7

Security Assurance in Information Systems

Richard G. Wilsher
the Zygma partnership
St. George's House, Bridge Street, Witham, Essex, GB - CM8 1DY
e-mail: rgw_zygma@compuserve.com
Tel: +44/0 (13 76) 52 13 76; Fax: +44/0 (13 76) 50 28 45

Helmut Kurth
Industrieanlagen-Betriebsgesellschaft mbH
Einsteinstraße 20, D - 85521 Ottobrunn
e-mail: 100334,413@compuserve.com or *kurth@iabg.de*
Tel: +49/0 (89) 60 88 31 43; Fax: +49/0 (89) 60 88 34 18

Abstract

This paper presents the results of five key European Union-sponsored projects in the field of information security within the framework of the EC's INFOSEC programme, and on the basis of findings within those projects takes a critical look at evaluation criteria in the context of their rôle in supporting overall service and system security assessment and assurance.

A proposed model for System Accreditation and its developments towards a general solution for assessing complex systems are described. Both desk studies and practical application of the concepts to real problems are considered.

The ITSEC is examined in the light of the defined commercial requirements for system accreditation and against the assurance needs of complex services and systems as exemplified by telecommunications services in particular. These examine, *inter alia*, the scoping of ITSEC, the suitability of its outputs for re-use in other Evaluations or assessment processes (e.g. System Accreditation), and its flexibility for use in a commercial domain.

The authors offer the tenet that whilst Evaluation may be a valuable process for assessing simple products, it is insufficiently flexible for the evaluation of complex subjects/targets and has too restricted a scope for being the basis for any true system or service assessment, for which broader and more flexible processes are required, principally System Accreditation. Evaluation criteria as presently conceived can, at best, support and contribute to these process.

The paper concludes with a short review of some available options for realisation of a practical and commercially acceptable assurance scheme incorporating ITSEC, and of actions which could stimulate progress in this area.

S. K. Katsikas et al. (eds.), *Information Systems Security*

Keywords:
Accreditation; Assessment; Certification; Distributed Systems; Evaluation; Information Systems; INFOSEC; ITSEC; Security Policy;

1 INTRODUCTION

This paper describes investigative work addressing evaluation and information system accreditation within the EC's INFOSEC programme. It in this area, including the application of its findings to practical subjects both within INFOSEC and in the commercial domain.

2 OVERVIEW OF SYSTEM ACCREDITATION

Today, commerce is increasingly dependent upon complex information systems, for which it is becoming increasingly less straightforward to provide confidence that such systems have adequate security. The security assessment of large, complex, distributed systems requires careful analysis of the domains over which they extend, their operational and managerial influences, the relevant contribution of security functions within those domains to their collective security, and the identification of the appropriate means and levels of assessment which should be applied to deliver the overall assurance being sought.

System Accreditation (hereafter referred to as Accreditation) is a process which can achieve this assurance, by undertaking a wide-ranging review of business objectives and risks against evidence of steps taken to specify the business's requirements for security, the ways in which those requirements have been met and the effectiveness of the measures put in place. Where attention needs to be focused on technical components of the total solution, ITSEC can be an important assessment tool. However, the ITSEC is only suited to assessing technical components and Accreditation is the vehicle for putting to use evaluation results within the context of overall system assurance.

3 THEORETICAL STUDIES

3.1 Commercial System Accreditation (INFOSEC S2012)

INFOSEC Project S2012 addressed three specific objectives: a survey of user requirements for commercial accreditation, an analysis of the relationship between Evaluation and Accreditation, and development of a framework for an Accreditation process. S2102 addressed the idea of commercial accreditation, developing a framework Accreditation process.

User Survey - Key Parameters

The User Survey collected over 400 interview reports, revealing that some 90% of interviewees were in favour of Accreditation.

