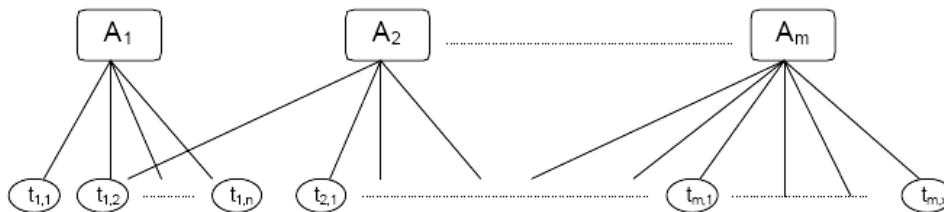


# Une nouvelle approche d'audit : L'utilisation des fonctions de croyance pour la certification WebTrust

## 1. L'équation d'audit entre le modèle probabiliste et la théorie de l'évidence

### 1.1. Equation d'audit : limite du modèle probabiliste

D'un point de vue pratique, l'évaluation du risque d'audit s'effectue par l'agrégation d'un certain nombre d'évaluations élémentaires, issues chacune de travaux menés par l'auditeur.



L'auditeur obtient ainsi l'évaluation des comptes A<sub>1</sub>, ..., A<sub>m</sub>, à partir des tâches t<sub>1,1</sub> ... , t<sub>m,x</sub>. L'objectif d'un modèle d'évaluation du risque d'audit est donc de pouvoir déterminer l'étendue des travaux nécessaires afin de répondre à la double contrainte d'atteindre un niveau de risque de contrôle suffisant (contrainte de qualité) et de ne pas dépasser ce niveau par des travaux supplémentaires superflus (contrainte de coût).

Les normes américaines (Statements on Auditing Standards, ou SAS) et les normes internationales de l'IFAC (International Auditing Standards, ou ISA) fournissent un modèle de base d'évaluation du risque d'audit, très largement adopté par l'ensemble des cabinets d'audit. Selon ces normes, le risque d'audit (i.e. le risque que l'auditeur se trompe en émettant son opinion) est fourni par une équation ensembliste (appelée « équation d'audit »), composée de l'enchaînement des risques suivants :

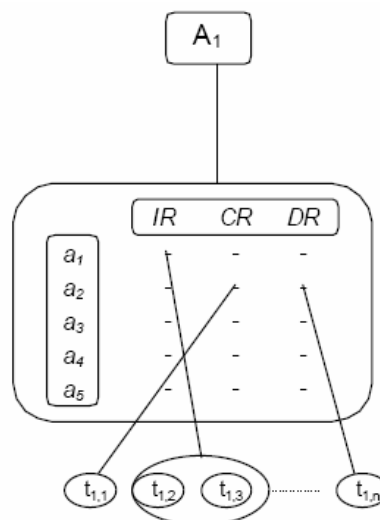
$$IR \times CR \times DR = AR, \text{ avec :}$$

- AR (Risque d'audit) : risque final qu'il demeure une erreur (significative) dans les comptes publiés. AR n'est pas quantifié explicitement par les SAS et les ISA ; l'auditeur restant seul juge du niveau de risque acceptable. Bien que ces normes n'imposent pas de risque quantifié, les exemples qu'elles proposent, ainsi que les méthodologies et les systèmes experts utilisés par les firmes d'audit, posent AR = 0,05
- IR (Risque inhérent) : évaluation portant sur l'environnement et mesurant le risque de l'entreprise à transcrire une information erronée sous forme d'écriture comptable,
- CR (Risque de contrôle) : évaluation de l'incapacité du contrôle interne à détecter et corriger l'erreur existant dans le flux d'informations comptables.
- DR (Risque de détection, ou de non détection) : évaluation de l'incapacité de l'auditeur à détecter et corriger les erreurs subsistant dans les comptes être publiés. DR peut être lui-même décomposé selon les différentes procédures d'audit utilisées :
  - Ra : inaptitude de la revue analytique à détecter l'erreur,
  - KI : risque d'erreur subsistant après la vérification complète d'un certain nombre d'éléments clé (Key items),
  - Stat : risque d'erreur subsistant après une vérification sur un certain nombre d'éléments, hors éléments clé, sélectionnés par échantillonnage statistique.

