



APPLYING ICS TIME METRICS to GLOBALPLATFORM SMART CARDS

William List & Dr. David Brewer

www.gammassl.co.uk

w.list@ntlworld.com dbrewer@gammassl.co.uk

Agenda

- Introduction
- Time metrics
- GPCS reminder
- Risk treatment plans (RTPs)
- Example
- Conclusions



Time Metrics



The Fundamental Principle

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

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



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

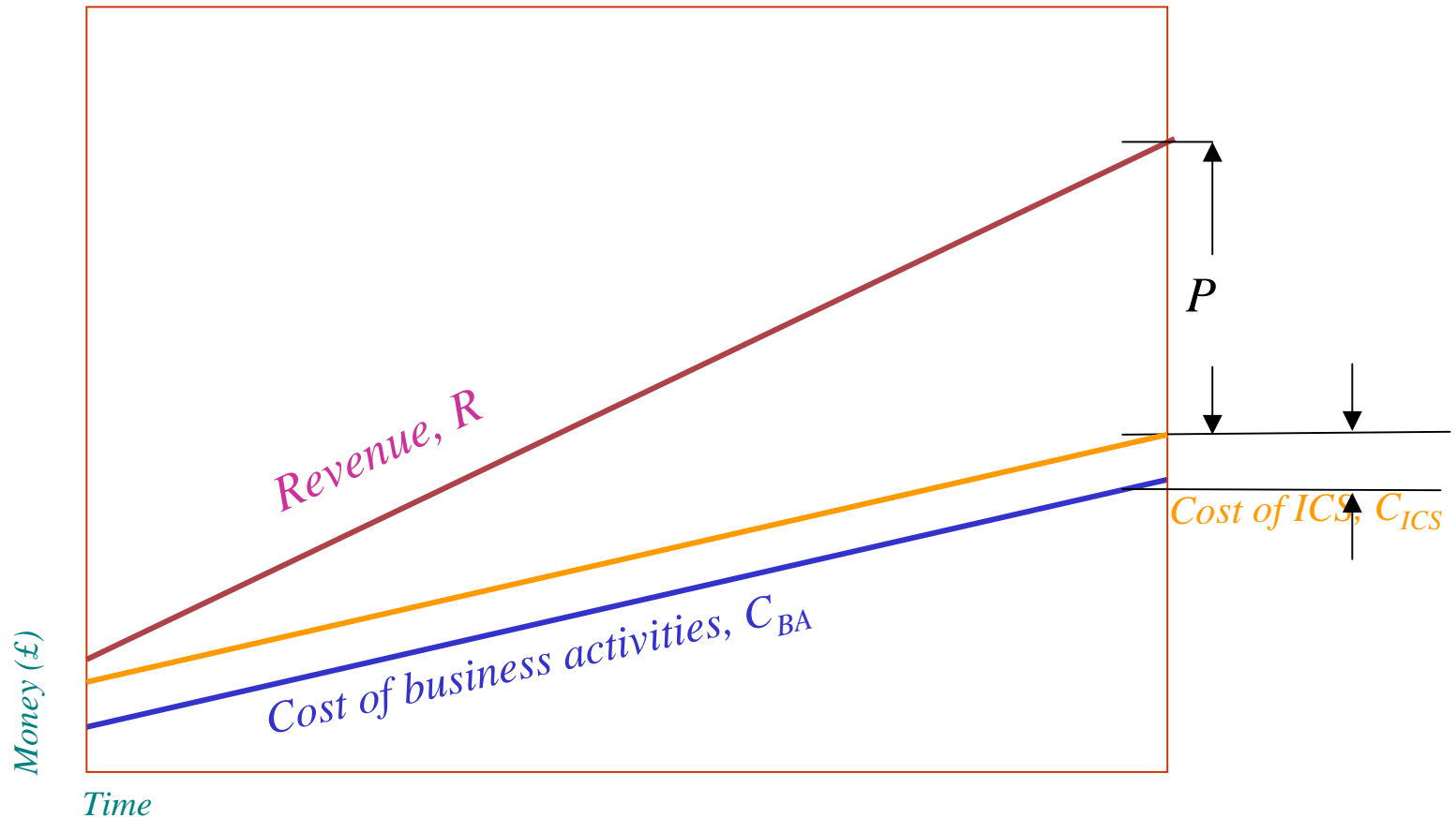


Parameter Definition (Money)

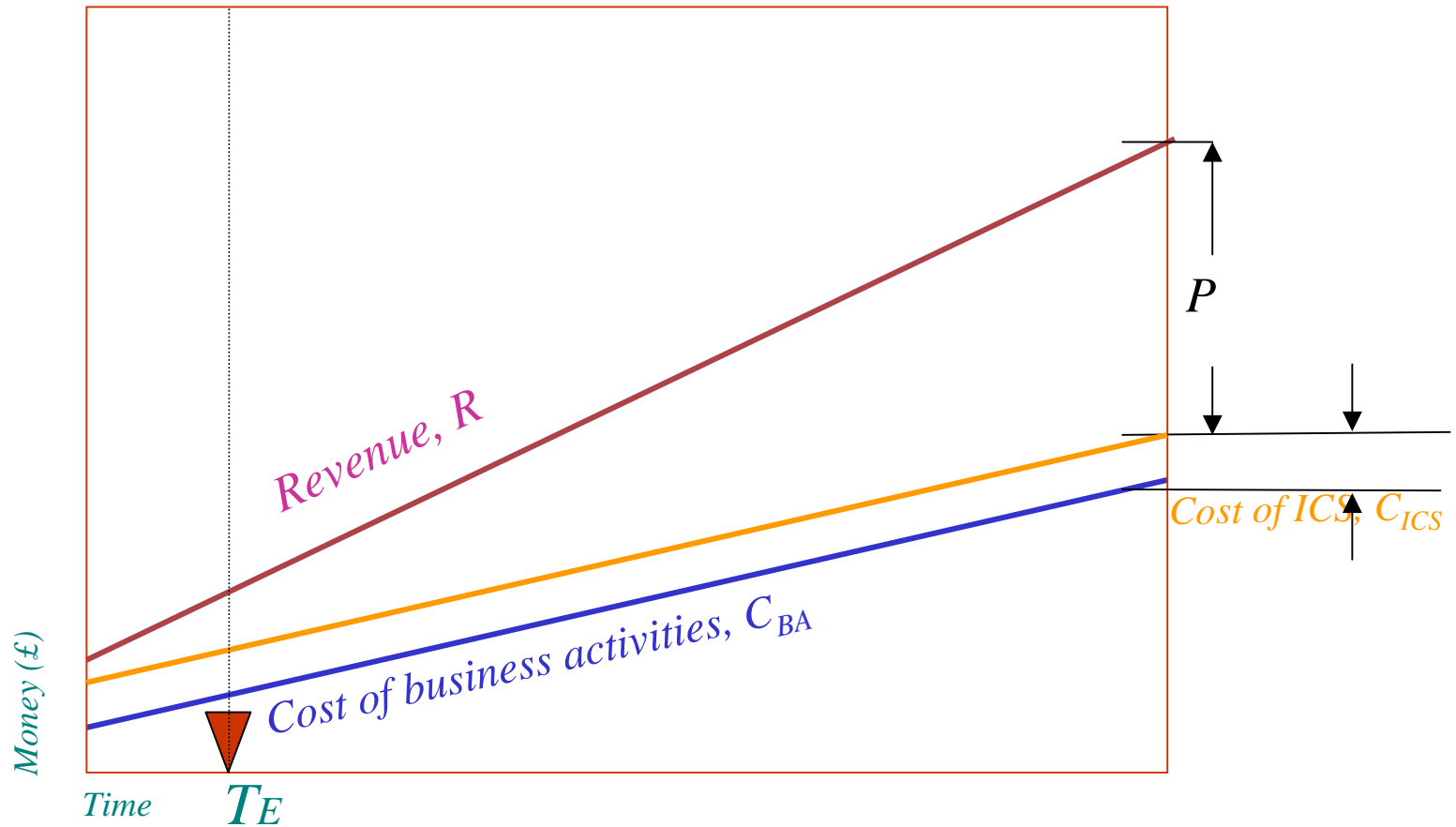
- Cost of doing business, C_{BA}
- Cost of internal control, C_{ICS}
- Impact penalty, I_P
- Cost of fix, C_F



