The Relevance of the Common Criteria to Sarbanes-Oxley and Corporate Governance

Dr. David Brewer, Gamma Secure Systems Limited & William List, CA, Hon FBCS, CIPT, W^{m}List & Co.

For many chief executives, concerned with meeting their organisation's business objectives whilst complying with new legislation such as Sarbanes-Oxley, the utility of the Common Criteria must seem an irrelevance. Yet there is an important link.

Laws and regulations concerning corporate governance dictate that a system of internal control is an essential element in the structure. Information security is a subset of that internal control system. Well formed controls provide assurance that the majority of events will be detected in sufficient time to counter any adverse impact on the organisation, whilst others assist recovery when disaster strikes.

Most controls concern information in one form or another and, in this modern age, many of these involve IT. This paper argues the case for the Common Criteria and concludes that for some IT based controls, Common Criteria evaluation is an imperative. It also identifies those areas where action can be taken to strengthen the link between the Common Criteria and corporate governance.

OVERVIEW

We begin with an overture summarising the purpose of corporate governance, the principles of internal control, the extensiveness of business risk and how information security fits. We then examine the effectiveness of an internal control system (ICS) and draw some conclusions about well-formed controls. In examining the Common Criteria (CC), using recent work on the GlobalPlatform smart cards and previous work in attempting to produce a Protection Profile (PP) for a typical financial accounting package, we draw our conclusions regarding the ability of the CC to deal with well formed controls. This allows us to summarise our conclusions regarding the relationship between corporate governance and the CC, and state our recommendations towards taking maximum advantage of that relationship now and how to strengthen it in the future.

OVERTURE

Corporate governance

Laws and regulations concerning the governance of large organisations (e.g. [1], [2], [3]) have existed ever since the 19th century. These cover disclosure of information, anti-discrimination, privacy protection, product quality, directors' conduct and suchlike. Many have been produced to fulfil a perceived need to protect the public in general and minorities in particular, and some have been imposed in reaction to specific failures of the public interest, such as Polly Peck, Maxwell Pensions, Enron, and WorldCom.

Many laws and regulations specify the imperative for an organisation to achieve its business objectives whilst looking after its stakeholders. Part of the requirement is the need for organisations to have an internal control system (ICS), which is the means by which an organisation achieves its business objectives and manages its business risks.

Internal control

An ICS exists in two basic 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.

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.

The model also shows that the effectiveness of the internal controls must be regularly reviewed and action taken as appropriate. This is a requirement of various corporate governance laws and regulations. It is also a sound management technique, known as the Deming or Plan-Do-Check-Act (PDCA) model, and is 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]).

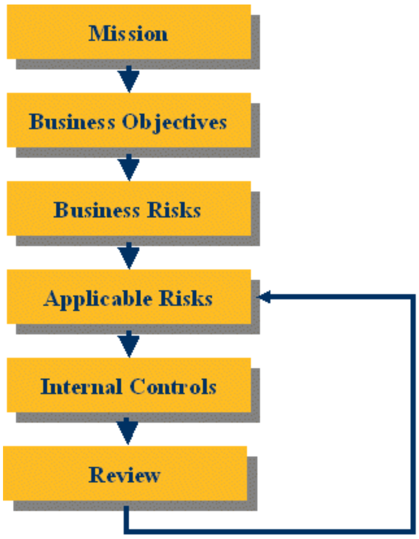


Figure 1: The APB model of internal control

Extensiveness of business risk

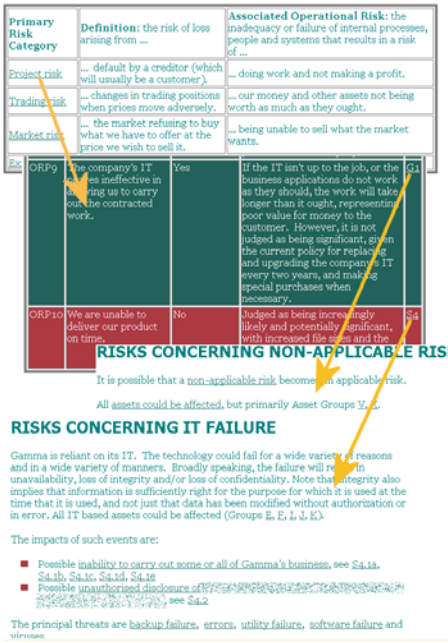
Business risks are all encompassing. For example, they concern an organisation's ability to produce and market its products and services, issue invoices, receive payment and control its exposure to financial market fluctuations. The new Basel accord [9] partitions risk into internal (i.e., internal to the organisation) and external influences.

