Opportunity Exploitation Plans

By Dr. David Brewer and Mr. William List, CA, FBCS, CITP

Introduction

In this paper, we extend this time model [1] to address the first part of internal control by considering *opportunities* and *benefits*, being respectively the converse of events and impacts. The paper then proposes a methodology for creating Opportunity Exploitation Plans (OEPs), being the converse of RTPs, and illustrates it using data from a case study example.

Background

The time paper "Measuring the effectiveness of an internal control system" [1] proposes that an Internal Control System (ICS) can be considered to be made up of 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.

That paper restricts its considerations to the second part. It introduces time as a metric to measure the effectiveness of an ICS by noting the time at which some event occurs, the time of its detection and the time that the problem caused by the event is fixed, relative to a "time window" on the expiry of which some adverse impact occurs. The paper asserts that an effective ICS is one that detects the event in sufficient time to do something positive about it before the impact occurs. The paper also introduces a methodology for specifying Risk Treatment Plans (RTPs), for example as required by ISO/IEC 27001:2005.

The Time Theory Revisited

On the right we recall the extant theory which deals with RTPs and thus the second part of internal control. In this column we explain how OEPs work by contrast to RTPs. Events become *opportunities* and impacts become *benefits*. There is still a time window, but in this case on expiry of the time window the opportunity is lost.

At some time T_O an opportunity O arises. It may be created internally by the organisation, or externally. Associated with the opportunity is a benefit B. There is a window T_W and when it expires, the benefit goes away. In other words, we have a lost opportunity. We detect the benefit at T_D. There is an associated cost to reap the benefit C_R, which we do at time T_R provided $T_R < T_W$.

The Extant "Time Model" Concept

The Time Model [1] explains that an effective internal control system (ICS) is able to detect events in sufficient time to doing something about them before the onset of a disaster, or failing that has plans and processes in place to mitigate the impact. The diagrams illustrate the relationships between the time of detection (T_D if detected by the ICS, or if detected by some other means T_M, e.g. reported on CNN); the time that the damage caused by the event is fixed (T_F), should it be possible and appropriate to fix it, or otherwise resolve the problem; and the time limit after which (T_W), if the damage is not fixed, some impact penalty I_P (whether financial or otherwise) is incurred.

If we do not detect the opportunity, it merely passes us by. There is no cost and no gain. On the other hand we might detect the opportunity but fail to succeed in our response. In this case, as shown in Figure 1, there is a cost (C_R) but no benefit. Of course, in practice, the loss of one opportunity might give rise to another. We would model each of these separately.

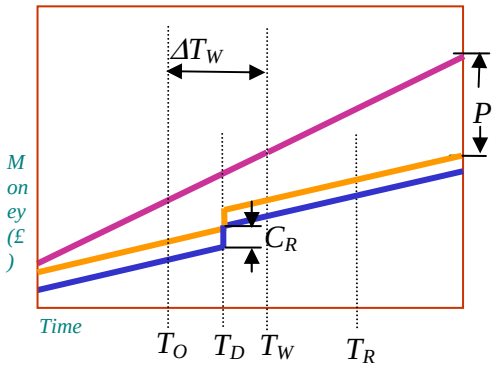


Figure 1: Too late, the opportunity is lost, it has consumed resource to pursue but there is no benefit

If we detect the opportunity in time (indeed, maybe we have a head start because the opportunity is of our own creation), we may reap the benefit (see Figure 2).

Thus OEPs are the converse of RTPs. In the one case (RTPs) if nothing is done there is a loss. In the other (OEPs) there is no gain.

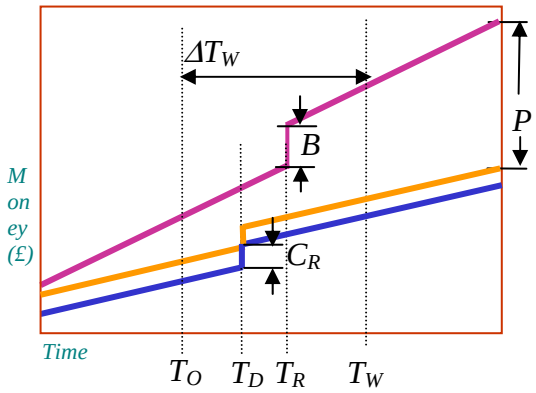
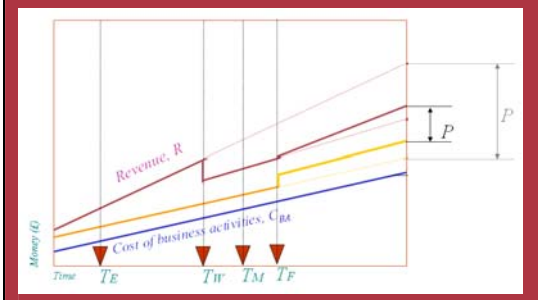