The broad expectations of coverage of such a system were expressed as:

Environment	66%;	Personnel	74%
Procedural	83%;	Physical	83%;
Technical	91%		

System Accreditation Process Model

The Accreditation Model has been developed from user requirements, accounting for the current ITSEC Evaluation scheme, and is the reference for subsequent Accreditation-relevant work addressed by this paper. It has been designed to be flexible and configurable. Since the environment and security needs differ between sectors, organisations and between systems within an organisation, the process may be tailored to the needs of a specific sector, service or system. This provides for selection of the level of assurance at which the Accreditation should be targeted, the model proposing three initial levels, of increasing confidence. The model also describes how Accreditation is correlated with other activities (including Evaluation). A primary objective of the model is to avoid duplication of effort and to maximise re-use of evaluations and assessments.

The model has five distinct phases and for each provides a description of the inputs and outputs required together with a detailed flow of activities. The five phases are:

Accreditation planning: In which the Accreditation is tailored for the specific system. This stage also defines the responsible bodies for each activity along with a time and cost limit for the total process. The required assurance level and the consequential level of detail of the Accreditation have also to be established;

Input collection: Definition of input documents needed for each activity and their minimal requirements for content and presentation. The documents are then collected and checked for completeness.

Technical review: Each document is checked for internal consistency, consistency with the other documents and overall quality. For each document the reviewers will indicate whether it (and the security functions described therein) is accepted without change, accepted subject to minor changes, not accepted due to major changes needed or completely rejected as unfit for purpose.

After successful review of the documents, the Accreditor may decide to perform some additional tests of individual security functions. The Accreditor may simply define these tests and witness their execution by the sponsor or by an independent tester, or they may decide to perform the tests themselves.

Preparation of the Accreditation report: This phase summarises the review results, delivers the Accreditation result (either Full Accreditation, Limited Accreditation or Partial Accreditation), and indicates the achieved assurance level.

Planning for re-Accreditation:. If changes are made to the system, its environment or its purpose, the validity of the Accreditation may change also. This requires a re-Accreditation of the system. The Accreditation report describes limitations and boundaries of the Accreditation and specifies the areas where changes may influence its continuing validity.

ITSEC's Relationship to System Accreditation

The project reviewed two key issues concerning ITSEC and Accreditation: the relationship between the two processes, and what results could emanate from Evaluation as input to Accreditation (at present an evaluation report is virtually a dead-end).

Evaluation and Accreditation differ significantly in scope. An ITSEC Evaluation assesses the validity of claims made about the security features of a product (or system). Accreditation measures whether a particular information system meets the organisation's security objectives. Thus, while an Accreditation could benefit from the availability of ITSEC Evaluation reports it might equally proceed successfully where there is no significant need for evaluated components. Furthermore, an ITSEC Evaluation alone would never be capable of fulfilling the expectations placed upon Accreditation.

The S2012 review identified a number of inconsistencies between ITSEC's approach and the needs of whole system assessment, highlighting the need for clarification on topics such as the purpose of the different ITSEC assurance levels, the precise type of policy intended (corporate, system, technical) when referring generally to 'security policy', and the intention to refer to a collection of IT components under laboratory conditions when it refers to 'system evaluation'.

In particular, it was determined that such clarifications must account for the needs of Accreditation ensuring that the Evaluation process provides results specifically intended for re-use by Accreditors. These results should assist in the Accreditor's effectiveness assessment, addressing such matters as the vulnerability and weaknesses identified during Evaluation, likely threats which could exploit these weaknesses and their consequential impacts, guidance on potential countering measures and safeguards, assumptions made within the Evaluation regarding the environment and non-IT security measures in the operational system, and the effects of changes or reconfigurations to the evaluated product.

3.2 Service Assurance (INFOSEC S2109)

This project considered the need for security assessments in telecommunications services and, significantly, examined the feasibility of performing a security evaluation of an existing trusted third party telecommunications service.