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. Brewer and Nash pointed that out in 1988 in presenting their paper on Chinese Walls [12] (which concerns the 1986 UK Financial Services Act): "At lunch time go into a London pub and just listen to all the insider dealing going on!" The Institute goes further by saying "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

We reinforce this conclusion in our paper examining the effectiveness of internal control [13], which uses the *same* theory to explain a variety of events concerning the failure of corporate governance, quality control and information security.

Like many organisations, Gamma's ICS [14] has always dealt with these issues. Figure 2 shows how the business risks, documented along the lines of the new Basel accord, are broken down into risk treatment plans [13], which collectively identify all the financial, quality and information security controls. There is a "statement of applicability" (SOA, see [8]) which goes into further detail, identifying how all the applicable information security controls, described in ISO/IEC 17799, are implemented. The management system of this ICS, which follows the UK Audit Practice Board guidance (figure 1), is both ISO 9001 and BS 7799-2 certified.



Primary Risk Category	**Definition:** the risk of loss arising from ...	**Associated Operational Risk:** the inadequacy or failure of internal processes, people and systems that results in a risk of ...
Project risk	... default by a creditor (which will usually be a customer).	... doing work and not making a profit.
Trading risk	... changes in trading positions when prices move adversely.	... our money and other assets not being worth as much as they ought.
Market risk	... the market refusing to buy what we have to offer at the price we wish to sell it.	... being unable to sell what the market wants.
Ex		

ORP9	The company's IT proves ineffective in allowing us to carry out the contracted work.	Yes	If the IT isn't up to the job, or the business applications do not work as they should, the work will take longer than it ought, representing poor value for money to the customer. However, it is not judged as being significant, given the current policy for replacing and upgrading the company's IT every two years, and making special purchases when necessary.	G1
ORP10	We are unable to deliver our product on time.	No	Judged as being increasingly likely and potentially significant, with increased file sizes and the	S4

RISKS CONCERNING NON-APPLICABLE RISKS

It is possible that a non-applicable risk becomes an applicable risk.

All assets could be affected, but primarily Asset Groups V, X.

RISKS CONCERNING IT FAILURE

Gamma is reliant on its IT. The technology could fail for a wide variety of reasons and in a wide variety of manners. Broadly speaking, the failure will result in unavailability, loss of integrity and/or loss of confidentiality. Note that integrity also implies that information is sufficiently right for the purpose for which it is used at the time that it is used, and not just that data has been modified without authorization or in error. All IT based assets could be affected (Groups E, F, I, J, K).

The impacts of such events are:

- Possible inability to carry out some or all of Gamma's business, see S4.1a, S4.1b, S4.1c, S4.1d, S4.1e
- Possible unauthorised disclosure of [redacted], see S4.2

The principal threats are backup failure, errors, utility failure, software failure and viruses

Figure 2: An implementation of the APB model showing how information security is just part of internal control of internal control

EFFECTIVENESS OF INTERNAL CONTROL

Time metrics

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 [13].

Figure 3 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.

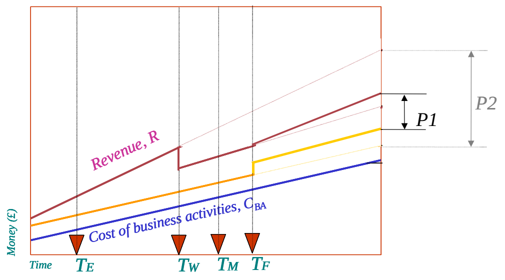


Figure 3: The impact of detecting an effect too late

The event occurs at time *T_E*. On expiry of some "time window" (see [13]) 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 4 illustrates what would happen if the event was detected in good time.