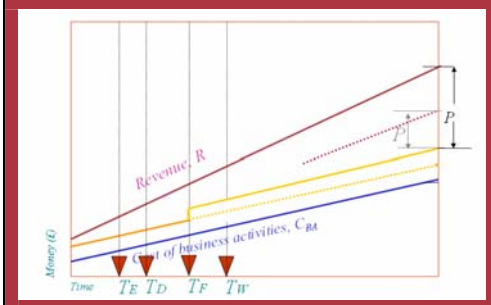
Figure 2: In time: the benefit is reaped within the time window

The first figure (below) shows the effect of detecting the event too late. The event happens (time T_E). It is not detected by the ICS, but by management (time T_M), for example, because sales are down. By this time the impact has occurred (since $T_M \geq T_W$). Some time later management fix the problem (time T_F) but there is an associated cost with that "fixing" activity. The remedy, in this case, is able to restore some of the revenues but not all. In consequence, the overall profit is significantly less than what would have resulted if the impact had not occurred.



The effect of detecting the event too late

In the second figure, the ICS detects the event (time T_D) in sufficient time for the problem to be rectified before the impact occurs (time (T_W). There might still be an associated cost to fix, but that may well be significantly less than in the previous scenario because of the earlier detection. More importantly there is no impact penalty. Consequently the overall profit is close to what it would have been if the event had not occurred and, in t his case, considerably higher than in the previous scenario.



The effect of detecting the event in good time

Our paper [1] explains how cost considerations can affect the design of an effective ICS, and thereby how to strive an acceptable balance between the cost of failure and the cost of control.

Opportunity Exploitation Plans (OEPs)

Structure

OEPs are similar in structure to RTPs, as shown in Table 1.

RTP	OEP
Explanation of the *event*	Explanation of the *opportunity*
Assets *affected* (i.e. assets to be protected)	Assets *exploited* (Note all these ought to be in the list of assets to be protected)
Impacts	*Benefits*
Threat agents	*Facilitating* agents
	Risks (with reference to *RTPs* that deal with them)
Risk statements, looking at each *event-impact* pair, asking questions such as "*what if it doesn't work*" until the *residual risk is acceptable*	*Opportunity* statements, looking at each *opportunity-benefit* pair, asking questions such as "*how can I take advantage of this*" until *optimum advantage has been taken*

Table 1: Correspondence between the content of a RTP and an OEP

Note that there is no correspondence in an RTP for the OEP risk parameter. This is highlighted by the shaded blank cell in Table 1. Although it might be argued that a RTP may have associated opportunities we have chosen to deliberately ignore this possibility and thereby introduce an asymmetry into the theory. The reason for this is that, as far as we can judge, such opportunities are either illegal or unethical as the corresponding OEP may imply deliberate action on behalf of the malefactor to create the opportunity. Insurance fraud would be an example.

Figure 3 shows an extract from a real OEP (from our case example), showing the structure and exemplifying its content. The various components of the OEP, as indicated in Table 1, are explained in the following paragraphs.

