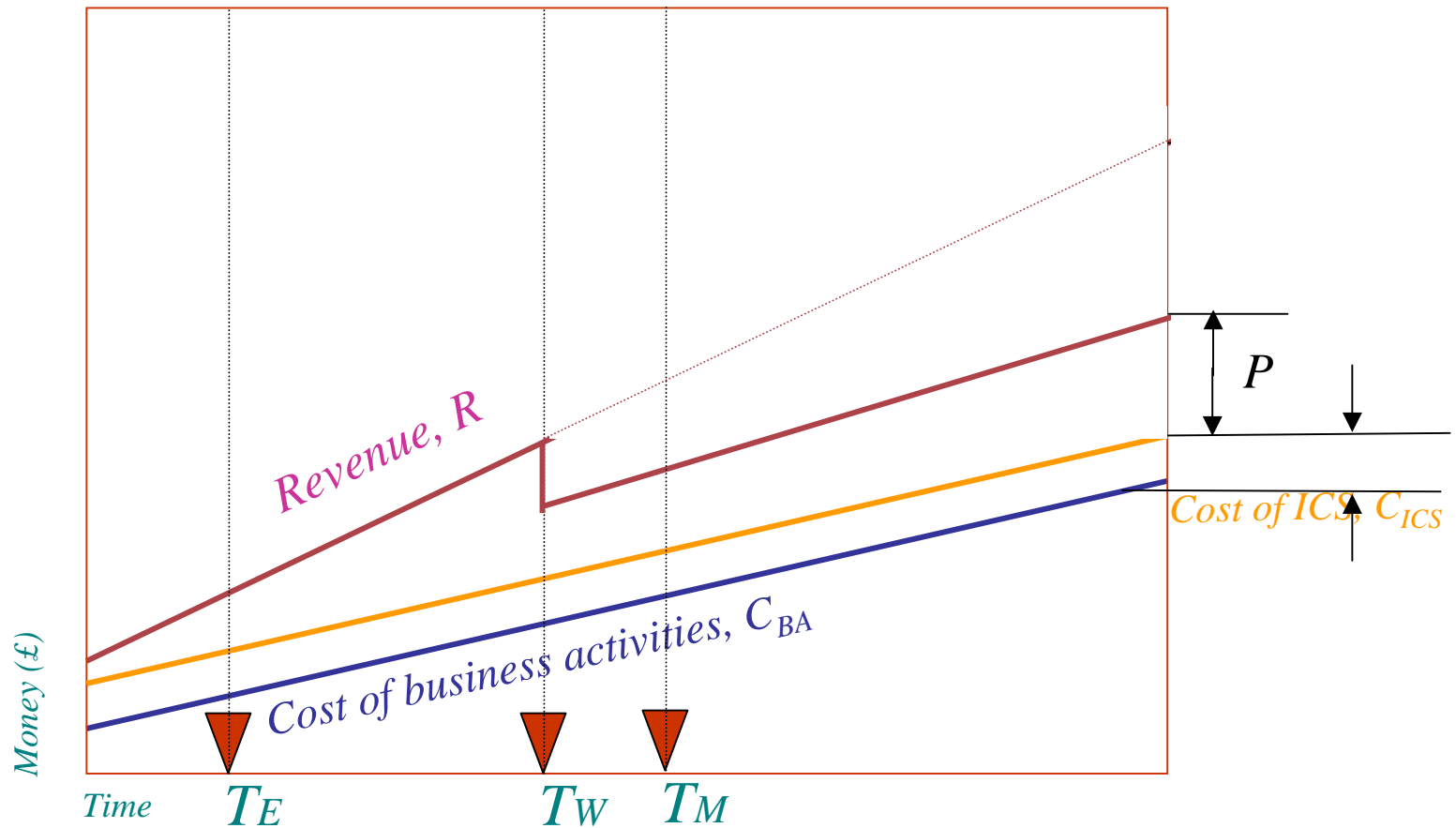
Fundamental Model (too late)



