Exploiting an Integrated Management System

By Dr. David Brewer MIOD, Dr. Michael Nash FBCS, William List CA, hon. FBCS

Introduction

In this paper we propose a structure for an integrated Management System (MS) and show how it can be exploited to assist an organisation to achieve its mission by fulfilling *all* aspects of its business objectives.

Our proposed structure:

- Satisfies the principles specified by the UK Audit Practices Board [1] for internal control;
- Complies with the requirements of ISO management system standards.

We start with a consideration of the Deming model of process management and show how it is implicit in both the advice given by the UK Audit Practices Board on how to structure a system of internal control, and the requirements of ISO management system standards.

We then explain how a MS can implement the Deming model, and fulfil all aspects of an organisation's business objectives, using Opportunity Exploitation Plans (OEPs) and Risk Treatment Plans (RTPs).

Taken together, the OEPs and RTPs should identify all the procedures necessary for an organisation to meet its business objectives and ensure that business is conducted in accordance with its legal, regulatory, contractual and corporate governance obligations. However, there is a limitation in the Deming model in that omissions are only detected after the event. We explain why this is dangerous and that there is therefore a requirement for some other form of analysis of potential risks, a "Safety Net". We suggest how one can be implemented using "Alternative Ideas Lists" (AILs).

We present a case study, using a Sales and Marketing paradigm to exemplify the OEP, RTP and Safety Net concepts, and show how these concepts can be exploited in fulfilment of all other business objectives.

Finally, we draw our conclusions.

The Deming Model

Following the publication of the Turnbull Report [2], the UK Audit Practices Board published a set of guidelines on the structure of an Internal Control System (ICS) [1], see Figure 1.

Figure 1: The APB model of internal control

As shown in the figure, there are activities associated with the internal controls, and therefore form part of the ICS, but which do not constitute the internal controls themselves. These activities (mission, business risks, applicable risks and review) are the means for establishing and policing the ICS. The review loop, which seeks to determine the effectiveness of the ICS and take action accordingly, is well known in ISO circles as the Deming model or Plan-Do-Check-Act (PDCA) cycle:

- PLAN: decide what you want to do;
- DO: do it;
- CHECK: determine how well it is working;
- ACT: take action accordingly.

There are now many widely accepted standards that are based on a Deming model. Amongst these are three well known international standards:

- ISO 9001 [3], which is a specification for a Quality Management System (QMS);
- ISO 14001 [4], which is a specification for an Environmental Management System (EMS);

- ISO/IEC 27001[1] [5], which is a specification for an Information Security Management System (ISMS).

Common to all of these standards is an explicit PDCA framework and thus the Deming model. Furthermore, the process required by each of these standards matches the guidelines of the UK Audit Practices Board for effective internal control.

Now that these standards are firmly established, the Certification Bodies (i.e. the organisations that certify organisations as being conformant to these standards) are advocating an integrated approach, whereby an organisation has a single MS that is conformant to several standards. The primary driver behind this initiative is the realisation that having independent MS, and by implication each being under the direction of distinct, autonomous management teams, is not conducive to good business practice. There is a grave danger that each would pull in different directions and not necessarily work together as a cohesive force in pursuit of a common objective. The good news is that such integration is well within the art of the possible [6].

Thus in proposing an integrated MS structure it makes sense to base it on this common PDCA framework.

Implementation

Internal Control

An ICS is the way in which management deploys the organisation's resources to achieve the organisation's objectives. It has 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.

OEPs and RTPs

ISO/IEC 27001 recognises the necessity of selecting controls on the basis of their ability to reduce risk to an acceptable level. It introduces the concept of a Risk Treatment Plan (RTP) as the means to select the appropriate controls, i.e., those that should reduce risk to an acceptable level and no others.

RTPs, however, only address the second part of an ICS. In order to address the first part, we have devised the complementary concept of an Opportunity Exploitation Plan (OEP) [7].

