LES CRITERES D'EVALUATION

DE LA SECURITE

DES SYSTEMES D'INFORMATION

(ITSEC)

CIGREF

Octobre 1992

SOMMAIRE

1. Préambule

2. Introduction

3. Les besoins en matière de sécurité des systèmes d'information et de communication

4. Présentation des ITSEC

4.1 Généralités
4.2 Fonctionnalités
4.3 Le système d'assurance sécurité

4.3.1 Assurance efficacité
4.3.2 Assurance conformité

4.4 Résultat de l'évaluation

5. Conclusion

6. Glossaire

7. Annexes

7.1 Informations utilisées dans une analyse de vulnérabilité
7.2 Critères de conformité par niveau
7.3 Exemple d'évaluation de la conformité pour le niveau E1
7.4 Enquête AFNOR - CIGREF - CLUSIF sur les besoins d'évaluation

1. Préambule

Cette étude poursuit trois objectifs :

- Information et sensibilisation

Le premier objectif de l'étude est de rendre plus facilement accessible la compréhension des documents ITSEC aux membres du Cigref. De l'avis de tous, les ITSEC sont d'un accès difficile. Si ce n'est la nécessité, l'obligation que les entreprises auront de s'équiper en matériels et logiciels informatiques répondant à des critères de sécurité spécifiés fait que nul - et notamment parmi les grandes entreprises, ne doit aujourd'hui ignorer ce que sont les ITSEC.

- Critique et transfert

La lecture et l'étude que nous avons faites des ITSEC nous ont amenés à formuler certaines réserves et certaines interrogations quant à la réponse qu'ils fournissent aux préoccupations actuelles des grands organismes. Persuadés que nous sommes de l'intérêt de faire entendre notre voix, nous les avons exprimées. Nous souhaitons que chacun puisse réagir à nos propositions.

- Expression des exigences clients

Enfin, le troisième objectif est de communiquer les besoins stratégiques, économiques et techniques des grands utilisateurs dans le domaine de la sécurité des systèmes d'information et de communication.

© CIGREF 1992

2. Introduction

La Communauté Economique Européenne s'est donnée pour mission le développement harmonisé des activités économiques dans l'ensemble de la Communauté. L'importance et l'intégration croissantes des systèmes d'information et de communication dans les activités économiques nécessitent la mise en place d'une stratégie globale visant à assurer une libre circulation de l'information à l'intérieur du marché unique tout en assurant une protection efficace des systèmes d'information dans l'ensemble de la Communauté.

Consciente de l'importance de la fiabilité et de la sécurité des systèmes d'information pour l'achèvement du marché unique, la Commission a proposé un ensemble de mesures concernant la protection des données et la sécurité des systèmes d'information.

Une décision du 31 mars 1992 du Conseil des Communautés Européennes en matière de sécurité des systèmes d'information (COM (90) 314) a concrétisé l'engagement communautaire dans ce domaine.

Les propositions issues de cette décision comprennent le déploiement d'une stratégie globale visant à assurer la sécurité des systèmes d'information et de communication ainsi que la création d'un groupe de hauts fonctionnaires (SOG-IS) chargés de conseiller la Commission sur les actions à mener dans ce domaine.

Le plan d'action communautaire définit six lignes d'action prioritaires :

1. le développement d'un cadre stratégique pour la sécurité des systèmes d'information

2. l'identification des besoins des utilisateurs et des prestataires de services en matière de sécurité des systèmes d'information

3. l'élaboration de solutions pour certains besoins à court et moyen termes des utilisateurs, des fournisseurs et des prestataires de services

© CIGREF 1992

4. l'élaboration de spécifications, normes, évaluations et certifications concernant la sécurité des systèmes d'information

5. le développement technologique et opérationnel en matière de sécurité des systèmes d'information

6. la mise en oeuvre de la sécurité des systèmes d'information

L'une des premières tâches du SOG-IS fut d'élaborer des critères européens d'évaluation de la sécurité des systèmes d'information (ITSEC ou Information Technology Evaluation Criteria) en réponse à la quatrième priorité communautaire, ainsi qu'un guide d'évaluation destiné aux laboratoires d'évaluation (ITSEM ou Information Technology Security Evaluation Manual).

Comme l'indique la Commission :

> *"Un des principaux objectifs qui sous-tendent l'élaboration de ces critères uniformisés au plan international est la compatibilité de la certification des évaluations effectuée par les organismes nationaux dans l'optique de la reconnaissance mutuelle des certifications qui synthétisent les résultats et attestent de la régularité des évaluations".*[1]

... et les ITSEC :

> *"bien que les utilisateurs aient la possibilité soit de se fier à la parole des fournisseurs, soit à tester eux-mêmes les produits, beaucoup préféreront se reposer sur les résultats d'une estimation impartiale effectuée par un organisme indépendant".*

Ces critères ont été constitués sur la base de la mise en commun et de l'harmonisation des méthodes et expériences accumulées par les autorités gouvernementales de l'Allemagne, la France, la Grande-Bretagne et les Pays-Bas.[2]

Les documents ITSEC/ITSEM constituent pour l'essentiel un référentiel de critères et une méthodologie d'évaluation de la sécurité de produits ou de systèmes existants ou à développer, en vue d'une certification, destinés à satisfaire aux exigences et besoins de sécurité des organismes gouvernementaux.[3]

---

[1] "Proposition de recommandation du Conseil concernant des critères communs d'évaluation de la sécurité des technologies de l'information".

[2] Toute chose égale, les ITSEC sont une version étendue et européenne du TCSEC (Trusted Computer System Evaluation Criteria ou "Livre Orange") du NCSC (National Computer Security Center) publié aux Etats-Unis en 1985 et utilisé par le DoD (Department of Defense, USA) pour l'évaluation de produits.

[3] Comme nous le verrons par suite, l'acceptation des ITSEC par le marché est largement conditionnée par l'extension du champ d'application des critères aux besoins commerciaux de sécurité, la compétence du

© CIGREF 1992

En France, l'initiative ITSEC/ITSEM a donné lieu à la création en 1992 du Centre d'Evaluation de la Sécurité des Systèmes d'Information Commerciaux (CESSIC). Le CESSIC est l'organisme technique chargé de l'évaluation proprement dite. Le Service Central de la Sécurité des Systèmes d'Information (SCSSI) est l'organisme d'accréditation et de délivrance du certificat.

Les objectifs du CESSIC sont :

- de satisfaire les demandes d'évaluation de la sécurité offerte par les équipements ou les systèmes de traitement de l'information proposés par les industriels pour répondre à la demande du secteur commercial.

- de positionner un savoir-faire national pour faire face à la concurrence internationale en matière d'évaluation.

- d'aider les commanditaires à établir leur cible de sécurité.

L'organisation mise en place ne semble pas répondre à la réglementation généralement admise dans le cadre européen :

- les ITSEC ne constituent pas une Norme internationalement reconnu (ISO), ni une Norme européenne (CEN) ;

- les fonctions d'accréditation des organismes de certification, d'accréditation des évaluateurs et de certification sont confondues en un seul organisme ;

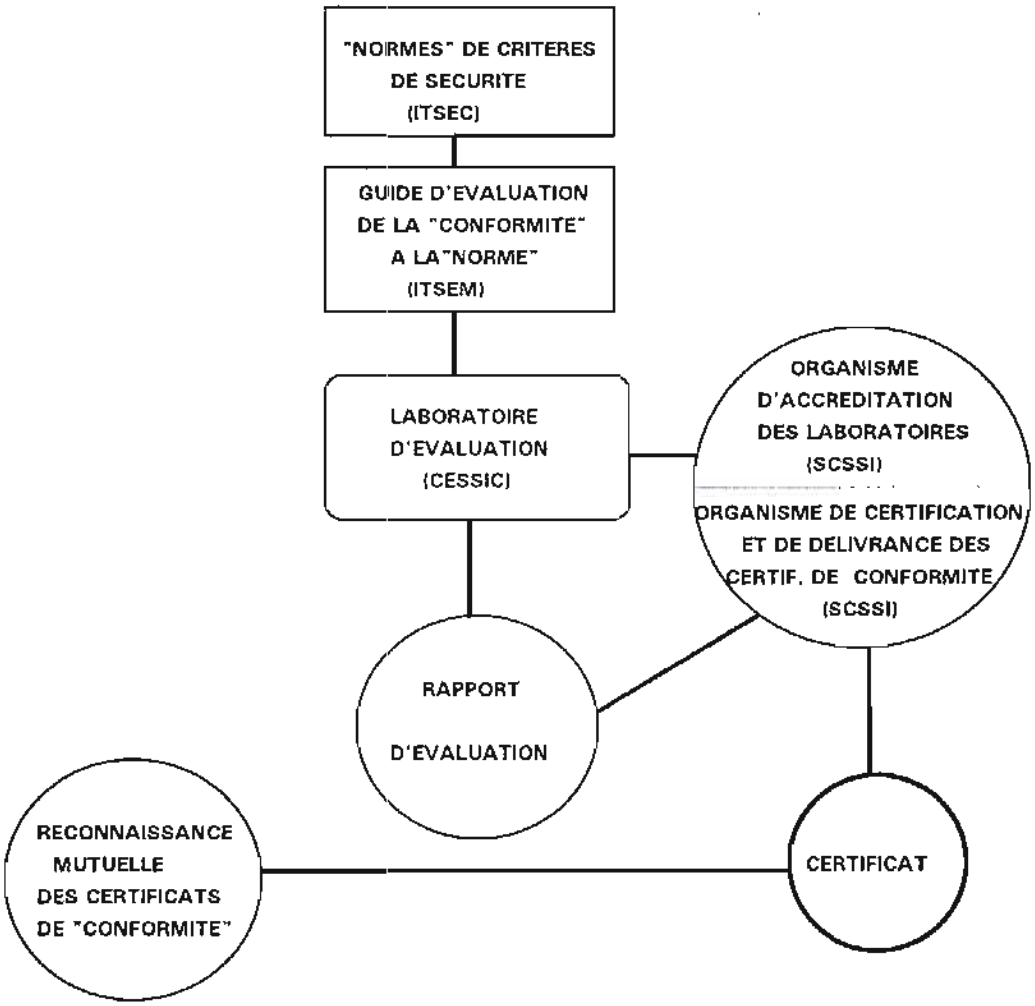
- le processus de reconnaissance mutuelle n'est pas clairement défini.

---

ou des laboratoires d'évaluation et les moyens financiers ainsi qu'à l'impartialité et l'indépendance de l'organisation mise en place.

© CIGREF 1992

Le dispositif de certification est le suivant :



La version 1.0 des ITSEC a été diffusé et présenté publiquement lors d'une consultation internationale se tenant à Bruxelles en septembre 1990. Une seconde version a été publiée en janvier 1991, intégrant les commentaires issus de la précédente réunion. Enfin, de nouveaux commentaires ont abouti à la version 1.2 de juin 1991, publiée par la Communauté Européenne.

La version 1.2 est actuellement disponible en français. Elle demeure valable pour une période de deux ans à compter de sa date de parution, soit jusqu'en 93/94. C'est sur cette version que porte la présente étude.

© CIGREF 1992

Afin de compléter le dispositif communautaire initié par les ITSEC, la Communauté a lancé un programme sur la sécurité de l'information (Security Investigation Programme, INFOSEC '92). Ce programme défini 14 tâches dont l'objet est d'éclairer les 4 premières lignes d'action du plan d'action communautaire.