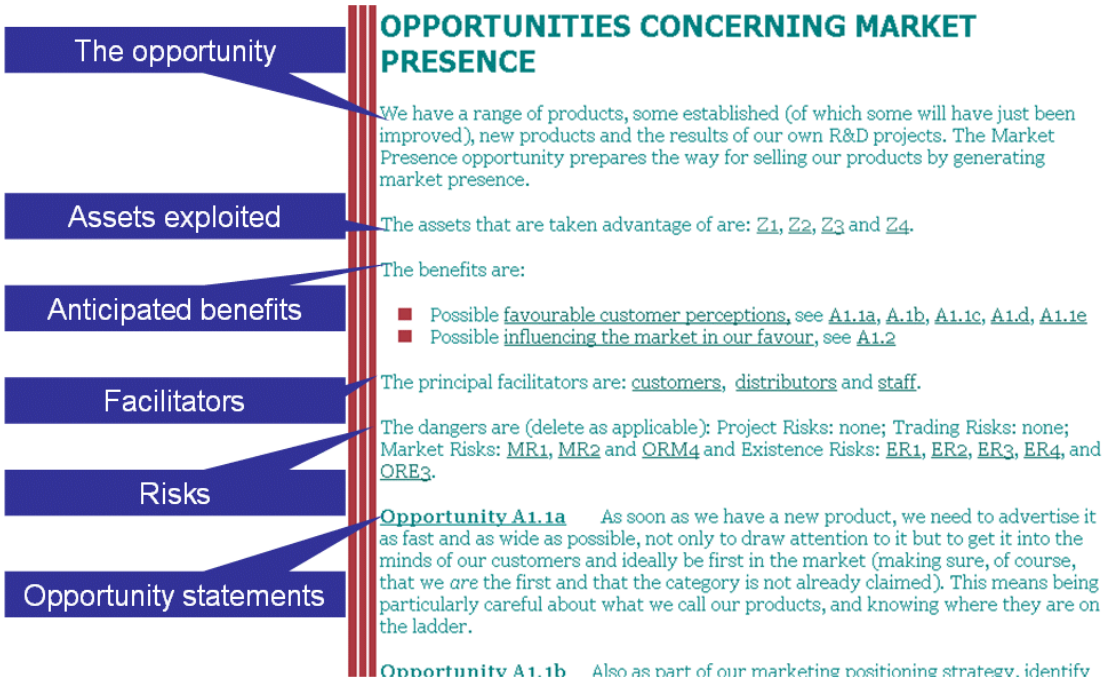


Figure 3: Extract of a real OEP showing the structure described in the following sections of this paper

The Opportunity

Our case study concerns sales and marketing. There are three generic opportunities that most probably apply to "for profit" organisations and they are: Market Presence, Enquiry and Product Delivery. These form the subject of the OEPs and correspond to the generic events described in [1], e.g. Theft, Acts of God, Fraud, IT Failure etc in the RTPs. The third opportunity is described as Product Delivery rather than Sales because in some organisations (and in particular our case study organisation) R&D, which is internally funded and does not result from a sale, presents the same type of opportunity.

By way of example, these three generic opportunities have been described by our case study organisation as follows:

- Market Presence: "We have a range of products, some established (of which some will have just been improved), new products and the results of our own R&D projects. The Market Presence opportunity prepares the way for selling our products by generating *market presence*."
- Enquiry: "The next step towards a sale is a customer enquiry."
- Product Delivery: "Once we have made a sale we have the opportunity to deliver the product. We also have the opportunity for delivering a product as the result of commissioning an internal research project. The product delivery opportunity may prepare the way for developing new products."

Exploited Assets

All organisations have assets. Certain of theses assets will be exploited to reap the benefits of an opportunity and are shown in an OEP. All assets should be protected through RTPs. For our case study organisation, the assets that may be exploited are:

- channels to market;
- existing favourable customer perceptions;
- product(s);
- unique selling points.

These assets are related to the opportunities as shown in the Table 2.

	The opportunity of:		
Assets that are exploited	Market Presence	Enquiry	Product Delivery
channels to market	✓	✓	
existing favourable customer perceptions	✓	✓	
product	✓	✓	✓
unique selling points	✓	✓	

Table 2: Relation of (example) exploited assets to (example) opportunities

Anticipated Benefits

In our analysis for this particular organisation of its sales and marketing processes, we identified the following list of benefits (in alphabetic order):

- close the sale and win the business;

- favourable customer perceptions;
- increased revenue;
- influencing the market in our favour;
- product improvements and new products.

These benefits are related to the opportunities as shown in Table 3.

Benefit	The opportunity of:		
	Market Presence	Enquiry	Product Delivery
close the sale and win the business		✓	
favourable customer perceptions	✓	✓	✓
increased revenue			✓
influencing the market in our favour	✓		
product improvements and new products			✓

Table 3: Relation of (example) benefits to (example) opportunities

Facilitators

The facilitator is the person or entity that initiates the opportunity. In our example organisation, the list of facilitators is (in alphabetic order):

- customers;
- distributors;
- staff.

