A.F.C.E.T.

Comité Technique "Sécurité et sûreté informatiques"

GLOSSAIRE DIDACTIQUE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

version 1.2 - octobre 1992

Ph. LASSIRE
G. REBOULET
G. RUGGIU
O. VELIN
K. YAZDANIAN

AFCET
Association française des sciences et technologies de l'information et des systèmes
156, boulevard Péreire
75017 Paris
tél : (1) 47 66 24 19 - Fax : (1) 42 67 93 12

REMERCIEMENTS

Nous remercions les membres du Comité Technique "Sécurité et sûreté informatiques" de l'A.F.C.E.T qui par une lecture attentive et leurs suggestions nous ont permis d'atteindre la version actuelle.

INTRODUCTION ET AVERTISSEMENT

Toute science ou technique qui se développe utilise pour exprimer ses concepts des termes spécifiques nouveaux ou assigne à des mots déjà connus des significations nouvelles. Les disparités qui peuvent exister au départ sont souvent dûes à l'usage des termes par les premiers pionniers, qui selon leur domaine de spécialité, leur ont donné des significations différentes ou nuancées.

La sécurité des systèmes d'information et informatiques n'échappe pas à cette règle. Son développement rapide et récent met l'utilisateur potentiel face à des termes inconnus ou pire équivoques, pouvant même trouver dans différents contextes des significations radicalement différentes.

Soucieux de ce problème, la comission d'étude "Audit" du Comité Technique "Sécurité et sûreté informatiques" de l'A.F.C.E.T. a voulu constituer ce

GLOSSAIRE DIDACTIQUE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Nul doute que son état actuel est imparfait, et surtout incomplet. Il appartient à tous ceux qui, animés de ces mêmes préoccupations, souhaitent apporter une contribution aussi infime soit-elle, de faire parvenir leurs remarques, suggestions et propositions au Comité Technique "Sécurité et sûreté informatiques" de l'A.F.C.E.T.

Qu'ils trouvent d'avance dans ces lignes notre reconnaissance d'avoir aidé à l'élaboration d'un document que nous estimons comme indispensable au monde de la sécurité.

A.

Abus de confiance. Délit ou acte consistant à détourner ou dissiper une chose, remise par la victime à l'auteur du délit en vertu de l'un des contrats énumérés par le texte, à charge, pour le détenteur, de rendre cette chose, de la représenter, ou d'en faire un emploi déterminé. L'abus de confiance comprend principalement le détournement et la dissipation.
Anglais : abuse of trust

Accès. Opération interactive, permettant à une entité de consulter, mettre à jour, stocker les ressources d'un système de traitement de l'information.
Anglais : access.

Accès (contrôle d'). Méthodes et procédures (physiques et logiques) de limitation des droits et possibilités d'accès aux ressources (logiciels, progiciels, fonctions...) d'un centre, ou d'un poste de traitement de l'information, ou d'un objet, aux seules personnes autorisées.
Anglais : access control.

Accès (liste de contrôle d'). Liste qui définit les catégories d'accès accordées ou refusées aux utilisateurs spécifiques d'un objet.
Anglais : access control list.

Accès (mécanismes de contrôle d'). Dispositifs matériels ou logiciels, procédures opérationnelles, procédures de gestion, ou la combinaison de ceux-ci, conçus pour détecter et empêcher les accès inautorisés au système.
Anglais : access control mechanisms

Accès (droits d'). Autorisation accordée à une entité authentifiée d'accéder à un objet pour lire, écrire, créer, compléter, exécuter, transmettre, effacer, modifier... Les droits d'accès (obligatoires ou discrétionnaires) proviennent généralement d'une politique de sécurité ou d'un modèle de sécurité.
Anglais : access right

Accès (matrice d'). Table conceptuelle des droits d'accès, indexée par sujet et objet.
Anglais : access matrix.

Accès (mode d'). Indication pour une action spécifique appliquée à un objet (lire, écrire, exécuter...)
Anglais : access mode.

Accès ("pouvoir" de modifier l'). Autorisation accordée à un usager authentifié de modifier son mode d'accès, ou de le transmettre à un autre usager authentifié.
Anglais : access permission.

Accident. Evénement fortuit, imprévu, extérieur à la victime et indépendant de sa volonté.
Anglais : accident

Accord. (définition à préciser)

Accréditation. Autorisation managériale donnée à une entité pour saisir, traiter, stocker, et transmettre des données sensibles et/ou stratégiques dans un but précis et dans un environnement spécifique.
Approbation d'un système ou réseau informatique autorisant son emploi pour traiter des informations classifiées dans son environnement opérationnel.
Cryptographie. L'accréditation d'un dispositif cryptologique comporte un indicateur permettant de désigner son type (authentification, signature, test), l'identificateur de l'entité, le numéro de série du dispositif sur lequel est préservée l'accréditation

(numéro de série de carte à mémoire). Par exemple, la clé publique RSA de l'entité, le numéro de bi-clé RSA du gestionnaire utilisé pour signer l'accréditation (chiffrement RSA sous la clé secrète du gestionnaire d'une empreinte de l'accréditation, résultat d'une fonction de compression ou de hachage des champs précédents de l'accréditation).
Synonyme : homologation
Anglais : accreditation.

Accréditer. Délivrer une accréditation.
Anglais : accredit (to)

Accréditeur. Autorité qui délivre l'accréditation (autorisation et approbation).
Anglais : accreditation authority

Accréditif. Ensemble de niveaux d'obligatoires de contrôles d'accès à l'ordinateur, aux traitements, aux fichiers et au réseau. L'accréditif reflétera généralement les niveaux sensibles de données évalués par l'accréditeur selon une classification : DIFFUSION RESTREINTE, CONFIDENTIEL, SECRET, TRES SECRET.
Anglais : accreditation range.

Accusé de réception. Action par laquelle le destinataire d'un message signifie à son émetteur qu'il a bien reçu le message et qu'il l'accepte.
En le protocole ETBAC/5 ce peut être, par exemple avec le RSA, sous la clé secrète de son émetteur, de la concaténation des éléments caractéristiques du fichier reçu, des date et heure d'acquittement et d'un champ d'acquittement rendant compte des contrôles de sécurité effectués.
Anglais : acknowledgement

Administration de la sécurité. Elle consiste à définir les responsabilités en matière de sécurité et les structures organisationnelles nécessaires à :

- la coordination de la mise en oeuvre des mesures de protection des ressources,
- la mise à jour des habilitations,
- la surveillance permanente du fonctionnement.

Anglais : security management

Agrément. Reconnaissance officielle de l'aptitude d'un dispositif de sécurité (cryptologique, TEMPEST ou informatique) ou d'un algorithme cryptologique à satisfaire un ensemble de spécifications techniques et contraintes d'exploitation. Au cours du développement d'un dispositif ou d'un algorithme, un agrément de principe peut être prononcé au vu d'une première évaluation. Cet agrément de principe vaut accord pour la poursuite du développement.

Agression. Attaque délibérée contre des biens et/ou des personnes.
Anglais : attack

Algorithme. Ensemble fini de règles déterminées servant à résoudre un problème au moyen d'un nombre fini d'opérations.
Anglais : algorithm

Algorithme de chiffrement de données. Transformation mathématique qui, associée à une clé secrète, fournit un résultat lorsqu'elle est appliquée à une donnée. Ce résultat est utilisé dans les opérations de sécurité (authentification, confidentialité, intégrité, signature, calcul de la clé de chiffrement). Les principaux algorithmes sont : RSA, DES, DEA .
Anglais : Data Encryption Algorithm (DEA).

Allocation de clé. Opération de remise des clefs, par le responsable de sécurité, aux différents utilisateurs
Anglais : key allocation

Alphabet cryptographique. Ensemble de lettres permettant de représenter les messages du système cryptographique
Anglais : cryptographic alphabet

Analyse de contre-mesures. cf contre-mesure (analyse de)

Analyse cryptologique. cf cryptanalyse

Analyse des fautes de sécurité. cf fautes de sécurité

Analyse du flot de sécurité. cf flot de sécurité

Analyse des menaces. cf menaces

Analyse des ressources. cf ressources

Analyse de risque. cf risque

Analyse de trafic. cf trafic

Application ou applicatif : Alors que l'on associe au mot projet la qualité de l'objet de l'étude, l'application est l'entité immatérielle à laquelle s'applique le résultat de l'étude. Elle se compose de l'ensemble des moyens en ordre de marche, assurant une fonctionnalité complète à un sous-ensemble de l'activité de l'entreprise ou du service public considérés.
L'application apparaît donc comme l'unité de mise en oeuvre de l'amélioration projetée.
Exemples d'applications gestion des commandes clients, facturation, comptabilité.
Anglais : application

Approbation. Reconnaissance officielle de l'aptitude d'un dispositif de sécurité (cryptologique, TEMPEST ou informatique) à satisfaire le besoin d'un système d'information et à être conforme avec la politique de sécurité définie dans le plan de sécurité du dit système. L'approbation d'un dispositif de sécurité est prononcée au vu des résultats d'une certification, menée par une équipe de certification indépendante des services ayant développé le dispositif.
Anglais : approval

Approche du risque. Celle-ci repose sur la connaissance et l'expérience des experts de l'application. Plusieurs critères peuvent être retenus :

- l'antériorité (connaissance des incidents et des problèmes survenus)
- l'appréciation du risque (montant des pertes consécutives au sinistre évaluées quantitativement et qualitativement)

Approche de vérification. A l'aide de moyens indépendants, a pour objectif de vérifier l'existence, la propriété et l'estimation des biens ou actifs de l'entreprise.
Anglais : verification approach

Arbitrage. Règlement d'une controverse en s'en remettant à un tiers. Celui-ci peut prendre part à une procédure corrigeant le litige, comme celle de production et de vérification d'une signature d'arbitrage.
Anglais : arbitration

Architecture de sécurité. Sous-ensemble du plan informatique décrivant la sécurité des systèmes d'information et informatiques.
Anglais : security architecture.

Architecture de sécurité d'un réseau. Sous-ensemble du plan télécoms qui définit la pertinence des services et des mécanismes de sécurité du réseau à mettre en place. L'OSI a établi un modèle de référence dans ce domaine.
Anglais : network security architecture

Archivage. Stockage de fichiers et de journaux associés à ces fichiers, généralement pour une période déterminée et pour consultation ultérieure. L'archivage doit conserver les logiciels nécessaires pour l'utilisation de ces fichiers et de ces journaux.
Anglais : file archiving

Artères de communication. Le moyen physique de connecter un poste à un autre pour transmettre ou recevoir des données.
Anglais : communication paths, communication channels, communication links

Assurance. L'assurance est une opération par laquelle l'assureur garantit à l'assuré, moyennant le paiement d'une rémunération appelée prime, le versement d'une prestation, en cas de la réalisation d'un risque. Elle est fondée sur le calcul des probabilités et la statistique.
L'assuré demande à l'assureur de le prémunir contre les conséquences financières d'un hasard défavorable.
ITSEC : Confiance qui être accordée à la sécurité fournie par une cible d'évaluation.
Anglais : insurance - assurance (ITSEC)

Assuré. Personne physique ou morale bénéficiant de garanties d'assurances.

Atténuation de la vulnérabilité (MELISA). Limitation des possibilités d'occurrence et des conséquences effectives des faits redoutés, par la mise en oeuvre de moyens de protection ou de prévention, appelés parades. La méthode MELISA met en jeu des coefficients d'atténuation dans la cotation de la vulnérabilité.

Attributs de la sécurité informatique. Caractéristiques de la sécurité informatique définis en termes de :

- besoins de sécurité : intégrité, confidentialité, disponibilité, (fiabilité, sauvegardes, backup, assurance...), cohérence (fonctionnelle, opérationnelle et socio-légales), auditabilité, possibilités de contrôle et de preuve.
- mesures et outils de protection : habilitation, accréditation, identification, authentification, autorisation, accusé de réception, acceptation obligatoire (non-répudiation), notarisation, comptabilisation, journalisation, facturation, chiffrement, scellement, signature, routage.

Anglais : security attributs

Attributs de la sûreté de fonctionnement (Sûreté de Fonctionnement) Attributs permettant a) d'exprimer les propriétés qui sont attendues du système et b) d'apprécier la qualité du service délivré, telle que résultant des entraves et des moyens de s'y opposer. Fiabilité, maintenabilité, disponibilité, sécurité-innocuité, sécurité-confidentialité.
Anglais : Attributes of dependability

Audit de sécurité des systèmes d'information et informatiques. Intervention d'évaluation, d'analyse et de diagnostic de la sécurité de l'organisation et de la gestion de ces systèmes, qui prend en compte les éléments essentiels que l'on trouve dans une étude de risques :

- Taxonomie des biens et ressources stratégiques et/ou sensibles de l'entreprise, ainsi que des contrôles et protections y afférents.
- Identification des menaces pesant sur ces biens et ressources.
- Evaluation des conséquences de la survenance de ces menaces en terme d'analyse de risques avec degré d'acceptabilité de ceux-ci.
- Définition des objectifs de sécurité de l'entreprise.
- Proposition d'un plan de mise en place des méthodes et techniques de protection et de contrôle.
- Evaluation du coût de la mise en place de ce plan.

Auditer implique donc un système de référence, constitué par la description du management de la sécurité des systèmes d'information et informatiques tel qu'il devrait être.
Anglais : audit

Authentifiant. Processus permettant de valider un message. En cryptographie, il est calculé en fonction du contenu d'un message et d'une clé secrète et, envoyé avec le message. Ceci permet au récepteur de détecter d'éventuelles modifications du message par un émetteur douteux. MAC (message authentification code) est un authentifiant.
Exemple :
Algorithme (DES en mode authentifiant.) K
Message de transaction M
Authentifiant MAC = G (M, K)
Message transmis MAC + M, ou G M
Anglais : authenticator

Authentification. Procédure conventionnelle permettant de s'assurer de la qualité d'une entité à partir d'une caractéristique physique spécifique de celle-ci ou d'un élément supposé détenu ou connu de cette seule entité.
Garantie apportée à une information d'identification : mot de passe, signature d'un message aléatoire.
1°) - Procédure qui vérifie que le message émis est authentique. C'est-à-dire qu'il est reçu tel qu'il a été envoyé et qu'il vient bien de la source prévue.
2°) - Procédure qui valide l'identité d'une entité telle qu'une personne, un terminal éloigné, ou l'émetteur du message
L'authentification est requise afin de valider l'échange d'accréditations qui permettent d'identifier de façon formelle les partenaires mis en relation lors d'un transfert dont elle constitue la première étape. Ces accréditations sont préalablement fournies par un gestionnaires lors de la personnalisation des dispositifs de sécurité (carte à mémoire).
Anglais : authentication.

Authentification d'entité (mécanismes d'). ISO/AFNOR : Les mécanismes d'authentification d'entité permettent la vérification de l'identité déclarée, par une autre entité.
L'authenticité de l'entité ne peut être assurée que pendant la durée de l'échange d'authentification. Pour garantir l'authenticité de données communiquées par la suite, l'échange d'authentification doit être utilisé conjointement avec un moyen de communication sûr (par exemple un service d'intégrité).
Un usurpateur d'identité peut rejouer, à une date ultérieure, un échange d'authentification valide (il s'agit là d'une forme de déguisement). Pour éviter un tel rejeu, on peut utiliser un paramètre variable dans le temps comme par exemple un horodateur, un numéro d'ordre ou une question (défi).
En règle générale, à des fins d'authentication, les entités génèrent et échangent des messages normalisés appelés jetons. Il faut procéder à l'échange d'au moins un jeton pour que l'une des entités soit authentifiée par l'autre entité et l'échange d'au moins deux jetons pour une authentification réciproque. Un jeton supplémentaire peut s'avérer nécessaire dans le cas où une question (défi) doit être envoyée pour engager l'échange d'authentification. L'authentification unilatérale offre à une entité l'assurance de l'identité de l'autre entité mais l'inverse ou la réciproque n'est pas vraie. L'authentification mutuelle fournit à chacune des deux entités l'assurance de l'identité de l'autre.
Les mécanismes d'authentification les plus souvent utilisés sont généralement inspirés du projet de norme ISO DP 10117 à savoir l'utilisation de l'algorithme RSA (DP9796) et peuvent s'appliquer selon deux types :

- l'authentification simple basée sur un échange d'accréditations entre deux partenaires,
- l'authentification réciproque basée sur l'échange des mêmes accréditations plus celui d'aléas signés par les deux partenaires.

Anglais : entity authentication mechanisms

Autorisation. Droit ou pouvoir accordé par une entité habilitée à un usager pour accomplir une action. L'autorisation consiste à accorder ou à refuser à l'usager un certain nombre de privilèges ou droits envers le système. Ceux-ci sont prédéfinis et dépendent de l'identité de l'usager.
Terme souvent utilisé pour désigner la fonction de contrôle d'accès logique.
Anglais : authorization

Autrui, tiers. Toute personne physique ou morale autre que l'assuré et ses préposés rémunérés ou non dans l'exercice de leur fonction. Sont notamment considérés comme autrui ou tiers, les clients de l'assuré.

Avis. Recommendation exprimée par un organisme officiel. Exemple : les avis de CCITT,...

B.

Back-up. cf secours

Banque de données. Une banque de données est une collection, un archivage d'informations primaires (livres, articles, documents visuels ou sonores, statistiques...) directement exploitables, généralement structurés en bases de données et recouvrant un domaine de connaissance.
Les banques de données sont généralement constituées et maintenues par des institutions spécifiques, des organismes publics ou d'associations professionnelles, qui en sont alors les producteurs.
Enfin, il faut signaler l'apparition de courtiers (brokers) en données qui jouent le rôle d'intermédiaires entre le serveur et l'utilisateur final.
Anglais : Data Bank

Barrière. Elément, dispositif ou procédure destiné à interrompre ou modifier le scénario d'un accident ou d'une agression de façon à en réduire la probabilité ou la gravité
Selon la norme NF X 40 001 Système extérieur qui protège les objets contre la détérioration par les "agents d'attaque" (cette définition ne convient pas à la terminologie "sécurité des systèmes").

Base de confiance d'un réseau informatique. Totalité des mécanismes de protection nécessaires à l'exécution de la politique de sécurité prévue par le réseau.
Anglais : trusted network base (TNB)

Base de confiance d'un système informatique. Totalité des mécanismes de protection d'un système comprenant matériel, logiciel, microprogrammation - L'entité qui est chargée de la mise en vigueur d'une politique de sécurité. Elle crée un environnement de protection de base et fournit, à l'utilisateur, des services supplémentaires exigés par le système informatique de confiance. L'aptitude d'une base de confiance à correctement mettre en vigueur une politique de sécurité dépend uniquement des mécanismes du TCB et de l'entrée correcte, par le personnel, des paramètres conformes à la politique de sécurité.
Anglais : Trusted computing base (TCB)

Base de connaissances. Ensemble d'informations représentant l'état des connaissances acquises dans un domaine donné.
Anglais : knowledge base

Base de connaissances (MELISA). Cette base de connaissances comprend la typologie des faits redoutés (menaces types et événements), les moyens de prévention, de détection, de correction et de protection (parades), les liens entre ces deux sous-ensembles (références croisées) et coefficients d'atténuation), les commentaires et explications, ainsi que les éléments de coûts.
Anglais : Knowledge base

Base de données. Ensemble d'informations exhaustives et généralement non redondantes nécessaires à une série d'applications automatisées et exploitées à travers par un système de gestion de base de données (SGBD) qui en assure la gestion. Les informations d'une base de données satisfont les 3 caractéristiques suivantes :

- Indépendancelogique (vis-à-vis des utilisateurs).
- Indépendance physique (vis-à-vis des matériels.
  Non-redondance sémantique des données

La conception d'une base de données (database design) est un processus, qui à partir de l'observation d'une situation réelle, aboutit à la définition de la base de données correspondante
Ce processus peut être décomposé en plusieurs étapes :

- Délimitation, dans le monde réel observé, des éléments qui présentent un intérêt pour la situation que l'on cherche à représenter ;
- Agrégation des éléments retenus en un ensemble structuré ; cette opération présuppose le choix d'un certain modèle de données ;
- Expression de la structure retenue à l'aide d'un langage de description ou de définition de données (data description language); on obtient ainsi une description de la base de données qui peut être communiquée à autrui ; le langage dépend du modèle de données utilisé, mais pour un même modèle il peut exister plusieurs langages ;
- Vérification que la description ainsi élaborée correspond bien aux besoins des applications (dans le cas où il n'en est pas ainsi, itération du processus de conception).

Le modèle de données (data model) est un ensemble de concepts et de leurs règles d'utilisation au moyen desquels on peut structurer un ensemble de données.
Anglais : Database

Bell-La Paluda (modèle formel de politique de sécurité). Il modélise les exigences de contrôle d'accès caractérisant une politique nationale de sécurité à l'aide d'un modèle basé sur le concept du moniteur de références et d'une politique de sécurité multiniveau de confidentialité.
Anglais : Bell La Paluda model

Biens informatiques. L'appellation biens informatiques désigne l'ensemble des actifs gérés par l'informatique dont on veut assurer la sécurité.
On dénombre des biens physiques (locaux, matériels informatiques) et informationnels (données, programmes).
Anglais : EDP assets

Bloc. Ensemble d'instructions et de déclarations compris entre deux délimiteurs (en général début et fin).
Anglais : Block

Boîte noire. Dispositif ou programme de sécurité conçu pour n'être compréhensible et modifiable que par son auteur ou ses ayant-droits
Anglais : Black box

Bombe logique. Une bombe logique est un programme contenant une fonction malveillante généralement associée à un déclenchement différé. Exemple réel de bombe logique : un programmeur, prévoyant son licenciement, insère dans un programme de paie une fonction de reformatage des disques durs dont l'exécution est déclenchée si son nom disparait du fichier personnel.
Anglais : Software bomb

Brewer-Nash. (modèle formel de politique de sécurité). Il modélise les exigences de contrôle d'accès visant à assurer la confidentialité pour le client, ce qui est typique de certains organismes financiers.