Pour chaque compte ou classe de transaction, cet enchaînement d'événements doit être appliqué au niveau de chacune des assertions (ou objectifs d'audit), dont les plus unanimement reconnus sont :

- Réalité (Existence ou Occurrence): ce qui est enregistré est correctement enregistré,
- Exhaustivité (Completeness) : tout ce qui doit être enregistré l'est effectivement,
- Droits et obligations (Rights et Obligations): tous les engagements figurent dans les états financiers,
- Valorisation (Valuation ou Allocation): les méthodes de valorisation sont correctement appliquées
- Présentation (Presentation et Disclosure): les normes de présentation des états financiers sont respectées.

Dans la pratique, ce modèle constitue le fondement des méthodologies et des systèmes experts développés par les cabinets d'audit. Il s'agit donc de formaliser un système d'aide à la décision basée sur une structure de réseau où chaque information (= élément de preuve) est repérée par rapport à la procédure qui la met en évidence et à l'assertion qu'elle tend à justifier. Le modèle des SAS et ISA peut finalement être représenté par un regroupement des travaux d'audit selon deux axes procédures/Assertions :



Le problème consiste donc dans l'évaluation, puis l'agrégation des informations recueillies au niveau de la matrice afin de calculer le niveau de risque d'erreur final effectif, et de le comparer au niveau de risque considéré comme acceptable par l'auditeur.

Cette approche considère toutes les composantes de l'équation ensembliste comme autant de probabilités. Le caractère subjectif de certaines évaluations, souligné maintes fois par les SAS et les ISA, impose de les traiter par des probabilités subjectives, donc conditionnée par le degré de connaissance  $K$  propre à chaque auditeur. Les évaluations étant des probabilités, l'équation d'audit devient une équation probabiliste, utilisant le multiplicateur comme opérateur d'agrégation. Et c'est justement de là où viennent les critiques.

En effet, de nombreuses critiques (Cushing et Loebbecke<sup>1</sup>, Waller<sup>2</sup>) se sont élevées contre le traitement probabiliste de l'équation d'audit, portant notamment sur :

<sup>1</sup> CUSHING (B.E.), LOEBBECKE (J.K.) : « Analytical approaches to audit risk : a survey and analysis »; *Auditing : Journal of Practice & Theory*, n°3 (Fall); 1983, pp.23-41.

- les conditions d'indépendance des variables. A titre d'exemple, la prise en compte des effets prévention et détection qui sont définis tous les deux comme les constituants du risque de contrôle par les normes d'audit, alors que l'effet préventif est également pris en compte dans le risque inhérent.
- la difficulté d'évaluer une probabilité conditionnelle très dépendante de l'appréciation subjective de chaque auditeur.
- la propriété de commutativité de l'opérateur multiplication dans l'équation d'audit n'est pas établie. En effet, son utilisation entraîne une stricte équivalence d'impact sur le risque d'audit AR entre deux éléments évalués au même niveau (Il est ainsi équivalent pour AR que IR=0,05, les autres composantes = 1, ou bien que le KI (risque détection sur les éléments clé) =0,05, les autres composantes = 1 : dans les deux cas on aura AR = 0,5). Or est-on certain que les différentes composantes du risque affectent de la même manière le risque global ? Peut-on par exemple mettre sur le même plan IR, évaluant le cadre dans lequel intervient l'auditeur, et donc qu'il subit, et DR ou KI, évaluant ses travaux inscrits dans ce cadre ?
- l'impossibilité de distinguer dans le modèle SAS et ISA entre l'absence totale d'assurance que le système fonctionne (par exemple système non testé), et le fait qu'il ne fonctionne pas : dans les deux cas, SAS et ISA imposent de retenir une probabilité de risque d'erreurs de 100%. Or ces deux événements sont de natures très différentes.

