SECURITY EVALUATION FOR IT PRODUCTS

A vendors' guide to ITSEC

Contents

Securing the future

here might be easier tasks than selling software, but buying software is not one of them. In the fiercely competitive computer industry, users welcome measures that help them differentiate between products on grounds of quality.

One area of differentiation is security. Purchasers have an increasing concern with issues of security. If software developers want their products to reach the shortlist and win selection, they will have to offer specific proof that their products are up to standard, even if security is not a major function.

This booklet has been prepared for the guidance of software and hardware developers and other vendors involved in selling IT products. It is aimed at managers responsible for the development and marketing of products.

It explains the role of ITSEC - Information Technology Security Evaluation and Certification - and how it can help bring products to market with the advantage of a recognised international standard.

The emergence of standards is one of the signs of a maturing industry. Everyone agrees they are important. In the area of security the ITSEC Scheme has already prepared the ground - by defining an international standard, documenting it, and setting up support mechanisms for testing products.

The process of ITSEC certification is designed to add value to the development process; it is not a mere administrative overhead or bureaucratic rubber-stamp. As this guide will explain, the process focuses developers' attention on the quality of security afforded by a product, and will be of assistance even if a developer is not seeking a full evaluation.

It is now up to software developers to take advantage of the process. In the life of every successful product there is a window of opportunity. For any IT product, the ITSEC Scheme is a chance to win a stamp of approval that will hold real value for prospective purchasers.

Why ITSEC is needed

Computer security is now high on the list of priorities for IT users and vendors. The increasing accessibility of personal computers creates potentially easier access to computer-held data. This places organisations at risk and can, in extreme cases, threaten the survival of the business. There are many factors involved:

- *PC applications are often linked to mainframe computers, offering easy remote access to corporate resources, using a low-cost modem.*
- *The spread of open and client-server systems has posed a new problem. 'Standard' software packages are chosen for their familiarity and widespread popularity, but this could be an open door to a knowledgable unauthorised user.*
- *National boundaries disappear in electronic mail systems, workgroups, and remote systems.*

These and other factors point to the need for increased security. But security has to be implemented and, increasingly, organisations are looking for simple yet effective means of ensuring that their systems are secure.

Any security conscious organisation will have procedures, staff training and a culture of security at levels appropriate to the business. But how do they ensure
that the actual products and systems that they use have security built into them?

The answer is to make sure that any IT product, such as an applications package or systems software, offers safeguards, so that it can easily be absorbed into secure operations. This is particularly important in buying 'off-the-shelf' software packages. Vendors need to be aware of the need for built-in security to agreed standards, and prove that their products can provide this.

Yet assessing the security level is not easy without a technical yardstick. Part of the UK Government's responsibility is to establish such standards and measures, and the evaluation and certification scheme has grown from this recognition.

The UK Scheme is managed and administered by a Certification Body jointly operated by the Department of Trade and Industry (DTI) and the Communications-Electronics Security Group (CESG). The Scheme is designed to provide an umbrella for determining standards and procedures for the evaluation of security.

ITSEC certification of a software product means that users can rely on an assured level of security, for any product they are about to purchase. It is a sign of confidence - like the quality kite-mark seen on consumer products.

An international standard

Given the global nature of the software industry, the standard has to be internationally acceptable. To achieve this, it was essential to establish liaisons with other national organisations sharing the same concerns.

In the last decade a number of individual countries have developed their own security standards. One concern was to avoid artificial trade barriers by making sure that products could be evaluated to a common set of criteria in each country. Accordingly, four countries, France, Germany, the Netherlands and the UK, co-operated in establishing common criteria under the ITSEC title. The harmonised approach to evaluation is documented in ITSEM, the Information Technology Security Evaluation Manual. Both are recognised and published by the Commission of European Communities.

For many companies compliance with US standards security standards is also essential. To support this, ITSEC also predefines functionality classes that can provide compatibility with the US Department of Defense's Orange Book.

A commercial decision

There is a clear commercial focus in the ITSEC Scheme. Certification should be assessed in terms of the commercial benefit it brings to the company seeking certification - either users seeking to assure the computer-based systems on which they increasingly depend, or vendors seeking to gain access to new or broader markets by offering more secure products. Equally, vendors should consider the extensive markets that might be closed to them if they do not have certification, especially as some procurement agencies now consider it mandatory.

The potential user of the UK ITSEC Scheme also needs to assess the benefits of certification against the costs. Measuring against an established standard inevitably costs money, because it depends on professional independent assessment. It also calls for an investment of time and resources from the company seeking certification.