These facilitators are related to the opportunities as shown in Table 4. Note the facilitator "staff". At the outset it was tempting to divide this category into its components: marketing, sales, support, help desk, etc. However, we found that it was company policy to make all staff responsible for ensuring customer satisfaction, no matter what their role in the organisation. It was therefore decided to group all of these facilitators under the one heading. This did not pose a problem in creating the OEPs.

Facilitators	The opportunity of:		
	Market Presence	Enquiry	Product Delivery
customers	✓	✓	
distributors	✓		
staff	✓		✓

Table 4: Relation of (example) facilitators to (example) opportunities

Risks

In exploiting an opportunity there may be risks. Rather than attempt to deal with these at the same time as developing the OEP, we factor these out into the RTPs. In the example given in Figure 1, these are referenced to the organisation's principle risk register, which in this case is partitioned into project risks (risks resulting from having a contract to supply goods and services), trading risks (risks resulting from trading in the money market), market risks (risks relating to the market that the organisation provides its goods and services to, which is not the money market) and existence risks (risks, common to all organisations, by virtue that they exist). The OEP refers to the risks applicable to the opportunity under consideration. In the example, the risk register refers to the RTPs that deal with those risks.

Opportunity Statements

The opportunity statements form the bulk of the OEP. They follow the same structure as described in [1] for risks but with the following similarities and differences:

- Similarities:
  - The statements are grouped in *threads* (see [1]);
  - The statements are written in natural language with a "tell it like a story approach".
- Differences:
  - Whereas in creating a RTP it is usual to ask "what if that does not work", in creating an OEP it is usual to ask "and what further opportunity can we exploit";
  - Whereas in a RTP a thread ends with a statement accepting that the residual risk is acceptable, an OEP thread ends with a statement that no further exploitation is beneficial.

We are unable, for reasons of commercial sensitivity, to publish all the opportunity statements that were produced for our case study example. However, the following extracts have been permitted:

> **Opportunity A1.1a** As soon as we have a new product, we need to advertise it as fast and as wide as possible, not only to draw attention to it but to get it into the minds of our customers and ideally be first in the market (making sure, of course, that we *are* the first and that the category is not already claimed). This means being particularly careful about what we call our products, and knowing where they are on the ladder.
>
> ….
>
> **Opportunity A1.1e** We reinforce this publicity by telling as many people that we know, for example existing customers and distributors. Distributors ought then to advertise on our behalf. In taking all of these steps (A1.1a, … and A1.1e) to advertise the product we will have met our current requirements for taking advertisement advantage of the product.

Note the final statement in this thread ("In taking all these steps … the product") is the statement concerning the (current) maximum exploitation of the opportunity.

Summary and Conclusions

In this paper we have extended the time model proposed in [1] to cover the first part of an ICS. In doing so, we have introduced the concept of an OEP and have explained its structure with the aid of a case study example.

OEPs appear to be a useful counterpart to RTPs in practice. OEPs provided a major contribution to the case study project described in this paper by focussing attention on the first part of an ICS, i.e., the procedures for "getting the job done".

Although our case study was of necessity restricted to the subject of sales and marketing, the existence of other examples is easy to postulate. Take, for example, a hospital. The principal opportunity, indeed the very reason for its existence, is that a "patient requires treatment". Benefits will include "saving a persons life". There are controls, but the vast majority of hospital procedures are of the OEP form.

The OEP concept is therefore an essential component of an ICS.

References

[1] "*Measuring the effectiveness of an internal control system*", Brewer, D.F.C., List, W., March 2004, http://www.gammassl.co.uk/topics/time

[2] "*Information security management systems - Requirements*", ISO/IEC 27001:2005

About the authors

Dr. David Brewer is a founder director of Gamma. He has been involved in information security since he left university, and is an internationally recognised consultant in that subject. He was part of the team who created the ITSEC and the Common Criteria, and has worked for a wide range of government departments and commercial organisations both at home and abroad.

William List, CA, hon FCBS, CITP

Dr. David Brewer

Mr. William List, CA hon FBCS CITP, is the proprietor of W^{m}. List & Co. He has been involved in security and audit for some 40 years. He has been involved in the development of secure business applications and the development of various accounting and IT standards. He retired as a partner in KPMG. He is the immediate past chairman of the BCS security expert panel.

Both are currently part of the international team developing the 7799 family of standards, and are two of the driving forces behind the Part 2 ISMS standard. They provided training in implementing ISO/IEC 17799 and have assisted many clients to build ISMSs since 1998 in Europe, East Africa and the Far East.