

Janvier 2019 – document final

Le risque informatique

Document de réflexion

AUTEURS
Marc ANDRIES, David CARTEAU, Sylvie CORNAGGIA,
Pascale GINOLHAC, Cyril GRUFFAT, Corinne LE MAGUER

CONTRIBUTEURS
Roméo FENSTERBANK, Thierry FRIGOUT,
Pierre HARGUINDEGUY, Christelle LACAZE

ACPR
BANQUE DE FRANCE

SYNTHÈSE DE LA CONSULTATION PUBLIQUE LANCÉE EN MARS 2018

Le document de réflexion sur le risque informatique a été mis à jour suite aux commentaires reçus après sa publication le 31 mars 2018 et à la conférence de l'ACPR tenue le 18 septembre 2018, au cours de laquelle s'est tenue une table ronde consacrée au risque informatique.

Dix-sept répondants français et étrangers (établissements des secteurs de la banque et de l'assurance, associations professionnelles, autorités) ont bien voulu participer à cette consultation publique en répondant aux douze questions et en fournissant leurs commentaires généraux.

Les commentaires ont souligné la qualité des réflexions, de même que le très fort intérêt de structurer les différents éléments d'une définition et d'une catégorisation du risque informatique.

Suite à ces interactions, les mises à jour qui ont été effectuées concernent notamment :

- **La clarification de la définition du risque informatique**, afin de bien faire ressortir que celle-ci inclut toute inadaptation ou défaillance qui affecterait l'un des trois macro-processus de gestion du système d'information. Plusieurs commentaires reçus soulignaient que ces risques ne se limitaient pas au seul système d'information mis en œuvre par la fonction informatique, mais qu'ils pouvaient également concerner des éléments informatiques gérés par les utilisateurs eux-mêmes (« *shadow IT* »). Le document de réflexion a été revu pour faire clairement mention de ces éléments. De même, il est précisé dorénavant que les risques liés à un mauvais usage des utilisateurs sont bien inclus.

- **La définition de la cybersécurité** a également été élargie pour indiquer que ces efforts de protection et de réaction visaient aussi à éviter les négligences pouvant donner lieu à une activité informatique malicieuse.

- **Des clarifications sur l'organisation à mettre en œuvre pour la maîtrise de risques informatiques.** Ainsi, le document insiste sur l'importance d'une organisation selon le modèle des trois « lignes de défense », prônée par les textes internationaux [1]. Cette organisation s'applique déjà au risque opérationnel, mais souvent imparfaitement au risque informatique, alors que celui-ci en fait partie. Selon ce modèle, la fonction informatique (qu'elle soit tout entière confiée à la direction des services informatiques ou partagée avec les métiers) a la charge de la mise en œuvre opérationnelle du système d'information et de sécurité. Elle doit ainsi identifier ses risques et définir ses politiques et normes destinées à les maîtriser, y compris en matière de sécurité. Au sein de la deuxième ligne de défense, la fonction de gestion des risques a vocation à déterminer la tolérance de l'établissement aux risques informatiques, fixer la stratégie et les politiques de sécurité pour respecter cette tolérance, ainsi qu'elle doit contrôler les vérifications effectuées par la première ligne de défense.

1 Banque des règlements internationaux (2015) : « Principes de gouvernance d'entreprise à l'intention des banques », juillet.

Autorité bancaire européenne (2013) : « Lignes directrices sur la gouvernance interne selon la directive//36/EU », notamment les paragraphes 28 et suivants.

Association internationale des superviseurs d'assurance (2017) : « Document d'application sur le contrôle de la cybersécurité des organismes d'assurance » (« *Application Paper on Supervision of Insurer Cybersecurity* ») paragraphe 97 et suivants, septembre.