Starting the process

In the UK, ITSEC evaluations are carried out by accredited organisations, known as CLEFs: Commercial Licensed Evaluation Facilities. Their job is to carry out an analysis of design, implementation, development, production and distribution, against agreed security standards. This is done as a commercial service, using guidelines and metho-dologies which are recognised internationally as being both objective and repeatable.

CLEFs have been selected after a rigorous process designed to ensure that they have the skills and experience to carry out evaluations. All of the CLEFs are well-established companies who have provided computer hardware and software services over many years. In each case, their experience covers both the public and private sectors, with particular experience in the practical issues associated with implementing sophisticated secure systems and networks. They are also all members of the Computing Services Association and are bound by the Association's Code of Practice.

Companies - both vendors and suppliers - can currently select from four CLEFs, details of which are given at the end of this guide. CLEFs will bid for evaluation work on a commercial basis, and the resulting contract is between the vendor/supplier and the chosen CLEF.

Types of products already evaluated

The standards created under the ITSEC Scheme are designed to apply to both products and systems. Products include software and hardware components, such as applications packages and communications equipment. Systems are defined as specific IT installations, which operate in a known environment for a specific purpose.

CLEFs have already evaluated a variety of products including:

- *operating systems*
- *access control devices*
- *databases*
- *multiple domain facilities*
- *communication and encryption devices*

A complete list of evaluated products is available from the UK Certification Body.

The benefits of evaluation

For users ...

rom the view of a prospective user, there are several benefits in purchasing a product whose security has been evaluated by one of the CLEFs.

- *Successive waves of technology over the last 15 years have added to the IT inventory, but diminished control. The advent of the personal computer has brought immense power to users, often at the cost of a unified, tightly controlled approach to security. Departmental systems have sprung up, leaving many organisations with a heterogeneous, even fractured IT framework.*

- *In moving to off-the-shelf products (such as word processors and databases for use on PCs), a user can introduce vulnerability alongside availability. Such packages have to be integrated with existing systems, some of which might be bespoke and sensitive. So, choosing a product that is certified brings a degree of confidence and diminishes some of the threats posed by unauthorised use of IT assets, such as fraud and unauthorised access to data.*

- *There are also commercial benefits in using a certified product. It is likely to be well-established, and internationally available. Business partners between whom there is exchange of information are likely to trust software which is certified.*

- *When developing specific applications in-house, it is now common to use standard building blocks integrating packaged applications, sometimes with fourth generation languages. The need for confidence in the security of such building blocks is likely to sway the choice in favour of products which have been certified.*

- *An important by-product of certified building block architectures is the introduction of technical standards in-house. The process of analysing what levels of security are appropriate to which applications is itself a revealing exercise, out of which a new discipline emerges. Having technical yardsticks makes well-ordered security much easier to implement.*

...for vendors

The benefits of assessment are far-reaching for those involved in the development and marketing of hardware and software products.

- *One benefit of ITSEC certification is its international standing. This makes products attractive in specific national markets where regulations in security will be increasingly in line with ITSEC requirements.*

- *The benefits of imposing a disciplined approach to security feed back into the development process. The benefits will be available to other products from the same stable, whether certified or not.*

The ITSEC criteria have been developed with the interests of developers and vendors in mind. Within the UK ITSEC Scheme, for instance:

- *Levels of assurance are hierarchical so that an appropriate level of security can be selected, according to the needs of the supplier and the expected market area.*

- *Security claims can be precisely stated, for instance through semi-formal notation, and are not therefore tied to operating system functionality. This provides flexibility for product suppliers and allows extra features to be exploited.*

There are other benefits. For instance, 'quality' has always been difficult to quantify in software development. The imposition of outside standards, using defined terms and proven methodologies, produces a measurable improvement in quality. Even the use of an agreed terminology can help, such as ITSEC's definitions of the principles of confidentiality, integrity and availability.

Independent validation is also a cost-effective way of 'auditing' security features because of the experience and facilities available from a CLEF. The process can be swift, and once complete, it is valid internationally.

