



# APPLIED RESEARCH IN INTERNAL CONTROL – A ROAD MAP

For the past three years, Gamma Secure Systems Limited and W<sup>m</sup>List & Co. have engaged in a programme of applied research into internal control. As shown in the road map:

1. Effective internal control is a fundamental part of corporate governance and is a requirement of the various laws and regulations.
2. The UK Audit Practices Board has proposed a model of an internal control system.
3. Our research shows:
  - a. Internal control requires a management system to establish, operate, maintain and improve the internal control system.
  - b. There are two parts to internal control. The first, which concerns the processes for “doing the work”, can be described in terms of exploiting opportunities to create benefits. The second, which concerns the controls for ensuring the “the work is done properly”, can be described in terms of addressing events to mitigate adverse impacts.
  - c. There is benefit on using an “Alternative Ideas List” (AIL) to assist organisations select the most appropriate controls to meet their particular needs.
4. There are various international standards (e.g. ISO 9000, ISO 14000, ISO/IEC 27001) that specify the requirements of such a management system. All are conformant to ISO Guide 72. ISO/IEC 27001 is the best fit to the UK Audit Practices Board model.
5. ISO/IEC 27001 uses an AIL derived from ISO/IEC 17799 for information security management. Other AILs can be used to cover other aspects of internal control, e.g. financial recording and presentation, sales, marketing, and quality.

The road map identifies a variety of Gamma/W<sup>m</sup>List publications and shows their inter relationships. The principal paper, “*Measuring the effectiveness of an internal control system*” (<http://www.gammasl.co.uk/topics/time/time040317.pdf>) (also referred to as the “time paper”) is that an effective system of control is one that can detect the event in sufficient time for something sensible to be done about it before the impact occurs. It explains the time metrics and how they are used to measure the operational and cost effectiveness of controls. It also describes the methodology for creating “tell it like a story” RTPs (risk treatment plans), and this addresses the second part of internal control. Our paper “Opportunity Exploitation Plans” (<http://www.gammasl.co.uk/topics/ics/OEP.pdf>) explains how to create OEPs (opportunity exploitation plans) and thus addresses the first part of internal control. Our paper “Exploiting an Integrated Management System” (<http://www.gammasl.co.uk/topics/ics/MSExploitation.pdf>) explains the AIL concept and brings all three concepts (AILs, OEPs and RTPs) together to construct an integrated management system addressing the whole of internal control.

There is a variety of supporting papers and presentations on the Gamma web site, including “*Fast track ISMS certification*” (<http://www.gammasl.co.uk/topics/ics/FTISMS.pdf>) presents a methodology for implementing management systems; and “*Applying ICS time metrics to GlobalPlatform smart cards*” (<http://www.gammasl.co.uk/topics/eSmart2004P.pdf>) and “*The relevance of the Common Criteria to Sarbanes-Oxley and corporate governance*” (<http://www.gammasl.co.uk/cc/iccc5DBPaper.pdf>) apply the time metrics and RTP concepts in specific contexts.

Gamma’s own internal control system implements all the concepts described in these publications and is certified to both ISO 9001:2000 and ISO/IEC 27001.



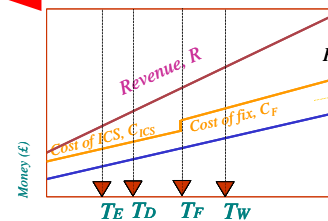
**Laws and regulations concerning Corporate Governance**

Includes Turnbull, Sarbanes-Oxley, the proposed EC Directive, Basel 2 ...

*"An effective system of control is one that can detect the event in sufficient time for something sensible to be done about it before the impact occurs"*

**Time metrics**

The time metrics help to establish the operational and cost-effectiveness of the internal controls. This is fundamental to the successful realisation of the various corporate governance laws and regulations



**Gamma's internal control system uses all of the concepts embodied in this roadmap and is certified to ISO 9001 and ISO/IEC 27001**

See [www.gammasl.co.uk/topics/ics/gamma.html](http://www.gammasl.co.uk/topics/ics/gamma.html)

Requires organisations to have a sound system of



The UK Audit Practices Board Model of internal control

**Internal Control**

Requires a management system (MS) to establish, operate, maintain and improve the internal control system

**Management System**

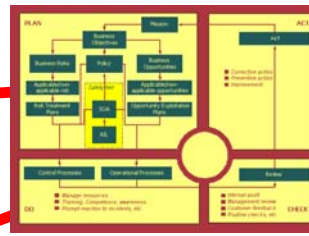
Alternative Ideas Lists exist to assist organisations to select appropriate controls and comply with a variety of laws, regulations, standards and best practice.

**Alternative Ideas Lists (AILs)**

**ISO/IEC 17799**

**ISO/IEC 27001**

ISO/IEC 27001 combines with the UK Practices Board model, AILs, OEPs and RTPs to create an overall architecture for an integrated management system



is an example

**Exploiting an Integrated Management System**

*This paper introduces the AIL concepts and brings it together with OEPs and RTPs to create an overall architecture for an integrated management system*

**Opportunity Exploitation Plans (OEPs)**

**OPPORTUNITIES CONCERNING MARKET PRESENCE**

200 have a range of products, some established (of which some will have just been approved) 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.

The events that are taken advantage of are: 1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

The benefits are:

- Possible favourable customer relationships, as well as A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z.
- Possible additional revenue.

The principal facilities:

The dangers are (from Market Risk): 1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

Opportunity A.I.L. is as fast and as wide as possible. It is a list of all the products of our customers which we are the first to see and that the category is not already covered by a product which is particularly useful about what we sell our products, and where they are in the market.

**Measuring the effectiveness of an internal control system**

*This paper describes, in the context of corporate governance and internal control, the time metrics, the Gamma-List RTP approach together with examples of their application*

**FAST TRACK ISMS CERTIFICATION**

*This paper describes a methodology, and the results of its application, for obtaining ISMS certification from a standing start in 4-6 months. Work that only needs to be done once is done only once, to the benefit of every participating organisation*



There are a number of internationally recognised management system standards (e.g. ISO 9001) All are conformant to ISO Guide 72. The "best fit" to the UK Audit Practice Board model is ISO/IEC 27001