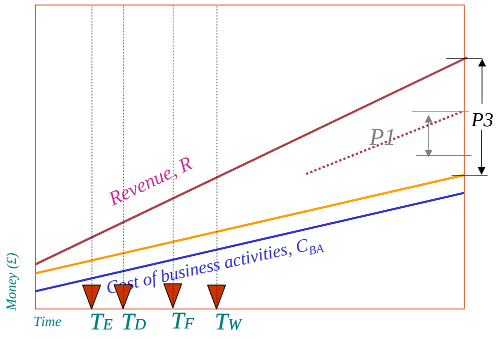


Figure 4: The impact of detecting an event in good time

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 3. 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.

Using these concepts, [13] classifies controls as belonging to seven classes. 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 defensive action within the time window, the third after. 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.

Well-formed controls

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. Suppose, for example, that someone forgets to lock the safe, a thief correctly guesses their victim's PIN or someone "borrowed" the battery from a smoke detector. Given this, there are three alternatives:

- Accept the risk, in other words let us not be concerned if the control fails

- Strengthen the control (and this is where the most important CC concepts of *strength of function* and *hierarchic* functional components come into play)

- Deploy an additional control, whose purpose is to detect the failure of the first.

Detection can result in immediate automatic action. A control that uses the CC security function requirement FAU_ARP.1 (Security alarms) would be a good example. Detection may also defer to a human for action. A control using the CC security function requirement FPT_TST.1 (TSF testing) would be an example. Other components of this control would be the procedures for the human to invoke the FPT_TST.1 function and take action, as appropriate, on its outcome. A bad example would be a control that detects a problem but does not let any other procedure/process or person know. That would be an example of a badly formed control.

Given these observations, a well formed control is one that has been constructed so that any error, or failure perpetrated during execution is capable of prompt detection. Such a control is also termed a self-policing procedure (see [8]). Its value is that it promptly detects a control failure, allowing some other procedure/process to take over. As shown in [13], if this is not done, a control failure may go undetected and ultimately manifest itself following expiry of the time window. A classic case of this is also cited in [13], where organisations having placed reliance in anti-virus measures never check that the virus signature libraries are up-to-date, but just assume that they are.

COMMON CRITERIA

Controls and security function requirements

So far we have been talking about internal controls. In the preceding section we quoted two examples of security function requirements (SFRs) drawn from the 132 defined in the CC. However, it is important to recognise that SFRs are not controls, nor were they intended to be such. SFRs are functions. They are the ingredients out of which the technical aspects of controls may be specified: in our FPT_TST.1 example we said "Other components of this control would be the procedures for the human to invoke the FPT_TST.1 function and take action, as appropriate, on its outcome."

The CC addresses those aspects of a control that are outside the scope of an evaluation as assumptions (see [15]), which are treated as being as axiomatic by an evaluator: it is the responsibility of the organisation that uses the product to ensure that those assumptions are met in practice. Thus, CC evaluation will only look at the IT aspects of a control that are within scope of the evaluation. Evaluation inspires confidence that the control functionality of an IT product will do what it is supposed to do and not do what it is not supposed to do. This is a unique proposition and provides a solid platform with which to build a robust system of internal control. However, is it really necessary?

Failure modes

To answer this question, we must first understand how a control may fail.

The code is wrong or fails to address all circumstances

If we reconsider the two previously mentioned SFRs:

- FAU_ARP.1 may fail either because it does not recognise the security violation or because it does not take the appropriate action when it does.
- FPT_TST.1 may fail if (a) the tests are run under the wrong conditions; (b) the tests give incorrect results; or (c) authorised users are not in practice given the capability to verify the integrity of data or executable code.

In each of these cases, the implementation of the function is incorrect with respect to its specification. In the case of some other functions, which involve a secret (such as a cryptographic key or a password), failure may also be due to weaknesses in the algorithm.

Clearly if these functions had been fully tested or evaluated then the probability of the failure would have been materially reduced.

The assumptions are not implemented correctly or the users fail to operate correctly

This cause of failure concerns the attendant management processes. No matter how correct the IT implementation nor how strong the algorithm, if the secret is disclosed then the function will not have the expected effect. If the access rights of users are incorrectly input into the computer, then the access control decisions will not reflect what management intends. The latter is a specific case of an (undetected) input error. Similar types of failure would be the use of an incorrect computational formula (e.g. the wrong rate curves in "mark to market" calculations used in derivatives trading), or incorrect standing data (e.g. the wrong foreign exchange rates).