C.

Cage de Faraday. Enceinte (pièce ou container) spécialement conçue pour atténuer les effets des radiations électromagnétiques.
Anglais : Shielded enclosure

CAM (MARION). Comité d'Application de la Méthode constitué d'un groupe polyvalent (multi-compétences) interne à l'entreprise.

Canal. - 1° Moyen matériel ou organique de la transmission d'un message, d'une information. Ensemble des moyens de transmission d'un signal de son lieu d'émission à son lieu de réception.
- 2° Processeur d'entrée/sortie mettant en relation la mémoire d'un ordinateur et un ou plusieurs organes périphériques.
Anglais : Channel

Canal caché. Moyen de transmission d'un message ou d'une information qui n'utilise pas les mécanismes officiellement destinés à la transmission

Capacité. Quantité maximale d'informations que peut traiter ou contenir un équipement informatique.
MARION : perte maximale que l'entreprise pourrait subir sans mettre en péril sa survie (capacité financière) ou ses objectifs (capacité objective).
Anglais : Capacity - sert parfois à traduire le terme anglais "capability" (liste de droits).

Captation. Manoeuvre répréhensible en vue de déterminer une personne à consentir une libéralité.

Carte a mémoire. Carte embossée en chlorure de polyvinyle ou équivalent dont les dimensions standard sont 85,6 x 54 mm et dans laquelle est encastré un support de mémorisation d'informations numériques. A cette définition répondent plusieurs types de cartes :

- La carte à piste magnétique, qui porte des bandes magnétiques d'une capacité de quelques kilobits, très répandues comme carte de crédit.
- La carte à microprocesseur (ou carte à puce) contenant des mémoires (ROM, EPROM ou EEPROM, jusqu'à plusieurs kilo-octets, RAM pour les besoins du microprocesseur), les circuits ALU du processeur, un algorithme de sécurité, et qui est capable de dialoguer avec un terminal (TPE, TPV, GAB, lecteur de cartes...). Le microprocesseur sous l'action d'un programme, appelé aussi masque assure :
  - la communication avec le monde extérieur via un protocole normalisé (ISO 7816-3)
  - la gestion de la mémoire, sa structuration et son exploitation en contrôlant les accès (écriture, lecture, mise à jour) aux données en fonction des choix de l'application (accès libre, présentation de PIN code, authentification,...)
  - la mise en œuvre d'algorithme cryptographique utilisant des données secrètes de la carte (le microprocesseur en interdisant la communication vers l'extérieur)
- La carte optique pour enregistrement holographique (quelques kilobits) ou laser (quelques mégabits)

Dans les cas d'authentification, de signature et de calcul de clé de chiffrement, le microprocesseur exécute l'algorithme de sécurité.
Anglais : Active card, smart card, chip card, micro-circuit card.

Carte fille. Carte détenue par le porteur, contient l'algorithme de sécurité et au moins une clé secrète spécifique.

Carte mère. Composant électronique qui contient d'une part l'algorithme de sécurité et d'autre part la méthode de calcul des clés contenues dans les cartes détenues par les porteurs (cartes filles). Elle contrôle l'exactitude des résultats fournis par les cartes filles dans les opérations d'authentification, de signature. Elle permet ainsi d'authentifier une carte fille présentée par un porteur.

Cas. Se dit de tout fait qui est arrivé ou qui peut arriver.

Casseur. Personne inautorisée s'introduisant dans un système informatique pour y effacer ou modifier les données des fichiers.
Anglais : Cracker

Catégorie d'accès. Classe d'autorisation d'accès donnée à des utilisateurs, programmes et traitements pour leur affecter des ressources ou des groupes de ressources.
Anglais : Access category

Catégorie d'usager. Désigne les différents types d'intervenants d'une application opérationnelle :

- la production informatique (système, exploitants, réseau, Infocentre..),
- les gestionnaires de l'application,
- les études,
- les utilisateurs internes,
- les utilisateurs externes.

Dans chaque catégorie, on sera conduit à distinguer un ou plusieurs un plusieurs groupes d'usagers ayant les mêmes droits sur les mêmes ressources.

Causalité. Modèle formel pour la sécurité développé en France (CERT/ONERA)

Cause. Les causes sont des événements ou circonstances qui affectent défavorablement la gestion. Evénement antécédent, action qui a un effet. Les contrôles, causes, effets, conséquences et risques font partie des éléments de l'analyse de risques.
Anglais : Cause

Centralité (d'un poste). Point nodal ou position centrale d'un poste dans un réseau.

Centralité (indice de). Evaluation d'un poste par rapport au poste central en ce qui concerne l'accès aux informations, le pouvoir de décision et le degré d'autonomie dans un réseau de communications. Résultat d'un calcul (Bavelas): l'indice de centralité d'un poste est égal à la somme de toutes les distances divisée par la somme des distances pour le poste considéré ; l'indice de centralité d'un réseau est la somme des indices de centralité des postes qu'il comporte.

Centre de distribution des clefs. Programme qui génère et distribue des variables cryptographiques.
Anglais : Key distribution center

Certification. Engagement personnel sur la portée d'une information, généralement réalisé par la transmission d'un mot de passe. Processus qui regroupe les notions de scellement et de signature. Le scellement contrôle que le message est identique au message de départ et que le fichier reçu est identique au fichier écrit. La signature contrôle qu'un message ou une donnée a bien été émise par l'émetteur attendu.
Délivrance d'un document officiel fondé sur un examen indépendant de la conduite et des résultats d'une évaluation et indiquant dans quelle mesure :

- un système ou réseau informatique répond à l'exigence de sécurité convenue avec l'autorité d'homologation

- un produit COMPUSEC répond à des impératifs de sécurité préalablement définis.

Anglais : Certification

Certificat de conformité. Document délivré conformément aux règles d'un système de certification, indiquant avec un niveau suffisant de confiance qu'un produit, un processus, ou un service dûment identifiés restent conformes à une norme ou à un autre document normatif spécifié.

Certification de conformité. Acte par lequel une tierce partie témoigne qu'il est raisonnablement fondé de s'attendre à ce qu'un produit, un processus, ou un service dûment identifiés soient conformes à une norme ou à un autre document normatif spécifié.

Certification TEMPEST. Certification de conformité accordée à un équipement électrique ou électronique, fabriqué selon les normes d'anti-compromission préconisées par un laboratoire officiel. Les résultats de la série tests effectués garantissant que l'équipement ne radie, ni n'émane de signaux compromettants, directement ou indirectement.
Anglais : TEMPEST Certification

CESSI. Commission d'Evaluation de la Sécurité des Systèmes d'Information (MELISA). Elle est formée de personnel interne représentant les fonctions concernées de l'entreprise (responsables du fonctionnement et utilisateurs du système d'information).

Chaîne. Type de réseau de communication où les postes sont égrenés en relais le long d'une ligne de communication entre deux postes situés aux deux extrémités.

Chemin de confiance. Mécanisme qui permet à un opérateur privilégié d'une station de travail de communiquer avec la base de confiance informatique (TCB).
Anglais : Trusted path

Chemin critique. Enchaînement de processus sécurisés appartenant à une (ou plusieurs) section critique.
Anglais : Critical path

Cheval de Troie . A l'image de son homologue grec, un cheval de Troie informatique est un programme en apparence inoffensif contenant une fonction illicite cachée. Cette fonction est utilisée notamment pour pénétrer par effraction dans l'ordinateur et consulter, modifier ou détruire des informations. Exemple réel de cheval de Troie : le programme STRIPES.EXE sous MS/DOS affiche à l'écran un drapeau américain. Pendant cette opération la fonction illicite tente de copier les mots de passe présent sur l'ordinateur.
Anglais : Trojan horse

Chiffre-clé. Résultat d'un calcul portant sur les chiffres (ou les caractères) composant un code (numérique ou non) pour permettre une vérification automatique lors de la saisie de ce code.

Chiffrement. Le chiffrement consiste à transformer un texte en clair en un cryptogramme (texte inintelligible, en utilisant des moyens de cryptographie, un algorithme et une clé. L'opération inverse s'appelle le déchiffrement. La méthode applique un algorithme aux lettres et aux chiffres d'un texte en clair. Une distinction est faite entre chiffrement et codage. Ce dernier utilise un dictionnaire de codes au lieu d'un algorithme. Le chiffrement peut être irréversible, auquel cas le déchiffrement correspondant est impossible.
Anglais : Ciphering, encipherment, encryption.

Chiffrement de bout en bout. Chiffrement d'informations au niveau du système émetteur, le déchiffrement s'effectuant au niveau du système destinataire.
Anglais : End-to-end encipherment

Chiffrement de voie. Chiffrement des informations transitant sur chaque liaison du système de communication.
Anglais : Link by link encipherment

Cible : Etat futur de l'organisme que l'on souhaite atteindre. Cet état futur peut être caractérisé par plusieurs niveaux de description :

- les relations entre les systèmes d'information, les fonctions et les domaines d'activité de l'organisme (solution conceptuelle)
- les règles d'organisation et traitement qui en découlent (solution organisationnelle)
- les supports techniques et moyens de traitement qui sous-tendent la mise en oeuvre de ces règles (solution technique)

Anglais : Target

Cible d'évaluation (ITSEC). Système ou produit des technologies de l'information qui est soumis à une évaluation de sécurité.
Anglais : Target of Evaluation (TOE)

Cible de sécurité (ITSEC). Spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation. La cible de sécurité doit spécifier les fonctions de sécurité de la cible d'évaluation. Elle pourra aussi spécifier les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui seront employés.
Anglais : Security target

Clair. Message en clair
Anglais : plain texte

Classe de BI (MARION). Classe de Budget Informatique de l'entreprise pris en compte par la méthode, pour la pondération des facteurs de l'audit (étape 3) et le calcul des coûts de base des moyens de sécurité (étape 5).

Classe de fonctionnalité (ITSEC). Ensemble des exigences minimales concernant la fonctionnalité de sécurité d'une cible d'évaluation, défini comme faisant partie des critères d'évaluation.
Anglais : Functionality class

Classes de menaces. Elles sont au nombre de cinq :

- Naturelles : tremblements de terre, inondation, foudre, etc.
- Techniques : pannes d'ordinateur et périphériques, etc.
- Humaines : maladies et accidents atteignant le personnel.
- Sociales : Volontaires (agressions, divulgation, modification...)
- Accidentelles (erreurs)

Anglais : Threat classes

Classification des chemins d'accès. Les chemins d'accès à une ressource seront définis de manière exclusive par groupe d'utilisateurs dans un dossier de fonctionnement élaboré par l'administrateur de sécurité. Les 6 classes de chemin d'accès sont :

- accès au traitement par lots (batch),
- accès en mode transactionnel,
- accès en mode interactif (TSO et autres),
- accès en mode vidéotex,
- accès en mode système et utilitaire.
- accès en mode télétraitement par lot (remote batch)

Classification DIC. Expression quantitative du besoin de sécurité en terme de Disponibilité, Intégrité, Confidentialité.
La sécurité des données traitées et traitantes repose sur la satisfaction de ces 3 exigences ou propriétés (besoins, spécifications) de sécurité fondamentales :

disponibilité, intégrité, confidentialité (voir attributs de la sécurité et mots eux-mêmes). Une ressource non classifiée ne présente pas de risques significatifs. Vis-à-vis de la sécurité, elle ne doit pas satisfaire à des propriétés particulières. Certaines écoles se reportent plutôt à la *classification PIC* (Pérennité, Intégrité, confidentialité).

Clé. Information alphanumérique permettant d'identifier un ensemble de données. *Cryptographie*. La clé de chiffrement est utilisée comme base de calcul dans l'algorithme de chiffrement.
Anglais : Key

Client (ITSEC). Personne ou organisme qui achète une cible de sécurité.
Anglais : customer

Cocitation. Co-occurrence de citation de deux auteurs dans un article. Cette méthode permet de regrouper les articles par domaines jusqu'au niveau le plus fin et de faire émerger les noms des véritables spécialistes.

Codage. Transformation (ou traduction) d'un message selon un code ou un algorithme convenu.

Code. - 1° Ensemble des signes, signaux et symboles, ainsi que leurs règles fonctionnelles d'application. Synonyme de langage.
- 2° Ensemble de règles et de conventions définies à l'avance, permettant de représenter des données d'une manière biunivoque sous une forme discrète.
Anglais : Code

Code d'authentification du message. (MAC Message Authentication Code) C'est un authentifiant à clés symétriques de type DES, classé en standard X9.9 par l'ANSI. Le MAC est calculé à partir du texte en clair d'une transaction (par exemple financière). Le résultat obtenu est associé au texte de la transaction, puis l'ensemble est acheminé vers le récepteur. Voir aussi empreinte où sceau
Anglais : Message Authentification Code (MAC)

Code d'identification personnel (code confidentiel). C'est une information confidentielle que connaît l'usager et qui permet d'assurer son authentification. Il doit être individuel et avoir une durée de validité limitée. Il est donc nécessaire de le modifier périodiquement.
Anglais : Personal Identification Number (PIN)

Code d'intégrité du message. Code servant à assurer l'intégrité des données par redondance de l'information (utilisation de CRC par exemple).
Anglais : Message Integrity Code (MIC)

Cohérence de sécurité. Homogénéité des protections et des contrôles où les quelques points faibles existants ne compromettant pas la sécurité d'ensemble.

Cohésion de fonctionnalité (ITSEC). Aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la mesure dans laquelle les fonctions de sécurité de la cible d'évaluation coopèrent d'une manière qui les fait se soutenir mutuellement pour fournir un ensemble intégré et efficace
Anglais : Binding of functionality

Commanditaire. Personne ou organisme qui demande une évaluation.
Anglais : Sponsor

Commettant. Celui qui charge une autre personne d'exécuter certains actes pour son compte.

Communication. - 1° En théorie des communications, désigne le processus par lequel l'information est transmise d'un émetteur à un récepteur.

- 2° Au sens large et par extension abusive désigne le message ou l'information que l'on a, à transmettre.
- 3° Au sens étroit désigne la nature même et le sens du processus : la relation inter-humaine par laquelle des interlocuteurs peuvent se comprendre et se faire comprendre ou s'influencer l'un et l'autre.

Communications (Théorie des). Formalisation théorique du processus général par lequel un système-source influence un autre système-destinataire par la manipulation de signaux circulant dans des canaux organises et hiérarchisés selon une configuration donnée. La théorie des communications s'appuie sur des "modèles" divers (cybernétiques, théorie de l'information, linguistique, théorie des rôles...) selon son domaine d'application.

Communication en transmission de données. Interconnexion de plusieurs circuits de données en tandem au moyen d'équipements de commutation pour permettre la transmission de données entre les ETTD.
Anglais : Data call

Communication virtuelle (circuit virtuel). Service offert sur un réseau exploité en commutation par paquets, selon lequel une procédure d'établissement et de libération de la communication détermine une période de communication entre deux ETTD pendant laquelle les données sont transmises dans le réseau en mode paquet. Toutes les données sont remises par le réseau dans l'ordre dans lequel elles ont été recues par le réseau.
Anglais : Virtual call, virtual circuit

Commutateur de données (centre de commutation de données). Noeud d'un réseau de transmission capable de transférer des données d'une ligne de transmission à une autre par commutation de circuits, de messages, ou par paquets.
Anglais : Data switching exchange

Commutation de circuits. Méthode de communication qui relie, à la demande, deux ou plusieurs utilisateurs et permet leur utilisation exclusive d'un circuit de données pendant la durée de la communication (exemple le réseau téléphonique).
Anglais : Circuit switching

Commutation de données. Forme de télécommunications destinée à un transfert d'informations entre installations de traitements de données.
Anglais : Data communication

Commutation de messages. Processus de transfert de messages par réception, stockage et retransmission de messages complets dans un réseau de données (non-exclusif)
Anglais : Message switching

Commutation par paquets. Processus de transfert de données au moyen de paquets munis d'adresses, dans lequel la voie est occupée seulement pendant la durée de la transmission du paquet, la voie étant ensuite disponible pour le transfert d'autres paquets (exemple TRANSPAC).
Anglais : Packet switching

Compactage des données (compression). Technique cryptographique consistant à retirer un certain nombre de caractères d'une information selon une loi déterminée. La réduction de longueur qui en découle brouille la compréhension du message. Les caractères ôtés sont transmis séparément au destinataire qui dispose des moyens de les reconstituer.
Anglais : Data compression

Compensation (d'erreur). (Sûreté de Fonctionnement) Forme de traitement d'erreur où l'état erroné comporte suffisamment de redondance pour permettre la délivrance d'un service non entaché d'erreur.
Anglais : Compensation (error ~)

Complexité. Science de la gestion de l'incertain dans les sociétés modernes. La complexité apparaît comme une dimension universelle de l'univers des systèmes, qui ne dépend pas seulement du nombre d'éléments qui constituent chacun d'eux, non plus que de leur densité, c'est-à-dire de leur nombre moyen en un emplacement donné (densité linéaire, superficielle ou voluminique).
La complexité d'un organisme est perçue par un récepteur donné comme une fonction d'un ensemble d'espérances préétablies d'occurrences qui varient actuellement selon la culture des individus (probabilité subjective). Elle apparaît comme comme une dimension psychologique majeure de la perception et comme un facteur latent de la perception esthétique.
En algorithmique, mesure permettant d'évaluer le temps (complexité temporelle) et le matériel (complexité spatiale) nécessaire à l'exécution d'un algorithme.
Anglais : Complexity

Comportement (d'un système). (Sûreté de Fonctionnement) Ce que fait un système.
Anglais : Behavior (system ~)

Composant. Dispositif (matériel et/ou logiciel) chargé d'une fonction spécifique dans un ordinateur ou un réseau télécoms. Par exemple les composants d'un réseau télécoms sont des modems, contrôleurs de communication, contrôleurs de grappe, commutateurs.
ITSEC : partie identifiable et autonome d'une cible d'évaluation.
Anglais : Component

Composant autotestable. (Sûreté de Fonctionnement) Composant comportant des mécanismes de détection d'erreur.
Anglais : Self Checking component

Composant de base (ITSEC). Composant identifiable au niveau hiérarchique le plus bas de la spécification produite au cours de la conception détaillée.
Anglais : Base component

Composant (d'un système). (Sûreté de Fonctionnement) Un autre système.
Anglais :Component (system ~)

Composition (ITSEC). Processus de combinaison des résultats de l'évaluation de l'exactitude et de l'efficacité d'une cible d'évaluation pour produire un étalonnage de garantie.
Anglais : Composition

Compromission. Violation de la sécurité d'un système, telles que révélation, modification ou destruction de données sensibles ou classifiées, par captation de rayonnement ou autre (matériel, câbles, écrans, etc...).
Anglais : Compromise

Compte rendu de sécurité. Qualité ou état qui enregistre, par individu rendu ainsi responsable, les violations et les essais de violation du système de sécurité.
Anglais : accountability - log

Concept. Idée représentée par un mot. Connaissance résumant l'expérience d'un objet ou d'une donnée pour quelqu'un.
Anglais : Concept

Concept de moniteur de référence. Concept de contrôle d'accès se rapportant à une machine abstraite qui s'interpose entre tous les accès de sujets à objets afin d'en maintenir la sécurité au niveau voulu.
Anglais : Reference monitor concept

Conception architectonique (ITSEC). Phase du processus de développement dans laquelle sont spécifiés la conception et la définition de haut niveau d'une cible d'évaluation.
Anglais : Architectural design

Conception pour la vérification. (Sûreté de Fonctionnement) Méthodes et techniques de conception d'un système destinées à faciliter sa vérification.
Anglais : Design for verifiability

Concluant(e). Qui apporte une preuve.

Condition d'environnement anormal. Définition de l'environnement spécifique pour lequel la mission, la fiabilité n'a plus à être assurée, mais dans lequel les risques d'accident doivent rester inférieurs au risque acceptable. Il doit y avoir cohérence entre les niveaux de risque acceptable et la probabilité des conditions anormales non retenues.

Condition d'environnement normal : Définition de l'environnement spécifique pour lequel les performances nominales du système doivent être assurées.
Les spécifications sont définies en utilisant des critères de probabilité pour rejeter certaines conditions et perturbations. Il doit y avoir cohérence entre l'objectif de fiabilité et la probabilité des conditions et perturbations non retenues.

Confiance (de). Qui comporte ou indique une caractéristique de sécurité confirmée par une certification. Un dispositif est dit de confiance s'il a été reconnu conforme à une norme de sécurité.
Synonyme s : garant, garanti, certifié, sûr, protégé
Anglais : Trusted

Confidentialité Propriété qui assure que l'information n'est pas rendue disponible, ni révélée à des personnes, entités ou processus inautorisés. Qualifie d'une manière générale toute procédure visant à restreindre la diffusion d'une information définie comme "sensible" ou "stratégique". La confidentialité des données et des programmes est confrontée aux risques de divulgation. Elle concerne le secret de l'information, c'est-à-dire les mesures à prendre pour interdire la divulgation volontaire ou involontaire des biens informationnels classifiés. Ces biens informationnels constituent le patrimoine économique de l'entreprise. Vouloir préserver un degré de confidentialité peut résulter d'obligations légales, contractuelles mais aussi déontologiques (bases de données : personnel, dossiers médicaux...). C'est également l'établissement de procédures administratives, techniques, physiques et juridiques appropriées qui assurent le caractère confidentiel des informations.
Lors du transport des informations, la confidentialité peut être assurée par la mise en oeuvre des fonctions cryptographiques.
Anglais : Confidentiality, privacy

Configuration (ITSEC). Sélection de l'un des ensembles de configurations possibles des caractéristiques d'une cible d'évaluation.
Anglais : Configuration

Confinement. Préservation des données au niveau de sécurité déterminé.
Anglais : Confinement

Confirmation. Auto-contrôle technique et validation d'une saisie, généralement effectués par une simple commande au clavier.

Connexité. Propriété formelle d'un réseau de communications permettant à tous les membres du groupe de communiquer, directement ou indirectement avec chacun des autres, et donc avec tous.

