MANAGEMENT MANAGING THEIR RISKS

William List CA FBCS and Dr David Brewer

W^{m}. List & Co
Gamma Secure Systems Limited

W^{m}. List & Co, 46 Snakes Lane, Woodford Green, Essex IG8 0DF, United Kingdom
Phone/Fax +44 20 8504 6480
w.list@ntlworld .com

Gamma Secure Systems Limited, Diamond House, 149 Frimley Road,
Camberley, Surrey, GU15 2PS, United Kingdom
Phone: + 44 1276 702500
Fax: +44 1276 692903
www.gammassl.co.uk
dbrewer@gammassl.co.uk

ABSTRACT

Every organisation has an internal control system (ICS), some very complex others very basic. These are created on a risk basis. The paper proposes a methodology whereby management can monitor the effectiveness and cost effectiveness of their ICS. In addition it proposes a methodology of managing the ICS and for determining the required controls which is operable by the senior management. It also suggests that the use of IT tools to maintain the documentation of the management system would lead to greater efficiency and assist in training the people involved in the implementation and maintenance of the effective controls.

A much larger paper on this topic can be found at www.gammassl.co.uk/topics/time

KEY WORDS

Management system, Internal Control system, effectiveness, risk treatment plans, ISMS manual, ISO/IEC17799, BS7799-2.

TITLE

MANAGEMENT MANAGING THEIR RISKS

1 INTRODUCTION

All organisations have an internal control system (ICS). In large organisations it is formalised, in the very small organisations it is often implemented by the boss being involved everywhere. Most organisations are somewhere in between these two extremes.

Laws and regulations, (e.g. OECD[1], Sarbannes-Oxley [2], EU draft directive[3]). concerning corporate governance dictate that a system of internal control is an essential element in achieving effective governance. ICSs have two parts:

- Procedures to perform the work necessary to conduct the organisations business. These are called operational procedures.
- Procedures to ensure that the business is conducted as expected. These are called controls.

This description is expanded in COSO [15] and in the UK Audit Practices Board guidance [4]

Information security forms a subset of the ICS as do the other procedures in the IT.

The controls part of the ICS is designed to address the risks the organisation faces and specifically to provide assurance that the majority of events will be detected in sufficient time to counter any adverse impact on the organisation. Some controls try to prevent the event others are designed to detect events that occur and yet others assist recovery when disaster strikes.

It is axiomatic that things will go wrong - people do not always perform as expected, great new products do not sell as well as expected, criminals attack the organisation, acts of God occur, etc. This has always been the case. The conundrum facing management is to decide how much resource to deploy to create just sufficient controls to limit the possibility of bad events occurring and to limit the damage when they do occur.

This paper is divided into the following sections:

- Internal control which summarises the structure of an ICS and discusses the relationship with information security and effectiveness measures.
- Development where a methodology to manage the ICS is proposed together with a different approach to creating a risk treatment plan tailored for senior management participation.
- Conclusion which draws all the strands together.

2 INTERNAL CONTROL

1.1 Internal control structure

The UK Audit Practice Board ([4]) describes a model of internal control, which shows (see figure 1) that the controls flow down from the organisation’s mission statement, business objectives and business risks.