Actions et tâches correspondantes

ACTION LINE 1 Development of a Strategic Framework for the Security of Information Systems	**T.01 Definitions within Information Systems Security** *To develop and test a multi-lingual basis for information security terms and concepts.* **T.02 Awareness Programme** *To create a framework for the planning, development and dissemination of information security awareness material in Europe.* **T.03 Incident Reporting** *To study the implications of creating a common structure for recording and reporting incidents.*
ACTION LINE II Identification of User And Service Provider Requirements for the Security of Information Systems	**T.04 Inventory of Security Organisations** *To create an inventory of relevant 'security organisations' including their roles and responsibilities.* **T.05 Legislation/Regulation of Information Security** *To analyse the existing legislation/regulations pertaining to information systems within the Member States.* *To make proposals that could create a basis for legal harmonisation on information security matters* *To consider information security as an element in any future European legal alignment*
ACTION LINE III Solutions for Immediate and Interim Needs of Users, Suppliers and Service Providers	**T.06 ITSEC - Evaluation of Trail Period** *To ensure the widest European participation in the application and use of ITSEC.* **T.07 ITSEC and Standardisation** *To review the contents/structure of ITSEC to establish its potential as an International Standard, in support of the SOG-ITS study mandate.* *To establish the National, European and International Standards processes most suitable form ITSEC acceptance.* *To further development of ITSEC as an international "standard".* **T.08 ITSEC - Predefined Functionality Classes** *To first create and make available (for example to T.10) an administrative process in which functional classes/profiles can be articulated in a structured way consistent with ITSEC direction and language.* *To create specific user functionality classes on security that reflect the needs of specific sectors (prioritised by highest threats etc., as determined)*

© CIGREF 1992

ACTION LINE IV Development of Specifications, Standardisation, Evaluation and Certification in respect of the Security of Information Systems	**T.09 Architectural Guidelines** *To produce a recommended approach to security in the architecture of distributed systems, taking account of current work in this area* *To provide justifications which will enable SOG-IS and other actors to support this recommendation for future R&D projects.* *To support the definition of ITSEC evaluatable targets in the context of the architecture of open distributed information systems.* **T.10 European Security Profile Alignment** *To achieve a common or consistent European set of functional profiles (flexible enough to embody security aspects to various levels of desired assurance by sector/industry) and to create guidelines to support the specific prototyping of such profiles within subsequent architectural and operational infrastructures* **T.11 Verification of Security Profiles** *To create a software tool to assist evaluators in verifying security protocols. This tool should be able to identify design errors and "weak spots" in the security protocol.* **T.12 ITSEC - Commercial Accreditation** *To develop guidelines, possibly on a sector by sector basis, on how ITSEC evaluation/certification should be used in the process of commercial accreditation of secure systems.* **T.13 Conformance Testing and Security** *To promote a preliminary study aimed at evaluating the appropriateness of existing recognised organisations to perform conformance testing for the security aspects of IT products.* **T.14 Risk Analysis** *To formulate a strategy for the introduction of risk analysis processes throughout Europe based on an analysis of existing and planned Risk analysis and Management methodologies.*

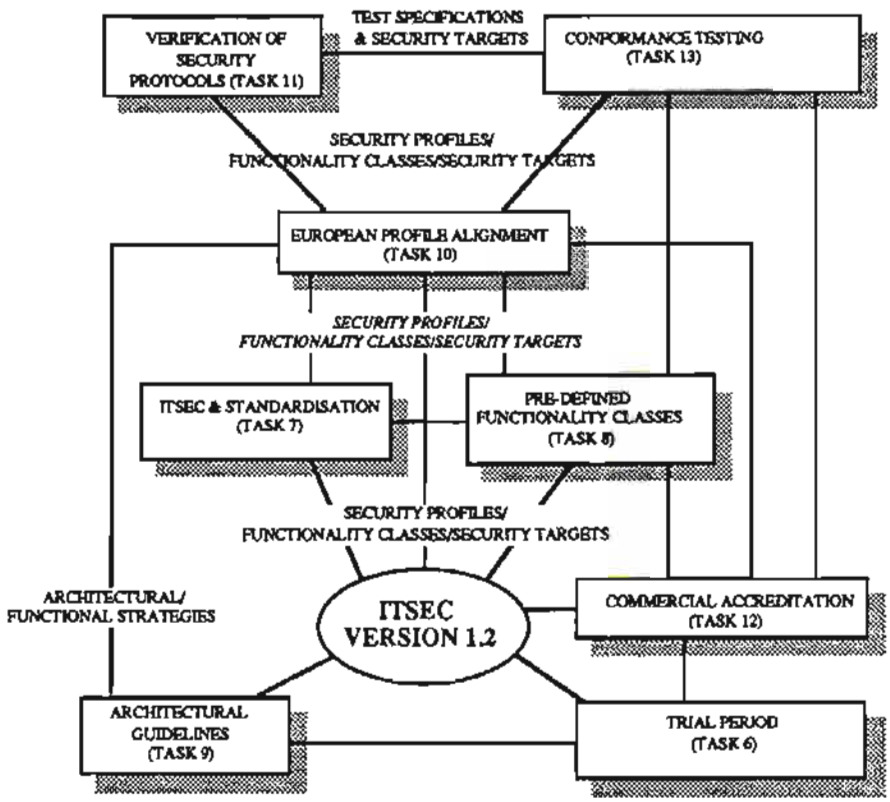


Diagram 9 - ITSEC/SECURITY INVESTIGATIONS INTERDEPENDENCIES

© CIGREF 1992

Les critères constituent une brique de base essentielle du cadre défini par l'action communautaire. Ils feront incontestablement référence en matière de sécurité des systèmes d'information. Le graphique précédent permet de visualiser les tâches directement liées aux ITSEC.

Une seconde section de travaux dans le domaine de la sécurité des systèmes d'information a été initié par la Commission en août 1992 dans le cadre INFOSEC (Work Plan 93).

Ce plan défini 5 domaines d'investigation :

- Sécurité des télécommunications
- Critères d'évaluation
- Cadre sécuritaire
- Amélioration de la confidentialité des applications
- Exploration et intégration.

Seize nouvelles tâches ont été identifiées :

- Politique et gestion de la sécurité
- Aspects transnationaux et inter-opérateurs de la sécurité
- Boucles locales de sécurité et leur gestion
- Classes de fonctionnalités et sécurité des profils utilisateurs/services
- Modèles de sécurité pour la fourniture de services
- Interfaces de programmation d'application (API) génériques de sécurité pour les services numériques
- Modèles pour la législation et la régulation en sécurité des télécommunications
- Pré-évaluation ITSEC/ITSEM
- Exigences pour les services d'évaluation tierce partie
- Besoins des utilisateurs en matière de sécurité des SI commerciaux
- Amélioration des messageries privées
- Amélioration de la sécurité des applications multimédias et télétravail
- Exploration et Intégration

© CIGREF 1992

3. Les besoins en matière de sécurité des systèmes d'information et de communication

Une bonne sécurité exige une expression des besoins d'informatisation qui prenne en compte, spécifiquement, les besoins de sécurité. Dans trop de cas en effet, au niveau de l'expression des besoins fonctionnels comme au niveau de l'organisation, de la description du futur processus, ou de la définition des produits et des systèmes (matériel ou logiciel), la sécurité n'est pas, ou insuffisamment prise en compte.

En effet, entre un **utilisateur** qui exprime des besoins (en général sous forme de fonctions à satisfaire), un **informaticien** qui doit délivrer un système qui satisfasse ces fonctions et un **fournisseur** qui doit fournir partie ou totalité des éléments composants du système ou un produit, il y a nécessité de critères, d'une démarche et d'un langage communs facilitant la communication, la coordination et la prise en compte de la sécurité dans les projets, tout en garantissant un niveau d'assurance parfaitement défini.

Cette assurance exige des critères **objectifs, pertinents** et **efficaces**.

Les utilisateurs attendent :

- des produits et systèmes auxquels ils puissent croire quant à leur niveau de sécurité par rapport à un besoin exprimé (conformité et assurance).

- des produits comparables, dans le temps et dans l'espace, quant à leur niveau de sécurité (pérennité et transparence).

© CIGREF 1992

Ces exigences doivent s'appliquer :

- aux **besoins commerciaux** courants, et non aux seuls besoins gouvernementaux et militaires et intégrer les besoins de flexibilité des organisations.

- à des systèmes d'information et de communication pris dans leur globalité, et non à leurs seuls composants.

- à des architectures techniques et applicatives de plus en plus ouvertes (entreprise étendue), complexes et hétérogènes.

Pour cela, les utilisateurs souhaitent disposer :

- de normes et standards auxquels ils puissent se référer dans les relations avec leurs fournisseurs et dans l'élaboration de leurs systèmes d'information et de communication.

- de méthodes harmonisées de développement des systèmes à sécuriser et d'évaluation du niveau de protection qu'offrent ces systèmes.

- d'une reconnaissance mutuelle internationale des évaluations de sécurité par les fournisseurs ainsi que des certificats auxquels ils se réfèrent.

© CIGREF 1992

4. Présentation des ITSEC

L'objectif de ce chapitre est de présenter sous une forme synthétique la démarche et les principaux concepts des ITSEC.

4.1 Généralités

4.1.1 Introduction

Les trois exigences classiques en sécurité (ou exigences DIC) sont la Disponibilité de service, l'Intégrité et la Confidentialité des données.

Disponibilité : propriété visant à prévenir un délai inacceptable d'accès autorisé à une information, à une donnée ou à des ressources informatiques.

Intégrité : propriété visant à prévenir la modification non autorisée d'une information ou d'une donnée ;

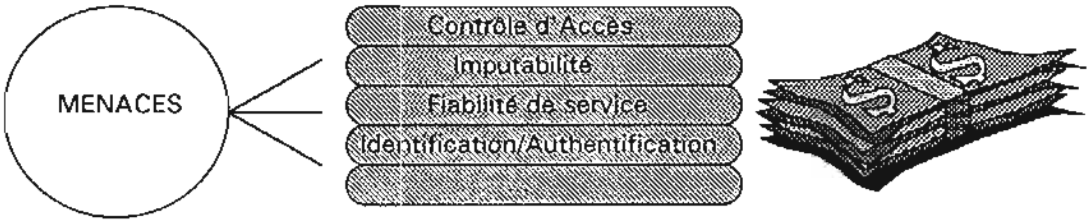
Confidentialité : propriété visant à prévenir la divulgation non autorisée d'une information ;

Afin de satisfaire les exigences de sécurité des organismes, le commanditaire d'une évaluation détermine d'abord des **objectifs** de sécurité. Les objectifs de sécurité sont définis au regard des **menaces** et des **contraintes** (lois, règlements, pratiques régissant les informations sensibles, ...) qui pèsent sur le système d'information, ainsi qu'au regard de la **valeur** des objets à protéger.

L'entreprise doit en particulier établir la liste des objets et opérations qu'elle entend voir protéger, identifier des menaces potentielles et les classer selon leur importance pour la société.

© CIGREF 1992

La détermination des objectifs de sécurité permet à l'utilisateur de choisir un produit ou de faire développer un système composé de **fonctions** de sécurité (par exemple, contrôle d'accès, auditabilité, récupération d'erreur, etc ...) conformes à ses objectifs et dont l'efficacité est adaptée aux menaces identifiées.



Les ITSEC proposent une liste de fonctions génériques de sécurité ainsi que des classes prédéfinies de fonctions courantes de sécurité répondant à des objectifs similaires de sécurité.

Des **mécanismes** de sécurité, notamment les mécanismes critiques dont la défaillance entraînerait une brèche de sécurité, vont enfin permettre de spécifier de manière détaillée les fonctionnalités à implémenter et de leur attribuer un niveau de résistance approprié.

4.1.2 Définition du système ou du produit à évaluer.

L'évaluation proposée par les ITSEC s'applique à des **produits** logiciel et/ou matériel non spécifiques et à des **systèmes** répondant à des besoins spécifiques et fonctionnant dans des environnements d'exploitation particuliers.

Un système est généralement construit à partir d'un certain nombre de composants logiciels et matériels. Certains de ces composants sont développés spécifiquement pour un besoin donné (ex. : application) alors que d'autres sont achetés en standard.