Connexité (degré de). Dans un réseau, degré de difficulté avec laquelle on peut déconnecter un poste (un individu ou un groupe). C'est-à-dire l'isoler, en agissant sur ses liaisons ou canaux. Plus les canaux de communications sont nombreux entre les membres, plus le réseau est connexe, moins il sera facile d'isoler un poste. Le réseau le plus centralisé a le degré de connexité le plus bas puisque la rupture ou l'obstruction d'un seul canal isole au moins un poste.

Consilium fraudis. Se dit de l'intention frauduleuse du débiteur (ou d'un tiers) causant un préjudice aux créanciers.

Construction (ITSEC). Processus de création d'une cible d'évaluation.
Anglais : Construction

Contention (conflit). Situation se produisant lorsque deux stations de données, ou plus, tentent d'émettre en même temps sur une même voie, ou quand deux stations de données essaient de transmettre au même instant en mode bilatéral à l'alternat.
Anglais : Contention

Continuité de service. Absence d'interruption d'un service (ou du service informatique). Assurer la continuité du service informatique, c'est mettre en place des dispositifs préventifs qui évitent ou minimisent les interruptions et assurent la reprise des opérations en cas de sinistre. Seule la direction est apte à statuer sur la politique à tenir en pareille circonstance vis-à-vis des clients à livrer et à facturer, des fournisseurs et du personnel à payer, etc.... Il lui incombe de définir les activités à maintenir coûte que coûte (ce qu'on appelera les activités vitales).
Anglais : Continuity

Contrainte. En théorie des communications, est "contrainte" toute restriction des communications (canal obligatoire, limites de temps, impératifs de présentation ou de transmission du message, coûts de communication, etc...).

Contraintes d'équilibrage (MARION). Principe de la méthode qui permet de définir les parts respectives du budget à allouer à la prévention et à la protection de façon à minimiser l'espérance mathématique annuelle de sinistralité. C'est le point de jonction entre l'étude des risques maximaux (étapes 1 et 2) et l'étude générale des risques (étape 3).

Contre-certification. Engagement personnel d'un tiers sur la portée d'une information, généralement réalisée par la transmission d'un mot de passe.

Contre façon. Fabrication, par une des parties prenantes (individu, entité ou processus), d'une information qu'elle prétend ensuite avoir reçue d'une autre partie.
Anglais : Forgery

Contre-mesures. Voir parades
Anglais : Countermeasures

Contrevenant. Personne qui enfreint les lois ou règlements.
Anglais : Contravener

Contrôle. Détermination des écarts entre une valeur réelle ou un état atteint, et une valeur de référence ou un état à atteindre. Le contrôle peut couvrir le processus d'action et le résultat de ce processus. Les contrôles sont des opérations qui agissent sur des causes afin de tendre à réduire le risque.
Application. L'examen du système et des contrôles :

- la vérification des contrôles
- l'évaluation des contrôles

Anglais : Verification

Contrôle par balance carrée. Contrôle dans lequel la somme des totaux des différentes colonnes est comparée à la somme des totaux des différentes rangées.
Anglais : Crossfooting check

Contrôle par block. Système de protection contre les erreurs basé sur la vérification de certaines règles prédéterminées de composition des caractères.
Anglais : Block check

Contrôle de configuration (ITSEC). Sélection de l'un des ensembles de combinaisons possibles de caractéristiques d'une cible d'évaluation.
Anglais : Configuration control

Contrôle par dépassement. Contrôle permettant de détecter si la longueur d'une donnée dépasse une longueur stipulée.
Anglais : Overflow check

Contrôle des données. Opération vérifiant le niveau d'intégrité ou la qualité des données (adéquation aux spécifications).
Anglais : data check

Contrôle par double saisie. Vérification de l'exactitude de la saisie des données par la réintroduction au clavier de ces mêmes données.
Anglais : keystroke verification

Contrôle par écho. cf. Contrôle par retour de l'information.

Contrôle d'erreurs. cf procédure de contrôle

Contrôle de flux. Procédure de commande de la cadence de transfert des données entre deux points d'un réseau de données, par exemple entre deux ETTD, ou entre un ETTD et un noeud de réseau.
Anglais : Flow control

Contrôle de format. Contrôle servant à déterminer si les données respectent le format spécifié (type de caractère, ordonnancement, longueur de champ,...).
Anglais : Format check

Contrôle par fourchette. Combinaison de deux contrôles de valeur limite, l'un portant sur une limite supérieure et l'autre sur une limite inférieure.
Anglais : Range check

Contrôle de parité ou d'imparité. Contrôle vérifiant si, dans un groupe de chiffres binaires, le nombre des symboles "1" est pair (contrôle de parité) ou impair (contrôle d'imparité). Dans certain cas ce contrôle peut porter sur le nombre des symboles "0".
Anglais : Even parity check, odd parity check

Contrôle de présence. Contrôle servant à vérifier la présence au complet de données là où elles sont requises.
Anglais : Completeness check

Contrôle de redondance cyclique. Contrôle de la validité d'une information en redondance cyclique.
Anglais : Cyclic Redundancy Check (CRC)

Contrôle par retour de l'information - contrôle par écho. Méthode visant à contrôler l'exactitude de la transmission des données, selon laquelle les données

reçues sont retournées vers l'extrémité émettrice afin de les comparer avec les données originales conservées en mémoire dans ce but.
Anglais : Loop checking, message feedback, information feedback, echo check

Contrôle de séquence. Contrôle servant à déterminer si les enregistrements se succèdent selon un ordre établi.
Anglais : Sequence check

Contrôle sur total. Résultat obtenu en appliquant un algorithme à un groupe de données à des fins de contrôle.
Anglais : Hash total

Contrôle par totalisation. Comparaison des sommes calculées à partir des mêmes données dans des circonstances différentes ou avec des représentations de données différentes permettant de vérifier l'intégrité des données.
Anglais : Summation check, sum check

Contrôle de valeur limite. Contrôle permettant de déterminer si une valeur se trouve au-dessus ou en-dessous d'une limite ou encore si elle a atteint une limite stipulée.
Anglais : Limit check

Contrôle de vraisemblance. Contrôle servant à déterminer si une valeur est conforme à des critères définis :

- contrôle de cohérence entre deux ou plusieurs données,
- contrôle par rapport à un état antérieur.

Anglais : Reasonableness check - likelihood check

Contrôleur d'entrée/sortie. Dans un système de traitement de l'information, unité fonctionnelle qui commande le fonctionnement d'un ou de plusieurs organes périphériques.
Anglais : Input/output controller

Contrôleur de communication - frontal - processeur - unité de contrôle de transmission. Partie d'un ETTD qui prend en charge la gestion de ses communications de données à travers un réseau. Le terme "processeur frontal" ou "frontal" (front end processor) désigne plus particulièrement un organe interposé entre le réseau et un canal d'entrée/sortie d'un système de traitement.
Anglais : Communication controller, communication control unit, front-end processor

Contrôleur de grappe. Contrôleur de communication d'un ETTD constitué par une grappe de terminaux. Ce terme désigne souvent un organe qui assure en plus des fonctions de traitement pour la grappe.
Anglais : Cluster controller

Conversationnel (mode). Mode dialogué, mode interactif. Mode d'utilisation d'un système de traitement à partir d'un poste de travail dans lequel alternent les messages entrés par l'opérateur et les réponses du système de traitement.
Anglais : Conversational mode, interactive mode

Copie témoin (ITSEC). Copie d'une cible dévaluation et/ou de sa documentation, qui est conservée par le développeur et utilisée comme version définitive pour les besoins de la production et de la maintenance.
Anglais : Master copy

Correction. Action de corriger un état pour revenir à l'état de référence.

Correction (mesures de). La sixième des six fonctions de protection. Les mesures de correction doivent être conçues et mises en place immédiatement après que la reprise de la conduite normale des activités est assurée.

Corruption. Elle consiste du côté employé (corruption passive) à solliciter ou agréer des offres ou promesses, à solliciter ou recevoir des dons ou présents en vue de violer un devoir professionnel (par acte ou abstention que l'acte soit juste ou injuste, qu'il entre dans les attributions de l'employé ou soit seulement facilité par ses fonctions), et, du côté du corrupteur (corruption active) à proposer la corruption, dans le même dessein que celui visé plus haut, par les mêmes moyens, plus la menace et la voie de fait.

Coupable. Qui a commis un crime, une faute

Couverture. (Sûreté de Fonctionnement) Mesure de la représentativité des situations auxquelles le système est soumis durant sa validation par rapport aux situations auxquelles il sera confronté durant sa vie opérationnelle.
Anglais : Coverage

Craquer ou déplomber un ordinateur : Pénétrer illicitement dans un réseau en forçant les contrôles d'accès, par exemple les mots de passe.

Crédibilité. Garantie de détecter les défaillances.

Crédibilité. (Sûreté de Fonctionnement) Aptitude d'un système à fournir à ses utilisateurs des informations indiquant si le service délivré est correct.
Anglais : Trustability

Crime. Action très blâmable. Infraction que la loi punit d'une peine afflictive. Se dit d'une très grave infraction à la loi morale et à la loi civile, qui mérite d'être réprimée ou sévèrement blâmée.

Criminalité informatique. Ensemble des actes criminels commis en informatique à une époque donnée.

Criminalistique informatique. Ensemble des techniques mises en oeuvre par les auditeurs et experts en systèmes d'information pour établir la preuve du crime informatique et identifier les auteurs.

Criticité : Mesure objective ou subjective du degré de dépendance d'une organisation par rapport à la disponibilité de son système d'information et informatique pour effectuer normalement les travaux prévus.
Anglais : Criticality

Criticité (d'un système). (Sûreté de Fonctionnement) Sévérité maximum de ses modes de défaillance.
Anglais : Criticality (system~)

Croissance de fiabilité. (Sûreté de Fonctionnement) L'aptitude du système à délivrer un service correct est améliorée (augmentation stochastique des temps jusqu'à défaillance successifs)
Anglais : Reliabilty growth

Cryptanalyse (analyse cryptologique). Analyse d'un système cryptographique et/ou des données qu'il traite afin de déduire des variables ou données confidentielles telles que le texte en clair ou de la clé de chiffrement.
Anglais : Cryptanalysis, codebreaking

Cryptogramme. Message écrit à l'aide d'un système chiffré ou codé, afin de le rendre inintelligible.
Anglais : Ciphertext, cryptogram

Cryptographie. Science des écritures secrètes incluant les principes, moyens, méthodes de transformation des données, dans le but de rendre inintelligible un

texte en clair afin de masquer son contenu, empêcher sa modification ou utilisation illégale, ainsi que son opération inverse.
Synonymes : chiffre, systèmes cryptographiques. La cryptographie a recours à des algorithmes de chiffrement tels que DES, RSA et autres.
Anglais : Cryptography

Cryptographiques (systèmes). Voir cryptographie.

Cryptologie. Science qui couvre à la fois la cryptographie et la cryptanalyse.
Anglais : Cryptology

Cryptologique (analyse). Voir cryptanalyse.

Cyberpunks : Catégorie de "fouineurs" voulant prouver que la société télématique est fragile. Ils craquent les systèmes pour le démontrer.

D.

Dangers d'un système. Répertoire des événements redoutés et de leurs conséquences susceptibles d'être provoqués par le système.
Etre en danger : expression courante qui indique que l'on se trouve dans une situation de risque inacceptable d'accident.
L'acceptation courante du mot danger comme "menace potentielle pour le système ou son environnement est trop imprécise dans le cadre du vocabulaire sécurité des systèmes

DARM (MARION). Dossier d'Analyse des Risques Maximaux

Débouté. Rejet d'une demande faite en justice.

Déchiffrement. Opération inverse d'un chiffrement réversible.
Anglais : Decipherment, decryption

Déchiffrer. Traduire en clair le texte chiffré en utilisant les procédures correctes et spécialement la clé de déchiffrement.
Anglais : to decipher

Décision. Toute décision est le choix d'une solution à un problème.
Le décideur reconnaît qu'il y a problème lorsque lui apparaît un changement significatif dans le système qui détermine ses objectifs ou leur réalisation, ce qui implique une réaction de sa part. Trois types de conditions sont nécessaires pour qu'il sollicitation extérieure donne lieu à une décision et non à un acte réflexe :

- nécessité de plusieurs issues possibles et termes du choix explicites,
- nécessité d'un système de référence ou d'un modèle théorique,
- nécessité enfin d'un niveau d'information incomplet.

Déclarant (AFNOR-ISO). Entité qui est ou représente une entité principale désirant être authentifiée, ainsi que les fonctions qu'implique un échange d'authentification au nom de cette entité. Un déclarant dispose des fonctions nécessaires pour s'engager dans des échanges d'authentification au nom d'une entité principale.
Synonyme : Appelant
Anglais : Claimant

Décrypter (casser le code). Retrouver, sans en connaître la clé, le clair d'un cryptogramme qui ne nous est pas destiné, ou découvrir la clé d'un système de chiffrement
Anglais : Codebreaking, cryptanalysis

Décryptement. Action de décrypter

Défaillance. C'est pour un système la cessation de son aptitude à accomplir la fonction exigée de lui. On peut classer les défaillances en fonction :
a) - de leur causes :

- *Défaillances intrinsèques*. Celles qui sont attribuables à des faiblesses inhérentes au dispositif.
- *Défaillances extrinsèques*. Celles qui sont attribuables à l'application de contraintes supérieures aux possibilités définies du dispositif.

b) - de leur nature :

- *défaillances catalectiques*. Lorsque ces défaillances se produisent brusquement.
- *défaillances par dérive*. Celles qui résultent d'une évolution lente..
- *Défaillance critique*. Celle qui empêche l'accomplissement de la mission et fait encourir des risques jugés graves. (norme NF x 06501 : terme de fiabilité)
- *Défaillance de mode commun*

Anglais : Failure

Défaillance (Sûreté de Fonctionnement) : Evénement survenant lorsque le service délivré n'est plus conforme à la spécification. Transition de service correct vers service incorrect.

~ **bénigne**. Défaillance dont les conséquences sont du même ordre de grandeur (généralement en termes économiques) que le bénéfice procuré par le service délivré en l'absence de défaillance. Anglais : Benign failure

~ **catastrophique**. Défaillance dont les conséquences sont incommensurablement supérieures au bénéfice retiré de la délivrance d'un service en l'absence de défaillance. Anglais : Catastrophic failure

~ **cohérente**. Défaillance perçue identiquement par tous les utilisateurs du système. Anglais : Consistent failure

~ **de mode commun**. Défaillances résultant de fautes corrélées. Anglais : Common mode failure

~ **en valeur**. Défaillance telle que la valeur du service délivré n'est pas conforme à la spécification. Anglais : Value failure

~ **incohérente**. Défaillance dont les utilisateurs du système peuvent avoir des perceptions différentes. Anglais : Inconsistent failure

~ **par arrêt**. L'activité du système, si tant est qu'il en ait une, n'est plus perceptible aux utilisateurs, et une valeur constante du service est délivrée. Anglais : Stopping failure

~ **par écrasement**. Défaillance par omission persistante Anglais : Crash failure

~ **par omission**. Aucun service n'est délivré. Anglais : Omission failure

~ **séquentielles**. Défaillances qui ne surviennent pas dans la même fenêtre temporelle prédéfinie. Anglais :Sequential failure

~ **simultanées**. Défaillances qui surviennent dans une fenêtre temporelle prédéfinie. Anglais : Simultaneous failure

~ **temporelle**. Défaillance telle que les conditions temporelles de délivrance du service ne sont pas conformes à la spécification. Anglais : Timing failure

Défaut. Non conformité d'un individu aux prescriptions imposées pour un caractère (norme F x 06 004 : terme de contrôle de qualité)

Défaut critique. Défaut qui d'après le jugement ou l'expérience, est susceptible de conduire à un manque de sécurité, ou à des risques d'accidents pour les utilisateurs le personnel d'entretien, ou ceux qui dépendent du produit considéré, ou bien qui pourrait empêcher l'accomplissement de la fonction d'un produit final plus important.

Déguisement. Acte de prétendre être une autre entité dans le but d'accéder aux ressources de celle-ci.
Anglais : Masquerade

Délinquance. Ensemble de crimes et de délits. La délinquance informatique est l'ensemble des des crimes et délits commis sur ou par l'informatique.

Délinquant. Personne qui s'est rendue coupable d'un délit, d'une violation de la loi. Principalement en matière correctionnelle.

Délit. Tout fait illicite d'où naît un dommage. Le fait est illicite quand il est intentionnel. Toute infraction à la loi et punie par elle. C'est uniquement un terme de jurisprudence, qui ne s'applique d'ailleurs qu'aux violations de la loi qui ressortissent aux tribunaux inférieurs.

Déni de service. Mesures préventives affectées aux accès autorisés des ressources du système, ou temporisation de la durée critique des opérations. Pour l'ISO, prévention totale ou partielle des accès
Anglais : Denial of service

Déplomber (un logiciel). Violer les protections de ce logiciel.

Déprédation. Se dit particulièrement des malversations commises dans l'administration ou la régie de quelque chose ; elle comporte en outre l'idée de dégât.

Dérober. Prendre, s'emparer furtivement du bien d'autrui en prenant grand soin d'échapper aux regards.

D E S (Data Encrytion Standard). Algorithme de chiffrement symétrique à clés qui utilise la même clé pour le chiffrement et le déchiffrement. Cette clé doit être connue des différents correspondants mais doit rester secrète vis-à-vis des autres intervenants. Le DES assure l'intégrité et la confidentialité des messages transmis.

Détection. Action visant à déceler l'existence d'un objet, d'un phénomène... La quatrième des 6 fonctions de la protection. La détection en temps et lieu opportuns consiste à déceler qu'un acte interdit est en train d'entraver, d'une façon ou d'une autre, le déroulement d'une activité, ou bien que cet acte interdit a eu lieu si récemment, qu'il sera possible d'y mettre un terme, ou au moins limiter ses conséquences désastreuses.
MELISA : Détection de l'occurrence d'un événement. La détectabilité d'un événement a pour effet principal de réduire sa gravité effective par les possibilités de réaction de l'entreprise.
Anglais : Detection

Détection (d'erreur). (Sûreté de Fonctionnement) Identification d'un état erroné comme tel.
Anglais : Detection (error ~)

Détournement informatique. Soustraction frauduleuse (exemple : détournement de fichiers, de programmes, de données...) commise par un préposé d'une entreprise. La fraude est toujours commise par un tiers de l'entreprise.
Anglais : Embezzlement

Développeur (ITSEC). Personne ou organisme qui développe une cible de sécurité.
Anglais : developer

Développeur (sécurité du). (ITSEC) : ensemble des contrôles de sécurité physiques, procéduraux ou relatifs au personnel, imposés par un développeur à son environnement de développement.
Anglais : Developer security

Diagnostic (de faute). (Sûreté de Fonctionnement) Détermination des causes des erreurs, en termes de localisation et de nature.
Anglais : Diagnosis (fault ~)

Diagramme différentiel (MARION). Représentation graphique des résultats de l'audit permettant de hiérarchiser les insuffisances des facteurs de sécurité en fonction des risques potentiels.

Dictionnaire du chiffre (ou de codes). Document contenant chiffre et code équivalent. Egalement une technique de chiffrement employant la substitution de mot.
Anglais : Code book

Dictionnaire de données. Progiciel décrivant et gérant les éléments d'un système d'information et informatique. Chaque élément est identifié par un nom discriminant qui le différencie des autres. En général les dictionnaires de données fournissent divers renseignements à l'administrateur de données : documents d'analyse sémantique, fiches signalétiques des différents états à un moment donné, et. toutes les variables utilisées dans les différents programmes sont enregistrées avec leurs spécifications informatiques (type, longueur...) et logiques (contrôle à

effectuer, appartenance a des ensembles d'informations, restriction d'accès, etc.). Pour utiliser ces variables l'informaticien n'aura plus qu'à les nommer, le générateur ira ensuite directement rechercher dans le dictionnaire les descriptions correspondantes. De plus, le dictionnaire permettra de retrouver des impacts, par exemple de modifier tous les programmes ou les fichiers contenant une variable donnée dont on a modifié la longueur, et ce automatiquement. Enfin le dictionnaire gère les programmes, les fichiers et peut déterminer leurs taux d'utilisation ou contrôler les accès. A partir des descriptions du dictionnaire, l'informaticien peut définir des cas de valeur. Le système de test générera automatiquement le contexte d'un programme ou d'un ensemble et permettra de vérifier la qualité des contrôles. Certains systèmes peuvent aussi préciser quels sont les tests des programmes qui ont été contrôlés et permettent donc de vérifier que le jeu d'essai est complet.
Anglais : Data dictionary

Discret. Cet adjectif désigne une caractéristique de données ou de grandeurs physiques lorsqu'elles ne peuvent prendre qu'un ensemble fini ou infini dénombrable de valeurs distinctes et observées. En théorie cet ensemble peut être fini ou infini ; en pratique, il est toujours fini.
Discrétiser des données sur un ensemble de valeurs consiste à faire correspondre à chaque donnée que l'on doit enregistrer, la valeur qui lui est numériquement la plus proche dans l'ensemble discret.
Anglais : Discrete

Discrétionnaire (contrôles d'accès). Moyens de limiter les droits d'accès aux ressources aux seuls entités et/ou groupes d'entités habilités à utiliser ces ressources. Les contrôles sont discrétionnaires dans le sens que :

- une entité est capable de passer ses droits d'accès à une autre,
- le DAC est souvent employé pour renforcer la sélectivité d'accès,
- le DAC peut être changé par le gestionnaire de la ressource à sa discrétion (c'est-à-dire librement)

Anglais : Discretionary access control (DAC)

Disponibilité. Propriété de la sécurité des systèmes d'information qui associe les notions de fiabilité et de maintenabilité. On la définit comme la probabilité qu'un système fonctionne à un instant quelconque, dans des conditions déterminées d'exploitation et de maintenance. Elle a donc pour objectif de maintenir le niveau de service et de remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performances.
La disponibilité des prestations informatiques peut être mise en cause par des risques d'interruption de l'exploitation :

- défaillances affectant les unités centrales, les équipements périphériques, les réseaux et les logiciels (problèmes de fiabilité),
- grèves du personnel informatique,
- sinistres pouvant tenir à des causes accidentelles ou naturelles (incendies et inondations...) ou à des actes de sabotage et se traduisant par une destruction totale ou partielle des équipements,
- indisponibilité des informations,
- discordance,
- distorsion.