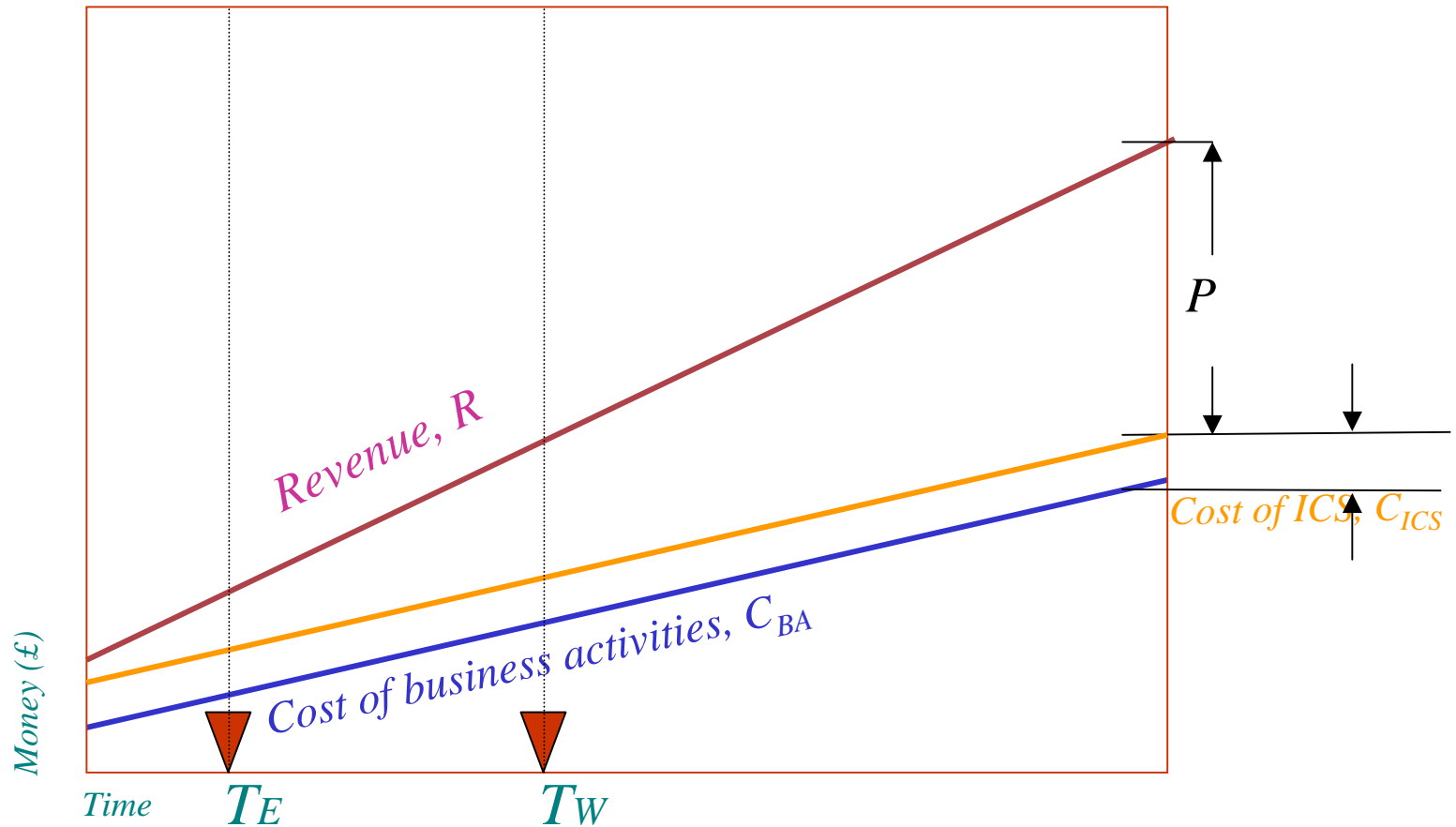
Fundamental Model (too late)



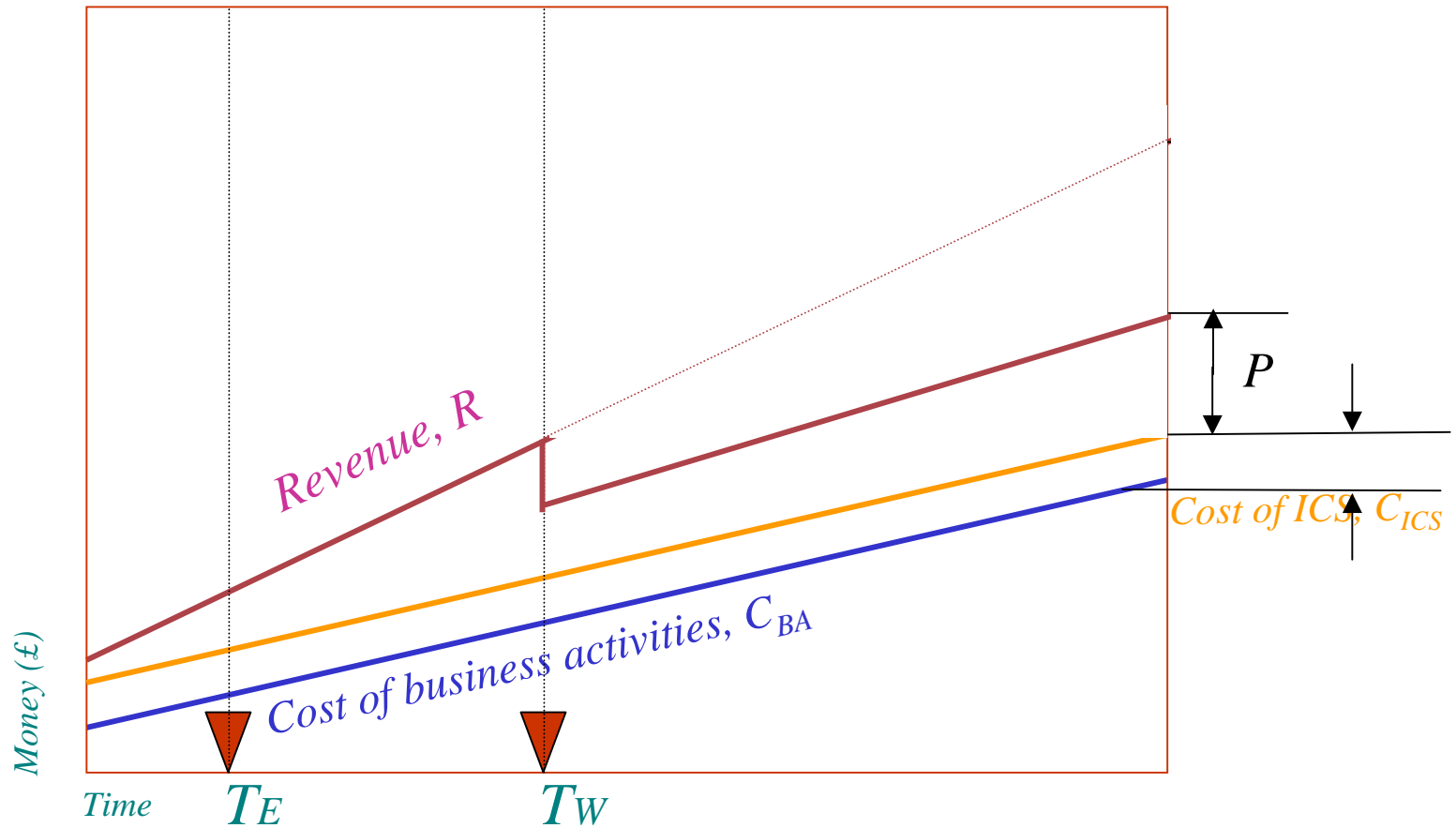
Fundamental Model (too late)