The function may fail because of some known error or physical condition.

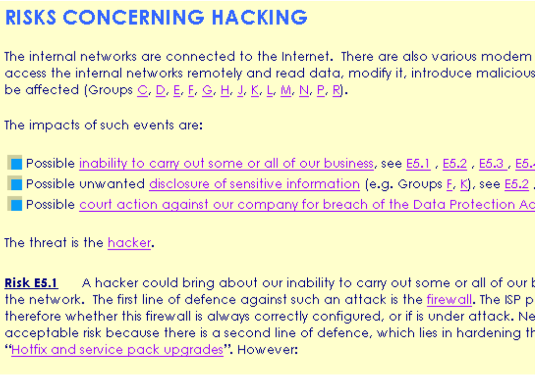
For example, the GlobalPlatform smart cards [16] facilitate the downloading of new applications onto the card. There are various security functions concerned with authorisation, confidentiality and integrity, but all said and done, if there is no room on the card, then the load operation will fail. The function detects this, rolls back to a safe state and reports the malfunction to the entity that requested the operation. The GlobalPlatform Card Security Requirements Specification [17] identifies a wide variety of other failure modes including program exceptions, power failure and adverse operating conditions.

Thus, in general, there is a wide variety of reasons why the IT components of a control may fail.

Detection

In developing a RTP, [13] invites us to consider these failure modes and ask the question "is this an acceptable risk?" If it is, no further action needs to be taken. If not [13] invites us to add further functionality/controls to detect and respond to the failure. In making a sound judgement, attention needs to be paid to the cost of the additional functionality/controls, the frequency of the failures they are intended to counteract, and the time of detection/correction.

Most people are aware of the move by banks to rollout “chip and PIN” for all credit cards. The move is predicated in part by the regulators, in part by the payment associations and in part by the banks themselves, to counter the increasing level of credit card fraud, which is fast becoming an unacceptable risk. Traditional authentication requires the comparison of a signature by the merchant. If the signature is forged and the merchant does not spot it at the time, then we have a control failure, which may well be identified by the bank at some later time, but after the expiry of the time window. By increasing the strength of the authentication mechanism, it is hoped that the frequency of successful authentication attacks will be significantly reduced. Any successful attack should, of course, still be detected by the traditional methods.



RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious 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 , E5.3 , E5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.2 .
- 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 or all of our b the network. The first line of defence against such an attack is the firewall. The ISP p therefore whether this firewall is always correctly configured, or if is under attack. Ne acceptable risk because there is a second line of defence, which lies in hardening th “Hotfix and service pack upgrades”. However:

Figure 5: An extract from an RTP written in accordance with [13]

For a card base of several million cards, if the implementation of “chip and PIN” is incorrect, millions of cards will possess the same error. In the RTP therefore it will be identified that the possibility of failure would be totally unacceptable and possibly irretrievable in administrative effort. Therefore there is a need for additional controls to limit the possibility that the “master card” (from which all other cards are copied) is incorrect. These controls could be subjected to:

- very full testing by the organisation
- contracted out testing by a specialist firm *or*
- a CC evaluation.

CC evaluation is particularly economic if the cost of evaluation is amortised over millions of products and shared by the various organisations involved.

Part of CC evaluation is to find out whether the security mechanisms can be bypassed, corrupted, disabled or otherwise circumvented. After an evaluation there remains the possibility that the evaluated process will fail. It *may* therefore be possible for an attacker to modify the implementation or inhibit how the card works, but the attack (should it prove successful) would be restricted to a small percentage of the card base. It would not effect the entire card base. The organisation should therefore identify other functions/controls would detect that, despite CC evaluation, the function (e.g. “chip and PIN”) has failed, which, based on an assumption of infrequent occurrence of failure, may operate outside of the time window.

In other cases an additional detection capability may be impractical or too expensive. In applying the time metrics to the GlobalPlatform smart card [18], we identified for some functions, e.g. writing a record to an audit log, that it would not be easy to detect after the fact that the record had been written incorrectly. Far better, therefore, to verify the correct implementation of that function prior to its use to a high evaluation assurance level.