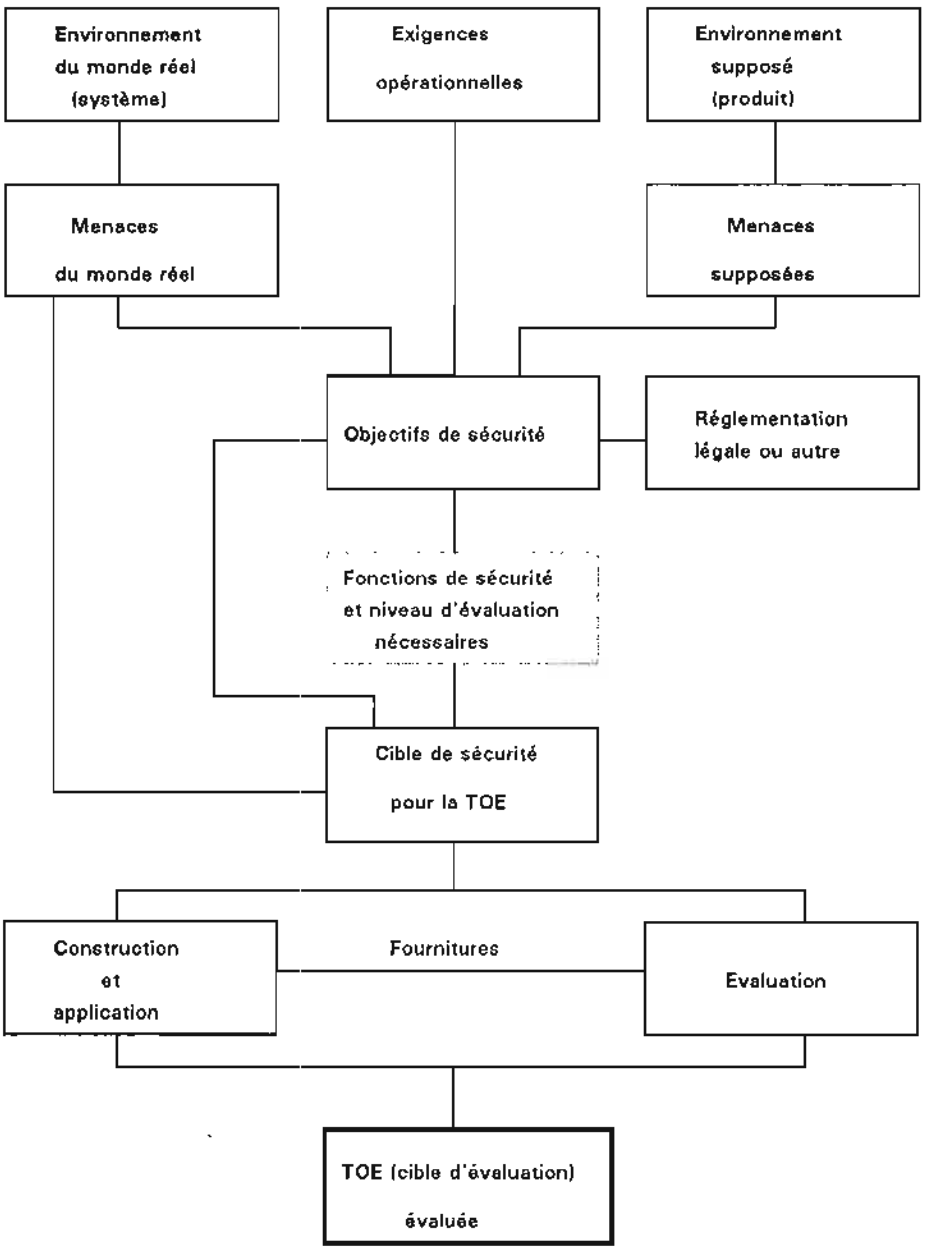
Des critères de sécurité identiques sont utilisés dans l'évaluation des produits et des systèmes.

© CIGREF 1992

4.1.3 Processus d'évaluation.

C'est le commanditaire d'une évaluation qui fournit à l'organisme d'évaluation les éléments nécessaires à celle-ci selon le niveau de sécurité recherché. Ce commanditaire peut être un **fabricant**, une **société de services** ou, plus rarement, un organisme **utilisateur.**

Tableau n° 1 : processus d'évaluation



© CIGREF 1992

Les étapes de mise en oeuvre sont les suivantes :

1. Le commanditaire détermine ses besoins opératiònnels ainsi que les menaces que la cible de l'évaluation est supposée parer, les contraintes organisationnelles, techniques, réglementaires, etc. , dans le langage ITSEC, ses **objectifs** de sécurité.

2. Une fois déterminées les **mesures non techniques** applicables (schéma directeur, mesures organisationnelles, consignes d'exploitation, contrôle du personnel, ...), l'identification des **besoins techniques** de sécurité va permettre de définir des **fonctions** et **mécanismes** de sécurité ainsi que le **niveau d'assurance** que la cible de l'évaluation - c'est-à-dire le produit ou le système - devrait atteindre pour offrir le niveau de confiance visé.

L'ensemble de ces éléments - dont la constitution et la rédaction est à la charge du commanditaire - devient la **cible de sécurité** pour le développement.

L'objectif de l'évaluation est de vérifier l'adéquation des contre-mesures aux menaces et la délivrance par un organisme reconnu et indépendant d'un certificat de conformité de la cible de l'évaluation à la cible de sécurité.

4.2 Fonctionnalités.

4.2.1 Cible d'évaluation.

La **cible de l'évaluation** ou **TOE** est définie comme tout produit ou système soumis à une évaluation.

La fonctionnalité d'une cible d'évaluation est appréhendée selon trois niveaux d'abstraction :

- les **objectifs** de sécurité (pourquoi)
- les **fonctions** de sécurité (quoi)
- les **mécanismes** de sécurité (comment)

© CIGREF 1992

4.2.2 Cible de sécurité.

La **cible de sécurité** est un document contenant la spécification des fonctions dédiées à la sécurité et le niveau d'assurance recherché. Elle fournit la base permettant d'évaluer la cible de l'évaluation.

La cible de sécurité comprend :

- la politique de sécurité du système (environnement du système, objectifs de sécurité, menaces et parades, ...) et/ou la description du produit (mode d'emploi du produit, environnement d'utilisation, menaces supposées, caractéristiques de sécurité, ...) ;

- la spécification des fonctions dédiées à la sécurité ;

- la définition des mécanismes de sécurité requis (optionnelle) ;

- la résistance minimum des mécanismes annoncée ;

- le niveau d'évaluation de la cible.

4.2.3 Regroupement de fonctions de sécurité ou"rubriques"

Afin de faciliter la description des fonctionnalités, les ITSEC fournissent une liste de fonctions de base intitulée "rubriques". Les regroupements de fonctions proposés par ITSEC sont :

- identification/authentification
- contrôle d'accès
- imputabilité
- auditabilité
- réutilisation d'objets
- fidélité
- fiabilité du service
- échange de données.

© CIGREF 1992

4.2.4 Classes de fonctionnalités prédéfinies

Les ITSEC autorisent que les fonctions de sécurité soient définies en référence à :

- des classes prédéfinies,
- des normes existantes,
- des fonctions spécifiques.

Classes prédéfinies

Les ITSEC proposent, à titre d'exemple, les classes prédéfinies suivantes :

- six classes : F-C1, F-C2, F-B1, F-B2, F-B3, F-B3 bis dont les exigences fonctionnelles sont proches du TCSEC ("Orange Book").

- cinq classes plus spécifiques : F-IN, F-AV, F-DI, F-DC, F-DX, dont les particularités sont les suivantes :

F-IN : forte intégrité (ex. : bases de données)
F-AV : forte disponibilité d'un système complet (ex. : système de contrôle de processus industriel)
F-DI : forte intégrité pendant les échanges de données
F-DC : forte confidentialité pendant les échanges de données (ex.: dispositif cryptographique)
F-DX : forte confidentialité et intégrité des échanges dans les réseaux (ex. : transmission d'informations sensibles sur un réseaux public).

Les normes existantes

Les normes de sécurité, lorsque celles-ci existent, peuvent servir de documents d'entrée pour la cible de sécurité.

© CIGREF 1992

Les fonctions de sécurité spécifiques

Il est possible, enfin, de spécifier individuellement chaque fonction dédiée à la sécurité. Elles doivent être complètement justifiées et il convient d'apporter la preuve qu'elles répondent effectivement aux objectifs de sécurité spécifiés.

4.2.5 Styles de spécification

Les ITSEC proposent trois styles de spécification différents dans l'ordre croissant du niveau d'exigence recherché :

- **Informel** :

- langage naturel
- classe prédéfinie

- **Semi-formel** (ou conventionnellement restreint) :

- langage des annonces de produits
- langage naturel restreint
- méthodes de conception structurées (ex. : SSADM, YSM, SADT, JSD, JSP, ...)
- "modèle informel de politique de sécurité"
- classe prédéfinie (adaptée).

- **Formel** :

- langage formel de spécification (Z, RAISE, VDM, GYPSY, ISO)
- modèles formels de politique de sécurité (BELL-LA-PALUDA, BREWER-NASH, EIZENBERG, LANDWEHR, CLARK-WILSON)
- classe prédéfinie (adaptée).

Plus le niveau de confiance exigé est élevé, plus les spécifications doivent être rédigées dans un style formel. Il convient néanmoins de conserver un style informel afin que l'utilisateur final soit à même d'exprimer correctement ses besoins.

© CIGREF 1992

4.3 Le système d'assurance sécurité

Le choix d'un produit ou le développement d'un système exige que l'on s'assure autant de la conformité des fonctions de sécurité aux objectifs de sécurité (ont-elles été correctement développées et sont-elles correctement utilisées ?) que dans leur efficacité face aux menaces.

C'est ce que l'on appellera, dans le langage ITSEC, **l'assurance dans l'efficacité** et **l'assurance dans la conformité**.

Assurance dans l'efficacité : assurance que les fonctions et mécanismes de sécurité fournis par le système ou le produit satisfont aux objectifs de sécurité déclarés et que les mécanismes résistent à une attaque directe.

Assurance dans la conformité : assurance que les fonctions et mécanismes de sécurité sont (ou ont été) correctement développés et exploités.

Si les tâches d'évaluation de l'efficacité et de la conformité sont imbriquées, les niveaux d'évaluation sont dans la pratique déterminés par les critères de conformité dans la mesure où les exigences liées à l'efficacité ne changent pas selon les niveaux.

4.3.1 Assurance-efficacité

L'évaluation de l'efficacité, comme l'évaluation de la conformité, est effectuée par rapport à la cible de sécurité. Son but est de vérifier si le niveau de confiance établi lors de l'évaluation de la conformité reste valable lors de l'utilisation du système ou du produit.

Les critères de cette évaluation sont les suivants :

-**pertinence** de la fonctionnalité
-**cohésion** des fonctions et des mécanismes (compatibilité et coopération)

© CIGREF 1992

-**résistance** des mécanismes
-**vulnérabilités** connues, au niveau du développement de la TOE
-**fiabilité** d'emploi
-**vulnérabilités** connues, au niveau de l'exploitation de la TOE.

L'efficacité est appréhendée selon 6 critères ou "aspects" dont 4 sont relatifs au développement et 2 à l'exploitation.

L'évaluation de l'efficacité en fonction de ces critères nécessite une documentation fournie par le commanditaire, ainsi que les résultats de l'évaluation de la conformité de la TOE.

L'évaluation de l'efficacité se ramène à une analyse de vulnérabilité de la TOE, c'est-à-dire à l'inventaire de toutes les possibilités de désactivation, de contournement, de corruption ou d'attaque directes des fonctions de sécurité.

Cette analyse requiert de la part du commanditaire la documentation adéquate selon le niveau de confiance recherché (définie à l'aide des critères de conformité).

La résistance des **mécanismes critiques** (ceux dont la défaillance génère une brèche de sécurité) est évaluée face à une attaque directe.

Les ITSEC distinguent 3 niveaux de résistance :

-**résistance de base** : efficace face à une menace aléatoire, mais insuffisante face à des attaquants compétents.

-**résistance moyenne** : bonne protection contre des attaquants ayant des moyens limités.

-**résistance élevée** : ne peut être mise en défaut que par des attaquants disposant de moyens exceptionnels.

Comme pour l'assurance-conformité que nous verrons par la suite, 7 niveaux d'évaluation sont proposés (E0 à E6). Si un mécanisme n'est pas suffisamment fort pour le niveau revendiqué, le niveau d'évaluation global sera E0, de façon à invalider la TOE pour l'usage qui en était prévu.

L'efficacité de la TOE est toujours évaluée dans le contexte d'une cible de sécurité donnée. Ainsi, les vulnérabilités connues d'un produit

© CIGREF 1992

intégré dans un système auront plus ou moins d'importance selon les spécifications du système.

Par ailleurs, les exigences et les options concernant la forme et le contenu de la cible de sécurité d'une TOE seront différents suivant qu'il s'agit d'un système ou d'un produit.

Critères concernant le développement ("construction")

La documentation produite par le commanditaire est celle requise pour l'évaluation de la conformité.

ASPECT 1 - Pertinence de la fonctionnalité

- Définition : aptitude des fonctions sélectionnées à contrer les menaces identifiées dans la cible de sécurité.

- Contenu de l'analyse : liens entre les fonctions et les mécanismes sélectionnés et les menaces correspondantes.

- Exigences probatoires : l'analyse doit montrer comment les menaces sont contrées. La documentation, conforme au niveau annoncé, doit produire toutes informations utiles à cet égard.

- Tâches de l'évaluateur : vérifier que tous les éléments nécessaires à l'analyse sont bien présents et que celle-ci a bien pris en compte toutes les informations requises pour le niveau annoncé.