RTPs draw a link between business *events* and adverse *impacts* to identify the controls necessary to reduce risk to an acceptable level [8]. OEPs draw a link between business *opportunities* and business *benefits* to create the procedures necessary to exploit the opportunities to reap the benefits.

Proposed MS Structure

Figure 2 shows the proposed structure of an integrated MS using this common PDCA framework. It is presented as four quadrants, one for each phase of the PDCA cycle. It embraces the RTP and OEP concepts necessary to identify *all* the internal controls, and thus establishes a complete system of internal control.

The operational procedures and controls are identified in the PLAN phase and put into practice in the DO phase. In the CHECK and ACT phases the organisation takes stock of the ability of its internal controls to meet its business objectives and satisfy its legal, regulatory, contractual and corporate governance obligations.

With the exception of the "safety net", which is discussed later, we explain the components of each quadrant in the following four sections.

Plan

Starting with the PLAN phase, the first activity is a statement of the organisation's mission. This activity serves the purpose of establishing the overall context of the ICS. This leads to a statement of the organisation's business objectives.

The business objectives give rise to:

- Statements of policy;

- Business risks;

- Business opportunities.

An example of a policy statement would be Henry Ford's famous remark "you can have any colour car you like, provided that it is black". The statement constrains the operational procedures and controls.

As suggested by [1], some risks, in the absence of any internal control, may be acceptable. In this case the risk is screened from further consideration

[1] This International Standard has replaced the widely used British ISMS Standard BS7799-2

and is termed a "non-applicable risk"[2]. If, in the judgment of the management, the risk is unacceptable, it is termed an "applicable risk". In this case, there will be a need for internal controls to reduce that risk to an acceptable level, and these are determined as a result of creating the RTPs.

Business opportunities are dealt with in a similar way. The opportunities are first distinguished as being applicable or not. The operational processes necessary to exploit the applicable opportunities are then derived from the OEPs.

Check

The CHECK phase includes three activities that are required by the Common PDCA Framework, being internal audit, management review and customer feedback. In addition, other check activities can be included such as the routine reconciliation checks.

Act

The ACT phase includes the three activities required by the Common PDCA Framework, being corrective action, preventive action and improvement.

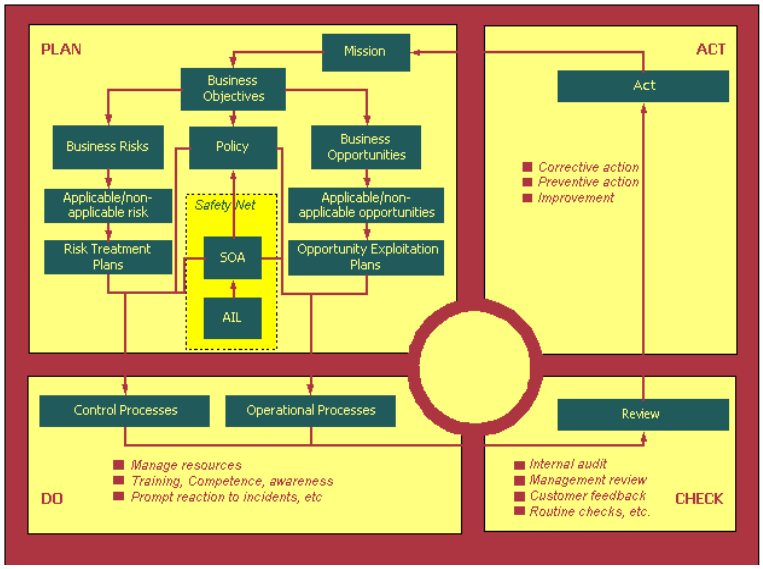

Figure 2: Integrated MS structure

Do

In the DO phase the operational procedures and controls are applied. As required by the Common PDCA Framework, there are a variety of other activities including:

- The management of resources;
- Ensuring that all staff are appropriately aware, suitably trained and are competent to carry out their respective responsibilities;
- Ensuring prompt reaction to incidents and opportunities.

