LES METHODES

MAGDA

Méthode d'**A**dministration et de **G**estion

des **D**roits et **A**ccréditations

Décembre 1997

Commission Techniques de Sécurité Logique

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANCAIS
30, Rue Pierre Sémard – 75009 Paris
Tél : 01 53 25 08 80 – Fax : 01 53 25 08 88 – www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Alain	**ALBINHAC**	
Jacques	**AUZAT**	*COMMERCIAL UNION FRANCE*
Robert	**BERGERON**	*CAP SESA TERTIAIRE*
Jacques	**BLANC-GARIN**	*BG CONSULTANT*
Jean-Claude	**GANDOIS**	*LEGRAND SA*
Claude	**GUERIN**	*COMPAGNIE GENERALE DE GEOPHYSIQUE*
Jean	**IVALDI**	*A.C.A.*
Charles	**LANGUEDOC**	*STRATEGIA*
Thierry	**LEFEVRE**	*CREDIT MUTUEL DE BRETAGNE*
Joël	**MATHE**	*APAVE de l'OUEST*
Noëlle	**PELTIER**	*BOUYGUES TELECOM*
Raphaël	**PRECIGOUT**	*XP CONSEIL*
Alain	**REFFRAY**	*EXPLOITIQUE*

avec l'aimable participation de : M. MOREL (Société Générale), M. MOULY (Secureware).

TABLE DES MATIERES

1. INTRODUCTION

1.1 Objectif du document

Le but du présent document est de proposer une méthode d'administration de l'allocation des droits d'accès aux ressources informatiques de l'entreprise.

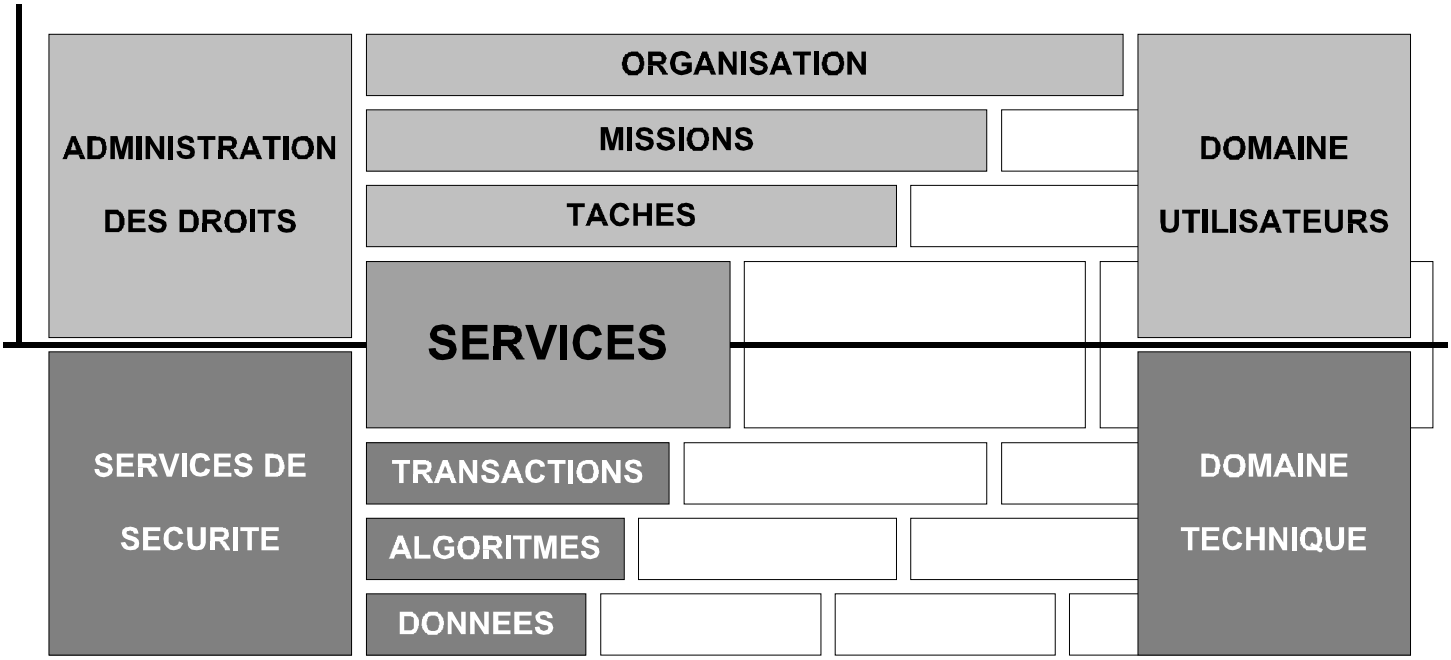
Il se consacre essentiellement à apporter un éclairage sous l'angle "gestion" des fonctions d'administration situées en amont de services de sécurité logique traditionnels, aboutissant principalement à :

- l'identification des travaux préliminaires indispensables avant la mise en œuvre des mécanismes de sécurité proprement dits,
- la définition des moyens organisationnels permettant de faciliter l'administration au jour le jour des droits d'accès et des systèmes de sécurité.

Ce document décrit un modèle d'administration « idéal », dont l'objectif est de répondre aux besoins des gestionnaires ; à ce titre il ne fait pas référence aux fonctionnalités techniques des outils actuellement disponibles sur le marché, et n'est en aucun cas un passage en revue des produits de sécurité et des fonctionnalités les plus usuels:

- mécanismes d'identification et d'authentification ou fonctions contribuant à la traçabilité,
- principes et méthodes de "single sign-on", notions de "pass tickets" et équivalents,
- architectures possibles des serveurs de sécurité,
- fonctionnalité et positionnement relatif des différents produits du marché,
- etc.

Pour être mise en œuvre, la méthode qui suit représente une grande combinatoire de situations complexes et il va sans dire qu'elle devra être supportée par des moyens logiciels appropriés. Conçu comme le « cahier des charges » d'un outil idéal d'administration des droits d'accès, le champ d'investigation du présent document peut être schématisé de la façon suivante :



1.2 La situation générale actuelle

Dans leur recherche de compétitivité, les entreprises doivent être flexibles. Les fusions, cessions, acquisitions, et leurs corollaires de restructurations accélèrent une vitesse de réorganisation déjà importante. Bref, l'entreprise bouge de plus en plus vite.

L'émergence, puis le raz de marée provoqués par la diversification des solutions techniques informatiques (réseaux, UNIX, Windows NT, INTERNET), ont favorisé l'atomisation des applicatifs sur des plates-formes techniques diversifiées. Il en résulte une croissance exponentielle des systèmes accédés et de leurs interactions.

En parallèle, l'impact des systèmes d'information sur l'organisation des entreprises s'est accru au point que les besoins de sécurité sont devenus l'un des enjeux majeurs de leur informatisation. Les critères de Disponibilité, d'Intégrité et de Confidentialité sont au cœur de toute politique de sécurité. Leur évaluation en terme de sensibilité à l'égard des fonctions desservies est l'une des tâches les plus précieuses dans la construction de l'édifice sécurité.

1.3 La problématique

Les risques patrimoniaux grandissent à l'égard de la disponibilité, de l'intégrité et de la confidentialité des systèmes d'information. La ressource « information » est devenue l'une des ressources vitales de l'entreprise. Porter atteinte à tout ou partie des critères cités ci-dessus peut, pour certains applicatifs, provoquer des dégâts irréversibles aux forces vitales de l'entreprise ou de l'organisme affecté.

L'accélération du besoin de flexibilité des organismes dans leurs accès aux systèmes d'informations, combinée à la croissance des systèmes accédés, entraîne un développement exponentiel des modifications concernant les acteurs et les droits d'accès devant leur être associés.

Les outils techniques de gestion des droits présents sur le marché ne sont pas cohérents entre eux et l'offre s'oriente vers des produits fédérateurs, proposés par les constructeurs ou offreurs de ce type de service, qui allègent ces contraintes mais ne règlent généralement pas la cohérence de

l'administration des droits à l'égard des risques liés à la valeur du patrimoine informations concerné.

La charge d'élaboration puis de mise à jour des droits d'accès et les imprécisions liées à la remarque qui précède, entraînent des coûts de gestion importants pour un résultat souvent imprécis donc improbable en terme de sécurité. La perte de maîtrise guette et l'administration des droits d'accès est au cœur des préoccupations de ceux qui ont à en répondre dans leurs propres organismes.

1.4 Constats et principes

On constate que la plupart des organismes de taille un tant soit peu conséquente qui ont recours à des systèmes hétérogènes sont confrontés à un certain nombre de problèmes majeurs dans la gestion quotidienne de leur sécurité logique :

- les systèmes de sécurité sont fréquemment administrés par les populations les plus aptes et les mieux placées pour les contourner (dépendance vis-à-vis des ingénieurs système, propagation des droits des équipes d'exploitation qui, pour lancer des travaux, se voient attribuer des droits exorbitants),
- le transfert des applicatifs vers des architectures à base de systèmes départementaux a provoqué une explosion de l'hétérogénéité des plates-formes et des méthodes d'administration correspondantes. Le nombre de combinaisons des accès possibles aux applications a crû au rythme de l'explosion des applications multiplié par le nombre de plates-formes les supportant,
- l'accélération des réorganisations d'entreprises née des rachats, fusions, absorptions, cessions, etc. se propage mal ou trop lentement dans l'attribution des droits d'accès dont la mauvaise gestion devient la règle ou au moins le risque,
- les restructurations et réorganisations entraînent des départs, des absences, des remplacements, des interventions d'acteurs externes mal gérées,
- Dans les organisations de type "projet", les méthodes en place sont incapables de gérer la sécurisation des groupes de travail ad-hoc ("task-forces").
- Dans l'état actuel des choses, la plupart des progiciels de sécurité d'accès logique (même ceux s'appuyant sur les nouvelles architectures de systèmes ouverts) laisse à la charge des "applications" (c'est-à-dire les programmeurs du Client) de définir les "Listes de Contrôle d'Accès", établissant une correspondance directe entre la ressource et le demandeur.

Mais face à la réalité décrite, les inconvénients de cette approche sont évidents :

- absence de souplesse face à des situations évolutives (nécessité de mettre à jour des composants qui ne sont pourtant pas concernés),
- recours forcé à un administrateur pour effectuer cette mise à jour (donc lourdeur et point de faiblesse),
- ajout d'un intermédiaire entre le gestionnaire ayant défini le niveau de criticité et l'activation des règles (introduisant en outre des risques d'hétérogénéité),
- gestion combinatoire insupportable dès que l'organisme dépasse une taille modeste et/ou que l'on a à faire à un environnement réellement ouvert (*n* utilisateurs confrontés à *m* ressources pour *p* types d'usages).

Idéalement, il faudrait maintenant disposer d'un outil permettant de définir d'une façon quasi-automatique le type de "serrure" ou de "cadenas" minimum requis par chaque ressource en fonction des opinions formulées par ceux qui ont en charge la sécurité de l'élément du patrimoine de l'entreprise (le propriétaire dont nous parlerons largement plus loin).

On a vu précédemment que, sauf exceptions, cette définition ne pourrait se faire au niveau global des ressources, et que, lorsqu'on parvenait à obtenir des quantifications, c'était à des niveaux assez élémentaires. L'outil idéal du paragraphe précédent pourrait malgré tout commencer à compléter l'état des lieux en appliquant des règles de bon sens de propagation.

Afin d'adapter la dynamique de la gestion des droits aux contraintes précédemment exposées, les développements de ce document sont en conséquence basés sur les principes suivants :

1. Il n'est pas concevable d'exiger des objets (ou ressources) qu'ils (ou elles) sachent par quels individus nommément désignés ils (ou elles) doivent accepter d'être accédés : objets et ressources doivent se contenter d'obtempérer à tout porteur d'une accréditation en bonne et due forme; c'est aux fonctions utilisatrices de définir à quels objets (ressources) elles ont besoin d'avoir accès pour mener à bien leurs missions,
2. La définition et l'arbitrage des droits d'accès doivent être une prérogative des "propriétaires" des objets et ressources ; ceci doit pouvoir être fait à leur niveau (c'est-à-dire sans intermédiaire) et dans un langage compréhensible pour eux,
3. Il n'est par contre pas concevable que le "propriétaire" d'un objet ou d'une ressource puisse conserver un contrôle individuel de tous les utilisateurs devant être habilités à accéder aux objets dont il a la charge ; tout au plus peut-on lui demander de définir les niveaux de sécurité requis pour ses objets, et de ponctuellement contrôler la pertinence de l'attribution des autorisations au niveau des différentes fonctions ou sous-fonctions de l'entreprise,
4. C'est par contre aux différents responsables hiérarchiques et/ou fonctionnels qu'il appartient d'une part de définir le niveau d'habilitation des employés et d'autre part leur affectation ; il n'est par contre pas dans leur prérogative ni leur compétence de définir la multitude des droits d'accès individuels des collaborateurs aux objets finaux;
5. L'accès final à un objet ou une ressource doit finalement être obtenu par la seule adéquation permanente (et si possible automatisée) entre des "droits d'en connaître" (ou "accréditation") obtenus par des utilisateurs (selon les mécanismes définis dans les chapitres qui suivent) et des "besoins de sécurité" définis pour chacun des objets et ressources de l'organisation ;
6. Etant donné que ces deux paramètres ont été obtenus par deux voies totalement dissociées, il est indispensable que les deux canaux (Propriétaires de Ressources d'une part et Responsables Hiérarchiques d'autre part) aient par ailleurs un langage commun ; c'est le fondement de ce document, qui s'appuie à cet effet extensivement sur la notion de sensibilité "DIC" ;
7. Enfin, il est indispensable d'isoler totalement au moyen d'un interface unique les aspects "Gestion" d'une part et "Technique" d'autre part de la sécurité, de façon à ce que toute modification de la philosophie ou de la conception d'un domaine n'entraîne pas la nécessité de modification dans l'autre domaine.

