COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

SERVICES FINANCIERS PAR INTERNET

Résultats du recensement Internet
au 31 décembre 2000 et recommandations
portant sur les aspects prudentiels

Décembre 2001

La présente étude a été faite par M. David Hagen, responsable de l'audit informatique, et par M. Claude Bernard. Elle a été discutée avant finalisation par le Comité informatique, un comité consultatif qui fonctionne auprès de la CSSF sous la présidence de M. Arthur Philippe, directeur. Ont également participé à la discussion l'Institut des Réviseurs d'Entreprises et l'Institut des Auditeurs - Conseil Internes.

Préface

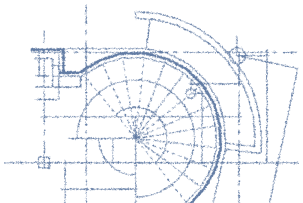
Au courant de l'année 2000, les services e-banking et e-brokerage passant par le réseau Internet ont connu un développement important sur la place de Luxembourg.

Afin d'analyser plus en profondeur la situation dans ce domaine, la CSSF avait procédé à un recensement de l'activité Internet au 31 décembre 2000 auprès de l'ensemble des entités dont elle assume la surveillance. Les principaux résultats de ce recensement furent publiés dans le rapport annuel 2000 de la CSSF. Le présent document complète cette publication initiale en reprenant l'ensemble des aspects recensés, à l'exception de certains dont l'analyse a montré qu'ils n'avaient pas été compris de façon uniforme et dont les réponses ne sont pas exploitables.

Avec le fort recul des marchés boursiers, et en particulier des valeurs technologiques du nouveau marché, l'activité e-banking et e-brokerage a subi plus récemment un ralentissement important et un repositionnement des établissements financiers s'est souvent avéré nécessaire. Certaines banques virtuelles n'entretenant pas de guichets ouverts au public et dont la stratégie commerciale repose entièrement sur la banque électronique, ont même arrêté leurs activités. Cette évolution a pu être observée sur un plan mondial et n'est pas encore venue à son terme à l'heure actuelle.

Faut-il en conclure que les services e-banking et e-brokerage n'ont plus d'avenir ?

La réponse est sans aucun doute négative car les établissements financiers qui proposent à leur clientèle des services e-banking et e-brokerage voient ce volet d'activités s'accroître, même si le taux de progression est plus faible que celui attendu à l'époque des marchés boursiers florissants.



En effet, dans le passé récent, ces services étaient prometteurs de profits importants et les établissements financiers avaient perçu la possibilité d'atteindre facilement une clientèle internationale désireuse de choisir le meilleur service ou le meilleur prix, sans distinction géographique du lieu d'établissement. De plus, le «phénomène» Internet bénéficiait au même moment auprès du public européen d'une publicité sans précédent de la part des médias qui pronostiquaient une société révolutionnée par la «net-économie». Certains établissements financiers ont été jusqu'à détacher les prestations par Internet des prestations traditionnelles, en créant des entités séparées et autonomes (business unit), considérées comme centres de profits.

Il est vrai que les prestations par Internet répondent à des caractéristiques spécifiques, notamment au niveau du marketing et de la segmentation des clients, qui peuvent justifier une gestion particulière en tant que «business unit», mais la réalité nous a enseigné que le comportement des consommateurs reste largement traditionnel et que l'effet de proximité de la prestation continue à jouer un rôle prédominant. La majorité des établissements financiers sont donc logiquement revenus à des concepts plus proches du comportement de leurs clients, à savoir la présence physique dans le pays de la prestation ou encore le concept «brick and click», où les services Internet sont intégrés dans l'activité globale des établissements sous la forme d'un canal de distribution spécifique au sein d'un environnement multi-canaux dont les guichets, les call-centers, les représentants et les partenaires locaux.

Les services financiers par Internet ne sont pas pour autant révolus. Bien au contraire, on remarque qu'ils s'inscrivent dans une stratégie tenant compte des réalités économiques et sociologiques actuelles et qu'ils continuent à contribuer de façon

significative au développement de l'activité des établissements financiers dans le cadre d'un schéma de croissance plus réaliste.

On se voit ainsi confirmé dans l'analyse que ce n'est pas Internet qui est générateur de potentialités et de profits grâce à de nouveaux comportements des consommateurs, mais que le produit financier et la qualité de la prestation restent à la base des revenus et de la capacité commerciale et bénéficiaire d'une entreprise financière.

Le marché s'étant profondément modifié, les résultats du présent recensement n'ont néanmoins pas perdu de leur intérêt. De nombreux sujets abordés gardent en effet leur importance, que les services e-banking et e-brokerage soient prestés via des entités spécialisées comme de par le passé récent ou que ces services représentent pour les établissements financiers un volet d'activités parmi d'autres comme c'est le plus souvent le cas actuellement.

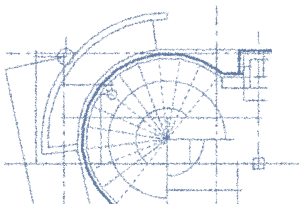
Dans le cadre de sa mission de surveillance prudentielle, la CSSF a associé la présente étude à la diffusion d'un certain nombre de recommandations qui portent sur des aspects de risques liés à des activités financières par Internet.

Dans la suite du document, des principes et recommandations figurent dans des encadrés jaunes et, en attendant d'éventuelles règles sur la matière, la CSSF recommande aux établissements financiers de les intégrer dans le développement de l'exploitation de leur fonctionnalité Internet. Ces recommandations sont aussi à voir comme une base de discussion dans le but d'élaborer une future réglementation. La CSSF encourage les établissements et autres personnes du secteur financier à lui communiquer leurs avis éventuels.

Les encadrés gris rappellent des aspects concernant le cadre réglementaire en vigueur ainsi que certains aspects des risques identifiés.

Le renforcement de la sécurité du canal de distribution Internet reste une tâche essentielle pour l'avenir même si la présente étude a pu dégager une prise de conscience élevée des risques auprès de la majorité des acteurs. La mise en place d'une solution intelligente de signature électronique contribuera de façon significative au renforcement de la sécurité et de la confiance dans l'Internet, non seulement auprès des établissements financiers mais également auprès de leurs clients.

Il incombe aux établissements financiers de participer au développement de la sécurité, mais aussi à la sensibilisation et à la formation des clients et du public, afin d'améliorer la confiance sans pour autant taire les risques. Il est dans l'intérêt général de la place financière d'accroître la sécurité à tous les niveaux de la chaîne opérationnelle, plutôt que de sous-estimer les risques de défaillances et de fraudes qui porteraient *in fine* préjudice à l'ensemble du secteur. Les conséquences économiques seraient importantes si le public venait à perdre toute confiance dans ce canal de distribution et une réponse insuffisante pour les établissements serait de se limiter à se dégager, à l'aide de clauses contractuelles, de leur responsabilité pour la rejeter sur l'utilisateur.



Contexte du recensement

La CSSF a procédé, à la date du 31 décembre 2000, à un recensement des services financiers disponibles par Internet auprès des établissements financiers établis au Luxembourg. Le questionnaire a été transmis à tous les établissements financiers pour lesquels la CSSF est l'autorité de surveillance, à savoir les établissements de crédit[1] (banques) et les autres professionnels du secteur financier (PSF), y compris les succursales d'établissements étrangers au Luxembourg et les succursales d'établissements luxembourgeois à l'étranger. Le recensement ne porte donc pas sur un échantillon des établissements, mais bien sur la population totale des établissements en activité à la fin de l'année 2000.

Le questionnaire distinguait les sites opérationnels au 31 décembre 2000 des projets devant aboutir au courant de l'année 2001. Il reprenait 48 questions regroupées en trois chapitres:

A. Site Internet / Stratégie Internet

B. Sécurité / Maintenance

C. Authentification du client / Données confidentielles

Les questions sont annexées au présent rapport.

Les questionnaires ont été dépouillés et une analyse approfondie est présentée ci-après. Certaines de ces questions n'avaient pas été comprises de façon uniforme par tous les répondants et ont été exclues de l'analyse, soit font l'objet d'un commentaire particulier.

Note spécifique pour les OPC:

Bien que non inclus dans le recensement, les recommandations reprises dans ce document sont en principe également applicables dans le domaine des organismes de placement collectif (OPC).

Les entités visées sont:

- les sociétés de gestion qui ont une infrastructure propre,
- les OPC qui ont une infrastructure propre,
- les administrations centrales des OPC.

Nous référons aux «Remarques spécifiques aux OPC», p. 58.

[1] La dénomination d'établissements de crédit au sens de la loi du 5 avril 1993, texte coordonné, est reprise sous l'appellation «banques».

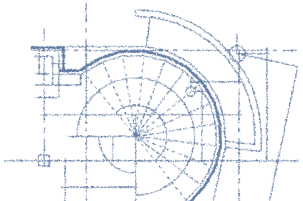


Table des Matières

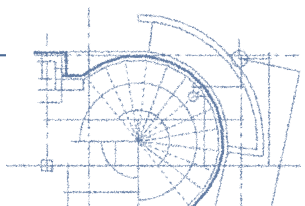
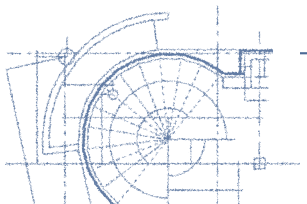


Table des Figures



A. Site Internet / Stratégie Internet

Au 31 décembre 2000, la CSSF a effectué son recensement auprès de 202 banques et 113[2] PSF.

Le questionnaire faisait la distinction entre trois catégories de sites:

- Les **sites informatifs**, qui présentent en général la société et ses produits, ainsi que d'autres informations générales à caractère public. Ces sites ne prévoient en principe pas d'identification de l'utilisateur. Une identification peut être néanmoins envisagée pour personnaliser le site et offrir, par exemple, la gestion de portefeuilles virtuels ou la simulation d'un crédit. Le fait qu'un utilisateur s'identifie sur un site informatif ne signifie pas qu'il soit client de l'établissement financier. L'établissement financier peut utiliser cette identification pour déterminer le comportement du public ou utiliser les résultats à des fins marketing, considérant ces utilisateurs comme prospects.

- Les **sites consultatifs**, qui nécessitent une identification et une authentification de l'utilisateur, lui permettant d'accéder à des informations personnelles comme, par exemple, la consultation de ses comptes ou de ses portefeuilles. Ces services ne sont donc offerts qu'aux clients de l'établissement. En effet, avant de pouvoir accéder à la consultation de ses données, l'utilisateur doit avoir reçu les informations qui lui permettent de s'identifier et de s'authentifier[3]. Les conditions régissant l'usage de ces informations d'identification sont définies dans un contrat entre l'établissement et le client.

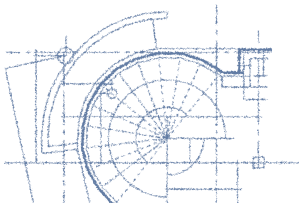
  La plupart du temps, pour des raisons d'efficacité et de rapidité, la mise à jour de ces informations personnelles n'est pas réalisée à travers un média physique (tape, CD-ROM), mais elle est réalisée au travers d'un lien avec le système central de l'établissement. Le site ne permettant que la consultation, ce lien de mise à jour est unidirectionnel du système central vers le site Internet.

- Les **sites transactionnels** permettent à l'utilisateur, sur base de son authentification, de réaliser des opérations bancaires, classiquement des virements ou opérations sur valeurs mobilières. Comme pour les sites consultatifs, les conditions de l'usage de ces informations d'identification sont régies par un contrat entre l'établissement et ses clients.

  Ces sites sont reliés au système central de l'établissement. Le lien est bidirectionnel dans le but de présenter les informations actualisées après chaque saisie d'ordre d'un client.

[2] Ces chiffres ne comprennent pas les succursales de PSF d'origine communautaire établies au Luxembourg et hors des dispositions générales.

[3] L'authentification diffère de l'identification en ce sens qu'elle est plus poussée. Elle garantit l'authenticité de l'identification. Voir aussi les chapitres C.1 à C.3 pp 50-51.



A. Site Internet / Stratégie Internet

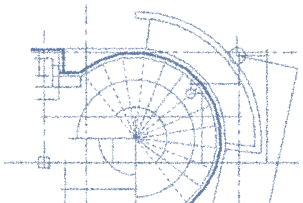
La CSSF opère une distinction principale entre «site informatif» et «site consultatif et/ou transactionnel» sur base de la notion d'authentification de l'utilisateur. Le site informatif est à considérer comme public et rien ne permet de supposer que tous ses utilisateurs sont clients de l'établissement. Un site est également considéré comme informatif s'il ne contient aucune donnée en rapport avec des clients individuels. Il peut, par conséquent, être hébergé par un fournisseur de services sans contraintes par rapport aux dispositions prévues par la circulaire IML 96/126 en matière de confidentialité en cas de sous-traitance du centre de traitement.

En ce qui concerne les sites informatifs qui présentent des informations régulièrement mises à jour (VNI, taux d'intérêts, ...), l'établissement doit s'assurer de l'intégrité de ces données et, en cas de sous-traitance, garder le contrôle de la mise à jour.

Les sites consultatifs et transactionnels, de par l'authentification des clients qui y est réalisée, tombent dans le champ d'application de la circulaire IML 96/126 pour ce qui est de la sous-traitance informatique[4]. La confidentialité des données doit être techniquement garantie[5], tant au niveau des données signalétiques qu'au niveau des transactions.

Les recommandations reprises dans ce document s'appliquent aussi, le cas échéant, aux établissements dont le réseau interne (LAN) est connecté à l'Internet dans le but d'offrir des services de consultation du Web ou de courrier électronique à leurs employés. Un établissement peut très bien disposer d'un site informatif hébergé auprès d'un tiers mais disposer d'une connexion Internet propre permettant à ses employés de surfer.

[4] Voir «Sociétés externes pour la gestion ou la maintenance» p. 42.
[5] Une garantie contractuelle prévue par un Service Level Agreement (SLA) est insuffisante.



A. Site Internet / Stratégie Internet

A.1. Nombre de sites

Sur 202 banques, 77 ont rapporté disposer d'une présence sur Internet, soit 38,12%.

Sur 113 PSF, 34 disposent d'une présence sur Internet, soit 30,09%.

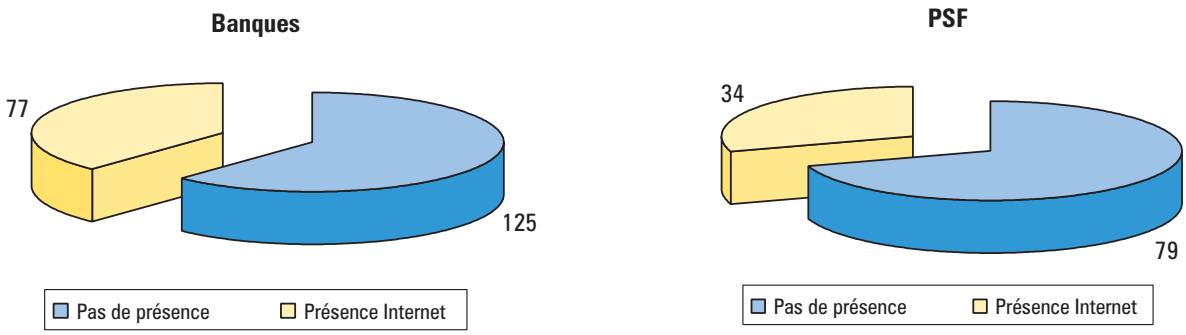


Figure 1: Nombre de présences Internet

Parmi les 202 banques, 13 ont soit un deuxième site Internet (8 sites), soit un second site en projet pour 2001 (5 projets). En ce qui concerne les PSF, 2 ont un projet de second site.

En termes de site Internet (et non de présence Internet) on a donc 85 sites pour 202 banques et 34 sites pour 113 PSF.

A.2. Nombre de projets

Parmi les 125 banques qui ne disposent pas encore d'un site, 27 ont un projet en cours. Sur 77 banques qui ont une présence Internet, 5 envisagent la création d'un deuxième site.

Parmi les 79 PSF qui ne disposent pas encore d'un site, 12 ont un projet en cours. Sur 34 PSF qui ont une présence Internet, 2 envisagent la création d'un deuxième site.