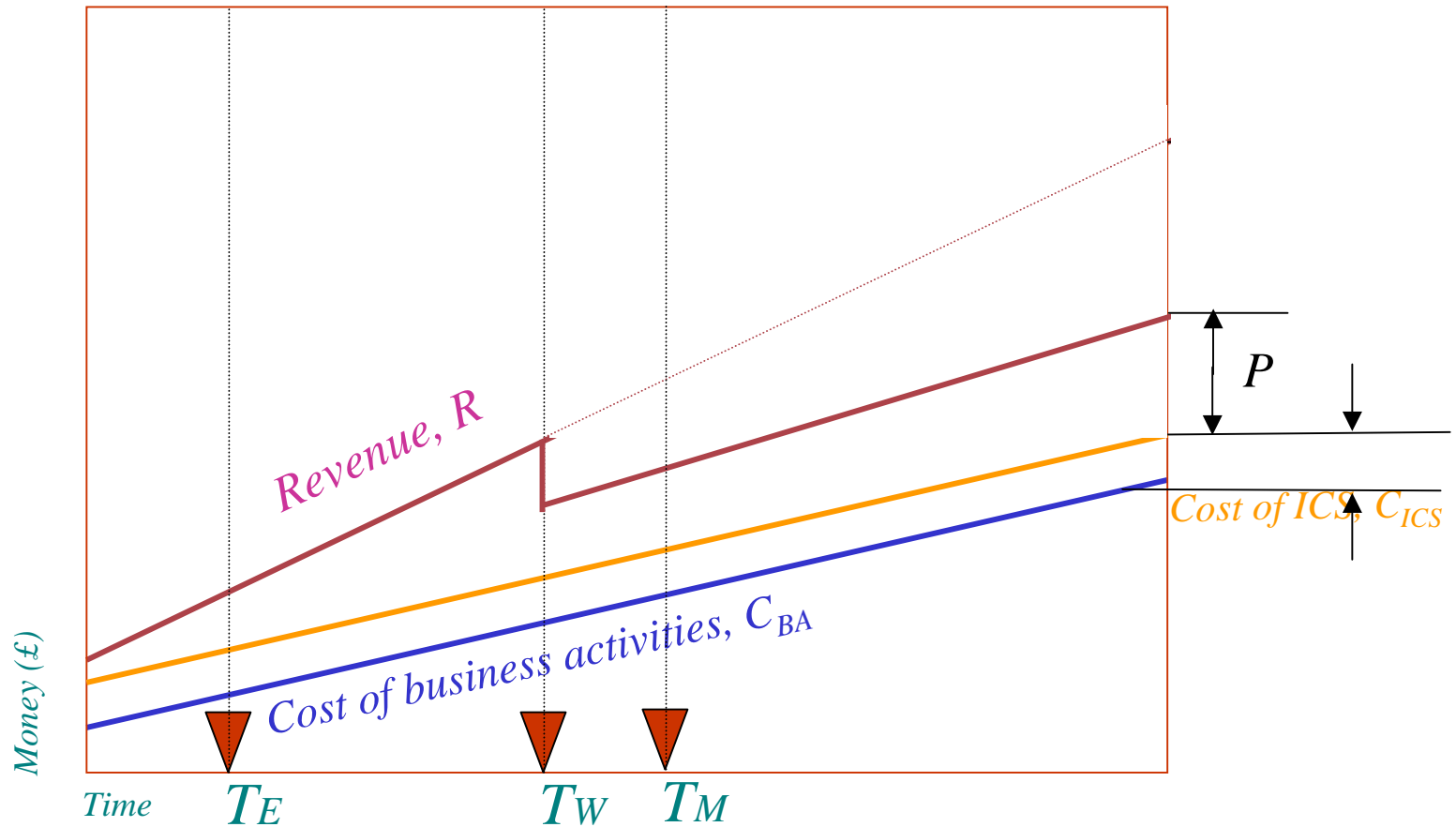
Fundamental Model (too late)



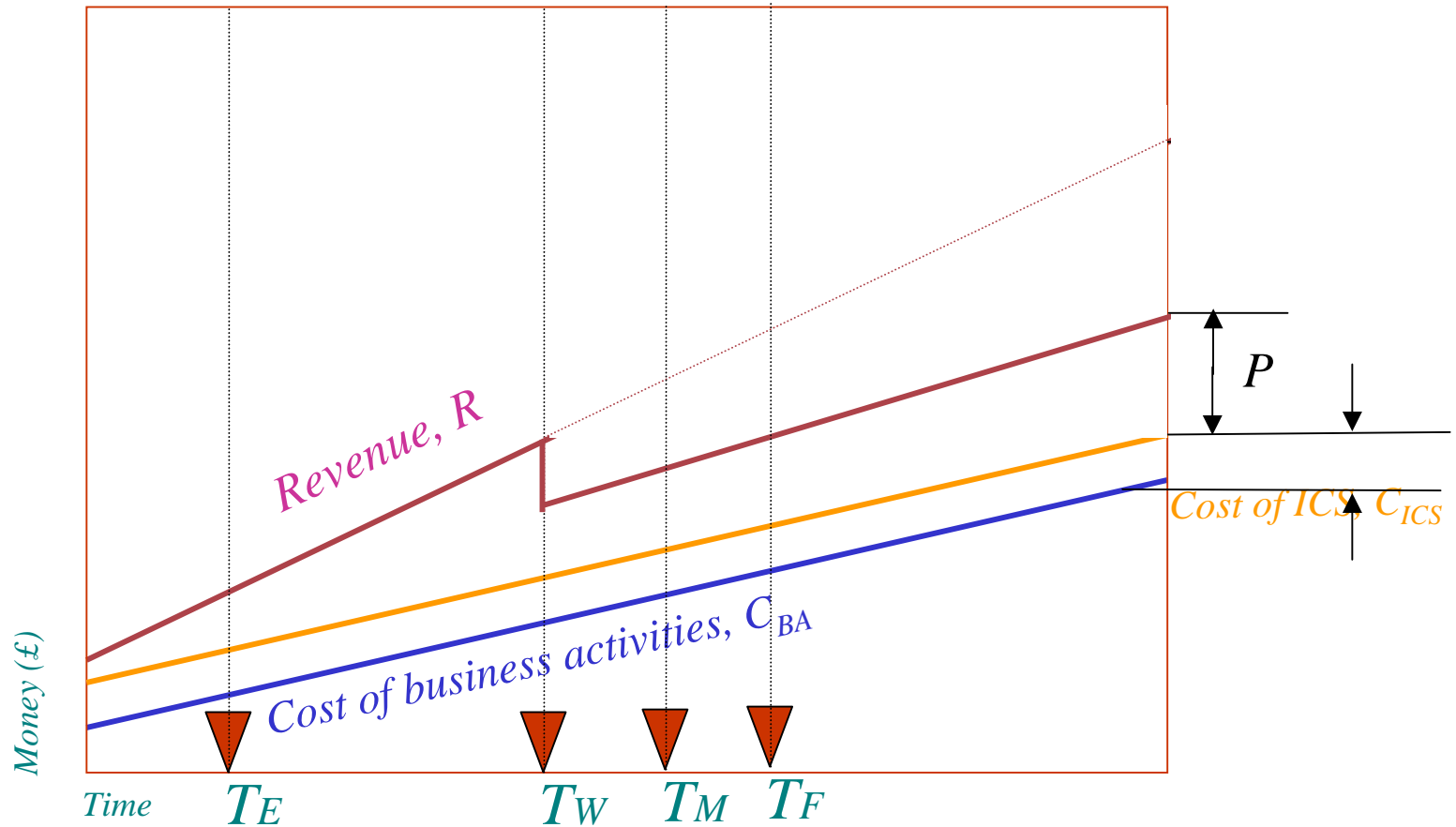
Fundamental Model (too late)



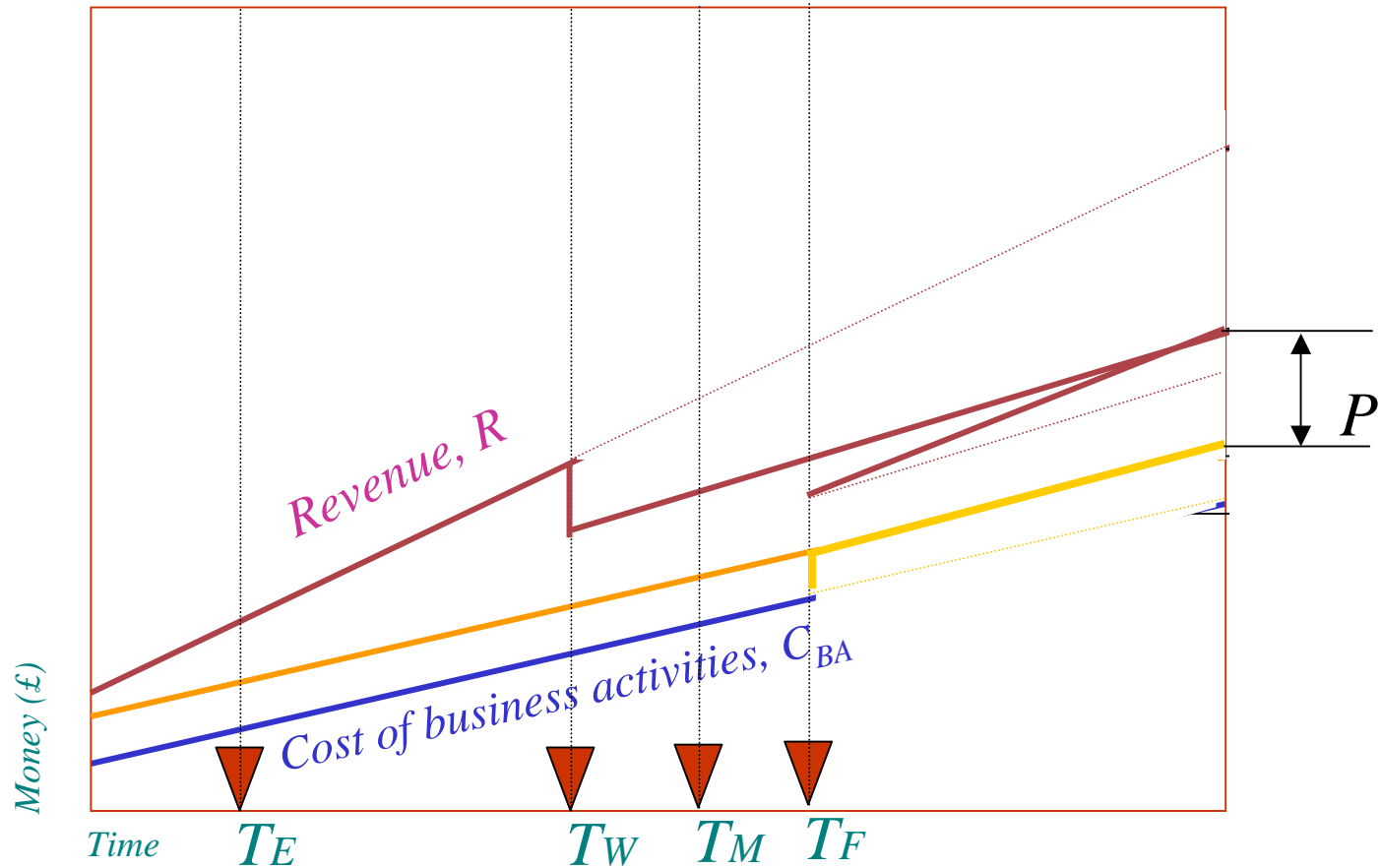
Fundamental Model (too late)