2. LES MODELES

2.1 Modélisation de la gestion des accès logiques

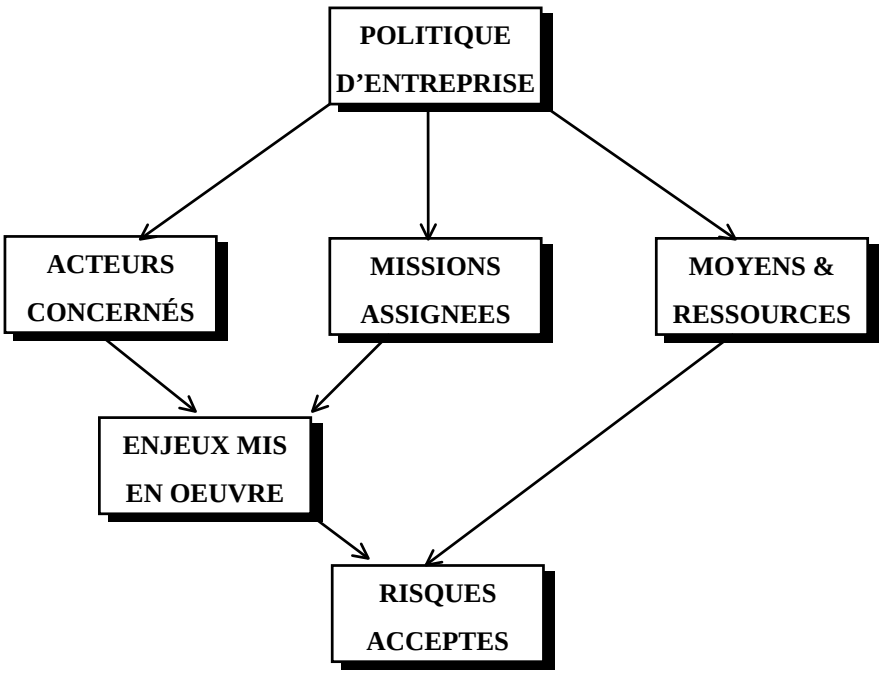


Schéma 1 : modélisation de la gestion des risques liés aux accès logiques de l'entreprise

Du point de vue des accès aux ressources, ce premier schéma met en évidence l'application d'une politique de sécurité de l'entreprise sous 3 axes concurrents puis convergents :

1. Les acteurs concernés c'est à dire les ressources humaines amenées à opérer,
2. Les missions assignées pour l'exécution des différentes tâches,
3. Les moyens et les ressources mis à la disposition de l'organisme pour travailler.

Ensuite la convergence des acteurs et des missions c'est à dire l'affectation de tel individu à telle mission représente la mise en œuvre d'enjeux plus ou moins importants.

Enfin, les enjeux mis en œuvre conjugués aux moyens concernés implique d'en connaître puis d'en accepter les risques.

On voit déjà apparaître dans ce premier schéma la volonté de dissocier le plus longtemps possible la notion d'acteur affecté à une mission, des ressources qui lui seront nécessaires pour exécuter cette mission.

2.2 Modélisation de l'administration de la sécurité

Les réflexions rassemblées dans ce document ont été organisées autour d'un modèle comportant les grands blocs fonctionnels suivants (Cf. schéma 2 et 3 page 7 ci-après) :

1. Le point de départ de la réflexion concerne la formulation des traits généraux de **l'ORGANISME** souhaitant mettre en place une sécurité logique cohérente. Ceci fait l'objet du chapitre 5 « lancement du projet ».
2. L'organisme comporte un certain nombre d'**UTILISATEURS** dont la position sera précisée dans un ORGANIGRAMME HIERARCHIQUE et pour lesquels on pourra définir une "**CAPACITE D'EN CONNAITRE.** Ces notions font l'objet du chapitre 5.2.1.
3. Cet organisme vit grâce à l'exécution d'un certain nombre de **FONCTIONS** ou de MISSIONS précisées par un ORGANIGRAMME FONCTIONNEL. La bonne exécution de celles-ci passe par la formulation d'une série de "**BESOINS D'EN CONNAITRE**"; ces notions sont développées dans les chapitres 3.2 et 3.5.
4. Dans le cadre des Missions ou Fonctions qui leur ont été confiées, les Acteurs doivent alors avoir accès (ou être amenés à en créer eux-mêmes) à un certain nombre de **SERVICES** dont il aura fallu faire l'**INVENTAIRE**, ceci est l'objet du chapitre 7.3.
5. Une fois ces Ressources inventoriées, et avant de pouvoir en déterminer le degré critique en termes de sécurité, il va être nécessaire de déterminer leur valorisation. Principalement, le **PROPRIETAIRE** est à même de procéder à cette évaluation en respect des politiques générales de l'organisme ; les observations correspondantes sont formulées au chapitre 7.3. également.
6. Pour qu'il puisse être concrètement procédé à l'exécution des Fonctions ou Missions mentionnées plus haut, l'organisme doit procéder en permanence à des **AFFECTATIONS** qui aboutissent pour chacun des acteurs et à un moment donné, par la conjonction des "Besoins d'en Connaître" et des "Capacités d'en Connaître", à l'attribution de "**DROITS D'EN CONNAITRE**" (également appelés dans certaines architectures "ACCREDITATIONS" ou "NIVEAUX DE SECURITE"); ces concepts sont étudiés aux chapitres 3.3. et 3.5.
7. Le résultat de l'évaluation par les Propriétaires du niveau critique des Services dont ils ont la responsabilité est formalisé par l'attribution à chaque Traitement d'un **BESOIN de SECURITE** (également appelées LABEL DE SECURITE) ; ce concept est évoqué dans le chapitre 3.4.
8. Finalement, c'est l'adéquation entre le "Droit d'en Connaître" accordé à un Acteur pour remplir sa fonction et le "Label de Sécurité" des objets ou ressources qu'il tente d'accéder qui aboutira à l'attribution du **DROIT d'ACCÈS** final ; cette dernière phase est étudiée au chapitre 10.

3. LES PHASES

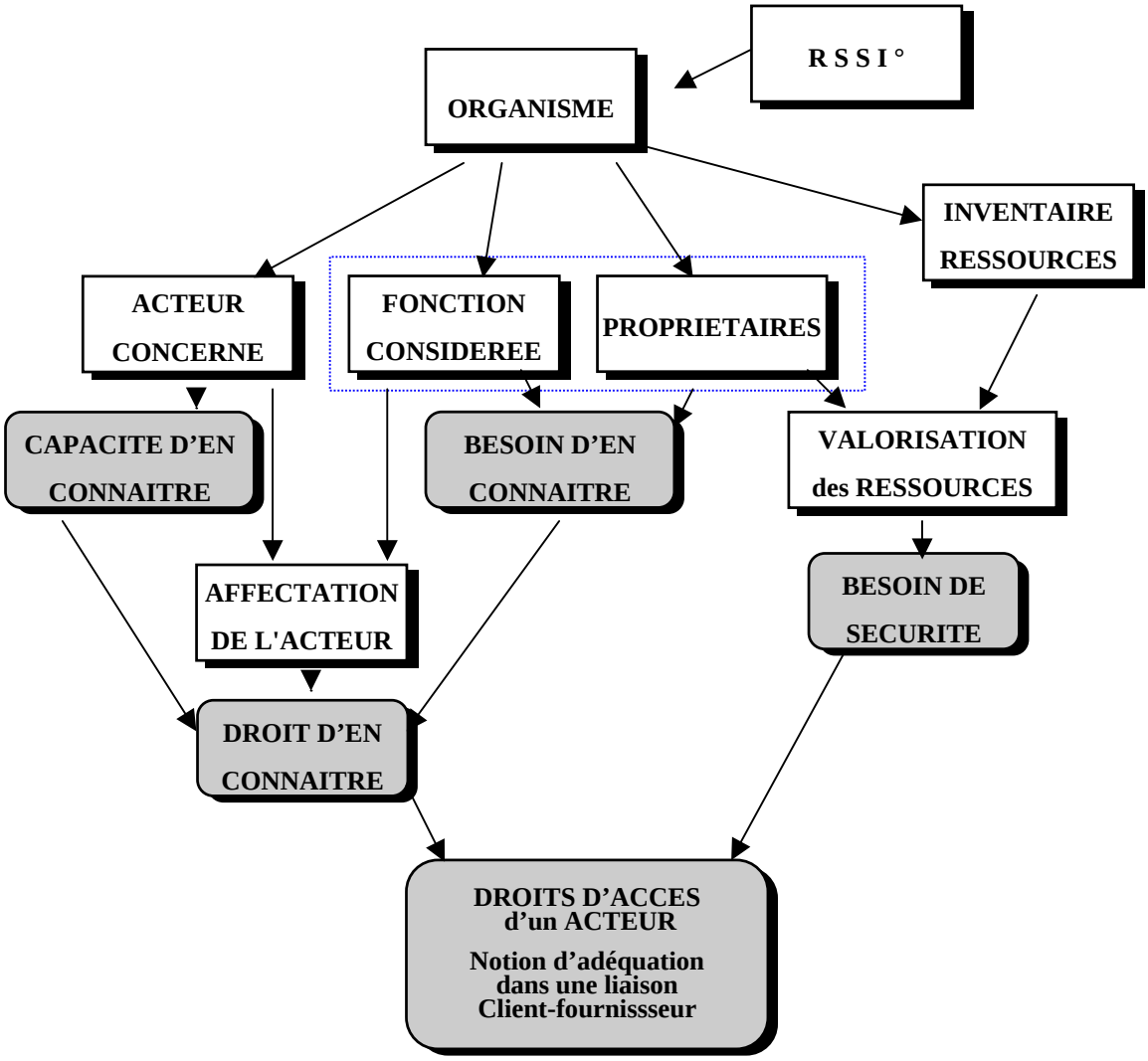


Schéma 2 : modélisation de l'administration des droits d'accès (capacité par personne physique)

Le RSSI (responsable sécurité des systèmes d'information) est à l'initiative de la mise en œuvre et du contrôle de la démarche dans toutes les composantes et à toutes les étapes.

Le schéma N° 2 ci-dessus illustre les axes de la démarche : l'affectation d'un acteur à une fonction d'une part et la valorisation du patrimoine ressources d'autre part.

L'acceptation des droits d'accès n'intervient qu'en dernier ressort par un arbitrage objectif entre la probable légitimité d'un droit d'en connaître d'un acteur et le besoin de sécurité des ressources sollicitées.

Dans cette cinématique, l'organisme accordera directement à ses acteurs une capacité à en connaître. Cette capacité d'en connaître sera confrontée et devra être en adéquation avec le besoin de sécurité, c'est à dire la valorisation, du patrimoine accédé.

Bon nombre d'organismes, pour des raisons culturelles ou organisationnelles, n'expriment pas la capacité d'en connaître au niveau d'une personne physique.

Elles peuvent opter pour une cinématique, telle que celle proposée ci-dessous en schéma 3 et 3 bis, qui intègre la notion de profil d'habilitation (ou métier ou encore rôle). C'est donc le rôle ou le métier considéré qui devient détenteur et porteur d'une capacité d'en connaître et d'un niveau d'habilitation valorisés en lieu et place des personnes physiques.

La nomination d'un collaborateur dans un métier (à un profil d'habilitation) prend alors une importance accrue.

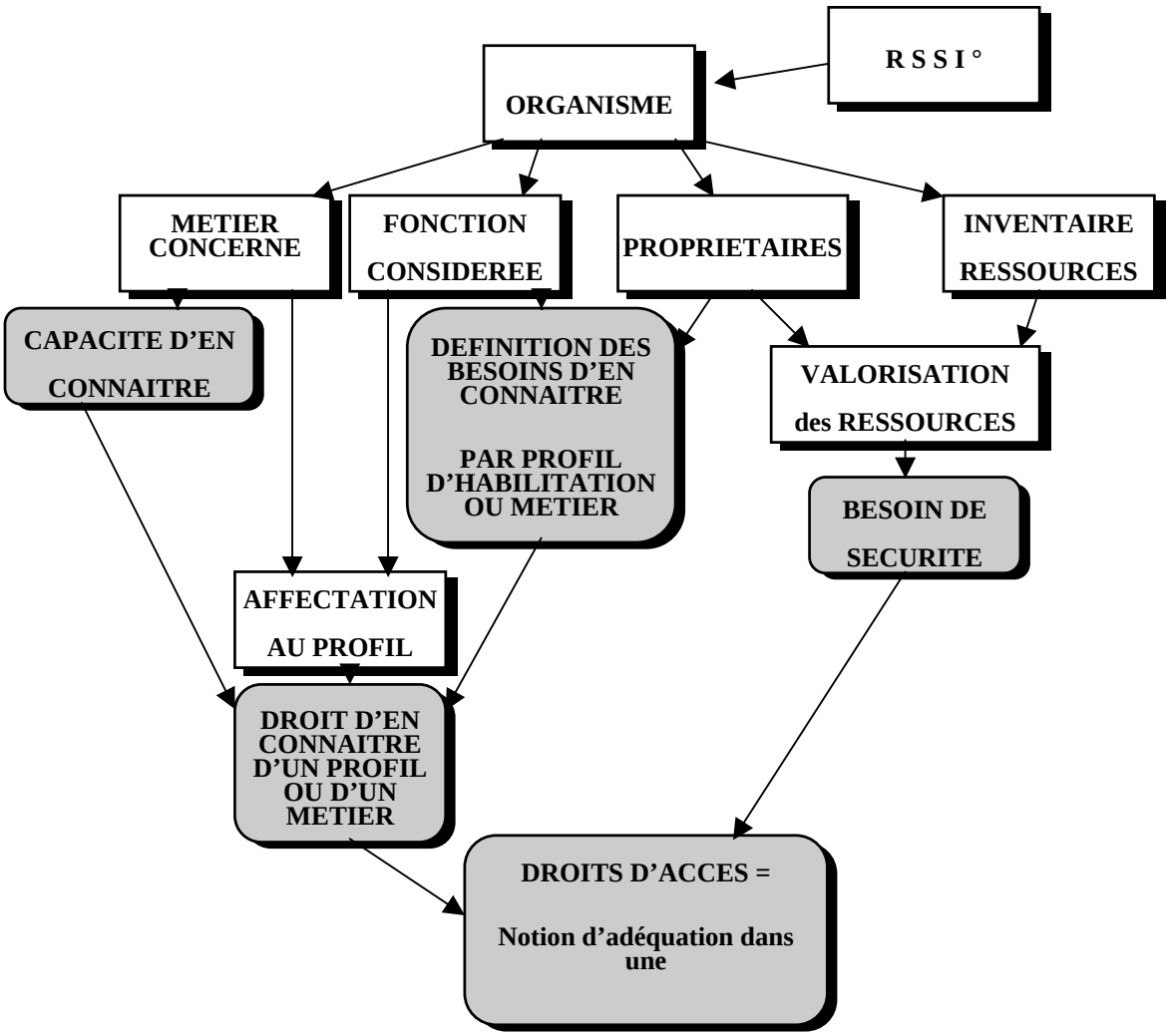


Schéma 3 : modélisation de l'administration des droits d'accès (par profil d'habilitation ou métier)