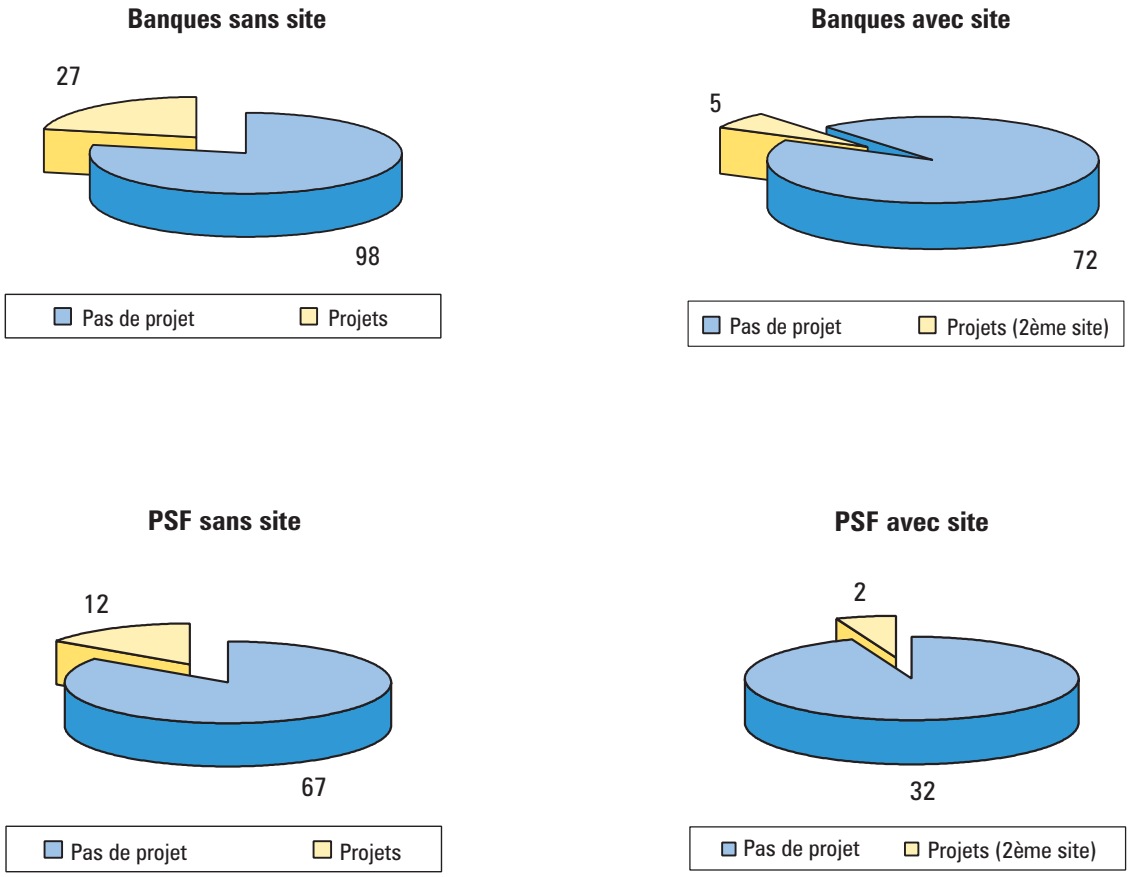


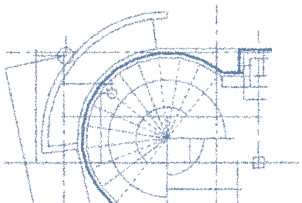
Figure 2: Nombre de projets

A.3. Nombre de modifications de type de site prévues

Sur les 77 banques qui ont déjà un site, 5 envisagent de modifier la nature du site[6] ou d'effectuer une revue importante des services proposés. Parmi les 113 PSF recensés, 12 ont un projet de modification.

Dans la majorité de ces cas, le second site est du type consultatif et/ou transactionnel et vient en complément à un site informatif existant. Cette volonté pour un même établissement de distinguer deux sites correspond pour partie à un impératif de confidentialité visant à séparer les clients des visiteurs «publics»[7], et pour partie à une volonté commerciale et/ou légale de distinguer les services et produits offerts.

[6] La nature du site passe de «informatif» à «consultatif» ou «transactionnel».
[7] Les clients disposent d'une communication, à caractère privée, qui est techniquement sécurisée par un autre protocole (ex.: HTTPS).



A.4. Présence sur d'autres pages

A la question «est-ce que votre établissement est présenté sur d'autres pages web au niveau de sites appartenant ou non au même groupe?», 99 banques et 43 PSF ont répondu par l'affirmative, alors que 103 banques et 70 PSF ont répondu par la négative. Ces chiffres se déclinent ainsi:

48	banques ayant déjà un site
12	banques ayant un projet
39	banques sans site, ni projet
99	**sont représentées sur un site tiers**

29	banques ayant déjà un site
15	banques ayant un projet
59	banques sans site, ni projet
103	**ne sont pas représentées sur un site tiers**

16	PSF ayant déjà un site
3	PSF ayant un projet
24	PSF sans site, ni projet
43	**sont représentés sur un site tiers**

18	PSF ayant déjà un site
9	PSF ayant un projet
43	PSF sans site, ni projet
70	**ne sont pas représentés sur un site tiers**

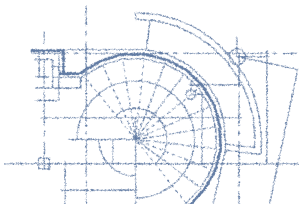
Figure 3: Nombre de représentations sur un site tiers

On doit considérer que seules les réponses positives sont fiables étant donné qu'un établissement répondant par la négative pourrait être représenté sur un site Internet sans avoir connaissance de cette représentation. Il est par conséquent plus exact de formuler le fait que 103 banques et 70 PSF n'ont pas connaissance d'être représentés sur un autre site.

La représentation de l'établissement sur un autre site peut se présenter sous forme d'une simple mention de l'adresse et du numéro de téléphone jusqu'à l'insertion de plusieurs pages de présentation dédiées à l'établissement sur un autre site (en général celui de la maison-mère). Au cas où l'établissement dispose déjà de son propre site, celui-ci peut être référencé au niveau du site de représentation.

Le contenu de ces pages de représentation dans le cadre d'un autre site, tout comme le contenu des sites gérés par l'établissement, doit être soumis à la CSSF en vertu du point 5.11 de la circulaire CSSF 00/15. La CSSF considère en effet que la présence d'un établissement sur un site Internet est une forme moderne de communication et de commercialisation. Les professionnels sont tenus de communiquer à la Commission le contenu de leurs messages publicitaires destinés à une diffusion à leur clientèle et au public. La Commission peut en demander la modification. Toute modification majeure d'un site doit également être soumise à la Commission.

Dans cet esprit, les établissements luxembourgeois sont de même responsables des publications faites à leur sujet sur les sites de tiers y inclus ceux opérés au niveau du groupe auquel ils appartiennent. Vu l'impossibilité d'avoir une maîtrise totale sur les informations publiées sur Internet au sujet de l'établissement, il s'agit ici d'une obligation de moyens et non de résultat. L'établissement doit donc mettre en œuvre tous les moyens techniques et organisationnels raisonnables dans le but de contrôler ces publications.



A.5. Répartition des sites par type

A.5.1. Sites existants

Sur les 85 sites bancaires opérationnels (85 sites pour 77 banques, étant donné qu'il existe des banques ayant plus d'un site),

- tous sont au moins de type informatif,
- 24 sont de type consultatif (24 sites pour 20 banques),
- 15 sont de type transactionnel (15 sites pour 11 banques).

Concernant les PSF, 33 sites sont informatifs et un site ne l'est pas. Ce site est orienté B2B, au même titre que deux autres, qui sont informatifs et transactionnels, sans pour autant être consultatifs. Parmi la totalité des 34 sites, 11 sont consultatifs et 12 sont de type transactionnel.

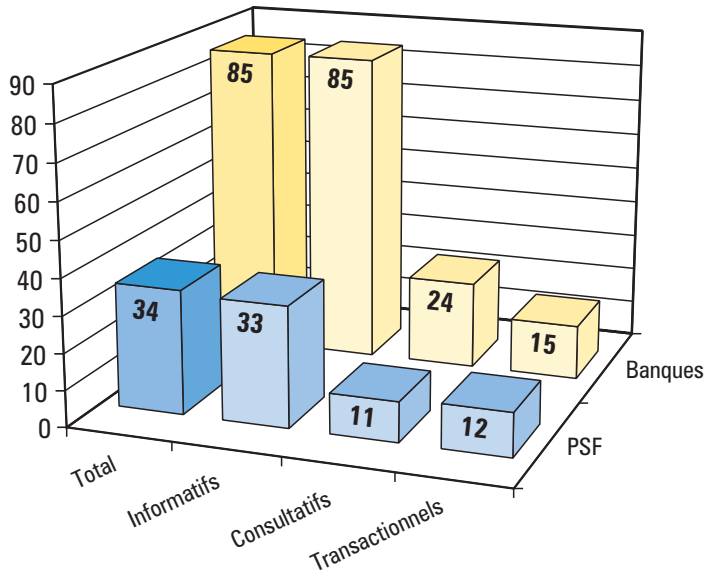


Figure 4: Répartition par type de site

Une étude plus fine des sites bancaires permet de détailler la combinaison de nature des sites, et donne les résultats suivant:

- 14 sites sont informatifs, consultatifs et transactionnels,
- 10 sites sont informatifs et consultatifs, mais pas transactionnels,
- 60 sites sont uniquement informatifs,
- 1 site est informatif et transactionnel, sans être consultatif.

La combinatoire des sites de PSF par type montre que:

- 9 sites sont informatifs, consultatifs et transactionnels,
- 1 site est informatif et consultatif, mais pas transactionnel,
- 21 sites sont uniquement informatifs,
- 2 sites sont informatifs et transactionnels, sans être consultatifs,
- 1 site est consultatif et transactionnel, sans être informatif.

A.5.2. Sites en projet

Sur les 32 projets de sites bancaires en cours (27 projets nouveaux[8], 5 projets de modification de site), 24 projets nouveaux et 4 projets de modifications sont transactionnels. Ceci montre que la tendance actuelle des nouveaux sites bancaires s'oriente fortement vers des services transactionnels dès leur ouverture, alors qu'à l'origine, les banques semblaient procéder de façon plus progressive, passant d'un site informatif, voire consultatif à l'ouverture, vers un site transactionnel quelques semestres plus tard. Il est probable que cette évolution n'est pas à imputer uniquement à une confiance grandissante dans ce canal de distribution, mais qu'elle peut également être attribuée à l'évolution de l'offre des produits logiciels qui permettent de gérer les transactions de manière fiable et sécurisée.

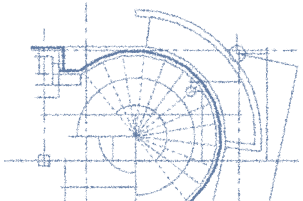
Parmi les 12 projets PSF en cours, tous aboutissent à un site informatif, 5 mènent à un site consultatif et un seul doit aboutir à un site de type transactionnel.

En comparant la nature des sites existants avec celle des sites en projet, on constate que les banques offrent de plus en plus de services transactionnels (opérations de virement, opérations sur titres), alors que les PSF ne suivent pas cette tendance. Une tentative d'explication serait à trouver dans le fait que la catégorie PSF regroupe des métiers très diversifiés alors certains ne s'adressent pas à un public cible suffisamment large pour justifier la mise en place de structures lourdes. Il est également possible qu'il s'agisse d'un phénomène de retard provenant de priorités différemment allouées par les banques et par les PSF.

Il est intéressant de remarquer que tous les sites bancaires (77 sites) sont au moins informatifs, alors qu'un site PSF est transactionnel mais pas informatif et deux sites sont informatifs et transactionnels sans être consultatifs.

Ceci laisse supposer que ces sites sont clairement orientés vers des services B2B, pour lesquels l'information publique n'est pas indispensable. Ainsi, il s'agit notamment de proposer aux distributeurs de fonds le passage d'ordres de rachat et de souscription. Un pareil site transactionnel mais non informatif peut être référencé sur le site informatif du distributeur.

[8] Par «nouveau», il faut comprendre des établissements ne disposant pas encore d'une présence Internet.



A.6. Limites sur les transactions financières

Sur 15 sites transactionnels bancaires, 10 appliquent des limites sur les transactions et 5 n'en ont pas.

Pour les PSF, 7 sites sur 11 appliquent des limites.

La tendance se confirme pour les projets, avec 11 projets bancaires fixant des limites et 3 projets n'en fixant pas. Le seul projet de site transactionnel PSF ne prévoit pas de limites.

Le dépouillement a montré une différence d'interprétation de la question, de telle sorte que la notion de «limite» a été le plus souvent comprise, soit comme une limite financière nominale par transaction (transaction ne pouvant pas dépasser un montant prédéfini), soit comme une limite fonctionnelle (montant ne pouvant pas dépasser le solde disponible), voire une combinaison des deux. Il en résulte une fiabilité réduite des analyses possibles de ces chiffres.

Dans le but de garantir une gestion saine des limites, la CSSF estime indispensable au moins la vérification du disponible (de préférence en temps réel en prenant en compte les transactions en cours) en vue de ne pas accorder un crédit non contrôlé au client. Cette vérification peut inclure des exceptions, notamment si le système permet la gestion d'approvisionnements futurs réguliers par un client ou lorsque l'établissement utilise une formule qui prend en compte les transactions en cours en vue de gérer un pourcentage contrôlé de crédit.

Toute limite doit être intégrée dans le dispositif général des limites fixées par l'établissement à l'égard d'une contrepartie ou d'un type d'exposition; ce principe gagne toute son importance si l'établissement exploite l'Internet comme canal de distribution parmi d'autres.

Dans le domaine du retail banking, des limites journalières, hebdomadaires ou mensuelles sont souhaitables. Celles-ci peuvent varier en fonction de la nature des transactions: virement entre deux comptes d'un même client, virements nationaux, virement internationaux.

L'application de telles limites doit être portée à la connaissance du client et figurer dans le contrat ou la convention que le client signe avec l'établissement dans le but de recourir aux services Internet.

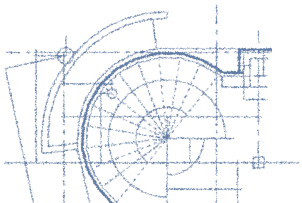
La définition et le bon fonctionnement de ces limites deviennent d'autant plus importants si le site est en Straight-Through-Processing[9] (STP) et que des contrôles manuels à priori ne sont donc plus possibles[10].

Un test de plausibilité sur les montants et les types d'opérations pourrait permettre d'élargir ces contrôles au niveau du flux de fonds et des bénéficiaires. Dans ce sens, la CSSF encourage ainsi l'utilisation de logiciels anti-blanchiment.

En conformité avec le point 5.4. et 5.5. de la circulaire CSSF 00/15, lorsque le client désire investir dans des produits qui peuvent comporter un risque élevé (produits dérivés ou autres instruments à effets de levier) ou quand le client envisage d'effectuer des opérations sur instruments financiers qui ne s'inscrivent pas par leur nature, par les instruments concernés ou par les montants en cause dans le cadre des opérations que le client traite habituellement, l'établissement est tenu d'avertir le client des risques inhérents. Si le canal Internet est utilisé, la CSSF recommande aux établissements que cet avertissement soit réalisé avant l'exécution de l'opération. Ceci serait le cas, par exemple, en ayant recours à des fenêtres supplémentaires, dotées de boutons d'acceptation, reprenant l'information sur le fonctionnement de ces produits et leurs risques.

[9] Voir aussi «Site relié au système bancaire / central», p. 37.

[10] Ceci s'applique également aux solutions STP qui n'utilisent pas le canal Internet.



A.7. Approche défensive ou offensive

Par approche défensive, on entend l'utilisation d'Internet en tant que canal de distribution supplémentaire pour les services traditionnellement prestés par l'établissement. On parle de la notion d'un établissement «multi-canaux».

L'approche offensive comprend les banques virtuelles qui offrent leurs services uniquement via Internet et les établissements qui offrent certains services uniquement disponibles via Internet en plus de leurs services traditionnels.

Il ressort du recensement, que les banques ont évalué la stratégie de leur site comme suit[11]:

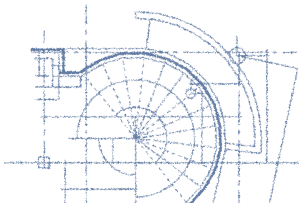
- Défensive
  - ➨ 80 sites, répartis en 11 sites consultatifs et transactionnels, 8 sites consultatifs mais non transactionnels, un site transactionnel mais non consultatif et 60 sites uniquement informatifs.
- Offensive
  - ➨ 5 sites, répartis en 3 sites consultatifs et transactionnels et 2 sites consultatifs mais non transactionnels.

Au niveau des PSF, l'évaluation est la suivante:

- Défensive
  - ➨ 30 sites, répartis en 5 sites consultatifs et transactionnels, un site consultatif mais non transactionnel, 2 sites transactionnels mais non consultatifs et 22 sites uniquement informatifs.
- Offensive
  - ➨ 4 sites, tous consultatifs et transactionnels.

La tendance nettement défensive se poursuit également au niveau des projets, avec 28 sites bancaires «défensifs» contre 4 sites «offensifs», et pour les PSF, la totalité des 12 projets de sites sont considérés «à stratégie défensive».

[11] Les réponses obtenues sont à apprécier avec prudence, particulièrement parce que la notion de «défensif» ou «offensif» est sujet à interprétation.