The process of evaluation

Overview

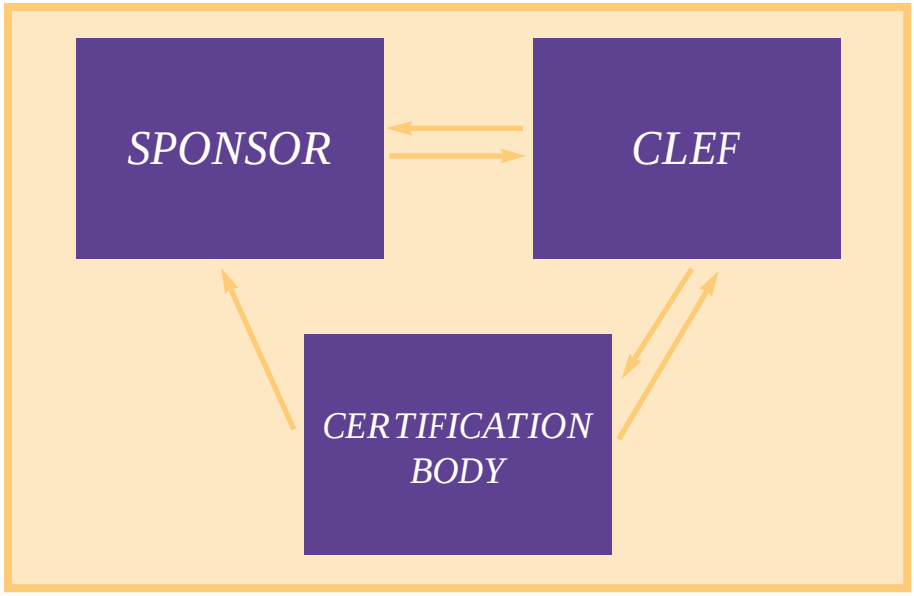
There are usually three participants in the evaluation process for products:

- *the Sponsor (or Developer)*
- *the CLEF*
- *the Certification Body*

The organisation paying for the evaluation is known as the 'Sponsor'. The sponsor is usually the product developer, but also might be the intended user, procurement body, or the developer's agent.

CLEFs carry out the assessment. They are monitored by the UK Certification Body and the National Measurement Accreditation Service (NAMAS).

Evaluation is carried out to an agreed 'assurance level' which defines the degree of confidence required in the product.



Information and feedback flows between the various parties during the evaluation process.

There are a number of distinct steps in the process of evaluation.

1. Decision to Evaluate - is security/evaluation necessary? (The responsibility of the Sponsor)
2. Preparation for evaluation - produce security target and deliverables (Sponsor)
3. Evaluation - measurement against security target (CLEF)
4. Certification review and award (Certification Body)

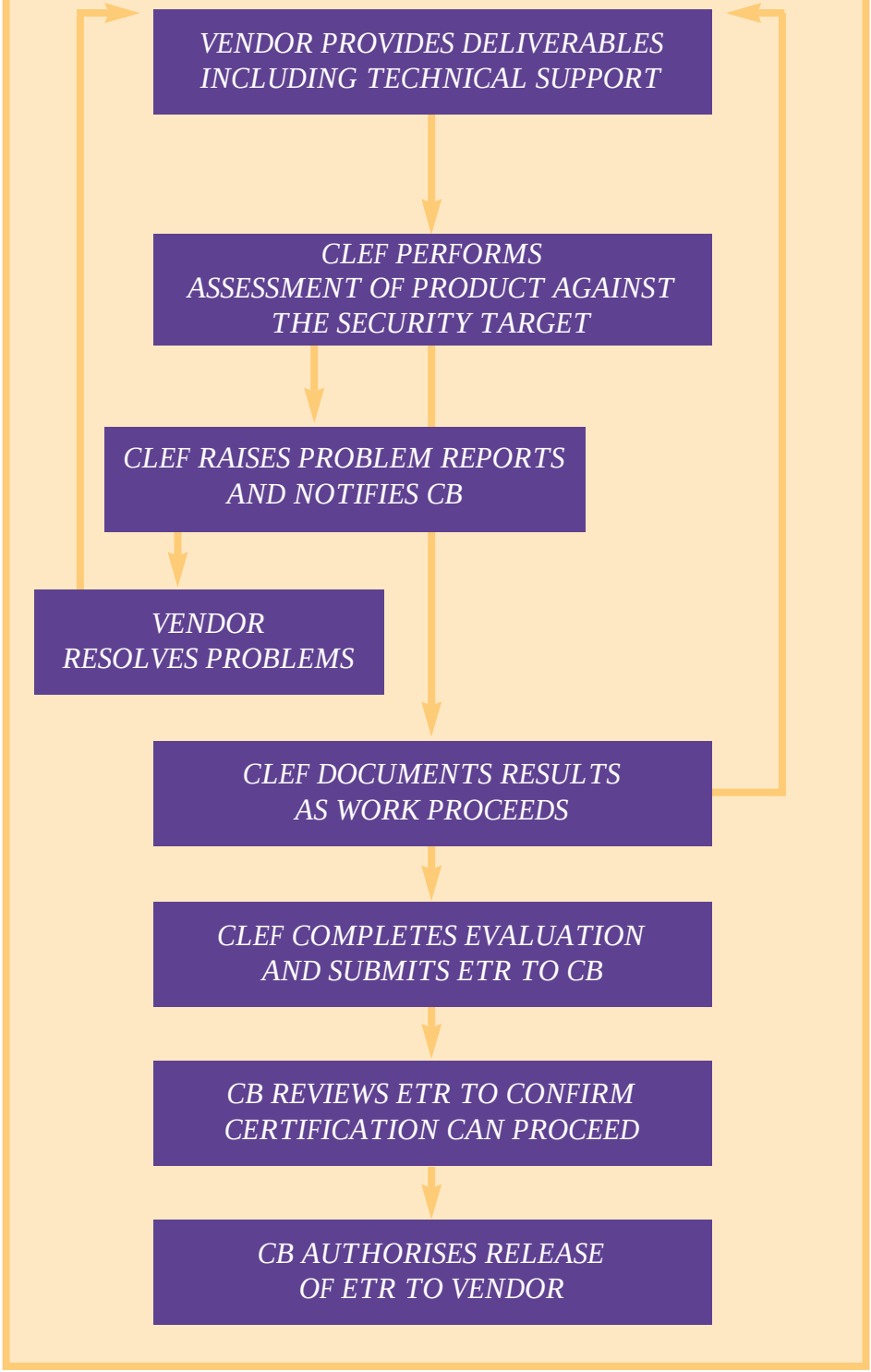
The Sponsor makes the decision to seek certification based upon a business plan or investment appraisal. Then the Sponsor prepares for evaluation. This includes definition of the product for evaluation, specification of the claims to be made for the product and the target assurance level. CLEFs and other specialist security consultants can advise and assist in this process.