One of the significant business assurances identified was the need to establish through contract some form of responsibility for demonstrating (e.g. through an independent assessment, such as Accreditation) as well as achieving a specified security performance (Quality of Service) level.

Study of the relationships between technical processes such as the S2012 Accreditation Model (which could include in their scope of review the implementation of business assurances) lead to the development of a trust assessment framework which illustrated how Evaluation, Accreditation and other related processes can inter-work in the provision of security assurance (on the basis that a System Evaluation is based upon a laboratory environment).

It is important in analysing large 'Targets of Assessment' that their complexity is managed. The study identified an absence of well-established methods for analysing complex systems, and developed and applied an initial set of criteria suitable as the basis of a strategy for decomposition and recombination, so as to partition the security assurance problem into more easily managed and assessed components.

In extending the S2012 study of ITSEC, S2109 identified a number of conflicts between the underlying assumptions of ITSEC and ITSEM as well as gaps between these documents and the technical characteristics of service supply in the telecommunications sector. Eleven areas in which there is need for clarification, interpretation or extension of either evaluation principles or of their application were identified. The principal points addressed were:

- The assumption that there is a single point of control is inappropriate;
- The telecommunications requirement for different assurance levels within a single target is not supported (although some would argue that this itself is not a workable solution);
- The timescales of telecommunications services evolution and of Evaluation durations are not matched;
- The ITSEC assumption that there is a single development and configuration environment does not hold, specifically in the telecommunications environment, and elsewhere generally;
- The security functions identified by ITSEC are not appropriate to the telecommunications sector;

Recommendations for further work on ITSEC was identified as a result of these findings.

3.3 ITSEC re-use and re-evaluation (INFOSEC S2114)

Task S2114 addressed areas where the ITSEC should be improved to suit commercial needs. These areas are:

- Re-Evaluation and Re-Rating;
- Interface to Accreditation;
- Effectiveness Assessment;
- ITSEC and Criteria for Safety Critical Systems.

The primary motivation for this study was the desire to achieve cost-effective security assessments which were capable of re-use and had the ability to cope with (relatively frequent) change.

The study concluded that the ITSEC needs significant improvements in these areas to be commercially acceptable. Suggestions for the improvement of both ITSEC and ITSEM were developed from the consortium's own experience of assessment of commercial products and systems.

Re-Evaluation was found to be a major problem with ITSEC and ITSEM, since the scheme proposed in those documents was found to incomplete and impracticable.

In the area of interface to Accreditation, the findings of task S2114 are based on the Accreditation Model developed by task S2012 of INFOSEC'92.

Special attention was paid to the use of the effectiveness assessment within an ITSEC evaluation. A new scheme for the effectiveness assessment was also introduced by this task which tries to make the results of this assessment a much more useful input for the accreditation process. The results of this study were intended to either enhance the ITSEC or any future criteria for the security assessment of commercial products or systems.

The study also found that ITSEC had the potential to be a basis for safety assessments, but that it needed extension in terms of specific terminology to cater for safety critical systems, whilst also needing the benefits promised by solutions to other deficiencies such as the interface to Accreditation and development of the effectiveness part.

To date, the recommendations made by this project have not been integrated into ITSEC although they address several of the criticisms of ITSEC from the commercial sector.

4 PRACTICAL STUDIES

In this section we identify application of the previously described study findings in practical contexts within INFOSEC projects.

4.1 Service Assurance (INFOSEC S2109)

General Description

Within S2109 the theoretical results of the assurance framework for a telecommunication service where applied to the CERDIAL service of Transpac, a division of France Telecom. CERDIAL is a prototype service offering the capability for digitally signed messages transferred via the Transpac X.25 network. The service includes the personalisation and issue of smart cards performed on a specific system under control of Transpac, a Certification Centre also operated by Transpac, and software for integration into a user workstation for generation of signatures and requesting certificates from the Certification Centre.