A.8. Clientèle visée

L'absence de frontières géographiques

Internet est un espace virtuel dans lequel les frontières ne sont plus géographiques. Il est impossible pour un établissement connecté à Internet de restreindre techniquement ses communications à certains pays, ce qui implique qu'il ne peut ni empêcher un individu localisé dans un pays particulier de consulter son offre de services, ni restreindre les transactions de ses clients lorsque ceux-ci se déplacent dans le monde.

Il peut persister encore une certaine incertitude juridique sur la validité de la notion de «disclaimer» qui peut protéger l'établissement en indiquant des restrictions sur la destination des informations ainsi que la responsabilité du contenu.

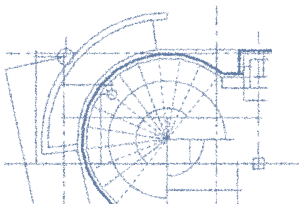
Cette incertitude persistera tant que les conditions de sollicitation et de prestations de services financiers à distance sans présence physique de l'établissement dans le pays d'accueil ne sont pas harmonisées.

A la question «est-ce que le site vise une clientèle spécifique?», le recensement pour les sites bancaires indique 45 «oui», contre 40 «non» et, pour les sites de PSF, 17 «oui» contre 17 «non».

La lecture des commentaires indiqués dans les réponses montre clairement deux interprétations différentes de cette question. Certains établissements ont répondu en considérant la clientèle spécifique visée par le site comme différente de la clientèle habituelle, alors que d'autres établissements ont considéré de fait leur clientèle comme spécifique par rapport aux métiers financiers traditionnels (par exemple, private banking, fonds, dépositaire de titres...).

Dans la mesure où Internet est considéré comme un canal de distribution de produits financiers offerts par un établissement pouvant se servir en même temps de canaux de distribution traditionnels, les risques financiers entrent dans le cadre général de la surveillance de l'activité de l'établissement, car il n'y a en principe pas de modification de l'activité elle-même ou des services. La dimension géographique est dûment à prendre en compte en raison de l'impact éventuel des volumes générés par l'Internet qui permet d'atteindre davantage de régions et de marchés.

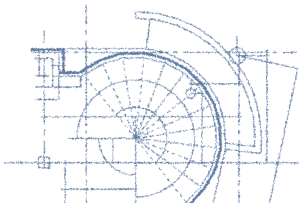
L'établissement devrait également éviter d'adresser explicitement à travers un site Internet une clientèle ou un marché qui ne devrait pas être ciblé. Afin d'éviter des conflits avec des juridictions étrangères, il est recommandé que l'établissement indique clairement, en utilisant des disclaimers, qu'un produit ou un service ne peut être offert à une clientèle donnée.



A. Site Internet / Stratégie Internet

La prestation transfrontalière de services financiers par Internet

La directive actuellement en discussion devrait régler un grand nombre d'aspects légaux au sein de l'Union Européenne, mais elle ne peut régler les aspects légaux internationaux dépassant le cadre de l'U.E., et en particulier la sollicitation et la prestation de services financiers sans présence physique dans le pays d'accueil. Actuellement, le cadre juridique pour la prestation de services financiers repose, à l'exception de la «libre prestation de services» au sein de la Communauté européenne, sur une présence physique de l'établissement financier dans le pays où ses services sont fournis. La surveillance prudentielle entre le pays d'origine d'un établissement financier et le pays d'accueil (succursale et filiale) est efficace et fonctionne grâce à une répartition des compétences. A l'heure de l'Internet, ce cadre juridique est insuffisant et les établissements financiers se protègent tant que faire se peut à l'aide de clauses spécifiques (disclaimer clauses) qui délimitent de manière contractuelle les juridictions avec lesquelles l'activité est possible ou refusée. La CSSF participe sur un plan international à la définition d'un cadre nouveau permettant la coopération entre autorités de contrôle afin de garantir la surveillance coordonnée de cette manière.



A.9. Nouveaux clients obtenus grâce au site

Seuls 8 banques et 5 PSF ont été en mesure d'évaluer le nombre de nouveaux clients obtenus grâce au site.

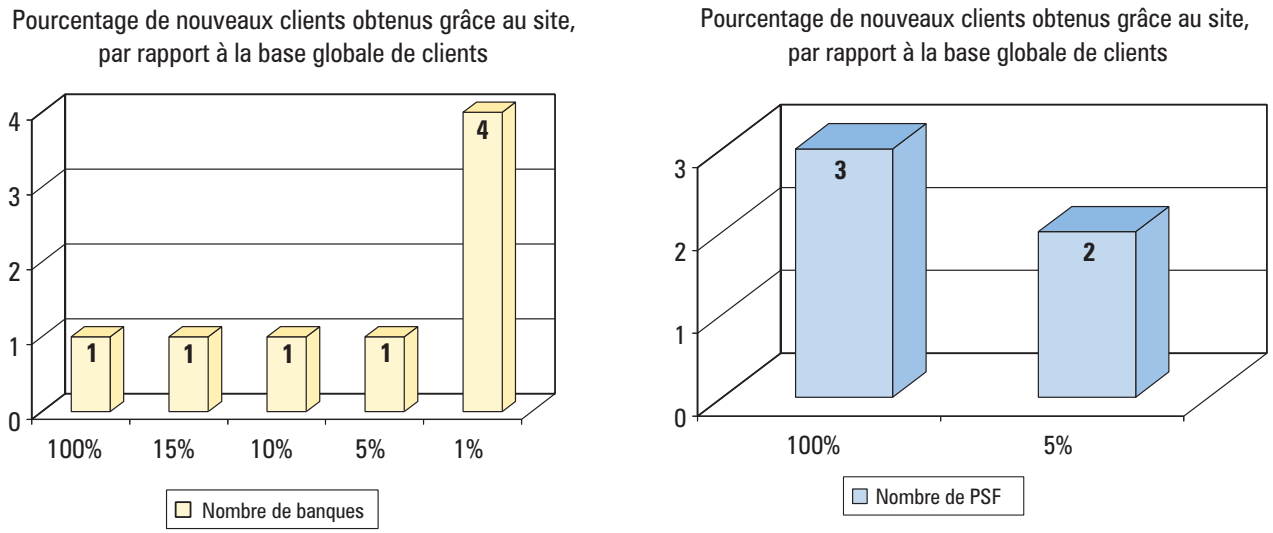


Figure 5: Pourcentage de nouveaux clients

La banque et les PSF indiquant 100% sont par définition des établissements utilisant Internet comme unique canal de distribution des produits et services financiers (terminologie de «Banque virtuelle» ou «PSF virtuel»).

Il aurait été intéressant de comparer ces chiffres à ceux d'autres pays, mais la CSSF n'a trouvé aucune source fiable et comparable concernant ce sujet.

A.10. Entrée en relation d'affaires sans présence physique

Les problèmes liés à l'ouverture de compte via Internet

A la suite de l'apparition du «Internet Banking», afin d'intégrer dans sa réglementation les spécificités techniques de ce canal de distribution, la CSSF adapte ses exigences en ce qui concerne la documentation de l'identification du titulaire d'un compte. Les exigences modifiées tiennent compte du fait que le site (transactionnel) doit permettre au client d'entrer en relation d'affaires avec l'établissement, notamment en ouvrant un compte sans présence physique, les documents d'ouverture de compte pouvant être mis à disposition via Internet. Contrairement à ce qui était requis jusqu'à présent, en cas d'ouverture de compte dans les guichets de l'établissement ou par correspondance, la photocopie de la pièce d'identité du titulaire ne doit plus être certifiée conforme à condition que la personne en question dispose déjà d'un compte auprès d'une banque située dans un pays membre du GAFI et à condition que le premier virement provienne de ce compte.

Les établissements souhaitant faire usage de cette possibilité d'entrée en relation d'affaires sans présence physique, doivent soumettre à la CSSF une proposition de procédure permettant de s'assurer que les exigences y liées seraient respectées.

A titre d'exemple, une procédure découlant des obligations professionnelles de l'établissement consisterait à ce que l'ordre de virement signé par le client soit remis par ce dernier à la banque luxembourgeoise, puis envoyé par celle-ci, complété par un numéro de référence que le client ne connaît pas, à la banque du client. Lors de la réception du transfert, la banque luxembourgeoise peut vérifier à l'aide du numéro de compte et du numéro de référence que l'argent provient effectivement d'un compte appartenant au client auprès de sa banque d'origine.

En effet, cette procédure garantit à l'établissement que le client est en possession d'un compte auprès de l'établissement émetteur et qu'il n'a pas effectué un versement.

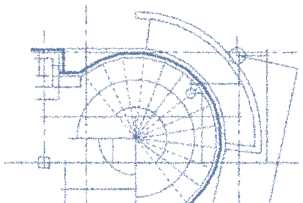
En général, l'ouverture de compte sans présence physique a été définie, par les établissements, comme incluant la procédure d'envois des documents d'ouverture de compte via courrier. Quelques établissements ont ajouté la notion de signature électronique à l'ouverture de compte via Internet (et ont donc répondu négativement à cette question).

Uniquement 5 banques (6,5%) ont indiqué qu'elles acceptent une ouverture de compte via Internet. Il s'agit de 3 sites transactionnels et de 2 sites purement informatifs.

Au niveau des PSF, 6 sites permettent l'ouverture de compte en ligne. Il s'agit de 4 sites transactionnels, d'un site qui est transactionnel mais pas consultatif et d'un site transactionnel, consultatif mais pas informatif.

Au niveau des banques, 4 des 27 projets de nouveau site et 2 des 3 projets de modifications de site envisagent l'ouverture des comptes en ligne.

Les projets de site concernant les PSF n'incluent qu'un seul qui permet l'ouverture de compte sans présence physique.



A. Site Internet / Stratégie Internet

Les obligations professionnelles en matière de blanchiment

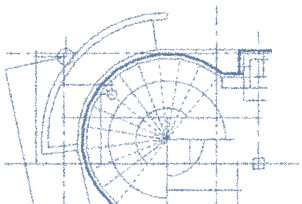
La loi modifiée du 5 avril 1993 sur le secteur financier définit un certain nombre d'obligations professionnelles à respecter par les professionnels du secteur financier afin d'éviter qu'ils ne soient utilisés à des fins de blanchiment. Ces obligations professionnelles ont été précisées dans les circulaires IML 94/112, BCL 98/153, CSSF 00/16 et CSSF 00/21:

- identifier les clients au moyen de documents probants. Par client il y a lieu d'entendre les clients directs et les ayants droit économiques des sociétés écrans; il s'agit non seulement de connaître l'identité du client, mais également de rassembler des informations sur ses activités et sur le but de la relation d'affaires recherchée;
- instaurer des procédures de contrôle interne et de communication adéquates afin de prévenir et d'empêcher la réalisation d'opérations de blanchiment;
- sensibiliser les employés aux dispositions contre le blanchiment et organiser des programmes de formation;
- suivre les opérations effectuées par les clients et examiner avec une attention particulière les opérations qui paraissent suspectes;
- coopérer avec les autorités en répondant de la manière la plus complète possible aux demandes d'informations et en informant, de leur propre initiative, le Parquet de tout fait qui pourrait être l'indice d'un blanchiment.

Rappelons le cadre réglementaire applicable en matière d'identification d'un client. L'identification d'un client, pour lequel un professionnel financier ouvre un compte, doit être faite et entièrement accomplie avant que le professionnel n'exécute une opération pour ce client.

Si, avant d'exécuter une opération pour le client et avant que l'identification du client ne soit entièrement accomplie, le professionnel accepte des fonds du client, serait-ce à titre provisoire et sur un compte bloqué, ou s'il accepte d'ouvrir un compte même non opérationnel pour le client, il doit savoir qu'il engage sa responsabilité s'il permet au client de disposer des fonds ou simplement de faire état de l'existence du compte.

Si, malgré les prescriptions existantes, l'identité d'un client et celle des ayants droit éventuels n'a pas été correctement établie, il est inadmissible qu'un professionnel financier se dessaisisse de biens, par décaissement ou par virement, au profit ou sur l'ordre de ce client, tant que l'identité du client n'a pas été établie à l'entière satisfaction du professionnel financier. En attendant, il incombe au professionnel financier de continuer à assurer la garde de ces biens dans l'intérêt des ayants droit, conformément aux conditions sous lesquelles il les a reçus, à moins qu'il ne les consigne si les conditions pour une consignation sont remplies.



A. Site Internet / Stratégie Internet

La relation entre un professionnel financier et son client s'établit «intuitu personae». Voilà pourquoi l'ouverture de compte à un nouveau client implique un jugement sur le client. Ce jugement doit être étayé par des informations sur le client, sur ses activités, sur le but de la relation d'affaires recherchée. L'importance pour le professionnel financier de disposer de ces informations consiste en ce qu'elles devraient lui permettre de réduire au mieux le risque d'être utilisé à des fins de blanchiment et plus tard de détecter les transactions qui sont suspectes parce qu'elles ne sont pas compatibles avec les informations reçues. Un fait insolite constaté au moment de l'identification pourrait être l'indice d'un blanchiment et devrait en tant que tel amener le professionnel à demander des informations complémentaires. Une attention particulière doit être exercée lorsque la motivation de la relation d'affaires recherchée n'est pas claire ou lorsque le client a recours à des constructions dont la justification économique n'est pas apparente (enchevêtrement de comptes, comptes à désignation pouvant induire en erreur, etc.).

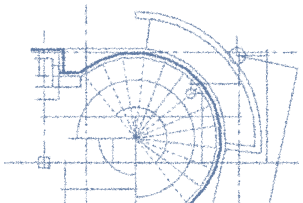
Toute ouverture de compte pour un nouveau client doit être soumise pour autorisation par écrit à un préposé ou à un organe du professionnel financier spécifiquement habilité à cet effet. Cette personne ou cet organe doit d'un côté apprécier s'il est indiqué d'ouvrir un compte à ce client, d'un autre côté porter la responsabilité pour l'identification du client et pour la documentation afférente.

Le professionnel financier ne saurait déléguer la responsabilité pour l'identification de ses clients, éludant ainsi son obligation de connaître ses clients avec la responsabilité que cette connaissance lui confère. Il ne saurait p.ex. se satisfaire d'un certificat établi par un tiers, quelle que soit sa qualité, attestant que ce tiers connaît l'identité du client, l'a vérifiée et dispose de la documentation requise.

Lorsque l'ouverture de compte pour un nouveau client se fait sur base d'une relation directe entre le professionnel financier et le client, mais à distance, c'est-à-dire sans que le professionnel et le client ne soient physiquement en présence l'un de l'autre, le professionnel doit veiller avec une attention particulière à recevoir non seulement toute la documentation requise, mais également des réponses complètes et satisfaisantes à toutes les questions qu'il sera amené à poser au client en vue de porter un jugement éclairé sur ce client et sur sa motivation.

Lorsque le professionnel du secteur financier délègue certaines opérations techniques ayant trait à l'identification de ses clients, il faut que cette délégation soit donnée dans un cadre défini de manière précise par la direction et à un partenaire professionnel qualifié. La CSSF n'accepte comme délégués que:

– les établissements de crédit et autres professionnels du secteur financier, admis à exercer leurs activités au Luxembourg en vertu de la loi du 5 avril 1993;



– les établissements de crédit et autres professionnels du secteur financier admis à exercer leurs activités à l'étranger et soumis à une surveillance prudentielle par une autorité compétente, lorsque le professionnel financier luxembourgeois a conclu par écrit avec ce partenaire étranger un accord de coopération spécifique, définissant avec précision les tâches déléguées en tenant compte des normes luxembourgeoises.

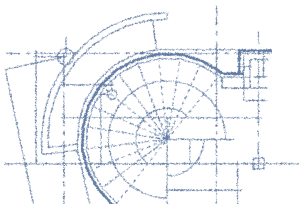
La délégation de l'identification ne réduit en rien les exigences concernant la documentation sur le client qui doit être disponible chez le professionnel financier au Luxembourg. Il s'ensuit qu'en cas de transfert d'un client par un partenaire bancaire, toute la documentation requise au Luxembourg doit également y être transférée.

La notion de «client» englobe non seulement la personne au nom de laquelle un compte est ouvert, mais également ses co-titulaires et ses mandataires ou les ayants droit économiques pour lesquels elle agit.

Sont aussi à considérer comme des clients en relation d'affaires ceux pour lesquels sont ouverts des comptes de passage, servant uniquement à une ou plusieurs opérations ponctuelles.

Les exigences sur la conservation des documents d'identification restent applicables.

La connaissance du client ne se limite pas au moment de l'ouverture de compte mais est à prendre en compte pendant toute la durée de la relation entre l'établissement et le client. Ceci est d'autant plus important quand il s'agit d'une solution en Straight-Through-Processing (STP).