The evaluation criteria are publicly available and are used to define the required target level.

The formal evaluation is scheduled to an agreed timetable, and the work itself varies according to the target level and the nature of the product. Material to be examined might include the design documentation, test plans and, for higher levels of certification, source code. The entire process is monitored by the Certification Body who examine the results, and then, if appropriate issue a certificate.

The certification applies only to a specific version of the product. When the product is amended or extended, top-up work may be needed to extend the certification.

THE EVALUATION PROCESS



The evaluation process in detail

step 1

THE DECISION TO EVALUATE

For product vendors the decision to evaluate is based upon a business case and cost/benefit analysis. This may be a broad assessment - market defining, sizing, understanding needs, establishing a pattern of demand for secure products - or an undertaking linked principally to a specific business opportunity. In both cases potential increases in business will underpin the decision.

step 2

PREPARATION FOR EVALUATION

The Security Target specifies the security features of the product and relates to:

- *The security objectives*
- *Possible security threats*
- *The environments in which the product is intended to operate.*

At this stage it is also necessary to specify the required level of security - measured from E1 to E6, with E6 being the highest level of security.

Some products may already be qualified in some way - for instance according to the US Department of Defense 'Orange Book' criteria. This may be taken into account and reduce the time and cost of the operation.

At this point, other operational factors are also taken into account, such as whether the product is to be run on a network. The evaluation only applies to a precise version, and to the specific hardware host to be used. Where products (eg databases) run on several hardware platforms, but are only evaluated on one platform, costs will be reduced for subsequent evaluations on other hosts. In this case all relevant deliverables must be made available to the evaluators.

Many of the deliverables, such as design documentation, are normal products of the development cycle. Sometimes sponsors request independent consultancy from ITSEC specialists regarding the Security Target or to review product documentation prior to evaluation. CLEFs have to remain independent, but may still advise on what information is required, and in what form it is acceptable.

step 3

EVALUATION

Evaluation is a testing process which reflects that of the development itself, verifying that certain requirements have been met.

In order to make the process as effective and trouble-free as possible, the CLEF should work very closely with the sponsor through the various stages of evaluation. This is undertaken as a single, seamless phase, comprising several clearly defined stages, during which the evaluators:

- *Assess the Security Target*
- *Produce an Evaluation Work Programme*
- *Agree a list of documents, material and support to be supplied*
- *Assess system correctness*
- *Test for evidence of security*
- *Assess the development environment*
- *Assess the operational environment*
- *Produce comprehensive evaluation reports.*

The initial stages are essential to ensure the smooth completion of the evaluation. For instance, assessing the Security Target is fundamental because all evaluation is performed against this document. Also, the Evaluation Work Programme identifies the various stages to be carried out and flags potential problems at an early stage.