- **Le rôle et le positionnement du Responsable de la sécurité des systèmes d'information (RSSI) sont également précisés.** En effet, la responsabilité de la sécurité doit s'adapter à la logique du modèle le plus robuste d'organisation, qui est celui des trois « lignes de défense ». Les établissements devraient disposer d'équipes chargées de la sécurité des systèmes d'information au sein de la fonction informatique (première ligne de défense), ayant à identifier les risques et définir en conséquence des procédures de sécurité, puis à en vérifier la mise en œuvre. Mais ils devraient également disposer au sein de la deuxième ligne de défense, dans la fonction de gestion des risques, d'une équipe chargée de la sécurité de l'information afin de proposer aux instances dirigeantes un niveau de tolérance acceptable à ces risques pour l'établissement, ainsi qu'une stratégie et des politiques de sécurité pour respecter cette tolérance, et de contrôler les vérifications effectuées par la première ligne de défense. Disposant de l'indépendance et de la capacité à s'exprimer devant les instances dirigeantes, le responsable de la fonction de gestion des risques devrait pouvoir alerter celles-ci en cas de situation de risque exceptionnel.

- **Deux facteurs de risque ont été ajoutés :**

  - « Défaut dans l'analyse de risques » : ce facteur de risque vient compléter ceux relatifs à la « gestion des risques », qui peuvent affecter le processus d'« organisation du système d'information ». Il permet de faire davantage ressortir le caractère essentiel des analyses de risques à conduire préalablement aux nouveaux projets, aux nouvelles activités, lorsque ceux-ci impliquent une évolution du système d'information ou peuvent avoir des conséquences sur celui-ci.

  - « Défaut dans les logiciels » : ce facteur de risque vient compléter ceux relatifs à la « Mauvaise gestion des changements (projets, évolutions, corrections) » qui peuvent affecter le processus de « fonctionnement du système d'information ». Cet ajout permet de préciser les exigences portant sur le niveau de qualité des applications, y compris du *shadow IT*.

Le document ainsi révisé suite à ces interactions fournit donc une catégorisation du risque informatique plus complète, afin de couvrir ses différentes dimensions et permettre de le traiter dans sa globalité.

SYNTHÈSE

L'émergence des cyberattaques ces dernières années a accru les préoccupations liées au risque informatique. Ces préoccupations ne sont pas propres aux secteurs de la banque et de l'assurance, mais elles ont une résonnance particulière en ce qui les concerne. En effet, ces secteurs représentent un maillon essentiel pour le bon fonctionnement de l'économie et la protection des intérêts du public.

Pour répondre à ces préoccupations, les autorités de supervision renforcent progressivement leur action. Des instances internationales élaborent de nouvelles règles en matière de risque informatique et les autorités, comme l'ACPR, agissant notamment dans le cadre du mécanisme européen de supervision unique bancaire, renforcent leurs contrôles.

Ce document de réflexion souligne que la maîtrise du risque informatique n'est plus seulement un sujet propre aux équipes informatiques mais qu'elle s'inscrit dans la démarche générale de contrôle et de maîtrise des risques pilotée par la fonction de gestion des risques. Le cadre de référence de gestion du risque opérationnel a donc vocation à être précisé pour mieux inscrire le risque informatique, dans toutes ses dimensions, au sein des catégories reconnues de risque opérationnel. Dans cette organisation, les instances dirigeantes sont directement impliquées, à la fois pour la mise en cohérence de la stratégie informatique et de l'appétit au risque, mais aussi pour la mise en œuvre et le suivi d'un cadre de maîtrise des risques.

Forts de leur expérience de contrôle, les services de l'ACPR ont élaboré une définition et une catégorisation du risque informatique, afin d'en couvrir les différentes dimensions et de pouvoir le traiter dans sa globalité. Cette catégorisation peut servir aux établissements placés sous son contrôle pour élaborer ou renforcer leur propre cartographie. Cette catégorisation couvre les trois grands processus de mise en œuvre et de gestion du système d'information, c'est-à-dire à la fois ce qui a trait à l'organisation de celui-ci, ce qui concerne son bon fonctionnement, et aussi sa sécurité. Pour chacun de ces grands processus, le document de réflexion indique une série de facteurs de risque, élaborée sur deux niveaux pour permettre une analyse assez fine. Pour chaque facteur de risque, sont indiquées les principales mesures de réduction et de maîtrise des risques attendues. Ces mesures sont indicatives et les établissements peuvent les adapter à leur contexte. Elles illustrent les meilleures pratiques habituellement constatées par les services de l'ACPR et visent à constituer un socle commun de maîtrise du risque informatique dans les secteurs de la banque et de l'assurance.