A.11. Sous-traitance pour la création des sites

Sur 77 banques, 62 banques (soit 80,5%) ont eu recours à des sociétés externes pour la création de leurs sites[12]. En nombre de sites, ce chiffre donne 70 sites sur 85 au total qui ont été réalisés à l'aide d'une assistance externe, soit 82,3%. La CSSF a constaté, lors des entrevues et contrôles sur place, que les établissements financiers sous sa surveillance ont eu recours massivement à des solutions totalement ou partiellement «clé en main» (en termes informatiques: solutions packagées).

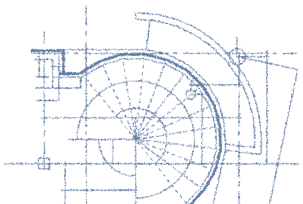
La CSSF n'a pas d'objection en ce qui concerne le recours à ces solutions «clé en main», qui permettent d'éviter le temps de développement d'une solution interne, mais attire l'attention sur l'obligation de l'établissement de garder la maîtrise de son système informatique. En effet, l'établissement doit connaître le fonctionnement des différents éléments du système et avoir la garantie que le fournisseur est dans l'impossibilité d'implémenter des fonctionnalités inconnues de l'établissement, particulièrement parce que ces fonctionnalités pourraient être accessibles depuis n'importe quel point du globe au travers d'Internet par des individus mal intentionnés[13]. De plus, l'établissement doit s'assurer de la continuité du système en cas de défaillance du fournisseur (circulaire IML 96/126).

Il serait souhaitable que l'établissement qui a recours à une solution «clé en main» fasse valider l'intégrité[14] de cette solution par un tiers. Au cas où la même solution serait utilisée par plusieurs établissements, cette validation peut être faite de manière collective pour les parties communes.

12 Voir aussi «Sociétés externes pour la gestion ou la maintenance», p. 42.

13 La question de l'intégrité des logiciels a toujours été à prendre en compte, mais dans le cadre des applications accessibles depuis Internet, le cadre opérationnel n'est plus limité à l'organisation interne de l'établissement puisque les opérations sont initiées non plus au guichet mais à distance. L'impact d'une fraude liée à l'utilisation d'un virus est immédiat et difficile à identifier.

14 L'intégrité est définie comme certitude que la solution dispose de toutes les fonctionnalités demandées mais ne comprenne pas de fonctions inconnues.



A.12. Budgets de création des sites bancaires

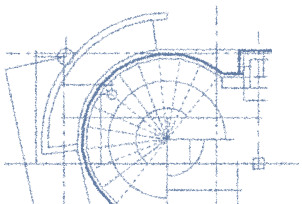
Sur 202 banques (85 sites), 23 banques (25 sites) n'ont pas été en mesure d'indiquer un budget des coûts de mise en œuvre du site Internet. Le taux de réponse par rapport au nombre de sites n'est donc que de 70,6%.

La répartition par tranche de € 1.000.000 est la suivante:

Euro		€	Sites informatifs	Sites consultatifs	Sites transactionnels
De 0	à	999.999	38	6	4
De 1.000.000	à	1.999.999	0	1	4
De 2.000.000	à	2.999.999	0	1	0
De 3.000.000	à	3.999.999	0	0	1
De 4.000.000	à	4.999.999	0	0	1
De 5.000.000	à	5.999.999	0	0	1
De 6.000.000	à	6.999.999	1	0	1
Supérieur	à	7.000.000	0	0	1

Figure 6: Budget de création de site par tranche de € 1.000.000 (banques)

Les sites informatifs se situent, à une exception près, tous dans un budget inférieur au million d'euro, ce qui en soit n'est pas étonnant puisqu'ils ne font appel à aucune fonctionnalité interactive particulière (pas d'authentification des utilisateurs, pas d'interfaces bilatéraux sophistiqués avec les applications bancaires etc.).



Le tableau suivant correspond à une description plus fine des budgets inférieurs au million d'euro.

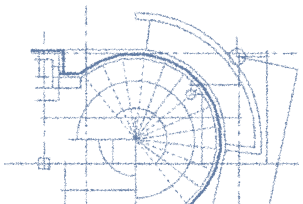
			Euro	€	Nombre de sites
De	0	à	9.999		6
De	10.000	à	99.999		29
De	100.000	à	199.999		6
De	200.000	à	299.999		1
De	300.000	à	399.999		1
De	400.000	à	499.999		1
De	500.000	à	599.999		0
De	600.000	à	699.999		1
De	700.000	à	799.999		2
De	800.000	à	899.999		1
De	900.000	à	999.999		0

Figure 7: Détails des budgets de création < € 1.000.000 (banques)

Une majorité des sites à budget relativement restreint (sites informatifs) ont coûté moins de 200.000 €.

Le premier tableau ne fait plus apparaître de nette tendance budgétaire pour les sites transactionnels, sachant que les montants s'échelonnent de 1 à 7 millions d'euros. Ceci s'explique probablement par la différence de stratégie suivie par les banques et par le degré d'intégration des applications web avec les applications bancaires. En moyenne, le rapport de coût entre un site simplement informatif et un site transactionnel varie de 5 à 35 (200.000 par rapport à 1.000.000 ou 7.000.000).

Le budget de création d'un site peut être influencé à la baisse si une solution transactionnelle existe déjà au sein du groupe de l'établissement.



A. Site Internet / Stratégie Internet

Concernant les PSF, 15 seulement ont rapporté un budget de création de leur site. Le tableau 3 a été composé selon une échelle non linéaire et plus représentative de l'échantillon.

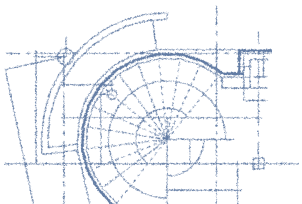
	Euro		€	Nombre de sites
De	0	à	20.000	10
De	20.001	à	1.000.000	2
De	1.000.001	à	4.000.000	3

Figure 8: Budget de création de site (PSF)

Parmi les 10 sites à budget réduit, 9 sont uniquement informatifs et un seul est informatif et consultatif.

Sur les deux sites à budget supérieur à 20.000 € et inférieur à 1.000.000 €, un est uniquement informatif et l'autre est consultatif et transactionnel, mais pas informatif, donc probablement destiné à une activité B2B.

Sur les trois sites à budget élevé, tous sont informatifs, consultatifs et transactionnels et deux sont plus proches de la borne inférieure (un million) que supérieure (quatre millions).



A.13. Délai de rentabilité des sites

Seulement 4 banques (5 projets) et 3 PSF (aucun projet) qui disposent d'une présence Internet ont indiqué un délai de rentabilité de leur site.

La difficulté de prévoir avec une précision raisonnable un délai de rentabilité se confirme par ce faible taux de réponse et le fait qu'aucune banque ou PSF n'ait indiqué des critères de calcul de rentabilité.

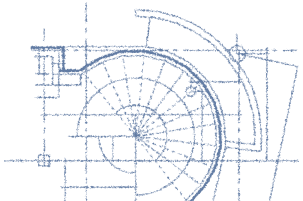
Les rares réponses fournies s'articulent autours de 3 années.

La CSSF apprécie ces estimations comme étant plutôt optimistes. Il est à noter cependant que les établissements ont tenu compte de la situation économique et ont revu ces estimations selon un schéma plus réaliste.

En tenant compte des investissements importants d'un site Internet (surtout transactionnel) et de la concurrence prononcée dans ce domaine, une présence Internet peut être considérée comme une obligation pour la rétention des clients et il devient dès lors difficile de calculer une rentabilité.

La réalité a montré que, en ce qui concerne les approches défensives, Internet est actuellement un centre de coût et non un centre de profit.

A court terme, la mise en œuvre de services par Internet entraîne de nouveaux coûts qui peuvent éventuellement permettre une réduction des coûts à long terme grâce à une automatisation de certains processus. Cette réduction ne doit pas se faire au détriment de la qualité des contrôles ou en générant une augmentation des risques (ex.: solution STP sans contrôles suffisants, architecture faiblement sécurisée, absence de revue des logs...).



A.14. Pourcentage de clients ayant souscrit une convention Internet

Les taux de réponse, 16,89% (13 sur 77 banques) et 11,76% (4 sur 34 PSF), sont très faibles.

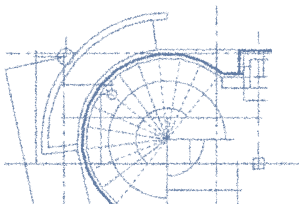
A l'exception des banques virtuelles (où 100% des clients ont souscrit une convention Internet) et d'une banque ayant indiqué 70% de conventions Internet par rapport au nombre total de clients, les rares réponses fournies donnent toutes des proportions inférieures ou égales à 20% (chiffre réel au 31.12.2000). En ce qui concerne les prévisions (estimation pour le 31.12.2001), les mêmes remarques sont à formuler avec une légère augmentation pour les sites n'ayant pas encore atteint les 20%.

Au niveau des projets, les prévisions sur un an correspondent principalement aux réponses des sites déjà en production, tandis que les prévisions sur 2 ans sont plus élevées.

Afin d'éviter une insécurité juridique, l'utilisation des services Internet doit être réglée par un contrat. Pour les sites consultatifs et transactionnels un contrat entre l'établissement et ses clients est nécessaire pour définir les conditions des services fournis. Ce contrat définit en particulier les responsabilités de l'établissement et du client, notamment en ce qui concerne l'utilisation des éléments d'identification du client. Le contrat doit également reprendre le mécanisme de preuve qui est d'application pour les transactions saisies via Internet. La CSSF encourage les établissements à recourir à des modalités de preuve[15] qui ne défavorisent pas systématiquement le client.

Les divers éléments réglés peuvent être inclus dans les conditions générales ou, ce qui est préférable, dans une convention à part entre l'établissement et le client.

[15] Parmi les éléments de preuve, interviennent les aspects d'authenticité, d'intégrité, de confidentialité et de non-répudiation des informations. Voir aussi «Authentification du client / Données confidentielles», p. 49.



A.15. Utilisation régulière des clients

Ici aussi, les taux de réponse, 12,99% (10 sur 77 banques) et 8,82% (3 sur 34 PSF), sont très faibles.

A l'exception des banques virtuelles (où 100% des clients utilisent régulièrement les services Internet), les rares réponses fournies se situent entre 40% et 60% avec une exception de 30%. Sur un an, les banques ne voient pas de grande évolution, ne fût-ce qu'une faible augmentation de ces pourcentages.

Au niveau des projets, les pronostics sur un an correspondent principalement aux réponses des sites déjà en production. De même, les prévisions sur 2 ans sont légèrement plus élevées à l'exception d'un site qui prévoit une baisse d'utilisation passant de 80% à 50%.

A.16. Acceptation d'hyperliens

46 des 85 sites bancaires acceptent des hyperliens vers d'autres sites (54,12%). Sur les 34 sites des PSF, 20 acceptent des hyperliens (58,82%).

En général les sites n'acceptent que des hyperliens (réciproques) internes à leur groupe ou de fournisseurs (ex.: informations financières).

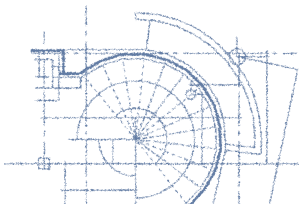
L'acceptation de liens vers d'autres pages Internet (ainsi que le fait d'être référencé par d'autres sites) peut entraîner des conséquences au niveau de la responsabilité du contenu. En effet, s'il n'est pas clairement mentionné que l'information à laquelle l'utilisateur accède via un lien n'est pas sous la responsabilité de l'établissement, celui-ci peut être induit en erreur.

Il y a lieu d'attirer l'attention sur l'importance des «disclaimers» qui mentionnent que l'information provient d'un tiers. De plus, il serait souhaitable, malgré la présence d'un disclaimer dégageant l'établissement de la responsabilité du contenu, que l'établissement vérifie régulièrement les informations accessibles via des liens (ex.: lien sur des pages externes reflétant un contenu qui, modifié, pourrait ne plus répondre au cadre réglementaire luxembourgeois).

En effet, l'établissement est tenu de préciser à l'utilisateur quelles données ne sont pas sous sa maîtrise et sa responsabilité, particulièrement si ces informations sont accessibles sur le site de l'établissement ou à travers un lien (ex.: informations financières de fournisseurs spécialisés dans ce domaine, lien externe sur des prospectus de fonds,...).

Il serait souhaitable qu'un établissement connaisse les sites qui font référence au sien, mais, en pratique, cette recherche peut s'avérer difficile.

Il existe des possibilités, dont par exemple l'utilisation de certaines fonctions de moteurs de recherche ou l'analyse des logs du serveur concernant les informations de type «referrer», qui permettent d'évaluer de quels liens proviennent les accès.



A.17. Bannières publicitaires

7 des 85 sites bancaires acceptent des bannières (8,24%).

Sur les 34 sites des PSF, 1 seul accepte des bannières publicitaires (2,94%).

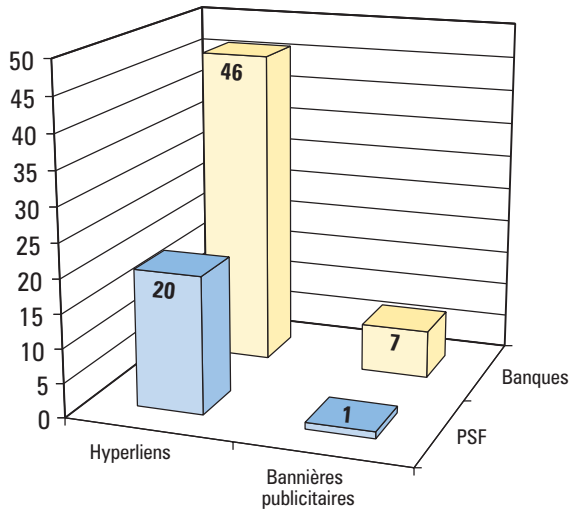


Figure 9: Acceptation d'hyperliens / bannières publicitaires

En général les sites n'acceptent que des bannières internes au groupe auquel appartiennent les établissements concernés.

La CSSF attire l'attention sur le fait que les bannières externes sont à considérer comme des liens externes pour lesquels l'établissement n'a pas la maîtrise du contenu[16].

[16] Voir «Acceptation d'hyperliens», p. 31.

A.18. Site Multilingue

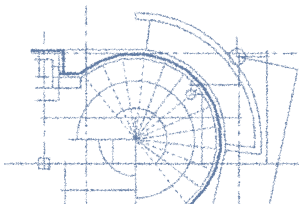
45 des 85 sites bancaires sont disponibles au moins dans deux langues (52,94%).

Sur les 34 sites des PSF, 16 sites sont multilingues (47,06%).

Hormis le fait que le contenu d'un site peut être présenté en plus de deux langues, voici la représentation des différentes langues (ordre décroissant des banques):

Langue	Banque Sites	PSF Sites
Anglais	44	14
Français	33	13
Allemand	33	9
Néerlandais	10	10
Italien	3	4
Scandinave	3	1
Espagnol	1	3
Portugais	0	1

Figure 10: Répartition des langues (sites)



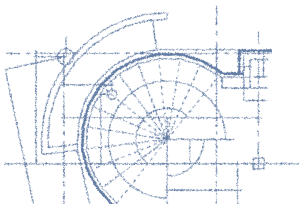
A. Site Internet / Stratégie Internet

Langue	Banque Projet	PSF Projet
Anglais	25	10
Français	17	9
Allemand	15	5
Néerlandais	7	1
Italien	3	5
Scandinave	3	0
Espagnol	3	3
Portugais	2	1

Figure 11: Répartition des langues (projets)

Dans les rares cas où le contenu du site varie d'une langue à l'autre, cette différence s'explique généralement par une adaptation dictée par les réglementations en vigueur dans les divers pays cibles.

Les établissements doivent soumettre pour approbation le contenu de leur site à la CSSF en français, en allemand ou en anglais. Si le contenu n'existe pas dans une de ces trois langues, l'établissement doit traduire le contenu du site. Si le site existe dans au moins une de ces trois langues, l'établissement doit s'engager à veiller à ce que toutes les versions linguistiques correspondent au contenu soumis à la CSSF.



B.1. Site relié au réseau interne (LAN)

Internet est un réseau mondial qui est, de par sa nature et sa destination, accessible à tous les utilisateurs travaillant avec des équipements qui se servent de protocoles standardisés du domaine public. Par conséquent, Internet est également ouvert à des utilisateurs mal intentionnés et disposant d'une grande visibilité sur les formats et protocoles d'échanges, ce qui rend ce réseau potentiellement peu sécurisé. Il importe, actuellement pour les établissements financiers et prochainement pour les clients «internautes», de mettre en place des outils de protection spécifiques à Internet et d'en vérifier la fiabilité. Cette mise en œuvre de la sécurité engendre un coût qui, de surcroît, est récurrent si les standards de sécurité sont régulièrement tenus à jour.

