

UN POINT SUR LE LIVRE BLANC DE LA COMMISSION BANCAIRE



Présentation du livre blanc

Publié en 1996 par la Banque de France et le Secrétariat Général de la Commission Bancaire (SGCB), le Livre Blanc sur la sécurité des systèmes d'informations dans les établissements de crédits constitue un document incontournable. Les banques et toutes les sociétés susceptibles de réaliser des opérations de crédit et de conservation de comptes (Crédit à la consommation, Bourse en ligne, etc.) doivent s'y référer afin d'appréhender les risques et les enjeux de l'informatique dans les milieux bancaires.

Voici quelques uns des principaux points abordés, assortis d'exemples simples.

XMCO | Partners

Les enjeux

L'informatique : le coeur du système bancaire

Le Livre Blanc demande aux banques et aux établissements de crédit d'assurer leur **devoir de sécurité** à l'égard de leur Système d'Information, de leurs clients et de l'ensemble du système bancaire.

Cette demande provient du constat que l'outil informatique est devenu le cœur du fonctionnement bancaire et qu'il constitue, de ce fait, une source de risques bien plus importante que dans n'importe quelle autre industrie.

L'informatique est l'**outil de production** des banques. Une défaillance informatique importante entraînerait des conséquences fâcheuses pour les clients ainsi que pour les autres établissements qui sont en relation avec l'organisme victime.

Ces risques sont d'autant plus importants que la possibilité de **reconstitution a posteriori des données perdues** ou endommagées est, aujourd'hui, devenue **irréaliste**, compte-tenu des volumes de transactions.



Une démarche Top-Down : sensibilisation au plus haut niveau de la banque



Afin de ne pas alourdir la réglementation bancaire déjà existante, la commission bancaire a préféré suivre le principe de type « **Best Practices** » avec la diffusion du Livre Blanc.

La démarche préconisée consiste à **impliquer la Direction Générale** de chaque établissement en lui attribuant l'application et le **contrôle** des moyens de sécurité informatique.

Le Livre Blanc propose, sans imposer, la méthode d'évaluation des risques "**Marion**" publiée par le CLUSIF.

Une démarche en 4 étapes pour maîtriser les risques

Comme il n'est possible d'agir efficacement que sur les risques identifiés, le Livre Blanc recommande une méthodologie d'évaluation des risques en **4 ETAPES** : **IDENTIFIER** les risques, les **CLASSER**, les **CHIFFRER** et les **ARBITRER**.



ETAPE 1 : IDENTIFIER LES RISQUES

Il est nécessaire **d'identifier et de lister des menaces** auxquelles le Système d'Information de la banque peut être confronté.

Ces dernières peuvent être de différentes natures : naturelles, accidentelles (incendie), humaines (volontaire ou involontaire).

Le rôle du DSI et du RSSI est alors de mettre en place des mesures de sécurité pour **diminuer l'impact de ces menaces** potentielles.

Exemples de menaces non classées :

- Inondation de la salle informatique principale
- Attaques de « déni de service » sur le site web
- Indisponibilité du réseau des distributeurs automatiques
- « crash » d'une partie de la base de données clients, etc.



ETAPE 2 : CLASSER LES RISQUES IDENTIFIES SELON LES CRITERES D.I.C.P

Chaque risque identifié lors de l'étape 1 doivent être classés en fonction des quatre critères suivants : **Disponibilité, Intégrité, Confidentialité et Preuve**.

Disponibilité : Tous les éléments susceptibles d'**interrompre la production** : pannes informatiques, électriques ou de télécommunications.

Intégrité : Tous les éléments capables de **corrompre le contenu** des données bancaires : valeurs sur un compte, modification imprévue des valeurs de change et/ou de titres.

Confidentialité : Tous les éléments liés au **secret bancaire**. Seules les personnes habilitées peuvent accéder aux informations stockées.

Preuve : Tous les éléments liés à l'audibilité et à la traçabilité des transactions : Z a transféré la somme X à Y le jour J.

Quelques exemples DICP :

Risque de type Disponibilité : Un pirate informatique peut, volontairement, à partir d'Internet, « planter » le site web de la banque utilisé pour la consultation des comptes.