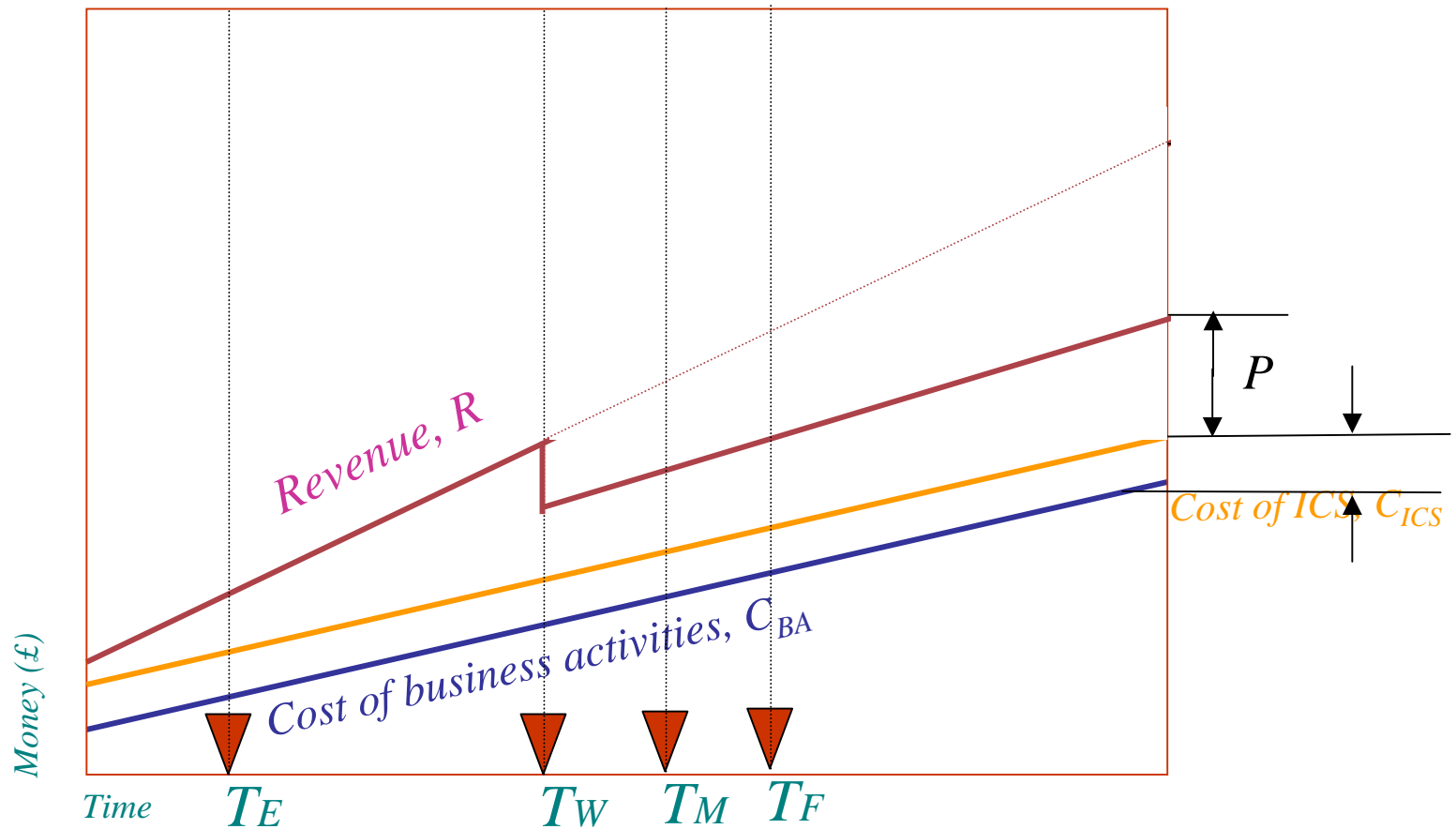
Fundamental Model (too late)



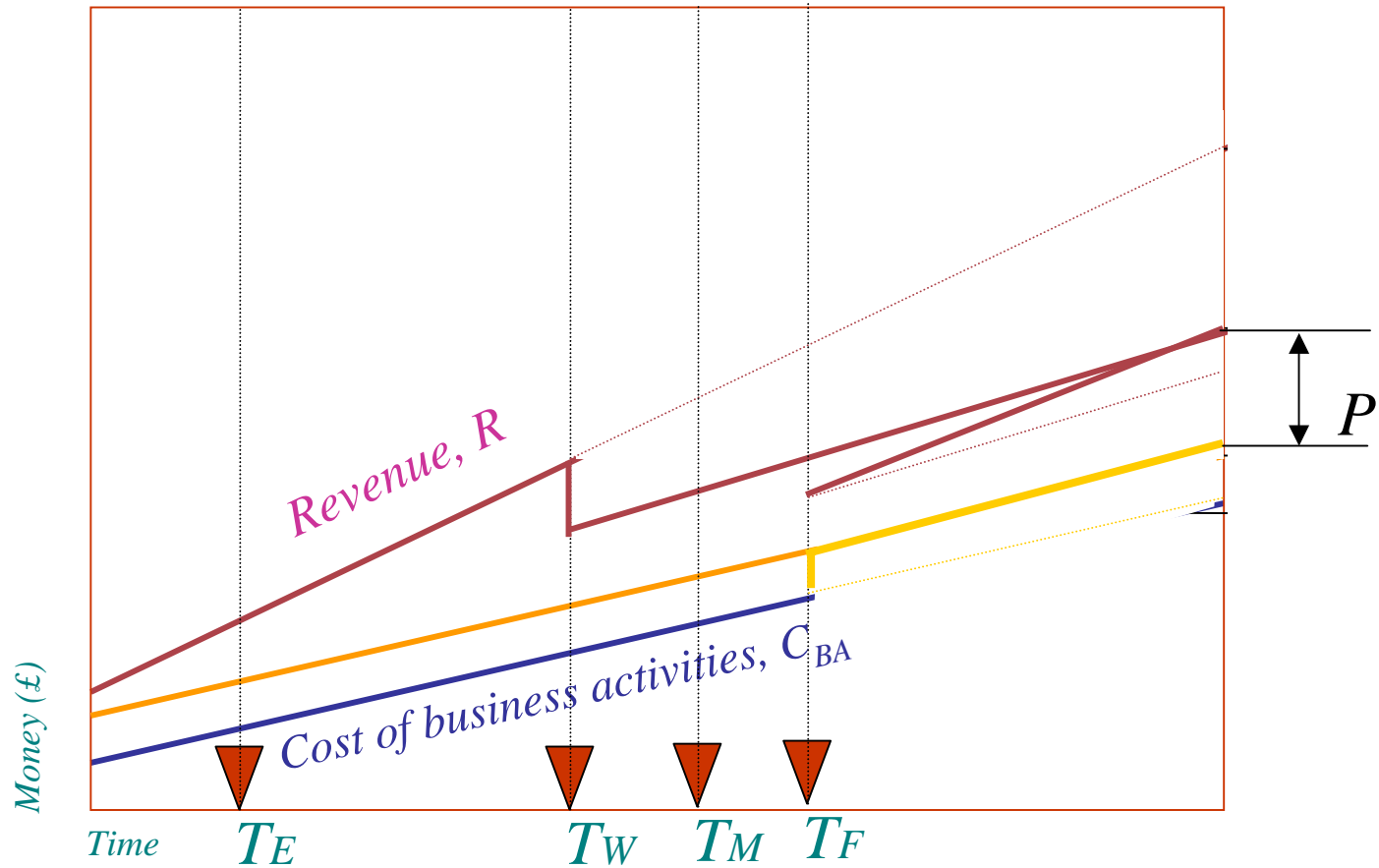
Fundamental Model (too late)