ASPECT 2 - Cohésion des fonctionnalités

- Définition : aptitude des fonctions de sécurité à se soutenir mutuellement pour former un ensemble intégré et efficace.

- Contenu de l'analyse : relations potentielles entre fonctions et entre mécanismes.

- Exigences probatoires : l'analyse doit permettre d'affirmer qu'aucun conflit n'est possible entre une fonction donnée (ou un mécanisme) et une autre fonction (ou un mécanisme).

© CIGREF 1992

- Tâches de l'évaluateur : cf aspect 1.

ASPECT 3 - Résistance des mécanismes

- Définition : résistance des mécanismes à une attaque directe en prenant en considération le niveau des ressources nécessaire à un attaquant pour réussir son attaque.

- Contenu de l'analyse : liste des mécanismes considérés comme critiques pour la TOE.

- Exigences probatoires : l'analyse doit démontrer que tous les mécanismes critiques présentent le niveau de résistance annoncé par le commanditaire.

- Tâches de l'évaluateur : cf aspect 1 + :

* vérifier que tous les mécanismes critiques ont bien été identifiés,

* pratiquer des tests d'intrusion confirmant la résistance minimale annoncée pour ces mécanismes.

ASPECT 4 - Evaluation des vulnérabilités générées lors du développement

- Définition : vulnérabilité identifiée pendant l'évaluation à partir des critères précédents, permettant la désactivation, le court-circuit, le contournement ou la corruption de fonctions ou de mécanismes.

- Contenu de l'analyse : liste des vulnérabilités fournies par le commanditaire (et connues de lui). Il doit être possible d'analyser les conséquences potentielles et de proposer des mesures pour les contrer.

© CIGREF 1992

- Exigences probatoires : l'analyse des conséquences doit démontrer que les vulnérabilités ne peuvent pas être exploitées :

* grâce à la présence d'autres mécanismes de sécurité,

* parce qu'en pratique, ces failles ne touchent pas la cible de sécurité ou peuvent être contrées par des mesures de sécurité externes définies dans la documentation.

- Tâches de l'évaluateur : cf aspect 1 + :

* vérifier l'exhaustivité de la liste fournie

* vérifier que les mesures de sécurité externes à appliquer sont correctement documentées

* tester l'intrusion pour vérifier si les vulnérabilités connues sont exploitables ou non.

Critères concernant l'exploitation ("exploitation")

La documentation à fournir par le commanditaire est celle qui est requise pour la conformité ainsi que :

- l'analyse de la fiabilité d'emploi
- la liste des vulnérabilités connues au niveau de l'exploitation

ASPECT 1 - Fiabilité d'emploi

- Définition : impossibilité de configurer ou d'utiliser la TOE sans les fonctions de sécurité prévues alors qu'un administrateur ou un utilisateur final croît en la présence de celles-ci.

- Contenu de l'analyse : l'analyse doit identifier toutes les possibilités de traitement de la TOE, y compris la récupération d'erreurs, avec tout ce que cela implique pour que la sécurité soit maintenue.

© CIGREF 1992

- Exigences probatoires : l'analyse doit montrer que toute erreur de traitement (ou de configuration) entraînant la désactivation (ou la non activation) de fonctions de sécurité soit facile à détecter.

- Tâches de l'évaluateur : cf développement aspect 1 + :

*faire des essais de configuration et d'installation à l'aide uniquement des manuels pour vérifier la fiabilité.

ASPECT 2 - Evaluation des vulnérabilités au niveau de l'exploitation

- Définition : vulnérabilité concernant l'exploitation identifiée pendant l'évaluation à l'aide des critères précédents, permettant la désactivation, le court-circuit, le contournement ou la corruption de fonctions ou de mécanismes.

- Contenu de l'analyse : cf aspect 4 développement, appliqué à l'exploitation.

- Exigences probatoires : cf aspect 4 développement, appliqué à l'exploitation.

- Tâches de l'évaluateur : cf aspect 4 développement, appliqué à l'exploitation.

© CIGREF 1992

4.3.2 Assurance-conformité

Les ITSEC définissent 7 niveaux de confiance (E0 à E6) par ordre croissant d'exigence du point de vue des preuves demandées :

E0 : assurance insuffisante.

E1 : cible de sécurité + description informelle de l'architecture de sécurité de la TOE.

E2 : E1 + description informelle de la conception détaillée + évaluation de la preuve des tests fonctionnels + système de gestion de configuration + surveillance de la diffusion.

E3 : E2 + évaluation du code source + évaluation de la preuve des tests de ces mécanismes.

E4 : E3 + modèle formel de politique de sécurité + spécification semi-formelle des fonctions de sécurité, des conceptions générale et détaillée.

E5 : E4 + correspondance conception détaillée/code source.

E6 : E5 + spécification formelle des fonctions de sécurité et de la conception générale compatible avec modèle formel de politique de sécurité.

A l'image de la structure des critères d'efficacité, on va trouver pour chaque niveau d'évaluation des critères traitant :

- d'une part, de la façon dont le produit ou le système seront développés ("construction" : processus de développement + environnement de développement),

- d'autre part, de la façon dont le produit ou le système seront utilisés ("exploitation" : documentation d'exploitation + environnement d'exploitation).

© CIGREF 1992

La structure détaillée des critères de conformité, plus complexe que celle de l'efficacité, est la suivante :

Critères concernant le développement ("construction")

-***Processus de développement*** :

Phase 1 - spécification des besoins
Phase 2 - conception générale
Phase 3 - conception détaillée
Phase 4 - réalisation

-***Environnement de développement*** :

Aspect 1 - gestion de configuration
Aspect 2 - langages de programmation et compilateurs
Aspect 3 - sécurité des développeurs

Critères concernants l'exploitation ("exploitation")

- ***Documentation d'exploitation*** :

Aspect 1 - documentation utilisateur
Aspect 2 - document d'administration

- ***Environnement d'exploitation*** :

Aspect 1 - livraison et configuration
Aspect 2 - démarrage et exploitation

Comme lors de l'évaluation de l'efficacité, pour chaque phase ou aspect, on retrouvera les rubriques suivantes :

- documentation commanditaire
- définition
- exigence de contenu et de présentation
- exigences probatoires
- tâches de l'évaluateur

© CIGREF 1992

A chaque niveau d'évaluation de la conformité, il faut satisfaire des critères de plus en plus exigeants qui seront répétés à chaque niveau de E1 à E6. Afin de ne pas alourdir inutilement l'étude, seul le niveau E1 est détaillé en annexe (7.3).

Des tableaux de synthèse proposés par le document ITSEC permettent de visualiser pour chaque niveau les éléments essentiels qui doivent être fournis par le commanditaire ainsi que le niveau d'évaluation auquel ils sont exigés pour la première fois par l'évaluateur (7.2).

4.4 Résultat de l'évaluation

L'évaluation de l'efficacité et de la conformité d'une TOE par rapport à sa cible de sécurité se traduit par un niveau d'évaluation et une cotation de la résistance minimum des mécanismes.

Le classement obtenu par une TOE comporte :

- une référence à la cible de sécurité pour une TOE donnée,
- le niveau dévaluation obtenu,
- le degré de résistance minimale des mécanismes de sécurité de la TOE.

Une TOE contenant une vulnérabilité exploitable non corrigée est retirée de l'évaluation et obtient le niveau E0.

Le processus d'évaluation se traduit par un rapport d'évaluation qui servira de base à une certification par un organisme de certification national approprié.

© CIGREF 1992

5. Conclusion

Les ITSEC adressent un problème important mais la démarche d'ensemble demeure encore limitée au regard des besoins et des enjeux posés par la protection des systèmes étendue d'information et de communication des grands organismes commerciaux.

Incontestablement, les ITSEC apportent des principes solides et un progrès important dans la mesure de la sécurité des systèmes d'information et de communication cependant que de nombreuses difficultés demeurent.

5.1 Les avancés significatives

Les ITSEC apportent d'abord une synthèse d'un certain état de l'art en matière de sécurité des systèmes d'information et de communication puisqu'ils intègrent les réflexions et les expériences accumulées depuis de nombreuses années dans plusieurs pays européens.

Ils offrent ensuite un instrument de mesure acceptable de la sécurité de ces systèmes, même si les critères demeurent limités à l'évaluation de systèmes et surtout de produits.

L'initiative ITSEC aura des incidences positives sur la normalisation dans le domaine de la sécurité, que se soit en matière d'évaluation de produit ou que se soit en matière d'évaluation de processus et d'assurance sécurité.

Face à l'insuffisance de l'offre commerciale, les ITSEC sont de nature à dynamiser le marché de la certification et de la sécurité.

Enfin, les ITSEC apportent déjà un certain niveau de structuration dans la démarche sécuritaire, notamment à travers les notions de cible de sécurité, de mesure de la sécurité ou d'assurance, ainsi qu'un langage amené à être partagé par le plus grand nombre.

© CIGREF 1992

5.2 Les difficultés

Comme toute tentative de synthèse, les ITSEC véhiculent des principes "éclairés" mais rencontrent également plusieurs difficultés dont certaines sont surmontables alors que d'autres paraissent beaucoup plus rédhibitoires.

La première difficulté, évoquée en introduction, tient à ce que les ITSEC constituent dans l'ensemble une synthèse inadéquate entre les besoins gouvernementaux et les besoins commerciaux, lesquels sont différents.

Les grands organismes commerciaux souhaitent pouvoir disposer de critères à la fois objectifs, simples, flexibles et à très forte couverture leur permettant de mesurer eux-mêmes, si nécessaire, le niveau de sécurité de tout ou parties de leurs systèmes d'information et de communication, d'évaluer et de comparer aisemment les offres du marché et enfin, de disposer de méthodes de conception et de réalisation de systèmes d'information sûrs mais économiques.

Les caractéristiques de ces systèmes sont leur complexité, leur hétérogénéïté, leur décentralisation et leur ouverture croissante à l'environnement de chaque entreprise (clients internes ou externes, fournisseurs, concurrents).

La seconde difficulté tient à l'absence, dans les ITSEC, de principes ou d'éléments de méthode permettant de spécifier opérationnellement les besoins des organismes ainsi que les objets et services à protéger (audit).

Plus proche encore du coeur de la démarche ITSEC, l'absence d'un mode opératoire facilitant la spécification de la cible de sécurité de la TOE, c'est-à-dire l'articulation cohérente entre les fonctionnalités de sécurité, les menaces et les niveaux jugés nécessaires, rend pour le moins difficile la mesure et l'évaluation de la sécurité d'un système ou d'un produit.

Dans le même ordre d'idées, on ne peut que constater la pauvreté voire l'inapplicabilité de certaines rubriques génériques de fonctions dédiées à la sécurité, telle la rubrique "échange de données" (OSI).

© CIGREF 1992

Les exigences des vendeurs et des utilisateurs devraient permettre, à terme, une extension importante du champ d'application des ITSEC à d'autres menaces, d'autres fonctions et d'autres classes de sécurité, le risque étant alors la prolifération d'applications locales (notamment sectorielles) et dérivées des ITSEC.

Une autre difficulté provient de ce que le champ d'application des ITSEC est limité aux mesures techniques de sécurité à l'exclusion, à de rares exceptions près (procédures d'exploitation, sécurité physique; ...), des mesures de sécurité non techniques telles l'organisation, le personnel ou l'administration de la sécurité, dont chacun s'accorde sur le caractère essentiel.

Traduisant en cela leur inadéquation relative aux besoins commerciaux courants, la plupart des exigences demandées à chaque niveau touchent uniformément l'ensemble des fonctions considérées.

Autrement dit, il semble difficile d'envisager les cas, pourtant fréquents, où l'objectif est exigeant pour certaines fonctions d'un produit ou d'un système (ex. : E4 pour des fonctions d'identification/authentification) et faible pour d'autres (ex. : E1 voire EO pour des fonctions de fiabilité de service). En l'absence de cette possiblité, nous avons constaté que bien peu d'entreprises, en l'état actuel de l'art, pourraient dépasser le niveau E2.

A ces incertitudes touchant l'évaluation et sa méthodologie, il faut ajouter celles ayant plus spécifiquement trait à la certification.

L'enquête AFNOR-CIGREF-CLUSIF reproduite en annexes montre que si une majorité d'entreprises commerciales souhaitent disposer de produits certifiés, une écrasante majorité n'accepte pas d'en payer le prix (39 % ne paieraient pas et 28 % > 2% du prix du produit), traduisant peut-être en cela le sentiment que la sécurité est pour l'utilisateur une exigence de base.