Pour éviter une pénétration sur le réseau interne d'un établissement financier, la meilleure solution est l'utilisation d'un serveur Internet qui n'est pas lié au réseau interne. L'échange entre le réseau interne et le réseau Internet se fait dans cette hypothèse par un moyen de communication temporaire (ex: tape). Cette structure ne se prête évidemment pas bien à l'exploitation d'un site interactif.

Dans le groupe des banques, 15 sites purement informatifs sont reliés au réseau interne de la banque. 7 sites consultatifs, 11 sites consultatifs et transactionnels et 1 site transactionnel mais non consultatif se trouvent sur le réseau interne des différentes banques.

46 sites informatifs, 3 consultatifs et 3 sites transactionnels sont en stand-alone.

Dans le groupe des PSF, on constate 5 sites informatifs, 1 site purement transactionnel et 8 sites consultatifs et transactionnels qui sont reliés au réseau interne du PSF correspondant.

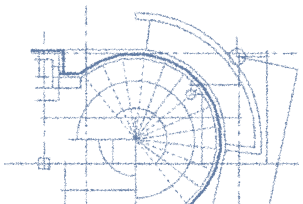
Les 17 sites informatifs ainsi que le site purement transactionnel, le site purement consultatif et le site consultatif et transactionnel n'ont pas de lien avec le réseau interne.

Les projets montrent les mêmes tendances: sur les 18 sites bancaires qui sont destinés à être reliés au réseau interne, 2 sont purement informatifs. Pour les PSF, un total de 5 projets de sites prévoient un lien avec le réseau interne. 2 de ces sites sont purement informatifs.

La plupart des connexions du serveur qui héberge le site Web sont protégées au moins par un «firewall».

Lorsqu'il existe un lien permanent entre le site Internet et le réseau interne, l'établissement doit s'assurer que les précautions nécessaires aient été prises.

A partir du moment où le réseau interne de l'établissement est connecté à Internet, même sans présence d'un site, l'établissement doit prendre les mesures nécessaires pour se protéger contre des accès non autorisés. La CSSF recommande l'application des «best practices» qui peuvent se décliner ainsi:



B. Sécurité / Maintenance

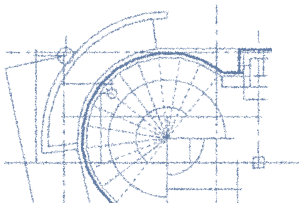
- Il est conseillé de protéger l'accès au réseau interne par au moins deux «firewalls»[17]. Ces «firewalls» sont de préférence de type différent et de système d'exploitation différent, de sorte que l'exploitation des failles du premier firewall par un intrus ne peut pas être reproduite sur le deuxième firewall.
- L'utilité des «firewalls» est optimale si elle est combinée à une paramétrisation méticuleuse et un suivi du log régulier. Il est recommandé de limiter les interfaces (segments de réseau) par firewall dans le but de garantir une gestion des règles simple et efficace. Les serveurs de données qui se trouvent dans la DMZ doivent contenir un minimum d'informations sensibles.
- Les transactions qui se trouvent sur un serveur dans la DMZ doivent être transmises au plus vite (de préférence en temps réel) vers le réseau interne.
- Un système de détection des intrusions (IDS[18]), connecté par exemple en amont du premier firewall ou sur la DMZ permet de faire une analyse des anomalies et de détecter une attaque éventuelle invisible pour les firewalls. Dans ce cas également, une paramétrisation ainsi qu'un suivi des logs sont d'une importance primordiale. Seul, un détecteur d'intrusion peut être capable de bloquer certaines tentatives d'intrusion (web tunneling, par exemple) en ajoutant une règle plus restrictive au niveau du firewall.
- Un logiciel anti-virus doit limiter la perte d'intégrité du système qu'il protège, en diagnostiquant la présence et en stoppant l'activité d'un virus éventuel. Un système corrompu doit être, soit reconstruit, soit récupéré d'une sauvegarde dont l'intégrité est garantie.
- Des procédures adéquates devront définir les actions à prendre en cas de détection d'attaque et devront indiquer comment revenir à une situation sécurisée de production[19].
- Des procédures concernant l'exploitation et la maintenance de cette infrastructure doivent être mises en place. Ces procédures doivent respecter les principes de la séparation des tâches et des 4 yeux[20].
- Un processus de veille technologique et de sécurité doit permettre à l'établissement de se tenir à jour en matière de faiblesses face aux intrusions et doit permettre de prendre connaissance des nouveaux outils et technologies disponibles (ex.: Reverse Proxy avec analyse du contenu).

Une configuration adéquate de certains de ces outils devrait également permettre à l'établissement de se protéger d'attaques internes.

En ce qui concerne la surveillance 24h/24h, nous référons à la partie «Sociétés externes pour la gestion ou la maintenance» p. 42.

Les établissements restent libres de présenter toute autre solution possible, à condition de pouvoir prouver qu'elle présente des caractéristiques de sécurité suffisantes.

17 La partie entre les deux firewalls est désignée par DMZ (Demilitarised Zone).
18 Intrusion Detection System
19 Voir aussi «Procédures en cas de détection d'une attaque», p. 45.
20 Voir aussi «Procédures relatives à la gestion et à la maintenance du site», p. 41.



B.2. Site relié au système bancaire / central

L'automatisation des traitements

La mise en place d'un traitement automatisé de bout à bout, désigné par «Straight-through processing (STP)», modifie les processus de traitement des opérations financières. Internet permet la désintermédiation, ce qui entraîne un transfert de la responsabilité de la saisie des données auprès du client.

Les applications informatiques d'un STP devraient inclure un substitut de l'expertise humaine qui existe au niveau de l'établissement et qui permet d'identifier des cas complexes d'erreurs dans la demande de clients. De plus, la mise en place d'un STP s'accompagne souvent d'une capacité accrue des volumes traités rendant impossible un contrôle exhaustif par l'homme. Il en résulte qu'une confiance accrue doit pouvoir être placée dans la qualité et l'intégrité des programmes informatiques, non seulement pour éviter des opérations de blanchiment d'argent[21], mais également pour éviter des fraudes basées sur un ajout de fonctions illicites (virus). Le STP accélère également le dénouement des opérations, tout particulièrement dans le domaine des valeurs mobilières, ce qui contribue à accentuer les difficultés dans le contrôle des risques.

Lors de la connexion d'une application Internet au système bancaire qui se fait le plus souvent directement à la base de données du système bancaire, l'établissement doit veiller à ce que des contrôles (applicatifs et / ou manuels) existants ne soient pas perdus sans qu'il existe des contrôles compensatoires. Il est donc important que l'établissement attribue une grande attention à la reprise des contrôles dans le nouveau système lors de la réalisation du projet et effectue des tests détaillés et intensifs avant la mise en production.

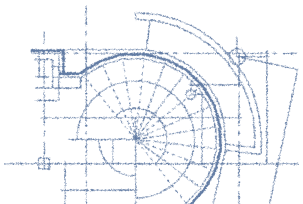
Le principe de la séparation des tâches ne peut plus être appliqué de la façon traditionnelle comme dans le cas de traitements manuels (saisie, validation, exécution) et doit être compensé par des contrôles de cohérence automatisés internes au système STP. Ceux-ci devraient être présents aussi bien lors de la saisie de l'opération par le client (contrôles d'input) que pendant le traitement de l'opération.

Le principe de la séparation des tâches et le principe des 4 yeux n'étant pas transposables tels quels à un système STP, l'établissement veillera à l'intégrité de la solution STP en appliquant ces principes lors de la mise en production et / ou du développement de cette solution.

L'automatisation des traitements, c'est-à-dire une saisie par le client suivie d'un traitement automatique nécessite un lien entre le site Internet et le système central de l'établissement.

Sur les 16 sites bancaires qui sont reliés au système central, 3 ne sont ni consultatifs ni transactionnels.

[21] L'établissement financier doit conserver une vigilance au delà de l'ouverture de compte, en s'assurant que les opérations financières restent compatibles avec le type d'opérateur économique. Ceci peut se traduire par une indication des opérations sortant du cadre habituel du client (par exemple, virement de montant bien supérieur à la normale ou de fréquence anormale).



B. Sécurité / Maintenance

Deux sites consultatifs et transactionnels et 8 sites purement consultatifs ne sont pas reliés au système central[22].

Uniquement 5 sites de PSF (tous consultatifs et transactionnels) ont une connexion avec le système central. Les autres (29) n'ont pas de liaison directe.

Aucun projet de site bancaire purement informatif ne prévoit une liaison avec le système central. Par contre 5 sites consultatifs et transactionnels et 3 sites consultatifs ne seront pas reliés au système central.

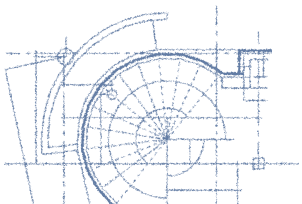
Au niveau des projets des PSF on constate un site purement informatif qui prévoit un lien avec le système central. 1 site consultatif et transactionnel et 3 sites consultatifs n'envisagent pas de créer une connexion avec le système central.

Lorsque l'établissement a recours à une solution STP, les traitements manuels et donc les contrôles possibles sont réduits. L'établissement doit donc veiller à prévoir des techniques permettant un audit de la solution STP.

Lors de la mise en place d'une solution STP, l'audit interne de l'établissement devrait être consulté pour donner son avis en matière d'organisation et de contrôle interne (point 5.4.4. de la circulaire IML 98/143) dans le but de garantir la disponibilité des informations nécessaires au contrôle interne (ex.: sondes logicielles[23]).

[22] Hormis les cas où les données sont mises à jour via un lien non permanent, on pourrait déduire un problème de compréhension de la question.

[23] Il s'agit de modules logiciels, propriétés de l'audit interne, qui sont intégrés à la chaîne STP sans interférer sur son fonctionnement, et qui permettent la corrélation de logs à différents niveaux de la chaîne. Un des objectifs de ces modules peut être la vérification de l'intégrité des traitements.



B.3. Aspects Internet inclus dans l'analyse des risques

La complexité d'Internet n'est pas uniquement technique. Certes, la connaissance technique facilite l'identification des risques, principalement ceux liés à la sécurité des systèmes, mais l'Internet modifie également les modèles économiques de par l'accessibilité mondiale et la rapidité de communication qu'il procure. La typologie de certains risques s'en trouve modifiée, comme les risques systémique et de réputation qui s'accroissent et certains risques opérationnels qui se transforment (par exemple, moins d'opérations et contrôles manuels mais plus de traitements automatisés).

Les enjeux pour la surveillance prudentielle s'articulent autour des deux axes, que sont l'identification des risques et leur maîtrise.

La classification des risques actuellement retenue par la CSSF dans le cadre du e-banking, est la suivante:

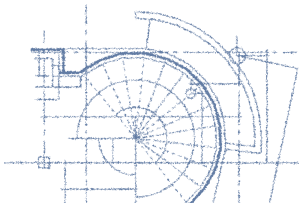
- Risques financiers
- Risques opérationnels
- Risques légaux
- Risques de développement
- Risques de réputation

L'enquête n'a pas recensé de site bancaire transactionnel où l'analyse des risques effectuée par l'établissement aurait ignoré les aspects spécifiques de l'Internet.

En revanche, 5 sites consultatifs ne prennent pas en compte les aspects Internet au niveau de l'analyse des risques.

Tous types de sites confondus, 40 sur 85 (47,06%) ont traité spécifiquement des aspects Internet. Si on enlève les sites informatifs, ce pourcentage s'élève à 80% (20 sur 25).

En ce qui concerne les PSF, 1 site consultatif et transactionnel, 1 site consultatif et 1 site transactionnel n'incluent pas Internet dans leur analyse des risques.

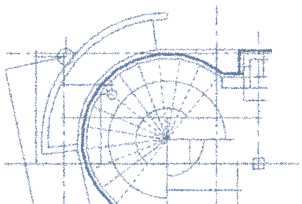


B. Sécurité / Maintenance

Les projets de création de sites, ainsi que les modifications significatives de sites existants, qui ne sont pas uniquement informatifs, sont à soumettre à la CSSF, qui les évalue sur les aspects suivants:

- La vision stratégique et la compréhension des enjeux, incluant la clientèle visée, les produits et services proposés, les volumes attendus et le seuil de rentabilité attendu,
- Le modèle fonctionnel décrivant également l'intégration des services Internet au sein de l'organisation et des applications informatiques existantes,
- L'architecture technique comprenant également les éléments physiques de protection du réseau (firewall et outils de détection d'intrusion)[24],
- Les aspects légaux, incluant les éventuels contrats de sous-traitance, les contrats ou conventions avec les clients et les clauses limitatives publiées sur le site (disclaimer clauses)[25],
- L'organisation et la séparation des tâches en relation avec l'activité par Internet, y compris l'organisation des tests d'acceptation et de mise en production des applications informatiques,
- Les procédures descriptives des tâches à réaliser dans le cadre de cette activité, conformément à la circulaire IML 96/126,
- L'audit interne[26] et externe[27], en tenant compte de l'étendue et de la périodicité des missions,
- La sous-traitance et le degré d'intervention des sociétés externes[28], y compris les mécanismes permettant d'assurer l'indépendance de l'établissement en cas de défaillance d'un ou plusieurs contractants,
- La sécurité du site, y compris la sécurité au sein des applications, les outils de cryptographie et d'authentification des clients (signature électronique), les mécanismes de preuve, les mécanismes de contrôle des intrusions et de modification de contenu du site,
- Les plans de continuité et de gestion de crise, y compris les délais de retour à la normale.

[24] Voir «Site relié au réseau interne (LAN)», p. 35.
[25] Voir «Pourcentage de clients ayant souscrit une convention Internet», p. 30.
[26] Voir «Internet inclus dans plan d'Audit», p. 46.
[27] Voir «Audit externe», p. 47.
[28] Voir «Sociétés externes pour la gestion ou la maintenance», p. 42.



B.4. Aspects de sécurité relatifs à Internet inclus dans la politique de sécurité

25 banques (24 sites purement informatifs et 1 consultatif) n'ont pas inclus les aspects de sécurité relatifs à Internet dans leur politique de sécurité.

De même pour les PSF, il s'agit d'un site transactionnel et de 10 sites informatifs.

Bien que pas encore précisément définis, la plupart des projets ont prévu d'inclure les aspects Internet dans la politique de sécurité. Il ne s'agit là pas uniquement des aspects de sécurité technique, mais aussi des aspects juridiques et opérationnels.

La CSSF insiste sur le fait que les risques de réputation liés aux sites informatifs sont importants bien que ceux-ci ne comportent en principe pas de nouveaux risques opérationnels. En effet, certaines altérations du message véhiculé ou du contenu du site à l'insu de l'établissement peuvent nuire gravement à l'image d'un établissement et même entraîner des conséquences juridiques. Ainsi, lors d'une attaque réussie, les «disclaimers» pourraient être modifiés ou supprimés. Des offres de produit ou des conditions peuvent être modifiées ou ajoutées; des messages incompatibles avec la politique d'affaires de l'établissement, voire en conflit avec la déontologie ou contraire à l'ordre public peuvent être ajoutés au contenu du site[29].

B.5. Procédures relatives à la gestion et à la maintenance du site

Dans le cas de 46 sites bancaires (54,11%) des procédures relatives à la gestion et la maintenance du site et de son infrastructure n'ont pas encore été rédigées. Abstraction faite des 60 sites informatifs, ce chiffre atteint toujours les 24%.

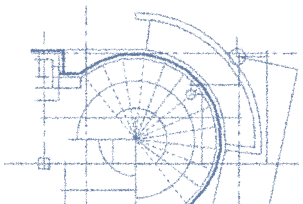
Au niveau des PSF, on constate que dans 22 cas (dont 18 sites informatifs) les procédures n'ont pas encore été rédigées.

La CSSF insiste sur l'importance des procédures qui doivent entre autres intégrer le principe des 4 yeux et le principe de la séparation des tâches.

Ces principes ne s'appliquent pas uniquement aux aspects transactionnels / comptables, mais également aux aspects concernant la configuration et l'exploitation des systèmes informatiques.

A titre d'exemple, il n'est pas souhaitable que la modification des règles de sécurité d'un «firewall» ou les paramètres des logs soient sous la responsabilité d'une seule personne.

[29] Les modifications illicites de clauses contractuelles peuvent être très sournoises. Ainsi, une phrase peut être ajoutée dans une couleur identique à celle du fond de l'écran, n'apparaissant ainsi qu'à l'impression en noir et blanc, mais pas à l'écran.