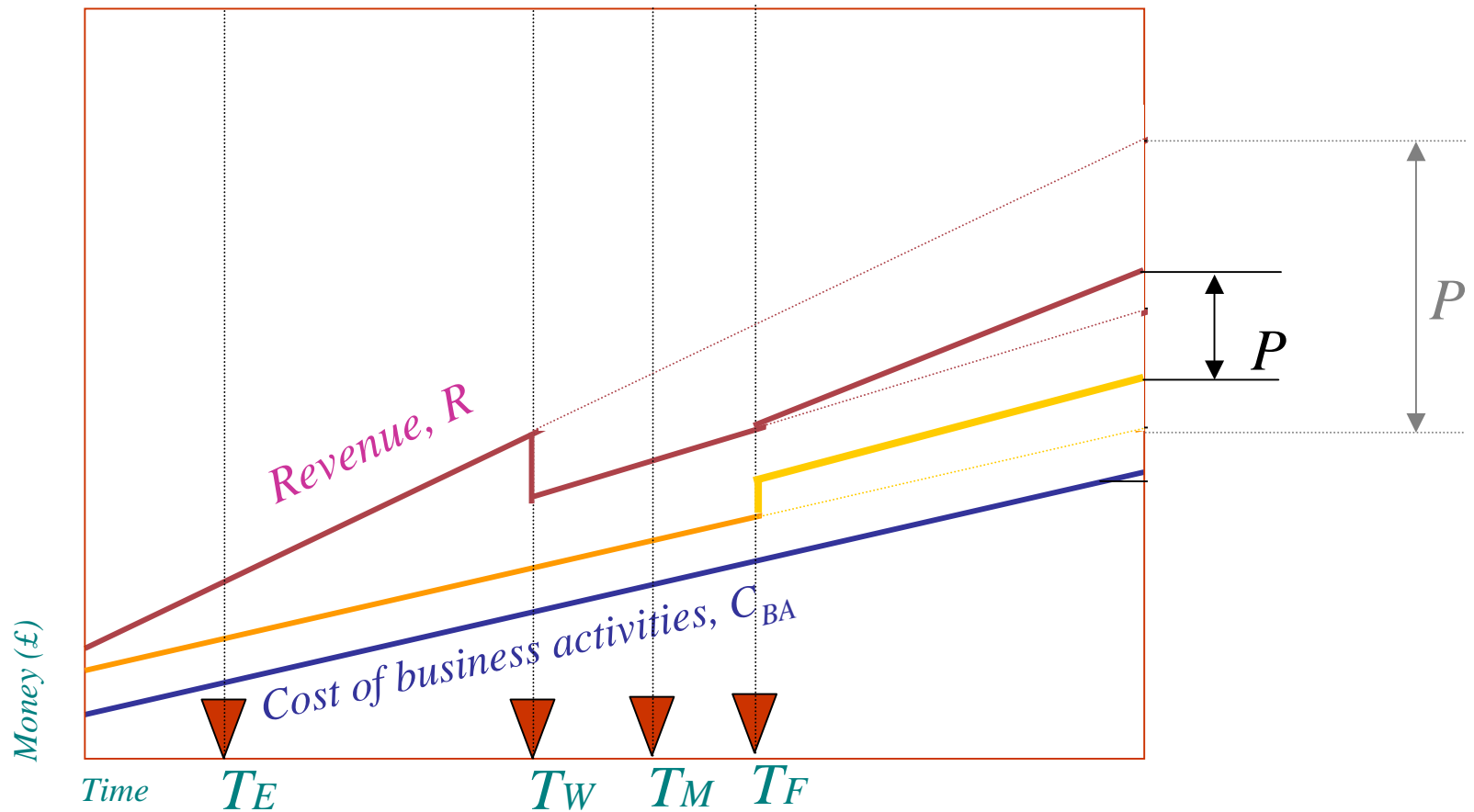
Fundamental Model (too late)