Risque de type Confidentialité : Un client malicieux qui possède un compte bancaire peut, par le biais du site web, lire les relevés de comptes d'un autre client.

Risque de type Preuve : Un employé de la banque peut effectuer un virement de compte à compte sans qu'aucune trace ne puisse être présentée, en cas de litige, sur le montant et la date.

Risque de type Intégrité : Pendant la sauvegarde nocturne de la base de données du système central, il est possible que les dates de valeurs soient effacées ou bien réinitialisées lors d'une coupure de courant qui surviendrait au même moment.

Une fois que ces risques ont été identifiés et classés selon l'un des critères DICP, l'évaluation peut commencer.



ETAPE 3 : EVALUER SON RISQUE MAXIMAL TOLÉRABLE (RMT)

Comme l'indique le Livre Blanc : « *Tout ne peut pas être fait tout de suite et à n'importe quel prix pour éviter toute forme de risque* ». Il est donc nécessaire d'établir des priorités en chiffrant les risques identifiés.

Le Livre Blanc apporte le concept de calcul du **Risque Maximal Tolérable (RMT)**.

Le calcul de ce facteur RMT servira ensuite de base à la stratégie de gestion des risques.



ETAPE 4 : CLASSER LES RISQUES SELON 2 CATÉGORIES: "STRATEGIQUE" et "NON STRATEGIQUE"

La Direction Générale arbitre les risques identifiés en fonction de l'impacts qu'ils ont sur l'activité de l'établissement. Pour cela, la commission bancaire propose une échelle à 5 niveaux (de 0 à 4) où **seuls les risques de niveau 2 et plus** doivent être pris en compte.

Niveau 0 : Risques « Extrêmement faibles »

Risques dont l'impact financier est négligeable.

Exemple : Panne momentanée d'un distributeur de billet.

Niveau 1 : Risques « Faibles »

Risques susceptibles d'occasionner des pertes financières faibles et peu gênantes pour le client.

Exemple : Panne d'un poste de travail ou fonctionnement temporaire en mode dégradée d'une agence.

Niveau 2 : Risques « Sensibles »

Risques susceptibles d'entraîner des pertes financières significatives, de nuire à l'image de marque de l'établissement ou de générer une infraction mineure à la législation.

Exemple : Indisponibilité du site web pendant plus d'une heure.

Niveau 3 : Risques « Critiques »

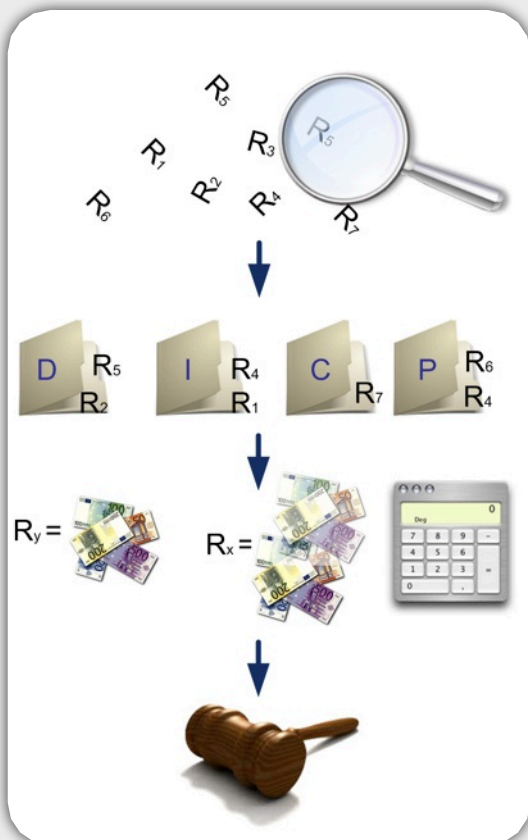
Risques qui peuvent engendrer des pertes financières inacceptables (ex : 30 % du RMT), ou bien une perte importante de clientèle.

Exemple : Failles de sécurité dans le site web transactionnel qui permettrait de voler et de transférer l'argent de comptes clients.