Par ailleurs, il n'existe pas actuellement d'éléments tangibles permettant d'évaluer le coût ou la durée d'une évaluation. Ce dernier élément est important. L'enquête précédemment citée indique que près de la moitié des entreprises interrogées n'accepteraient pas d'exploiter des produits certifiés datant de plus d'un an.

© CIGREF 1992

Cet aspect dépend du caractère concurrentiel ou au contraire monopoliste du marché de l'évaluation et de la certification, de la complexité du produit à évaluer, de la compétence des équipes d'évaluation, de l'industrialisation du processus d'évaluation (outils, méthodes, management de projets), de la maturité des commanditaires dans la définition de leurs cibles, de la nature de la cible (produit/système) et enfin, de difficultés techniques propres à l'évaluation (réévaluation des cibles, composition des résultats d'évaluation, ...).

Enfin, le problème de la reconnaissance mutuelle des certificats de conformité et notamment la position des états non membres de la Communauté (Etats-Unis, ...) conditionnera de toute évidence le développement ou non de l'approche européenne.

© CIGREF 1992

6. Glossaire

Assurance : confiance qui peut être accordée à la sécurité fournie par le produit/système évalué.

Certification : délivrance d'un certificat officiel confirmant les résultats de l'évaluation et l'application des critères retenus.

Cible de sécurité : document de spécification des objectifs, menaces, fonctions et mécanismes de sécurité exigés par le produit/système à évaluer.

Cible d'évaluation (TOE) : produit ou système qui est soumis à une évaluation de sécurité.

Commanditaire : personne ou organisme qui demande une évaluation.

Conformité : adéquation entre la cible de sécurité et le modèle de la cible d'évaluation.

Efficacité : assurance que le produit/système fournit la sécurité réelle ou prévue en exploitation.

Evaluateur : personne ou organisme indépendant qui effectue une évaluation.

Evaluation : estimation d'un produit/système par rapport à des critères d'évaluation définis.

Mécanismes : logique ou algorithme qui implémente une fonction.

Organisme de certification : organisme national indépendant et impartial qui effectue des certifications.

Produit : logiciel et/ou matériel non spécifique.

Système : développement spécifique pour un but particulier et un environnement opérationnel connu.

© CIGREF 1992

7. Annexes

Les annexes comprennent les éléments suivants :

7.1 Informations utilisées dans une analyse de vulnérabilité
7.2 Critères de conformité par niveau
7.3 Exemple d'évaluation de la conformité d'une TOE pour le niveau E1
7.4 Enquête AFNOR - CIGREF - CLUSIF sur les besoins d'évaluation

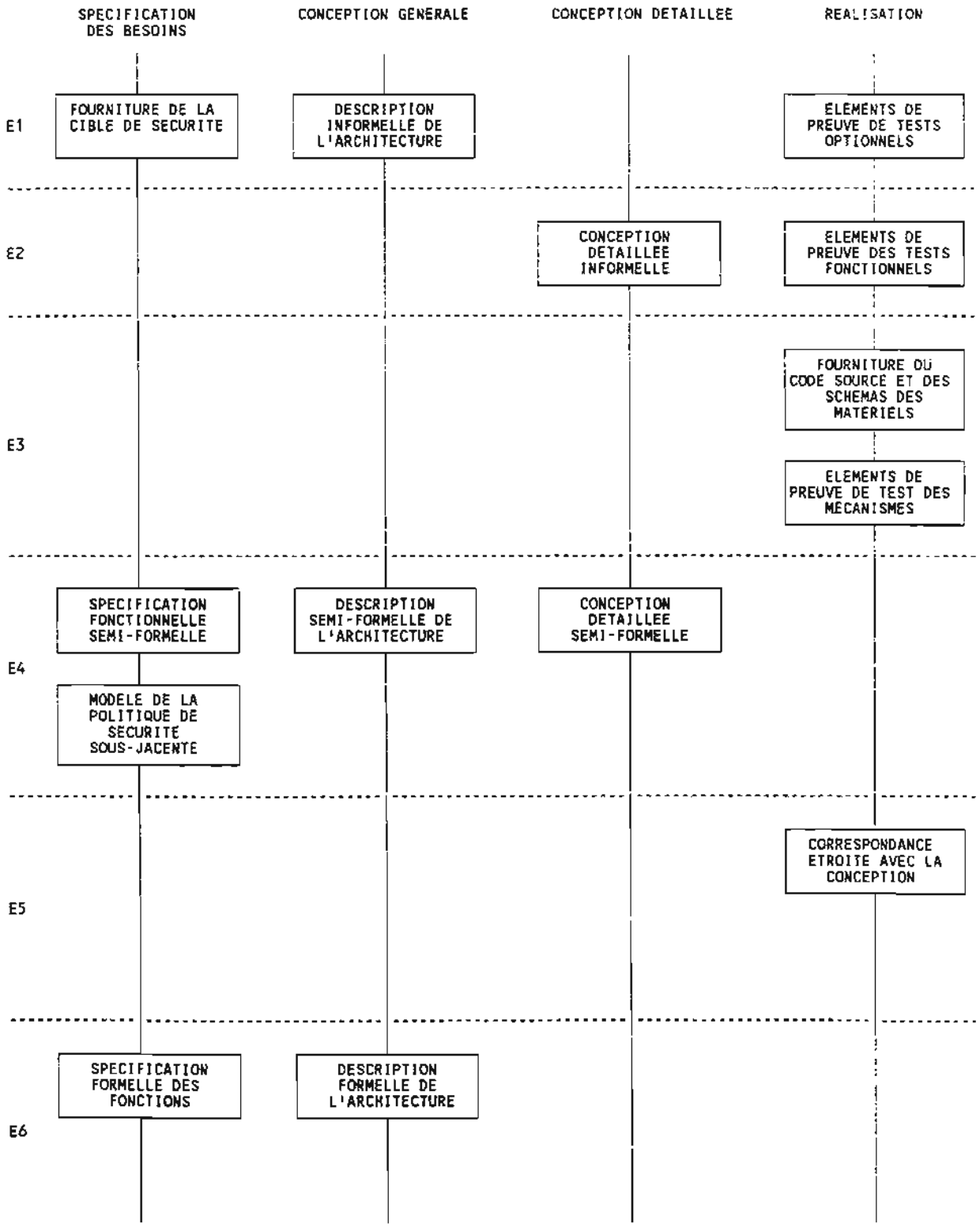
© CIGREF 1992

INFORMATIONS OBTENUES D'UNE ESTIMATION DE LA CONFORMITE UTILISEES POUR EFFECTUER UNE ANALYSE DE VULNERABILITE

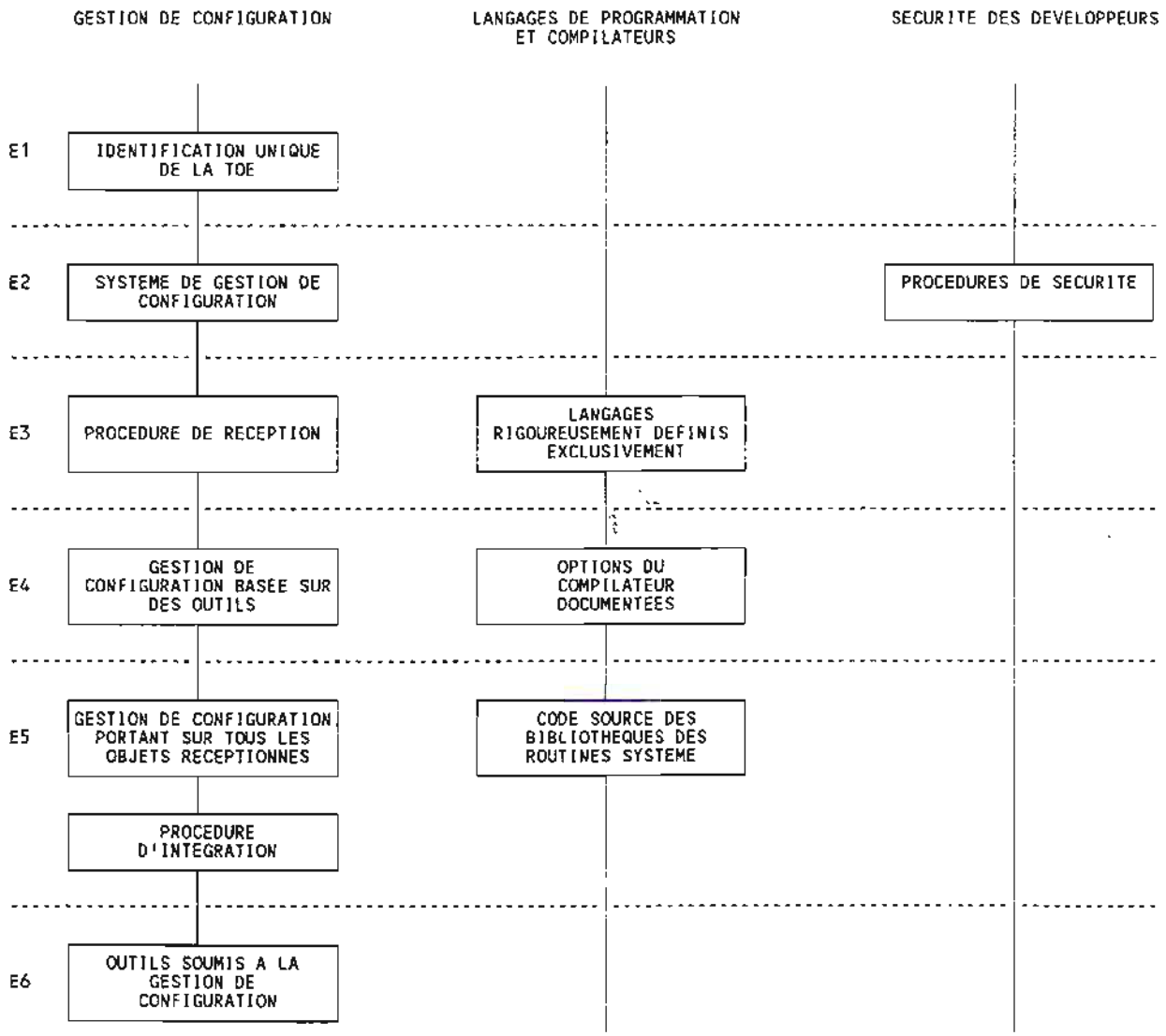
INFORMATION	E1	E2	E3	E4	E5	E6
CIBLE DE SECURITE (menaces, objectifs, fonctions, mécanismes, niveau d'évaluation, résistance des mécanismes)	✓	✓	✓	✓	✓	✓
MODELE FORMEL DE POLITIQUE DE SECURITE				✓	✓	✓
FONCTIONS (informel)	✓	✓	✓	✓	✓	✓
FONCTIONS (semi-formel)				✓	✓	
FONCTIONS (formel)						✓
CONCEPTION GENERALE (informel)	✓	✓	✓			
CONCEPTION GENERALE (semi-formel)				✓	✓	
CONCEPTION GENERALE (formel)						✓
CONCEPTION DETAILLEE (informel)			✓			
CONCEPTION DETAILLEE (semi-formel)				✓	✓	✓
REALISATION (schémas des matériels et code source)				✓	✓	✓
REALISATION (code objet)						✓
EXPLOITATION (documents d'utilisation et d'administration, livraison et configuration, démarrage et exploitation)	✓	✓	✓	✓	✓	✓
	PRESENTER		DECRIRE		EXPLIQUER	