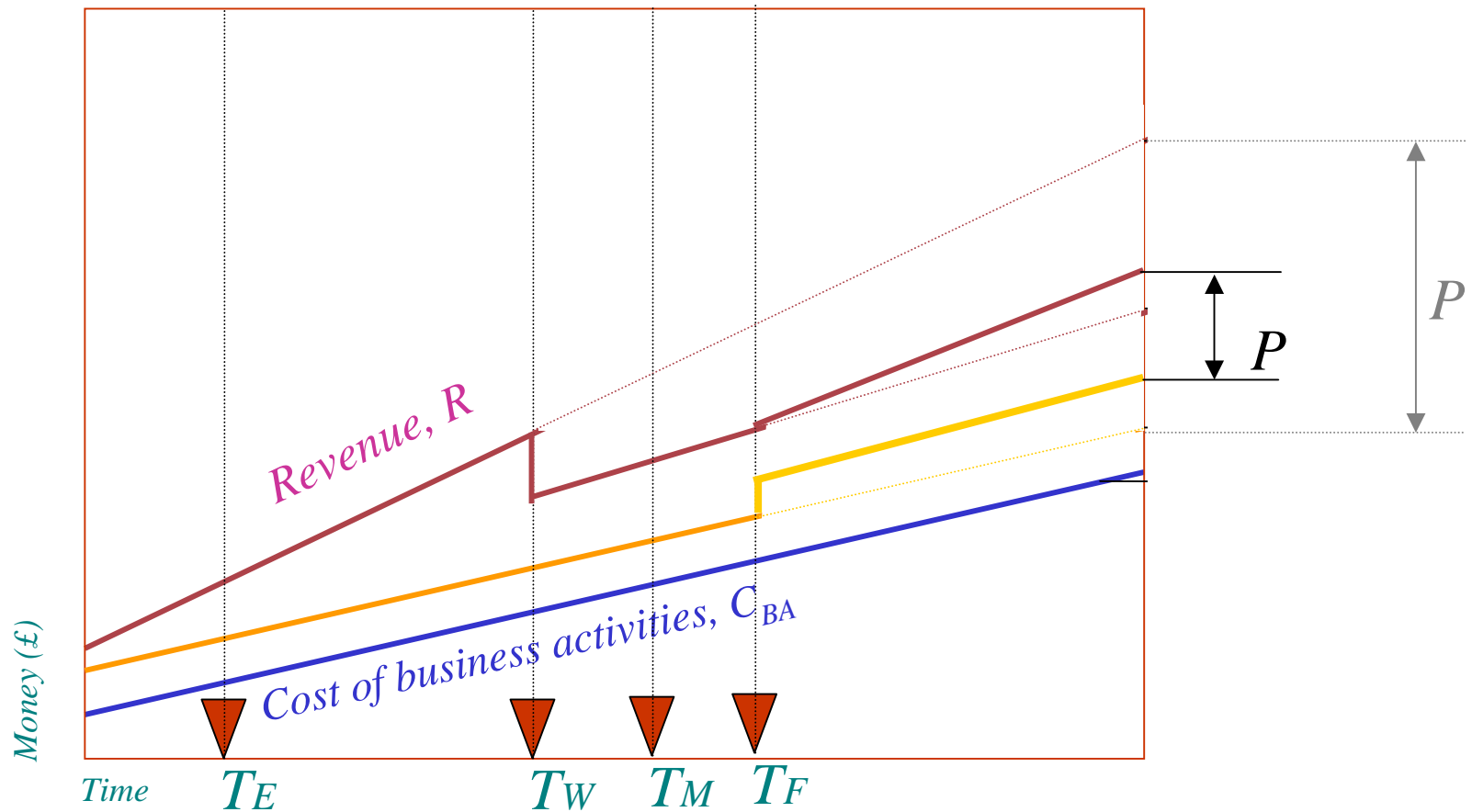
Fundamental Model (too late)



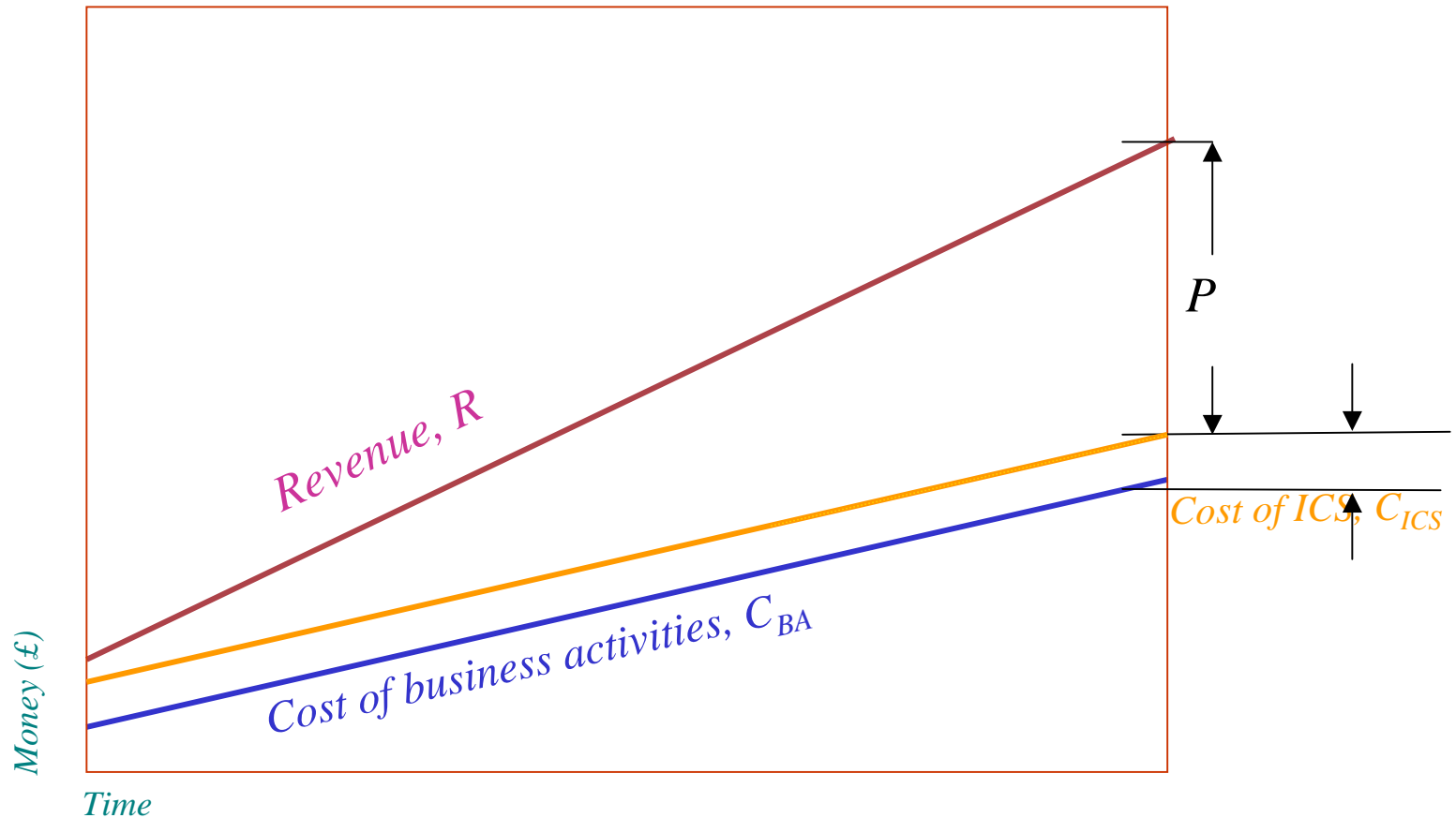
Fundamental Model (too late)