Par extension, assurer la disponibilité des traitements informatiques c'est viser à assurer la continuité de fonctionnement des matériels, des informations traitantes et traitées en contrôlant la fiabilité, la maintenabilité, l'accessibilité, la présence, la sauvegarde, le back-up et la reprise après incident.
Sûreté de fonctionnement : sûreté de fonctionnement par rapport au fait d'être prêt à l'utilisation. Mesure de la délivrance d'un service correct par rapport à l'alternance service correct-service incorrect.

Dissémination. Dispersion, éparpillement.

Dissuasion. Action visant à amener quelqu'un à renoncer à son projet. La seconde des 6 fonctions de la protection. Dans la hâte fréquente de prendre des mesures

préventives, on oublie trop souvent la dissuasion. Dissuader signifie décourager : décourager quelqu'un d'agir en raison de la peur, ou de la prise de conscience d'éventuelles circonstances ou conséquences difficiles, et même désagréables.
Dans le portrait-robot du criminel informatique, la peur de la détection inattendue joue un rôle essentiel.
Le but de la dissuasion est de réduire la menace qui plane sur les biens, et par voie de conséquence, la vulnérabilité de ces biens aux pertes.

Distorsion. En théorie des communications, perturbations des éléments du message. La distorsion est dite intrinsèque s'il y a altération interne (exemple destruction partielle du message) ; elle dite extrinsèque si la perturbation vient de l'extérieur.

Diversification fonctionnelle. (Sûreté de Fonctionnement) Approche pour le développement d'un système destinée à fournir des services identiques via des conceptions et de. réalisations séparées.
Anglais : Design diversity

Distraire. Approprier, dérober, voler, usurper.

Diversion. Opération visant à détourner l'attention de l'adversaire du point ou on veut l'attaquer.

Documentation (ITSEC). Information écrite (ou autrement enregistrée) sur une cible d'évaluation exigée pour l'évaluation. Cette information peut, mais ce n'est pas nécessaire, être rassemblée en un seul document constitué dans ce but.
Anglais : Documentation

Documentation de gestion (ITSEC). Information fournie par le développeur d'une cible d'exploitation à l'usage de ceux qui en gèrent son mode d'emploi et son l'exploitation.
Anglais : administration documentation

Documentation d'exploitation (ITSEC). Information fournie par le développeur d'une cible d'évaluation pour spécifier et expliquer le mode d'emploi à l'usage des clients.
Anglais : operational documentation

Dol. Manoeuvres frauduleuses destinées à tromper quelqu'un pour l'amener à passer un acte juridique.

Domaine d'activité : Ce concept est utilisé pour localiser globalement une application ou le champ d'investigation d'un projet ou sous-projet. Par exemple dans une banque on isolerait : les domaines "dépôts", "engagements" etc.
Il faut noter que ce concept domaine d'activité est différent du "secteur d'activité" comme administration, service public, agriculture...
Les secteurs d'activité impliquent une typologie des organismes, alors que les domaines d'activités constituent une typologie interne à un organisme donné.
Anglais : Activity domain

Dommage. Se dit de tout dégât causant un préjudice sérieux, ce en quoi les intérêts sont compromis ; il s'applique plus particulièrement à une perte matérielle.
Un dommage quel qu'il soit résulte toujours de la concrétisation d'une menace.
Préjudice causé par un système à son environnement passif conduisant à une diminution de l'intégrité physique des personnes ou de la valeur initiale des biens ou des équipements. Types de dommages :

- paralysie par arrêt du système de fourniture des données
- perte physique de biens d'investissement qui ont un coût très élevé
- fraudes et détournements divers par vol d'informations, vol de temps, calcul, constitution de créanciers imaginaires

- dégâts à l'environnement, aux usagers, aux autres personnes.

Dommage corporel. Toute atteinte corporelle subie par une personne physique résultant d'un événement imprévu et extérieur à la victime.

Dommage matériel. Toute détérioration ou destruction d'une chose ou substance, toute atteinte physique à des animaux, résultant d'un événement imprévu et extérieur à la chose endommagée.

Dommage immatériel. Tout préjudice pécuniaire, résultant de la privation de la jouissance d'un droit, de l'interruption d'un service rendu par une personne, par un bien ou immeuble ou de la perte d'un bénéfice et qui est la conséquence directe de dommages corporels ou matériels garantis.

Dommage immatériel consécutif. Tout préjudice pécuniaire qui ne se traduit pas par une atteinte physique à un bien ou à une personne mais qui est la suite d'un dommage matériel ou corporel garanti.

Dommage immatériel non-consécutif. Tout préjudice pécuniaire qui ne se traduit pas par une atteinte physique à un bien ou à une personne mais qui est la suite d'un dommage matériel ou corporel non-garanti.

Donnée. Valeur numérique, chaîne de caractère ou chaîne de bits. Valeur prise par une information au cours de son traitement par le système d'information.

Double signature. Procédure visant à renforcer l'authentification de l'origine d'un message. Elle est prise en compte dans les profils à sécurité jointe et disjointe. Quel que soit le nombre de signatures transmises par l'émetteur, le récepteur ne délivre qu'un seul acquittement par fichier.

E.

Ecoute. Interception passive, donc sans altération, de l'information transitant par une ligne de télécommunication. L'écoute constitue une violation de la confidentialité.

Efficacité. Caractère de ce qui tend à ce que le résultat de l'action soit aussi conforme que possible à son objectif (satisfaction des objectifs, convivialité, adaptabilité aux changements, sensibilité de fonctionnement...). Le degré d'efficacité est égal à la somme des résultats obtenus sur la somme des objectifs.
ITSEC : Propriété d'une cible d'évaluation qui représente la mesure dans laquelle elle assure la sécurité dans le contexte de son exploitation réelle ou prévue.
Anglais : Effectiveness

Efficience ou productivité. Capacité de rendement.
Propriété de la qualité définie comme une dépense de ressources pour obtenir un résultat, représentant lui-même une progression vers un but. Le degré d'efficience est égal au montant des ressources sur le montant des résultats obtenus.
Voir aussi : productivité, rendement
Anglais : Efficiency

Effraction. Forcement d'une protection.

Elément. Un élément est un objet quelconque, concret ou abstrait, qui possède une certaine identité qui permet de le distinguer d'autres objets dans l'univers étudié. Ce concept d'élément est celui de la théorie des ensembles.
Anglais : Element

Eléments (ensemble d'). Un ensemble d'éléments est une collection d'objets vérifiant une ou plusieurs propriétés, en particulier la proprité d'appartenance à cet ensemble. Les éléments d'un sous-ensemble d'un ensemble référentiel **E** d'une structure définissent un composant de cette structure.

Elimination des fautes. (Sûreté de Fonctionnement) Méthodes et techniques destinée à réduire la présence (en nombre et en sévérité) des fautes
Anglais : Fault removal

Emission. Commande d'exécution ordonnant au système de transmettre une donnée.

Empreinte ou sceau. Résultat calculé à partir d'un texte ou message, par une méthode connue seulement de l'expéditeur et du destinataire et permettant de vérifier son intégrité après réception
voir aussi : signature
Anglais : Message Authentication Code

Emulation. Simulation imitant généralement la structure et le comportement d'un dispositif.

Entité : Élément ou ensemble d'éléments ayant une existence propre et indépendante dans un monde à représenter.
Objet concret ou abstrait, observé dans le réel étudié, et qui possède une certaine identité permettant de le distinguer des autres objets.
Anglais : Entity

Entité principale (AFNOR-ISO). Entité dont l'identité peut être authentifiée.
Anglais : Principal

Entité Relation (modèle). Modèle de représentation des données utilisé pour la constitution de bases de données.
Il utilise les concepts d'entité, d'attributs d'entité (propriétés d'une entité n'ayant pas d'existence propre mais trouvant une sémantique à travers leur association avec une entité) et de relations entre entités (association de plusieurs entités pour constituer une information particulière)
Anglais : Entity Relationship Model

Entraves (à la sûreté de fonctionnement). (Sûreté de Fonctionnement) Circonstances indésirables, mais non inattendues, causes ou résultats de la non-sûreté de fonctionnement. Fautes, erreurs, défaillances.
Anglais : Impairments (to dependability)

Entreprise. L'entreprise est un groupement humain hiérarchisé qui met en oeuvre des moyens intellectuels, physiques, financiers, pour extraire, transformer, transporter, distribuer des richesses ou produire des services, conformément à des objectifs définis par une direction, personnelle ou collégiale en faisant intervenir à des degrés divers les motivations de profit et d'utilité sociale.
A partir d'un point de vue morphologique et physiologique, l'entreprise est un ensemble coordonné d'organes agencés selon des finalités spécifiques pour remplir certaines fonctions, en exécutant des opérations plus ou moins complexes et répétitives qui aboutissent à la livraison au marché d'objets ou prestations de services dont la vente est génératrice d'un résultat.

Entropie. Quantité moyenne d'information dans l'espace des messages fournie par un message donné.
Nombre qui mesure la moyenne de l'information d'un ensemble de messagesdont la somme des probabilités est égale à 1. Si Pi est la probabilité de chaque symbole, l'entropie de l'ensemble est :

$$H = -\sum_{i=1}^{N} Pi \log_2 Pi$$

où N est le nombre de messages (cf quantité d'information)
Anglais : Entropy

Environnement. Ensemble de tout ce qui est extérieur au système. Cette définition appartient au technolecte de la sécurité des systèmes. L'environnement comprend notamment des facteurs physiques, chimiques, biologiques, psychiques et sociaux.
Linguistique : voisinage d'un élément dans un énoncé, c'est-à-dire ce qui reste de cet énoncé après suppression de l'élément en question.
Anglais : Environment

Environnement actif. Partie de l'environnement spécifique susceptible d'influencer le système.
Anglais : Active Environment

Environnement d'exploitation (ITSEC). Mesures d'organisation, procédures et normes qui doivent être utilisées au cours de l'exploitation d'une cible d'évaluation.
Anglais : Operational Environment

Environnement d'un système. (Sûreté de Fonctionnement) Les autres systèmes ayant interagi ou interféré, interagissant ou interférant, ou susceptible d'interagir ou d'interférer avec le système considéré.
Anglais : Environment (system ~)

Environnement de développement (ITSEC). Ensemble de mesures d'organisation, des procédures et des normes utilisées au cours de la construction d'une cible d'évaluation.

Anglais : Development Environment

Environnement logique de l'information. Organisation ponctuelle ou ensemble des démarches formalisées mises en application pour atteindre des objectifs de sécurité.
Anglais : Information logical environment

Environnement passif. Partie de l'environnement spécifique pouvant être influencé par le système.
Anglais : Passive environment

Environnement physique de l'information. Il comprend :

- Les matériels de traitement, de stockage, de reproduction, de transport, de façonnage et de protection des supports de l'information (ordinateurs, photocomposeuses, machines de reproduction, bandes et disques magnétiques, photographies, supports papiers, etc.).
- Les équipements nécessaires à leur fonctionnement (alimentation électrique, climatisation, ventilation, protections électromagnétiques éventuelles, etc.

Anglais : Information physical environment

Environnement spécifique. Partie de l'environnement sélectionné en fonction de son degré d'influence sur le système ou de sa sujétion au système.
Anglais : Specific environment

Equivalence. Correspondance dans les deux sens. Relation réflexive, symétrique et transitive. Exemple l'identité est une équivalence.

Equivalence linéaire. Longueur du plus petit registre à décalage, rebouclé selon une fonction linéaire, produisant la même suite d'éléments d'informations que celle produite par un générateur pseudo-aléatoire.
Anglais : Linear Equivalence

Erreur. (Sûreté de Fonctionnement) : Partie de l'état d'un système - par rapport au processus de traitement - qui est susceptible d'entraîner une défaillance. Manifestation d'une faute dans un système
Anglais : Error

Erreurs coïncidentes. (Sûreté de Fonctionnement) Erreurs produites sur la même entrée.
Anglais : Coincident error

Erreur détectée. (Sûreté de Fonctionnement) Erreur reconnue en tant que telle par un algorithme ou un mécanisme de détection.
Anglais : Detected error

Erreur latente.(Sûreté de Fonctionnement) Erreur qui n'a pas été reconnue en tant que telle.
Anglais : Latend error

Escroquerie. Action d'obtenir la remise d'une chose convoitée en usant de certains moyens en vue d'un certain résultat, et dans le cadre d'un certain état d'esprit. Trois éléments dont la réunion forme le délit d'escroquerie (art. 405 C. pén.). Les principaux moyens de délit sont :

- usage de faux nom
- usage de fausse qualité
- manoeuvres frauduleuses (par mise en scène, par document, par publicité, par intervention d'un tiers).

Espace des messages. Ensemble des messages possibles.
Anglais : Message space

Essai. Mise en œuvre préalable à l'exploitation en vue d'établir la conformité à des spécifications.

Estimation. Examen préliminaire des caractéristiques de sécurité d'un système, avant évaluation approfondie.
Anglais : Assessment

Estimation de la vulnérabilité (ITSEC). Aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la mesure dans laquelle les vulnérabilités découvertes dans la cible d'évaluation compromettront réellement sa sécurité telle qu'elle est spécifiée dans la cible de sécurité.

Etalonnage. Mesure de la confiance qui peut être accordée à une cible d'évaluation, comprenant une référence à sa cible de sécurité, un niveau d'évaluation établi par l'estimation de l'exactitude de sa mise en application et la prise en considération de son efficacité dans le contexte de son exploitation réelle ou prévue, enfin, de façon optionnelle, une estimation de la résistance minimale de ses mécanismes de sécurité dans le cadre de cet emploi.
Anglais : Rating

ETTD. Equipement terminal de traitement de données. Expression qui dans le vocabulaire officiel des télécommunications désigne un appareil connecté à un réseau capable de recevoir et/ou émettre des données
Anglais : Data Terminal Equipement (DTE)

Etat (d'un système). (Sûreté de Fonctionnement) Condition d'être par rapport à un ensemble de circonstances.
Anglais : State (system ~)

Etude de sécurité. Partie d'un programme de sécurité destinée à évaluer la probabilité d'un événement redouté défini et à proposer un plan d'action.

Evaluation. Comparaison à des normes ou critères. Détermination d'une valeur ou d'une quantité '(exemple évaluation de la fiabilité)
Mesure permettant d'apprécier la qualité et/ou la sécurité d'un système par rapport à un référentiel établi par l'entreprise ou par rapport à des lois, normes, ou règles de gestion généralement admises (règles de l'art).
COMPUSEC : Examen technique détaillé, par une autorité compétente, des aspects touchant à la sécurité d'un système ou produit informatique, afin de confirmer la présence de la fonctionnalité de sécurité requise, l'absence d'effets secondaires indésirables découlant de cette fonctionnalité et le caractère inaltérable de celle-ci. L'évaluation détermine dans quelle mesure sont satisfaits les impératifs de sécurité d'un système ou réseau informatique ou d'un produit COMPUSEC, et détermine le niveau d'assurance du système ou réseau informatique, ou la fonction sûre du produit.
ITSEC : Evaluation d'un système ou d'un produit des technologies de l'information par rapport aux critères définis.
MELISA : Nom donné au déroulement de cette méthode pour un système d'information donné, comprenant, d'une part l'analyse de l'existant, et d'autre part, la détermination de nouvelles parades et l'évaluation de la vulnérabilité résiduelle.
Anglais : Evaluation

Evaluation des menaces. Détermination de la source, de l'étendue et de la nature des attaques possibles contre le système, y compris l'environnement de l'attaque.
Anglais : Threat assessment

Evaluation du produit. Evaluation technique des dispositifs de sécurité d'un produit pour déterminer le niveau de confiance qui peut être placé dans ce produit en fonction des "Critères d'évaluation des produits de confiance" qui lui sont

applicables (par exemple, système d'exploitation, système de gestion de base de données, réseaux d'ordinateurs, sous-systèmes de sécurité d'ordinateurs).

Evénement. Modification au sein du système ou dans son environnement avec influence sur le système, susceptible de déclencher des traitements.
MELISA. Un des scénarios possibles dont l'aboutissement est une menace type (sinistre).

Evénement naturel. Evénement stable par rapport aux choix d'organisation, actuels ou futurs ; événement caractéristique de l'activité considérée ou pouvant survenir dans le cadre d'un déroulement normal de cette activité.

Evitement. Action visant à ne pas subir un événement nuisible, un risque,... La première des six fonctions de la sécurité. L'évitement peut être réalisé en évitant toute menace potentielle, ou bien encore en éliminant ou en transférant ailleurs tout bien potentiellement menacé.

Evitement des fautes. (Sûreté de Fonctionnement) Méthodes et techniques permettant de tendre vers un système exempt de fautes. Prévention des fautes et élimination des fautes.
Anglais : Fault avoidance

Exactitude. Conformité avec la réalité, la vérité (correction, fidélité, justesse, rigueur, véracité, vérité, sincérité des comptes, authenticité, véridicité).
Pour une application, l'exactitude des données sera vérifiée tout au long des étapes suivantes : préparation des données d'entrée, conversion des données, transmission des données, matériel, validité des fichiers, données en cours de traitement, calculs, opérations physiques, corrections d'erreurs, distribution des états de sortie.
ITSEC : propriété d'une représentation d'une cible d'évaluation qui fait qu'elle reflète exactement la cible de sécurité pour ce système ou ce produit.
Anglais : Correctness, Accuracy

Exclusif. Un événement A est exclusif de l'événement B, si toute occurrence de A rend impossible l'occurrence de B.

Exigences (*ITSEC*). Phase du processus de développement dans laquelle la cible de sécurité d'une cible d'évaluation est identifiée et décrite
Anglais : Requirements

Exigences concernant le contenu et la présentation. (*ITSEC*). Partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui explicite ce que chaque élément de documentation identifié comme relevant de cette phase ou de cet aspect doit contenir
Anglais : Requirements for content and presentation

Exigences concernant les éléments de preuve. (*ITSEC*). Partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui définit la nature des éléments de preuve destinés à montrer que les critères relatifs à cette phase ou à cet aspect sont satisfaits.
Anglais : Requirements for evidence

Exigences concernant les procédures et les normes. (*ITSEC*). Partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui identifie la nature et/ou le contenu des procédures ou des approches normalisées qui doivent être adoptées ou utilisées quand la cible d'évaluation est en exploitation réelle.
Anglais : Requirements for procedures and standards

Expert. Spécialiste expérimenté et reconnu dans un domaine donné.
Anglais : Expert

Expertise. Analyse d'un système, d'une situation, etc. réalisée par un expert ; étendue de la connaissance d'un expert.
Anglais : Expertise

Exploitation. (*ITSEC*). Processus d'utilisation d'une cible d'évaluation.
Anglais : Operation

Exposition aux risques. C'est le résultat financier potentiel d'une menace qui fixe la fréquence probable de son occurrence.

Extorquer. C'est voler à quelqu'un par violence morale.

F.

Facilité d'emploi (ITSEC). Aspect de l'estimation de l'efficacité d'une cible d'évaluation qui couvre la commodité d'emploi de ses fonctions et de ses mécanismes de sécurité en exploitation réelle.
Anglais : Ease of use

Facilité de réalisation (MELISA). Facilité avec laquelle une catégorie de sujets est capable de réaliser l'événement conduisant à la réalisation d'une menace type.

Facteurs d'action. Ensemble des conditions des causes et des principes qui déterminent et, quand on les découvre, permettent d'expliquer la nature, les origines et les limites d'une action quelconque. Parmi les facteurs d'action les plus communs on peut citer :

- la situation objective du sujet de l'action (opérateur, entreprise, etc.) au moment de la décision d'agir ;
- les moyens matériels, techniques, financiers et institutionnels dont on peut disposer ;
- les obstacles matériels, techniques, financiers et institutionnels qui peuvent se présenter ;
- l'état d'esprit, les qualités physiques, morales et intellectuelles des agents et partenaires de l'activité concernée.

Anglais : Action factors

Facteurs de sécurité (MARION). L'ensemble des éléments techniques, organisationnels et humains ayant une influence sur la sécurité du système d'information. La méthode MARION recense 27 facteurs (22 en prévention, 5 en protection).
Anglais : Security factors

Factorisation. Ensemble des facteurs premiers d'un nombre (ou d'un polynôme). Recherche et détermination de cet ensemble.
La sécurité de l'algorithme de chiffrement RSA est basé sur la complexité (c'est-à-dire la difficulté) de la factorisation des produits de deux grands nombres premiers.

Faille (vice caché). Défaut d'un système permettant de contourner ses mécanismes de protection ou d'en réduire l'efficacité.
Anglais : Flaw

Falsification. Altération volontaire dans le but de tromper.
Cas particuliers : falsification de données, falsification de programmes.