RTPs

The development of RTPs is a fundamental requirement of [8], although the British Standard does not (and quite rightly) dictate how it should be done. Our approach [13] (illustrated in figure 5), which is event-impact driven, has found great success in engaging Board members (see [19]). Note, however, that traditional government approaches, which use threat and asset value (e.g. CONFIDENTIAL, SECRET, TOP SECRET, etc.) as input parameters, will also identify the need for CC evaluated products and place requirements on strength of function. Regulations in other sectors, e.g. the German Digital Signature Law, impose similar constraints.

Evaluation requirements

Having decided what is to be CC evaluated from an RTP (ideally from a Board perspective), the question then remains how to ensure that the evaluation delivers the required assurance.

The CC offers two approaches:

- The organisation may express its requirements in a Protection Profile (PP)

- The organisation may consider the claims made in vendors' Security Targets (STs) and corresponding CC certification reports.

Sometimes an organisation will do both.

One of the strengths of the CC is the richness of the Part 2 vocabulary in expressing IT control functionality. It does this particularly well for individual IT components. In terms of the overall preventive, detective and reactive mix of functions, we counted 69 SFRs that are preventive in nature, 38 that are detective and 1 reactive (FPT_RCV.1 (Manual recovery)). The remainder are support functions and cannot be directly associated with a control class.

The CC portal (see [15]) at the time of writing lists 195 evaluated products, which include operating systems, smart cards, firewalls and intrusion detection devices. Some of the smartcards have been evaluated together with financial application software (electronic purse and payment applications). It also lists 38 distinct PPs. Some also address the business applications. For example, [20] specifies the security requirements for an automated cash dispenser and [21] specifies the security requirements for an electronic purse.

We are concerned that in [20] an environmental objective to reconcile the amount of money that the computer believes has been dispensed (which, of course places a requirement on the TOE to calculate it) with the amount of money actually dispensed is not specified. Such a control would address a wide range of failures, such as once recently reported in the UK, where £20 bank notes were inadvertently loaded in to the £10 note dispenser. We also found it difficult to trace the business requirements down to the IT components that are intended to implement them because there is a lack of refinement in the identified SFRs. In contrast, the business requirements stated in [21], which include unauthorised creation or loss of electronic value (i.e., money) and support for countering money laundering, are traceable to the SFRs with the aid of comprehensive cross references and the judicious use of in-line application notes.

In attempting to develop a PP for a typical financial accounting package, as reported at ICCC4 List [22] had discovered that there was no easy way to specify the reporting of errors to the user(s), or of specifying batch processing control requirements.

GlobalPlatform elected not to develop "yet another" smart card PP [16], but instead developed the CSRS [17]. Freedom from the language constraints of the CC enabled GlobalPlatform to express its functional requirements in a very precise and comprehensible manner. Yet, as reported in ICCC2 [23], Kekicheff *et al* were able to achieve much of this within the language constraints of the CC, albeit with a considerable amount of lateral thinking. The use of FDP_ACC and FDP_ACF to express the requirement for byte-code verification is an example. The idea here is that use of a load file (an access control decision) is dependent on whether the application code passes byte-code verification. Traditionally, that decision is based on a simple security parameter. In the GlobalPlatform case a complex algorithm (i.e., byte-code verification) has to be performed before the access control decision can be made. Kekicheff *et al* appreciated that the purpose of the PP/ST is to "point the evaluator in the right direction and ensure that he/she asks the right questions". [23] cites other instances where such innovation is required.

We believe that the major difficulty in capturing the business requirements in the PP/ST is due to the fact that the language used by the CC is far more alien than that traditionally used in IT, and even the latter is far removed from the everyday business language used by business people. It appears that often a great deal of ingenuity is required to translate the RTP (business) requirements into the language of the CC. In short, therefore, there is a language barrier. However, this should not form an impediment to using the CC but it really puts people off.

We note that the rationale in the Visa Open Platform PP (OP3), referred to in [23], and that in the CSRS [17], describe the ability of the SFRs to meet the security objectives in the form of a story, and may therefore be regarded as a prototype RTP in the style of [13].

SUMMARY

Analysis of business risk using [13] will identify where CC evaluation of the IT components of internal controls is an imperative. Execution of CC evaluation then provides assurance in the well-being of those parts of the internal control system that place heavy reliance on IT components. Sound internal control is a prerequisite for corporate governance. The link between corporate governance and the CC is thus established.