Niveau 4 : Risques « Stratégiques »

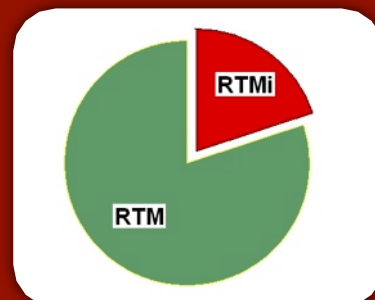
Risques susceptibles de causer l'arrêt immédiat (ou à court terme) d'une activité de l'établissement, ou d'entraîner des sanctions judiciaires.

Exemple : Panne informatique qui entraînerait la perte de la base de données avec l'impossibilité de restaurer une partie des comptes clients sous des délais raisonnables.



LES DEFINITIONS...

RMT : « la part des fonds propres que la banque, en fonction de sa stratégie, "accepte" de perdre en cas de catastrophe, auquel on peut ajouter la part des résultats opérationnels ("cash-flow") qui pourrait également absorber ce sinistre et les garanties, notamment les remboursements possibles "garantis" par la police d'assurance couvrant ces risques. »



RTMi : Le RTMi est le coût maximal lié à un sinistre informatique.

Le problème du RMT : Evaluer le risque tolérable

Le Livre Blanc apporte le concept de **Risque Maximal Tolérable** dans sa démarche en quatre étapes présentée ci-dessus.

Le RMT au centre des attentions

Pour bien saisir le rôle du **RMT** au sein du Livre Blanc Bancaire, il existe deux formules simplifiées.
Pour un scénario « sinistre informatique » dans la banque, le risque est défini par la formule suivante :

$$\text{Risque} = (\text{Probabilité d'apparition du sinistre}) * (\text{Conséquences financières si le sinistre survient})$$

Le livre Blanc stipule que la somme des risques doit être inférieure au RMT.

$$\text{Somme des Risques} \leq \text{RMT}$$

L'évaluation du montant du RMT constitue donc une étape fondamentale pour l'établissement bancaire : le RMT est le majorant de l'équation de gestion des risques.

Comment calcule-t-on le RMT ?

Quelle somme d'argent la banque accepte-t-elle de perdre en cas de panne informatique pour ne pas couler? Cette perte peut-elle être « amortie » par les bénéfices annuels et par les assurances?

Le RMT c'est la « VALUE AT RISK »

Voici la formule de calcul du RMT :

$$\text{RMT} = \alpha * \text{Fond Propre} + \beta * \text{Bénéfices} + \gamma * \text{Montant de la Garantie d'Assurance}$$

α est le pourcentage des fonds propres de l'établissement fixé comme limite de perte maximale en cas de sinistre informatique total. L'exemple donné par le Livre Blanc est 20 %.

β est le pourcentage du résultat brut d'exploitation annuel pouvant servir à éponger une catastrophe.

γ est la proportion estimée (taux de couverture probable), compte tenu des garanties prises (assurances...), qui peuvent servir de compensation monétaire (ou technique) en cas d'accident au sein du système d'information.

La détermination fine du montant du RMT peut s'avérer être un véritable casse-tête. Le choix de l'évaluation du RMT incombe uniquement à la Direction Générale, seule entité habilitée à arbitrer parmi les différents enjeux.

Il est important de ne pas oublier que le **RMT n'est qu'une estimation**. Sa détermination permet de **fixer une valeur précise** dans un univers de **risques flous**. Celle-ci sera ensuite utilisée comme base pour des arbitrages.

La plus grande valeur ajoutée, en ce qui concerne le calcul du RMT, n'est pas l'exactitude de la valeur obtenue mais le fait que **la Direction Générale engage une telle démarche de maîtrise des risques informatiques**.



LA PREUVE PAR L'EXEMPLE...

Exemple d'évaluation du RMT

Afin d'illustrer les éléments théoriques présentés ci-dessus, nous proposons l'étude du cas d'un établissement financier. Celui-ci propose à ses clients l'achat et la vente de produits financiers (actions, options, futures, warrants) uniquement sur Internet. Les achats peuvent être réglés comptant ou de manière différée (SRD). L'établissement réalise donc des opérations de crédit.

Nous commençons par l'évaluation du montant du RMT.