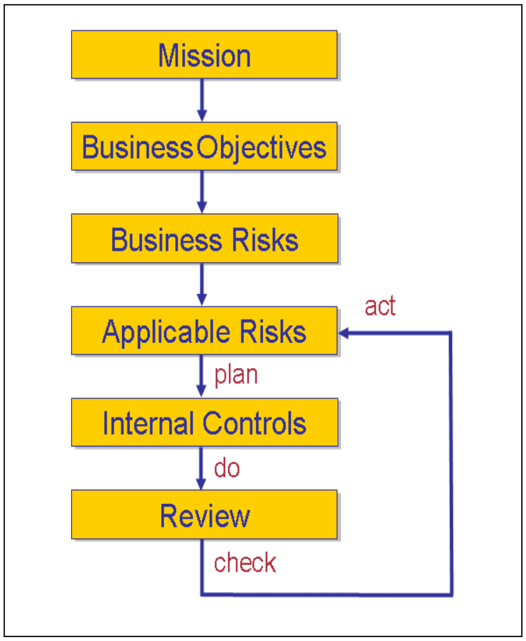


Figure 1 The APB model of internal control

The model also shows that the effectiveness of the internal controls must be regularly reviewed and action taken as appropriate. This is a sound management technique, known as the Deming or Plan-Do-Check-Act (PDCA) model, and is a fundamental principle of standards that conform to ISO Guide 72 [5], such as ISO 9001 (Quality, [6]), ISO 14001 (Environmental, [7]) and BS 7799-2 (Information Security [8]).

1.2 Relationship with information security

The IT Governance Institute [10] concludes that IT should be aligned with the business objectives. Why ever should it not be? The institute's work is a realisation that main board directors in countless organisations have failed to realise that IT is just a tool of the trade, and therefore treat it as something different - aided and abetted by some IT people. The same is true of information security, which, as ISO/IEC 17799 [11] reveals, is not the exclusive realm of IT.

1.3 Effectiveness of internal control

It is axiomatic that things will go wrong (Murphy's Law) and therefore there is a need for an appropriate mixture of preventive, detective and reactive controls. In particular, it is always possible for a control to fail. The effectiveness of an ICS can be measured by the ability of its controls to detect an event in sufficient time to do something positive about it before the occurrence of an adverse impact. (see Annex A for summary of the rationale). This analysis gives rise to the concept of a continuum of control over seven classes.

Controls can be classified as belonging to seven classes (see figure 2)

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.	

Figure 2 Control class definitions

Class 1 corresponds to a preventive control. Such a control either pre-empts the event from occurring, or detects its occurrence as it happens and is able to take immediate defensive action. Medical inoculations, locked doors, and computer access control mechanisms fall into this group. Classes 2-4 correspond to detective controls. All three detect the event after it has happened. The first two facilitate prompt defensive action, the third after the impact has occurred. Intrusion detection devices, whether they concern physical or computer security, and medical health checks fall into this group. Classes 5-7 correspond to reactive controls. They react to the occurrence of the impact, rather than the event itself. Business continuity plans fall into this group, the class distinction being dependent on the state of preparedness.

This mechanism can be used to identify controls that are the most cost effective to address the identified risks at a detailed level.

1.4 Measurement and improvement

Any measurement of the quality of an ICS needs to be independent of external events, for example how many attempts a hacker may make a at introduce a virus. All systems maintain logs of incidents. The information in these logs should include data to show how long it took to detect the incident and how long it took to fix. The extra information will permit an effective analysis to be made of whether, in the light of real incidents, the ICS is performing as expected. Comparison with previous statistics can demonstrate improvement in the ICS.

2 DEVELOPMENT OF A MANAGEMENT SYSTEM

2.1 The management system

The literature describing an ICS (e.g. [4]) does not include a concept of a management system to be part of the whole ICS. ISO standards do propose the concept of a management system [5] and the concept has been implemented in ISO 9000 [6], ISO 14000 [7], and BS7799-2 [8]. Of these the easiest to convert to a management system for the whole ICS is that in BS7799-2[8]. This could be accomplished as shown in figure 3.