Security Assessment

To gain the assurance necessary for such a security critical service, a "Service Security Target" was developed describing the security aspects and security policy of the overall service as well as the assumed threats in a very general nature. From this document three different targets for a system accreditation where derived:

- the smart card personalisation system;
- the Certification Centre system;
- the user system (i.e. where the service access application is integrated).

In the context of the task, the user system was considered to be beyond the scope of the task (since the software may be integrated into different types of workstations operating in different environments).

For the two other systems an Accreditation Plan was developed which identified for each system several products that should be the target of an ITSEC Evaluation. This lead to the Accreditation plan shown in the schematic, Figure 1.

Figure 1 shows how product-type 'Primary' evaluations are undertaken on key applications and a second tier of 'Composite' Evaluation could take place, taking within its scope the results of previous primary evaluations (some offering economy by being used more than once). The broader areas of assessment where Accreditation would be required are also indicated.

For each of those products a Security Target document was developed and a pre-evaluation was performed which identified: the documents required for an ITSEC evaluation (including identifying those not available); a suitable assurance level (which should correspond to the minimum assurance level for the product as demanded from the accreditation plan); the effort needed to produce the missing documentation as well as to complete the evaluation.

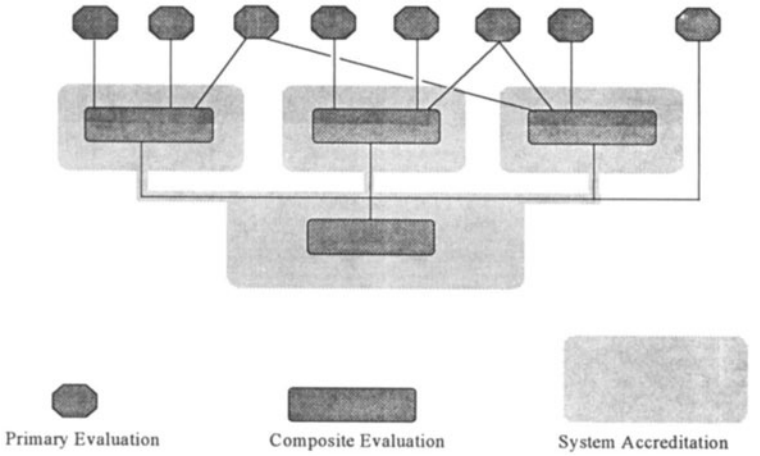

Figure 1 CERDIAL Accreditation Plan.

Conclusion

By analysing a specific target for security assessment, and applying the specific ITSEC requirements against the broader aspects of a System Accreditation, this project was able to illustrate in a pragmatic and implementatble fashion some key relationships between these two forms of assessment.

4.2 EBRIDGE (INFOSEC S2301)

General Description

S2301 was one of the INFOSEC '94 Trusted Third Party Services pilot applications. The main goal of the INFOSEC'94 programme was to build field trial demonstrator systems which showed the applicability of the digital signature technology within a pan-European network.

Within the ebridge project digital signature techniques where added to the prototype of the European Business Register (EBR), which links the official business registers of four European countries (France, United Kingdom, Italy and Denmark). The EBR prototype was developed by task E2001 under the ENS programme. With the extensions implemented by

the ebridge project, users of the EBR service can ask for a signed business register entry from one of those four countries using an on-line service and receive the official information for any company in the four countries officially signed within a few seconds

Within the ebridge project, the signature within the service broker environment is generated by a special system, the Protected Electronic Signature Machine (PESM). The PESM is central to the security of the total service and was developed with very high security protection requirement. Although developed specifically within ebridge, it can be used within other environments where a large number of digital signatures are generated without human intervention (e.g. within a Trusted Third Party which certifies public keys).

Security Assessment

Within the ebridge project a pre-evaluation of the PESM at the level E3 of the ITSEC was performed and an accreditation plan as well as detailed security plan for the total service broker system has been developed.