## **1.2. Equation d'audit : apports de la théorie de l'évidence**

Srivastava et Shafer ont donc développé un modèle d'évaluation du risque d'audit basé sur la théorie de l'évidence et l'utilisation des fonctions de croyance permettant cette distinction. Selon leurs travaux, la représentation de l'incertitude d'une preuve d'audit avec une fonction de croyance s'effectue de manière subjective, faute d'informations objectivement mesurables. L'idée de base de la théorie de l'évidence est que l'on évalue, non pas directement un élément A, mais toutes les parties de l'ensemble  $\theta = \{A; \bar{A}\}$ , où A = l'événement « absence d'erreur » et  $\bar{A}$  = l'événement « présence d'erreur ».

Si par exemple, l'auditeur effectue une revue analytique et qu'il affecte  $m = 0,6$  à l'événement A et qu'en outre, rien ne l'indique à penser que ce compte contient des erreurs (car aucune preuve positive de l'existence d'une erreur), alors  $m(A) = 0,6$  et  $m(\bar{A}) = 0$ , donc  $m(A, \bar{A}) = 0,4$  afin que  $m(\theta) = 1,0$ . De même, si  $m(A) = 0,6$  et  $m(\bar{A}) = 0,1$  donc  $m(A, \bar{A}) = 0,3$  afin que :  $m(\theta) = 1,0$ . On remarque que  $m(A, \bar{A})$  constitue la mesure de l'ignorance, provenant du manque de preuve quant à l'absence totale d'erreurs. Autrement dit, l'auditeur dispose d'une preuve directe que A est vrai à hauteur de 0,6 et aucune preuve directe qu'il y ait une erreur. Il est donc pleinement plausible qu'il n'y ait aucune erreur, sachant que le risque maximum de se tromper est de 0,4 (ou de 0,3 dans le second cas).

Présenté sous forme vectorielle le modèle de l'évaluation du risque basé sur la théorie de l'évidence est de la forme suivante:

---

<sup>2</sup> WALLER W.S.: Auditor's risk assessments: Effects of task experience, conditioning information, and precision on second order uncertainty, Working Paper , University of Arizona, 1995.

$$\left| \begin{array}{c} \underline{IR} \\ m_1 \\ m_2 \\ m_3 \end{array} \right| \oplus \left| \begin{array}{c} \underline{CR} \\ m_1 \\ m_2 \\ m_3 \end{array} \right| \oplus \left| \begin{array}{c} \underline{RA} \\ m_1 \\ m_2 \\ m_3 \end{array} \right| \oplus \left| \begin{array}{c} \underline{KI} \\ m_1 \\ m_2 \\ m_3 \end{array} \right| = \left| \begin{array}{c} \underline{AR} \\ 0,95 \\ m_2 \\ m_3 \end{array} \right|$$

Avec :

$m_1$  = croyance qu'il n'y a pas erreur,

$m_2$  : croyance qu'il y a des erreurs,

$m_3$  = ignorance,

$\Phi$ : règle de combinaison de Dempster<sup>3</sup>.

Ainsi, en remplaçant la probabilité par une fonction de croyance, ce modèle permet de distinguer les évaluations des situations de preuves d'audit bien différentes quant à leur impact sur la fiabilité réelle des états financiers. Cette amélioration s'effectue par l'acceptation de la subjectivité de l'évaluation.

Contrairement au traitement probabiliste, ce modèle ne fait pas l'objet d'application au sein des cabinets d'audit. Cependant, depuis sa publication, ce modèle fait l'objet de nombreuses expérimentations, dont celles de Srivastava dans le cas des missions d'assurance WebTrust.

## 2. L'utilisation de l'approche évidentielle dans une mission WebTrust

Dans un article publié par Srivastava et Mock<sup>4</sup>, ces auteurs ont développé un cadre conceptuel de raisonnement en matière de recherche d'évidence dans une mission WebTrust. Ils proposent une approche structurée pour collecter, évaluer et agréger des éléments probants (éléments de preuve ou évidences) appropriés pour les assertions, objectifs et sous objectifs liés à une mission d'assurance WebTrust. Ceci en réponse à la difficulté du modèle d'audit par les risques traditionnel d'incorporer des évidences interliées ou de considérer les relations entre les différentes variables.