Faute. (Sûreté de Fonctionnement) Cause adjugée ou supposée d'une erreur. Cause d'erreur évitée ou tolérée. Conséquence de la défaillance d'un composant pour le système qui le contient ou pour le, ou les composants qui interagissent avec lui.
Anglais : Fault

~ **accidentelle**. Faute apparaissant ou créée de manière fortuite. - Anglais : Accidental fault

~ **active**. Faute qui produit une erreur. - Anglais : Active fault

~ **corrélées**. Fautes attribuées à une cause commune. - Anglais : Related fault

~ **de conception**. Résultat d'imperfections commises soit au cours du développement d'un système (l'expression des besoins à la recette, compris l'établissement des procédure d'exploitation ou de maintenance), soit au cours de modifications ultérieures. - Anglais : Design fault

~ **dormante**. Faute interne non activée par le process de traitement. - Anglais : Dormant fault

~ **douce**. Faute éliminée directement par le traitement d'erreur. - Anglais : Soft fault

~ **dure, ou solide**. Faute nécessitant d'être passivée. - Anglais : Hard or solid fault

~ **externe**. Faute résultant de l'interférence ou des interactions d'un système avec son environnement physique ou humain. - Anglais : External fault

~ **humaine**. Conséquence d'imperfections humaines. - Anglais : Human-made fault

~ **indépendantes**. Fautes attribuées à des causes différentes - Anglais : Independant faults

~ **intentionnelle**. Faute résultant d'une action délibérée - Anglais : Intentional fault

~ **intermittente**. Faute temporaire interne. Faute dont les conditions d'activation ne peuvent être reproduites ou qui se manifeste suffisamment rarement. - Anglais : Intermitent fault

~ **interne**. Partie de l'état d'un système qui, lorsqu'activée par les traitements, produira une ou des erreurs. - Anglais : Internal fault

~ **opérationnelle**. Faute apparaissant durant l'exploitation système. - Anglais : operational fault

~ **permanente**. Faute dont la présence n'est pas reliée à des conditions ponctuelles, interne (processus de traitement) ou externes (environnement). - Anglais : Permanent fault

~ **physique**. Conséquence de phénomènes physiques adverses. - Anglais : Physical fault

~ **temporaire**. Faute qui n'est présente que pour une durée limitée. - Anglais : Tempory fault

~ **transitoire**. Faute temporaire externe. - Anglais : Transient fault

Faux. En logique,une des deux valeurs de vérité, l'autre étant VRAI
Anglais : False

Faux en écriture. faute commise sur un document écrit et pouvant être :
un faux matériel : modification de la réalité écrite par contrefaçon, simulation, omission, fausse signature, ...
un faux intellectuel : écriture d'une réalité modifiée par exemple fabrication d'un faux certificat, d'une fausse attestation, d'un faux diplôme, ou fabrication de documents authentiques comportant des faits contraires à la réalité.

Fiabilité. (Sûreté de Fonctionnement) Sûreté de fonctionnement selon le point de vue de la continuité du service délivré. Mesure de la continuité de la délivrance d'un service correct ou, de façon équivalente, mesure du temps jusqu'à défaillance.
Anglais : Reliability

Fiabilité stabilisée. (Sûreté de Fonctionnement) Aptitude du système à délivrer un service correct est préservée (identité stochastique des temps jusqu'à défaillance successifs).
Anglais : Stable reliability

Fichier. Ensemble d'informations. Par extension peut désigner le support matériel de l'information.
Anglais : File

Fichier d'audit. Fichier de journalisation des événements d'un système (notamment des événements traitant de la sécurité)
Anglais : Audit file

Flot. Elément en déplacement. Exemples : flot d'informations, flot de données, flot de clés.
Anglais : Stream, flow (cf information flow, flow control model)

Flot de clés. En cryptographie, suite d'informations secrètes créées à l'aide d'un générateur de pseudo-aléa et utilisées par un dispositif de calcul pour obtenir le cryptogramme. Chaque élément de cette suite est appelé "clé de rang".
Anglais : key-stream

Flux. Flot entre deux points identifiés
Anglais : Flow

Fonction. C'est le rôle joué par un élément dans un ensemble ; que celui-ci soit matériel, organique, économique, social ou intellectuel : fonctions de l'entreprise (technique, commerciale, financière, sécurité, logistique...), fonction d'autorité, fonction mathématique...
L'accomplissement d'une fonction consiste en opérations effectuées au sein d'un système, quelque soit la nature de celui-ci :organisme , économie, société, culture, institution.
Selon le fonctionnalisme, un système ou une structure peuvent être définis par leur mode de fonctionnement et par l'ensemble des fonctions qui les constituent. Les comportements dysfonctionnels sont, tôt ou tard, éliminés
Anglais : Function

Fonction auto-reproductrice. Une fonction auto-reproductrice possède la faculté de créer des répliques d'elle-même au sein d'autres programmes. Elle est difficile à éliminer car elle se multiplie et l'oubli d'un seul exemplaire suffit pour que le système soit de nouveau totalement contaminé, car chaque copie peut à son tour se reproduire.

Fonction d'un système.(Sûreté de Fonctionnement) Ce à quoi un système est destiné.
Anglais : Function (system ~)

Fonction de confiance. Fonction dont le déroulement est est accord avec la politique de sécurité.
Anglais : Trusted function

Fonctions à déclenchement différé. Une fonction à déclenchement différé est une fonction d'un programme dont l'exécution est différée jusqu'à ce qu'une certaine condition soit remplie : date, heure, durée, comptage, événement particulier, concomitance d'événements, etc.

Fonction illicite. Fonction d'un programme inautorisée, indocumentée et qui ne participe en rien aux objectifs officiels du programme. Une fonction illicite:

- a un caractère malveillant : la fonction peut avoir un effet destructeur logique (par exemple effacement de fichiers), plus rarement un effet destructeur physique (par exemple variations rapides et extrêmes du bras de lecture disque), un effet inhibiteur (saturation d'un canal I/O, saturation mémoire, boucle de programme) ou un effet purement modificateur ; elle peut en outre entraîner le vol ou la divulgation de données (par exemple, interception de mots de passe lors des modifications, avant chiffrement).
- n'est d'aucune utilité pour toute autre personne, morale ou physique, que ses concepteurs,
- s'exécute sans que l'utilisateur en ait conscience,
- est sanctionnée par la loi n° 88-19 du 5 janvier 1988 contre la fraude informatique.

Toute infection informatique utilise une ou plusieurs fonctions illicites.

Fonction(s) de protection. La protection se décompose en six fonctions principales qui doivent toutes être appliquées, pour assurer la protection des systèmes d'information - l'évitement, la dissuasion, la prévention, la détection, la reprise, la correction.
Anglais : Protection Functions

Fonction(s) de sécurité. Caractéristique active d'une cible d'évaluation qui contribue à la sécurité.
Anglais : Security functions

Fonction temps réel. (Sûreté de Fonctionnement) Fonction qui doit être remplie dans des intervalles de temps finis régis par l'environnement.
Anglais : Real time function

Fonctionnalité de sécurité. (ITSEC) Les fonctions de sécurité d'une cible d'évaluation prises dans leur ensemble.
Anglais : Security Function

Forclusion. Perte de la faculté de faire valoir un droit par l'expiration d'un délai.

Formel. Ce qui est exprimé avec précision et sans équivoque.
En logique, un énoncé formel est exprimé dans un langage formalisé, c'est-à-dire complètement spécifié par des règles d'écriture mécaniques, excluant tout recours à l'interprétation (ou aux interprétations s'il y en a plusieurs) de ce langage.
Ex : les langages de programmation sont des langages formel.
Plus généralement, est formel, tout ce qui se rapporte à la forme par opposition au fond : la syntaxe est formelle alors que la sémantique s'intéresse à la signification.

Fouine.(bidouilleur). Personne s'intéressant fortement au fonctionnement et modification des systèmes.
Anglais : Hacker

Fourniture. Le terme fourniture englobe :
- les matériels (matières premières, produits semi-ouvrés ou finis pièces, composants, équipements, systèmes...),
- la documentation et les logiciels,
- les prestations de service.

Fraude. Action en générale faite de mauvaise foi par un tiers (tromperie, falsification, dol, escroquerie). Plus spécifiquement tricherie ou utilisation non autorisée d'un système. Action de déjouer un système de protection sans le saboter.
Voir aussi : détournement
Anglais : Fraud

Fréquence. Nombre d'occurrences dans une période de temps donnée.
Anglais : Frequency

Fréquence maximale d'anomalie. Nombre maximal d'anomalies acceptable pour une période donnée.
Anglais : Fault-rate threshold

G.

Garantique. Se définit comme l'utilisation commerciale des techniques de sécurité, notamment la cryptologie.

Générateur d'options stratégiques. Outil conceptuel qui peut permettre d'identifier les systèmes d'information à vocation stratégique.
Le générateur fixe d'abord l'attention sur une série de cibles stratégiques et sur les coups stratégiques qui peuvent permettre de les atteindre. les applications informatiques qui peuvent appuyer ou définir des coups stratégiques, et ces coups eux-mêmes sont en quelque sorte pointés sur les cibles stratégiques. Trois catégories de cibles :

- les fournisseurs
- les clients
- les concurrents.

Générateur de pseudo-aléa. Matériel ou logiciel exécutant un algorithme produisant une séquence de nombres ou de symboles pseudo-aléatoire.
Anglais : Pseudo-random generator

Génération de clés. Opération permettant de créer les clés nécessaires aux systèmes cryptographiques.
Anglais : Key generation.

Génie logiciel. Discipline recouvrant l'ensemble des méthodes, des outils et des techniques d'aide à la conception, à la spécification, à la production, à l'évaluation, à la validation et à la maintenance de logiciels.
Anglais : Software engineering, software environnement (CASE)

Génie logiciel (atelier de). Ensemble d'outils informatiques d'aide à la conception, à la spécification, à la production, à l'évaluation, à la validation et à la maintenance de logiciels, utilisable sur un ou plusieurs matériels.
Anglais : Software engineering Workshop

Gestion. Mise en œuvre, manipulation selon des règles bien définies. Les processus de gestion mettent en œuvre l'action humaine collective, dans le cadre de ce qu'il est convenu d'appeler des organisations.

Gestion des clés. Principes et/ou procédures, automatisés ou non, relatifs à la génération, le stockage, la distribution, l'application, l'utilisation, l'archivage et la destruction des clés cryptographiques.
Anglais : Key management

Gestionnaire : personne ou groupe de personnes, responsables des activités d'un organe (division, service, bureau, atelier, équipe, projet). Le gestionnaire décide, fait réaliser, et évalue les réalisations.

GFA
voir groupe fermé d'abonnés

GFU
voir groupe fermé d'usagers

Granularité. Taille élémentaire des ensembles d'objets, d'informations ou de données, considérés comme un tout pour les besoins de la sécurité ou de l'intégrité.
Anglais : Granularity

Gravité (MELISA). Gravité de la conséquence pour l'entreprise, de la réalisation de la menace. Cette gravité peut être potentielle ou effective.

Gravité potentielle : considérée indépendamment de tout élément de prévention ou de protection opérationnel ou prévu, et de toute réaction possible en cas de détection de l'occurrence de l'événement.
Gravité effective : atténuée par la détection de l'occurrence de l'événement et par les réactions effectivement déclenchées par cette détection.

Groupe fermé d'abonnés (GFA). Regroupement d'abonnés partageant un même service accessible uniquement à ces abonnés. Désigne une option de sécurité proposée par TRANSPAC et basée sur ce principe.
Anglais : Closed subscriber group

Groupe fermé d'usagers (GFU). Equivalent du groupe fermé d'abonnés. Désigne sur un réseau public commuté un ensemble d'abonnés disposant d'un sous-ensemble de numérotation inaccessible aux autres usagers.
Anglais : Closed user group.

H.

Hacker. (anglais)
voir fouine

Habilitation. Autorisation, délivrée à un utilisateur d'un système, d'accéder à certaines données classifiées de ce même système. Implicitement. Ce terme englobe tous les niveaux d'habilitation du confidentiel au très secret. Chaque organisation à ses propres définitions de l'habilitation et des niveaux associés. Néanmoins, on utilise généralement les niveaux de classification suivants : très secret, secret, confidentiel, diffusion restreinte pour l'entreprise ou pour l'industrie (groupement de plusieurs entreprises sur un projet. Par exemple Airbus)
Anglais : Clearance

Habilitation de session. Autorisation délivrée à un sujet pour une session
Anglais : Session clearance

Harmonique. Onde de fréquence multiple entier de la fondamentale. Les conditions de propagation des harmoniques peuvent être très différentes de la fondamentales (surtout pour les ondes électromagnétiques), sont souvent à l'origine d'écoute à distance.

Homologation. Procédure d'autorisation délivrée par une administration pour mettre en service un type d'équipement.
Anglais : Approval

I.

Icône (pictogramme, image). En informatique, désigne la représentation graphique d'une fonction ou d'un objet (cf interface graphique).
Anglais : Icon

Identifiant. C'est une propriété ou un ensemble particulier de propriétés d'un individu ou d'une relation telle qu'il n'existe pas deux occurrences de cet individu ou relation pour lesquelles cette propriété puisse prendre une même valeur. Sa définition résulte le plus souvent d'un choix de gestion. Il peut être :

- soit, un code plus ou moins secret (exemple : n° de terminal physique et logique),
- soit, un état physique (empreintes digitales) ou logique (nom de l'état civil).

Anglais : Identifier

Identificateur distinctif (AFNOR-ISO). Information qui distingue une entité sans ambiguïté dans le processus d'authentification.
Anglais : distinguishing identifier

Identification. Procédure par laquelle on s'assure de l'identité d'un correspondant. L'élément primordial dans le contrôle d'accès est l'établissement d'une identification formelle et unique pour chaque individu ou entité à qui l'accès doit être accordé. Ceci est généralisé en deux étapes :

- la présentation d'une identité prétendue par un individu,
- la présentation d'une information détenue personnellement pour vérifier l'identité prétendue.

Il y a trois méthode de base permettant de vérifier l'identité prétendue d'un individu, qui reposent sur la reconnaissance :

- d'un élément connu de l'individu (mot de passe ou un ensemble de faits appartenant a son passé)
- d'un élément possédé par l'individu (clé, carte d'accès, badge)
- d'un élément au sujet de cet individu (empreintes digitales, voix, signature, iris de l'oeil, mesures anthropométriques du visage, aurogramme, etc...).

Anglais : Identification

Identification de l'utilisateur. Identification d'un utilisateur par un identifiant reconnu par le système.
Anglais : User-id

Impact. Quantification des conséquences d'un sinistre (niveau conventionnel dans le cadre d'une échelle qui parfois peut être illustré en francs).

Implémentation (ITSEC). Phase du processus de développement dans laquelle la spécification détaillée d'une cible d'évaluation est traduite en matériels et logiciels réels.
Anglais : Implementation

Imputabilité. Caractère de ce qui est imputable. Possibilité de considérer une personne comme l'auteur d'une infraction.
ITSEC : Voir journalisation
Anglais : Imputability

Incertitude. Inverse de l'information. cf information.

Incident. Suite d'événements conduisant à un état final caractérisé par une perte dans le système et/ou son environnement.

Incidente. Information donnée involontairement par un émetteur à un récepteur, à l'occasion d'un échange ayant un tout autre objectif.

Indicateurs : Ce sont des moyens de mesure, quantitatifs ou efficacité, délais, risques...) liés à la vie d'un organisme.
La mise en évidence de ces variables et leur mesure permettent d'apprécier le fonctionnement de chaque composant de l'organisme à un instant donné. L'auditeur est amené à étudier les paramètres de la vie de l'organisme (sociaux, économiques, informationnels d'activité, de qualité...) par comparaison avec des valeurs habituelles, des règles de l'art, des standards, des ratios, formuler un diagnostic, déterminer un traitement.
Dans le cadre de la planification informatique, il sera amené de même à analyser le fonctionnement des applications, à définir les remèdes à apporter (nouvelles applications, projets à mettre en oeuvre, évolution des matériels et des logiciels...) avec les plans correspondants année par année, compte tenu de l'impact prévisible sur le fonctionnement de l'organisme. Enfin de façon périodique ou même en permanence, l'auditeur devra suivre l'avancement des travaux et l'évolution des différents indicateurs par rapport aux valeurs initiales et aux valeurs-objectifs ou prévisionnelles fixées, de façon à pouvoir prendre les décisions qui s'imposent.
Indicateurs de résultats : mesurant l'activité productrice : quantité ou qualité de la production, délais...
Indicateurs de moyens : mesurant la consommation des ressources : hommes, machines, énergie, immatériel, services, finances. On est généralement amené à définir et utiliser des indicateurs composés de type efficacité (résultats/moyens) ou de rentabilité (bénéfices/coûts).
Indicateurs de risque : permettant, indépendamment de toute mesure d'efficacité ou de rentabilité, d'apprécier le risque (probabilité d'incident ou d'échec) et les enjeux correspondants pour une application informatique ou un projet.
Indicateurs ou spécifiques de fonctionnement : mesurant toutes les variables intéressantes de l'organisme, suivant le point de vue où l'on se place ; on étudiera ainsi les aspects :

- économiques et financiers
- sociaux
- technologiques.

Anglais : Index, indicator

Indice de risque. Différence entre l'habilitation minimum (ou droit d'accès de l'utilisateur) et la classification maximum des données traitées par le système. Algorithme variable suivant les méthodes.
Anglais : Risk index

Infections informatiques (CLUSIF). Elles regroupent : chevaux de Troie, bombes logiques, vers et virus. Ce sont des programmes ou des parties de programme malveillant qui, loin de résulter en une exploitation utile pour l'utilisateur, sont destinés à perturber, à modifier ou à détruire tout ou partie des éléments indispensables au fonctionnement normal de l'ordinateur.
Elles utilisent un ensemble de fonctions caractéristiques :

- fonction illicite,
- fonction d'auto-reproduction,
- fonction de déclenchement différé.

Infographie. Désigne l'ensemble des matériels et procédés liés à la production de dessins, images et graphiques au moyen de périphériques spécialisés après traitement informatique.
Anglais : Computer graphics

Information.
a) - Elément de connaissance effective, obtenu par la recherche, observation ou études, susceptible d'être représenté à l'aide de conventions pour être à la base de la communication des connaissances.
Toute information peut être considérée sous deux aspects :

- celui de sa signification qu'on appelle son contenu sémantique,
- celui de sa structure qu'on appelle syntaxe.

b) - Renseignement fourni par un agent émetteur ou source à l'intention de destinataires ou récepteurs et donnant la réalisation d'un événement.
c) - Propriété purement quantitative d'un ensemble d'événements susceptibles d'être classés ou organisés. Le nombre d'opérations requises pour que le classement ou l'organisation cohérente de cet ensemble soit effectué est la mesure inverse de la quantité d'information contenue dans cet ensemble. La somme des incertitudes de la mise en ordre de l'ensemble (ou de la prévision de l'événement à venir) est l'entropie du système.
En informatique, on distingue souvent l'information traitée, constituée par les programmes et les données de l'utilisateur, de l'information traitante constituée par les logiciels nécessaires au traitement.

- Informations *primaires* (à la source) ou *fatales* qui sont généralement enregistrées pour les actes de gestion.
- Informations *modèles* (de synthèse) qui sont structurées pour alimenter les modèles de décision utilisés par l'organisation. Elles proviennent le plus souvent de l'extérieur.
- Informations *aléatoires* (autonomes), elles sont requises par un décideur en dehors de tout programme général.

Anglais : Information

Information d'authentification de l'échange (AFNOR-ISO). Information échangée entre le déclarant et le vérificateur au cours du processus d'authentification de l'entité principale.
Anglais : Exchange authentication information (exchange AI)

Information d'authentification pour la vérification (AFNOR-ISO). Information utilisée par le vérificateur pour vérifier une identité déclarée lors de l'échange de l'information d'authentification.
Anglais : Verification authentication information (verification AI)

Information classifiée. Information stratégique qui est possédée, utilisée ou produite sous le contrôle des autorités d'un pays. Par extension, information (ou matériel) stratégique d'une entreprise qui est possédée, utilisée, produite, et classifiée par celle-ci.
Anglais : Classified information

Information confidentielle. Information sensible ne devant être communiquée qu'aux personnes habilitées à la connaître.
Anglais : Confidential information

Information sensible. Information (classifiée) qui selon la décision d'une autorité compétente, doit être protégée (disponibilité, intégrité, confidentialité) parce que sa révélation inautorisée, son altération, sa perte ou sa destruction causeraient des dommages au bon fonctionnement de l'entreprise.
Anglais : Sensitive information

Information stratégique. Information sensible dont l'importance est telle pour la pérennité de l'entreprise, qu'il convient d'en assurer tout particulièrement la disponibilité, l'intégrité et la confidentialité.

Information (théorie de l'). La théorie de l'information a pour objet de définir et d'étudier les quantités d'information, le codage de celles-ci, les canaux de transmission, etc. Dans ce contexte, quantité élémentaire permettant de réduire l'incertitude de la mise en ordre d'un ensemble de données.
Anglais : information theory

Informatique. Science du traitement rationnel, notamment par machine automatique, de l'information considérée comme le support des connaissances et communications dans les domaines technique, économique et social. (Académie française, avril 1966). L'informatique couvre concrètement quatre activités :

- *L'informatique de gestion*, pour tout ce qui touche aux affaires et à la gestion d'une entreprise : comptabilité, gestion du personnel, gestion commerciale, gestion des stocks, etc.
- *L'informatique graphique*, soit la représentation de données et des résultats sous forme de graphes ou d'images.
- *L'informatique industrielle*, qui est l'utilisation de l'informatique en milieu industriel pour la conduite des processus de fabrication.
- *L'informatique scientifique*, ou utilisation de l'informatique pour les calculs scientifiques

Anglais : computer science

Infraction. En droit pénal, c'est l'acte ou l'omission interdits par la Loi sous menace d'une peine. C'est donc la violation d'un engagement ou de la Loi. L'infraction s'appelle contravention, délit ou crime, selon qu'elle est passible de peines de simple police, correctionnelles ou criminelles. On distingue quatre éléments généraux dans l'infraction : l'élément légal, l'élément matériel, l'élément moral, l'élément injuste. Le Droit des Affaires recense les infractions suivantes : le vol, l'escroquerie et les infractions voisines (extorsion, chantage), l'abus de confiance (détournement, dissipation) et les infractions voisines (abus de blanc seing, détournement d'objets saisis, détournement d'objets donnés en gage), le recel de choses, les faux en écritures, la corruption.