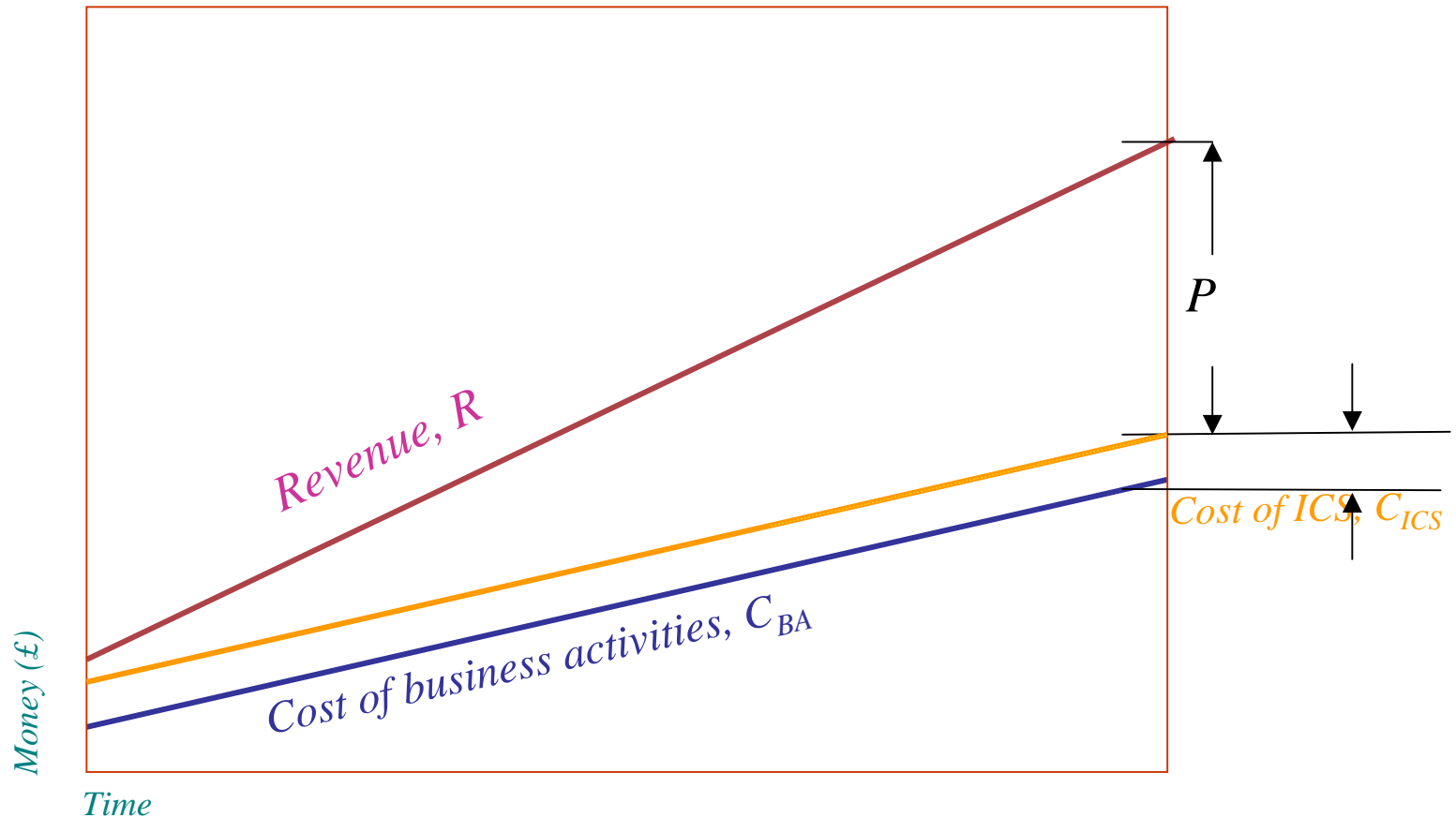
Fundamental Model (too late)