L'apport de cette méthode qui remplace l'approche par les risques par celle de la théorie de l'évidence, réside dans l'utilisation des fonctions de croyance. D'après les travaux de Srivastava et Shafer qu'on vient d'exposer brièvement, les fonctions de croyance fournissent un meilleur cadre d'expression de la force des preuves que celui donné par l'approche probabiliste. De plus, d'après Curley et Golden<sup>5</sup>, les fonctions de croyance offrent une promesse, comme un langage, pour représenter des degrés de croyance et, particulièrement, pour capturer des degrés de justification et de support.

Mais comment consacrer ces vertus annoncées des fonctions de croyance au service d'une mission WebTrust ?

<sup>3</sup> La règle de combinaison de Dempster a pour objet l'agrégation d'évaluations (énoncées sous forme de masses d'évidence), provenant de sources diverses, et portant sur un même événement.

<sup>4</sup> Srivastava, R.P et Mock T.J : « Evidential reasoning for WebTrust Assurance Services »; *débats lors de 32ème conférence sur les sciences des systèmes, Hawaii 1999*

<sup>5</sup> Curley, S. P. et J. I. Golden. 1994. "Using belief functions to represent degrees of belief". *Organization Behavior and Human Decision Processes*. 271 – 303.

## 2.1 Structure et validation des assertions

En matière d'audit financier, on retrouve plusieurs variables et types de preuves qui amènent essentiellement à une conclusion booléenne ou binaire : vrai ou faux, ou alors opinion sans réserve ou opinion avec réserves. Cependant, en matière de missions d'assurance WebTrust, les facteurs sont plus nombreux et aboutissent à n conclusions possibles au lieu de deux (opinion sur les pratiques commerciale, opinion sur la protection des données, opinion sur la sécurité...). Les assertions sont, en effet, au niveau des différents principes WebTrust individuels.

Ainsi, afin de prendre compte de la spécificité des missions WebTrust, chacun des principes sera considéré comme l'assertion principale à prouver. Les critères sous-jacents seront les objectifs, eux-mêmes divisés en sous objectifs, dans les cas où ces critères doivent collecter des preuves suffisantes et appropriées (en quantité et en qualité) afin de prouver que chaque objectif est atteint. Quand chaque objectif a été validé, l'assertion elle-même se retrouve approuvée. Les assertions, les objectif et les sous objectifs sont liés d'une manière à ce que chaque assertion n'est vérifiée que si et seulement si les objectifs afférents et les sous objectifs qui les soutiennent ont été atteints. Les assertions, les objectif et les sous objectifs sont liés d'une manière à ce que chaque assertion n'est vérifiée que si et seulement si les objectifs afférents et les sous objectifs qui les soutiennent ont été atteints.