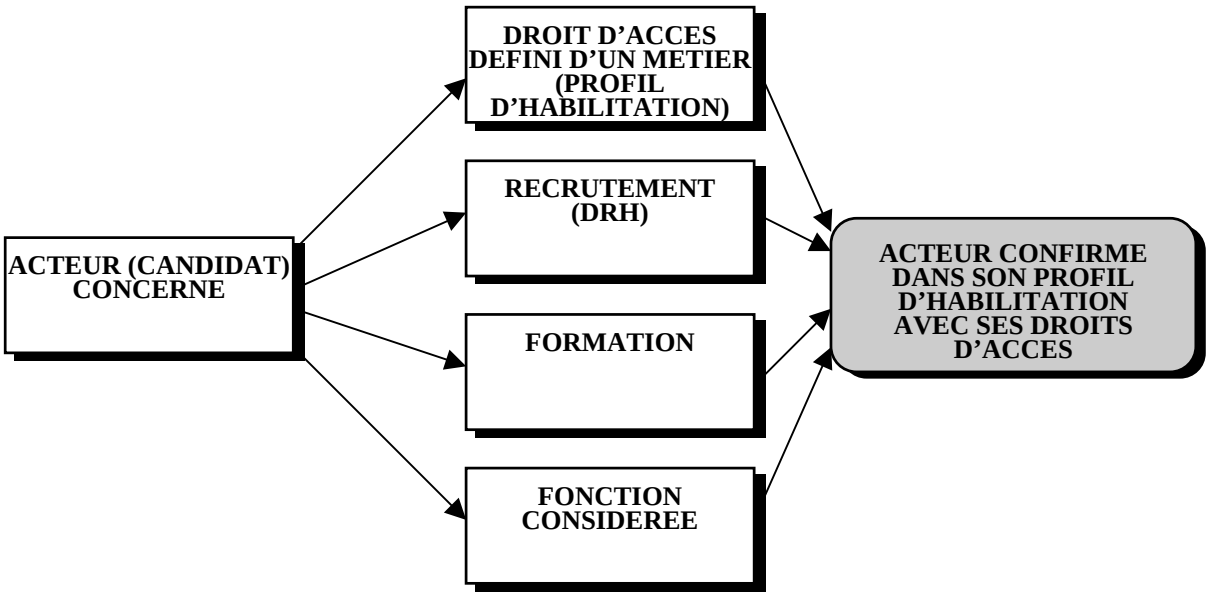


Schéma 3bis : transfert des droits d'accès à un acteur par son affectation à un profil d'habilitation

Ce processus peut-être rapproché de celui de l'héritage dans une architecture objet.

Dans ces schémas 3 et 3 bis, les droits d'accès sont transférés automatiquement aux acteurs par métier avec la capacité d'en connaître correspondante. Le fait d'affecter une personne à un métier témoigne de la reconnaissance d'une capacité à en connaître.

Par exemple : un collaborateur nommé guichetier dans une agence bancaire hérite des droits d'accès du rôle « guichetier » pour cette agence. Parallèlement on veillera à abroger (ou mettre à jour selon le cas) ses anciens droits d'accès.

On pourra adjoindre aux droits du métier des droits complémentaires et spécifiques. En fonction des besoins spécifiques exprimés et justifiés, on complète les droits « métiers » par un processus ponctuel tel que celui indiqué en schéma 2.

3.1 Phase 1 - lancement du projet

En application des recommandations du RSSI, la Direction de l'entreprise - en principe le Comité de Direction (CODIR)- doit objectiver la politique de sécurité :

- Le CODIR statue sur les options fondamentales de la politique de Sécurité qu'il veut faire instaurer,
- Le CODIR demande aux responsables d'activité de définir un étalonnage de sensibilité commun pour les grandes fonctions applicatives du système d'information et effectue éventuellement les arbitrages nécessaires. Cet étalonnage sera d'autant plus facile que les résultats d'un schémas directeur de sécurité (SDSSI) de type MARION ou MEHARI aura préalablement préparé, voire réalisé, le travail. Cet étalon permet aux propriétaires d'évaluer objectivement la criticité des ressources dont ils ont la charge.
- Le CODIR effectue également l'étalonnage du niveau d'habilitation qui sera, selon la culture de l'entreprise, attribué à chaque collaborateur ou à chaque domaine de compétence (ou métier). Cette notion permet de graduer la confiance qu'implique l'affectation d'un collaborateur ou d'un métier à des tâches. Cet étalon permet d'éclairer objectivement le jugement de la hiérarchie intermédiaire dans sa tâche d'affectation des hommes aux différents métiers ou tâches.
- Ces deux étalons doivent être calés selon une même règle de graduation puisque leur utilisation permettra d'apprécier les situations engendrées lors de l'utilisation d'une ressource valorisée par une grille d'étalonnage, par un métier ou un collaborateur valorisé par l'autre grille d'étalonnage.

3.2 Phase 2 - formalisation de l'organisation

Le CODIR assigne ensuite 2 grandes lignes de tâches :

1. A la DRH ou aux hiérarchies, elle confie le soin d'établir l'organigramme hiérarchique,
2. A l'Organisation, elle confie le soin d'établir l'organigramme fonctionnel.

3.3 Phase 3 - conduite des inventaires

Sur instructions du CODIR, la Direction Informatique réalise un travail de préparation significatif :

1. Etablissement d'un inventaire des moyens de production,
2. Recensement des applications et traitements fonctionnant sur ces moyens et contrôle par rapport au portefeuille applicatif ou vice versa.
3. Simultanément, on demande aux différents Responsables Fonctionnels intermédiaires (si et quand ils sont différents des responsables hiérarchiques) de recenser les fonctions nécessaires à l'accomplissement de missions des secteurs dont ils ont la charge, et de les décomposer en "tâches" élémentaires (c'est ce qui définira le "besoin d'en connaître" des personnels sous leur contrôle).
4. Par une investigation fondée sur les connaissances et relations habituelles entre la Direction Informatique et l'Organisation, ces entités vont identifier les propriétaires.

5. Enfin, à l'issue d'un travail conjoint entre les entités précédentes, on procède au raccordement entre d'une part les Applications et Traitements identifiées par la Direction des Systèmes d'Information et d'autre part les "Tâches" identifiées par les Responsables Fonctionnels.

Le résultat ultime de cette décomposition des applications en nomenclatures utilisateurs "fines" est la définition d'une série de "Services", pour lesquels peut-être avancée la définition suivante.

Un service relie, par une règle de sécurité, une tâche et les moyens techniques nécessaires à son établissement. C'est le résultat de l'association logique entre une tâche fonctionnelle d'un utilisateur et un traitement logiquement identifié parmi les ressources informatiques.

Il s'agit ici d'une notion essentielle à la méthode, car ces "Services" sont la charnière entre les domaines utilisateurs et techniques :

- Ces Services doivent rester effectivement compréhensibles pour les Responsables Fonctionnels, qui doivent savoir les traduire en termes de missions de leurs personnels.
- Simultanément, il faut que leur définition soit suffisamment explicite sur le plan technique pour que les systèmes de contrôle d'accès qui doivent prendre le relais de la présente phase d'allocation des droits puissent effectivement le faire sans aucune ambiguïté; dans les cas simples, on pourra quelquefois aller jusqu'au rapprochement avec les traitements élémentaires au sens des Systèmes d'Exploitation, mais il faudra à tout prix éviter d'atteindre un tel niveau de foisonnement dans les cas complexes.

3.4 Phase 4 - Valorisation des ressources

Suivant la politique de chaque entreprise, deux cas généraux peuvent se présenter :

- Soit on a défini que les propriétaires sont des propriétaires d'applications : il leur suffit alors de :
    - ◊ Valider le travail de décomposition des Applications en "Services" effectué lors de la phase précédente,
    - ◊ Valoriser (selon une classification de type DIC) les "Services" liés à leur(s) application(s) à partir de l'étalon approuvé par la Direction Générale,
    - ◊ Vérifier (par exemple à l'aide de simulations) que tout le travail fait à ce stade est bien cohérent avec les responsabilités qu'ils endossent au niveau de leur(s) application(s) en se mettant d'accord une dernière fois avec les Responsables Fonctionnels sur la justification des besoins de Services résultant de l'analyse des modules 6.3 et 7.4 ("besoin d'en connaître") et du minimum niveau de "capacité d'en connaître" requis pour y accéder.
- Soit on a défini que les propriétaires sont des propriétaires "d'objets cibles" (par exemple de fichiers ou de bases de données) : il faut alors procéder à 2 étapes intermédiaires, consistant :
    - ◊ Tout d'abord à décomposer ces objets en composants qui soient élémentaires sur le plan fonctionnel et simultanément insécables au plan de la distribution des droits.
    - ◊ Puis, en liaison directe avec la DSI, à établir un nouveau tableau croisé formalisant les relations entre "Services" et "Objets Elémentaires".

A ce stade, on pourra alors

- Demander aux Propriétaires de valoriser (toujours selon une classification DIC) les "Objets" dont ils ont la responsabilité,
- Simuler les effets de la propagation de ces classifications sur tous les "Services" qui accèdent à ces objets,
- Vérifier avec les Responsables Fonctionnels l'acceptabilité de ces propagations, d'une façon analogue au paragraphe 7.4.1.,
- Procéder avec la DSI et les Responsables Fonctionnels aux ajustements nécessaires.

3.5 Phase 5 - Gestion des hommes

S'appuyant sur l'organigramme hiérarchique défini plus haut, sur attribution du niveau d'habilitation étalonné par le CODIR, et si nécessaire avec l'aide de la DRH, tous les Responsables Hiérarchiques identifient et codifient la "capacité d'en connaître" de chacun des personnels sous leur contrôle.

Selon la culture de l'entreprise, deux options sont prévues par la méthode :

- Attribution directe à un collaborateur (personne physique) d'un niveau d'habilitation précis sélectionné dans l'étalon proposé par le CODIR. C'est la démarche sécurité la plus évidente, mais son application semble difficile dans bon nombre d'organismes français.
- Création de domaines de compétences porteurs d'un niveau d'habilitation représentatif de la confiance attribuée aux collaborateurs qui seront affectés à ces domaines.

Simultanément, les Responsables Fonctionnels enregistrent l'affectation de leurs personnels aux différentes tâches ou domaines de compétences ainsi répertoriés, (cette phase pouvant être précédée, dans certaines d'entreprises, par une présélection des personnels possédant le profil minimum requis (par exemple à l'aide de simulations)).

3.6 Phase 6 - Démarrage

Tous les éléments sont maintenant en place pour pouvoir attribuer à chaque individu une accréditation conforme à sa mission et ses capacités. Cependant, il peut être très important de procéder à des simulations intensives avant la mise en place réelle de façon à pouvoir corriger des déphasages potentiels importants :

- Il peut tout d'abord y avoir une série d'anomalies dues aux imprécisions des inventaires et aux failles de communication entre les différents intervenants. Il faut donc par exemple pouvoir :
    - ◊ Identifier les ressources sans propriétaire et vice versa,
    - ◊ Identifier les responsables sans personnel et vice versa,
    - ◊ Identifier les personnels sans affectation et vice versa,
    - ◊ Etc.
- Il peut ensuite arriver que les besoins que formulent les Responsables Fonctionnels pour leurs personnels soient totalement incompatibles avec les exigences de protection formulées par certains Propriétaires, ou bien il se peut encore que les exigences finales soient incompatibles avec les structures et ressources humaines en place. Il faut procéder à des simulations qui permettent :

- ◊ D'identifier les ressources ne pouvant être accédées par personne,
- ◊ D'identifier les employés ne pouvant accéder aucune ressource,
- ◊ D'identifier les employés pouvant accéder toutes les ressources,
- ◊ D'identifier les services pour lesquels personne ne peut exercer les missions demandées,
- ◊ D'identifier les employés ne pouvant plus exercer leur mission actuelle,
- ◊ D'analyser les situations de cumuls critiques de fonctions,
- ◊ Etc.