As a corollary, consider the case where an organisation thought it did not have enough money to pay all of its staff. It therefore made most of them redundant. The IT director subsequently reported that the financial reports were in error and, in fact, the organisation was cash rich. Sad to say, this is a true story. Clearly, a gross failure of internal control, but had the organisation previously ascertained its dependence on IT, well formed controls perhaps using CC evaluated components would have saved the day!

RECOMMENDATIONS

1. **Organisations should be encouraged to consider information security as an integral part of internal control**. The UK Audit Practice Board guidance [4] shows how this can be done. The work of the IT Governance Institute [10] reinforces this conclusion. The ISO 9001 [6] and BS 7799-2 [8] standards add detail, and [14] describes an example implementation.

2. **Organisations should be further encouraged to identify circumstances in RTPs where substantial confidence in the proper performance of IT parts of the total system is necessary for commercial or technical reasons**. Guidance on how this can be done is given in [13], [19] and in this paper.

3. **Organisations that have already produced PPs should be encouraged to determine exactly how these PPs contribute to their internal control requirements (or those of their members) and to make that clear to their suppliers**. The GlobalPlatform CSRS [17] represents a major step towards this objective, particularly because of its in-depth consideration of off-card (i.e., components outside the scope of evaluation) business-related issues. Further guidance is given in [18].

4. **Vendors, already experienced in CC evaluation, should be encouraged to determine how their products actively contribute to internal control, to reflect that fact in their product offerings, marketing and product improvement**. Use of the event-impact driven RTP approach ([13], [17], [18]) provide a means by which this can be done.

5. **Other vendors should be encouraged to determine the role their products play in internal control, and the likely need for CC evaluation**. If they determine that CC evaluation is an unlikely requirement, what other assurances can they give for correct implementation and what other functions/controls are required in order that their product forms part of a well-formed control.

6. **The CC authorities should take account of the important role that the CC has to play in corporate governance and internal control and take appropriate steps to make it easier to express and evaluate the requirements of internal control**. Formalisation of the RTP approach taken in [13] and [18], and taking account of the difficulties described in this paper and references [22] and [23] may provide a suitable starting point.

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

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

[15] "Common Criteria", ISO/IEC 15408:2000, available from www.commoncriteriaportal.org/public/developer/

[16] "Dealing with smart cards as evaluated systems", Kekicheff, M., *et al*, Proceedings of the Fourth International Common Criteria Conference, Stockholm, Sweden, 2003 (available from www.gammassl.co.uk/topics/smart cards/iccc4.html)

[17] "Card Security Requirements Specification", Version 1.0, May 2003, GlobalPlatform, www.globalplatform.org

[18] "Applying ICS time metrics to GlobalPlatform smart cards", Brewer, D.F.C., List, W., Proceedings of e-Smart 2004, Sophia Antipolis, France, 2004

[19] "Fast track ISMS certification", Brewer, D.F.C., List, W., August 2004, www.gammassl.co.uk/topics/ics/FTISMS.pdf

[20] "Automatic Cash Dispensers/ Teller Machines", PP/9907, registered at the French Certification Body (available from www.commoncriteriaportal.org/public/files/ppfiles/PP9907.pdf)

[21] "Intersector Electronic Purse and Purchase Device (version without Last Purchase Cancellation)", Version 1.3, March 2001, PP/0101, registered at the French Certification Body (available from www.commoncriteriaportal.org/public/files/ppfiles/PP0101.pdf)

[22] "The role of system certification in meeting an organisation's corporate objectives", List, W., Proceedings of the Fourth International Common Criteria Conference, Stockholm, Sweden, 2003

[23] "The Open Platform Protection Profile", Kekicheff, M., *et al*, Proceedings of the Second International Common Criteria Conference, Brighton, UK, 2001(available from http://www.gammassl.co.uk/topics/OP3-ICCC2.html)

About the authors

William List, *CA, hon FBCS, CITP*

Dr. David Brewer

Dr. David Brewer (right) 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.

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 from KPMG. He is the chairman of the BCS security expert panel and a member of the ICAEW IT faculty committee.