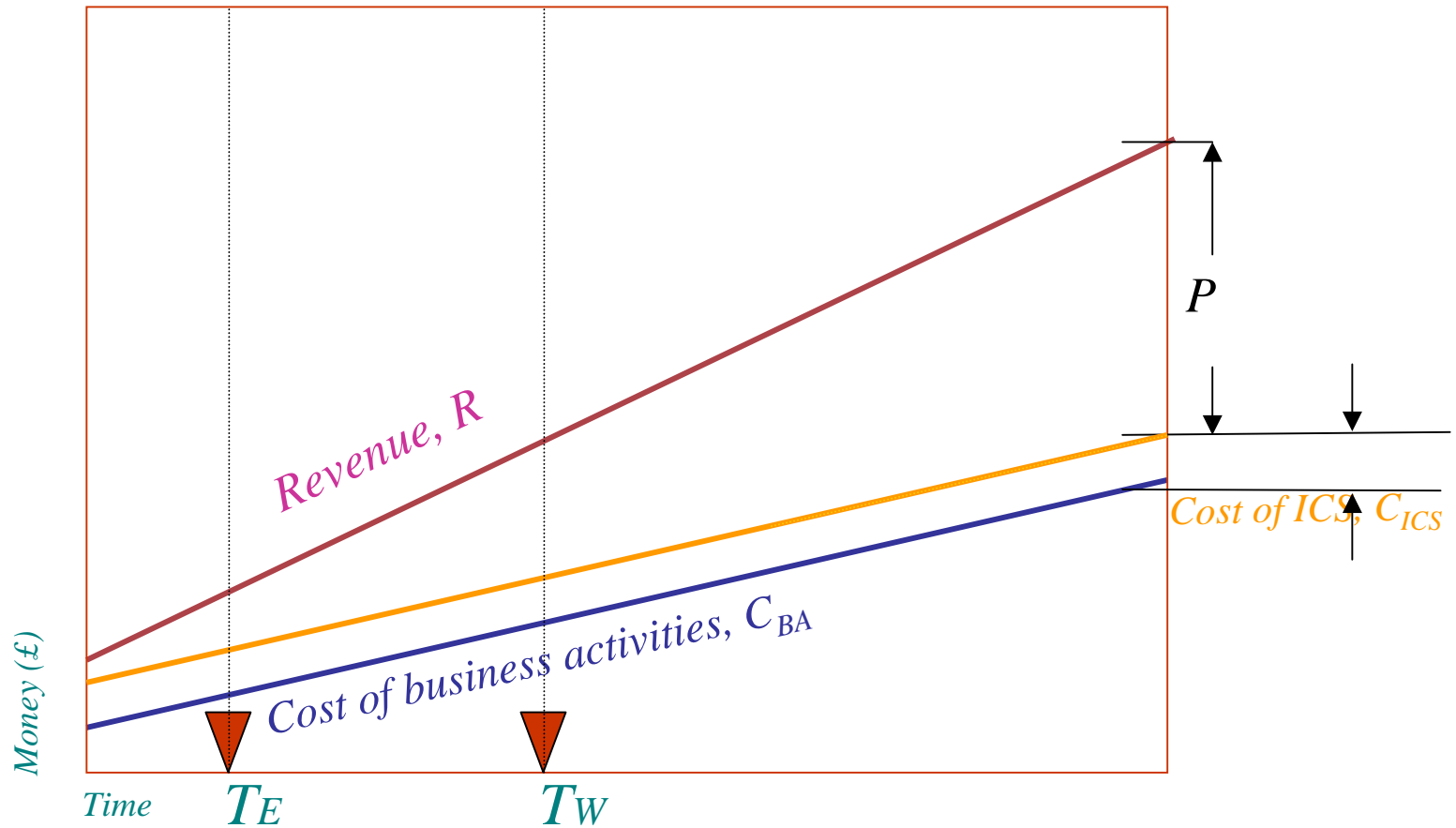
Fundamental Model (too late)



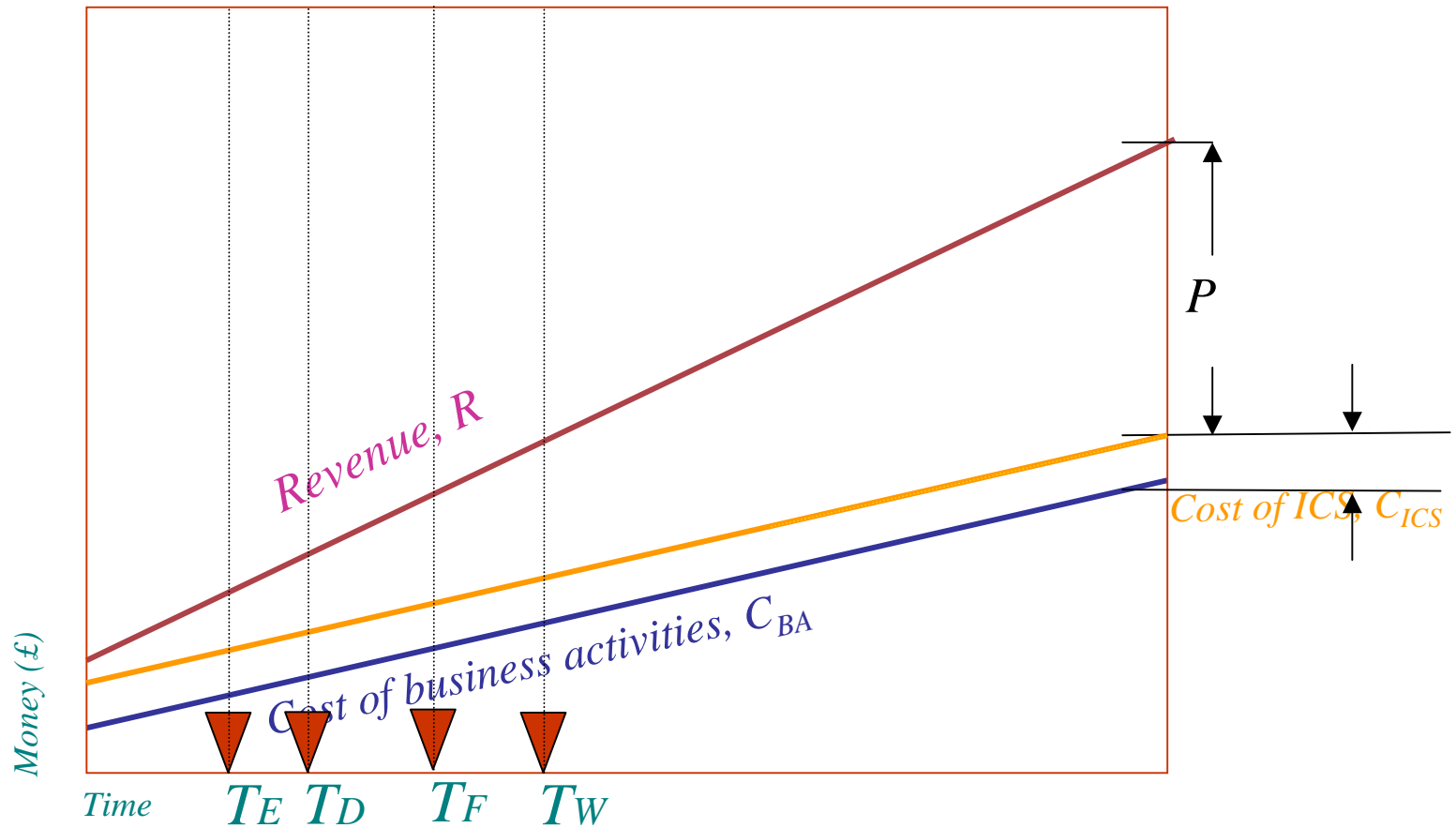
Fundamental Model (in time)