SOMMAIRE

6 **Introduction**

9 **Le risque informatique et son ancrage dans le risque opérationnel**
9 1 État des lieux de la réglementation au plan international
11 2 La démarche de définition et de catégorisation du risque informatique au sein de l'ACPR

15 **Organisation du système d'information et de sa sécurité**
16 1 Implication des instances dirigeantes
17 2 Alignement de la stratégie informatique avec la stratégie métier
18 3 Pilotage budgétaire
19 4 Rôles et responsabilités de la fonction informatique
21 5 Rationalisation du système d'information
22 6 Maîtrise de l'externalisation
24 7 Respect des lois et règlements
25 8 Gestion des risques

29 **Fonctionnement du système d'information**
30 1 Gestion de l'exploitation (systèmes et réseaux)
32 2 Gestion de la continuité informatique d'exploitation
35 3 Gestion des changements (projets, évolutions, corrections)
37 4 Qualité des données

39 **Sécurité du système d'information**
40 1 Protection physique des installations
41 2 Identification des actifs
41 3 Protection logique des actifs
48 4 Détection des attaques
49 5 Dispositif de réaction aux attaques

51 **Annexe : catégorisation du risque informatique**



Introduction

De nombreuses instances internationales mettent l'accent, depuis plusieurs années, sur la montée du risque informatique au sein des secteurs de la banque et de l'assurance. Ces interventions résultent d'un double constat. En premier lieu, les activités des établissements reposent désormais en totalité sur des systèmes d'information automatisés, y compris pour la relation avec la clientèle [1], et ces environnements sont devenus complexes à gérer. En second lieu, les dommages informatiques, malgré toutes les précautions prises, deviennent des risques majeurs pour l'exercice des activités de ces établissements. En particulier, la capacité de nuisance des cyberattaques n'a cessé de progresser ces dernières années. Alors qu'au début ces attaques portaient principalement sur les équipements des clients et avaient donc un caractère unitaire, peu perturbant dans l'ensemble, elles visent désormais directement les environnements informatiques des établissements et peuvent avoir des conséquences majeures, y compris systémiques, en raison des relations d'interdépendance croissantes qui lient les différents acteurs financiers.

En réponse, les instances qui produisent les standards internationaux applicables aux secteurs de la banque et de l'assurance ont commencé à formuler leurs attentes vis-à-vis de la profession. L'Autorité bancaire européenne (ABE) a ainsi adopté plusieurs documents normatifs sur les risques informatiques du secteur bancaire, notamment des lignes directrices à l'usage des autorités de supervision pour développer de manière uniforme leur évaluation des risques informatiques des établissements [2]. L'Autorité européenne des assurances et des pensions professionnelles (AEAPP [3]) a publié, un document de réflexion sur le risque cyber [4] et a engagé une revue de ce risque avec des acteurs majeurs de l'assurance.

Parmi les différents risques informatiques, ceux relatifs à la cybersécurité ont fait l'objet d'une attention toute particulière de la part de plusieurs autorités. Le G7 a déjà adopté des principes de haut niveau, non contraignants, qui ont vocation à orienter et unifier les actions en la matière [5] et il poursuit son action sur plusieurs plans pour intensifier les démarches des régulateurs du secteur. Le comité pour les paiements et les infrastructures de marché (CPMI [6]) de la Banque des règlements internationaux et l'organisation internationale des autorités de marché (IOSCO [7]) ont publié des orientations afin d'améliorer la résilience des infrastructures de marché

1 Ce que l'on appelle parfois la « digitalisation » des activités bancaires et financières.

2 EBA (2017) : « *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process* (SREP) », 11 mai 2017.

3 En anglais « *European Insurance and Occupational Pensions Authority* » – EIOPA

4 Rédigé par son Groupe des parties prenantes du secteur de l'assurance et la réassurance (IRSG) (2016) : « *Cyber risk – some strategic issues* », avril.