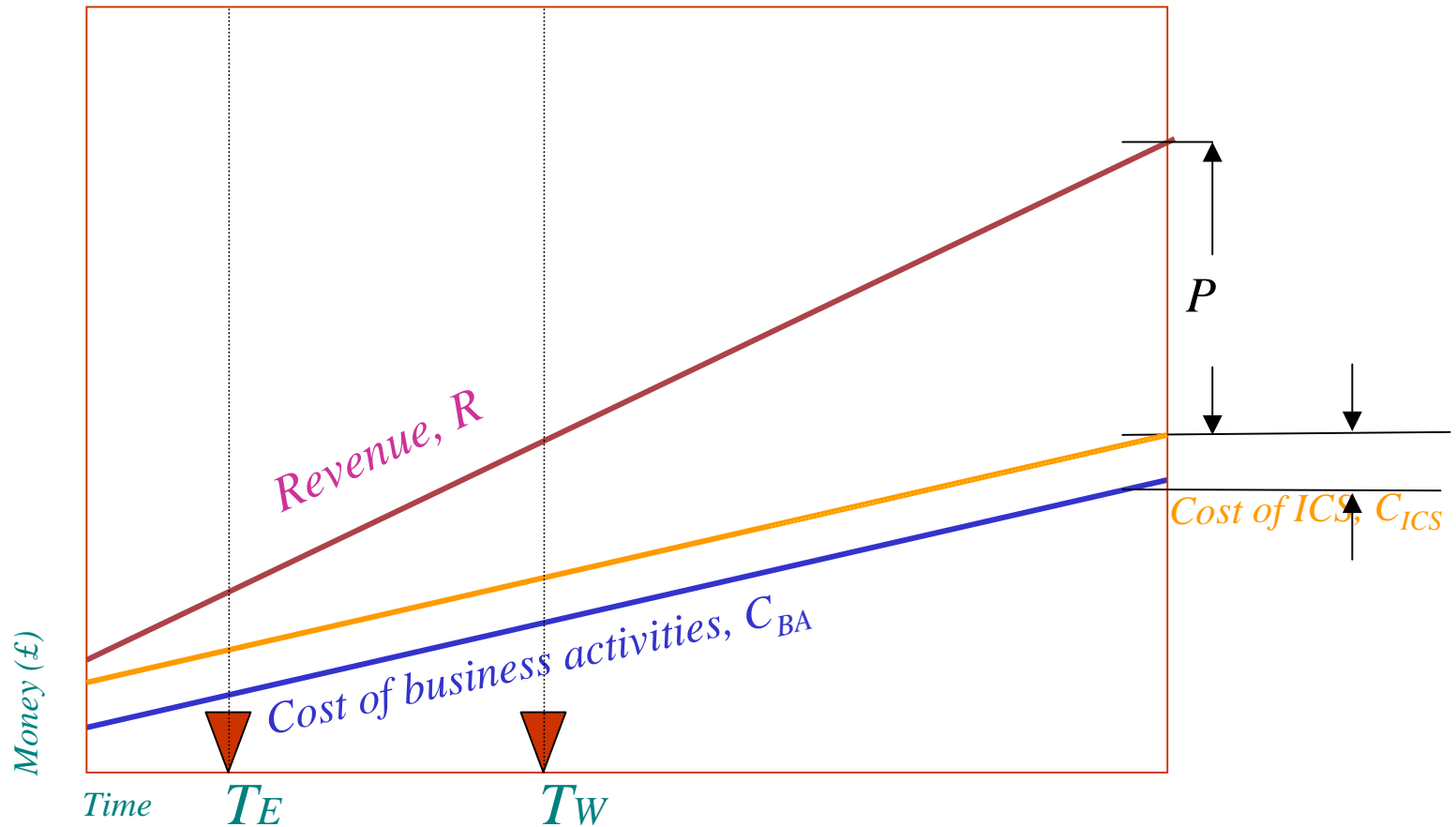
Fundamental Model (too late)



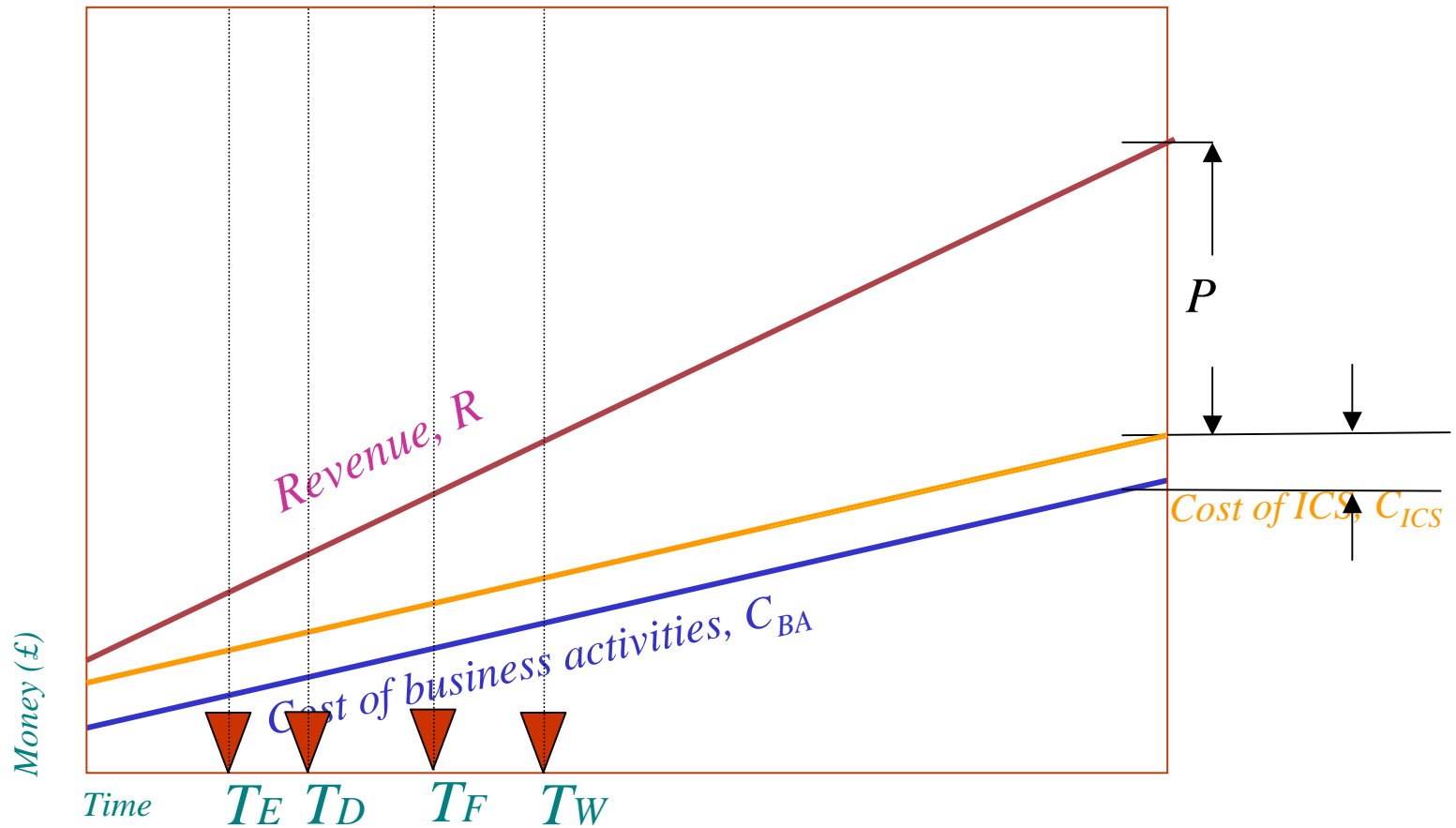
Fundamental Model (in time)