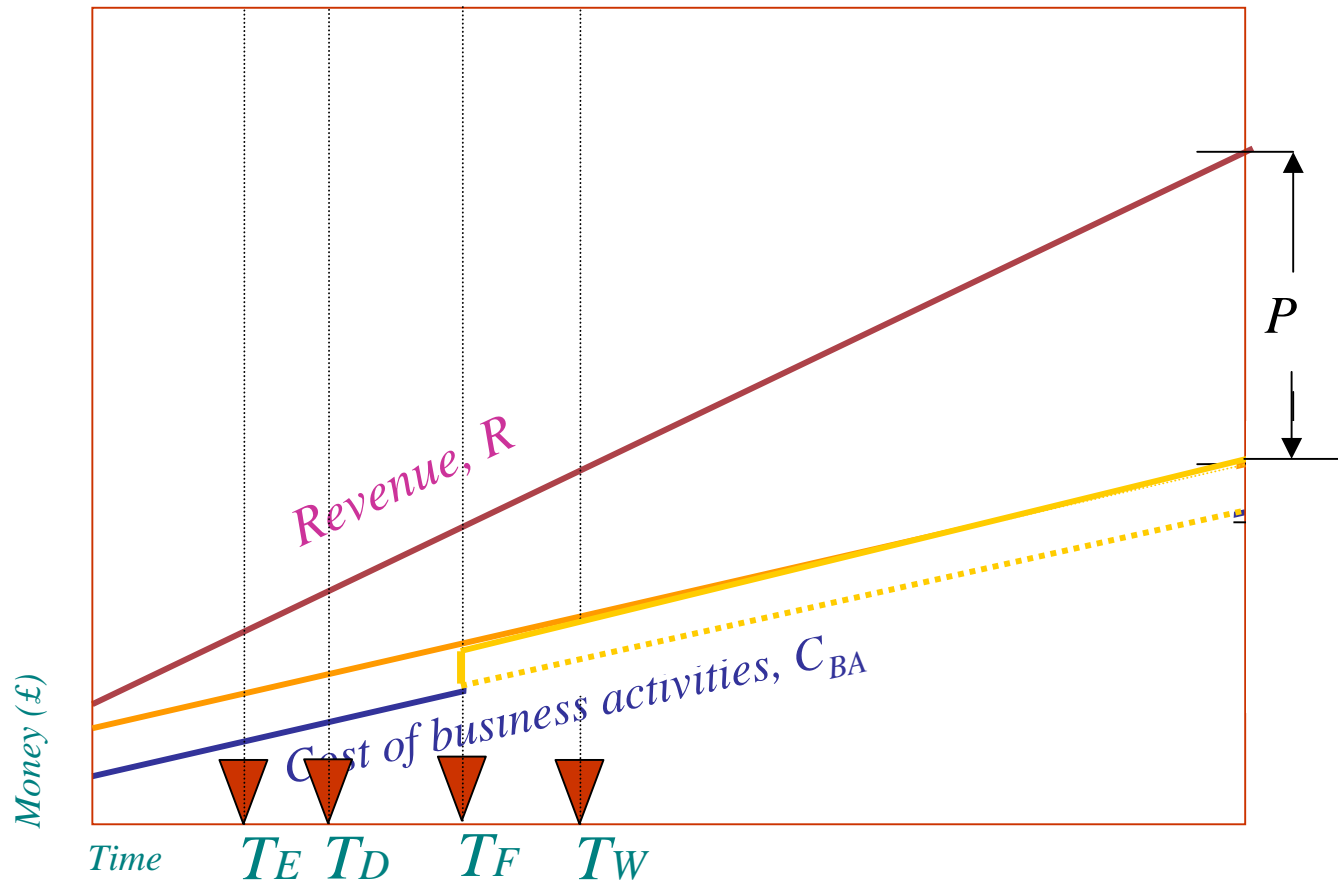
Fundamental Model (in time)