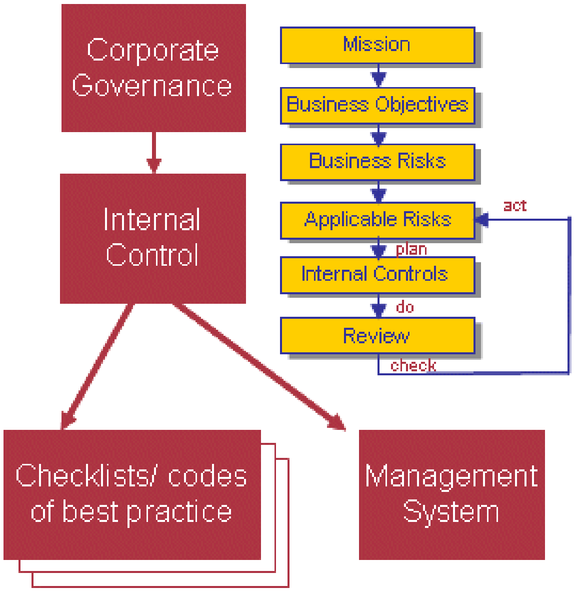


Figure 3 Incorporation of a management system in an ICS

It can be seen from figure 3 that the administration part of the management system is common and a wide variety of control ideas lists can be included to address the various aspects of an ICS, for example information security BS7799-2 [8], accounts preparation, controls over the IT (COBIT) [10], etc. This structure enables management to consider their business risks and then apply the appropriate controls from the checklists of the various areas. The management system should be recorded in a hypertext document. This has the following advantages:

- ❑ Maintenance is much easier to accomplish
- ❑ It (or appropriate parts) can be made available to staff on line which ensures that the current version is available and simplifies the task of awareness training

2.2 Traditional risk treatment

Traditionally the creation of risk treatment plans has involved performing a risk analysis to determine from a combination of identified threats, identified vulnerabilities, asset values and some probability factors where it is cost effective to apply controls and which controls to apply. Once the detailed exercises of the analysis are completed the risk treatment plan is written for presentation to management. Rarely do senior management involve themselves in the detailed analysis and even if they do they find the detail difficult to follow. This may well lead to a disconnect between the business risks that the management understand and the technical solutions from the risk analysis.

2.3 Our approach

We propose a different approach based on 'events' and 'impacts' where the risk treatment plan is the story of how the organisation deploys controls to address each event/impact pair until the residual risk of an occurrence is reduced to an acceptable situation

2.3.1 Events

The events referred to in this paper are concerns of the management likely to cause damage to the organisation. The insert (below) lists those events, which in our BS7799 work we feel are common across many businesses. In addition we would add other events that were specific to that particular organisation. Examples would be '*our sales are materially reduced*', '*our customers do not pay us*', etc.

Events that are likely to be common across many businesses are:

- Theft
- Acts of God, vandals and terrorists
- Regular fraud
- IT failure
- Hacking
- Denial of Service attacks
- Disclosure
- Breach of the law

Typically, any occurrence of such events would be reported to management, the speed of reporting being a function of their severity. Think of the event as a newspaper headline.

2.3.2 Impacts

Likewise, it is possible to characterise the damage, or impact of an event in a standard manner. The insert (below) lists those impacts, which again in our BS7799 work we feel are common across many businesses.