Limitations

Theoretically, the development of OEPs and RTPs should be sufficient to identify all the internal controls.

In practice, however, there may be errors of omission because risks and opportunities are imperfectly understood, particularly when the analysis is first carried out during the Plan phase of the PDCA cycle. These should be found and corrected during the Check and Act phases, but, of course, that may be too late to avoid preventable losses (or lost opportunities) to the organisation. As an additional *planning* check, we therefore introduce the concept of an "Alternative Ideas List" (AIL), which acts as a "Safety Net".

The Safety Net

The safety net consists of one or more Alternative Ideas Lists (AILs).

[2] Although it is prudent to have a RTP for treating the risk that a non-applicable risk becomes an applicable risk

An AIL is a set of suggested controls or operational procedures. Often these have been derived from a study of best practice of some particular discipline, such as information security, quality and finance. A MS may use as many AILs as management wish. An example of an AIL is Annex A to ISO/IEC 27001. Another is the Product Realisation requirements (section 7) of ISO 9001.

Each control (or operational procedure) in the AIL is reviewed to determine whether it is applicable to the organisation or not. There are three cases:

- Case 1: the control (or operational procedure) in the AIL is applicable and has been identified in a RTP (or OEP) already;
- Case 2: the control (or operational procedure) in the AIL is applicable but has not been identified in a RTP (or OEP);
- Case 3: the control (or operational procedure) in the AIL is not-applicable.

Case 2 indicates that there has been an error of omission in developing the RTPs (or OEPs). Thus the AIL acts as a safety-net for the OEP and RTP activities.

An SOA is an AIL for which all controls (or operational procedures) have been declared as being applicable or non-applicable.

Note that in Figure 2 there is a link between SOA and Policy. This is a practical device, as it is often simpler to introduce a missing control through the facility of creating a policy statement than it is to rework the RTPs or OEPs.

The safety net therefore consists of identifying and creating one or more Alternative Ideas Lists, then reviewing their contents to check that RTPs and OEPs are indeed complete, and finally creating the associated Statements of Applicability (SOAs) to record the results of the review.

Case Study

We have built a MS using this structure. It is certified as being conformant to both ISO 9001 and ISO/IEC 27001. This demonstrates that the proposed MS structure is conformant with the Common PDCA Framework. There are two AILs and associated SOAs, one for each standard.

We have extended the MS by the addition of two RTPs and three OEPs to address the risks and threats associated with Sales and Marketing. The first RTP deals with the risk that a niche product transitions to a commodity product and the second deals with the risk of failing to win business. The OEPs are described in [7], and concern market presence, customer enquiries and product delivery.

As a test of the Safety Net concept, we have identified and applied an AIL in support of the Sales and Marketing process. The chosen AIL was Ries and Trout's book entitled "*The 22 Immutable Laws of Marketing*" [9]. These "laws" do not constitute a standard in any sense of the word. Instead they are a set of suggestions, based on the authors' experience and observations concerning good marketing practice. The choice of [9] reinforces why we called an AIL an Alternative Ideas List as, being suggestions rather than requirements, Ries and Trout's laws are indeed a set of alternative ideas.

We decided that all of Ries and Trout's laws were applicable to the case study organisation. We then trawled through the two RTPs and three OEPs to determine where and how they referred to these laws. Perhaps unsurprisingly, we found that although none of the laws were mentioned by name the use of most of them were implicit in the RTPs and OEPs. There were some exceptions, which we generally dealt with by adding a few words to an OEP, as this fitted in better with the organisation's approach to sales and marketing.

What we did find surprising was the distribution: 16 laws referred to OEPs, whereas only 6 referred to controls. Had there been no OEPs, we would have had difficulty in justifying these 16 laws. Our conclusion is that most of these laws concern "doing the job", i.e. Part 1 of an ICS. The others concern "doing the job right", i.e. Part 2 of an ICS.