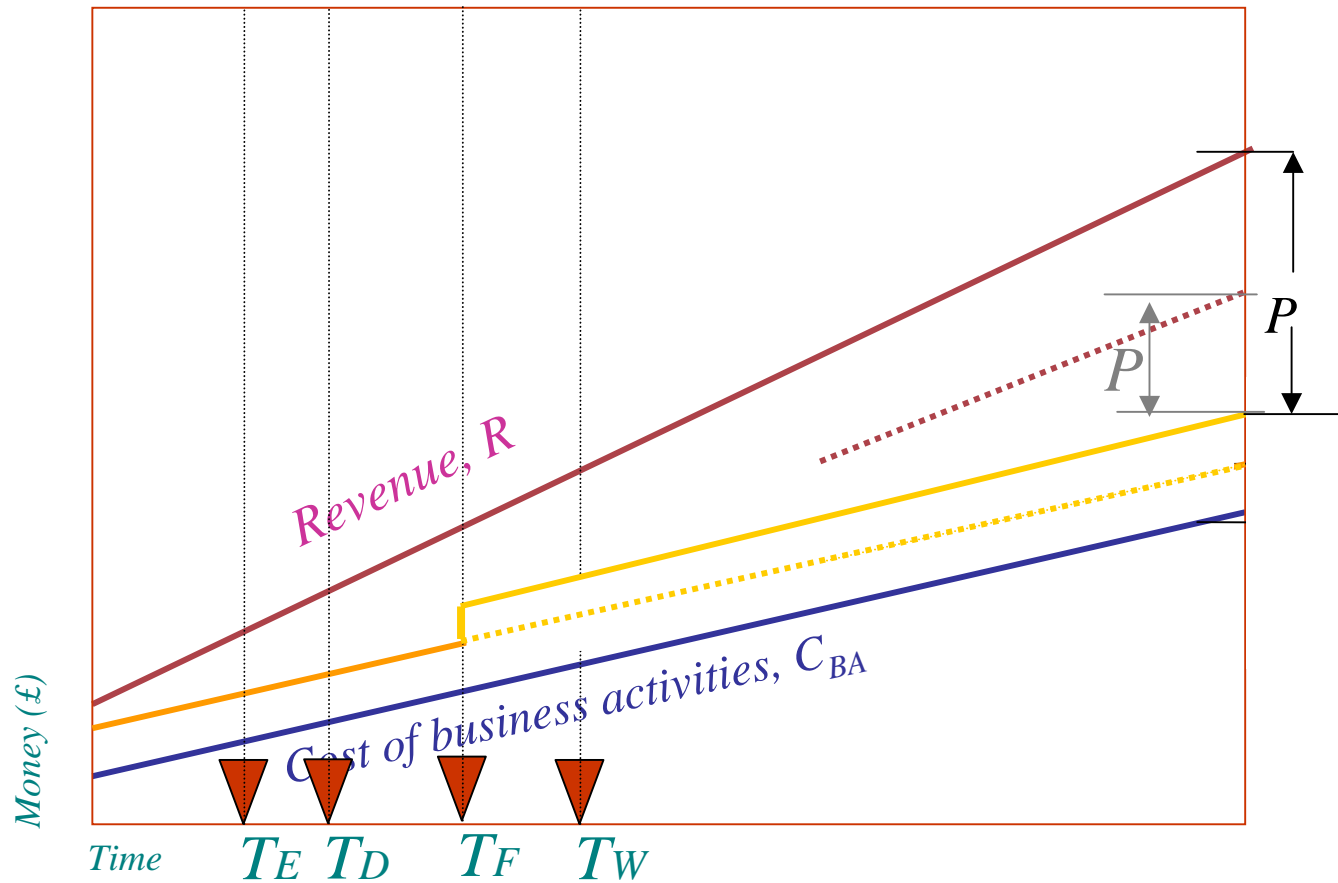
Fundamental Model (in time)



Fundamental Model (in time)



Fundamental Model (in time)



Continuum of Classes

- Preventive (Class 1)
- Detective (Classes 2 – 4)
- Reactive (Classes 5 – 7)