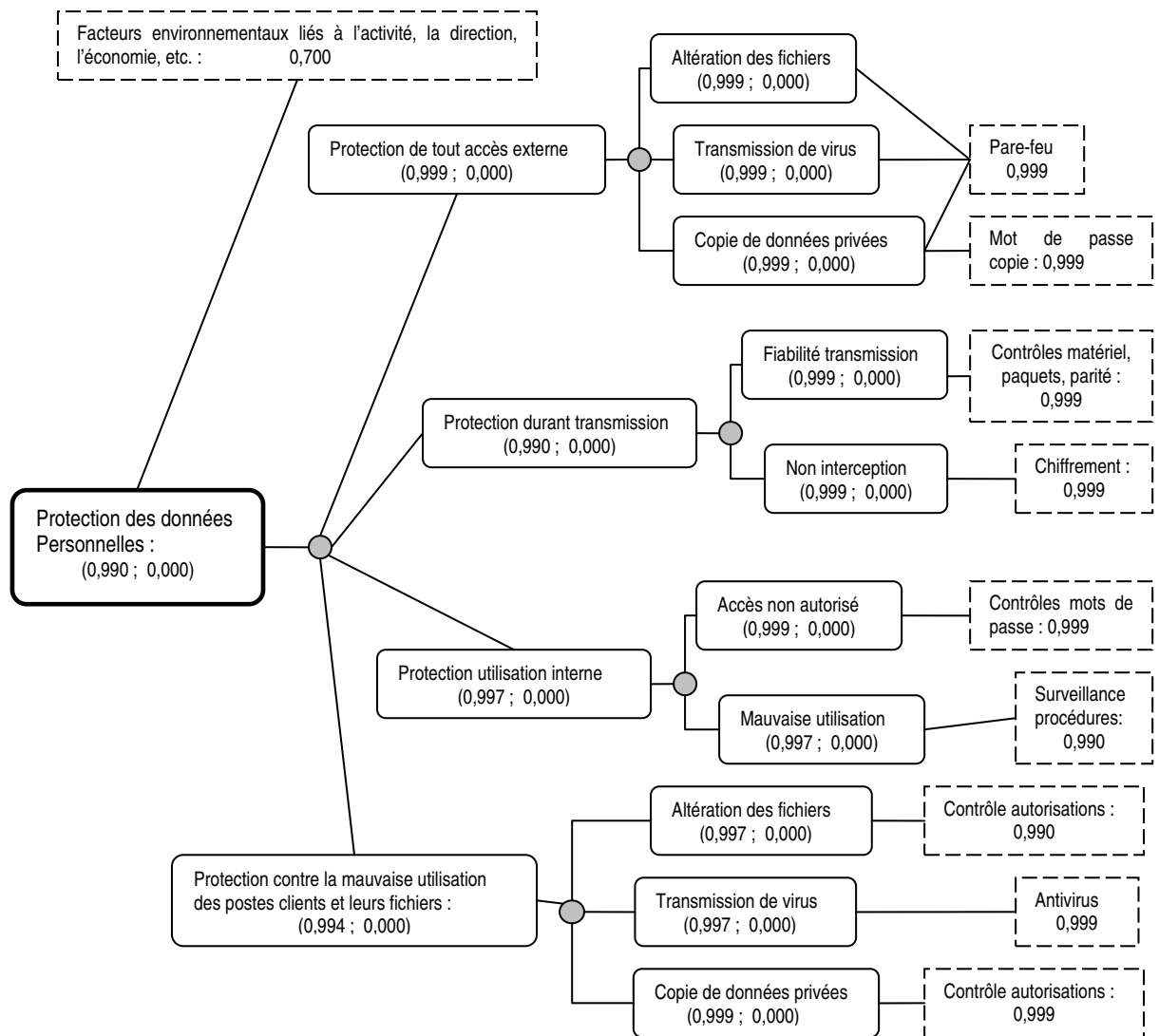
**«...Les assertions, les objectif et les sous objectifs sont liés d'une manière à ce que chaque assertion n'est vérifiée que si et seulement si les objectifs afférents et les sous objectifs qui les soutiennent ont été atteints... »**

A titre d'exemple, pour le principe de la protection des données personnelles, Srivastava et Mock déterminent la structure suivante (qu'ils appellent le réseau des preuves) d'après leur lecture de ce principe et des critères WebTrust et autres contrôles qui le soutiennent :

Assertion	Objectifs	Sous objectifs
Protection des renseignements personnels	Protection contre l'accès externe	Protection contre l'altération des fichiers
		Protection contre la transmission de virus
		Protection contre la copie de données personnelles
	Protection lors de la transmission	Fiabilité de la transmission
		Non interception de la transmission
	Protection contre l'utilisation interne frauduleuse	Protection contre l'accès non autorisé aux données privées
		Protection contre l'utilisation inappropriée
	Protection contre l'utilisation inappropriée des postes clients et leurs fichiers	Protection contre l'altération des fichiers
		Protection contre la transmission de virus
		Protection contre la copie de données personnelles