NIVEAU DE RIGUEUR

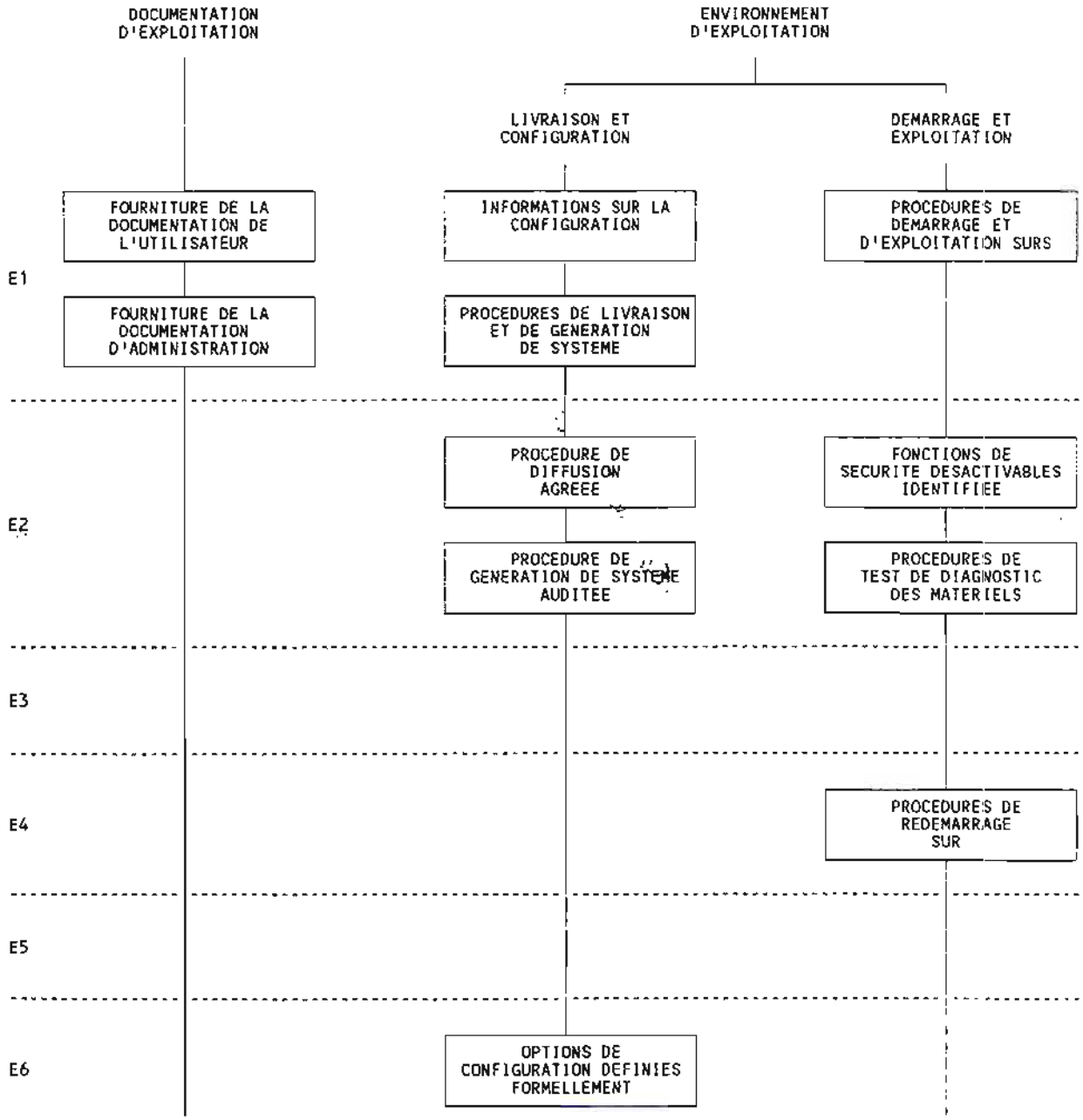
CRITERES DE CONFORMITE PAR NIVEAU - PROCESSUS DE DEVELOPPEMENT



CRITERES DE CONFORMITE PAR NIVEAU - ENVIRONNEMENT DE DEVELOPPEMENT



CRITERES DE CONFORMITE PAR NIVEAU - EXPLOITATION



7.3 Exemple d'évaluation de la conformité d'une TOE pour le niveau E1

NIVEAU E1

Critères concernant le développement ("construction")

- ***Processus de développement*** :

Le commanditaire doit fournir la TOE :

-cible de sécurité
-description informelle de l'architecture de la TOE
-documentation de test (optionnelle)
-bibliothèque des programmes de test et outils de test utilisés (optionnelle).

PHASE 1 - Spécification des besoins

- Définition : fourniture d'une cible de sécurité avec niveau d'évaluation visé et cotation de résistance minimum des mécanismes.

- Exigences de contenu et de présentation : présentation des fonctions de sécurité (style informel). Fourniture du mode d'emploi, de l'environnement d'exploitation, des menaces (produit). Fourniture de la Politique de Sécurité Système (système).

- Exigences probatoires : adéquation de la fonctionnalité à son emploi et aux menaces (produit). Adéquation aux objectifs de sécurité et aux menaces (système).

- Tâches de l'évaluateur : vérifier l'adéquation des informations aux exigences de contenu, de présentation et de preuve. Vérifier la cohérence de la cible.

© CIGREF 1992

PHASE 2 - Conception générale

- Définition : spécification de haut niveau distinguant ce que fait la TOE et comment elle le fait. Séparation entre composants dédiés à la sécurité et autres composants.

- Exigences de contenu et de présentation : présentation de la structure générale de la TOE, des interfaces externes, des matériels et microprogrammes, de la fonctionnalité de sécurité.

- Exigences probatoires : description de la façon dont les fonctionnalités de sécurité sont fournies.

- Tâches de l'évaluateur : cf phase 1.

PHASE 3 - Conception détaillée

- Définition : spécification de composants élémentaires permettant de produire le matériel et/ou le logiciel. Identification les composants dédiés à la sécurité des autres composants.

- Exigences de contenu et de présentation : aucune.

- Exigences probatoires : aucune.

- Tâches de l'évaluateur : aucune.

PHASE 4 - Réalisation

- Définition : programmation ou fabrication des composants élémentaires, tests unitaires, intégration, test d'ensemble de la TOE.

- Exigences de contenu et de présentation : documentation de test (optionnelle) bibliothèque des programmes de test et outils de test utilisés (optionnelle).

- Exigences probatoires : éléments de preuve de tests (optionnelle).

© CIGREF 1992

- Tâches de l'évaluateur : tests des fonctionnalités de sécurité, tests complémentaires pour les erreurs, vérification des résultats des tests du commanditaire.

- ***Environnement de développement***

Le commanditaire doit fournir :

- Liste de configuration identifiant la version de la TOE à évaluer.

ASPECT 1 - Gestion de configuration

- Définition : contrôle des processus de développement, de production et de maintenance.

- Exigences de contenu et de présentation : identification unique du numéro de version.

- Exigences probatoires : présenter comment la TOE est identifiée de façon unique.

- Tâches de l'évaluateur : cf développement phase 1.

ASPECT 2 - Langages de programmation et compilateurs

- Définition : non ambigüe.

- Exigences de contenu et de présentation : aucune.

- Exigences probatoires : aucune.

- Tâches de l'évaluateur : aucune.

© CIGREF 1992

ASPECT 3 - Sécurité des développeurs

- Définition : ensemble des mesures de sécurité physiques, mesures organisationnelles, techniques, de gestion du personnel, etc, garantissant l'intégrité du développement et la confidentialité des informations.

- Exigences de contenu et de présentation : aucune.

- Exigences probatoires : aucune.

- Tâches de l'évaluateur : aucune.

Critères concernant l'exploitation ("exploitation")

- *Documentation d'exploitation*

Le commanditaire doit fournir :

- Documentation utilisateur
- Documentation d'administration

Remarques : la documentation est un élément important . C'est l'un des principaux moyens de dialogue entre le développeur d'une TOE et ses clients.

ASPECT 1 - Documentation utilisateur

- Définition : ensemble des informations fournies par le développeur à l'utilisateur final (ex. : manuels de références, guides de l'utilisateur).

- Exigences de contenu et de présentation : présentation des fonctions dédiées à la sécurité et des conditions d'une exploitation sûre.

- Exigences probatoires : présentation de la manière dont un utilisateur final peut utiliser la TOE de façon sûre.

© CIGREF 1992

- Tâches de l'évaluateur : cf. développement phase 1.

ASPECT 2 - Documentation d'administration

- Définition : ensemble des informations fournies par le développeur à l'administrateur.

- Exigences de contenu et de présentation : présentation des fonctions dédiées à la sécurité, des procédures, responsabilités, conditions d'installation et de configuration, relevant d'un administrateur, distinction fonctions de contrôle des paramètres de sécurité/fonctions d'accès aux informations.

- Exigences probatoires : présentation de la manière dont la TOE peut être administrée d'une façon sûre.

- Tâches de l'évaluateur : cf développement phase 1.

- ***Environnement d'exploitation***

Le commanditaire doit fournir :

- Documentation de livraison et de configuration
- Documentation de démarrage et d'exploitation

ASPECT 1 - Livraison et configuration

- Définition : non ambigüe.

- Exigences concernant les procédures et les normes : présentation de l'impact des différentes configurations sur la sécurité des procédures de livraison et de génération du système.

- Exigences probatoires : présentation de la façon dont les procédures de transfert (configuration, démonstration, ...) maintiennent la sécurité.

© CIGREF 1992

- Tâches de l'évaluateur : cf développement phase 1.

ASPECT 2 - Démarrage et exploitation

- Définition : ensemble des procédures utilisées par l'administrateur pour l'exploitation sûre de la TOE (démarrage, sauvegardes, maintenance, restauration).

- Exigences concernant les procédures et les normes : présentation de la façon dont les procédures assurent un démarrage et une exploitation sûre.

- Exigences probatoires : cf aspect précédent.

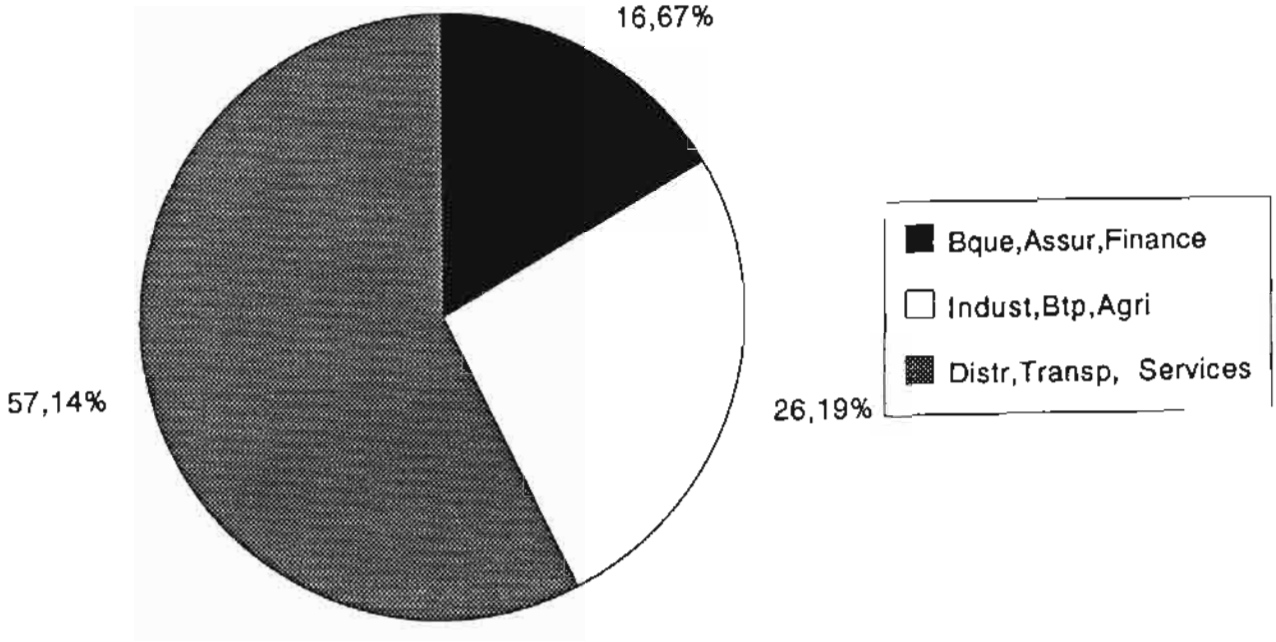
- Tâches de l'évaluateur : cf développement aspect 1.

© CIGREF 1992

ENQUETE

SUR LES CRITERES D'EVALUATION DE LA SECURITE DES SYSTEMES D'INFORMATION

REPARTITION PAR SECTEUR D'ACTIVITE



Q-1

Quelle sont les priorités en matière de sécurité des systèmes d'information dans votre entreprise ?