A detailed risk assessment was performed which identified the risk looking at the system as if it was a commercial service. Based on this risk assessment a security plan was developed, which identified and described the set of countermeasures that would reduce the total risk value to an acceptable level. Some of those countermeasures identified protection functions that need to be implemented in the PESM to protect it from potential misuse and interference. Those measures have been implemented in a prototype way to demonstrate their feasibility.

All the security relevant functions of the PESM have then been assessed in an ITSEC evaluation. Due to the prototype status of the project some remaining vulnerabilities have been identified during the evaluation, which need to be addressed before the PESM can pass an evaluation successfully. All vulnerabilities can be overcome with moderate effort.

The results of the evaluation have then been used in a Pre-Accreditation work. This work assessed the non-IT security measures as far as they have been implemented in the prototype.

Conclusion

The project used the results from the INFOSEC tasks S2012, S2109 and S2114 to perform the security analysis of the total ebridge service. The project demonstrated the feasibility of the security framework established by those INFOSEC tasks and showed how evaluation and accreditation mutually support the assessment of a security critical public service.

4.3 BOLERO (S2302)

General Description

The BOLERO project is another INFOSEC '94 pilot application. It developed an electronic digital-signature-based solution to the issue of negotiable documents. This is based upon a 'Registry' which holds details of ownership of maritime Bills of Lading on behalf of the parties involved (shippers, carriers, banks, etc.). Bills of Lading are generated, transacted and surrendered via a Registry, using authenticated instructions based upon public-key digital signature mechanisms.

Security Assessment

Security assessment of BOLERO drew on the experience of S2012 for the general Accreditation Process Model and S2109 for the decomposition criteria and experience gained in re-combining decomposed complex systems. BOLERO developed an extended two phase model of the Assessment process. It dealt with the following activities:
Assessment Planning;

- Scoping the Assessment;
  - Identifying major Domains;
  - Identifying Components (iterative);
  - Selecting Assessment Methods and Criteria;
  - Preparing Assessment Plan;
- Assessment Conduct;
  - Conducting Low-level Assessments;
  - Conducting High-level Assessments;
  - Preparing Overall Service Assurance .

The first phase, based on work undertaken in S2109, addressed the specific BOLERO circumstances. These assessments do not cover the entirety of the BOLERO project, but represent a selection made on the basis of:

- a risk assessment undertaken earlier in the project;
- requirements to assess the functioning of TTPs;
- a desire to explore further the issues concerning the provision of assurance in multi-provider services.

Development of the Assessment Plan involved determining the differing domains which existed, and how the designated methods of assessment should be undertaken re-used and combined to lead to the provision of an overall Service Assurance. This is illustrated in Figure 2, following.
The BOLERO objective was to conduct pre-assessments, checking the suitability of the necessary inputs without undertaking all tests and producing formal reports (such as certificators would require for the purposes of issuing certificates). The approach taken illustrates clearly the need for re-use of evaluation results, i.e. the need to employ the Crypto Toolbox and Crypto Kernel evaluation results each in two places, and the subsequent incorporation of Evaluation results into Accreditations. Selection of Evaluation level E3 for cryptographic components is a deliberate attempt to focus attention on key potential vulnerabilities.

There is also need to deliver an overall assurance as to the compatibility of all the key service elements, effectively an overall Service Accreditation. Within the project the Management Team assumed the rôle of the overall service broker, but clearly, in a commercial service, there is a need for the broker to sponsor this final assurance so as to be able to provide to users an assured single source of supply. Each Accreditations should concentrate on the effectiveness of the collective measures when working in co-operation with one another.