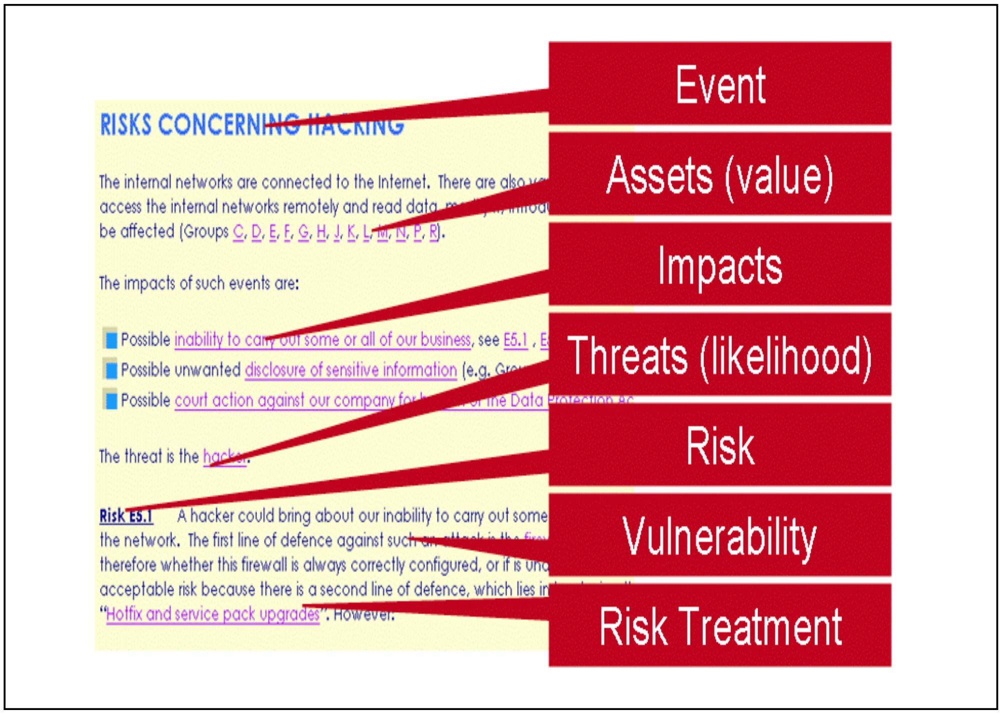
Impacts that are likely to be common across many businesses are:

- Customer dissatisfaction
- Adverse press coverage
- Loss of revenue
- Unanticipated costs
- Inability to carry out some or all of its business
- Loss of the monetary value of buildings and contents

The occurrence of an event may give rise to several impacts and may also trigger other events.

2.3.3 Risk Treatment Plans

Risk treatment is an ISO term that is means the "*treatment process of selection and implementation of measures to modify risk* [14]". We can use this concept to develop a simple methodology for applying our fundamental theory. Figure 4 shows a fragment from our stylised form of a BS7799-2:2002 Risk Treatment Plan (RTP).



RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also
access the internal networks remotely and read data
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 , E
- Possible unwanted disclosure of sensitive information (e.g. Gro
- Possible court action against our company for breach of the Data Protection Ac

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 fire
therefore whether this firewall is always correctly configured, or if is un
acceptable risk because there is a second line of defence, which lies in
"Hotfix and service pack upgrades". However.

Figure 4: A fragment of a stylised Risk Treatment Plan

2.4 Our structure for Risk Treatment Plans

The process of producing the RTPs can be described in terms of a series of steps

Step 1 - identify the events

Name the event and briefly describe it, those in the list above and the business events.

Step 2 - identify the assets

We usually start with a generic list that includes such things as:

- ❑ Buildings and contents
- ❑ IT hardware and networks

We will add to this list and otherwise modify it as necessary. The assets that require protection are derived from the analysis, rather than the other way round (which unfortunately seems to be the conventional way of carrying out a risk assessment).

Step 3 - identify the impacts

Our usual approach is to start with the standard impacts described above and augment them with client specific impacts as required.

Step 4 - identify the threats

We usually start with a generic list of threat agents that includes such entries as:

- ❑ Errors and mistakes.
- ❑ Fire, flood and other forms of "natural disaster"
- ❑ Hackers

We will add to this list and otherwise modify it as necessary.

Step 5 - produce the RTPs

This step is repeated for each event.

First (see Figure 4), write down the description of the event and list the assets that are affected.

RISKS CONCERNING **HACKING**

The internal networks are connected to the Internet. There are also various modem connections. It may be possible for some unknown person to access the internal networks remotely and read data, modify it, introduce malicious programs and cause other damage.

All IT based assets may be affected (Groups E, F, G, H, I, J, K).

Second, identify the applicable impacts and order them in the priority they are to receive.

The impacts of such events are:

Probable inability to carry out some or all of our business, see S5.1, S5.2 , S5.3 , S5.4

Possible court action against us, see S5.5

Probable loss of all forms of data and information, see ?