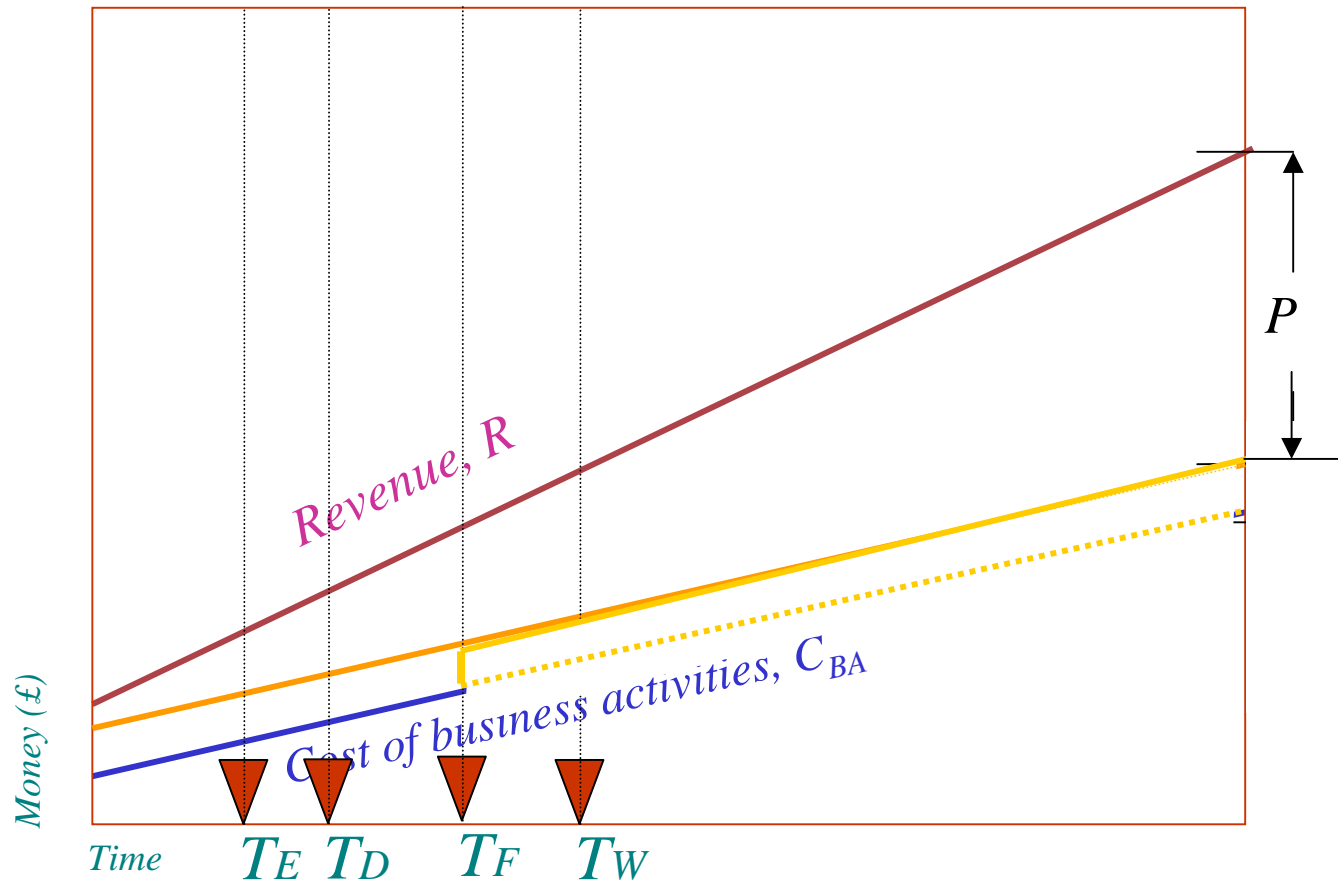
Fundamental Model (in time)



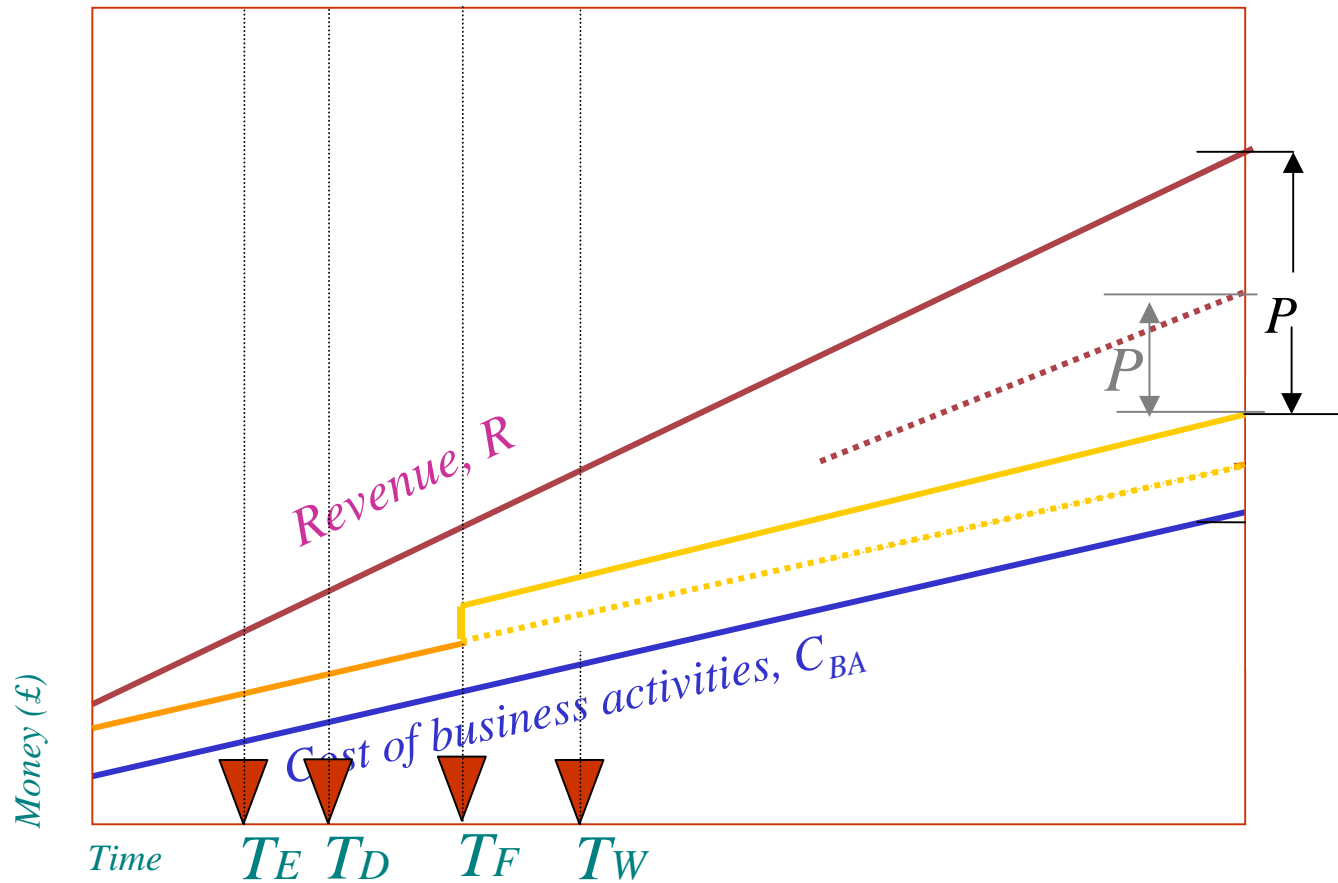
Fundamental Model (in time)



Fundamental Model (in time)



Fundamental Model (in time)



Continuum of Classes

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	
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	Detective
5	Fails to detect the event but has a partially deployed BCP	
6	Fails to detect the event but does have a BCP	
7	Fails to detect the event and does not have a BCP	
		Reactive