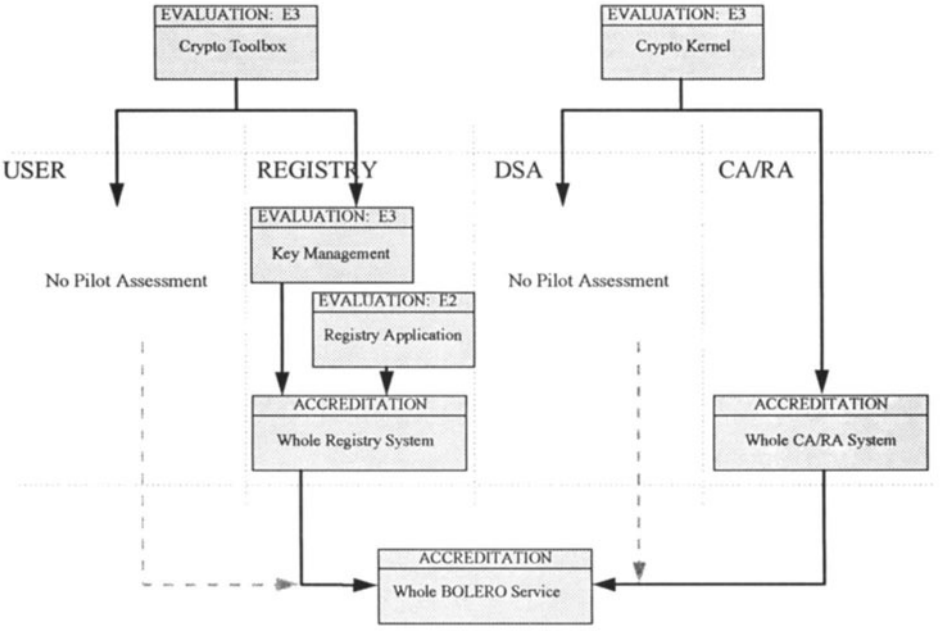

Figure 2 BOLERO Assessment Plan.

Conclusion

The BOLERO project has shown how Evaluation can support the provision of assurance but also that a more flexible scheme is required to encompass all aspects of the system and cope with multiple ownership and re-use of results to achieve economical assessments.

5 APPLICATION IN THE 'REAL WORLD'

The authors have knowledge of a limited number of commercial applications of Accreditation. They occupy a number of distinct sectors and are from a range of countries; however, they share a number of common traits. Each has been undertaken effectively in isolation (and generally without awareness of the others), and hence without sharing of information between them. Each has illustrated the point that there is a need to have a flexible scheme able to be tailored for each specific accreditation. Each case has had the criteria for its accreditation developed in this manner, and the level of detail or rigour used for the accreditation has varied considerably. Rather than demonstrating indiscipline or lack of control, this diversity demonstrates one of the fundamental principles of the S2012

Accreditation model - that of taking a risk-based approach, setting the requirements for evidence accordingly.

Thus, one interpretation of the Accreditation model has consisted of a set of procedural steps and approvals, verifying at key stages during system development the quality of development, conformity to standards, and coherence between system specification and the developed system. This accreditation was intended for internal assurance only.

Another accreditation activity has taken a stronger approach, addressing confidentiality requirements which, for the commercial world, were particularly high. This accreditation was required to produce a publicly available assurance statement for the service in question and identified the need to establish criteria which were based on the ITSEC, but which employed 'reinforced' criteria for the review of effectiveness of confidentiality measures. Additionally, coverage of all aspects of the system's operation was included (i.e. procedures, physical environment, etc.).

This variation of depth of assessment is itself an indication of a range of assurance levels being required, although in the absence of any linkage between these Accreditations, it cannot be regarded as a related set of measures.

6 OVERALL CONCLUSIONS

The foregoing has identified a viable approach to System Accreditation which has broad commercial support but no sufficiently-developed basis for it to be applied with any reasonable consistency. From the work undertaken within these projects, the following conclusions can justifiably be drawn:

Several tasks within the INFOSEC programme have contributed towards establishing and finding application for a framework that can be used in an efficient way to assess the security assurance of complex systems and (even more complex) telecommunication services. ITSEC-style evaluations play an important role within this framework, but are far from being sufficient to provide the assurance necessary for systems or services. Indeed, without a place within an assurance framework, the utility of ITSEC Evaluations is limited to products, and perhaps governmental systems where cost is not a prime consideration.