Hypothèses : L'établissement possède 15 millions d'euros de fonds propres et nous fixons, comme le recommande le Livre Blanc, α à 20%. L'établissement réalise 5 millions d'euros de résultats bruts. La direction générale choisit de fixer β à 10%. C'est-à-dire que 10% des résultats d'exploitation peuvent servir à épouser les pertes en cas de sinistre.



Enfin, nous ne choisissons pas la valeur du **montant de l'assurance** γ . Cette variable sera l'inconnue de notre équation. Nous tenterons ainsi d'en faire une évaluation afin de choisir au mieux le système d'assurance que l'établissement doit adopter.

Reprenons la formule du calcul du RMT :

$$\text{RMT} = \alpha * \text{Fonds Propres} + \beta * \text{Bénéfices} + \gamma * \text{Montant de la Garantie d'Assurance}$$

Et dans notre cas :

$$\text{RMT} = (15\,000\,000 * 20\%) + 5\,000\,000 * 10\% + \gamma = 3\,500\,000 \text{ €}$$

Nous avons donc le montant du RMT de l'établissement. Il nous faut encore définir δ_i , la part du RMT global associée aux risques informatiques (le RMT_i). Nous fixons cette part à 1/5. C'est-à-dire que 20% des risques de l'établissement peuvent être attribués à des sinistres informatiques.

$$\text{RMT}_i = \text{RMT} * \delta_i = \text{RMT} * 1/5 = 700\,000 \text{ €}$$

Dans notre cas, nous identifions deux risques R1 et R2. L'un est de type Intégrité et l'autre, de type Disponibilité.

R1 : « Piratage d'un compte sur le site avec transfert frauduleux vers un compte extérieur »

Le montant maximum d'un transfert depuis le site vers un compte extérieur est de 500 000 euros. Soit $V1 = 500\,000 \text{ €}$

$$R1 = \mu_1 * V1, \text{ avec } V1 = 500\,000 \text{ €}$$

Reste à définir la probabilité d'occurrence μ_1 d'un tel sinistre.

$$R2 = \mu_2 * V2, \text{ avec } V2 = 20\,000\,000 \text{ €}$$

R2 : « Attaque Internet du site web entraînant une indisponibilité d'une journée »

La somme des pertes engendrées, pour l'ensemble des clients, par l'impossibilité de vendre ou d'acheter en fonction des variations des marchés financiers peut être très importante. Nous fixons la perte totale à 20 millions d'euros, soit $V2 = 20\,000\,000 \text{ €}$.

Imaginons alors **3 cas de figure**:

CAS N°1 : LE CAS IDÉAL	CAS N°2 : LE CAS RÉEL	CAS N°3 : LE CAS CRITIQUE
L'établissement maîtrise la sécurité de son système d'information. Les probabilités d'occurrence μ_1 et μ_2 sont donc très faibles.	La sécurité du système est imparfaite , mais les employés et les clients demeurent fiables. Les probabilités d'occurrence μ_1 et μ_2 ne sont pas négligeables.	Le système est vulnérable et exposé à des utilisateurs peu scrupuleux. Les probabilités d'occurrence μ_1 et μ_2 sont élevées.
Soit : $\mu_1 = 1/1000$ et $\mu_2 = 1/250$. RTMi évalué à 700 000 euros	Soit : $\mu_1 = 1/10$ et $\mu_2 = 3/100$	Soit : $\mu_1 = 1/10$ et $\mu_2 = 1/20$.
La somme des risques est alors définie comme suit : $R1 + R2 = (500\ 000 * 1/1000) + (20\ 000\ 000 * 1/250)$ = 80 500 €	Nous définissons la somme des risques ($\mu_1 * V1 + \mu_2 * V2$) de la manière suivante: $R1 + R2 = (500\ 000 * 1/10) + (20\ 000\ 000 * 3/100)$ = 50 000 + 600 000 = 650 000 €	La somme des risques est alors définie de la manière suivante : $R1 + R2 = (500\ 000 * 1/10) + (20\ 000\ 000 * 1/20)$ = 50 000 + 1 000 000 = 1 050 000 €
80 500€ << RTMi Avec un RMTi évalué à 700 000 €, l'établissement est alors dans une situation où la somme des risques est très inférieure au RMTi	L'établissement est alors dans une situation où la somme des risques est proche du RMTi .	L'établissement est alors dans une situation où La somme des risques est supérieure au RMTi .
Dans le cas n°1 où $R1 + R2 \ll \text{RMTi}$, l'établissement peut choisir de réduire la part de risque informatique de sa police d'assurance.	Dans la cas n°2 où $R1 + R2 \approx \text{RMTi}$, l'établissement doit renforcer sa sécurité et adapter le contrat d'assurance relatif aux risques informatiques.	Dans la cas n°3 où $R1 + R2 > \text{RMTi}$, l'établissement doit agir μ_1 et μ_2 et tenter de trouver des solutions pour réduire V1 et V2.