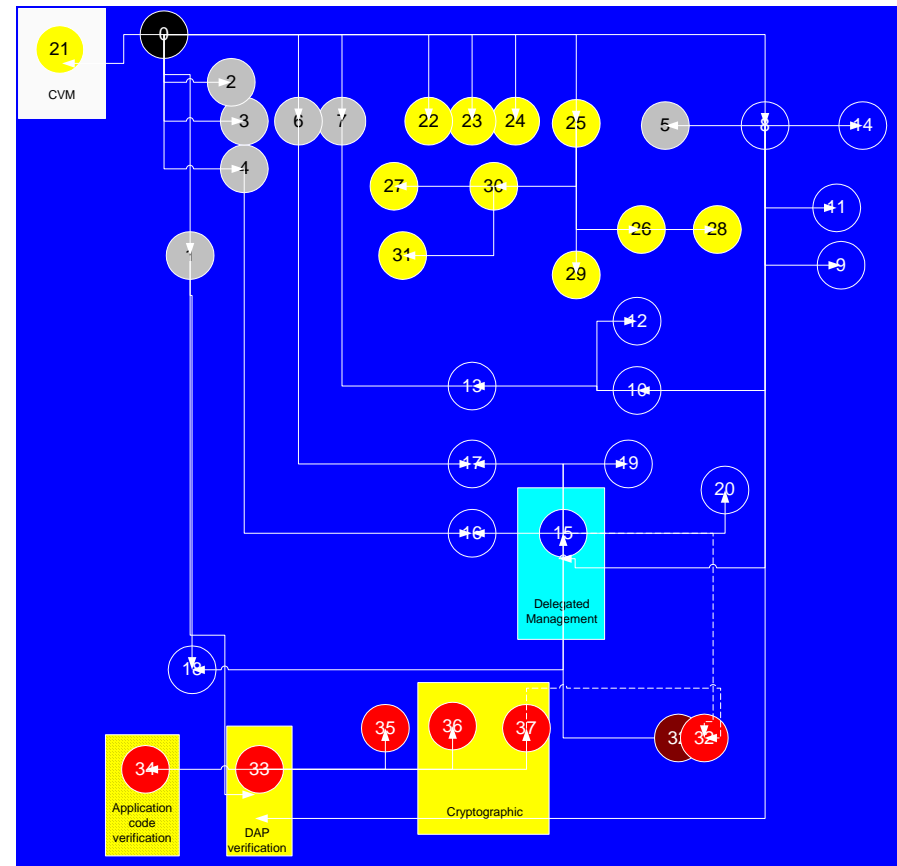
Packages

- 37 functional packages:

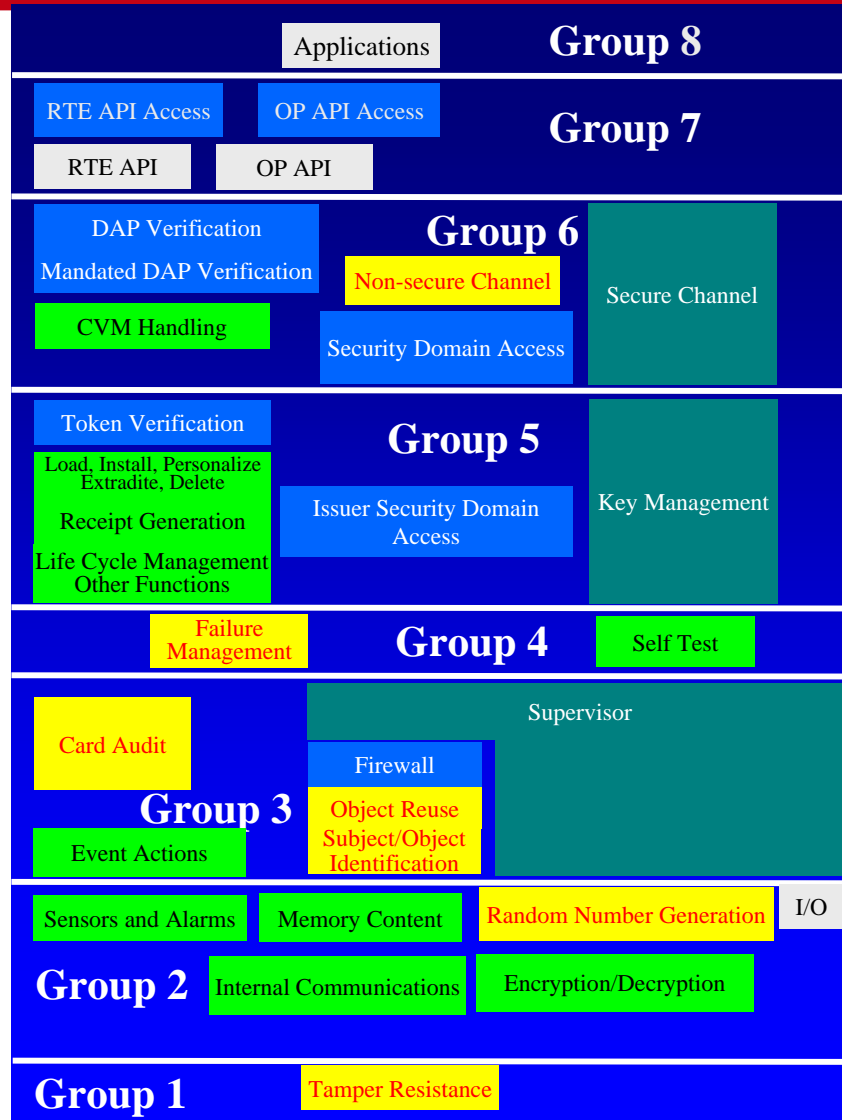
- Core
- 7 ISD Packages
- 13 SD Packages
- 11 SCP Packages
- 6 others

- Allows card configuration to be tailored to suit business/risk environment

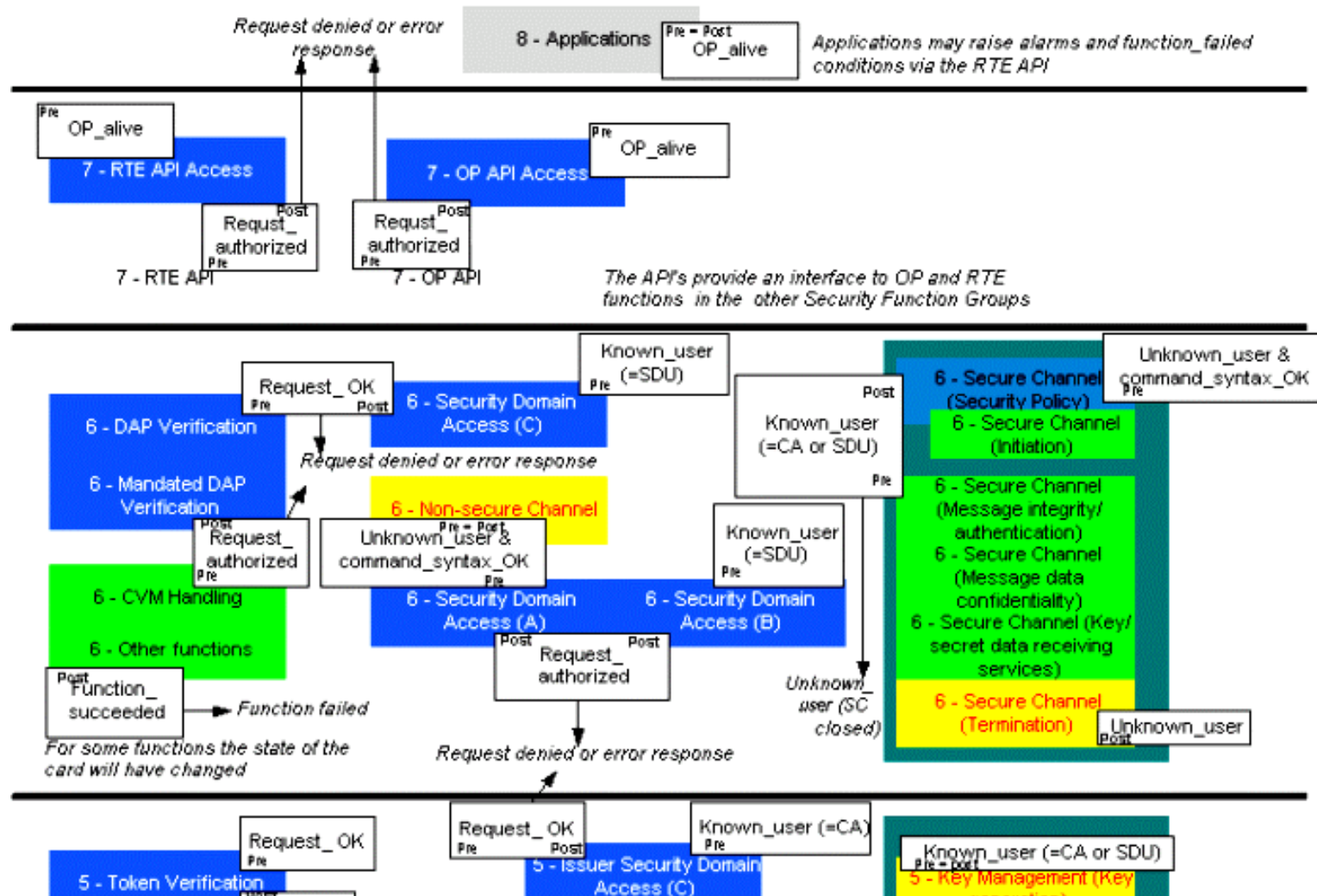
- Causes problems with PPs



Security Architecture



The Detail (1)



Control Classifications

■ On Card

- *Mostly 1 (preventive) or 2 (detective)*
- *OK IF card works as expected*

■ Off Card

- *PP are assumptions/assertions*



What if controls fail?