Possible/Probable unauthorised disclosure of classified information, see S5.2 , S5.3

Third, list the applicable threats.

The principal threat is the hacker.

NOTE: In the example the term 'hacker' denotes anyone acting in the role of a hacker be they insiders or third parties

Fourth, repeat the steps 5a - 5d below until all the impacts have been dealt with.

Step 5a - identify the risks leading to a particular impact for known threats

Consider the event and the impact.

The first question to ask is "what is being done about it already? ".

We then ask, what do these procedures and technology accomplish in terms of this particular event-impact? And write down the answer in narrative form. Say how a threat agent, in the context of this event, could bring about the impact under consideration,

A hacker could bring about the inability of the organisation to carry out some or all of its business by mounting a denial of service (DoS)[1] attack on the network.

[1] The objective here is to freeze or lock up resources of the target network. Ultimately, the target becomes inaccessible and unable to respond. DoS attacks come in two varieties: network flooding (e.g. “ping flood”), crashes/overloads (e.g. “SYN flood”, “ping of death”, “teardrop”, “LAND”)

You then write down, in as few words as possible, what the (established) procedures and technology will do about this, The first line of defence against such an attack is the firewall provided by our ISP as a managed service.

You then identify any residual risk

We do not know therefore whether this firewall is always correctly configured, or if is under attack.

NOTE: this is tantamount to saying, "what if the first control does not work?"

We then ask if this risk is acceptable or not.

If the risk is not acceptable you then identify other actions that could be (or are) taken

We will ensure that our ISP is liable for damage by hacking. Legal Department says this is not possible -action rejected.

We have a second line of defence, which lies in hardening the network components in accordance with the IT policy for "Hotfix and service pack upgrades".

The residual risk is therefore acceptable

NOTE: The hotfix and service pack policy would be described elsewhere as it applies to a number of RTPs -but in essence would say "*we apply all fixes notified to us by suppliers for software in use. In addition we review CERT notifications of known vulnerabilities and implement necessary fixes*"

The analysis proceeds in this way until all of the controls that are used (or are to be used) and their effects have been documented. It concludes with a statement that the risk is acceptable or even though it is unacceptable nothing, cost effective can be done about it so the organisation will live with it

The next thread might consider hostile code insertion.

Step 5b - identify the risks leading to a particular impact for unknown threats

It is prudent to ensure that appropriate controls are in place to deal with the situation where the event has occurred for some unanticipated reason, i.e., the threat agent and/or the attack method was not known or anticipated at the time the analysis is performed.

Should a hacker effect a DOS attack despite our efforts then we will disconnect our network, take any cleansing actions required, notify internal users of the reason. Once the incident is investigated we will restart the network. Customer relations department will have preprepared notices informing customers, press etc of the position and the actions we are taking

Step 5c - dealing with unacceptable residual risks

If a thread terminates with an unacceptable residual risk we need to do something about it. What needs to be done about the unacceptable risk is agreed - which at the very least will be to investigate the options. Actions that need to be followed up are added to a 'To-Do-List'. It is then a question of project managing the To-Do-List. Of course, whilst a particular problem is being resolved, we are running an unacceptable risk. It is possible that we cannot do anything about that apart from keeping our fingers crossed. Otherwise, it would be appropriate to introduce some short-term measure.

Step 5d - optimising the ICS

The RTP thus far describes the control structure that exists and, via the To-Do-List, also that which is planned for the future.

Identify the class (1-7) for each control (figure 2). Use the event and impact data and figure 2 to determine whether a different class for a particular control would be more appropriate. Make your decisions in the context of the other controls; in particular the other controls in the same thread.

Cross check all the controls identified as required with the other ideas lists and where those said to be best practice are not to be used confirm either that they do not apply or amend the RTPs to add them in.

Step 6 - maintenance

There will be incidents and changes in technology in use or business circumstances which will require the RTPs to be revised. The general management system process will force reviews at regular intervals for all the documentation of the management systems including the RTPs.