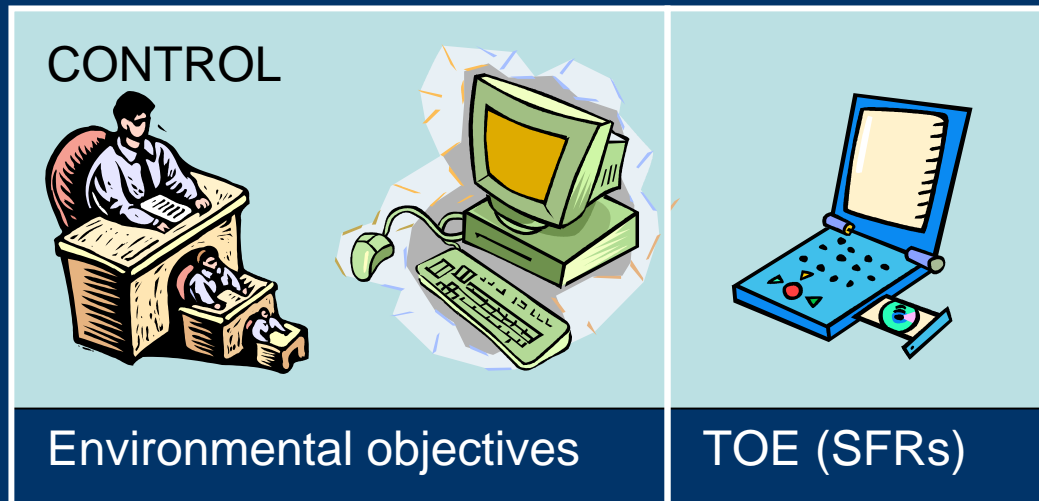
Well Formed Controls

- Axiomatic that things go wrong (Murphy)
 - Accept the risk
 - Strengthen control
 - Add a detective control
- Well formed if capable of prompt detection of failure
- Also known as self-policing (see BS7799-2)

COMMON CRITERIA

Controls and SFRs

- SFRs are not controls, but parts of them



- Correct, cannot be bypassed ...

Failure Modes

- The code is wrong or fails to address all circumstances
- The assumptions are not implemented correctly or the users fail to operate correctly
- The function may fail because of some known error or physical condition

Risk Treatment Plans

Event

Assets

Impacts

Threats

Risk

Vulnerability

Risk Treatment

RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various modems that can access the internal networks remotely and read data, modify it, introduce malicious code or 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](#) , [E5.2](#) , [E5.3](#) , [E5.4](#)
- Possible unwanted [disclosure of sensitive information](#) (e.g. Groups [F](#), [K](#)), see [E5.2](#) , [E5.3](#) , [E5.4](#)
- Possible [court action against our company for breach of the Data Protection Act](#)

The threat is the [hacker](#).

Risk E5.1 A hacker could bring about our inability to carry out some or all of our business through the network. The first line of defence against such an attack is the [firewall](#). The ISP provides a second line of defence, therefore whether this firewall is always correctly configured, or if is under attack. Not considered an acceptable risk because there is a second line of defence, which lies in hardening the network through [“Hotfix and service pack upgrades”](#). However:

Risk Treatment Plans

- Ask what if control doesn't work
 - Accept risk
 - Strengthen
 - Detect

RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious 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](#) , [E5.2](#) , [E5.3](#) , [E5.4](#)
- Possible unwanted [disclosure of sensitive information](#) (e.g. Groups [F](#), [K](#)), see [E5.2](#) ,
- Possible [court action against our company for breach of the Data Protection Act](#)

The threat is the [hacker](#).

Risk E5.1 A hacker could bring about our inability to carry out some or all of our b the network. The first line of defence against such an attack is the [firewall](#). The ISP p therefore whether this firewall is always correctly configured, or if is under attack. Ne acceptable risk because there is a second line of defence, which lies in hardening th [“Hotfix and service pack upgrades”](#). However:

Risk Treatment Plans

- Ask what if control doesn't work
- But what if detective control too late!

RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious 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](#) , [E5.2](#) , [E5.3](#) , [E5.4](#)
- Possible unwanted [disclosure of sensitive information](#) (e.g. Groups [F](#), [K](#)), see [E5.2](#) ,
- Possible [court action against our company for breach of the Data Protection Act](#)

The threat is the [hacker](#).

Risk E5.1 A hacker could bring about our inability to carry out some or all of our business through the network. The first line of defence against such an attack is the [firewall](#). The ISP provides a second line of defence, therefore whether this firewall is always correctly configured, or if is under attack. Nevertheless, this is not an acceptable risk because there is a second line of defence, which lies in hardening the network through [“Hotfix and service pack upgrades”](#). However:

Argument for CC Evaluation

- Detective control is too late or impractical
- Impact is big-time
- Examples
 - Chip and PIN
 - Writing audit records

Evaluation Requirements

- Ability to express control requirement in PP/ST
 - Automated cash dispenser (PP/9907)
 - Electronic purse (PP/0101)
 - Financial accounting packages
 - GlobalPlatform
- Language barrier – doable – but can put people off

SUMMARY

- RTPs identify where CC is an imperative
- CC evaluation gives assurance in those parts of internal control
- Sound internal control prerequisite for corporate governance
- Hence link between corporate governance and the Common Criteria

RECOMMENDATIONS

1. Consider security as part of internal control
2. Use RTPs to identify need for evaluation
3. Determine how existing PPs contribute
4. Ditto vendors' STs
5. Vendors of other IT consider same
6. CC authorities help to ease language barrier

The Relevance of the Common Criteria to Sarbanes-Oxley and Corporate Governance

*Dr. David Brewer,
www.gammassl.co.uk &
William List, CA, Hon FBCS, CIPT
w.list@ntlworld.com*