4. DEROULEMENT DE LA METHODE

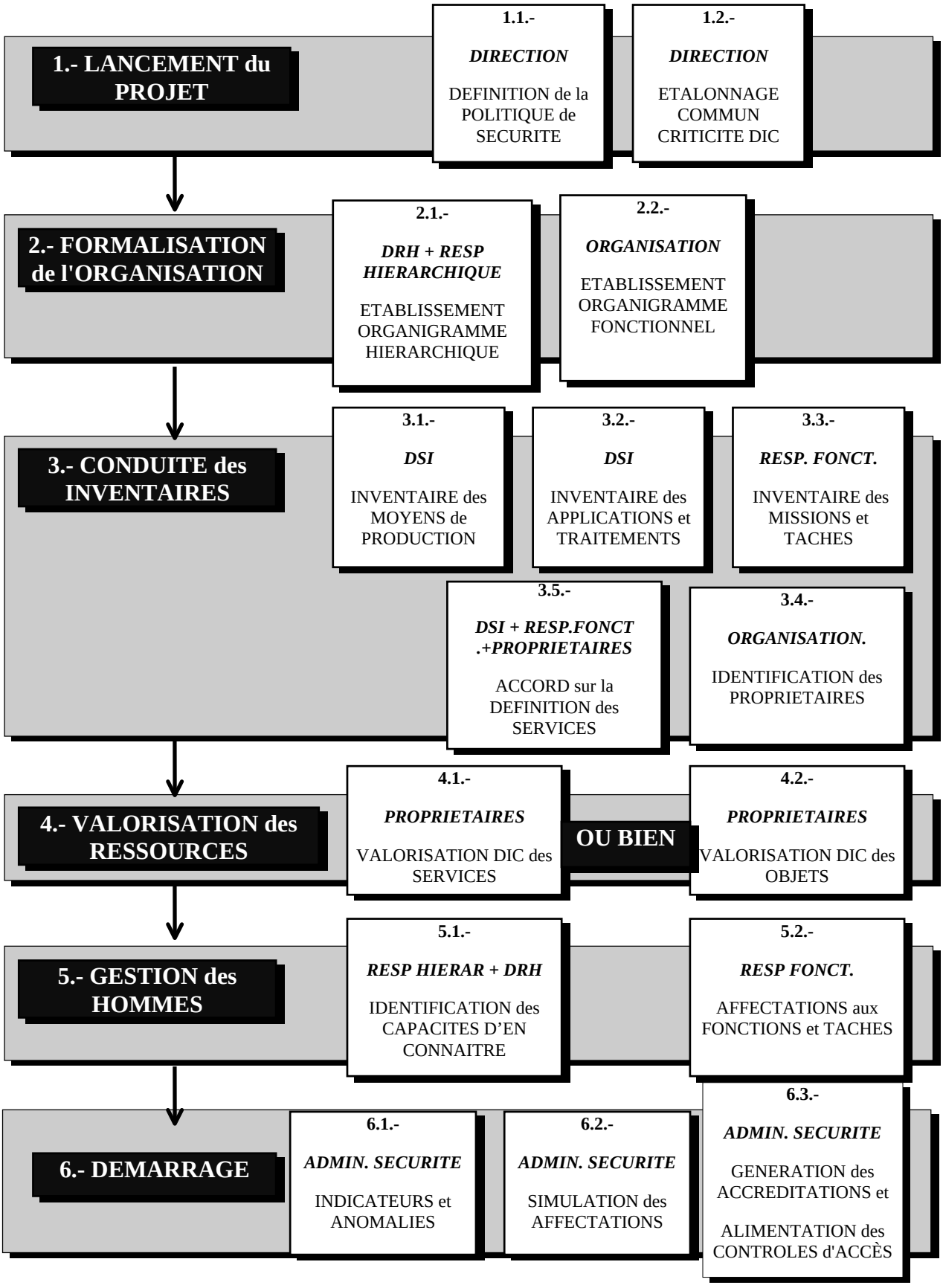


Schéma 4 : déroulement de la méthode

4.1 Rôle de l'équipe sécurité

Outre le fait qu'elle est probablement à l'origine de la mise en œuvre de la méthode, l'équipe sécurité est présente à la réalisation de chacune de ces étapes. Elle apporte aux décideurs le support méthodologique permettant d'objectiver leurs choix et aux opérationnels l'approche méthodologique qui agrège le réalisme du terrain avec les décisions stratégiques. Son rôle d'exécution se verra minimisé au profit d'un rôle d'organisation et de pédagogie.

4.2 Apports de la méthode

La méthode MAGALI comble le vide qui existait entre les SDSSI et les outils techniques de contrôle des droits. Correctement appliquée :

- Elle permet de formaliser l'organisation concourant à l'attribution des droits d'accès
- Elle constitue une aide à la décision dans l'attribution des droits
- Elle aide à l'audit des droits d'accès
- Elle aide à la gestion, voire l'approche industrielle de la gestion des droits
- Elle constitue un référentiel sécurité du patrimoine système d'information

Les concepts mis en œuvre sont les suivants :

1. La méthode prévoit la prise en compte de la **valeur patrimoniale objective** des informations.
2. Cette valeur est **propagée** aux objets techniques à protéger grâce à un inventaire exhaustif technique et fonctionnel des applications utilisées.
3. Le **niveau d'habilitation** accordé aux différents acteurs est déterminé d'une manière individuelle par la hiérarchie immédiate. Il correspond généralement à un profil de qualification auquel est associée la personne. Ce profil de qualification est un élément porteur d'un niveau de confiance.
4. La méthode permet que la gestion des individus d'une part, la gestion des fonctions, et la gestion des ressources d'autre part soient réparties entre des acteurs différents et effectuées d'une façon totalement indépendante, tout en garantissant implicitement une **mise en cohérence permanente.**
5. Les variables techniques relatives à la multiplicité des plates-formes techniques sont **banalisées** dans une approche modélisée des droits d'accès qui privilégie le fonctionnel pour déboucher in-fine sur un interfaçage simplifié avec les solutions techniques.
6. Les missions d'Administrateur Technique évoluent, du fait que les tâches administratives à proprement parler sont complétées au profit d'un renforcement des tâches d'animation et d'audit.

5. LANCEMENT DU PROJET

5.1 Définition de la politique sécurité de l'organisme

5.1.1 Politique d'accès

Le système d'attribution des droits doit fixer une ligne de comportement stratégique vis à vis de la gestion des droits.

Tout d'abord, il faut se décider quant au choix d'une politique de gestion des droits du type :

- Ne rien protéger sauf ce qui est jugé sensible ("tout est permis, sauf ce qui est formellement interdit") : c'est le mode DAC.
- DAC (Discretionnary Access Control : contrôle d'accès discrétionnaire) : se dit d'une politique de contrôle d'accès dans laquelle c'est le propriétaire d'un objet qui indique les droits d'accès des différents utilisateurs. Les objets non répertoriés sont, par défaut, considérés comme non sensibles. Cette démarche est la moins lourde mais elle a pour inconvénient de laisser des intervalles incontrôlés dans la gestion de droits.
- Tout protéger sauf ce qui est jugé non sensible ("tout est interdit, sauf ce qui explicitement autorisé") : c'est le mode MAC.
- MAC (Mandatory Access Control : contrôle d'accès obligatoire) : se dit d'une politique de contrôle d'accès dans laquelle les droits d'accès aux objets sont fixés par un règlement basé sur les niveaux de sensibilité des informations et les niveaux d'habilitation des différents utilisateurs. Les objets non répertoriés sont considérés comme interdits par défaut. Cette gestion est la plus sûre mais elle est devient vite extrêmement lourde à mettre en œuvre.

Cette décision initiale a son importance car dans le 1er cas, une nouvelle ressource oubliée peut ne pas être protégée. A l'inverse, le principe d'exclusion tend à bloquer des droits si on en paramètre l'ouverture préalable.

Ainsi, l'organisme devra adopter une gestion de type DAC ou MAC.

Un compromis s'impose, et la démarche proposée dans ce manuel permet de transiter d'une logique DAC vers une logique MAC (il paraît irréaliste d'exiger d'un organisme ayant un passé et un présent souple qu'il bascule brutalement dans un univers à contrôle total), puis de gérer cette logique avec souplesse tout en augmentant la sécurité globale.

5.1.2 Options d'administration

Les choix d'administration vont être proposés au CODIR et l'amèneront à statuer :

- Si les droits doivent être accordés par la structure hiérarchique ou par la structure fonctionnelle.
- Si un responsable cumule ou non les droits de ses subordonnés (fonctionnels ou hiérarchiques).
- Si l'attribution des droits doit se faire avec double contrôle : délégation hiérarchique d'une part, délégation fonctionnelle d'autre part.

5.2 Etalonnage commun de la criticité DIC

5.2.1 Echelle de criticité - étalonnage

Dans les principes exposés en introduction, on a vu que l'ensemble du schéma de sécurité proposé reposait sur la conjonction entre la vision qu'avaient des Propriétaires d'objets des besoins de sécurité de ceux-ci et la vision qu'avaient les Responsables Fonctionnels des niveaux d'habilitations qu'ils pouvaient attribuer à ces derniers.

Dans ce cadre de responsabilité partagée, il est essentiel que soit défini un langage et un étalon commun de ce qui est "grave", "très grave", ou "sans importance".

Il semble que la notion de "sensibilité DIC" soit de plus en plus familière à de nombreux acteurs concernés par la sécurité des systèmes d'information, et qu'elle puisse être utilisée pour la gestion des contrôles d'accès, qui peuvent effectivement mettre en cause les trois critères de Disponibilité, Intégrité, et Confidentialité.

Il faut fournir d'une part aux propriétaires un étalon standard pour tout l'organisme, qui leur permettra de se caler correctement par rapport à une échelle de sensibilité reconnue de tous et surtout, validée par une étude de risques approuvée par le CODIR et d'autre part aux responsables hiérarchiques une grille équivalente de formalisation des niveaux d'habilitation.

Un exemple de scénario est proposé pour chaque grande fonction et chaque critère DIC ainsi que la typologie des pertes pouvant lui être associées. Le niveau admissible des pertes est hiérarchisé par le CODIR ou les responsables de fonctions dans une grille de criticité. Cette grille sera utilisée par les propriétaires pour valoriser les ressources dépendant de leur domaine.

On peut proposer comme base le modèle ITSEC qui pourra être complété par des informations spécifiques à l'organisme. Une fois que l'on a défini les étalons communs à l'organisme, la classification des objets est obtenue à l'aide d'une analyse de risques portant sur les systèmes d'informations existants (à l'occasion d'un SDSSI MEHARI ou MARION par exemple) ou sur les systèmes d'information en cours de conception ou de mutation (application d'une démarche d'intégration de la sécurité dans les projets du type INCAS). L'un des résultats de ces analyses de risque sera donc la classification de tous les objets analysés en terme DIC. Pour les Propriétaires, chaque domaine applicatif ou fonction applicative pourra ainsi être valorisé (après que tous se soient mis d'accord sur la signification des mots "nul", "faible", sensible" etc.) par rapport à un modèle du type :

NIVEAU de SENSIBILITE	D	I	C	NIVEAU DES ENJEUX
NIVEAU 0	x	x	x	ENJEU NUL
NIVEAU 1	x	x	x	ENJEUX FAIBLES
NIVEAU 2	x	x	x	ENJEUX SENSIBLES
NIVEAU 3	x	x	x	ENJEUX CRITIQUES
NIVEAU 4	x	x	x	ENJEUX STRATEGIQUES

5.2.2 Niveau d'habilitation - étalonnage

Dans les principes exposés en introduction, on a vu que l'ensemble du schéma de sécurité proposé repose sur la reconnaissance de la notion de criticité DIC à l'égard du patrimoine. Il est donc pertinent d'étalonner l'attribution des niveaux d'habilitation par une approche de même nature.

Ce niveau correspond au niveau de risque qu'un organisme accepte de courir en accordant à une personne physique des droits et donc un pouvoir lui permettant d'agir sur la confidentialité, l'intégrité, la disponibilité d'un bien matériel ou immatériel mis à sa disposition dans le cadre d'une mission précise.

Selon la culture managériale de l'entreprise, le niveau d'habilitation peut être :

- attaché à une personne physique (ce qui correspond à la culture anglo-saxonne ou aux procédures du domaine de la défense) et auquel cas on parlera de notion de degré de confiance
- attaché à un profil de qualification qui correspond à une notion de métier et dans ce cas, c'est l'action d'affecter une personne à ce profil qui témoigne du degré de confiance accordé.

Dans ces deux cas, le contexte opérationnel (par exemple la fonction ou l'affectation) ne doit pas influer sur le degré de confiance mais lui être combinée afin d'effectuer les bons choix de management, ce sur quoi nous reviendrons.

Cette notion de degré de confiance existe depuis longtemps dans de nombreux domaines et ce n'est pas le contexte des contrôles d'accès logiques aux informations qui la rend nécessaire. A titre d'exemple on peut citer des domaines où elle se pratique couramment :

- Habilitation défense nationale,
- Niveau de signature dans l'engagement de dépenses d'une entreprise,
- Niveau d'autorisation dans l'engagement de risques d'une banque,
- Confier les clés du coffre,
- Ou tout simplement le code d'alarme des locaux,
- Etc.

5.2.2.1 Principes

Parler de degré de confiance est une affaire extrêmement délicate. Les lois sociales ainsi que les textes traitant de l'informatique et des libertés imposent la plus grande prudence à ce sujet. Le niveau de sensibilité du dialogue social dans une entreprise est un facteur qui amplifie cette nécessaire prudence. Les organisations proches des domaines de la défense ou bien de culture anglo-saxonne se sont, depuis longtemps, accomodées de ces contraintes. Dans beaucoup d'autres organismes, on se refusera à parler de degré de confiance accordé à un individu et on lui préférera la notion de profil de d'habilitation (ou profil de droit) accordé à une personne et porteuse d'un niveau de confiance cohérent avec l'affectation de cette personne. Au plan du fonctionnement de la méthode MAGALI, cette nuance est acceptée. Elle doit néanmoins être manipulée avec précaution puisqu'elle a pour effet d'interposer un profil d'habilitation entre la personne physique et les informations accédées, ce qui peut réduire l'efficacité du concept.

Malgré tout, dans les entreprises et dans les organismes, la réalité quotidienne nécessite de connaître puis d'inclure à une structure opérationnelle le degré de confiance, le profil de droit (ou le profil de qualification) que l'on peut accorder à un individu. Les critères de choix qui sont à prendre en compte pour cette évaluation sont des critères objectifs et subjectifs.

Les critères subjectifs ne sont pas exposés dans ce document puisqu'ils ne concernent que la responsabilité et la conscience de ceux qui les prennent en compte à tort ou à raison.

Les critères objectifs, quant à eux, ne posent pas de problèmes spécifiques parce qu'ils s'expliquent au quotidien dans le vécu de l'entreprise ou de l'organisme. Ils sont connus, publiés par des canaux

différenciés. Ils peuvent être calqués sur des critères identiques aux critères d'embauche ou de promotion :

- Niveau de formation, cursus professionnel,
- Niveau de grade ou de qualification,
- Ancienneté dans une entreprise,
- Ancienneté dans un poste ou dans un grade,
- Confiance accordée aux salariés prestataires de services,
- Objectifs atteints, motivation, bilan annuel,
- Etat psychologique ou physiologique au moment de l'affectation
- Casier judiciaire,
- Etc.