1 - Organisation de la sécurité

2 - Sensibilisation

3 - Sécurité physique

4 - Elaboration suivi des schémas directeurs

5 - Architecture de sécurité des systèmes et réseaux

6 - Plan et moyens de secours et de sauvegarde

7 - Sécurité logique

8 - Sécurité exploitation

9 - Audit

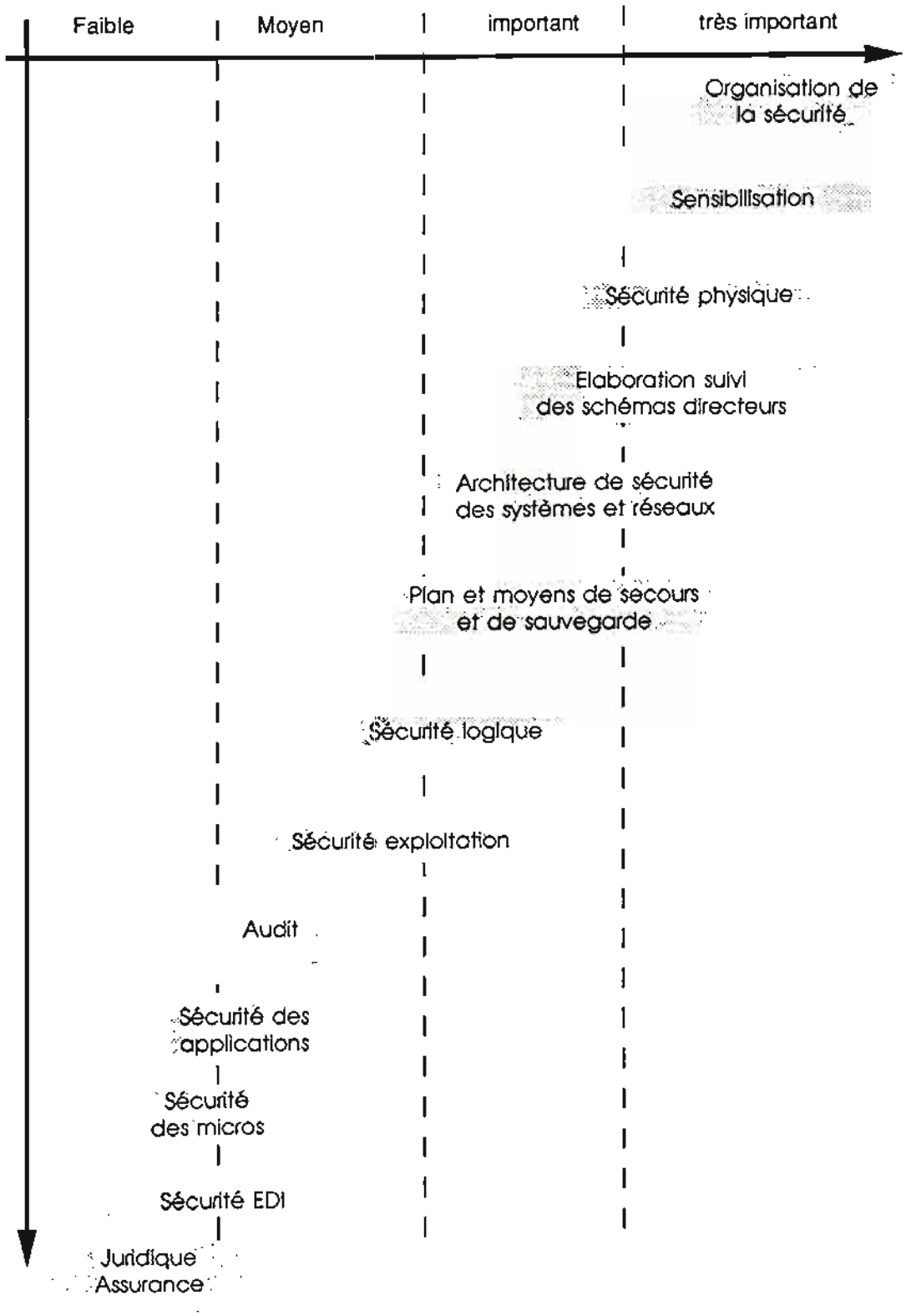
10 - Sécurité des applications

11 - Sécurité des micros

12 - Sécurité EDI

13 - Juridique/Assurance

ESTIMATION GENERALE

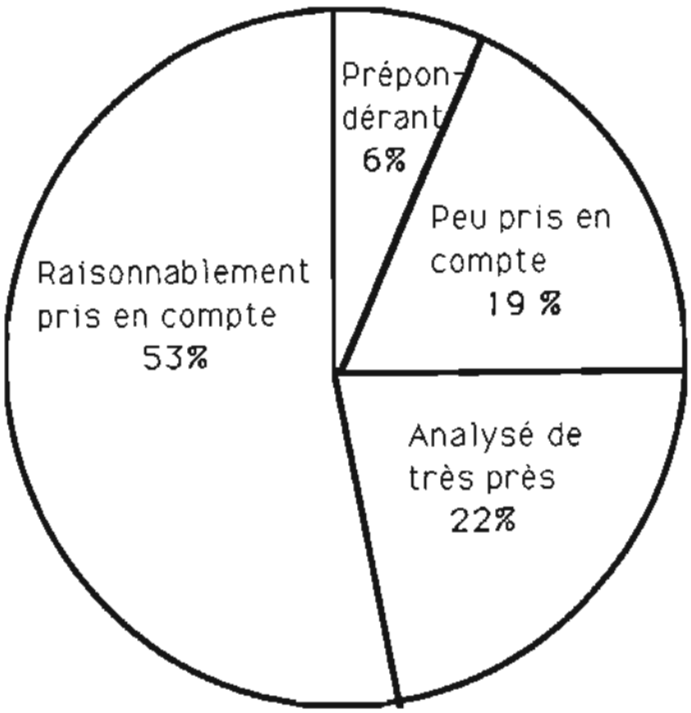


ENQUETE AFNOR - CIGREF - CLUSIF

Sur les critères d'évaluation des systèmes d'information

Q-2

Lorsque vous devez mettre en oeuvre des produits ou des services en informatique et en télécommunication, le niveau de sécurité offert par ceux-ci est-il :

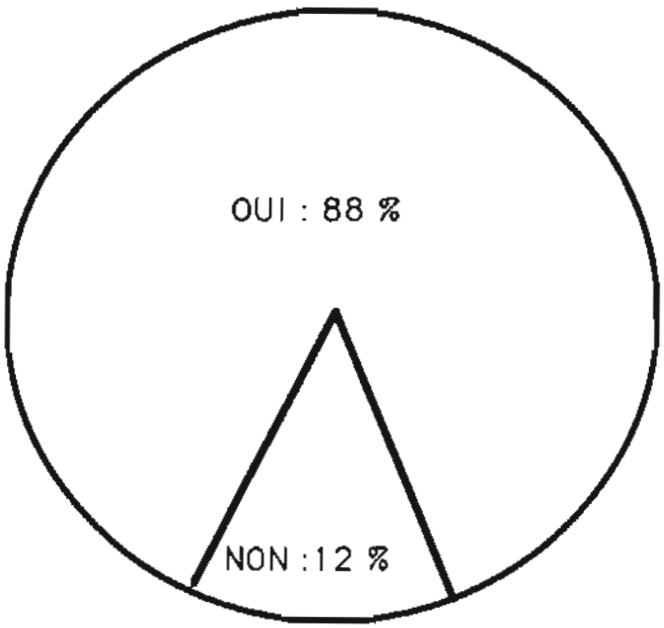


ENQUETE AFNOR - CIGREF - CLUSIF

Sur les critères d'évaluation des systèmes d'information

Q-3

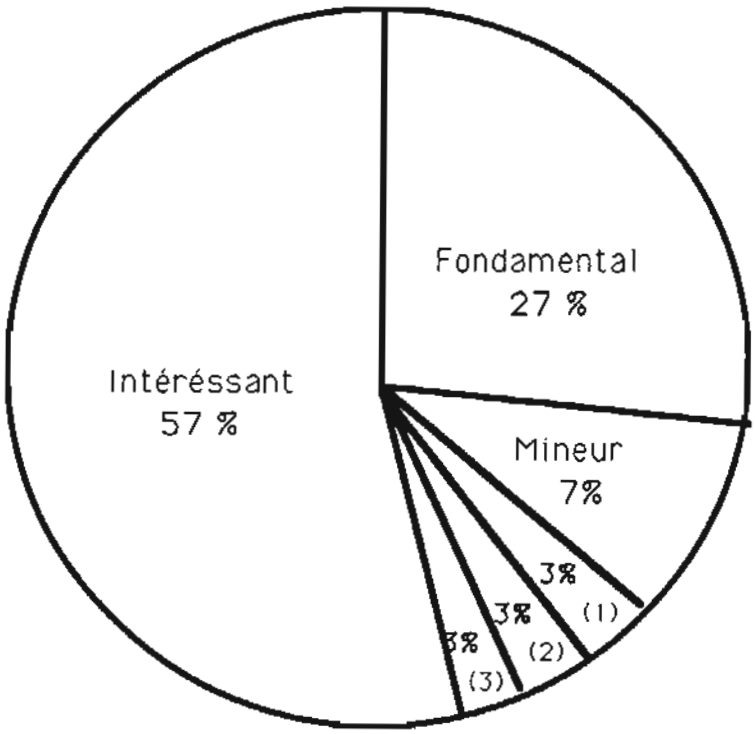
Afin de faciliter la prise en compte de la sécurité dans les
produits
services informatiques
télécommunications
souhaiteriez vous disposer d'un mode STANDARDISE et FORMEL d'expression de vos besoins (sous forme de niveau requis par fonctionnalité) ?



ENQUETE AFNOR - CIGREF - CLUSIF
Sur les critères d'évaluation des systèmes d'information

Q-4

S'il existait des organismes agrées pour certifier le niveau de sécurité offert par les produits et services selon un processus standardisé et formel diriez vous que pour votre entreprise cela serait :

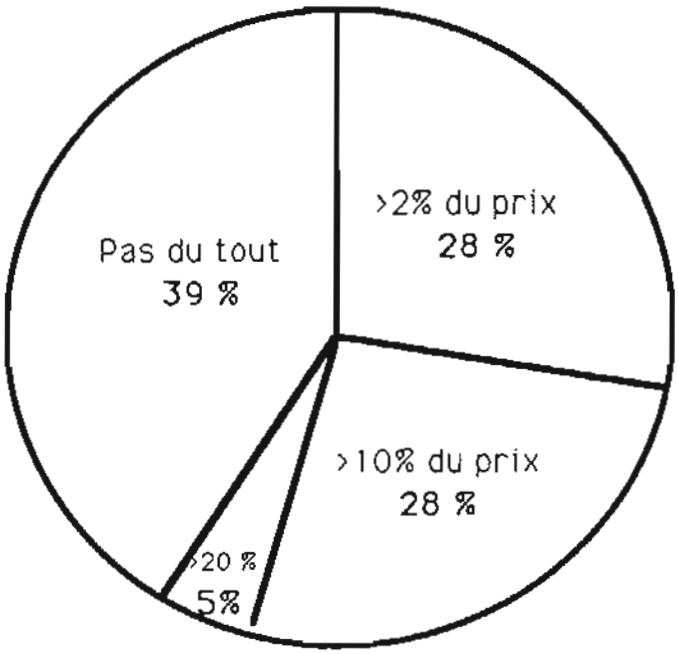


(1) Sans intérêt
(2) Point de départ de la sécurisation du système
(3) certification DOD (Orange Book)

ENQUETE AFNOR - CIGREF - CLUSIF
Sur les critères d'évaluation des systèmes d'information

Q-5

Accepteriez-vous de payer cette certification ?