Initiateur d'authentification (AFNOR-ISO). l'entité qui engage l'échange d'authentification.
Anglais : Authentication initiator

Instruction. Elle constitue le plus petit élément non décomposable d'un programme ; une instruction est un ordre donné à l'ordinateur. Un programme est une suite logique d'instructions.
Anglais : Instruction, statement

Intégrité. Propriété qui assure l'inaltération des informations lors de leur stockage, leur transport ou l'exécution des traitements. Recouvre en fait plusieurs notions :

- exactitude et réalité : l'information initiale a-t-elle été fournie par quelqu'un qui en avait le pouvoir, est-elle exacte, n'a-t-elle pas été modifiée par erreur (volontaire ou involontaire),
- exhaustivité : toutes les informations produites ont-elles été réceptionnées et traitées,
- auditabilité : s'assurer du bon déroulement des traitements et de leur exactitude,
- non répudiation : avoir des moyens de preuve dans l'exécution des fonctions (un message a été émis et reçu).

L'intégrité est donc l'état d'une chose qui est demeurée intacte (synonyme : intégralité, plénitude, totalité). En matière de sécurité, intégrité est plus qualitatif qu'intégralité, réservé généralement à ce qui est mesurable (entier et total). C'est la deuxième des grandes propriétés de la sécurité des systèmes d'information et informatiques (classification DIC).
Sûreté de fonctionnement : Fait de demeurer intact, donc d'éviter modifications ou suppressions indésirées.
Anglais : Integrity

Intégrité des données. L'intégrité des données d'un système d'information est vérifiée si elles traduisent fidèlement les données du réel représenté (au sens comptable) par ce système d'information. Elle traduit donc la qualité des données qui n'ont pas été altérées, détruites ou perdues par accident ou malveillance.
La notion d'intégrité des données s'applique non seulement à chacune d'entre elles, mais aussi à leur ensemble pour éviter les absences ; le mot intégrité concerne à la fois l'authenticité, l'exactitude, l'exhaustivité et la présence de chaque donnée mémorisée et sa complétude par rapport au champ du réel que l'on veut représenter. Ainsi des programmes modifiés illégitimement, des fichiers dégradés

représentent un réel danger pour l'entreprise. Le souci d'intégrité des données traitées en ordinateur à deux origines :

- d'une part le processus de transformation de l'information depuis l'entrée des données jusqu'à l'édition des résultats après calcul (saisie initiale, contrôle près du point d'origine, conciliation des entrées et des sorties, réinsertion des données corrigées,contrôles de démarcation...), pour la plupart des applications de gestion, est un processus en "boucle ouverte"; Rares sont les entreprises qui vérifient par un autre algorithme la valeur des résultats calculés par le programme lui-même;
- d'autre part, la souplesse d'évolution des applications présente, en contre partie, une certaine facilité de modifications frauduleuses. Dans le cas du transport de données, l'intégrité peut être assurée par la mise en œuvre d'une fonction de scellement. Les mécanismes d'intégrité sont décrits dans la norme IS0 8730. Ils sont basés sur l'algorithme DES (IS 8731-1) qui permet d'obtenir une compression des données appelée "sceau".

Anglais : Data integrity

Interface. Jonction entre deux matériels ou logiciels leur permettant d'échanger des informations par l'adoption de règles communes, physiques ou logiques.
Anglais : Interface

Interface graphique. Qualifie un mode de communication entre ordinateur et utilisateur utilisant pour l'essentiel des pictogrammes (ou icônes) et une souris, ce qui limite l'utilisation du clavier (caractéristique des machines APPLE au début, ce type d'interface tend à se répandre de plus en plus à travers des logiciels tels que WINDOWS ou X-WINDOWS).

Intrus. Qui s'introduit quelque part sans avoir qualité pour y être admis, sans y avoir été admis.
Anglais : Intruder

Intrusion. Action de s'introduire dans une société, dans un emploi, dans un système. On peut citer plusieurs types d'intrusion :

- introduction dans un système sans y être admis,
- personne autorisée du système essayant d'élargir ses privilèges
- personne autorisée utilisant ses privilèges à des fins autres que ceux accordés.

Sûreté de fonctionnement : Faute externe opérationnelle intentionelle.
Anglais : Intrusion

Irrépétible. Terme de droit. Qui ne peut être répété, redemandé, des frais irrépétibles.

J.

JCL. Terme utilisé au départ par IBM pour désigner les commandes du système d'exploitation. Le jargon informatique a adopté ce sigle pour tout système (IBM ou non).
Anglais : Job Control Language

Jeton (AFNOR -ISO). Information d'authentification transportée durant l'échange d'authentification.
Anglais : Token

Journal. Fichier dans lequel le système d'exploitation mémorise les opérations des utilisateurs d'un système informatique et les modifications réalisées sur les ressources.
Anglais : Log

Journal des anomalies. Relevé des anomalies ou liste d'incidents ou d'erreurs obtenu par un logiciel de surveillance et reflétant la séquence d'états et le contexte précédant immédiatement l'apparition des défauts.
Synonyme : relevé des défauts
Anglais : fault trace

Journal d'audit. C'est un fichier qui enregistre chronologiquement tous les événements effectués par une entité donnée (ordinateur et périphériques, système d'exploitation, moniteur transactionnel, moniteur interactif, système de gestion de base de données, progiciel d'aide à la sécurité, etc.). Il constitue un cheminement logique reliant une suite d'événements et permettant de retrouver les transactions qui ont été effectuées. Il y a deux types de journaux : le journal d'audit comptable et le journal d'audit d'exploitation.
Anglais : Audit trail, journal, log

Journal d'audit comptable. Il enregistre tous les événements et opérations d'une base de données, des différents moniteurs et autres. Ce fichier permet par exemple :

- de suivre les données d'une transaction tout au long de ses traitements,
- de reconstituer, après incident ou panne, toutes les opérations sur les données.

Anglais : Accounting audit trail

Journal d'audit d'exploitation. Il enregistre tous les événements et opérations qui ont lieu durant le déroulement des opérations système. Il permet de suivre, le déroulement des opérations, l'emploi des ressources, la gestion des performances ainsi que tous les accès au système.
Anglais : Operation audit trail

Journalisation de sécurité. Rassemble toutes les fonctions destinées à enregistrer l'exercice des droits d'exécutions d'actions relevant de la sécurité
Anglais : security log

L.

Langage de quatrième génération (L4G). Langage évolué permettant une réalisation rapide des applications y compris, dans certains cas, par l'utilisateur lui-même.
Anglais : Fourth generation language

Lettres de créance (laisser-passer). Données transmises par une entité pour établir l'envoi de l'identification et les droits d'accès.
Anglais : Credentials

Livraison (ITSEC). Processus par lequel une reproduction de la copie témoin d'une cible d'évaluation est transférée du développeur à un client.
Anglais : delivery

Logiciel. Ensembles des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitements de données
Anglais : Software

Logiciel d'audit. De façon générale, logiciel d'interrogation doté des fonctions nécessaires à l'auditeur. Peut aussi désigner un ensemble de procédures écrites dans un langage traditionnel (procédural) pour remplir certaines fonctions spécifiques d'audit.
Anglais : Audit software

Logiciel d'interrogation. Programme permettant, avec une programmation relativement simple, des interrogations sur des fichiers selon des critères variés. Outil très utilisé en Audit.
Anglais : Query software

Logiciel de surveillance. Logiciel qui assure la surveillance d'un système informatique pour détecter, enregistrer et éventuellement corriger des erreurs. Ce logiciel peut posséder des fonctions d'alerte.
Anglais : Error control software

Logique maligne. (Sûreté de Fonctionnement) Faute de conception intentionnelle.
Anglais : Malicious logic

Lucifer. Méthode de chiffrement IBM dont le D.E.S. est dérivé.
Anglais : Lucifer

M.

MAC. Message Authentication Code - Mandatory Access Control
Cf Code d'authentification du message

Machine virtuelle. Fonctionnalité d'un système d'exploitation qui permet à chaque utilisateur de se servir du système comme s'il disposait de toutes les ressources du matériel.
Anglais : Virtual machine

Maille d'étude. Caractérise le niveau analytique de l'étude de l'existant (données et traitement) ou de la représentation des solutions futures (données et traitements). La maille d'étude sert à définir le niveau de description des différentes cibles qui sont abordées successivement au cours de l'élaboration du schéma directeur.

Mainframe. Ordinateur puissant à vocation universelle utilisé comme système central de traitement de l'information dans les grandes entreprises ou administrations.
Anglais : Mainframe

Maintenabilité. Capacité de pouvoir localiser et réparer les éléments défaillants en cours de fonctionnement ou de pouvoir modifier efficacement les applicatifs.
Sûreté de Fonctionnement : Mesure de la délivrance continue d'un service incorrect ou, de façon équivalente, mesure du temps jusqu'à restauration du service depuis la dernière défaillance survenue.
Sûreté de Fonctionnement : Facilité avec laquelle la maintenance d'un système peut être effectuée. Mesure de la délivrance continue d'un service incorrect ou, de façon équivalente, mesure du temps jusqu'à restauration du service depuis la dernière défaillance survenue.
Anglais : Maintenability

Maintenance. Ensemble d'actions tendant à prévenir ou à corriger les dégradations d'un matériel ou logiciel afin de maintenir ou de rétablir sa conformité aux spécifications.
La maintenance des applications représente les modifications apportées aux programmes, aux documents, aux fichiers ou à la base de données, et au système de communication - Anglais : Maintenance

~ **corrective**.(Sûreté de Fonctionnement) Actions entreprises durant la vie opérationnelle d'un système destinées à préserver ou améliorer son aptitude à délivrer un service en conformité avec la spécification. - Anglais : Corrective maintenance

~ **curative**. (Sûreté de Fonctionnement) Maintenance corrective destinée à éliminer des fautes ayant produit des erreurs qui ont été signalées. - Anglais : Curative maintenance

~ **préventive**. (Sûreté de Fonctionnement) Maintenance corrective destinée a éliminer des fautes avant qu'elles ne produisent des erreurs. - Anglais : Preventive maintenance

Maître d'oeuvre. Généralement le maître d'oeuvre est le chef de projet et représente le domaine et le bureau d'études informatique. Il est responsable de la conception du système et de la qualité technique du projet. Il veille au respect de la méthodologie met en place les revues de projet, détermine les indicateurs de qualité... Les documents de synthèse sont établis sous sa responsabilité en accord avec le maître d'ouvrage.

Maître d'ouvrage. Utilisateur final et bénéficiaire de l'investissement qui, quel que soit le type d'application :

- Initie l'opération et s'engage sur sa rentabilité.
- Définit les besoins.

- Elabore la fiche d'investissement et, après accord, passe commande au maître d'oeuvre.
- Participe à l'élaboration de l'avant-projet et de l'étude détaillée.
- Suit la réalisation du produit et procède à sa recette.

Maliciel cf infection
Anglais : Malware

Malveillance. Intention de nuire, visée criminelle. Les actes de vandalisme de sabotage, de fraude, de détournement, d'altération volontaire, sont des actes de malveillance.

Malversation. Implique une gestion frauduleuse, quelle qu'en soit la forme. Elle désigne toute faute grave commise par cupidité dans l'exercice d'une charge, d'un emploi, dans l'exécution d'un mandat.

MARION (méthode). Ensemble méthodologique public conçu et développé à partir de 1984 par le CLUSIF (260 personnes représentant les principaux experts et utilisateurs français en 1991). La méthode vise à réduire les vulnérabilités en accidents, erreurs et malveillances afin d'assurer la sécurité dans les domaines de la Disponibilité, de l'Intégrité et de la Confidentialité. Les règles de base sont : cohérence des moyens de sécurité les uns par rapport aux autres et adéquation des moyens aux enjeux. La méthode comprend 6 étapes :

- Analyse des risques maximaux.
- Expression du risque maximum admissible.
- Analyse des moyens de sécurité (audit de survol d'environ 700 questions réparties en 27 facteurs). Opérationnelle et publique.
- Evaluation des contraintes.
- Choix des moyens.
- Orientations et rapport (Schéma directeur de sécurité des systèmes d'information).

Masquage de faute. (Sûreté de Fonctionnement) Effet résultant de l'application systématique de la compensation d'erreur, même en l'absence d'erreur.
Anglais : Fault masking

Masque. Programme inséré dans la ROM d'une carte à microprocesseur dont les fonctions essentielles sont :

- la gestion du protocole d'échange avec le lecteur
- les mécanismes d'accès à la mémoire
- la mise en œuvre des mécanismes de sécurité

Anglais : Mask

Mécanisme (ITSEC). Dispositif matériel ou logiciel qui réalise une fonction particulière.
Anglais : Mechanism

Mécanisme de contrôle d'accès. Dispositif matériel ou logiciel, procédure opérationnelle ou managériale et les diverses combinaisons de ceux-ci conçus pour détecter et prévenir les accès inautorisés au système
Anglais : Access control mechanism

Mécanisme critique (ITSEC). Mécanisme interne d'une cible d'évaluation qui n'est pas protégé par d'autres mécanismes et dont la défaillance créerait une vulnérabilité.
Anglais : Critical mechanism

MELISA (méthode). Ensemble méthodologique d'analyse de la vulnérabilité des systèmes d'information, conçu et développé pour la Délégation Générale pour l'Armement (DGA) dès 1984.

Dans les diverses étapes d'élaboration d'un schéma directeur de la sécurité des systèmes d'information, MELISA couvre les phases de sensibilisation, d'analyse de l'existant et d'aide à la détermination des mesures à mettre en place. MELISA couvre partiellement les phases de suivi et de contrôle de ce schéma directeur.

Mécanisme subversif. Mécanisme permettant la pénétration délibérée des protections d'un système à l'aide de chausse-trappes (portes dérobées), cheval de Troie et autres mécanismes.
Anglais : Subversive mechanism

Mémoire virtuelle. Fonctionnalité d'un système d'exploitation qui permet aux programmes de fonctionner, même si la taille physique est supérieure à celle de la mémoire centrale du matériel.
Anglais : Virtual memory

Menace : Evénement de probabilité non nulle pouvant nuire à la sécurité. Indice d'un danger ; ce danger lui-même. Un dommage quel qu'il soit, résulte toujours de la concrétisation d'une menace. Les problèmes de sécurité se réfèrent donc aux menaces qui pèsent sur les biens informationnels de l'entreprise, biens que l'on peut en ce sens recouvrir sous le vocable de "cible".
Toute action menée dans le cadre d'une politique de sécurité exige la connaissance la plus exhaustive possible exhaustive des menaces.
Menaces physiques : naturelles (tremblement de terre, crue, foudre, chaleur...), techniques (court circuits, panne d'alimentation...),
Menaces humaines : accidents, maladies, grèves...
Menaces sociales : involontaires (erreur, maladresse, insuffisance technique...), volontaires (divulgation, espionnage, vol, fraude, malversation, piratage, sabotage, malveillance, détournement..)
Anglais : Threat

Menace active. Menace de changement illicite de l'état du système (modification ou répétition de messages, insertion de faux messages, déguisement en une entité autorisée, et déni de service).
Anglais : Active threat

Menace passive. Menace sur la confidentialité des données qui ne provoque aucun changement de l'état du système (écoute ou enregistrement des données, accès en lecture à des informations créées, transmises, affichées, enregistrées, imprimées...).
Anglais : Passive threat

Menace type (MELISA). L'ensemble infini des menaces possibles est ramené dans MELISA à un ensemble fini de menaces caractéristiques, appelées menaces types, spécifiques de l'approche considérée (valeur intrinsèques-ressources sensibles , valeurs de nécessité-ressources vitales, bases spécialisées etc... Chaque menace type peut elle-même être l'aboutissement de divers scénarios appelés "événements".

Message : La signification d'un message est systémique. Chacun des acteurs et l'objet de la communication sont reliés entre eux dans *un système de communication*. Trois fonctions :

- en tant qu'*information* le message peut modifier le nombre et le domaine des alternatives, le choix ou la probabilité des choix,
- en tant que facteur d'*instruction* il modifie *l'efficacité du choix* (*processus d'apprentissage*),
- en tant que facteur *instituant* il modifie l'évolution des résultats recherchés et les critères de choix.

Les communications du *décideur* s'opèrent au travers des *réseaux* situés dans le produit des 3 sous-systèmes de finalisation, d'organisation et d'animation
Anglais : Message

Messages parallèles. Messages chiffrés avec le même flot de clés.
Anglais : Parallel messages

Mesures anti-infection. L'utilisation judicieuse de ces mesures doit permettre de réduire les risques liés aux infections informatiques à un « niveau acceptable ».
Les mesures à mettre en oeuvre se répartissent en cinq catégories :

- les mesures de *prévention* visent à réduire la probabilité qu'un système soit touché par une infection informatique,
- les mesures de *protection* visent à réduire les conséquences d'une infection informatique en limitant ses conséquences, en particulier entre l'instant de l'intrusion et celui de la détection,
- les mesures de *détection* et de diagnostic sont destinées à identifier l'infection, afin de pouvoir y appliquer les moyens d'élimination et de réparation adéquats,
- les mesures *d'élimination* visent à réduire les conséquences d'une infection informatique en réduisant le délai qui s'écoule entre détection et expulsion (disparition complète de l'infection informatique),
- les mesures de *réparation* visent à réduire les conséquences d'une infection informatique en optimisant et accélérant le processus de remise en état du système informatique.

Mesures de reprise. cf Reprise

Mesures de sécurité. Totalité des mécanismes et techniques qui protège les biens informationnels.
Anglais : Security measures

Méthode : C'est une démarche reflétant une philosophie générale définie et proposant des outils spécifiques pour manipuler des concepts aptes à donner une représentation fidèle des systèmes étudiés et à favoriser l'innovation. En informatique, démarche généralement structurée en étapes, qui permet d'analyser et de concevoir les systèmes d'information en utilisant des modèles, des langages et des outils.
Anglais : Method

Méthode d'audit de sécurité des systèmes d'information. A l'instar des autres méthodes d'audit, une méthode d'audit de sécurité des systèmes d'information et informatiques doit comprendre : des outils spécifiques (techniques : d'interview, de classification et de représentation, d'évaluation et de mesure du risque, heuristiques et statistiques...), des méthodes d'approche (analytique, psycho-analytique, psycho-sociologique, analyse et gestion des risques, systémique, holographique, tomogrammique, topologique, taxonomique, boxologique, globalistique...), la mise en œuvre d'un questionnaire type pour les cas généraux et d'un questionnaire spécifique pour le métier de l'entreprise, la présentation d'un rapport normalisé (points forts et faibles, degré d'acceptabilité du risque, recommandations, synthèse). Les méthodes MARION (publique) et MELISA (semi-publique) intègrent l'audit de sécurité des systèmes d'information et informatiques. La plupart des cabinets véritablement spécialisés en audit possèdent généralement leur propre méthode pour compléter significativement les résultats obtenus par MARION ou MELISA. Pour information, un bon questionnaire type doit couvrir environ 6.000 à 8.000 questions.
Anglais : Information System security audit method

Méthodologie. La méthodologie est la science qui s'efforce de découvrir, caractériser, classifier - et également de présenter - les méthodes qu'utilise l'esprit humain pour poser ou pour résoudre un problème. Elle entraîne une technique d'emploi de ces méthodes construite sur l'adaptation des caractères généraux de celle-ci (servant à leur classification) et sur les caractères généraux des problèmes.
Anglais : Methodology

MIPS. Nombre de millions d'instructions exécutées par seconde par un ordinateur. "Unité" très utilisée pour comparer des machines entre elles. A interpréter avec beaucoup de précaution.

Anglais: MIPS

Mode dégradé. Qualifie un système informatique qui continue de fonctionner avec des fonctionnalités réduites. Le mode de fonctionnement dégradé peut porter sur les fonctions et les sécurités du système informatique.
Anglais : Failsoft, graceful degradation

Modèle. Un modèle est un ensemble de concepts, de règles et de convention (graphiques en particulier) qui permettent de représenter des phénomènes. Il simule artificiellement une situation de la réalité qu'il tente de reproduire. La difficulté essentielle dans la réalisation d'un modèle tient à la détermination des variables ou paramètres dont il doit tenir compte, qui doivent y être incorporés.
Un modèle est donc la description des états possibles de l'univers du discours, comprenant en particulier les classifications, les règles et les contraintes.
Anglais : Model

Modèle conceptuel de données : Il permet de mettre en évidence la sémantique du système d'information, c'est-à-dire de donner à chaque mot du vocabulaire nécessaire à l'entreprise pour traduire son activité une signification précise, notamment en montrant les rapports qui existent entre le sens de chacun d'eux. Il met en évidence :

- des objets (ou individus) tels que : produit, fournisseur, commande, entrepôt.
- des relations, telles que : Réceptionner, stocker.
- des propriétés telles que : nom du produit, quantité en stock.

Il comprend :

- objets (ou individus)
- relations
- propriétés et identifiants
- cardinalité
- contrainte d'intégrité

Modèle conceptuel des traitements : il comprend :

- événements (ou résultats)
- synchronisations
- opérations
- un processus.

La description *conceptuelle des traitements* permet de décomposer l'activité de l'entreprise en *processus* qui s'appuient sur des événements qui sont le fondement même de cette activité, chaque *processus* étant alors décrit sous la forme d'un *enchaînement synchronisé d'opérations*, lesquelles trouvent leur description sous la forme d'un ensemble structuré de règles de gestion.
Elle met en lumière les cycles, les synchronisations, les points décisionnels, indépendamment des moyens ou de toute répartition des tâches par service ou *poste de travail* et fournit par là le support d'une réflexion sur le sens des actions mêmes par l'entreprise.

Modèle logique : Il consiste :

- Pour les données, à définir des structures logiques de données, des hiérarchies d'accès logiques.
- Pour les traitements, à les répartir entre les hommes et les machines et pour ceux qui sont automatisés, entre des modes conversationnels ou différés, centralisés ou répartis, ce qui conduit à définir des types de services ou postes de travail.

Modèle physique : Il consiste :

- Pour les données, à spécifier une organisation d'implantation en fichiers ou base de données utilisant tel moniteur.
- Pour les traitements automatisés, à décrire un découpage en programmes, et pour chaque programme la structure dans laquelle les traitements prévus s'intègrent.

Modèle de sécurité.