ITSEC and ITSEM themselves don't provide the interfaces to other security assurance activities that are necessary and already established in the commercial world for the assessment of the security of complex IT-applications and systems. This is one of the main reasons why ITSEC evaluations are currently not very well accepted in the commercial world. Since the ITSEC was not developed as a part of such a wider framework, there are several deficiencies with both the criteria and the evaluation scheme when one considers how to use the evaluation results as input to the assessment of the security of systems or services. But even when the results are useful in a wider context, the way in which these results are obtained is often too expensive and pays no attention to the dynamics within commercial systems and services. This indicates the need for a more flexible, and in some ways pragmatic, approach to undertaking evaluations. Such flexibility should be able to cope with system evolution and change, and with differences in operational environments (e.g. where a service involving a number of providers of aspects of the service has been accredited it is unreasonable to expect to re-evaluate and re-assess all aspects of the provision of the service).

The assurance assessment framework produced by several INFOSEC tasks has been applied not only to INFOSEC projects like €bridge and BOLERO, but also for the assessment of

systems in different commercial sectors. The results show that the framework is useful and applicable but of course needs some enhancements and modifications. Focusing too much on evaluations as the methods for gaining assurance has been shown to be too narrow an approach to a very complex problem.

The limited experience gained confirms the need for a framework which can tailor the process to the practical and commercial needs. Such a framework should take into account best applicable practices from the audit and accounting professions, whilst recognising that such methods are frequently less enquiring than the proposed accreditation model.

Generally, Accreditation is recognised as being a 'good thing' but commerce lacks sufficient examples to adopt as rôle models. A more coherent framework could foster the development of a consistent approach which would in turn encourage wider recognition and greater uptake of such a standard, whether *de facto* or *de jure*.

The INFOSEC tasks mentioned in this paper have addressed aspects of these problems and tried to provide solutions. So far, most of these results are neglected by the EC and national certification bodies in Europe and no initiative has been taken to modify ITSEC and ITSEM in a way which makes them more useful for commercial systems and services.

7 FUTURE OPPORTUNITIES AND DEVELOPMENTS

The authors believe that there is a strong argument for a coherent approach taking the results of the work described, and other, related, valuable efforts, and develop these into a more substantial and validated set of System Accreditation Guidelines. It possible that those sectors providing a range of services to the public and commercial sectors at large may jointly undertake an initiative to establish standards, but this will be on a sectoral basis (e.g. telecommunications, manufacturing, banking, etc.) and these may not ultimately share a generally common, or necessarily compatible, approach.

Some form of initiative is required to co-ordinate the consolidation of this work, to take advantage of appropriate practices from existing professional approaches, to involve real users and to validate the models against real-world applications. Solutions should move towards resolving the dichotomy of a commercial need to have flexible responses which are cost effective and national bodies administering certification schemes heavily focused on ITSEC with little appreciation of what the commercial users want and are prepared to pay for.

Emphasis should be placed on self-assessment, allowing for greater cost-effectiveness for the end user. A key requirement in this regard would be a willingness on the part of accreditors to accept such practices. The adoption of self-assessment would be beneficial in allowing more in-depth analysis (against defined criteria and methods), whilst applying the specific skills of the accreditors to ensure the work was undertaken in the required fashion.

Action by national bodies and/or the EC could enable the erosion of barriers to adoption of some of these more enlightened views and help to develop viable, commercially acceptable, longer-term solutions. Indeed, some national schemes in this direction do already exist.
However, the EC itself could take a more committed attitude towards its own programmes and be prepared to support (and indeed, where justified, openly reject) the findings of work it sponsors by pro-actively following-up recommendations offered to it. The authors believe that valuable support could be provided by adopting the following recommendations.