B.6. Sociétés externes pour la gestion ou la maintenance

La sous-traitance de développements et d'exploitations de plateformes Internet

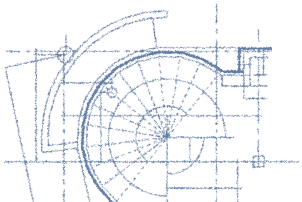
La technologie mise en œuvre par les établissements financiers pour fournir leurs services et produits par Internet est non seulement très spécifique et requiert un personnel aux qualifications particulières, mais elle nécessite également des investissements importants en ressources humaines et en matériel. De ce fait, les établissements financiers établis au Luxembourg ont eu recours dans leur quasi-totalité à des solutions développées, soit par des fournisseurs externes, soit par la maison-mère ou une entité du groupe. Cette sous-traitance des développements a pour principale conséquence positive de permettre aux établissements financiers d'être assez rapidement opérationnels avec des produits complexes et sécurisés, pour des coûts moindres que ceux d'un développement interne. En revanche, les risques «de développement» s'en trouvent accrus: une moindre maîtrise des applications et une dépendance vis-à-vis du fournisseur sont les désavantages les plus évidents.

L'acquisition de progiciels pour assurer une prestation de services financiers sur Internet n'est que la première étape dans la mutualisation des ressources. Une nouvelle tendance a vu le jour, qui consiste pour les établissements financiers à envisager une mutualisation des aspects opérationnels de l'Internet, c'est-à-dire la surveillance des éléments du réseau et des tentatives d'intrusions, ainsi que l'exploitation partagée par plusieurs établissements d'une architecture unique (matériels et logiciels). Ce besoin est également suggéré par certains fournisseurs, qui voient là une opportunité d'entrer dans une activité récurrente d'exploitation au lieu de rester cantonnés dans une position de fournisseur de logiciels et de services de maintenance. Les solutions de mutualisation qui sont envisagées ne sont pas simples à réaliser dans le contexte réglementaire actuel, en particulier parce qu'il est techniquement difficile de dissocier les aspects de sécurité (authentification du client, confidentialité des informations échangées) des aspects fonctionnels de prestation des services, de telle sorte que le sous-traitant puisse jouer un simple rôle d'agent technique sans visibilité sur les transactions des clients. La sous-traitance auprès d'un nombre restreint de prestataires, qu'elle soit au niveau des développements ou de l'exploitation, peut provoquer un risque en cas de défaillance d'un prestataire ou de ses applications. Une faille dans la sécurité ou une erreur dans l'exploitation a un impact direct sur l'ensemble des établissements faisant appel au sous-traitant. La sous-traitance en cascade est de plus en plus courante dans le domaine Internet, lorsque le sous-traitant principal se contente de coordonner d'autres prestataires très spécialisés (progiciel, hébergement, sécurité...), mais éventuellement moins au fait des contraintes des métiers financiers.

Plus de la moitié des sites bancaires, 52 sur 85 (61,18%), et 18 de 34 (52,94%) des sites de PSF ont recours à des sociétés externes pour la gestion ou la maintenance de leur site.

Les projets des banques montrent une baisse de cette tendance: 10 sur 32 (31,25%).

Il est intéressant de noter que le recours à l'outsourcing de la création du site (82,3%) est plus important que celui de la gestion du site (61,2%), ce qui s'explique probablement par la charge de travail requise, les compétences requises et les problèmes de la confidentialité qui se posent dans le cadre de la gestion des sites.



Concernant la sous-traitance du centre de traitement d'un site, la CSSF considère que la confidentialité doit être garantie entre l'établissement financier et ses clients. Toute encryption destinée à garantir la confidentialité doit être sous contrôle exclusif de l'établissement financier et du client. Des données consultatives ou transactionnelles ne doivent pas transiter de façon lisible sur un des systèmes informatiques accessibles à des tiers. Techniquement, les transactions du client, à destination du système central de l'établissement, transitent par le site Internet et la confidentialité est assurée habituellement par le mécanisme standard SSL ou TLS. Or, ce mécanisme SSL/TLS n'est prévu qu'entre le navigateur du client et le site Internet. Il devient dès lors techniquement difficile de prévoir une sous-traitance de la gestion du site Internet sans que les transactions ne soient accessibles par le tiers sous-traitant. Néanmoins, si tel était le cas et que la sous-traitance puisse se faire sur des données cryptées, le décryptage de SSL/TLS suivi d'une ré-encryption par un autre mécanisme doit être sous contrôle exclusif de l'établissement financier. Ne sont susceptibles de convenir que des solutions basées sur des crypto-box[30] ou des algorithmes de passage direct de SSL/TLS vers la nouvelle encryption.

Le recours à la sous-traitance de la surveillance du réseau résulte principalement de l'accessibilité 24h/24h par Internet. En effet, lorsque l'établissement est fermé, le site ou l'accès Internet est, en règle générale, encore actif. Ceci implique que les risques d'une attaque persistent 24h/24h et 7 jours sur 7.

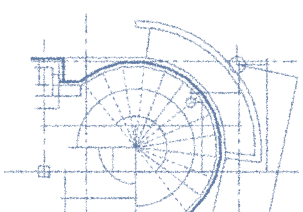
Le principe fondamental qui guide les recommandations de la CSSF en matière de sous-traitance de la surveillance, concerne l'impossibilité par le fournisseur d'avoir accès à des données confidentielles. Le deuxième principe est que l'établissement doit garder une maîtrise suffisante de son réseau.

La visibilité du fournisseur est donc limitée à des données techniques concernant l'infrastructure de l'établissement. Il ne peut pas avoir accès à des données concernant des transactions même anonymisées. N'appartenant pas au secteur financier, le tiers pourrait utiliser ces informations à des fins propres[31]. L'établissement veillera à ce que le fournisseur ait une connaissance réduite au strict minimum en ce qui concerne son infrastructure et ses règles de sécurité. L'établissement s'assurera que le fournisseur s'engage à restreindre l'accès à ces informations au personnel impliqué et identifié nominativement.

En vue de conserver la maîtrise de son infrastructure, l'établissement doit garder au minimum la gestion du firewall qui donne l'accès au réseau interne, mais la situation où le fournisseur intervient dans la gestion d'autres éléments du réseau peut être envisagée.

30 Un crypto-box est un équipement physiquement et logiquement protégé. Le terme anglais adéquat est «tamper proof crypto device». Aucune donnée intermédiaire, ni aucune clé de cryptage ne peut être extraite de l'équipement. Dès la tentative d'intrusion, même physique, l'équipement efface de manière irréversible les données avant de s'arrêter de fonctionner.

31 N'étant pas un établissement financier, le tiers n'est pas soumis au cadre légal régissant la profession. A titre d'exemple d'utilisation d'informations tierces à des fins propres, la vue d'un achat massif d'actions d'une entreprise peut laisser supposer une hausse rapide du cours et inciter le tiers à acheter ce titre, ce qui s'apparente à un délit d'initié.



En aucun cas, le fournisseur ne pourra modifier les règles du firewall donnant accès au réseau interne. Il serait envisageable qu'en cas d'une attaque le fournisseur puisse fermer le site. En cas de détection d'une attaque, le fournisseur pourra éventuellement ajouter une règle restrictive au niveau du firewall (autre que celui qui donne accès au réseau interne) nécessaire au blocage de l'attaquant.

Au cas où le fournisseur serait amené à réaliser des modifications de configuration / règles sur un des éléments du réseau, au moins un log permettant de retracer les détails de ces modifications devra être mis à disposition de l'établissement. L'établissement doit être en mesure de comprendre les effets de ces modifications. Il y a lieu de prendre en compte les conditions de la circulaire IML 96/126 (point 4.5.2.1).

B.7. Solution de secours

Seulement 34 (40%) des sites bancaires et 14 (41,18%) des sites de PSF disposent d'une solution de secours au cas où des éléments du site ne seraient plus opérationnels.

Au niveau des sites bancaires on recense 2 sites consultatifs et transactionnels et 6 sites consultatifs qui n'ont pas encore défini une solution de secours.

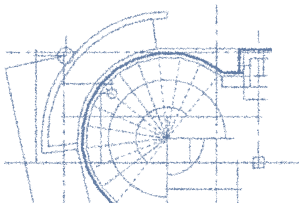
En ce qui concerne les PSF, il s'agit de 2 sites consultatifs et transactionnels, d'un site transactionnel et d'un site consultatif.

Au niveau des banques les projets montrent une évolution vers le haut (18 sites – 52,94%) tandis que les projets des PSF tendent vers le bas (4 sites – 28,57%).

Les établissements doivent se rendre à l'évidence que la période de la crise n'est pas le moment opportun pour établir des procédures de secours.

Internet doit être pris en compte dans le plan de continuité de l'établissement. En fonction de l'appréciation de l'importance que représente cette activité pour l'établissement, une indisponibilité à court terme dégage des risques de réputation tandis qu'une indisponibilité à long terme peut engager des risques financiers (et plus particulièrement pour les sites B2B).

La dépendance vis-à-vis de prestataires tiers est également à prendre en compte pour les solutions de secours. A titre d'exemple, un site peut être indisponible à cause d'une défaillance d'un ISP (Internet Service Provider) unique (non-redondant).



B.8. Procédures en cas d'indisponibilité

26 sites bancaires et 11 sites PSF sont dotés de procédures au cas où le site serait en partie ou entièrement indisponible. Ceci équivaut à 30,56% et 32,35% respectivement.

Au niveau des sites bancaires, 5 sites consultatifs et transactionnels et 4 sites consultatifs n'ont pas encore défini des procédures en cas d'indisponibilité.

En ce qui concerne les PSF, il s'agit de 2 sites consultatifs et transactionnels, d'un site transactionnel et d'un site consultatif.

Pour les sites purement informatifs, la CSSF recommande de prévoir au moins une procédure relative à la communication aux clients de l'indisponibilité du site (risque de réputation).

En ce qui concerne les sites consultatifs et transactionnels, l'établissement doit définir les procédures de déclenchement du plan de secours (voir ci-dessus).

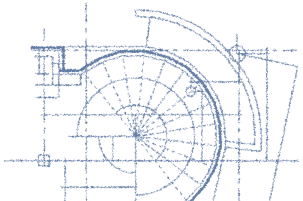
B.9. Procédures en cas de détection d'une attaque

42 sites bancaires et 14 sites PSF sont dotés de procédures en cas de détection d'une attaque. Ceci équivaut à 49,41% et 41,18% respectivement.

Au niveau des sites bancaires des procédures en cas de détection d'une attaque ont été mises en place dans le cadre de tous les sites transactionnels. Par contre, on recense 3 sites consultatifs où les procédures n'ont pas encore été rédigées ou sont en cours de rédaction.

En ce qui concerne les PSF, il s'agit de 3 sites consultatifs et transactionnels et d'un site consultatif.

La CSSF rappelle l'importance d'une procédure de déclenchement du plan de secours et d'une procédure qui définit comment revenir à l'état normal de production après la désactivation du site à cause de la détection d'une tentative d'attaque ou après la restauration du site après une attaque réussie. Cette procédure doit également permettre d'analyser des éléments faibles qui ont permis l'attaque afin de donner des indications utiles permettant d'améliorer la sécurité.



B.10. Internet inclus dans le plan d'audit

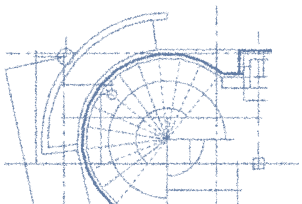
45 sites bancaires et 21 sites PSF incluent les aspects Internet dans leur plan d'audit interne. Ceci représente 52,94% pour les banques et 61,67% pour les PSF.

Parmi les banques qui n'incluent pas les aspects Internet dans le plan d'audit interne, on trouve 2 sites consultatifs mais pas de site transactionnel. Pour les PSF, il s'agit d'un site consultatif et de 2 sites transactionnels.

Au moins dans le cas où l'établissement exploite un site consultatif et / ou transactionnel, les aspects Internet doivent être régulièrement repris dans les plans d'audit interne.

La CSSF recommande aux établissements de s'assurer que les auditeurs internes possèdent les connaissances nécessaires et une maîtrise suffisante pour exercer ces contrôles spécifiques (point 5.4.5. de la circulaire IML 98/143).

Lorsque le service d'audit interne ne dispose pas d'une compétence suffisante pour procéder à cet audit, il peut recourir aux services d'un expert externe. Ce recours à des tiers professionnels doit respecter les principes énoncés dans le point 5.4.9. g) de la circulaire IML 98/143. Rappelons la condition d'indépendance de l'expert par rapport au réviseur d'entreprise de l'établissement et le fait que ces missions d'audit interne menées par des experts externes ne peuvent pas être confondues avec des missions de conseil qui ont été exercées lors de l'élaboration ou de l'implémentation du projet Internet.



B.11. Audit externe

36 sites bancaires et 7 sites PSF ont subi un audit externe par une société spécialisée dans ce domaine. En ce qui concerne les sites bancaires où l'audit externe n'a pas encore été réalisé, un seul est transactionnel. Sur les 27 sites de PSF qui n'ont pas été audités par une société externe, 5 sites sont transactionnels.

Lorsque le site est connecté au réseau interne de l'établissement, ce qui est normalement le cas pour les sites consultatifs ou transactionnels, un audit technique externe avant la mise en production du site est indispensable.

L'audit en question doit couvrir les aspects de sécurité technique (validation de l'infrastructure, test de pénétration, ...) ainsi que l'organisation et les procédures liées à la gestion du site (principe des 4 yeux, principe de séparation des tâches, ...).

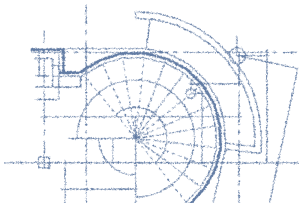
L'audit doit être réalisé par une société possédant des connaissances spécialisées dans le domaine. Cette société ne doit en aucun cas avoir participé au développement du site et doit avoir les outils et les connaissances nécessaires pour réaliser cette mission. Pour des raisons d'indépendance, le réviseur externe de l'établissement ne devrait pas effectuer cet audit.

A la fin de l'exercice au cours duquel le site a été mis en production, le réviseur externe doit se prononcer, dans son rapport analytique annuel, sur les aspects Internet (point 3.4.4. de la circulaire CSSF 01/27 relative aux règles pratiques concernant la mission des réviseurs d'entreprises).

B.12. Application de l'audit externe aux aspects de sécurité technique

Sur les 36 audits externes relatifs à des sites bancaires, 31 ont couvert les aspects de sécurité technique. Ceux qui ne les ont pas pris en compte se réfèrent à 3 sites consultatifs et transactionnels et 2 sites informatifs.

Tous les audits externes réalisés sur des sites de PSF couvrent les aspects de sécurité technique.



B.13. Application de l'audit externe aux aspects procéduraux et organisationnels

Sur les 36 audits externes relatifs à des sites bancaires, 14 ont couvert les aspects concernant les procédures / organisation relatifs au site. Ceux qui ne les ont pas pris en compte se réfèrent à 6 sites consultatifs et transactionnels et 4 sites consultatifs et 12 sites informatifs.

Sur les 7 audits externes relatifs à des sites de PSF, 5 ont couvert les aspects concernant les procédures / organisation relatifs au site. Ceux qui ne les ont pas pris en compte se réfèrent à 2 sites consultatifs et transactionnels.

B.14. Eléments hors du Luxembourg

En ce qui concerne les éléments (ex.: serveur, base de données, ...) constituant le site, 23 sites bancaires (27,06%) et 10 sites de PSF (29,41%) disposent d'éléments qui ne sont pas situés au Luxembourg.

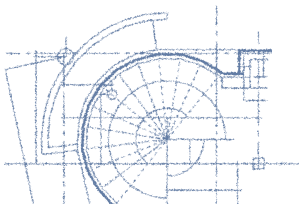
En général il s'agit de serveurs Web informatifs, hébergés auprès d'un fournisseur externe ou d'une autre société du groupe.

Les tendances semblent à la baisse vu que 6 (18,75%) projets bancaires et un seul projet PSF envisagent des éléments hors du Luxembourg.

Un site informatif peut être hébergé à l'étranger. A partir du moment où un matériel informatique sur lequel transitent des données confidentielles est situé en dehors du Luxembourg, les données doivent être encryptées et le processus de décryptage doit uniquement être opéré par l'établissement qui est responsable de ces données.

A cet égard, rappelons que des données sur des transactions (même anonymisées) sont aussi à considérer comme des données confidentielles.

Le principe proposé est que les données confidentielles doivent être encryptées depuis l'établissement jusqu'au client, sans possibilité pour des tiers de les accéder sous forme lisible. Aucun transcodage, c'est-à-dire décryption et réencryption selon un autre standard, ne peut avoir lieu hors de l'établissement luxembourgeois, car il comporterait une possibilité d'intrusion durant le transcodage, à la fois en visualisation des données et de la transaction.



C. Authentification du client / Données confidentielles[32]

L'authentification permet de garantir l'identification. En s'identifiant, l'utilisateur indique que c'est lui, en s'authentifiant, il prouve que c'est lui.