Clearly it is probable that in completing the RTPs certain detailed risks will be overlooked. During the maintenance phase consideration of the incidents that have occurred will lead to identification of missing detailed risks. In addition for technical threats and vulnerabilities organisations should implement fixes from CERTs and suppliers as they become available.

3 RESULTS IN PRACTICE

We have applied this method of risk analysis (together with our Hypertext ISMS Manual) in a number of client situations. In particular it was applied in the Government of Mauritius as a part of a contract to implement ISO/IEC17799 throughout the government. The results of using this method were that senior Civil Servants were able to identify the necessary IT and user controls to limit their business risks to an acceptable level within some few weeks of first hearing about the method. Four departments managed to attain 'certification' to BS7799-2 within four months of commencing the task of building their ISMS manuals. The Government of Mauritius made a presentation on this contract to the 7799 Goes Global conference in December 2004 [16].

4 CONCLUSION

The requirement to demonstrate an effective internal control system, at least over financial reporting, is increasingly become a regulatory requirement for listed companies. All organisations have some sort of internal control system and if it is well managed then the organisation will benefit.

All internal control systems require to be managed, otherwise they themselves are out of control. To achieve this we propose that organisations use the system described in BS7799-2[8] augmented by additional ideas lists or codes of best practice so that the system is seen to cover all business areas.

The management need metrics to determine if the ICS is effective (and cost effective). We propose that the concept of detecting events before they damage the organisation or limiting any damage that occurs is the basis for demonstrating efficiency of an ICS. Confirmation of the effectiveness can be achieved by analysing the inevitable incidents to determine if the objective has been met.

The crucial area in ICS design is to identify the business risks and explicitly link the controls in place to those risks. We propose a formalised narrative description of risks and the risk treatment which commences by identifying the events of concern to the organisation and their impact, should they occur, on the organisation. The narrative then describes the controls (to be) implemented to reduce the risk to an acceptable level

5 REFERENCES

[1] Organisation for Economic Co-operation and Development, Corporate Governance, see http://www.oecd.org/

[2] Sarbanes-Oxley Act of 2002, USA Congress, an Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes, see http://news.findlaw.com/

[3] "Proposal for a Directive of the European Parliament and of the Council on statutory audit of annual accounts and consolidated accounts and amending Council Directives 78/660/EEC and 83/349/EEC", COM2004-177 (see http://europa.eu.int/eur-lex)

[4] "Briefing paper - Providing Assurance on the effectiveness of Internal Control" issued by the Audit Practices Board July 2001, see http://www.apb.org.uk/ Copies from ABG Professional Information

[5] "Guidelines for the justification and development of management system standards", ISO Guide 72:2001

[6] "Quality management systems – Requirements", ISO 9001:2000

[7] "Environmental management systems - Specification with guidance for use", ISO 14001:1966

[8] "Information security management systems - Specification with guidance for use", BS 7799-2:2002

[9] The Bank of International Settlements, the "New Basel 2 Accord", see http://www.bis.org/

[10] The IT Governance Institute, see the Board Briefing and the COBIT Framework in particular, http://www.itgi.org/

[11] "Information technology - Code of practice for information security management", BS ISO/IEC 17799:2000

[12] "Chinese Wall Security Policy", Brewer, D.F.C., Nash, M.J., Proceedings of the IEEE Symposium on Research in Security and Privacy, May 1989, Oakland, California. (pp 206-14). Also see www.gammassl.co.uk/topics/chinesewall.html

[13] "Gamma's ICS", August 2004, www.gammassl.co.uk/topics/ics/gamma.html

[14] Risk management —Vocabulary —Guidelines for use in standards: ISO guide 73:2002

[15] COSO Internal Control - Integrated framework - Executive summary,

www.coso.org/publications/executive_summary_integrated_framework.htm

[16] Government of Mauritius presentation to 7799 Goes Global conference London December 2004 http://www.gammassl.co.uk/topics/ics/fast.html. Paper download button is at the foot of the page.