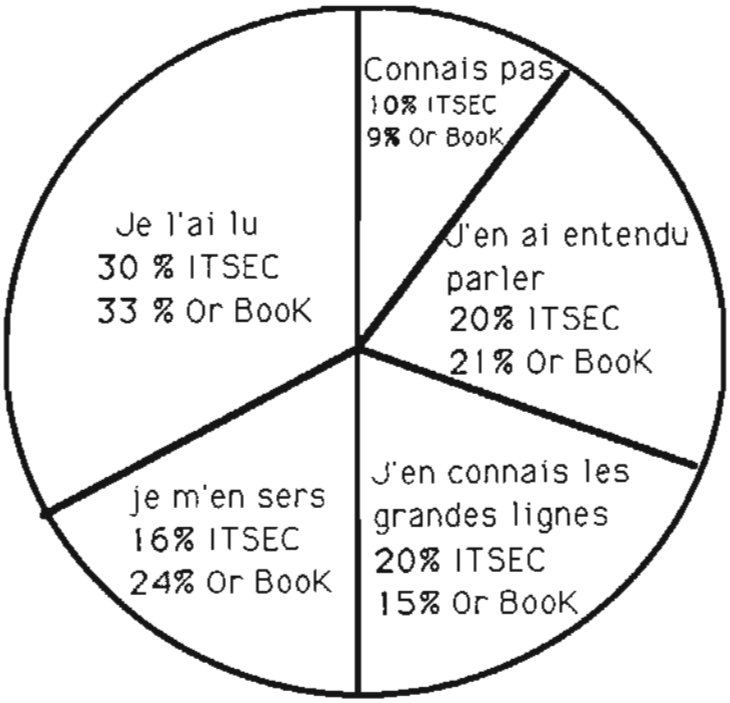


ENQUETE AFNOR - CIGREF - CLUSIF

Sur les critères d'évaluation des systèmes d'information

Q-6

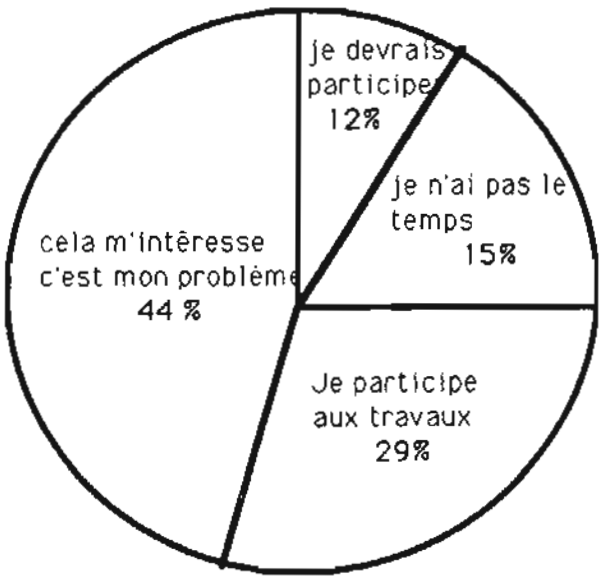
Que savez-vous des systèmes d'évaluation européen
Livre Blanc / ITSEC ?
ou américain
Livre Orange / TCSEC-DOD ?



ENQUETE AFNOR - CIGREF - CLUSIF
Sur les critères d'évaluation des systèmes d'information

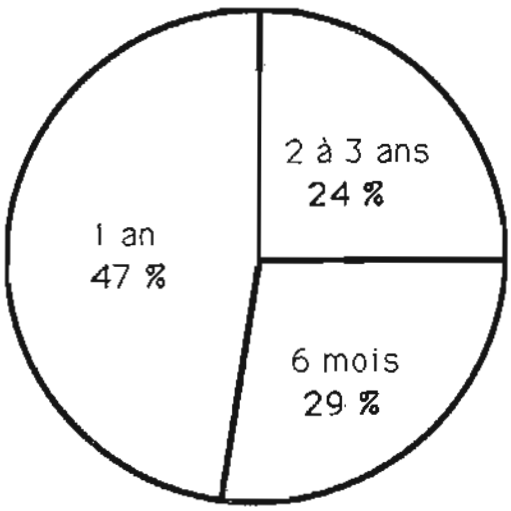
Q-7

Concernant les travaux européens ITSEC, considérez vous :



Q-8

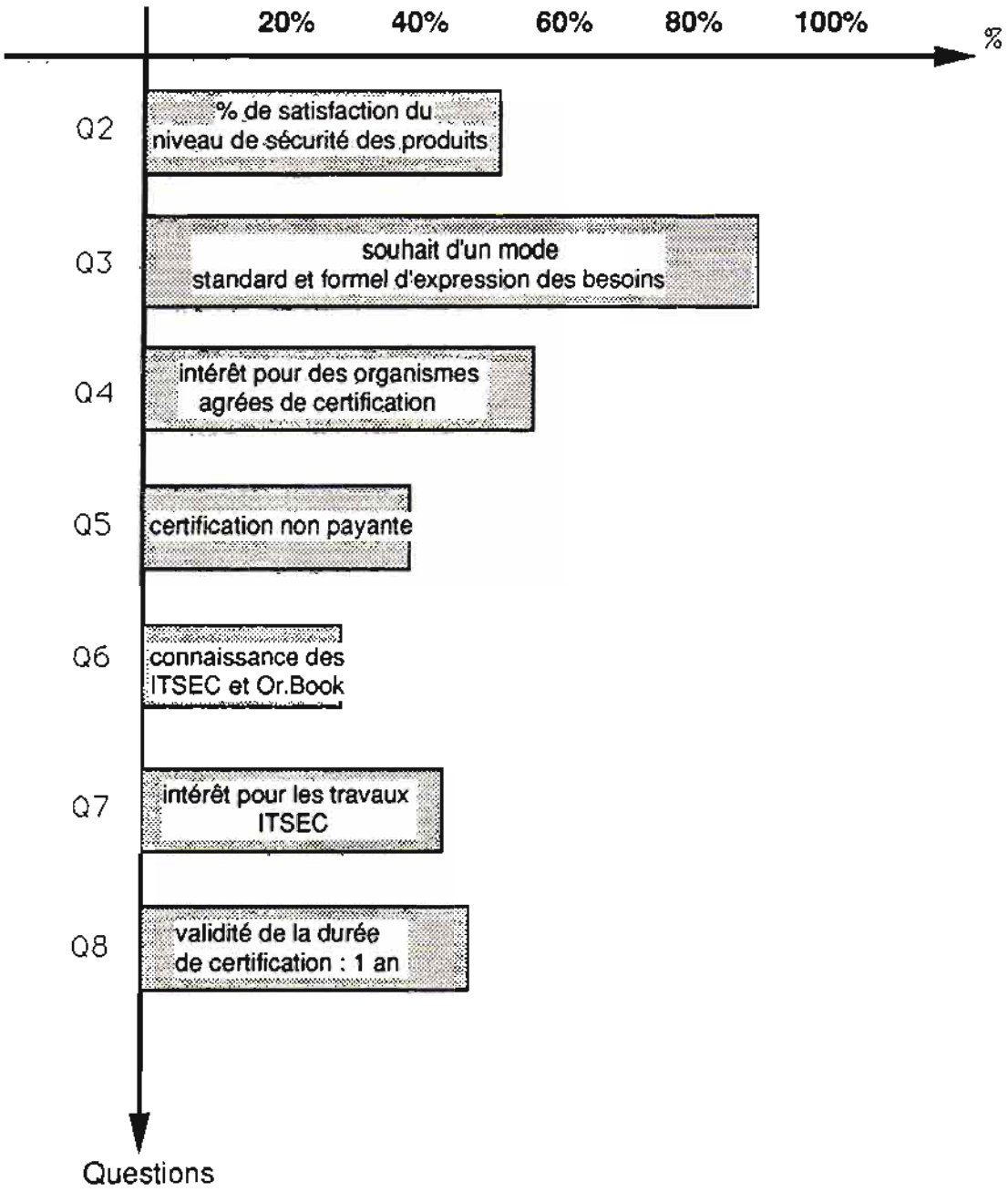
Accepteriez vous d'exploiter des produits certifiés datant de : 6 mois - 1an - 2 à 3 ans ?



ENQUETE AFNOR - CIGREF - CLUSIF

Sur les critères d'évaluation des systèmes d'information

LES TENDANCES PRIORITAIRES



ENQUETE AFNOR - CIGREF - CLUSIF

Sur les critères d'évaluation des systèmes d'information

CRITERES D'EVALUATION

DE LA SECURITE DES

SYSTEMES D'INFORMATION

(ITSEC)

QU'EST-CE QUE LES ITSEC ?

DES CRITERES POUR ASSURER

L'OBJECTIVITE DES EVALUATIONS

ET PERMETTRE LA CERTIFICATION

DE PRODUITS ET DE SYSTEMES

EVALUATION :

ESTIMATION D'UN SYSTEME

OU D'UN PRODUIT

AU REGARD DE CRITERES DEFINIS

CERTIFICATION :

DECLARATION FORMELLE CONFIRMANT LES RESULTATS D'UNE EVALUATION ET L'APPLICATION CORRECTE DES CRITERES D'EVALUATION

POURQUOI LES ITSEC ?

- UNE BASE DE CONFIANCE DANS LA SECURITE DES SYSTEMES ET PRODUITS UTILISES

- UNE BASE POUR LA RECONNAISSANCE MUTUELLE DES RESULTATS DES EVALUATIONS

- UNE BASE POUR COMPARER DES OFFRES CONCURRENTES

- UNE BASE POUR VERIFIER L'ADEQUATION D'UN PRODUIT A SON ENVIRONNEMENT

LES PARTENAIRES

- LE COMMANDITAIRE :

  CONSTRUCTEUR, SSII, REVENDEUR
  UTILISATEUR

  IL COMMANDE, FOURNIT LA
  CIBLE DE SECURITE (OBJECTIFS,
  FONCTIONS, NIVEAU) ET PAYE
  L'EVALUATION

- LE LABORATOIRE D'EVALUATION :

  IL EVALUE LA CIBLE
  D'EVALUATION (TOE)

- L'ORGANISME DE CERTIFICATION :

  IL CONTROLE L'EVALUATION ET
  DELIVRE LE CERTIFICAT

- L'ORGANISME D'ACCREDITATION :

  IL ACCREDITE LE LABORATOIRE
  ET L'ORGANISME DE
  CERTIFICATION

LA CIBLE DE SECURITE

ELLE COMPREND :

- POLITIQUE DE SECURITE DU SYSTEME OU NOTICE DU PRODUIT
- SPECIFICATION DES FONCTIONS DE SECURITE
- FORCE MINIMUM DES MECANISMES
- NIVEAU D'EVALUATION VISE

FONCTIONALITE

- SOUPLESSE DES REFERENCES :

- FONCTIONS SPECIFIQUEMENT DEFINIES
- UTILISATION DE CLASSES PREDEFINIES
- REFERENCE A DES NORMES EXISTANTES

- 3 STYLES DE SPECIFICATION :

  INFORMEL, SEMI-FORMEL, FORMEL

- 3 NIVEAUX D'ABSTRACTION :

  OBJECTIFS, FONCTIONS, MECANISMES

FONCTIONALITE (suite)

TITRES GENERIQUES OU "RUBRIQUES"

- IDENTIFICATION & AUTHENTIFICATION
- CONTROLE D'ACCES
- IMPUTABILITE
- REUTILISATION D'OBJETS
- FIDELITE
- FIABILITE DU SERVICE
- ECHANGE DE DONNEES

ASSURANCE SECURITE

- **EFFICACITE :**

  ESTIMATION DE LA CAPACITE DES FONCTIONS DE SECURITE ET DES MECANISMES A RESISTER A UNE ATTAQUE DIRECTE

- **CONFORMITE :**

  SEPT NIVEAUX D'EVALUATION EXPRIMANT LA CONFORMITE DE L'IMPLEMENTATION DES FONCTIONS ET DES MECANISMES

CRITERES D'EFFICACITE

- PERTINENCE DE LA FONCTIONNALITE
- COHESION DE LA FONCTIONNALITE
- FORCE DES MECANISMES
- ESTIMATION DE LA VULNERABILITE : DEVELOPPEMENT
- FIABILITE D'EMPLOI
- ESTIMATION DE LA VULNERABILITE : EXPLOITATION

CRITERES DE CONFORMITE

1. DEVELOPPEMENT

- PROCESSUS DE DEVELOPPEMENT

4 PHASES :

- EXIGENCES
- CONCEPTION GENERALE
- CONCEPTION DETAILLEE
- REALISATION

- ENVIRONNEMENT DE DEVELOPPEMENT

3 ASPECTS :

- CONTROLE DE CONFIGURATION
- LANGAGES ET COMPILATEURS
- SECURITE DES DEVELOPPEURS

CRITERES DE CONFORMITE (suite)

2. EXPLOITATION

- DOCUMENTATION OPERATIONNELLE

2 ASPECTS :

- DOCUMENTATION UTILISATEUR
- DOCUMENTATION ADMINISTRATEUR

- ENVIRONNEMENT OPERATIONNEL

2 ASPECTS :

- LIVRAISON ET CONFIGURATION
- DEMARRAGE ET EXPLOITATION

SPECIFICATION DE LA CONFORMITE

LES CRITERES SPECIFIENT :

- LA DOCUMENTATION A FOURNIR
- LES EXIGENCES DE CONTENU ET DE PRESENTATION
- LES EXIGENCES PROBATOIRES
- LES TACHES DE L'EVALUATEUR