Analysis of the Sales and Marketing Practice document revealed that, following adjustment to the OEP just referred to, there were no laws which had not been implemented but there were instructions that did not correspond to, or contradicted, Ries and Trout's laws. These instructions corresponded to the requirements of the RTPs and OEPs that did not feature in Ries and Trout's laws, but nevertheless were required, not as a matter of policy but as a result of the directors' analysis of risk treatment and opportunity exploitation.

Further Exploitation

The Case Study as described covers Sales and Marketing, Information Security and Quality. However, the Case Study organisation's MS also addresses finance in that credit and market-trading risks are included in the business risk analysis (PLAN phase), and there are corresponding RTPs and financial procedures and controls in place. What is missing, if anything, is the "financial" AIL to go with it. This is currently under construction.

Summary and Conclusions

In this paper we have proposed a structure for the management system component of an ICS. The proposed structure:

- Covers both parts of an ICS, through the use of RTPs and OEPs;
- Captures all the recommendations of the UK Audit Practices Board's model of internal control;
- Conforms to the Common PDCA Framework;
- Adopts a *safety net* concept, using AILs and SOAs.

We have built a MS using this proposed structure and have extended it to cover Sales and Marketing, by the addition of two RTPs, 3 OEPs and a new AIL. This demonstrated the ease of extending a MS that is structured in the proposed manner.

We successfully used a text book for the AIL. This demonstrates that AILs can take many forms and do not necessarily have to be formal international standards. The discovery of "laws" included in the AIL, which were agreed to be applicable but were not referenced in any RTP or OEP, demonstrates the effectiveness of the safety net concept.

The fact that the RTPs and OEPs required a number of operational procedures that were not listed in the AIL reinforces the fact that the AIL is simply a set of alternative ideas that are not exhaustive and may or may not be applicable. ISO/IEC 27001:2005 makes a similar remark, observing that an organisation may require additional controls to those specified in Annex A to ISO/IEC 27001:2005

Many of the ideas in this particular AIL relate to Part 1 of an ICS. Their applicability could not have been justified without the presence of the OEPs.

References

[1] "*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 info@abgpublications.co.uk

[2] "*Internal Control, Guidance for directors on the Combined Code*" (The Turnbull Report), Institute of Chartered Accountants in England and Wales, see http://www.icaew.co.uk/

[3] "*Quality management systems – Requirements*", BS EN ISO 9001:2000

[4] "*Environmental management systems - Specification with guidance for use*", BS EN ISO 14001:1966

[5] "*Information security management systems – Requirements*", BS EN ISO/IEC 27001:2005

[6] "*The Similarity between ISO 9001 and BS 7799-2*", Brewer, D.F.C., Nash, M.J., http://www.gammassl.co.uk/topics/ics/9001Similarities.pdf, October 2005

[7] "*Opportunity Exploitation Plans*", Brewer, D.F.C., List, W., November 2005, www.gammassl.co.uk/topics/ics/OEP.pdf

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

[9] "*The 22 immutable laws of marketing*", Ries, A., and Trout, J., HarperCollins, 1994, ISBN 0 00 638345 9

About the Authors

Dr. David Brewer

Dr. David Brewer 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. He was one of the driving forces behind the international ISMS standards, and has assisted many clients to build ISMSs since 1998 in Europe, East Africa, the Middle East and the Far East.

Dr. Michael Nash

Dr. Michael Nash has a long background in information security. His first involvement came in 1985, working initially within NATO using the US TCSEC "Orange Book", and then setting up and managing the first UK security evaluation facility. He helped develop the UK national criteria, the ITSEC and finally the Common Criteria. On the other side, he has advised many major vendors and user organisations how to implement and improve information security, through the use of BS 7799 and related techniques. He has been involved in international standardisation for more than fifteen years, most recently as the Project Editor for the Guide to the Development of Protection Profiles and Security Targets, ISO/IEC TR 15292.

William List, CA, hon FCBS, CITP

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, and is also part of the international team developing the international ISMS standards. He retired as a partner in KPMG. He is the immediate past chairman of the BCS security expert panel.