## 2.2 L'utilisation de l'approche évidentielle : exemple pour l'assertion de protection des données personnelles

Reprenons le cas de l'assertion de protection des données personnelles dont Srivastava et Mock ont dessiné le réseau de preuves. Le diagramme suivant résume l'utilisation de l'approche évidentielle pour cette assertion :



Dans ce diagramme évidentiel, les rectangles arrondis sont les nœuds de variables et représentent les assertions (1<sup>er</sup> niveau), les objectifs (2<sup>ème</sup> niveau) et les sous objectifs (3<sup>ème</sup> niveau). Chacun de ces rectangles est doté d'un couple de valeurs de type (vrai ; faux) que l'assertion ou l'objectif ont été validés ou pas. Pour l'exemple de l'objectif «protection de tout accès externe », d'après l'agrégation des travaux et procédures de vérification, l'objectif est atteint à 0,999 et rien n'indique qu'il ne l'est pas (car la mesure la négation est de = 0,000). Quant aux rectangles en pointillés, ils représentent les nœuds de preuves, c'est-à-dire l'ensemble des procédures et contrôles effectués par le vérificateur. Enfin, les cercles pleins reliant les différents nœuds de variables représentent une relation logique de type « ET » entre les nœuds de variables à sa droite (sous objectifs ou objectifs) et la variable plus centrale à sa gauche (objectif ou assertion). Ainsi, cette relation implique, par exemple, que l'assertion « protection des données personnelles » n'est validée que si et seulement si l'ensemble des quatre objectifs à sa droite ont été atteints.

Par conséquent, pour déterminer si l'assertion est validée, le vérificateur doit effectuer l'ensemble des procédures indiquées dans les rectangles en pointillés (nœuds de preuve). Chaque procédure effectuée agit en tant qu'élément de preuve, fournissant un support (ou éventuellement un non-support, ou alors un support mitigé) à l'assertion ou objectif auquel elle

affectée. Ainsi, dans notre exemple, les données sont jugés protégés si et seulement si les objectifs suivants ont été atteints : protection contre tout accès externe, protection durant la transmission, protection contre une mauvaise utilisation interne et protection contre la mauvaise utilisation des postes clients et leurs fichiers. Ces objectifs sont eux-mêmes subdivisés en sous objectifs, de telle manière que pour la protection durant la transmission par exemple, cet objectif n'est atteint que si et seulement si les sous objectifs « transmission fiable » et « non interception » ont été validés.

Sur la base des constatations après chaque procédure, le vérificateur peut estimer le niveau de soutien de chaque élément de preuve à l'assertion ou objectif correspondant. Ce niveau de soutien est exprimé grâce aux fonctions de croyance. D'ailleurs, dans leur article sur l'approche évidentielle dans une mission WebTrust, Srivastava et Mock ont utilisé ces fonctions de croyance et un programme informatique appelé « Auditor Assitant »<sup>6</sup> pour agréger ces éléments de preuve. Pour revenir à l'exemple illustré ci-dessus, la croyance globale soutenant l'assertion de protection des données personnelles est de 0,99 (contre 0 que l'assertion n'est pas vérifiée). Un pareil niveau élevé peut être réconfortant pour un vérificateur, surtout que le principe de protection des données personnelles peut s'avérer très préjudiciable pour un expert comptable qui rate sa mission.

Considérons un autre scénario pour l'assertion de protection des données personnelles, afin de mieux voir cette approche sous toutes ses facettes. Supposons que le vérificateur trouve que le site Web ne possède pas de contrôles fiables pour le sous objectif « protection contre tout accès non autorisé aux données personnelles ». Il exprime un niveau de soutien de 0,9 pour la négation de l'objectif. Même si les autres éléments de preuve donnent les mêmes niveaux de support positif aux variables afférentes, la croyance globale que l'assertion « protection des données personnelles » est vraie est uniquement de 0,189, avec une croyance de 0,730 que c'est faux, d'après les calculs de la fonction de croyance et du programme « Auditor Assitant ». C'est que la connexion des objectifs entre eux par un opérateur logique de type « ET » fait que l'assertion ne peut être validée que si et seulement si ses quatre objectifs sont atteints. Avec un pareil bas niveau de croyance que l'assertion est validée (0,189) et un tel niveau élevé qu'elle ne l'est pas (0,730), l'expert comptable doit envisager d'exprimer une opinion avec réserves, voire même annuler sa mission, selon son arbitrage entre le coût et l'avantage de sa décision.