5 G7 (2016) : « *Fundamental elements of cybersecurity for the financial sector* », octobre, et G7 (2017) : « *Fundamental elements for effective assessment of cybersecurity in the financial sector* », octobre.

6 Committee on Payments and Market Infrastructures – CPMI

7 International Organisation of Securities Commissions – IOSCO

face aux attaques cyber [8]. L'Association internationale des contrôleurs de l'assurance (AICA [9]) a également publié un document de réflexion sur le risque cyber du secteur de l'assurance [10] et poursuit avec un document d'application.

Dans l'ensemble de ces textes, le risque informatique est reconnu explicitement ou implicitement comme un risque opérationnel, tel qu'il avait été documenté puis encadré par le Comité de Bâle sur le contrôle bancaire (CBCB) à partir de 2003. Pour autant, il reste encore à préciser l'inclusion et le traitement du risque informatique au sein du risque opérationnel pour que les mêmes principes de traitement s'y appliquent.

De leur côté, les autorités de supervision développent également fortement leur action dans le domaine du risque informatique. Dès novembre 2014, lorsque lui a été transférée la compétence de supervision directe des établissements bancaires de la zone euro les plus importants (« *significant institutions* »), la Banque Centrale Européenne (BCE), avec l'assistance des autorités nationales de supervision rassemblées dans le « mécanisme de supervision unique » (MSU), a immédiatement lancé plusieurs actions de contrôle sur pièces et sur place. Des questionnaires d'évaluation sur la cybersécurité ou sur les pratiques d'externalisation des activités informatiques ont permis de prendre rapidement la mesure des forces et faiblesses du secteur, puis d'engager des actions correctrices. De nombreux contrôles sur place, menés le plus souvent par les autorités nationales, ont complété la démarche et permis de disposer d'informations précises sur les actions à mener.

Une telle démarche était déjà bien ancrée en France, puisque la commission bancaire avait publié en 1996 un livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit et qu'elle s'était dotée depuis 1995, au sein des équipes d'inspection sur place, d'une équipe dédiée pour les risques liés aux systèmes d'information. Forte de cet existant, l'ACPR a pris part aux actions de la BCE, à la fois en mettant ses contrôleurs sur pièces à disposition des équipes conjointes de supervision (« *Joint supervisory team* ») du MSU et en confiant la réalisation de contrôles sur place aux inspecteurs de la Banque de France. Dans les domaines où elle a autorité directe, comme celui des entités bancaires « moins importantes » (« *Less-significant institutions* »), les autres entités du secteur bancaire (sociétés de financement et prestataires de services de paiement notamment) et celui de l'assurance, l'ACPR mène également de nombreuses interventions au titre de ses contrôles permanents et de ses contrôles sur place. L'importance toujours croissante des risques informatiques représente un défi permanent en termes de développement des ressources et des compétences. Pour y répondre, l'ACPR a poursuivi ses actions de formation et elle a complété les équipes dédiées du contrôle sur place en constituant un réseau d'experts en matière de risque informatique, composé d'une vingtaine de participants. Ces experts représentent l'ACPR dans les différentes instances internationales qui travaillent sur le risque informatique et la cybersécurité.