5.2.2.2 Classification du niveau d'habilitation

On a vu dans le chapitre 1 que l'établissement d'une grille universelle d'étalonnage était essentiel, et qu'on pouvait, afin de simplifier la mise en œuvre, classifier le niveau d'habilitation selon le modèle ci-dessous. Cette grille indique le niveau de risque que l'on accepte d'engendrer en affectant une personne physique à un profil de droit :

NIVEAU 0	ACCES OU MANIPULATION D'OBJETS NE PRESENTANT AUCUN RISQUE
NIVEAU 1	ACCES OU MANIPULATION D'OBJETS PRESENTANT UN RISQUE LIMITE
NIVEAU 2	ACCES OU MANIPULATION D'OBJETS SENSIBLES
NIVEAU 3	ACCES OU MANIPULATION D'OBJETS CRITIQUES
NIVEAU 4	ACCES OU MANIPULATION D'OBJETS STRATEGIQUES

L'étalonnage de cette grille doit être cohérent avec celui de la grille de criticité des ressources. La mise en cohérence des 2 grilles (personnes ou métiers, et objets) est l'un des moteurs de la méthode MAGALI, elle permet d'objectiver les risques liés à l'attribution des droits.

Les organismes qui le souhaitent peuvent différencier le profil d'habilitation d'un même individu à l'égard des critères DIC (disponibilité, intégrité, confidentialité). Cette complication apparente peut au contraire être utilisée de manière efficace dans l'attribution de droits d'accès logiques. La prise en compte de ce principe ne peut être que le fruit d'une réflexion spécifique à chaque organisme et ne constitue pas une règle.

6. FORMALISATION DE L'ORGANISATION

6.1 Principes

Gérer les droits d'accès dans un organisme complexe nécessite de décliner progressivement les **identités des acteurs** dans leur **position hiérarchique** ainsi que dans leur **fonction,** puis de gérer cette situation dans une parfaite adéquation avec la **réalité opérationnelle** (entendons par réalité opérationnelle : les embauches, les départs, les mutations, les réorganisations qui modifient, suppriment, créent, étendent ou limitent des droits, les affectations temporaires, la création de groupes de travail adéquats...). La réalité des organigrammes d'entreprises étant parfois floue, il parait souhaitable que les notions d'organigrammes hiérarchique et fonctionnel soient suffisamment dissociées pour s'adapter à toutes les situations, quitte à ce qu'elles soient « plaquées l'une sur l'autre » lorsque le contexte l'exigera.

6.2 Établissement de l'organigramme hiérarchique

6.2.1 Identification des « acteurs » (ou utilisateurs)

Dans une organisation idéale, il est essentiel que la gestion des droits d'accès soit raccordée au système de gestion informatisé du référentiel (l'annuaire) des personnels. Ceci doit s'opérer le plus dynamiquement possible, voire en temps réel. Si tel n'est pas le cas, un chargement manuel s'impose.

Dans ces conditions, les délais et procédures de mise à jour de l'annuaire informatisé doivent être extrêmement rigoureux. Cette remarque vaut autant pour la mise à jour des noms, prénoms, que pour celle des fonctions occupées, du service de rattachement, des dates effectives de validité. L'annuaire devenant l'un des socles de la gestion des droits d'accès, la qualité de sa mise à jour est stratégique.

Bien entendu, le référentiel 'source' doit être protégé, ainsi que le chemin des mises à jour vers le système de gestion des droits d'accès.

6.2.2 Organigramme hiérarchique

Après avoir pris en charge manuellement ou automatiquement la liste des acteurs, la description détaillée de l'ensemble de la structure hiérarchique doit être établie et prise en compte dans le dispositif d'attribution des droits. La hiérarchie peut seule définir les niveaux d'habilitation et/ou de délégation des personnels sous son contrôle (niveaux qui seront essentiels pour ultérieurement pouvoir accorder, modifier, ou supprimer les droits liés à l'activité de telle ou telle personne).

S'il n'existe pas un organigramme hiérarchique suffisamment à jour pour servir de base à l'enrichissement de la méthode, une série d'interviews des principaux niveaux hiérarchiques permettra d'en constituer le cadre. Il faut ensuite poser la question à chaque intéressé afin de savoir de qui il dépend hiérarchiquement : en clair, « qui le note, qui l'augmente».

Le décodage du puzzle hiérarchique risque également d'être révélateur d'anomalies liées à un historique de management plus ou moins bien géré : prérogatives d'ancienneté, prérogatives de positions débouchant sur des droits exorbitants, etc.

L'absence d'organigramme va générer une approche par « tâtonnements ». Les réponses sont à prendre avec prudence, les collaborateurs peuvent confondre (et on les comprend) les notions de responsable hiérarchique (qui note, qui augmente,...) avec celle de responsable fonctionnel (qui donne les moyens de travailler, qui distribue le travail,...). Il faut être prudent tout au long de l'élaboration des organigrammes et, lorsqu'il est nécessaire de les dissocier, de ne jamais confondre les notions de fonctionnel et de hiérarchique

6.3 Etablissement de l'organigramme fonctionnel

6.3.1 Fonctions d'utilisateurs (ou d'usagers) Fonctionnels

Il s'agit de la définition précise et codifiée des fonctions liées aux métiers de l'Organisme qui souhaite mettre en place une politique de Sécurité.

L'organigramme fonctionnel doit décliner progressivement l'organisme sous forme de fonctions/ sous fonctions/ activités/ etc. Sa définition jusqu'au niveau le plus élémentaire (ceci n'est pas péjoratif) de décomposition par tâches de travail s'effectuera dans l'étape 3.3 « inventaire des missions et des tâches ». Au stade où nous en sommes il faut décliner l'organigramme jusqu'au niveau du poste de travail, qui souvent sera redondant entre plusieurs individus.

L'organigramme fonctionnel est particulièrement adapté aux structures « projets » ou aux activités transverses qu'engendrent les organisations modernes des entreprises. D'autre part, les implantations géographiques différenciées peuvent engendrer des structures fonctionnelles différentes des structures hiérarchiques : un collaborateur commercial en province peut fonctionnellement dépendre d'un chef des ventes situé en région parisienne et hiérarchiquement du chef d'établissement de province.

Exemple : Direction Financière

Département Comptabilité

Division Métropole et DOM

Secteur Comptabilité Nord-Pas-de-Calais

Unité de Comptabilité Clientèle

Groupe Gestion Factures

Le recensement des fonctions, sous-fonctions, activités est en général déjà réalisé dans la plupart des organismes. Si c'est le cas, et si la mise à jour en est rigoureuse, il est réutilisable dans le système de gestion des droits d'accès. S'il ne l'est pas, il faut s'attaquer à cette tâche qui, si elle n'est pas épaulée par des moyens logiciels, peut se révéler longue et fastidieuse. La gestion actuelle des droits d'accès a probablement engendré ce travail sous une forme ou sous une autre.

6.3.2 Fonctions d'administration technique des systèmes

Il ne s'agit pas ici de traiter des fonctions d'administration des logiciels de contrôle d'accès ou de mise à jour des droits d'accès, mais des fonctions d'exploitation informatique, d'administration des réseaux ou d'équipes systèmes, etc. (cette liste n'est pas exhaustive); c'est à dire de gestion technique des équipements supportant les systèmes d'information.

Par définition, les droits d'accès de ces acteurs seront nettement différenciés de ceux des utilisateurs fonctionnels puisqu'ils ne se réfèrent pas à l'exercice direct des métiers de l'organisme. Ces droits n'en sont pas moins sensibles, au contraire : les risques liés à ces activités sont très importants de par la violence d'impact des actions qu'ils autorisent et par la difficulté technique qu'il y a à juguler les risques engendrés. Par exemple les besoins d'accès d'une équipe d'exploitation ou d'un administrateur de réseau ou d'une équipe système sont extrêmement difficiles à réguler, et à défaut, ils sont très dangereux à l'égard des systèmes d'information concernés.

Il convient donc de préciser les droits fonctionnels des équipes techniques. Cet organigramme fonctionnel doit également être décliné en fonctions/ sous-fonctions puis tâches d'administration.

Exemple : Direction informatique

Département exploitation

Secteur pilotage et pupitre

Unité de gestion du système central

Tâche de gestion des sauvegardes

Tâche de lancement des travaux

7. CONDUITE DES INVENTAIRES

7.1 Principe

Dans ce chapitre on appelle inventaire :

- Le recensement des moyens de production supportant l'exécution concrète du fonctionnement des systèmes d'information y compris la gestion technique des données : « les ordinateurs ».
- Le recensement des applications constitutives de ces systèmes d'information et plus précisément des traitements fonctionnels qui doivent s'établir entre l'activité (fonctionnelle et opérationnelle) et les ressources.
- Le recensement des propriétaires pouvant statuer de la criticité des dits objets et de l'opportunité ou non d'accorder à telle fonction utilisatrice le droit accéder,
- Le recensement des services, charnière ultime de la démarche MAGALI vers les outils techniques d'administration des droits
- Le recensement des missions et tâches pouvant accéder à ces services, cette dernière étape étant la forme de déclinaison la plus fine de l'organigramme fonctionnel.

7.2 Inventaire des moyens de production

Pour le périmètre de la méthode, nous limitons la portée du vocable « moyens de production » aux serveurs de toutes plates-formes permettant d'accéder aux ressources qu'ils exploitent et qui sont à protéger : il s'agit donc de serveurs de toutes dimensions, éventuellement d'ordinateurs personnels.

Cette tâche doit naturellement être confiée aux équipes de production ou d'administration de réseau où encore d'architecture technique.

Il est important de cerner le périmètre exact défini à la mise en œuvre des accès logiques. Tous les serveurs ou ordinateurs individuels doivent être répertoriés afin de ne pas omettre « l'ordinateur placé dans un coin de salle noire et que tout le monde oublie » mais qui détient des données extrêmement sensibles. Cette remarque un peu caricaturale vaut particulièrement pour les organisations complexes où l'architecture des systèmes d'informations a fait proliférer les « machines » et où le périmètre du parc est parfois flou.

Il faut recenser les serveurs d'entreprise ou « mainframes » et les recenser s'il le faut en tenant compte de leur partitionnement fréquemment répandu dans ces architectures : par exemple le mainframe « cloisonné » entre les partitions production, études, intégration-recette, infocentre,... Le niveau d'inventaire doit s'en tenir à ce simple recensement du moins dans un premier temps.

Il faut ensuite répertorier les serveurs mutualisés ou spécialisés par l'architecture technique-applicative ou bureautique: le serveur monétique, le serveur télématique, le serveur bourse ou front-office, le serveur d'impression, le serveur mutualisé de fichiers administratif, etc.

Il faut enfin recenser le parc d'ordinateurs individuels connectés ou non à ce réseau. La prise en compte des ordinateurs individuels dans l'inventaire des moyens de production à protéger est affaire de culture d'entreprise

7.3 Inventaire des applications et des traitements

7.3.1 Inventaire au plan fonctionnel

La recherche d'un langage commun permettant à un utilisateur d'exprimer fonctionnellement son « besoin d'en connaître » auprès d'un technicien informaticien « pur et dur », qui manipule de manière industrielle des nomenclatures essentiellement techniques, n'est pas chose aisée.

Bien sûr, il y a les contre-exemples où l'utilisateur est capable d'exprimer ses « besoins d'en connaître » sous des dénominations identiques à celles utilisées par les équipes techniques et les équipes de projet. Ces cas ne constituent pas la règle dans des systèmes d'information importants et/ou complexes. Il faut donc articuler le dispositif de telle sorte que le lien puisse être établi entre le monde fonctionnel des utilisateurs et le monde technique des informaticiens.

La première étape de réalisation de ce lien consiste à faire dresser un inventaire des applications et traitements (par les équipes de projet si possible) dans un mode d'expression qui soit compréhensible ultérieurement des utilisateurs dans le cadre de leur « besoin d'en connaître », puis des techniciens lorsqu'il faudra mettre en cohérence le besoin ainsi exprimé avec les ressources techniques mises en œuvre.

Moyen de production après moyen de production, la Direction des Systèmes d'Information va identifier les applications fonctionnant sur ces systèmes puis identifier les principaux traitements composant ces applications.

Cet inventaire est fonctionnel, il ne recense pas les ressources techniques des systèmes. L'étude doit plutôt être menée par les équipes de maîtrise d'œuvre afin d'identifier les applicatifs et les traitements sur un plan « métier ». Répétons le une fois encore : la qualité de cet inventaire est stratégique car il va constituer le trait d'union entre l'expression, pas toujours bien exprimée des Utilisateurs en situation de travail d'une part, et la réalité opérationnelle des ressources en ligne exprimée par les nomenclatures ésotériques des informaticiens d'autre part.

Exemple très simplifié de ce que peut être cet inventaire :

Moyen de production	Application	Traitements fonctionnels	Description complémentaire
Grand système : partition de production	Paie	Modification des éléments variables pour les cadres	Transaction terminal MODVAR1
Grand système : partition de production	Paie	Modifications des éléments variables pour les employés et ouvriers	Transaction terminal MODVAR2 et 3
Mini-système : partition de production	Comptabilité	Saisie des factures clients	Transaction CLI1/CLI2/CLIRT
Serveur Novell	Comptabilité	Saisie des relances	Accès à l'interface applicatif RELANCES

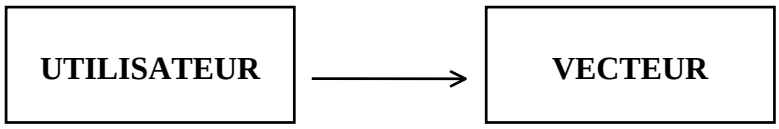
			Préciser sous quel directory.
Serveur Novell	Comptabilité	Saisie des écritures	Accès au logiciel de comptabilité CMTA

7.3.2 Inventaires par typologie de traitement

L'enrichissement des traitements fonctionnels ne serait pas complet s'il n'était complété d'une notion fondamentale : la typologie de traitement.