The evaluators produce detailed reports on each stage of the assessment, always bearing in mind the way the product will be used in real life. For example, the impact of a minor fault in the product might be limited by advice provided in the manuals. If the evaluators discover flaws which could be exploited by an attacker, the Certification Body must be notified.

Other problem reports note aspects of the development that might become significant later, although not actually causing a fault in the system. This might include comments on the develop-ment environment, or instances of unusual coding practices. These do not necessarily preclude certification.

The Certification Body plays an active role in all stages of the evaluation process. It approves the Security Target and the Evaluation Work Programme in advance, and monitors the actual assessment along with the resolution of problem reports.

A key objective of the Certification Body is to check that the evaluation has been conducted in accordance with the appropriate criteria methods and proceedures and that the evidence provided supports the evaluation conclusions.

step 4

CERTIFICATION

The Certification Body reviews all the documentary evidence provided by the evaluators and determines whether the Security Target has been met. If it has, then a certificate is awarded.

Should there be any exploitable flaws in the product, the sponsor and the Certifier can agree on modifications.

step 5

RE-EVALUATION

The Certification Body will advise on whether a re-evaluation is necessary if a product has been modified. The work involved can be minimised during the first evaluation by classifying product components according to their influence on the security features. Thereafter, whenever changes are made to the evaluated product, the Sponsor, CLEF and Certifier can use the classification to determine more easily the impact on certification and what action should be taken.

The role of the CLEFS

There are many ways in which the chosen CLEF can assist the sponsor during the evaluation process, and even before it. The CLEF can help in writing the specifications (both requirement and functional), and in helping with decisions about the operational version to be used for evaluation (host, operating system environment, etc).

The CLEF prepares a proposal based on an initial meeting, usually giving a firm price for the pre-evaluation consultancy, and a budgetary estimate for the evaluation itself.

Pre-evaluation consultancy is optional, but enables the sponsor to draw on the CLEF's experience and resources. CLEFs can advise sponsors on the suitability of the contents and presentation of their products. Such help might cover the issues of development methodology, documentation, and configuration management. Such advice may well save time and effort in the long term.

Another issue is the level of assurance the sponsor can expect from the evaluation. The CLEF advises on this, and also agrees the timescales for the evaluation. The supplier has a period before the formal evaluation during which the Certification Body will be assessing the adequacy of the programme and the Security Target.

The timescales take into account the interactions that might be necessary to complete the evaluation, including consulting the supplier on various aspects of the software and its development.

The CLEF's job is to report to the Certification Body during the evaluation and at its completion. The CLEF sends the final Evaluation Technical Report to the Certification Body. It is subsequently released to the client, with the certificate.

During the evaluation process the CLEF maintains a close level of contact with the sponsor to ensure that all the parties understand the process fully. If any faults are identified during evaluation, the Certifier will agree with the sponsor an appropriate action, such as modification and re-evaluation. Every effort is made to achieve certification to the required level, in partnership with other members of the ITSEC process.

At the end of the evaluation, evidence is securely archived and other material returned to the Sponsor or destroyed.

Where to go for more information about ITSEC:

Head of the Certification Body
UK IT Security Evaluation
and Certification Scheme
PO Box 152, Cheltenham
Gloucester GL52 5UF
Tel 01242 238739

Information about the Scheme is also available from the CLEFs:

Admiral Management Services Ltd (CLEF)
Kings Court, 91-93 High Street
Camberley, Surrey GU15 3RN
Tel 01276 686678
Verner Parke or Tom Craig

EDS Defence Ltd (CLEF)
Wavendon Tower, Wavendon
Milton Keynes, Bucks MK17 8LX
Tel 01908 281177
Colin Foster or John Robinson

Logica UK Ltd (CLEF)
Cobham Park, Downside Road
Cobham, Surrey KT11 3LX
Tel 01932 866748
David Cherrill or Andrea Cumming

Secure Information Systems Ltd (CLEF)
Sentinel House, Harvest Crescent
Ancells Park, Fleet, Hants GU13 8UZ
Tel 01252 778837
Tony Fisher

Data Sciences UK Ltd (CLEF)
Meuden House, Meuden Avenue
Farnborough, Hants GU14 7NB
Tel 01252 513739
Bob Finlay or George Mullen

UK IT*sec*

Issue 2, March 1996

dti
the department for enterprise