### **3. Limites et conclusions sur l'approche évidentielle**

Même si ce modèle proposé utilise un large éventail de détails, il reste moins complet que ce que pourrait donner son application intégrale pour les missions WebTrust. A titre d'exemple, les nœuds de preuve (procédures de vérification) représentés pour le principe de la protection des données personnelles ne constituent qu'une partie de l'ensemble des éléments de preuve préconisés par WebTrust ou dictés par les réalités des missions. De même, les nœuds de variables (assertions, objectifs et sous objectifs) ne constituent pas la totalité des préconisations dictées par les critères et exemples de contrôle publiés dans le principe WebTrust 3.0 de protection des données personnelles. Le critère de déclaration des pratiques et les sous objectifs qui lui sont rattachés ne sont, par exemple, pas inclus.

Ce modèle gagne donc à être enrichi, en pratique, à travers une meilleure délimitation de tous les éléments de preuve, de toutes les variables (assertion, objectifs et sous objectifs) et de toutes les

---

<sup>6</sup> Shafer, G., P.P. Shenoy and R. P. Srivastava .1988. AUDITOR'S ASSISTANT: A Knowledge Engineering Tool For Audit Decisions. *Travaux du symposium sur les problèmes d'audit de l'Université de Touche Ross Kansas* (May): 61-79.

relations qui puissent exister entre elles selon le principe de protection des données personnelles.

De plus, comme en matière d'approche d'audit classique, ce modèle utilise certaines évaluations subjectives dépendant de la nature du vérificateur, de son aversion au risque et de ses connaissances professionnelles. Il en est ainsi, par exemple, pour l'évaluation du risque inhérent découlant des facteurs environnementaux, de la qualité de la direction ou de la nature de l'activité. Car, il n'est pas évident que deux vérificateurs différents apprécient le même sujet de la même façon. De même pour l'utilisation de sondages statistiques comme éléments de preuve afin de vérifier un sous objectif. Là aussi, un risque d'erreur, même si marginal, subsiste.

Loin de la perfection, certes ; mais l'utilisation des fonctions de croyance et de l'approche évidentielle aura le mérite de proposer une approche plus structurée et de mieux intégrer les relations entre les variables et celles entre les éléments de preuve. Les fonctions de croyance donnent plus de vigueur et de probité aux éléments de preuve que l'approche probabiliste classique, car elles mesurent un évènement, son contraire et l'ignorance de l'un et de l'autre. Leur application pour les missions d'assurance basées sur des critères structurés, de type WebTrust, paraît plus adaptée.

Encore une fois, ce sont des académiciens de la trempe de Srivastava, Shafer, Mock et les autres qui jouent leurs rôles de catalyseurs et d'innovateurs dans les diverses sciences et disciplines. Malheureusement, l'utilisation des fonctions de croyance pour les missions d'audit et d'assurance est restée sur les publications universitaires et les papiers de recherche. Son introduction dans la pratique par les cabinets et firmes d'audit tarde à se concrétiser. En effet, la tendance est plutôt conservatrice, dans une conjoncture où les risques professionnels pour les auditeurs sont de plus en plus élevés, et où les tentatives expérimentales paraissent périlleuses et aventureuses...

Nabil Ghodhbane  
Expert comptable

#### Bibliographie :

- LESAGE Cedric: Evaluation du risque d'audit: proposition d'un modèle linguistique. Cahiers de Recherche CEREG n° 9713, 2000.
- SRIVASTAVA Rajendra P., MOCK Theodore J.: Evidential Reasoning for WebTrust Assurance Services. Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999.