7.3.2.1 Notion de « vecteur »

Toute exécution d'une fonction quelle qu'elle soit dans un ordinateur se traduit par l'exécution d'un segment plus ou moins important de code que nous nommons universellement « exécutable ». Ainsi seront indifféremment considérés comme exécutables : un traitement dans un moniteur transactionnel, une requête adressée à une base de données au travers un SGBD, un exécutable type Word ou Excel sous Windows, un logiciel « data-mover » assurant une sauvegarde, une commande à un système propriétaire, un programme batch placé ou non sous contrôle d'un automate, etc. Les variétés sont nombreuses mais le concept est aisé à comprendre.



Par définition, ces entités sont toutes celles par lesquelles transitent la demande d'information de l'utilisateur et constituent des « vecteurs ». Mais ce sont elles aussi qui véhiculent les menaces, quand elles deviennent pas pleinement des amorces de risques.

Pour ce type d'objets, la mise sous contrôle strict peut souvent ne pas être opportune voire même concevable (par exemple programmes utilitaires ou modules de Système d'Exploitation); en outre, les progrès de la technologie ne permettant pas encore, dans de nombreux cas, d'assurer une gestion intrinsèque sophistiquée de nombreux vecteurs (imprimantes, stockages de masse...).

Dans certains cas des traitements fonctionnels ne peuvent être régulés par des outils techniques mais uniquement par des dispositions applicatives contenues dans le vecteur ou dans une table en concordance avec le vecteur. Dans ce cas, c'est à ce stade de l'étude que l'inventaire devra être enrichi : par exemple, un même traitement, sous un même exécutable permet de générer des ordres de virement et les droits doivent selon les individus (et le niveau d'habilitation) être accordés avec des plafonds progressifs .Par exemple, X a droit d'émettre des virements jusqu'à 50KF et Y a droit jusqu'à 500 KF. Auquel cas, les mécanismes de sécurité devront pouvoir interfacer avec les mécanismes applicatifs chargés de réguler ces seuils.

7.3.2.2 Notion de « cible »

Un exécutable a généralement pour mission de consulter ou de modifier des données. Selon que son utilisation est correctement régulée ou non, c'est l'exécutable qui risque de porter atteinte à la confidentialité, à l'intégrité, à la disponibilité des informations. Le vecteur peut lui même être la cible d'un autre vecteur : par exemple, une manipulation sous un éditeur peut altérer un exécutable et en changer le mode de fonctionnement.

Ce sont les seules entités dans lesquelles les utilisateurs sont réellement intéressés. Mais ce sont aussi celles qui sont la proie finale de toutes les erreurs, fraudes, et malveillances véhiculées par les éléments précédents.

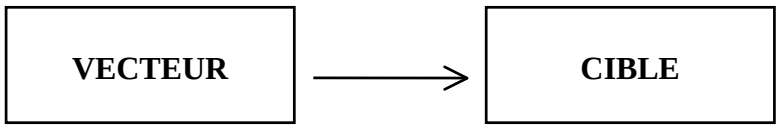
Il s'agit le plus souvent d'éléments d'information ou d'algorithmes, et la situation des cibles est très différente de celle des vecteurs par plusieurs aspects :

- à l'opposé des vecteurs, il est vital que chacun des objets de ce type soit parfaitement identifié et possède des moyens de protection spécifiques, puisque d'une part c'est finalement du bien fondé ou du mal fondé de son accès que naîtra l'éventuelle perte de sécurité, et que d'autre part, la sécurisation des vecteurs étant encore en général très fallacieuse, c'est à ce niveau qu'on devra exercer tous les efforts ;
- par contre, on dispose d'un peu plus d'outils généraux pour assurer la gestion de la sécurité de ces cibles : même si rien n'est généralement disponible au niveau de la protections des enregistrements individuels d'une table ou d'un fichier, la plupart des Systèmes d'Exploitation actuels met à disposition des moyens de restriction de l'accès soit aux tables ou fichiers eux-mêmes, soit au niveau des répertoires qui les recensent.

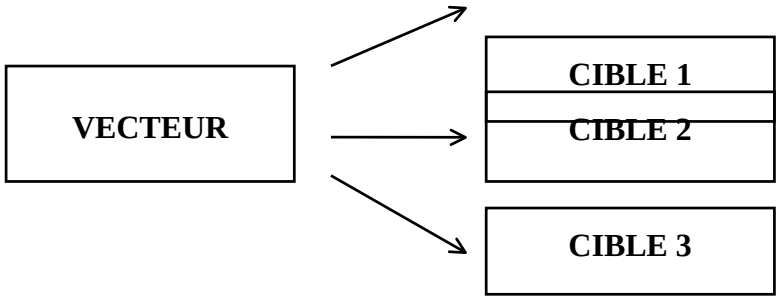
7.3.2.3 Les deux typologies de traitements

Il ne peut être question de protéger tous les vecteurs et toutes les cibles sans risquer de compliquer à l'infini une gestion déjà délicate. Il est donc important de protéger la bonne ressource - vecteur ou cible - au cas par cas avec opportunité et pour cela on va distinguer deux types de traitements :

- **les traitements spécialisés**, c'est à dire ceux qui sont canalisés dans un type d'exécution précis et dont la déviation n'est pas possible à partir de leur exécutable normal. Concrètement ils viennent consulter ou modifier une cible précise : exemple, une transaction TP modifie de façon extrêmement dirigée un fichier précis.



- **les traitements généralisés (ou banalisés)**; c'est à dire ceux qui permettent à partir d'un exécutable donné d'effectuer des opérations très diverses sur des cibles diversifiées : exemple une application Word ou Excel permettant de modifier de nombreux de fichiers. Pire encore, un programme éditeur capable d'altérer tout fichier placé sous son exécution.



On voit dans ces quelques schémas et exemples que selon le cas il sera opportun de protéger la ressource vecteur et dans d'autres les ressources cibles.

Un rapprochement de ces concepts avec les populations d'utilisateurs devient pertinent. Ainsi il sera préférable, a priori, dans les organisations où les ressources sont massivement mutualisées (exemple des traitements TP s'exécutant sur un grand système), de réglementer les accès des utilisateurs fonctionnels en protégeant les objets vecteurs puisqu'ils sont canalisés vers des algorithmes précis agissant sur des cibles limitées. Lorsqu'il s'agira de ressources peu mutualisées, par exemple les fichiers bureautique d'un serveur on protégera les cibles c'est à dire les fichiers dans leurs répertoires. (La protection contre les virus macros requiert cependant des approches spécifiques).

Lorsqu'il s'agira de réglementer les accès des équipes d'informaticiens, les ressources à protéger seront toutes assimilées à des cibles : vis à vis de ces populations les vecteurs étant à considérer comme des cibles.

7.4 Inventaire des missions et des tâches

Cette étape a pour objet de déterminer le « besoin d'en connaître » d'un utilisateur en situation de travail. Nous avons étudié plus haut la formalisation de l'organigramme fonctionnel. Couche par couche, filière par filière cela a permis de reconstituer « qui donnait à qui les instructions de fonctionnement » déclinant ainsi progressivement la stratégie opérationnelle de l'organisation.

La définition la plus fine de l'organigramme nous amène à un niveau générique d'inventaire des missions insuffisamment détaillé pour identifier « le besoin d'en connaître » d'un utilisateur en situation de travail. Il va donc falloir, par un zoom complémentaire, décomposer plus finement la structure fonctionnelle, définir les activité, tâches et sous-tâches constitutives des « besoins d'en connaître » concrets.

Commençons par la définition du PETIT LAROUSSE

Besoin : "ce qui est nécessaire ou indispensable",

Connaître : "être renseigné sur l'existence et la valeur de quelque chose".

Dans le cadre de sa fonction, chaque employé se voit confier des missions définies par sa hiérarchie dans le cadre de la politique de l'entreprise. Pour les accomplir, un certain nombre de "ressources" lui sont nécessaires qui constituent son "besoin d'en connaître". Cette notion doit correspondre aux "outils" minimum que doit mettre à sa disposition l'entreprise pour qu'il mène avec succès ses missions.

7.4.1 Expression et validation du besoin

Dans un monde idéal, les besoins en ressources auxquels est confronté chacun des employés pour mener à bien sa mission devraient être définis par les responsables fonctionnels ou hiérarchiques respectifs, puis être validés par les "propriétaires" des différentes ressources concernées.

Pour éviter les imprécisions génératrices de gabegies, de manques ou des deux, la déclinaison de l'organigramme fonctionnel doit être continuée au niveau le plus fin des missions et des tâches. A partir de ce zoom, l'inventaire des traitements fonctionnels décrivant le « besoin d'en connaître d'un utilisateur devient possible sans excès.

L'expression, la formalisation et la validation du besoin aboutissent à la définition de "catégories" d'habilitation représentatives des droits "génériques" de groupes d'employés.

On peut donc modéliser ce processus en disant que l'accomplissement d'une mission définit un droit d'en connaître (besoin d'en connaître pondéré par la capacité d'en connaître) qui constitue une catégorie d'habilitation, composée d'habilitations et d'accréditations.

La certification qualité est exigeante concernant la définition des postes et lorsque l'opportunité s'en présentera, on pourra mettre à profit cette démarche pour s'approprier des résultats dont l'utilisation se révélera certainement fructueuse pour cette phase.

C'est le rôle des responsables fonctionnels qui doivent aller dans le détail des tâches réalisées dans leur périmètre de compétence. Hélas, dans la pratique, le besoin de ressources est souvent exprimé et justifié par l'employé, qui va ensuite quémander une habilitation.

Plusieurs cas pourront se présenter :

1. Premier circuit (celui que recommande la présente méthode) : les responsables fonctionnels décomposent finement les fonctions, missions, activités et tâches dont ils ont la charge puis décomposent les besoins jusqu'au niveau le plus fin c'est à dire celui de service. Ils peuvent bien entendu s'appuyer sur l'organisation pour l'exécution de cette tâche.
2. Second circuit : le propriétaire désigne les fonctions ou services susceptibles d'utiliser les ressources sous son contrôle et dans quelles conditions elles peuvent le faire ; les responsables de ces fonctions et services procèdent ensuite à l'affectation de leurs employés ;
3. Troisième circuit : le besoin est exprimé par l'employé et/ou son responsable hiérarchique, puis validé ou non par le propriétaire de la ressource pour laquelle une demande est présentée ;
4. S'il n'existe aucun propriétaire, le besoin est exprimé par l'employé puis validé par son hiérarchique ou l'administrateur de la sécurité.

La mise à disposition des ressources ne peut se concevoir que dans le cadre d'une allocation temporaire de moyens définis à partir de l'expression du besoin. Ceci ne pourra se faire de façon satisfaisante qu'à la condition que l'entreprise ait réalisé un inventaire complet de ses ressources et qu'elle valide avec rigueur les mises à jour permanentes dans les affectations des hommes.

Le besoin est directement lié à la fonction mais reste évolutif car il dépend de variables aussi diverses que :

- La durée : si la date de début est en général maîtrisée, la fin peut être liée à une période d'intérim par exemple, mais aussi à des obligations techniques, professionnelles ou juridiques,
- Le lieu : une restriction peut être imposée sur le lieu à partir duquel certaines opérations doivent être réalisées,
- La plage d'utilisation : typiquement les besoins d'un employé sont censés être, sauf exception justifiée, bloqués les jours de fermeture de l'entreprise et pendant ses congés,
- Les impératifs du contrôle interne : le principe de séparation des pouvoirs peut entraîner le refus de certaines autorisations pour des emplois sensibles,

La sécurité la plus élémentaire voudrait qu'en cas de changement de poste ou de fonction, le besoin d'en connaître de tout employé soit redéfini et que ses précédents droits soient purement annulés et

ramenés à la catégorie la plus faible. Cette opération est facilement automatisable si l'entreprise dispose d'un organigramme informatisé, tout changement de poste entraînant automatiquement la modification des droits.

Les fonctions d'un poste pouvant évoluer (à la hausse comme à la baisse), il est concevable que le besoin d'en connaître nécessite aussi une adaptation pour permettre à l'employé de remplir ses nouvelles missions. Après formalisation, justification et validation comme lors de la définition initiale, l'évolution peut s'effectuer de plusieurs façons suivant les principes de gestion retenus lors de la conception du système d'habilitations.

7.4.2 Les typologies d'accès

Les différents mécanismes de contrôle d'accès prévoient, avec plus ou moins de précision, les typologies d'accès auxquels les utilisateurs ont droit à l'égard des objets accédés. Ces catégories sont variables selon les plates-formes et les outils mais il est nécessaire de pouvoir communiquer avec ces outils au travers d'une normalisation qui peut être la suivante :

TYPOLOGIE DE L'ACCES	D	I	C
Lecture seule	non	non	oui
Ecriture seule	non	oui	non
Lecture et écriture	non	oui	oui
Modification technique	non	oui	non
Migration, déplacement	oui	non	non
Copie, transmission	non	non	oui
Impression	non	non	oui
Destruction	oui	non	non
Création	non	oui	non

On voit dans le tableau qui précède que, dans la logique de notre démarche, cette normalisation se combine bien entendu avec notre « fil rouge » qu'est la logique des critères DIC. Son utilisation judicieuse dans la superposition progressive des éléments de la démarche permet de mettre en cohérence les éléments tels que la capacité d'en connaître (valorisée DIC), le besoin d'en connaître (profilé DIC tel que ci-dessus), la valorisation des traitements (valorisés par le propriétaires).

Cette superposition constitue le moteur logique de la méthode.

7.5 Identification des propriétaires

7.5.1 Le « propriétaire d'application »

Si on en croit le questionnaire MARION (facteur 102, questions 4 et 5), "chaque application ou donnée doit être placée sous la responsabilité d'un "... dépositaire ou propriétaire nommément désigné, responsable des règles, procédures et autorisations d'utilisation des informations dont il a la

charge..." ; "...la liste des propriétaires et le descriptif de leur domaine doivent faire l'objet d'une publication diffusée aux personnes concernées...".