L'authentification se base en général sur une ou plusieurs des caractéristiques suivantes:

- Quelque chose qu'on connaît (ex.: mot de passe, numéro d'identification)
- Quelque chose qu'on possède (ex.: smart card[33], code carte[34])
- Quelque chose qu'on est (ex.: biométrique (rétine, empreinte digitale))

Séparément, tous ces éléments ont des défauts. Quelque chose qu'on connaît peut être deviné. Quelque chose qu'on possède peut être volé. La meilleure protection peut être fournie par une authentification sur base de caractéristiques propres à la personne, mais ce type d'authentification est le plus onéreux et le plus lourd à implémenter.

La signature électronique

La directive 1993/93/CE a été transposée en droit luxembourgeois dans le cadre de la loi du 14 août 2000 portant sur les services de la société de l'information. Cette loi reprend les principes énoncés, à savoir le principe de reconnaissance de la signature électronique comme identification d'une personne physique, le principe de signature avancée et de certificat qualifié, ainsi que le principe d'accréditation libre des autorités de certification[35].

Un nombre croissant d'établissements financiers utilisent la signature électronique comme mécanisme de preuve lors des transactions passées par Internet. La CSSF encourage les établissements financiers à utiliser la signature électronique à condition que l'attribution des éléments cryptographiques (les clés électroniques) et des certificats soit effectuée de manière professionnelle et sécurisée. Les établissements financiers qui utilisent la signature électronique (PKI) sont actuellement leur propre autorité de certification. La CSSF devra cependant analyser les conséquences qu'aurait l'usage de certificats émis par une autorité de certification tierce pour compte des clients d'un établissement financier.

La CSSF est en faveur de l'utilisation de solutions d'authentification basées sur des mécanismes de PKI (Public Key Infrastructure). Au cas où l'établissement serait sa propre autorité de certification, la CSSF recommande l'émission de certificats qualifiés (aux termes de la loi du 14 août 2000) afin de garantir une valeur juridique à la signature électronique avancée. En effet, en cas de litige sur la signature, l'usage d'un certificat non qualifié implique que l'établissement doit démontrer que celui-ci pourrait être assimilé à un certificat qualifié.

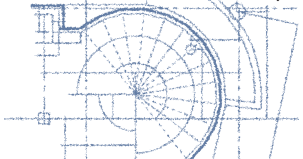
Les solutions d'authentification non PKI, n'utilisant pas la notion de clé publique / clé privée, peuvent être acceptées et sont analysées au cas par cas par la Commission.

32 Cette section traite de certains aspects pratiques. Elle ne doit pas être comprise comme une analyse exhaustive des aspects juridiques.

33 Il s'agit d'une carte, souvent au format d'une carte de crédit, équipée d'une puce électronique qui permet de stocker des informations comme, par exemple, une clé privée. Un lecteur de carte est nécessaire pour lire les informations. En règle générale, l'extraction des informations de la carte exige l'introduction d'un PIN (Personal Identifier Number).

34 Il s'agit d'une carte, souvent au format d'une carte de crédit, sur laquelle est indiqué un code de sécurité (en règle générale au moins 16 positions). Celle-ci est considérée comme élément physique (quelque chose qu'on possède) étant donné qu'il est difficile de retenir la composition du code de sécurité.

35 L'autorité de certification a pour rôle d'émettre des certificats électroniques en garantissant l'attribution de chaque certificat à un signataire donné.



C. Authentification du client / Données confidentielles

C.1. Identifiant basé sur le nom du client

Par identifiant on entend un élément unique (normalement une chaîne de caractères) qui est associé à un seul client. Les systèmes e-banking utilisent l'identifiant en tant que référence pour un client spécifique. L'identifiant peut être le nom du client, son numéro de compte ou tout autre chaîne de caractères unique.

Un seul site bancaire et 4 sites PSF utilisent le nom du client en tant qu'identifiant. Les autres sites utilisent le numéro de compte, un numéro de convention ou un nickname (alias).

Aucun des projets, ni au niveau des banques, ni au niveau des PSF, envisage d'utiliser le nom du client en tant qu'élément d'identification.

Dans le but de garantir la confidentialité des informations passant entre le client et l'établissement, la CSSF recommande de n'utiliser ni le nom du client, ni le numéro de compte en tant qu'identifiant. En effet, même en cas d'utilisation des services Internet à partir d'un endroit public (cybercafé), si des informations seraient extraites du PC utilisé, l'identité de l'utilisateur ne serait ainsi pas divulguée.

C.2. Authentification basée sur un mot de passe

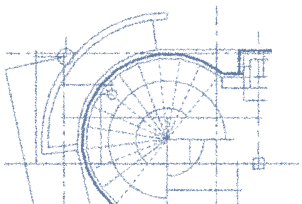
22 des sites bancaires utilisent au moins un mot de passe pour l'authentification de l'utilisateur. Parmi les 22 sites il y a 2 sites purement informatifs. Parmi les 63 sites bancaires qui n'utilisent pas de mot de passe 2 sont consultatifs et transactionnels et 3 sont consultatifs.

Parmi les 10 sites de PSF qui utilisent un mot de passe il n'y a pas de site purement informatif. Par contre il y a 1 site consultatif et transactionnel et 1 site consultatif qui n'utilise pas de mot de passe pour l'authentification des utilisateurs.

A titre d'exemple, les recommandations que la CSSF considère comme devant être généralement suivies au niveau des caractéristiques essentielles des mots de passe, sont les suivantes:

- Longueur minimale de 8 caractères
- Au minimum un caractère numérique et un caractère alphabétique
- De préférence un caractère de type «spécial»
- Changement régulier du mot de passe et historique des derniers mots de passe utilisés

Au cas où le client a un doute sur la confidentialité de son mot de passe (ses éléments d'identification), il doit avoir la possibilité de désactiver l'accès Internet (soit en téléphonant à l'établissement, soit via le site lui-même).



C.3. Elément physique d'authentification

En tant qu'élément physique il faut entendre par exemple, une carte à puce (smartcard), un digipass (calculette), une code-card ou l'appareil biométrique.

18 sites bancaires ont indiqué qu'ils utilisent un élément physique qui permet d'authentifier le client. Les 18 sites comprennent un seul site qui est purement informatif.

Au niveau des PSF, il y a 4 sites consultatifs et transactionnels qui ont recours à un élément physique pour l'authentification. Par contre 5 sites consultatifs et transactionnels, 1 consultatif et 2 transactionnels n'utilisent pas d'élément physique pour l'authentification.

Il est à noter que parmi les banques, 8 sites sont plus qu'informatifs, mais ils n'ont pas encore prévu l'utilisation d'une authentification forte.

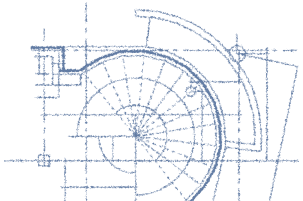
Aucun des projets relatifs au PSF ne prévoit l'utilisation d'un élément physique.

Etant donné que les trois formes d'authentification peuvent être contournées si elles sont utilisées séparément, la CSSF recommande l'utilisation d'une combinaison d'au moins deux de ces caractéristiques. Par exemple, l'utilisateur s'identifie avec son numéro d'identification et s'authentifie à travers son mot de passe (quelque chose qu'il connaît) et à travers la saisie de 2 caractères aléatoires de sa carte de sécurité (quelque chose qu'il possède) qui contient les 16 caractères du code carte.

Cet élément physique peut jouer un rôle important en cas de litige concernant une transaction, lors de l'analyse du mécanisme de preuve, puisqu'il pourrait confirmer la négligence du client qui divulgue à la fois l'information qu'il connaît et celle qu'il possède.

C.4. Elément persistant sur le poste client

Pour 9 sites bancaires et 4 sites PSF, il existe un élément d'authentification qui persiste sur le poste du client. On citera pour exemple, une clé qui serait stockée sur le disque dur du poste utilisateur.



C.5. Agrégation

Les «agrégateurs»

Il s'agit de sociétés opérant des sites Internet dont le principal service consiste à agréger des données de clients auprès de différents établissements présents sur le web. Typiquement, un agrégateur consolide à la demande de son client les données de son compte en banque, de ses portefeuilles de valeurs mobilières, de ses «mileages» accumulés auprès de compagnies aériennes, de ses semaines de multi-propriété («timeshare»), etc., de manière à lui présenter une synthèse de ses avoirs.

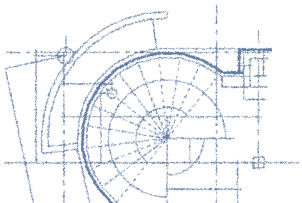
Les agrégateurs ont vu le jour aux Etats-Unis et commencent à proposer leurs services en Europe[36]. Ces sociétés ne sont que rarement des professionnels du secteur financier, bien que la majorité des informations qu'elles collectent soient de type bancaire. Les établissements financiers luxembourgeois seront probablement confrontés au phénomène d'agrégation et à ses conséquences: perte de contact avec le client, agrégation non connue car le client ne communique pas obligatoirement à la banque le fait qu'il utilise de tels services. Aux Etats-Unis, les agrégateurs sont déjà en cours de mutation, car du fait qu'ils possèdent davantage d'informations que les banques sur leurs clients, ils sont en mesure de proposer des informations synthétiques sur le positionnement de chaque établissement financier agrégé: comportement du client par rapport au type d'avoirs, pourcentage des actifs gérés auprès de chaque banque, etc. Ces nouveaux services sont le plus souvent négociés avec les établissements financiers en faisant intervenir une collaboration sous la forme de «data feed» des avoirs des clients agrégés: l'information n'est plus agrégée sous forme «sauvage», mais elle est obtenue auprès de l'établissement financier qui met à disposition les données sous une forme prédéfinie à la manière des fournisseurs d'informations financières qui proposent les cours boursiers. L'étape ultime de la mutation des agrégateurs est atteinte lorsque ceux-ci fournissent le logiciel d'agrégation aux établissements financiers qui deviennent eux-mêmes agrégateurs.

L'impact des agrégateurs pour le secteur financier luxembourgeois est encore mal connu, mais les conséquences au niveau prudentiel sont importantes, particulièrement si l'agrégation est faite de manière sauvage. Les établissements financiers peuvent subir une perte de réputation issue d'une agrégation de mauvaise qualité. Les agrégateurs qui ne bénéficient pas d'une compétence bancaire peuvent également être moins sensibles à la confidentialité des données.

Le problème des sociétés qui ont pour but d'agréger des données du client, financières et autres, ne s'est pas encore présenté dans un cas concret au Luxembourg.

2 sites bancaires et 2 sites de PSF ont indiqué qu'ils autorisent le client à communiquer ses éléments d'identification à un tiers.

[36] Exemples d'agrégateurs aux Etats-Unis: Corillian, eBalance et Yodlee
La Citibank avait lancé Myciti.com et J.P.Morgan avait créé chase.com (tous les deux utilisent le software de Yodlee). En Allemagne la Deutsche Bank avait créé Moneyshelf.



C. Authentification du client / Données confidentielles

L'interprétation de cette autorisation est difficile à faire sous un angle juridique; il se peut que des établissements se croient protégés par une clause dans la convention signée par le client.

En ce qui concerne les projets aucun établissement de crédit et aucun PSF ne prévoit l'autorisation du client à communiquer les éléments d'identification à un tiers.

Les risques propres à l'agrégation sont liés entre autres à la responsabilité de l'utilisation de données confidentielles et au flou juridique. En effet, la responsabilité en cas de données erronées ou de problèmes techniques devrait être clarifiée. Bien qu'un contrat entre l'agrégateur et le client de l'établissement agrégé puisse exister, il faut noter que les agrégateurs ne tombent, en règle générale, pas sous la surveillance d'une autorité publique.

La CSSF recommande aux établissements visés d'inclure cette problématique dans les contrats (conventions générales) avec leurs clients, particulièrement si l'agrégation est «sauvage[37]» et donc inconnue de l'établissement. En effet, le client qui confie ses éléments d'identification à l'agrégateur, lui donne implicitement la possibilité technique de réaliser des transactions en son nom.

En cas d'agrégation négociée entre l'établissement et l'agrégateur[38], l'établissement doit être en mesure de distinguer entre l'utilisation de son site par le client ou par l'agrégateur et veillera à définir précisément les droits et responsabilités de chacun[39].

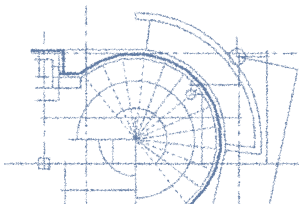
Bien qu'un système d'agrégation puisse être protégé de la même manière qu'un site transactionnel, celui-ci, par sa nature, est une cible préférée pour les attaques. En cas d'attaque réussie, le «hacker» dispose des éléments d'identification de plusieurs comptes par client. Les possibilités de fraudes seraient donc importantes et la question de la responsabilité se poserait alors.

Notons pourtant qu'au Luxembourg, l'agrégation sauvage (screen scraping) est rendue difficile, étant donné que les établissements utilisent majoritairement des systèmes d'authentification qui ne sont pas limités à un simple mot de passe.

37 L'agrégation «sauvage» fait souvent appel à la technique du «screen scraping» qui consiste pour l'agrégateur à capter l'information du client sur base de la position sur l'écran. En cas de modification du layout par l'établissement, il existe un risque important pour l'agrégateur de collecter des données erronées.

38 L'agrégation se fait dans ce cas le plus souvent au moyen d'une communication standardisée différente du service Internet offert au client (data feed).

39 A titre d'exemple, l'agrégateur ne sera pas autorisé à passer des ordres au nom du client.



C.6. Technologies utilisées

Le tableau suivant reprend le nombre d'établissements qui ont indiqué l'utilisation de différentes techniques pour leur site Internet:

	Applet Java	Javascript	ActiveX	Html (sans autre composante)	Autres
Banques	21	18	3	9	7
PSF	8	6	1	2	5

Figure 12: Différentes technologies utilisées

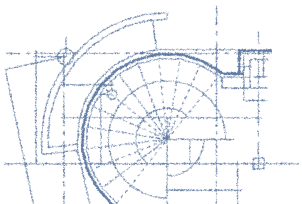
En ce qui concerne les projets, tant pour les banques que pour les PSF, les technologies prévues ne sont pas encore clairement définies.

Les technologies utilisées influencent largement la nécessité de versions actuelles des browsers chez les clients. En effet en fonction des technologies utilisées par l'établissement, le client est obligé d'avoir une certaine version du browser qui peut comporter de nouvelles faiblesses au niveau de la sécurité.

Il faut donc trouver un équilibre entre l'utilisation de nouvelles technologies et l'obligation des utilisateurs d'actualiser les softwares utilisés.

L'utilisation de certaines technologies n'est pas sans risque, particulièrement si le client n'a pas connaissance des risques qu'il court. Diverses technologies permettent d'accéder à toutes les ressources du PC du client et représentent donc un point d'entrée idéal pour l'installation de virus. L'utilisateur doit, soit paramétrer finement son navigateur pour limiter les fonctionnalités de ces technologies, soit apprécier la confiance qu'il accorde aux sites web qu'il accède. Un utilisateur peu averti pourra être enclin à accepter toutes les fonctionnalités de ces technologies afin de pouvoir communiquer avec son établissement financier, s'exposant ainsi sans le savoir à l'importation de virus issus de sites douteux visités antérieurement. Il n'est pas exclu que de futurs virus aient pour fonction de s'approprier les identifiants des clients d'établissements financiers ciblés.

Il appartient donc aux établissements de mesurer l'impact au niveau du client des technologies utilisées et, le cas échéant, de l'informer sur les risques qu'il encourt et comment se protéger.



C.7. Critères de choix de la technologie

En général c'est le choix de la solution qui impose la technologie utilisée. En d'autres termes, le fournisseur, choisi par l'établissement, impose sa technologie.

C.8. Utilisation de SSL[40]

La technologie SSL permet d'encrypter le canal établi entre le client et l'établissement. Cette solution est actuellement la plus utilisée pour garantir la confidentialité des données échangées.

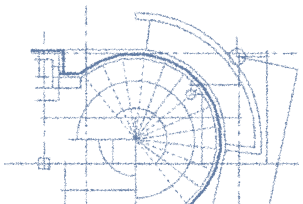
27 sites bancaires et 9 sites PSF utilisent une connexion SSL entre le client et le site. Ceci inclut 5 sites bancaires purement informatifs. Aucun site PSF purement informatif n'utilise SSL.

43,75% des projets bancaires (14 sur 32) et 16,67% des sites PSF (2 sur 12) prévoient une connexion SSL.

Plusieurs niveaux d'encryption existent en ce qui concerne une connexion SSL. Actuellement l'encryption 128 bits est la plus répandue.

La CSSF décourage fortement l'utilisation d'une encryption inférieure à 128 bits (notamment 40 bits), bien que celle-ci exige déjà que le client utilise une version actuelle du browser.