8 RECOMMENDATIONS

The authors recommend that focus be put upon research and development activities for security assurance in areas able to produce guidelines and criteria for cost-efficient and effective assessments. They believe this should be in a number of key areas:

- Development of the ideas promoted in this paper into more substantial guidelines and criteria;
- Significant commercial enterprise involvement in establishing needs and expectations;
- Revision of ITSEC/ITSEM to fit better into an overall security assessment framework, accounting for recommendations made within the cited projects as well as wider contributions;
- Pilot validation of such measures so as to gain early practical experience and establish confidence in the methods..

The EC could support these developments as they did for the development of ITSEC and ITSEM, and also promote the use of the results in a similar way, perhaps drawing them into any new INFOSEC programme. Additionally, there could be much-improved integration between EC programmes, particularly in the security domain to make the security activities more relevant to the needs of other programmes and conversely using them to provide feedback on the suitability and potential development of ITSEC/ITSEM and System Accreditation models.

Specifically, the EC could support the development of a European Accreditation Model with specified criteria for assessment purposes, the goal being endorsement as a reference model for practical Information System Assurance across the EU Member States.

9 REFERENCES

The following documents are the principal references for the projects concerned and will themselves give reference to other specific deliverables offering greater detail than can be accommodated in this brief paper.

E2307, (1995) EC ENS PROJECT "LEGAL and SECURITY ISSUES in TRANS-BORDER TELEMATIC APPLICATIONS".

ITSEC, (1991) INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA, VERSION 1.2, Provisional Harmonised Criteria.

ITSEM, (1993) INFORMATION TECHNOLOGY SECURITY EVALUATION MANUAL, VERSION 1.0, Provisional Harmonised Methodology.

S2012, (1993) EC INFOSEC PROJECT "ITSEC - COMMERCIAL ACCREDITATION of IT SYSTEMS": FINAL REPORT.

S2109, (1994) EC INFOSEC PROJECT "SECURITY EVALUATIONS and COMMUNICATIONS SYSTEMS" : FINAL REPORT.

S2114, (1994) EC INFOSEC PROJECT "EAGLE - RE-USE and RE-EVALUATIONS": FINAL REPORT.

S2301, (1995) EC INFOSEC PROJECT "ebridge": FINAL REPORT

S2302, (1995) EC INFOSEC PROJECT 'BOLERO': "IDENTIFICATION OF TARGETS OF ASSESSMENT".

8 BIOGRAPHIES

KURTH, Helmut

After his graduate in mathematics, Helmut Kurth worked for several years at the Univerity of Bonn doing research in applied mathematics and computer science. In 1984 he joined IABG, a german technical consultancy company. His main area of work since that time is IT security.

Work in this area included the analysis of complex systems for security vulnerabilities, the design and implementation of IT systems and components needing high security as well as the development of evaluation criteria and accreditation methods. He has also worked in a number of tasks within the EC's INFOSEC programme.

Helmut Kurth gave presentation on many international conferences for IT security including the National Computer Security Conference, the IEEE Symposium on Security and Privacy, The European Symposium on Research in Computer Security (ESORICS) and EUROSEC.

WILSHER, Richard G.

After graduating with an Honours degree in Computer Science in 1977, Richard Wilsher started his career developing real-time software systems,. In 1988 he joined the Secure Systems Division of Nortel, managing software and systems development departments before becoming a technical consultant. Whilst with Nortel he created a pan-European consortium to undertake a number of tasks within the EC's INFOSEC programme.

In 1993 he established his own information systems security consultancy, the Zygma partnership. Through this he undertakes system security assessments and accreditations for clients in the commercial sector, whilst continuing to participate in a number of EC programmes.

He has acted as rapporteur at international workshops, and has previously presented papers at the 1995 ENS Conference and at Eurosec '95.