ANNEX A

Figure A1 shows the impact on the bottom line of an event that is detected by the organisation's management far too late to do anything about it.

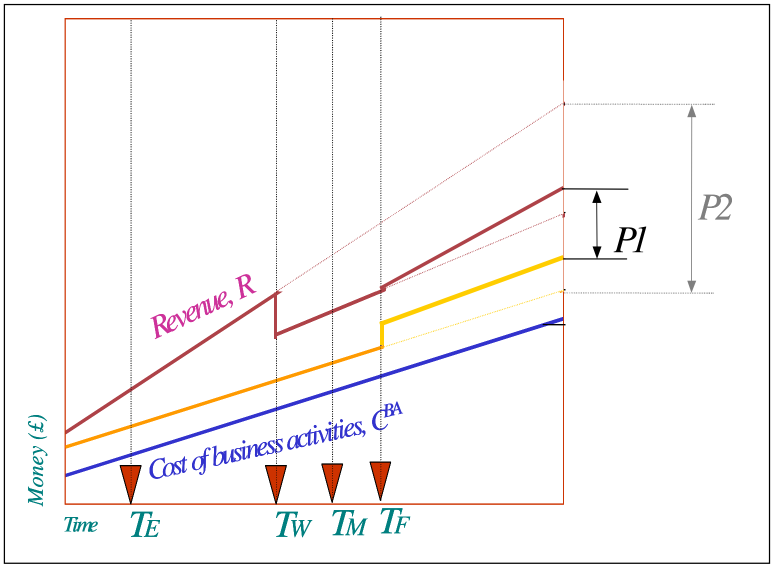


Figure A1: The impact of detecting an effect too late

The event occurs at time T_E. On expiry of some "time window" (the time between an even occurring and an impact on the organisation) at time T_W, there is an impact in the form of a dramatic reduction in revenue. Management discover the problem at time T_M and fix the problem at time T_F. There is a cost involved in fixing the problem and therefore a consequent increase in costs. Fixing the problem has a beneficial effect on revenues, but the profit (*P1*) is significantly less than it would have been had the event never occurred (*P2*).

Figure A2 illustrates what would happen if the event was detected in good time.

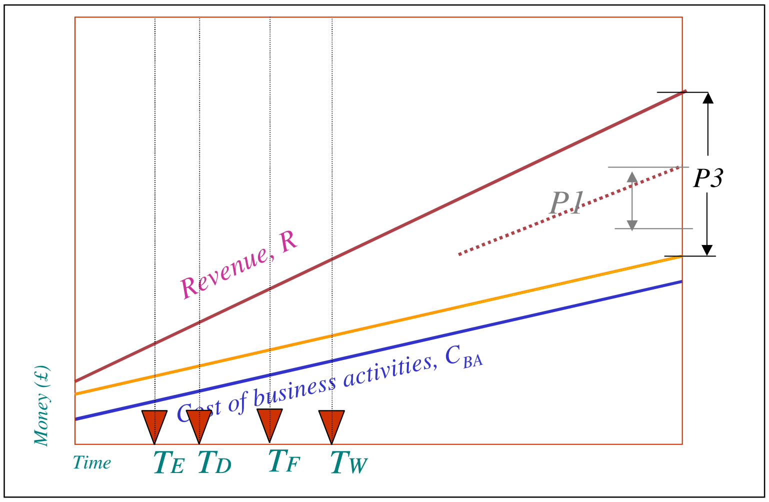


Figure A2: The impact of detecting an event in good time

In this case, the event is detected by the ICS at time T_D and fixed well before the expiry of the time window. There is an associated cost to fix, but that may be considerably less than the equivalent case in figure A1. Because remedial action takes place before the expiry of the time window there is no revenue penalty. Consequently the profit (*P3*) is significantly greater than in the previous case.