Modem (modulateur-démodulateur). Dispositif permettant de transformer des informations numériques en un signal analogique pouvant être transmis sur une liaison de données (réseau téléphonique par exemple).
Anglais : Modem

Monétique. Terme général s'appliquant à toutes les opérations concernant l'argent et qui utilisent des procédés électroniques, des cartes magnétiques, des cartes à mémoire, des TPV (terminaux points de vente),centre d'autorisation...

Mot de passe. Nom généralement donné à un code secret. Information confidentielle, souvent composée d'une chaîne de caractères, qui peut être utilisée pour l'authentification d'un usager ou d'une ressource ou pour le contrôle d'accès à une ressource. L'accès est autorisé lorsqu'il y a identité entre le mot de passe fourni par l'utilisateur et le mot de passe de référence détenu par le système lui-même.
Anglais : Password

Moyen : Elément employé sur le parcours de l'action pour atteindre un objectif ou réaliser un projet. La réalisation d'un dessein éloigné dans le temps exige d'atteindre des étapes intermédiaires déterminées qui mènent à lui. Ce sont les moyens qui, dans des cas déterminés, peuvent masquer le but lointain. La remarque de Vaihinger sur l'hypertrophie des moyens par rapport à la fin souligne que les hommes dans la réalisation de desseins intermédiaires déterminés, sont absorbés par une foule de ceux-ci et qu'ainsi les actions qui sont conçues comme les moyens pour atteindre le but lointain deviennent des objectifs autonomes.
D'une certaine façon, un parcours d'action détermine déjà les moyens qu'il faut mettre sur pied pour la réalisation d'un projet. L'estimation des moyens se fonde apparemment sur les postulats d'efficacité, d'économie, et pose aussi des question de moralité. La programmation et la planification reposent, entre autres, sur la nécessité de prévoir quels moyens il faut mettre en oeuvre et dans quelle succession. On les choisit en fonction de la sécurité et de ce qu'on nomme la probabilité d'efficacité.
Moyens informatiques : physiques (matériels, liaisons spécialisées, liaisons par RTC, Transpac,...), moyens logiques (programmes systèmes, utilitaires logiciels généraux,...).
Anglais : Means

Moyens de prévention (MARION). Moyens visant à réduire la probabilité d'occurrence d'un sinistre.

Moyens de protection (MARION). Moyens visant à réduire le coût d'un sinistre.

Moyens pour la sûreté de fonctionnement. (Sûreté de Fonctionnement) Méthodes et techniques permettant de fournir à un système l'aptitude à délivrer un service conforme à la spécification, et de donner confiance dans cette aptitude. Prévention des fautes, tolérance aux fautes, élimination des fautes, prévision des fautes.
Anglais : Means (for dependability)

Mystification. Tromperie effectuée par un préposé ou un tiers aux dépens d'un utilisateur autorisé pour s'approprier ses droits d'accès.
Anglais : Spoofing

N.

Niveau de risque. Une mesure qualitative de chacune des deux composantes du risque, la probabilité d'occurrence d'un événement redouté et le montant de la perte consécutive. Le niveau de risque est un moyen. Il sera toujours évalué arbitrairement, qu'il soit qualifié ou quantifié. Mais il faut le définir pour pouvoir atteindre notre but qui est de décider si ce niveau de risque est acceptable.

Catégorie I Négligeable : n'occasionne aucun préjudice au personnel, ni aucun dommage au système.

Catégorie II Marginal : Peut être neutralisé ou contrôlé sans préjudice au personnel ou dommage pour le système.

Catégorie III Critique : Occasionne des préjudices au personnel ou des dommages importants au système.

Catégorie IV Catastrophique : Occasionne la mort ou blessure grave au personnel, ou dommages majeurs pour le système et exige une action corrective et immédiate pour la survivance du personnel et du système.

Catégorie V Létal : peut entraîner la mort de l'entreprise.

Anglais : Risk level

Niveau de sécurité acceptable. Caractéristique d'un système, qui bénéficie d'un programme de sécurité, et dans lequel chaque événement indésiré présente un risque acceptable.
Anglais : Acceptable security level

Non-déduction. Modèle formel pour la sécurité développé aux États-Unis

Non-interférence. Modèle formel pour la sécurité développé aux États-Unis

Non-Répudiation. Impossibilité pour un correspondant de nier avoir reçu ou émis un message. La non-répudiation suppose l'authentification du correspondant et l'enregistrement irréfutable du message transmis (comme dans une carte à micro-circuit) ou auprès d'un tiers jouant un rôle de notaire (fonction de notarisation) ou d'arbitre. Cette fonction est supportée par la mise en oeuvre de la signature. Elle est généralement basée sur l'algorithme RSA. Les clés publiques ont un exposant égal à 3 et un modulo qui ne sera pas inférieur à 512 bits (dans un proche avenir les clés RSA seront de modulo supérieur à 512 bits).
Synonyme : acceptation obligatoire
Anglais : Non repudiation

Notarisation. Enregistrement des données chez un tiers de confiance pour recours ultérieur aux données et assurance de l'exactitude de leurs caractéristiques (contenu, origine, date, délivrance).
Anglais : Notarization

O.

Objet (ou individu) : C'est le reflet d'une entité manipulée par l'organisme, ou dont il s'accorde à reconnaître une existence propre en dehors de tout contexte.
Chaque objet est décrit par une liste de propriétés qui lui sont spécifiques, et à un ensemble donné de valeurs prises par ces propriétés correspond une occurrence de l'objet.
MELISA : nom générique donné aux différentes ressources matérialisant le système d'information de l'entreprise (les données elles-mêmes, leurs supports, les systèmes de traitement et l'ensemble des logiciels associés.
Anglais : Object

Obligatoire.
Anglais : Mandatory

Obtention de la sûreté de fonctionnement. (Sûreté de Fonctionnement) Méthodes et techniques destinées à fournir a un système l'aptitude à délivrer un service conforme au service conforme à la spécification. Prévention des fautes et tolérance aux fautes.
Anglais : Procurement (of dependability)

Oeuf (déposer un). Les pirates laissent parfois une trace de leur passage avec leur signature. Cela peut aller d'un simple message jusqu'à la bombe qui se déclenchera seule ou lorsque l'on essaiera de la désamorcer.

P.

Passivation (de faute). (Sûreté de Fonctionnement) Actions destinées à empêcher une nouvelle activation d'une, ou des fautes.
Anglais : Passivation (fault ~)

Pénétrabilité. Caractère de ce qui est pénétrable, perméable.
Anglais : Penetrability

Pénétration. Violation d'un système protégé.
Anglais : Penetration

Pérennité. Etat, caractère de ce qui dure. La pérennité des prestations informatiques peut être évaluée et maîtrisée par la mise en oeuvre de l'analyse et la gestion des risques et l'application des propriétés de la sécurité (voir classification DIC).
Synonyme : survivance, survivabilité
Anglais : Perenniality, everlastingness

Performabilité. (Sûreté de Fonctionnement) Mesure combinée performances-sûreté de fonctionnement.
Anglais : Performability

Péril. Etat, situation où l'on court de grands risques. Grandeur à deux dimensions associée à une phase précise de la vie du système et caractérisant un événement redouté par :

- sa certitude d'occurrence
- le montant de la perte consécutive.

Anglais : Peril

Perte. Préjudice quantifié.
Anglais : Loss

Pertinence de la fonctionnalité. Aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la mesure dans laquelle les fonctions et les mécanismes de sécurité de la cible d'évaluation contrent dans la pratique les menaces réelles ou possibles identifiées dans sa cible de sécurité.
Anglais : Suitability of functionality

Piège à ours (poser un). cf oeuf (déposer un)

Pirate. Terme générique employé pour désigner celui qui craque ou attente à l'intégrité d'un système informatique, de la simple duplication de disquette à l'accès aux ressources d'un centre de calcul (vol, pillage, plagiat des programmes et des brevets..).
Anglais : Hacker

Plan de sauvegarde. Ensemble de moyens prévus afin de minimiser les conséquences de toute perturbation importante de l'exploitation. Il permet le redémarrage des applications à la suite de la concrétisation d'un risque de type : panne, vol, sabotage matériel ou immatériel, erreur d'exploitation. Il comprend l'ensemble des règles de sauvegarde concernant tous les fichiers classés stratégiques lors de l'étude de sécurité. Il doit comporter notamment :

- le nombre de générations
- la périodicité
- le lieu et la durée de stockage des sauvegardes
- la prévision des sauvegardes en site dans des locaux physiques distincts des salles machines. Egalement des sauvegardes hors sites, externes à l'entreprise.

Ces règles sont définies lors de l'étude conceptuelle. Les sauvegardes en site sont incluses dans les procédures d'exploitation de l'application et automatiquement déroulées suivant les consignes des dossiers de fonctionnement.
Les sauvegardes hors site sont effectuées sous la responsabilité de l'exploitation.
Le plan de sauvegarde peut comprendre :

- le plan de reprise rapide
- le plan d'exploitation dégradé sur le site
- le plan de substitution

Anglais : Safety plan

Plan de sécurité. Ensemble de mesures destinées à assurer la sécurité des personnes et des biens.
Anglais : Security plan

Plan de sécurité informatique. Ensemble de moyens préventifs, protectifs, organisationnels et procéduraux susceptibles d'assurer et de maintenir la pérennité de fonctionnement du système informatique en dépit des menaces.
Anglais : Information system security plan

Point de reprise. (Sûreté de Fonctionnement) Instants durant l'exécution d'un processus dont l'état courant peut ultérieurement nécessiter d'être restauré.
Anglais : Recovery point

Politique de sécurité. Ensemble de règles spécifiant ce qu'est la sécurité dans un contexte particulier. Exemples :

- sécurité obligatoire ou par mandat
- sécurité discrétionnaire
- sécurité multiniveau

Porte-clés. C'est une carte à mémoire contenant des clés secrètes servant à paramétrer un algorithme cryptographique décrit dans le système opératoire de la carte. Chaque clé secrète (inaccessible par l'interface) est repérable grâce à un identifieur de clé (accessible par l'interface).
Un porte-clés matérialise donc ainsi une ou plusieurs fonctions secrètes de la forme gC (C étant la clé secrète contenue dans la carte). Les paramètres secrets sont physiquement protégés dans le microcircuit de la carte. Ainsi l'usager ne sait pas reproduire ni simuler les fonctions secrètes dont il dispose.
Pour établir un lien personnalisé entre le porteur et la carte, on peut mettre en oeuvre un mécanisme de mot de passe de calcul. Quand un tel mécanisme a été activé dans le porte-clés, l 'usager doit présenter correctement le mot de passe préalablement à une exécution de calcul mettant en œuvre cette clé secrète.

Porte dérobée.
Anglais : Trap-door

Poursuite. (Sûreté de Fonctionnement) Forme de recouvrement d'erreur ou la transformation de l'état erroné ; consiste à trouver un nouvel état à partir duquel le système peut encore fonctionner.
Anglais : Forward Recovery

Préjudice. Implique une atteinte certaine à des droits réels, voire usurpation. Dommage financier ou commercial qui peut se concrétiser dans le cas de la réalisation d'un risque.
Anglais : Prejudice, detriment

Prévention. Ensemble des mesures qui tendent à empêcher certains risques de se produire. La troisième des 6 fonctions de la protection. Par tradition, c'est la prévention que l'on accorde généralement le plus de valeur. Mais bien entendu, cette valeur est fonction du coût et de l'efficacité. Le coût de la prévention doit être inférieur à la valeur de la perte potentielle qui serait subie, si la fonction prévention n'existait pas. La prévention totale est un concept purement théorique, car elle

signifierait que tout auteur potentiel d'un crime informatique échouerait dans toute tentative d'atteindre le but qu'il s'est fixé. Méthode ou comportement permettant de réduire le risque d'un type de sinistre ou d'empêcher un fait générateur de se produire.
Anglais : Prevention

Prévention des fautes. (Sûreté de Fonctionnement) Méthodes et techniques destinées à empêcher l'occurrence ou l'introduction de fautes.
Anglais : Fault prevention

Prévision des fautes. (Sûreté de Fonctionnement) Méthodes et techniques destinées à estimer la présence, la création et les conséquences des fautes.
Anglais :Fault forecasting

Processeur de sécurité. Equipement contenant une ou plusieurs cartes mères, réalisé souvent à base de PC ou compatibles sur lesquels sont connectées des cartes d'extension (cartes ADD-ON) qui sont le support des cartes mères.
Anglais : Security processor

Programme. Suite ordonnée d'instructions et d'expressions (algorithme) destinée à une machine donnée, écrite dans un langage reconnu par cette machine, et correspondant à la formulation d'un traitement.
Anglais : Program

Propriétaire. Le propriétaire est le garant des spécifications d'une application, dès sa conception et pendant toute sa vie. Par extrapolation, il est en général propriétaire des ensembles de données qu'il génère : bases de données, états, écrans. La définition de tous les aspects relatifs à son domaine relève de sa responsabilité.
Anglais : Owner

Protection. Ensemble de moyens de toute nature propres à satisfaire le concept de sécurité. Action de protéger, par des mécanismes logiciels et/ou matériels, des données, des traitements, des fichiers, des mémoires des matériels des périphériques et un environnement. La protection constitue avec la sauvegarde et l'audit les 3 grands fondements de la sécurité. Voir fonctions de protection.
Anglais : Protection, security

Pseudo-aléatoire. Caractère d'une suite d'informations présentant l'apparence de l'aléa (c'est-à-dire vérifiant des tests statistiques d'aléa) et cependant engendrée d'une façon déterministe et reproductible.
Anglais : Pseudo-random

Q.

Qualité. La qualité d'un produit ou d'un service est son aptitude à satisfaire les besoins des utilisateurs. La qualité s'exprime par un ensemble de caractéristiques mesurées que l'on peut comparer avec un autre ensemble de caractéristiques prévues dans la définition d'un référentiel. La qualité est donc une grandeur multi-dimensionnelle laquelle on peut trouver de nombreux référentiels, un pour chaque produit.
Anglais : Quality

Quantité d'information. Mesure de l'incertitude d'un message ou d'un événement par rapport à l'ensemble des messages (ou des événements) possibles.
Si un message de probabilité Pi est émis, le gain d'information de réception est : $I = - \log_2$ - l'unité d'information est le bit et correspond à la réception d'un message de probabilité 1/2.

ℝ.

Randonneurs : Hackers (fouineurs) qui se baladent d'un système à l'autre en volant à chaque fois les clés leur permettant de violer le système connecté suivant .

Recette. Tests effectués par l'utilisateur dans ses locaux, après installation de tout ou partie du système avec la participation du fournisseur pour vérifier que les dispositions contractuelles sont bien respectées.
Synonyme : Test de recette ou de réception
Anglais : Acceptance test

Recouvrement d'erreur (Sûreté de Fonctionnement) Forme de traitement d'erreur où un état exempt d'erreur est substitué à l'état erroné.

Reconnaissance. Contrôle et acceptation d'une identification (Une reconnaissance peut être ou non authentifiée).

Redondance. Elément supplémentaire destiné à pallier la défaillance de l'élément normal en vue d'assurer la continuité d'une fonction vitale.
En *théorie de l'information*, pseudo-information ou information inutile parce que déjà émise. Eléments ou parties de message n'apportant aucune information nouvelle. La mesure de la redondance revient à mesurer la connaissance a priori possédée par le récepteur, du message qui lui parvient (ou de la partie considédée de ce message). La fonction de la redondance est de favoriser l'assimilation au niveau pratique en évitant la saturation rapide du récepteur.
Anglais : Redundancy

Reprise. (Sûreté de Fonctionnement) Forme de recouvrement d'erreur où le système est ramené dans un état survenu avant l'occurrence d'erreur.
Anglais : Backward recovery

Reprise (mesures de). Action de reprendre une opération (traitement, activité, ensemble d'informations) en vue de retrouver un état antérieur. La sixième des 6 fonctions de protection. Les mesures de reprise sont nécessaires dans une multitude de cas, et pour un très grand nombre d'activités. Le coût de la reprise peut être très important, et doit être pris en considération lorsqu'on tente d'évaluer le coût d'une perte potentielle. Par exemple, la perte de compétitivité résultant d'espionnage industriel par vol d'informations et de documents, doit inclure le coût de la perte éventuelle du produit, le coût associé aux poursuites judiciaires si une action en justice est intentée, les coûts de développement, les installations de production qui ne servent éventuellement plus à rien, sans compter les engagements commerciaux qui peuvent déjà avoir été pris.
Anglais : Recovery measures, roll back measures

Répudiation. Acte consistant à nier avoir émis (répudiation à l'émission) ou reçu (répudiation à la réception) un message déterminé.
Anglais : Repudiation

Ressource. Dans un système informatique, toutes fonctions, dispositif ou rassemblement de données nécessaires à l'exécution une tâche et qui peuvent être allouées aux utilisateurs ou aux programmes. Le temps est considéré comme une ressource.
Anglais : Resource

Restauration (du service).(Sûreté de Fonctionnement) Transition de service incorrect à service correct.
Anglais : Restoration (service ~)

Risque. Dans le langage courant, se dit d'un mal qui peut arriver ou ne pas arriver quoiqu'il soit plus probable qu'il arrivera, mais qui est toujours moins imminent que le péril.
En gestion de risques, éventualité d'un événement pouvant causer un dommage. Il se mesure par une grandeur à deux dimensions associée à une phase précise de la vie du système et caractérisant un événement redouté par :

- sa probabilité d'occurence
- le montant de la perte consécutive

Dans le terme risque nous retrouvons les concepts de probabilité (probabilité, possible, éventuel) et de redouté (événement redouté, perte, accident, danger, préjudice). Par risque, nous entendons une menace dont nous sommes informés, mais dont les effets ne peuvent être prévus dans le temps et dans l'espace.
Selon les anglo-saxons, un risque est le produit de la probabilité d'occurrence d'un accident par le montant des pertes consécutives. Ceci représente une réalité très différente suivant que la probabilité ou que les pertes sont élevées, tout en se voyant attribuer la même valeur. Le mot risque est souvent mal utilisé. Le feu en lui-même n'est pas un risque. Un risque est la destruction que le feu peut occasionner.
La *mesure du risque* établit une relation entre la probabilité et l'intensité de la menace et les conséquences prévisibles en cas de réalisation.
L'*analyse du risque* apprécie les niveaux de risques acceptables ou non au regard des impératifs de sécurité. C'est une étude complète et précise des biens qui constituent le système, de leur vulnérabilité dans le but d'évaluer les pertes prévisionnelles, consécutives à certains événements, caractérisés par leurs probabilités d'occurrence.
La *maîtrise du risque* apprécie les niveaux de risque acceptable par une combinaison des actions préventives et défensives. Les contrôles sont nécessaires pour réduire les risques. Par conséquent avant d'évaluer les contrôles dans n'importe quel contexte, il faut identifier les risques avec leurs contrôles prévisionnels, révélatifs, et correctifs. La liste des risques suivants inclut les plus défavorables effets que l'organisation de gestion peut rencontrer:

- interruption de service
- erreurs de décision de gestion
- fraude et détournement
- sanctions légales
- coûts excessifs, baisse de revenus
- pertes ou destructions des actifs
- perte de compétitivité.

Les risques ne surviennent pas uniquement par absence de contrôle, les risques existent. Les contrôles agissent pour réduire ou éliminer les menaces, mais même avec contrôles, les menaces existent avant que les risques surviennent. Une menace peut générer plus d'un type de risques.
En outre, les divers risques qui peuvent survenir à partir d'une menace particulière ne surviendront sûrement pas avec la même
probabilité.
Anglais : Risk

Risque acceptable. Valeur d'un risque pouvant être accepté par les utilisateurs du système et défini de façon explicite par les responsables.

Risques (gestion des). Application aux problèmes de la sécurité, de la méthode d'évaluation des coûts et des enjeux. C'est la détermination de l'espérance mathématique des catastrophes. C'est un problème global à aborder en tenant compte de tous ses aspects, psychologiques, politiques ou financiers, en prenant en charge les difficultés suivant leur nature, l'origine des incidents, les motivations des intervenants, les objectifs des fraudeurs, etc.
Dans le principe, la démarche est simple :

- analyser les risques et les inventorier
- définir les mesures de prévention
- s'assurer

Anglais : Risk management

R.S.A. Sigle composé des initiales des noms de MM. Rivest, Shamir, et Adleman et désignant un algorithme de chiffrement mis au point au MIT. Il nécessite 2 clés distinctes :

- La clé dite publique, qui peut être connue de tout le monde, sert au chiffrement du message.
- La clé dite secrète, connue uniquement du destinataire, sert au déchiffrement.

Le système est conçu de telle sorte que la connaissance de la clé de chiffrement ne permet pas de calculer avec les moyens actuels, la clé de déchiffrement. La sécurité de RSA est basée sur la difficulté de factoriser des produits de deux grands nombres (de l'ordre de 100 chiffres décimaux). L'algorithme RSA peut être utilisé pour authentifier ou signer des messages.

S.

Sabotage. Malfaçon volontaire d'un outillage commercial, industriel, d'une affaire. Acte matériel tendant à empêcher le fonctionnement normal d'un service, d'une entreprise, à rendre inutilisable une machine, une installation. Forme de malveillance visant à mettre brutalement un système hors d'état de fonctionner. Généralement, opération organisée dans la clandestinité, à différentes fins (idéologiques, politiques, sociales, économiques...) et exécutée individuellement ou par groupe réduit en vue d'attenter à des personnes ou de détruire des biens.

Sabotage immatériel. On distingue quatre catégories principales de sabotage immatériel qui sont dans l'ordre du moins grave au plus grave :

- La falsification : fabrication de données, modification ou destruction de procédures d'exploitation ou de sauvegardes.
- Les infections informatiques : bombe logique, cheval de Troie, virus, ver, qui sont des programmes malveillants qui, loin de résulter en une exploitation utile pour l'utilisateur, sont destinés à perturber, à modifier ou à détruire tout ou partie des éléments indispensables au fonctionnement normal de l'ordinateur.
- Le sabotage immatériel total.

Sabotage immatériel total. Il consiste à détruire logiquement les sauvegardes au fur et à mesure de leur émission (fichiers, librairies, documentations, ...), puis à créer un incident d'exploitation (éventuellement un virus) impliquant le rechargement des sauvegardes.