Les missions de ce type de propriétaires seront de :

- Identifier clairement ce dont il a été déclaré propriétaire,
- Préserver la cohérence de l'application par rapport à elle-même et aux règles de gestion de l'entreprise,
- Définir une grille de classification - par exemple de type DIC-, cohérente avec les étalons généraux définis pour l'organisation, de la gravité des atteintes à la sécurité des objets dont il a la garde,
- Affecter ensuite à chacun de ses objets ou ressources (ou groupes d'objets ou de ressources) un "label" formalisant leurs "besoins de sécurité", tenant compte de la grille de classification et de la valeur intrinsèque des objets (Cf. chapitre suivant),
- Définir, en liaison avec les différents responsables fonctionnels, les différents "besoins d'en connaître", c'est-à-dire les ressources nécessaires à l'exécution des différentes fonctions, et les types d'accès autorisés pour chacune de celles-ci (lecture, mise à jour, validation, création/destruction, copie, exécution d'un programme, ...),
- Revoir périodiquement la validité des différentes classifications (tant au niveau des "Besoins de Sécurité" des objets que des tables de "Besoins d'en Connaître",

Fréquemment, ce rôle de propriétaire est implicitement confié à la maîtrise d'ouvrage d'un domaine applicatif donné. Les missions resteront les mêmes que celles du propriétaire d'application tel que décrit ci-dessus. Dans d'autre cas, ce sera le responsable fonctionnel d'un domaine qui sera implicitement ou explicitement considéré comme le propriétaire de l'applicatif desservant le domaine. On aura fréquemment des exemples de ce type : le chef comptable responsable fonctionnel du domaine comptabilité et propriétaire des applications - donc des traitements - de comptabilité.

7.5.2 Le « propriétaire qualité »

Les responsables de la sécurité informatique considèrent souvent que les ressources informatiques (logiciels, données,...) relèvent de la notion de propriétaire. Dans cette approche, et en toute logique, le propriétaire est alors décrit comme une victime potentielle. En conséquence de quoi, des droits lui sont accordés, en rapport avec son statut de propriétaire, comme par exemple celui de se protéger contre les agressions dont son patrimoine pourrait faire l'objet. Cette approche est une approche patrimoniale, et comme dans un musée, des dispositions sont prises pour que les visiteurs n'aient aucun acte de nature à porter atteinte à l'intégrité du patrimoine. Toujours dans cette approche, les ressources informatiques sont principalement considérées comme partie de l'actif de l'entreprise. Elles constituent donc une part de la contrepartie du capital de la société et les actionnaires sont les propriétaires des ressources informatiques.

Cette approche ne doit pas être rejetée, mais elle ne doit plus être l'approche principale. Elle est celle de l'actionnaire (et encore?), pas de l'entrepreneur. En effet, vu du côté entrepreneur, ce qui est intéressant dans un patrimoine, ce n'est pas sa valeur qui relève du bilan de l'entreprise, mais l'usage que l'on peut en faire qui relève du compte de résultat puisqu'on se trouve dans une dynamique emploi-ressources.

Ce changement de point de vue est capital et peut paraître iconoclaste. En effet dans ce schéma, on ne parle plus de propriétaire avec des droits mais de fournisseur avec des devoirs.

Contre un droit d'usage, le fournisseur interne ou externe, met à la disposition de ses clients-utilisateurs, des ressources conformes aux besoins, explicites ou implicites de ceux-ci. L'explicite porte généralement mais pas exclusivement sur les caractéristiques fonctionnelles de la ressource et s'exprime au travers d'un contrat, d'un cahier des charges, etc. L'implicite porte sur l'obligatoire et notamment sur la sécurité qui, en conséquence, doit être garantie même lorsque ce besoin n'est pas formellement exprimé.

Le fournisseur a donc des devoirs vis à vis de ses clients-utilisateurs. Il a le devoir de mettre à leur disposition des ressources dont la disponibilité, l'intégrité, la confidentialité (notamment pour des informations nominatives) sont garanties. Dans ce dernier cas il s'agit d'une contrainte non pas vis à vis du client-utilisateur mais par rapport aux tiers concernés voire impliqués par les informations.

Pour satisfaire ces devoirs, le fournisseur se doit de mettre en place une organisation fiable et cohérente susceptible d'inspirer la confiance suffisante dans son aptitude à satisfaire ses engagements, tant vis à vis de ses client utilisateurs que vis à vis des tiers. Quand il s'agit des tiers, ce qui est exprimé, traduit semble-t-il assez bien l'esprit de la loi informatique et liberté : si l'organisation ne donne pas une confiance suffisante, la CNIL est susceptible d'exiger que des dispositions supplémentaires soient mises en œuvre.

Ce qui est dit ci-dessus n'est rien d'autre que l'obligation d'assurance qualité qui s'impose au fournisseur. Cette vision renverse complètement les rôles par rapport à l'approche propriétaire et on comprend alors que le fournisseur doit plus exiger de son organisation que de ses clients-utilisateurs.

Il peut également exiger que sont client soit sous assurance qualité, voire certifié par un organisme tiers indépendant, l'auditer, l'obliger à mettre en place une fonction sécurité indépendante de la fonction production, etc. L'exigence doit être adaptée au risque encouru par le fournisseur, basé sur la confiance dans le client-utilisateur, d'autant que ce risque est in-fine celui du client-utilisateur.

7.5.3 Identification du propriétaire

La liste des traitements constitue la base permettant de rechercher des propriétaires. L'annuaire ou les organigrammes - notamment le fonctionnel - constituent le réservoir où l'on ira rechercher les noms des propriétaires. La désignation du propriétaire ne doit pas être une démarche unilatérale. Une procédure doit décrire les conditions de sélection et l'intéressé doit avoir connaissance des traitements dont il a la charge. La signature d'un acte de prise en charge de patrimoine constitue une démarche souhaitable. Il serait inadmissible que l'on découvre lors d'un audit ou pire lors d'un incident que quelqu'un était désigné propriétaire sans en avoir été avisé ou que le périmètre des applications et traitements dont il est en charge soit modifié à son insu.

L'identification des propriétaires n'est pas toujours aisée et la facilité parfois inexacte consistant à nommer propriétaire d'une application le responsable fonctionnel du domaine sera à utiliser avec une prudence raisonnée. Une autre facilité consistant à transférer par forfait le rôle de propriétaire vers l'administrateur sécurité est à bannir formellement. On n'accepte pas les traitements « orphelins » ce qui implique de rechercher vaille que vaille des propriétaires à ces traitements.

7.6 Accord sur la définition des services

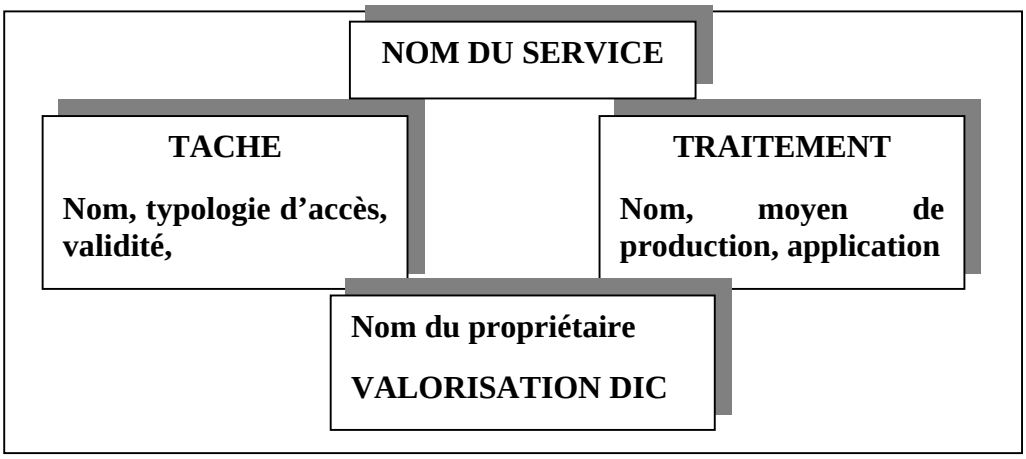
7.6.1 Notion de "services"

Les équipes d'informaticiens en charge de la gestion des outils techniques sont catégoriques, c'est l'expression fonctionnelle du traitement qui pose problème dans la gestion des droits d'accès. Si l'on parvient à correctement structurer la demande fonctionnelle et à la rendre exploitable par les techniciens en charge des droits d'accès, l'enchaînement avec les mécanismes techniques devient naturellement plus aisé.

Les outils fédérateurs d'administration des droits d'accès qui dominent actuellement le marché intègrent la notion de services. Définissons un « service » :

- Un service est le résultat d'une association logique entre une tâche fonctionnelle utilisateur et une transaction logiquement identifiée parmi les ressources informatiques. Dans et agrégat logique **la tâche est par définition insécable au plan fonctionnel et le traitement insécable au plan sécurité logique informatique.** Afin d'éclairer la compréhension de ce concept, on peut l'identifier à la définition de l'atome dans le Petit Larousse, à savoir : parcelle d'un corps simple, la plus petite partie d'un élément qui puisse entrer en combinaison »,
- Le service est le trait d'union entre le monde de l'administration que nous décrivons dans cet ouvrage et le monde de la gestion des droits dont l'alimentation devient mieux structurée, plus automatisée. Le service permet de relier, par un règle de sécurité objective, une tâche aux moyens techniques nécessaires à son accomplissement.
- Plus les éléments sont insécables fonctionnellement et logiquement et plus leur administration est facilitée à l'égard des révisions des droits d'accès nécessités par la vie de l'entreprise.

On peut schématiser un service comme suit :



7.6.2 Accord sur la définition des services

Le propriétaire est identifié, une négociation doit s'engager entre lui et les responsables fonctionnels qui ont formalisé sous forme de tâches les attentes des utilisateurs de leur domaine de compétence (ou d'autorité).

L'organisation - avec le support de l'informatique - a combiné les tâches avec les traitements : cette combinaison a donné naissance aux services. En validant l'existence d'un service, le propriétaire accepte de facto qu'un utilisateur (et son besoin d'en connaître) accède par un traitement aux ressources implicitement attachées au traitement. Cette acceptation n'est pas nominative : le propriétaire ne valide pas l'accès d'une personne physique mais celui d'un utilisateur ou d'un groupe d'utilisateurs fonctionnels : exemple, les guichetiers ou le groupe « guichetiers ».

8. VALORISATION DIC DES SERVICES OU OBJETS

L'établissement d'une grille d'étalonnage universelle dans une entreprise, qui suive les recommandations du chapitre premier, est une tâche essentielle. Cela permet de connaître quels sont les risques que l'on accepte de prendre en rendant accessible l'information à certaines personnes. Pour accroître l'opérabilité de la démarche, la grille d'étalonnage permet de classifier rigoureusement les besoins de sécurité des domaines applicatifs.

Il s'agit ici, pour chacun des services (tâches ou traitements) identifiés de déterminer quelle est le niveau de gravité d'une perte de sécurité. Par "perte de sécurité", on entend chacun des 3 axes de base chers aux ouvrages sur la sécurité informatique : **D**isponibilité, **I**ntégrité, **C**onfidentialité.

Il peut paraître inadéquat de mentionner le critère "Disponibilité" lorsque l'on traite des moyens de la sécurité logique. Le sujet est malgré tout pertinent car de nombreuses attaques logiques peuvent aboutir à une paralysie partielle ou totale des moyens physiques (attaque de virus nécessitant l'arrêt des installations pour remise en état, effacement de fichiers ou d'informations système entraînant l'arrêt des applications, pénétrations aboutissant à la saturation des réseaux).

Selon une démarche bien connue des utilisateurs de la méthode MARION, c'est à leur "Propriétaire" (Cf. chapitre précédent) des différents services que l'on demandera de quantifier l'impact d'une défaillance de sécurité au niveau de chacune d'elles :

- Disponibilité : quelles sont les pertes directes ou indirectes de l'organisme en cas d'immobilisation de la ressource concernée pendant le temps nécessaire à sa remise en état,
- Intégrité : quelles sont les pertes potentielles si le contenu ou le fonctionnement de l'objet ou de la ressource a été altéré (soit d'une façon évidente : perte de donnée par exemple, soit de façon pernicieuse : dysfonctionnement aléatoire et fugitive d'un algorithme...),
- Confidentialité : à quelles pertes peut-on s'attendre lorsque, tout fonctionnant bien par ailleurs, des informations sont connues ou des ressources sont utilisées par des personnes non habilitées (soumission de traitements stratégiques, divulgations, travaux "en perruque"...).

Dans le cas (fréquent) de ressources partagées, il faut descendre les niveaux d'analyse jusqu'au stade où sera identifiable un seul propriétaire par unité cohérente sur ces ressources. Alors le « besoin de sécurité » de la ressource pourra être considéré comme étant le « pgcd » des attentes de chacun des utilisateurs.

Les critères d'appréciation par les "propriétaires" reprendront les bases élaborées par le CODIR et couvriront :

- Valeur patrimoniale de la ressource ou de l'objet,
- Coût de sa remise en état,
- Implications financières, commerciales, juridiques etc. de son indisponibilité, de sa perte, de son dysfonctionnement, ou de son usage frauduleux.

On aboutira par exemple à des notations du type :

- Niveau critique des éléments devant aboutir à l'établissement d'une facture Client = **D4 I4 C0**, degré critique d'éléments variables de paie = **D1 I3 C3.**

9. GESTION DES HOMMES

9.1 Identification des capacités d'en connaître

Il appartient au responsable hiérarchique de décider du niveau d'habilitation d'une personne physique c'est à dire d'évaluer le degré de confiance.

Nous avons vu dans le chapitre 1 que le CODIR aidait sa hiérarchie intermédiaire en donnant un référentiel de criticité mais également une liste des critères déterminants ou discriminants permettant d'affecter un niveau d'habilitation à une personne physique.

Le Responsable Hiérarchique est seul juge dans cette démarche mais il n'exécute en cela qu'un acte de management courant puisque la notion de confiance se manifeste et a besoin d'être objectivée à l'intérieur de l'entreprise de la même manière mais dans des domaines différents que nous avons déjà évoqué au chapitre 1.

Selon la culture d'entreprise, le niveau d'habilitation peut-être attribué soit au collaborateur personne physique, soit au profil d'habilitation représentatif d'une métier lui même porteur d'une confiance à toute personne que l'on associera à ce profil d'habilitation.