Le suivi permanent du RMTi et des nouveaux risques

Après les calculs, les arbitrages, les contrôles et les audits, il conviendra de faire évoluer en permanence le calcul du RMT et du RMTi.

Comme l'indique le Livre Blanc : « toute création ou modification importante de logiciel applicatif développé en interne, ou tout achat de progiciel applicatif doit faire l'objet d'une analyse de vulnérabilité donnant lieu à l'établissement d'un chapitre sécurité formalisé : consultable, maintenable et accessible ».

Les banques font aujourd'hui face à de nouveaux risques comme le "phishing", qu'elles intègrent à leur calcul du RMT.

Conclusion

Le Livre Blanc de la commission bancaire est un document incontournable pour tous les établissements bancaires ou les établissements de crédits. Ecrit il y a plus de 10 ans, ce document demeure une référence en matière de **gestion raisonnée des risques informatiques**.

Les audits de sécurité et les tests d'intrusion constituent des outils efficaces pour évaluer et réduire les risques liés à l'informatique dans un milieu bancaire.

Bibliographie

* [1] Livre Blanc sur la sécurité des systèmes d'information

http://www.banque-france.fr/fr/supervi/supervi_banc/publi/lbsecusys.htm



A propos d'Xmco Partners

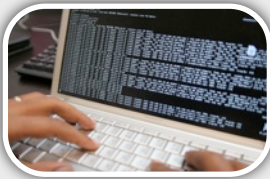
Le cabinet Xmco Partners réalise plus d'une dizaine d'audits de sécurité et de tests d'intrusion par mois sur des banques en ligne et des infrastructures web e-business. Nos clients sont tous des grands comptes français et internationaux.

Notre équipe "tests d'intrusion" est très certainement la plus expérimentée et la plus reconnue en termes d'audit de sécurité des applications Web (webapp pentests) et des sites de commerce en ligne.

Nos consultants possèdent une véritable expertise des intrusions informatique au sein des applications et des plateformes bancaires.

Les techniques d'attaques informatiques les plus récentes sont mises en oeuvre pour évaluer les plateformes web :


Fuzzing, SQL Injection, SOAP/XML injection, XSS et CSRF Attacks, HTTP parameters tampering, Sessions-id prediction, web-cache poisoning et bien d'autres.



Autres publications

Les consultants Xmco Partners publient régulièrement des études et des retours d'expériences relatifs à la sécurité informatique dans le domaine bancaire et des plateformes transactionnelles en ligne :

 La sécurité des sessions des frameworks applicatifs
<http://www.xmcopartners.com/article-owasp-session.html>

 Le guide PCI DSS de Visa/Mastercard pour la sécurité des transactions en ligne
<http://www.xmcopartners.com/article-paiement-bancaire-securises.html>

 La Loi sur la Sécurité Financière (LSF)
<http://www.xmcopartners.com/article-lsf.html>

Contactez XMCO PARTNERS

Pour contacter le cabinet Xmco Partners et obtenir des informations sur nos tests d'intrusion bancaires : +33 (0)1 47 34 68 61 ou info@xmcopartners.com.

A propos de l'auteur



Frédéric Charpentier, expert en tests d'intrusion des applications en ligne et des plateformes e-business.

De formation ingénieur (Ecole Polytechnique de Nantes), Frédéric Charpentier a intégré le cabinet Xmco Partners en 2002 après plusieurs expériences dans le milieu de la banque et des places financières.

Email : fcharpentier@xmcopartners.com