- How do we know?
- Do right people know?
- How can it be fixed?
- Does it matter?

Risk assessment



What is a Risk Treatment Plan?

■ **Risk Treatment:** *treatment process of selection and implementation of measures to modify risk [ISO Guide 73]*

RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also users who can access the internal networks remotely and read data, modify it, and introduce new data. This could 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](#)
- Possible unwanted [disclosure of sensitive information](#) (e.g. [Group C](#))
- 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 by attacking the network. The first line of defence against such an attack is the firewall, therefore whether this firewall is always correctly configured, or if it is unduly restrictive, is an acceptable risk because there is a second line of defence, which lies in the implementation of [“Hotfix and service pack upgrades”](#). However:



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 ways in which hackers can access the internal networks remotely and read data, modify it, introduce viruses, etc. (groups: [S](#), [D](#), [E](#), [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](#)
- Possible unwanted disclosure of sensitive information (e.g. Groups [F](#) and [G](#))
- 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 by accessing the network. The first line of defence against such an attack is the firewall. Therefore, whether this firewall is always correctly configured, or if it is undetected, is a key factor in accepting the risk because there is a second line of defence, which lies in the “Hotfix and service pack upgrades”. However:

Event

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

Common (but treatment might be different!)

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 vulnerabilities that could allow someone to access the internal networks remotely and read data, modify it, introduce malware, etc. The groups that could 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](#).
- Possible unwanted [disclosure of sensitive information](#) (e.g. Groups [C](#), [D](#), [E](#), [F](#), [G](#), [H](#), [J](#), [K](#), [L](#), [M](#), [N](#), [P](#), [R](#)).
- 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 by accessing the network. The first line of defence against such an attack is the [firewall](#). It is therefore whether this firewall is always correctly configured, or if it is not, whether this is an acceptable risk because there is a second line of defence, which lies in the [implementation of patches and service pack upgrades](#). However:

Impacts

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



Example

- We are an application provider

suppose our business requirement is

- *An EMV application*
- *Not owned by card issuer*
- *MUST be the only one on card*



Example RTP

**RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER
AND THEIR APPLICATIONS**



Example RTP

RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER AND THEIR APPLICATIONS

The card issuer may make take actions, for example in managing card content and attending to our requirements, that in practice are not in out best business interests. Likewise, other application providers, or their applications may also act in a manner that is prejudicial to our business. The assets concerned are our application and our customers' data.



Example RTP

RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER AND THEIR APPLICATIONS

The card issuer may make take actions, for example in managing card content and attending to our requirements, that in practice are not in out best business interests. Likewise, other application providers, or their applications may also act in a manner that is prejudicial to our business. The assets concerned are [our application](#) and [our customers' data](#).

The impacts of such events are: <<Consider highlighted one and incorporate/delete as appropriate>>

- Probable [customer dissatisfaction](#), see
- Possible [adverse press coverage](#), see
- Possible [court action](#), see
- Probable [loss of revenue](#), see
- Probable [unanticipated costs](#), see



Example RTP

RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER AND THEIR APPLICATIONS

The card issuer may make take actions, for example in managing card content and attending to our requirements, that in practice are not in out best business interests. Likewise, other application providers, or their applications may also act in a manner that is prejudicial to our business. The assets concerned are [our application](#) and [our customers' data](#).

The impacts of such events are: <<Consider highlighted one and incorporate/delete as appropriate>>

- Probable [customer dissatisfaction](#), see
- Possible [adverse press coverage](#), see
- Possible [court action](#), see
- Probable [loss of revenue](#), see
- Probable [unanticipated costs](#), see

The principal threats are [the card issuer](#), [other application providers](#), [other applications](#), [cardholders](#) and [attackers](#).



Example RTP

RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER AND THEIR APPLICATIONS

The card issuer may make take actions, for example in managing card content and attending to our requirements, that in practice are not in out best business interests. Likewise, other application providers, or their applications may also act in a manner that is prejudicial to our business. The assets concerned are [our application](#) and [our customers' data](#).

The impacts of such events are: <<Consider highlighted one and incorporate/delete as appropriate>>

- Probable [customer dissatisfaction](#), see
- Possible [adverse press coverage](#), see
- Possible [court action](#), see
- Probable [loss of revenue](#), see
- Probable [unanticipated costs](#), see

The principal threats are [the card issuer](#), [other application providers](#), [other applications](#), [cardholders](#) and [attackers](#).

Risk 1a Our contract with the card issuer is that there will only be one EMV application on the card, that one being ours. Suppose post-issuance there were two or more. We can take action to prevent a second application provider from loading such an application by having a veto on application downloads. The veto is established though inclusion of Package C (Mandated DAP Support, see [2]). Package C is a preventive measure.



Example RTP

RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER AND THEIR APPLICATIONS

The card issuer may make take actions, for example in managing card content and attending to our requirements, that in practice are not in our best business interests. Likewise, other application providers, or their applications may also act in a manner that is prejudicial to our business. The assets concerned are [our application](#) and [our customers' data](#).

The impacts of such events are: <<Consider highlighted one and incorporate/delete as appropriate>>

- Probable [customer dissatisfaction](#), see
- Possible [adverse press coverage](#), see
- Possible [court action](#), see
- Probable [loss of revenue](#), see
- Probable [unanticipated costs](#), see

The principal threats are [the card issuer](#), [other application providers](#), [other applications](#), [cardholders](#) and [attackers](#).

Risk 1a Our contract with the card issuer is that there will only be one EMV application on the card, that one being ours. Suppose post-issuance there were two or more. We can take action to prevent a second application provider from loading such an application by having a veto on application downloads. The veto is established through inclusion of Package C (Mandated DAP Support, see [2]). Package C is a preventive measure.

Risk 1b Notwithstanding the GlobalPlatform on-card controls, should they fail or some enterprising attacker find a way around them then other applications may be downloaded contrary to our wishes. These, should they exist, could be detected by periodic audit, but that can only be done if we have control of the card, i.e. our application or security domain is Selected. Also it might take too long compared to performing the transaction that the cardholder wishes to transact thereby giving rise to customer dissatisfaction. In monitoring the EMV transactions, we could look for a gross drop in the total number of transactions for all customers, but that would not distinguish between a customer using our card with another payment application on it, using a different card, or a true drop in business activity. . We therefore have to accept this risk..

Risk 1c

Delete application

Extradite application

Are solutions cost effective?

■ Chip and Pin

Cost effective IF
cost to implement <
decrease in cost of fraud



Example RTP - cost effective?

RISKS ADVERSE ACTIONS BY CARD ISSUER, OTHER APPLICATION PROVIDER AND THEIR APPLICATIONS

The card issuer may make take actions, for example in managing card content and attending to our requirements, that in practice are not in our best business interests. Likewise, other application providers, or their applications may also act in a manner that is prejudicial to our business. The assets concerned are [our application](#) and [our customers' data](#).

The impacts of such events are: <<Consider highlighted one and incorporate/delete as appropriate>>

- Probable [customer dissatisfaction](#), see
- Possible [adverse press coverage](#), see
- Possible [court action](#), see
- Probable [loss of revenue](#), see
- Probable [unanticipated costs](#), see

The principal threats are [the card issuer](#), [other application providers](#), [other applications](#), [cardholders](#) and [attackers](#).

Risk 1a Our contract with the card issuer is that there will only be one EMV application on the card, that one being ours. Suppose post-issuance there were two or more. We can take action to prevent a second application provider from loading such an application by having a veto on application downloads. The veto is established though inclusion of Package C (Mandated DAP Support, see [2]). Package C is a preventive measure.

EMV Pre loaded

All Changes?

EMV personalised

Is it worth it?

Others down load required



Summary

- CSRS includes concepts of time
- Selecting controls from options
 - *time to detect*
 - *Time to fix (or limit damage)*
 - *Most are preventative - class 1*

BUT



Summary (2)

- What of the off card controls?

- Each Actor should ask
 - *Will it work?*
 - *Will I find out if not?*
 - *In time to fix?*
 - *Does it matter?*
 - *Will it affect my profit?*



Conclusion

- Each Actor will do Risk analysis anyway
- In Event/impact form
 - *Which everyone can follow*
- Derive the card configuration required for risk profile
- Ensure better overall internal control





APPLYING ICS TIME METRICS to GLOBALPLATFORM SMART CARDS

William List & Dr. David Brewer

www.gammassl.co.uk

w.list@ntlworld.com dbrewer@gammassl.co.uk