Nous conseillons toutefois aux Responsables concernés de rejeter toute approche laxiste visant à distribuer des degrés de confiance égaux afin de ne pas poser de problème relationnel d'une part (de type Mme UNTEL à un niveau plus élevé que le mien et pourtant elle est moins ancienne) ou à faire en sorte que ces degrés de confiance soient d'un niveau élevé afin de ne pas avoir à gérer les conflits de demande de type « puisqu'on ne me donne pas ce qu'il faut, moi je ne « bosse » plus ».

A l'évidence cette approche managériale va probablement soulever un passé (un passif) ayant engendré des anomalies. La démarche proposée, à défaut de convaincre les responsables de le faire, leur donnera au moins la liste de ce qu'ils pourraient faire. **Sans équivoque, l'administration des droits d'accès se positionne avant tout dans un cadre de management dynamique et objectif.**

9.2 Affectations aux missions et aux tâches

Nous en sommes maintenant au stade où un Responsable Hiérarchique ou Fonctionnel est sur le point d'attribuer une fonction (dont on a déterminé le besoin d'en connaître) à un employé (dont on a déterminé le Degré de Confiance).

Un certain nombre de questions doivent être posées :

- Ai-je bien satisfait préalablement aux recommandations du référentiel établi par le CODIR en manière de criticité des accès dans le cadre du degré de confiance ?
- Ce collaborateur est-il apte à tenir ce poste et notamment l'accès demandé correspond-il bien au métier habituel du collaborateur (ce qui signifie concrètement qu'un collaborateur sorti de son métier habituel peut voir son degré de confiance baisser) ?
- Quel risque engendre l'affectation par rapport aux services accédés et valorisés DIC ?
- La valorisation DIC du patrimoine accédé est-elle compatible avec le niveau d'habilitation DIC accordé au collaborateur ou au profil d'habilitation ? Par exemple, un collaborateur dont le degré de confiance est classifié 1 est affecté à une tâche requérant un niveau D1 I3 C4. Il y

a à l'évidence déséquilibre et l'affectation avec son corollaire de droits ne peut être réalisée sans dérogation dûment réfléchie. Cela signifie qu'en cas de dépassement du niveau d'habilitation par la valeur du patrimoine on peut être amené à accorder une dérogation. Dans quel cas est-on habilité à l'accorder ?

- Les dates limites de validité du droit accordée sont-elles bien identifiées ?

Bien entendu, le supérieur qui réalisera cette affectation ne pourra le faire que dans la limite de son propre domaine de compétence. (voir administration en annexe 1)

10. DEMARRAGE : LE "DROIT D'ACCES"

10.1 indicateurs et anomalies

Les mécanismes proposés par la démarche méthodologique doivent permettre de déceler des anomalies qui procèdent du domaine purement sécuritaire et d'autres qui procèdent plus banalement du domaine de l'avancement du projet sécurité. Certaines révéleront des carences organisationnelles liées à l'histoire. Ce sont les directives de management qui permettront de les régler (ce qui est souhaitable) ou au contraire de les auditer. Sans que la liste qui suit soit exhaustive on peut citer les anomalies ou indicateurs que le système proposera :

- La liste des acteurs n'ayant accès à aucune ressource,
- La liste des acteurs « orphelins » sans supérieur hiérarchique ou fonctionnel,
- La liste des applications-traitements sans propriétaires,
- La liste des applications-traitements non valorisés,
- Les dates d'habilitations périmées,
- Les tâches non reliées à un service,
- Les traitements non reliées à un service,
- Les moyens de production sans application-transaction donc mal sécurisés,
- L'identification des ressources critiques (unicité de compétences...),
- Des possibilités de simulations (tentatives de pénétration, tracking,...),
- La grille d'étalonnage commune des niveaux de criticité (gravité et potentialité des incidents),
- La liste des droits d'en connaître par niveaux hiérarchiques et par grandes fonctions

10.2 Simulation des affectations

Les mécanismes de la méthode permettront de visualiser avant affectation les droits susceptibles d'être générés et de pouvoir en tirer des enseignements fonctionnels vis à vis des risques notamment. Cette possibilité offrira au responsable sécurité et à l'audit interne ou externe des possibilités extrêmement puissantes.

D'utiles comparaisons entre le niveau hiérarchique ou fonctionnel d'un utilisateur et la puissance (voire le caractère exorbitant) de ses droits permettront de révéler des faiblesses, du laxisme voire des connivences potentielles, préjudiciables à la sécurité.

Cette simulation permettra d'anticiper les négociations entre demandeurs et structure d'habilitations et minimisera la délicate situation dans laquelle se trouvent actuellement les dites structures d'habilitations entre les récriminations du type « j'ai pas c'qu'y'm'faut pour travailler, puisque c'est çà j'rent'chez moi » et les risques liés à une attribution forfaitaire des droits d'un « maillage » trop large.

10.3 Génération des accréditations et alimentation des contrôles

La liste des services ainsi enrichie sera proposée aux équipes techniques d'administration des droits. Elle leur permettra d'alimenter plus aisément les mécanismes techniques de contrôle des accès :

- Grâce à la précision et notamment le caractère insécable des traitements véhiculés par le service,
- Grâce à la précision de la typologie de l'accès, notamment par l'expression structurée du traitement qui permettra son association aisée avec les normes et nomenclatures techniques qui régissent l'administration des différentes plates-formes.

10.4 Le "Single Sign On"

10.4.1 Position du problème

Dans un réseau d'ordinateurs il est fréquent qu'un utilisateur ait à se connecter et à s'authentifier sur plusieurs de ces ordinateurs pour accéder à l'ensemble des applications dont il a besoin. Cela implique qu'il se connecte successivement à chacun de ces serveurs d'applications en validant son identité d'utilisateur légitime et en l'authentifiant conformément aux procédures en cours sur chaque serveur.

Si, dans ce contexte, l'utilisateur doit accéder à n ressources, on doit potentiellement gérer n identifiants individuellement reconnus et n mots de passe pour chaque utilisateur, avec leurs règles de syntaxe et de mise à jour. Certes certains de ces identifiants et authentifiants pourront être répétés, mais l'expérience montre que ce n'est pas le cas le plus fréquent et de plus l'utilisateur se voit toujours contraint de passer par de multiples procédures de log-on.

Cette situation induit couramment des failles dans la gestion des accès par rapport à l'objectif de sécurité d'accès visé : frustration des utilisateurs qui finissent fréquemment par inscrire de façon trop visible à proximité de leur poste de travail les identifiants et mots de passe.

En outre, elle crée également une complexification des tâches pour les administrateurs des autorisations d'accès qui ont à gérer les autorisations, et surtout les révocations, sur ces n systèmes.

10.4.2 Les solutions du type "SSO" ("Single Sign-On")

Historiquement, certaines solutions ont fait émerger le rôle de serveur d'identification-authentification spécifiquement dévolu à l'un des systèmes dans le réseau de l'organisme considéré.

Dès lors qu'un utilisateur s'est connecté valablement une première fois au système de validation des connexions, cet utilisateur l'est sur l'ensemble des systèmes dans cette "juridiction" avec les autorisations spécifiques à son profil.

De telles applications de "Sigle Sign-On" (SSO), sont apparues sur les systèmes hosts et sur systèmes ouverts et à réseau.

On les a vues s'étendre progressivement pour englober des environnements de plus en plus hétérogènes. C'est souvent à ce niveau que des extensions restent à consolider.

10.4.3 Les solutions de type "SSSO" (Secured Single Sign-On)

Le Sign-On unique a posé de façon plus aiguë le problème de la sécurisation des accès, dont il risquait d'élargir de façon critique les brèches dans un environnement interconnecté.

Ainsi, on a vu apparaître deux types de sécurisation :

- L'une sur un serveur d'accès remplissant les fonctions single sign-on ci-dessus, parfois complétées de mots de passe dynamiques.
- L'autre à base de serveurs de sécurité type KERBEROS générant des "pass-tickets" de connexion-authentification à l'intérieur de leurs domaines.

Aujourd'hui, c'est naturellement le marché des SSSO qui est le plus actif, et sur lequel il y a le plus de développements en cours pour généraliser les solutions. Les choix ne sont pas évidents a priori, et il est bon de les valider.

Il convient d'accompagner la mise en place du SSSO par des mesures d'une approche globale de la Sécurité et de la Productivité : Administration de la Sécurité, Définition et Mise à jour des profiles d'utilisateurs, Chiffrement des fichiers de SSSO, Traces d'audit, Interfaçage avec d'autres outils tels que les Firewalls, Pérennité des solutions ... et de s'assurer que ce faisant on n'introduit pas de nouvelles failles.

Pour être complet, le SSSO doit intégrer de réelles facilités d'administration et notamment d'habilitation-révocation unique.

11. ANNEXE - ADMINISTRATION DE LA DEMARCHE

Dans toute organisation fiable, l'allocation des ressources et l'administration des catégories d'habilitation doivent être confiées à une structure indépendante ayant reçu délégation de la direction générale pour gérer les collaborateurs de l'entreprise. Ceci doit se faire dans le cadre d'une procédure formalisée permettant de vérifier que le besoin et les droits sont justifiés et de contrôler a posteriori les décisions prises. En cas de doute sur le bien fondé de la demande, la structure doit se mettre en relation avec le "propriétaire" de la ressource concernée pour le consulter et obtenir son accord.

La méthode d'administration des droits d'accès que nous venons de décrire doit, pour fonctionner correctement, être régie par des droits et principes précis dont les options générales sont choisies par le CODIR.

C'est la structure hiérarchique qui attribue le niveau d'habilitation. **N** étant le niveau de l'interlocuteur hiérarchique, il ne peut le faire que pour les personnes de niveaux « **N-1** » à « **N-n** » dépendant de sa compétence. Selon les options prises par le CODIR il pourra décider jusqu'au niveau « **N-n** » ou bien ne pourra décider qu'au niveau N-1 et auquel cas en cascade successives jusqu'au niveau le plus bas.

C'est la structure fonctionnelle qui requiert les droits d'en connaître lors de l'accord sur la définition des services passée avec le propriétaire. Elle ne peut le faire que pour les missions et tâches dépendant de sa compétence fonctionnelle. La logique d'autorisation en cascade ou non selon les options du CODIR s'applique également.

C'est la structure organisation qui est habilitée à nommer les propriétaires. Seules les personnes répertoriées comme appartenant à cette instance peuvent être autorisées à désigner les propriétaires.

Seul le propriétaire peut valoriser les services, les traitements ou les tâches. Il ne peut le faire que pour les applications/traitements dont il a la charge patrimoniale.

Seule la structure informatique peut désigner les moyens de production et les applications-traitements fonctionnant dans le périmètre du système d'information concerné.

12. ANNEXE - GLOSSAIRE

Accréditation :	Autorisation et approbation délivrées par une autorité désignée à un système informatique ou réseau d'ordinateurs, à une organisation ou à un individu, et permettant à ceux-ci de traiter des informations ou des données sensibles (*ISO*).
Affectation :	Action émanant d'une autorité hiérarchique et plaçant un individu dans une fonction de l'organisation de travail pour exécuter les tâches afférentes.
Authentification :	Action de vérifier l'identité déclarée d'une entité (*ISO*).
Autorisation :	Attribution à une entité d'un droit d'accès, complet ou restreint, à une ressource (*ISO*).
Besoin d'en connaître :	Besoin légitime qu'a un destinataire potentiel d'une information sensible d'en connaître l'existence, d'y accéder ou de la détenir (*ISO*).
Capacité d'en connaître :	Elle reflète un degré de confiance attribuée à une personne par sa hiérarchie.
CODIR	Comité de Direction définissant la politique de sécurité
DIC	Critères de sécurité des systèmes d'informations (Disponibilité, Intégrité, Confidentialité)
Droit d'en connaître :	Résulte de la mise en relation du besoin d'en connaître et de la capacité d'en connaître. Il se traduit par un niveau d'habilitation.
Habilitation :	Droit accordé à un individu d'accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé (*ISO*).
Identification :	Moyen par lequel un utilisateur se fait reconnaître.
INCAS	Méthode du CLUSIF : « **IN**tégration dans la **C**onception des **A**pplications de la **S**écurité »
ITSEC	Critères internationaux d'évaluation de la sécurité des systèmes d'information
MAGALI	**M**éthode d'**A**dministration de la **G**estion des **A**ccès **L**ogiques aux **I**nformations conçue par le CLUSIF
MARION	**M**éthodologie d'**A**nalyse des **R**isques **I**nformatiques et d'**O**ptimisation par **N**iveau mise au point par le CLUSIF

MEHARI	**ME**thode **H**armonisée d'**A**nalyse de **R**isques **I**nformatiques mise au point par le CLUSIF
Niveau d'habilitation	Voir capacité d'en connaître
Organigramme fonctionnel :	Représentation graphique des différents éléments de l'organisation concernée et leurs rapports respectifs pour ce qui concerne la distribution du travail et des moyens de le réaliser.
Organigramme hiérarchique :	Représente les différents éléments de l'organisation concernée et leurs rapports respectifs pour ce qui concerne l'embauche, les évaluations et notations, les rémunérations, les affectations à des postes de travail,....
Organisme	Entreprise ou administration
Profil d'habilitation ou profil de droit	Niveau d'habilitation représentatif de la capacité à en connaître attribuée aux personnes associées à ce profil
Propriétaire :	Entité ayant reçu la mission d'assigner un niveau de criticité à une ressource informatique puis d'en déterminer les conditions d'accès dans le cadre d'une organisation préalablement maîtrisée.
SDSSI	Schéma directeur de sécurité des systèmes d'information
Service :	Résultat de l'association logique entre une tâche fonctionnelle d'un utilisateur et un traitement logiquement identifié parmi les ressources informatiques.
Tâche :	Séquence d'opérations élémentaires permettant d'effectuer un travail donné dans le cadre d'une affectation précise.
Traitements (ou process):	Mécanismes se traduisant obligatoirement par l'exécution d'un algorithme dans une machine et permettant à un utilisateur d'accéder à des ressources ou objets détenant ou représentant des informations.