[40] Secured Socket Layer



C.9. Utilisation d'autres méthodes d'encryption

En dehors d'une encryption SSL, le canal établi entre l'établissement et le client peut être encrypté par d'autres mécanismes. Il y a des solutions où le client, dans le but d'utiliser les services offerts par l'établissement, télécharge une Applet Java sur son ordinateur. Celle-ci peut réaliser l'encryption des données entre le client et l'établissement. Cette encryption peut être unique ou en plus d'une encryption SSL.

A la question «Est-ce que votre site utilise d'autres méthodes d'encryption (autres que SSL) ?» 12 banques et 6 PSF ont répondu par l'affirmative.

Quelques exemples de méthodes d'encryption sont: 3DES, IDEA.

Tandis que 3 projets bancaires envisagent l'utilisation d'une encryption en plus de SSL, aucun projet PSF ne mentionne ceci.

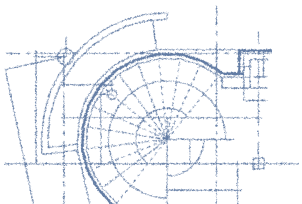
C.10. Version minimale du navigateur

30 sites bancaires et 10 sites PSF imposent une version minimale à l'utilisateur.

La raison principale pour qu'un établissement impose une version minimale est pour garantir la compatibilité au niveau des éléments de sécurité comme par exemple SSL (128bits), certificats électroniques, Java, ...

Bien que cette problématique ne soit pas encore toujours clairement définie au niveau des projets, on peut estimer qu'il s'agit des mêmes proportions.

Il s'agit de trouver un équilibre entre l'usage de nouvelles technologies disponibles et l'obligation pour les clients d'actualiser leur software, qui, en raison de leur complexité croissante, peuvent contenir de nouvelles failles. Voir aussi «Technologies utilisées», p. 54.

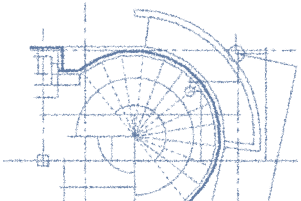


D. Remarques Finales

Le recensement a permis de mettre en évidence, d'une part la manière dont les établissements financiers ont abordé la mise en œuvre de sites sur Internet et, d'autre part, les faiblesses qui restent à combler pour permettre une réduction des risques liés à ce canal de distribution.

Malgré la mise en place d'une protection efficace par la majorité des établissements financiers présents sur Internet, il persiste un risque qui réside auprès du client et qui découle d'un manque de formation sur les dangers d'Internet. Un internaute qui ne protège pas son équipement informatique (son PC) des attaques externes par des mécanismes analogues à ceux mis en place par les établissements financiers (firewall personnel et anti-virus), s'expose à voir un jour ses informations d'identification appropriées par l'attaquant qui pourra ainsi réaliser des opérations bancaires en son nom. Ce type d'attaque n'a jusqu'à aujourd'hui eu lieu qu'à titre de démonstration de faisabilité, mais il reste à redouter l'apparition de certains virus spécialisés dans la collecte d'informations bancaires d'identification.

L'utilisation de la signature électronique avancée basée sur des certificats qualifiés au sens de la Directive européenne 1999/93/CE du Parlement européen et du Conseil et au sens de la loi du 14 août 2000, n'apportera une protection supplémentaire que dans le cas d'utilisation par l'internaute d'un périphérique sécurisé et intègre (lecteur de carte, par exemple) chargé du stockage des informations d'identification (clé privée) et de la cryptographie menant à la signature. Cette intégrité doit être poursuivie jusqu'à l'introduction de «l'élément qu'on connaît», c'est-à-dire le code confidentiel, au moyen d'un clavier inviolable et une visualisation des éléments principaux signés (le montant et le numéro de compte, par exemple), à l'aide d'un affichage également intègre.



D. Remarques Finales

D.1. Remarques spécifiques aux OPC

Pour toutes les entités sous la surveillance de la CSSF, qui font référence à des OPC sur leur site, la CSSF rappelle qu'il faut:

- enregistrer les OPC, pour lesquels elles assument la fonction d'administration centrale, auprès des autorités compétentes où les parts sont commercialisées,
- s'assurer que les OPC, pour lesquels elles n'assument pas la fonction d'administration centrale, soient enregistrés auprès des autorités compétentes des pays où les parts sont commercialisées.

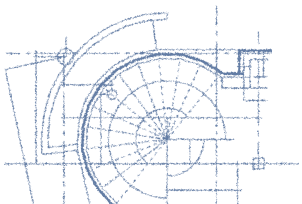
Il est rappelé dans ce contexte que même pour les OPCVM communautaires, une notification de la commercialisation de l'OPCVM auprès des autorités compétentes du ou des pays de l'U.E. où la commercialisation a lieu, est obligatoire.

Au cas où le promoteur opère un site Internet sous la dénomination de l'OPC (ou de la société de gestion) concerné, l'administration centrale devra s'assurer que les recommandations en matière d'Internet soient appliquées par l'opérateur du site.

En matière de lutte contre le blanchiment d'argent les dispositions de la circulaire IML 91/75 du 21 janvier 1991 relative aux organismes de placement collectif sont également applicables aux demandes de souscription reçues via le canal Internet.

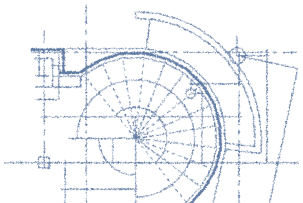
En ce qui concerne les sites de tiers qui publient des informations sur les OPC il est évident qu'il est quasiment impossible pour l'administration centrale de vérifier à priori ces données. Ceci ne doit cependant pas empêcher l'administration centrale de réagir de façon appropriée si elle obtient connaissance du fait que des données erronées sont publiées. Pour les informations publiées sur des sites de tiers qui permettent de souscrire et de faire racheter les parts d'un OPC, l'administration centrale devra s'assurer, dans la mesure du possible, que les données publiées sont correctes[41]. Le fait de pouvoir passer des ordres de souscription / rachat présuppose, en effet, qu'un lien entre l'administration centrale et l'opérateur du site tiers existe. Il va de soi que l'OPC concerné doit être enregistré auprès des autorités compétentes.

[41] Voir aussi «Présence sur d'autres pages», p. 13.



E. Annexe

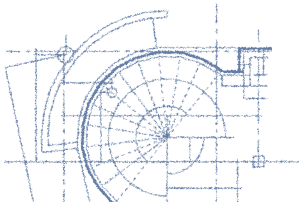
Questionnaire utilisé pour le recensement Internet



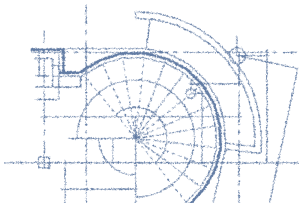
A) Site Internet / Stratégie Internet

	OUI / NON	Commentaire / Détails[1]
1. Est-ce que votre établissement dispose d'un site Internet?	❑ / ❑	Date de mise en production et adresse(s) du site …. / …. / …….. www. www. www.
2. Si votre établissement ne dispose pas encore de site, est-ce que la création d'un site est prévue[2]?	❑ / ❑	Date de mise en production prévue et adresse(s) du site …. / …. / …….. www. www. www.
3. Si votre établissement dispose d'un site, est-ce qu'une modification de la nature (informatif, consultatif, transactionnel) du site est prévue?	❑ / ❑	Type de modification et date de mise en production prévue …. / …. / ……..
4. Est-ce que votre établissement est présenté sur d'autres pages Web au niveau de sites appartenant ou non au même groupe? Si oui, veuillez indiquer les adresses.	❑ / ❑	www. www. www. www.
5. Est-ce que le site comprend des pages statiques (*site informatif*)[3] ? Si oui, avec quel contenu?	❑ / ❑	Ex.: Présentation de l'établissement, des produits
6. Est-ce que le site permet la consultation de données personnalisées du client *(site consultatif)*? Si oui, lesquelles?	❑ / ❑	Ex.: Consultation des soldes des comptes, des portefeuilles
7. Est-ce que le site permet de passer des transactions financières *(site transactionnel)*? Si oui, lesquelles?	❑ / ❑	Ex.: Virements, Ordres de bourse

1 Au cas où la réponse nécessiterait une annexe, veuillez la référencer dans la case correspondante.
2 Est considéré comme projet tout site où la mise en production est prévue avant le 31 décembre 2001.
3 A partir du point 5 du présent questionnaire, l'établissement fait référence au site existant (point 1) ou au projet de site (point 2). Au cas où votre établissement a répondu négativement aux points 1 et 2, la suite du questionnaire n'est pas à remplir.



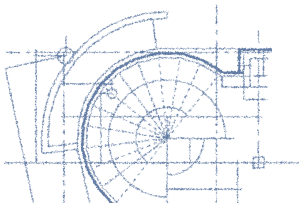
8. Y-a-t-il des limites pour les transactions financières? Si oui, lesquelles et comment sont-elles définies?	❑ / ❑	Ex.: Limite sur les volumes, Vérification du disponible
9. Est-ce que l'approche Internet de votre établissement est plutôt défensive (canal de distribution supplémentaire, et non prioritaire) ou offensive (banque virtuelle / canal de distribution majeur / enjeu principal)?	❑ / ❑	
10. Est-ce que le site de votre établissement vise une clientèle spécifique? Si oui, laquelle?	❑ / ❑	Ex.: Clients existants, Clients fortunés hors UE
11. Etes-vous en mesure d'évaluer le nombre de nouveaux clients obtenus grâce au site? Si oui, quelle est leur proportion approximative dans la base globale de clients?	❑ / ❑	%
12. Est-ce que votre établissement permet l'ouverture de compte via Internet (sans présence physique)? Si oui, à quelles conditions?	❑ / ❑	Ex.: Document d'identification certifié, Premier virement en provenance d'un compte nominatif
13. Est-ce que votre établissement a eu recours à des sociétés externes pour la création du site? Si oui, lesquelles et pour quels domaines?	❑ / ❑	
14. Quel est le budget (en €) dédié au projet de création de site hors dépenses d'exploitation (matériel, logiciel et ressources humaines)?		Site existant: chiffre réel, Projet: estimation €
15. Quel est le budget annuel (en €) dédié à l'exploitation et la maintenance du site (sécurité inclus)?		Site existant: chiffre réel, Projet: estimation €
16. Quel est le pourcentage du budget annuel informatique alloué à l'investissement du site?		Indiquer les deux années précédant la date de mise en production



Questionnaire utilisé pour le recensement Internet

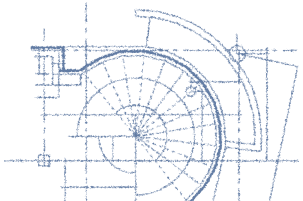
17. Quel est le pourcentage du budget annuel informatique alloué à l'exploitation pour le site?		Indiquer les deux années après la date de mise en production
18. Avez-vous estimé un délai de rentabilité du site? Si oui, sur base de quels critères?	❑ / ❑	Délai et critères
19. Quel est le pourcentage des clients ayant souscrit une convention Internet[4] vis-à-vis du nombre total de clients?	% %	Site existant: chiffre réel au 31.12.2000 et estimation pour le 31.12.2001 Projet: estimation 1 an et 2 ans après la mise en production
20. Quel est le pourcentage des clients utilisant régulièrement les services Internet vis-à-vis du nombre total de conventions?	% %	Site existant: chiffre réel au 31.12.2000 et estimation pour le 31.12.2001 Projet: estimation 1 an et 2 ans après la mise en production
21. Est-ce que le site accepte des hyperliens vers d'autres sites? Si oui, à quelles conditions?	❑ / ❑	Nature des sites et conditions
22. Est-ce que le site accepte des bannières publicitaires? Si oui, à quelles conditions (ex. uniquement intergroupe)?	❑ / ❑	Nature des bannières et conditions
23. Est-ce que le site est disponible en plusieurs langues? Si oui, lesquelles? Est-ce que d'autres langues sont prévues?	❑ / ❑	
24. Est-ce que le contenu du site diffère d'une langue à l'autre? Si oui, quelles sont les différences?	❑ / ❑	

[4] Les questions 19 et 20 ne s'appliquent qu'aux sites qui exigent que le client signe une convention en vue d'utiliser les services Internet.

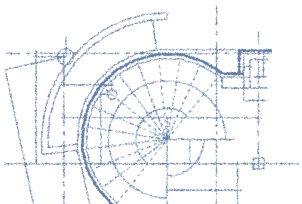


B) Sécurité / Maintenance

	OUI / NON	Commentaire / Détails
25. Est-ce que le site Internet est relié au réseau interne (LAN) de votre établissement? Si oui, existe t-il des protections?	❑ / ❑	Ex.: Firewall
26. Est-ce que le site Internet est relié au système bancaire / central de votre établissement (même à travers des équipements de sécurité)? Si oui, existe-t-il des protections?	❑ / ❑	Ex.: Firewall
27. Est-ce que l'analyse des risques effectuée par votre établissement comprend les aspects Internet? Si oui, lesquels?	❑ / ❑	Ex.: Volatilité des clients, Sécurité, ...
28. Est-ce que les aspects de sécurité relatifs à Internet ont été inclus dans la politique de sécurité de votre établissement?	❑ / ❑	
29. Est-ce que votre établissement a rédigé des procédures relatives à la gestion et la maintenance du site et de son infrastructure? Si oui, énumérez les types.	❑ / ❑	
30. Est-ce que votre établissement a recours à des sociétés externes (outsourcing) pour la gestion ou la maintenance du site? Si oui, lesquelles et pour quels domaines?	❑ / ❑	Ex.: Hébergement, Surveillance, Plan de secours, ...
31. Est-ce que votre établissement a prévu une solution de secours au cas où des éléments du site ne seraient plus fonctionnels? Si oui, laquelle?	❑ / ❑	Ex.: Redondance des firewalls
32. Est-ce que votre établissement a prévu des procédures (ex.: contact presse) au cas où le site serait en partie ou entièrement indisponible?	❑ / ❑	Ex.: Contacter les clients

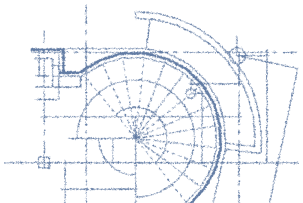


33. Est-ce que votre établissement a prévu des procédures (ex.: gestion de crise) en cas de détection d'une attaque?	❑ / ❑	Ex.: Couper la connexion
34. Est-ce que l'audit interne de votre établissement inclut les aspects Internet dans son plan d'audit?	❑ / ❑	
35. Avez-vous fait réaliser un audit externe Internet par une société spécialisée dans le domaine? Si oui, par qui et quels aspects ont été couverts?	❑ / ❑	
36. Est-ce que cet audit externe a couvert les aspects de sécurité technique?	❑ / ❑	
37. Est-ce que cet audit externe a couvert les aspects concernant les procédures / organisation relatifs au site?	❑ / ❑	
38. Est-ce que des éléments (ex. serveur, base de données) constituant le site ne sont pas situés au Luxembourg? Si oui, veuillez indiquer de quels éléments il s'agit ainsi que leur localisation et leur appartenance ou non au groupe.	❑ / ❑	



C) Authentification du client / Données confidentielles

	OUI / NON	Commentaire / Détails
39. Est-ce que l'identifiant du client est basé sur son nom? Si non, veuillez préciser s'il s'agit de son numéro de compte, de son numéro de convention, d'un nickname ou autre et si le client peut le modifier librement?	❑ / ❑	
40. Est-ce que l'authentification est basée sur un mot de passe? Si oui, est-ce que le client peut / est obligé de le changer?	❑ / ❑	Ex.: Changement du mot de passe obligatoire tous les 3 mois
41. Est-ce qu'il y a un élément physique (strong authentification) qui permet d'authentifier le client? Si oui, lequel?	❑ / ❑	Ex.: Code-card, Smart-card, Calculatrice token, ...
42. Existe-t-il un élément d'authentification qui persiste sur le poste du client? Si oui, lequel?	❑ / ❑	Ex.: Cookie, Fichier électronique, ...
43. Est-ce que votre établissement autorise le client à communiquer ses éléments d'identification à un tiers (ex.: service agrégateur)? Si oui, sous quelles conditions?	❑ / ❑	Ex.: Identifiant supplémentaire en lecture seule
44. Quelle est la technologie utilisée par votre site au niveau du client?		Cochez les cases correspondantes ❑ Applet Java ❑ Javascript ❑ ActiveX ❑ Html (sans autre composante) ❑ Autres:



45. Quels sont les critères qui ont conditionné votre choix pour ces technologies?		Ex.: Exigence d'un fournisseur,...
46. Est-ce que votre site utilise SSL? Si oui, sous quelles conditions?	❑ / ❑	Ex.: Encryption 40 bits acceptée
47. Est-ce que votre site utilise d'autres méthodes d'encryption? Si oui, lesquelles? En complément à SSL?	❑ / ❑	Ex.: IDEA
48. Imposez-vous un fournisseur ou une version minimale du Navigateur? Si oui, pour quelles raisons?	❑ / ❑	Ex.: IE 4.0 au minimum