Sas : Petit local en tampon entre une zone de sécurité nulle ou réduite et une zone à haute sécurité. Il est muni de deux ouvertures, chacune vers une zone, dont les portes ne peuvent pas s'ouvrir simultanément.

Sas informatique. Par analogie avec un sas (matériel), mécanisme contrôlant les échanges d'information entre une zone réduite et une zone à haute sécurité.

Saucisson ou salami. Fraude qui consiste à détourner quelques centimes sur des millions d'opérations.

Sceau électronique. Information auxiliaire associée à un message et garantissant l'authenticité et/ou l'intégrité de ce message. Technique pour engendrer cette information auxiliaire.

Scellement. Action de créer un sceau électronique, algorithme permettant de le calculer.

Scénario. Suite potentielle d'événements explicitement formulés. On peut parler de scénario d'accident, ou d'intervention ; on peut parler de scénario-type.

Secours. D'une manière générale on donne le nom de secours à toutes procédures et moyens matériels ou logiciels de sauvegarde. Ainsi, une bande de sauvegarde caractérise une copie sur bande magnétique alors qu'un secours désigne un centre informatique complet servant de secours à un autre centre.
Anglais : Back-up

Sécurité informatique. Faute d'un vocabulaire stabilisé, l'expression sécurité informatique fait partie d'une terminologie vague incluant le plus souvent des concepts extrêmement différents allant de la conception de bâtiments capables de protéger un site informatique contre une insurrection jusqu'à la mise en place de logiciels de sécurité très complexes, en passant par des techniques de back-up sophistiquées.

Définition proposée : Ensemble de mesures prises pour contrôler et assurer la protection des moyens de traitements et de supports de l'information.
Les propriétés majeures de la sécurité informatique peuvent s'analyser en terme de confidentialité, d'intégrité des biens informationnels et de disponibilité des services produits par l'informatique (Voir classification DIC).
C'est donc la garantie d'éviter toute forme de sinistralité. Selon la norme MIL 882 : Absence de circonstances susceptibles d'occasionner soit accident ou mort de personnel, soit dégradation ou perte d'équipements ou de biens.
Il est chimérique de rechercher une sécurité absolue ce qui revient à admettre que les phénomènes très peu probables ne se produisent pas.
ITSEC : Combinaison de la confidentialité qui empêche la divulgation inautorisée d'information, de l'intégrité, qui empêche la modification ou la suppression inautorisée d'information, et de la disponibilité, qui empêche toute rétention inautorisée d'information.
Anglais : computer security, EDP security

Sécurité-confidentialité (Sûreté de Fonctionnement) Sûreté de fonctionnement selon le point de vue de la prévention d'accès et/ou de manipulations non autorisés de l'information.

Sécurité des ordinateurs. (COMPUSEC) Mise en place sur système ou réseau de dispositifs assurant la sécurité des matériels, des micro-logiciels et des logiciels, afin de le protéger contre, ou de prévenir, la divulgation, la manipulation ou la suppression inautorisée d'informations.
Anglais : Computer Security

Sécurité d'un système. Situation du système vis-à-vis du niveau de sécurité acceptable. La sécurité d'un système peut être dans trois situations :

- non appréciable
- appréciée et non satisfaisante
- appréciée et satisfaisante

Degré de sécurité optimal, compatible avec les contraintes d'efficacité opérationnelle, les coûts et les délais, qui doit être obtenu par application systématique des principes de sécurité des systèmes (conception et conduite) au cours des phases successives de la vie du système (selon MIL 882)
Anglais : System security

Sécurité-innocuité. (Sûreté de Fonctionnement) Sûreté de fonctionnement selon le point de vue de la non-occurrence de défaillances catastrophiques. Mesure du temps jusqu'à défaillance catastrophique.
Anglais : Safety

Service. (Sûreté de Fonctionnement) Comportement d'un système, tel que perçu par son ou ses utilisateurs. - Anglais : Service

~ **correct**. Service délivré en ^conformité avec les spécifications du système. - Anglais : Correct service

~ **incorrect.** Service délivré non en ^conformité avec la spécification. - Anglais : Incorrect service

~ **temps réel**. Service qui doit être délivré dans des intervalles de temps finis régis par l'environnement. - Anglais : Real-time service

Session. Intervalle de temps pendant lequel peut agir un opérateur connu sans avoir besoin de se ré-identifier.
Anglais : Session

Sévérité (d'une défaillance). (Sûreté de Fonctionnement) Résultat de l'évaluation des conséquences sur l'environnement du système.
Anglais : Severity (failure ~)

Signature. Méthode d'authentification de l'origine d'un message, garantissant simultanément l'intégrité de ce dernier. C'est le résultat du chiffrement des données à signer ou, par souci d'optimisation, de leur sceau par la clé secrète du signataire. Elle est donc indissolublement liée au message signé et à l'identité du signataire.
Sa correction peut être vérifiée par l'utilisation d'une clé publique.
Anglais : Digital signature

Sinistre. Evénement catastrophique qui entraîne des pertes sur les actifs de la société (humains, matériels, logiciels, données). Fait dommageable pour soi-même et autrui, de nature à mettre en jeu la garantie d'un assureur. MARION : réalisation d'un risque.

Spécification. Indication précise d'un ensemble de conditions à remplir par un produit, un matériau, ou un procédé, qui inclut si nécessaire les méthodes qui permettent de déterminer si ces conditions sont remplies. Norme F x 6007 : terme de contrôle de qualité.
Anglais : Spécification

Spécification d'un système (Sûreté de Fonctionnement) Description agréée de la fonction ou du service attendu du système.

Stéganographie. Technique de dissimulation d'un message telle que l'encre invisible ou le micro-point.
Anglais : Steganography

Structure d'un système (Sûreté de Fonctionnement) Ce qui lui permet de faire ce qu'il fait.

Survivance (cf pérennité). Garantie de pouvoir continuer de travailler à la suite d'un sinistre : panne, destruction, sabotage, malveillance.
Barbarisme : survivabilité.

Substitution (ou codage). Technique de chiffrement qui consiste à remplacer chaque caractère du texte en clair par un autre caractère pris dans un alphabet de substitution. La substitution se fait sous le contrôle d'une clé qui sélectionne l'alphabet à utiliser.

Sûreté de fonctionnement. (Sûreté de Fonctionnement) Propriété qui permet aux utilisateurs d'un système de placer une confiance justifiée dans le service qu'il leur délivre.
Anglais : Dependability

Système. Ensemble d'éléments matériels, logiciels, humains, en interaction, organisé pour remplir une fonction ou une mission déterminée. Ce qui est extérieur au système est son environnement. Le nombre d'états possible pour un système est sa variété (terme officiel).
Sûreté de Fonctionnement : Entité ayant interagi ou interféré, interagissant ou interférant, ou susceptible d'interagir ou d'interférer avec d'autres entités . Ensemble de composants interconnectés en vue d'interagir.
Anglais : System

Système atomique. (Sûreté de Fonctionnement) Système dont la structure interne ne peut être discernée, ou n'est pas intéressante et peut être ignorée.
Anglais : Atomic system

Système à arrêt sur défaillance. (Sûreté de Fonctionnement) Système dont toutes les défaillances sont, dans une mesure acceptable, des défaillances par arrêt.
Anglais : Fail-stop system

Système à silence sur défaillance. (Sûreté de Fonctionnement) Système dont toutes les défaillances sont, dans une mesure acceptable, des défaillances par écrasement.
Anglais : Fail-silent system

Système informatique. Ensemble d'éléments interactifs matériels, logiciels, procéduraux et humains, organisés dans le but de remplir une fonction ou une mission informatique dans un environnement donné. Un système informatique peut comprendre plusieurs centres de traitement de l'information (CTI), terminaux etc..
Anglais : Data processing system

Système de secours. Partie d'un système informatique capable de se substituer à un élément défaillant pour assurer la continuité du service.
Anglais : back up

Système de sécurité informatique. Toutes les protections technologiques, toutes les procédures de conduites établies et appliquées au matériel et au logiciel et toutes les données qui ont pour objet d'assurer la protection des biens et de la vie privée.
Anglais : EDP security system

Système sûr en présence de défaillance. (Sûreté de Fonctionnement) Système dont toutes les défaillances sont, dans une mesure acceptable, des défaillances bénignes.
Anglais : Fail-self system

Système temps réel. (Sûreté de Fonctionnement) Système qui remplit au moins une fonction temps réel ou qui délivre au moins un service temps réel.
Anglais : Real-time system

T.

Technobandits. Pirates dont l'activité est de craquer les systèmes informatiques. Cf cyber punks

Technopathe. Néologisme qui est attribué aux informaticiens qui veulent détruire les programmes à l'aide de virus, vers...

Télécasse. Détournement de fonds ou d'informations perpétrés en craquant les systèmes.

TEMPEST. L'étude et le contrôle des signaux (rayonnements) suspects ou compromettants émis par des équipements de traitements ou de transmission d'information.

Test. (Sûreté de Fonctionnement) Vérification dynamique effectuée avec des entrées valuées. - Anglais : Testing

~ **aléatoire ou statistique.** Test où les jeux d'entrée sont sélectionnés selon une distribution probabiliste du domaine d'entrée. - Anglais : Random ou statistical testing

~ **basé sur des fautes.** Test destiné à révéler des classes de fautes spécifiques. - Anglais : Fault-based testing

~ **de conformité.** Test dont le but est de vérifier si le système satisfait ses spécifications. - Anglais : Conformance testing

~ **déterministe.** Méthode de test où les jeux d'entrée sont déterminés par un choix sélectif selon le critère retenu. - Anglais : Deterministic testing

~ **fonctionnel.** Test où les jeux d'entrée sont sélectionnés selon des critères relatifs à la fonction du système. - Anglais : Functional testing

~ **de recherche de fautes.**Test destiné à révéler des fautes. - Anglais : Fault-finding testing

~ **opérationnel.** Test destiné à évaluer la sûreté de fonctionnement, avec un profil d'entrée représentatif des conditions opérationnelles. - Anglais : Operational testing

~ **structurel.** Test où les jeux d'entrée sont sélectionnés selon des critères relatifs à la structure du système. - Anglais : Structural testing

Tolérance aux fautes. (Sûreté de Fonctionnement) Méthodes et techniques destinées à fournir un service conforme à la spécification en dépit des fautes.
Anglais : Fault tolerance

Trace d'audit de sécurité. Information recueillies ou utilisées en vue de permettre un audit de sécurité.
Anglais : security audit trail

Trafic d'influence. Il s'agit du fait d'un tiers qui sollicite ou reçoit des offres, promesses, dons ou présents pour obtenir ou tenter d'obtenir auprès d'un dépositaire de l'autorité publique, en abusant ainsi d'une influence réelle ou supposée, la faveur attendue par l'auteur de la rétribution.

Traitement d'erreur. (Sûreté de Fonctionnement) Opérations destinées à éliminer les erreurs, si possible avant qu'une défaillance ne survienne.
Anglais : Error processing

Traitement de faute. (Sûreté de Fonctionnement) Opérations destinées à éviter qu'une, ou des fautes ne soient activées à nouveau.
Anglais : Fault treatment

Transformations complexes sur l'information

- irréversibles : signature, intégrité des messages, contrôle d'accès

- réversibles symétriques : secret des communications, authentification du couple émetteur/récepteur, chiffrement des fichiers (DES)
- réversibles dissymétriques : en plus des propriétés des algorithmes symétriques, assurent l'authentification des sources, la signature, l'acquittement.

Transposition. Technique cryptographique qui consiste à permuter les caractères du texte en clair suivant une règle de transposition.

Trappe. Mécanisme matériel ou logiciel caché dans un système permettant de contourner des fonctions de sécurité ou de les mettre hors service. La connaissance de la trappe rend ces fonctions de sécurité efficaces.

Troie (cheval de). cf Cheval de Troie.

Type de risque (MARION). Les risques informatiques sont classés en dix types de risques (risques matériels, vols, etc.).

U.

Unité fonctionnelle (ITSEC). Partie fonctionnellement distincte d'un composant.
Anglais : functional unit

Utilisateur. Entité (personne, entreprise...) faisant appel aux technologies de l'information, qu'elle possède ou non ses propres équipements. En sécurité, l'utilisateur final doit respecter les règles sécuritaires édictées par le propriétaire des informations mises à sa disposition et les conditions d'utilisation des outils mis en place par l'informatique.
ITSEC : personne qui est au contact d'une cible d'évaluation en exploitation et qui utilise ses services et ses fonctions.
Anglais : end user

Utilisateur (d'un système).(Sûreté de Fonctionnement).Autre système (humain ou physique) qui interagit avec le système considéré.
Anglais : User (system ~)

Utilitaires (programmes de service). Anglicisme désignant les progiciels appartenant généralement au système d'exploitation et destinés à augmenter les possibilités de base de la machine. On range dans cette catégorie tous les progiciels de gestion technique, les bibliothèques, les programmes de traduction, etc.
Anglais : utility programs

V.

Validation. Fait de valider une chose, c'est-à-dire de déclarer qu'elle présente toutes les conditions requises pour produire son effet. Elle peut être :

- soit, une simple commande d'exécution de fin de saisie
- soit, une confirmation technique
- soit, une certification personnelle
- soit, une contre-certification par un tiers.

Anglais : Validation

Validation (Sûreté de Fonctionnement) Méthodes et techniques destinées à avoir confiance dans l'aptitude du système à délivrer un service conforme à la spécification. Elimination des fautes et prévision des fautes.
Anglais : Validation (dependability ~)

Vandalisme. Tendance à détruire stupidement, à détériorer par ignorance.

Ver : C'est un programme parasite qui consomme les ressources du système (mémoire vive, réseau, etc). Ce programme possède la faculté de se déplacer et de se reproduire au sein de la mémoire des ordinateurs. Il peut également déclencher des actions malveillantes. Exemple réel de ver : en novembre 1988 aux USA un ver introduit sur le réseau Internet a contaminé plus de 6.000 ordinateurs Unix en moins de 24 heures.

Vérification. (Sûreté de Fonctionnement) Processus consistant à déterminer si le système satisfait des propriétés, appelées conditions de vérification, qui peuvent être générales et indépendantes des spécifications, ou spécifiques et déduites des spécifications. - Anglais : Verification

~ **dynamique**. Vérification comportant l'activation du système. - Anglais : Dynamic verification

~ **de non-régression**. Vérification effectuée après correction afin de s'assurer que l'élimination de faute n'a pas eu de conséquences indésirables. - Anglais : Regression verification

~ **statique**. Vérification effectuée sans activer le système. - Anglais : Static verification

Vol. C'est le terme général qui sert à désigner l'action de s'approprier par ruse ou par force, ce que l'on sait être la propriété d'autrui.

Violation. Effraction

Virus. Un virus est un programme qui possède la faculté de créer des répliques de lui-même au sein d'autres programmes : il contient donc une fonction auto-reproductrice.
Certains virus marquent les programmes qu'ils ont contaminés par une empreinte afin de ne pas contaminer plusieurs fois le même programme. Cette empreinte est utilisée par certains produits anti-virus. D'autres produits utilisent une séquence de code caractéristique du virus. La plupart des virus micro-informatiques actuellement connus contiennent des fonctions à déclenchement différé. Ils se différencient les uns des autres par la façon de contaminer les programmes et par leurs effets.
Les virus se décomposent en deux grandes catégories :

- les *virus systèmes* dont le secteur de contamination est exclusivement le secteur de démarrage (boot) des supports.
- les *virus programmes* dont le secteur de contamination principal est constitué par les programmes exécutables. Ils se décomposent à leur tour en deux catégories :
  - *Virus par recouvrement* qui s'installe à l'intérieur d'un programme qu'il détruit en partie (données des fichiers, tables, pointeurs, programmes et librairies sources...). La force d'un virus par recouvrement est que

la taille du programme infecté n'est pas modifiée ce qui rend un repérage fondé sur la variation de la taille des programmes inopérant. La faiblesse d'un virus par recouvrement est que le programme infecté ne peut plus s'exécuter totalement normalement : de ce fait, l'utilisateur peut détecter assez rapidement le virus.

- *Virus par ajout* qui modifie un programme sans le détruire. Chaque fois que le programme est lancé, le virus s'exécute puis «rend la main» au programme qui fonctionne alors de la façon normale. La force d'un virus par ajout est que le programme infecté semble fonctionner normalement ce qui peut retarder la détection du virus. La faiblesse d'un virus par ajout est que la taille du programme est augmentée de la taille du virus, ce qui rend un repérage fondé sur la variation de la taille des programmes possible.

L'atteinte préalable des sauvegardes se fait soit naturellement (sauvegarde périodique du virus non détecté) ou en modifiant les procédures de sauvegardes (physiques parfois, logiques souvent).

VRAI. En logique, une des deux valeurs de vérités, l'autre étant FAUX
Anglais : True

Vulnérabilité. Etat de ce qui peut être facilement atteint. Qui est exposé sans protection au danger. Aptitude d'un système à subir des dommages prévus sous l'effet d'un acte de malveillance, d' un défaut de conception, de réalisation ou d'exploitation qui peut faciliter une attaque du système. Ce terme ne fait pas partie de la terminologie sécurité des systèmes mais de la terminologie de la vulnérabilité de systèmes.

BIBLIOGRAPHIE

Computer control & audit - William C. Mair, Donald R Wood, Keagle W. Davis - Q.E.D. INFORMATION SCIENCES, INC

Crime by computer - Donn Parker - SCRIBNERS

Dependability Basic Concepts and Terminology - Dependable Computing and Fault-Tolerant Systems vol 5 - J.C. Laprie - SRINGER- VERLAG, WIEN ,NEW-YORK

Dictionnaires : LAROUSSE, ROBERT, LITTRE

Glossaires : AFB, AFCET, AFNOR, ITSEC, MARION, MELISA, SCSSI, LMI, OI INFORMATIQUE, OTAN, PHILIPPE LASSIRE CONSULTANTS, SOCIETE GENERALE, etc.

L'Encyclopædia Universalis

La sécurité des réseaux - J.-M. Lamère, Y Leroux, J. Tourly - DUNOD Informatique

Les théories de l'action - La bibliothèque du CEPL

Méthode de conduite de projet - M. Gedin - LES EDITIONS D'ORGANISATION

Méthode générale d''analyse des applications informatiques - X. Castellani - MASSON

Passeport pour les réseaux - TELECOMS RESEAUX

Racines - Ministère de la Recherche et de L'Industrie

Sécurité informatique protection des données - AFNOR-EYROLLES

Security, accuracy, and privacy in computer system - James Martin - PRENTICE-HALL

Téléinformatique - C. Macchi, J.-F.Guilbert et treize co-auteurs - DUNOD

Théorie générale des systèmes - Ludwig von Bertalanffy - DUNOD

VERSION 1.2

Les auteurs :

Philippe LASSIRE - De formation capitaine au long cours, CNAM et ISSEC/ESSEC, Philippe LASSIRE est depuis 1982, gérant-directeur et fondateur du cabinet PHILIPPE LASSIRE CONSULTANTS. Il fut, auparavant, le directeur du département "organisation & informatique" et le contrôleur de gestion de plusieurs sociétés. Il a fondé le syndicat professionnel des auditeurs et experts en systèmes d'information (FIASI), dont il fut président pendant cinq ans. Il en est aujourd'hui le président honoraire. Depuis douze ans, il anime et/ou participe à des groupes de travail traitant de l'audit de sécurité des systèmes d'information (AFCET, AFNOR, CLUSIF). Certifié auditeur et expert en systèmes d'information, il enseigne à l'Institut National des Télécommunications (INT) et est auteur d'une méthode d'audit. Enfin, il est membre du Comité de Parrainage d'un mastère de l'INT et membre du Comité Directeur "Sécurité et Sûreté Informatique" de l'AFCET.

Gérard REBOULET - Enseignant au département informatique de l'IUT de Lyon, Gérard REBOULET s'intéresse depuis quelques années aux problèmes de sécurité, de sûreté de fonctionnement, d'audit des systèmes d'information, ainsi qu'à l'introduction de ces notions dans les cycles de formation.

Gilles RUGGIU - Gilles RUGGIU est Directeur de l'Informatique à la Sté BERTIN & Cie, qu'il a rejoint en 1984. Auparavant, il a travaillé pendant dix-sept ans au Laboratoire Central de Recherches de THOMSON-CSF, où il a dirigé le groupe de Recherches Informatiques. Ses travaux de recherches ont porté sur la conception et la logique des langages de programmation, l'architecture des ordinateurs, les systèmes temps réel, le génie logiciel et la protection des informations. Il a vingt-cinq ans d'expérience dans le domaine de la sécurité des systèmes d'information et sa spécialité est la cryptographie. Il est collaborateur extérieur du Service Central de la Sécurité des Systèmes d'Information (S.C.S.S.I.) où il enseigne la cryptologie. Gilles RUGGIU est membre du Conseil d'Administration de l'A.F.C.E.T.

Olivier VELIN - Responsable de la sécurité informatique, à la Direction de la Gestion Technique de la Société Générale[1], Olivier VELIN s'est intéressé pendant de nombreuses années aux problèmes de sécurité, d'audit des systèmes d'information en milieu bancaire.

Kioumars YAZDANIAN - Ingénieur de recherche au département d'Études et de Recherches en Informatique du CERT (ONERA) Kioumars YAZDANIAN a reçu une formation d'ingénieur en électronique puis de spécialisation en informatique avant de soutenir une thèse de doctorat en informatique. Il travaille depuis plus de quinze ans, dans le domaine des bases de données, sur le modèle relationnel et ses rapports avec la logique mathématique. Depuis quelques années il s'est intéressé aux problèmes fondamentaux de sécurité, notamment en ce qui concerne les bases de données et effectue des recherches dans ce domaine. Il enseigne à l'E.N.S.A.E., à l'I.N.S.A., au C.E.S.S.S.I. et dans divers autres organismes de formation.

[1] au moment de sa participation à la réalisation de ce glossaire