Ce « document de réflexion » a été rédigé par des experts informatiques du réseau constitué par l'ACPR. Il vise à communiquer sur les enjeux perçus concernant les risques informatiques, tant s'agissant de leur reconnaissance que de leur réduction. Il constitue une contribution aux réflexions sur la manière d'intégrer la maîtrise du risque informatique

8 CPMI-IOSCO (2016) : « *Guidance on cyber resilience for financial market infrastructures* », juin.

9 International Association of Insurance Supervisors – IAIS

10 IAIS (2016) : « *Issues Paper on cyber risk to the insurance sector* », août.

dans le cadre de gestion du risque opérationnel. Il pourra servir également aux travaux sur l'amélioration de la « résilience opérationnelle » des établissements, c'est-à-dire à leur capacité à absorber les perturbations opérationnelles de toute nature.

En premier lieu, le document propose une définition du risque informatique conçu comme une dimension du risque opérationnel. En second lieu, cette définition s'accompagne d'une proposition de catégorisation du risque informatique, afin d'en couvrir toutes les dimensions de manière cohérente. Pour chaque élément présenté dans cette catégorisation, le document indique ce qui paraît caractériser une bonne gestion des risques.



Le risque informatique et son ancrage dans le risque opérationnel

1 État des lieux de la réglementation au plan international

D'abord conceptualisée par les instances bancaires, la notion de risque opérationnel a ensuite été reprise par les instances du secteur de l'assurance. Le Comité de Bâle sur le contrôle bancaire a progressivement développé ses préconisations pour la maîtrise du risque opérationnel à partir de 2003 [11]. Il a ensuite ajouté des exigences en fonds propres pour faire face aux incidents de nature opérationnelle pouvant affecter les établissements [12]. Pour couvrir les multiples facettes du risque opérationnel, le Comité de Bâle a retenu une définition large, incluant les défaillances internes comme les évènements extérieurs, et axée sur le risque de perte financière, directe ou indirecte. Selon le Comité, le risque opérationnel recouvre en effet tout « risque de perte résultant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes, ou d'événements externes ». Cette définition, avec de légères nuances d'écriture, s'est retrouvée dans les différents cadres législatifs et réglementaires, notamment les directives européennes encadrant l'activité bancaire [13] et du secteur de l'assurance [14]. Elle est également reprise par la réglementation bancaire française [15]. Ce cadre a été volontairement conçu de manière large et flexible pour couvrir la grande variété des organisations et permettre aux établissements de le mettre en œuvre de façon proportionnée à l'importance et à la complexité de leurs activités.

Dans aucun de ces documents le risque informatique n'est explicitement visé, même si les différentes autorités s'accordent à l'y ranger au titre de la « défaillance des processus, du personnel et des systèmes », comme c'est par exemple le cas avec les pannes ou les erreurs informatiques, ou aussi au titre des « évènements externes » comme c'est le cas avec les cyberattaques. Cela tient au raisonnement initial des autorités normatives selon lequel les outils informatiques et le système d'information dans son ensemble étaient des éléments au service de l'activité des établissements, mais qu'ils n'étaient pas leur raison d'être. Selon cette approche, les risques principaux sont ceux spécifiquement liés à l'exercice de l'activité, comme les risques de crédit, de marché ou d'assurance. Une défaillance informatique n'est principalement perçue dans ce cas que par sa conséquence sur le métier qui en est l'utilisateur. La reconnaissance

11 BCBS (2003) : « *Sound practices for the management and supervision of operational risk* », *Basel Committee Publications* n° 96, février.

12 BCBS (2006) : « *International convergence of capital measurement and capital standards* », *Basel Committee Publications* n° 128, juin.

13 Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (Directive CRD IV). Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement (Règlement CRR, article 4).

14 Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II). L'article 1333) définit le risque opérationnel comme « le risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs ».

15 L'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'ACPR, définit dans son article 10 le risque opérationnel comme « le risque de pertes découlant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes internes ou d'événements extérieurs, y compris le risque juridique ; le risque opérationnel inclut notamment les risques liés à des événements de faible probabilité d'occurrence mais à fort impact, les risques de fraude interne et externe définis à l'article 324 du règlement UE n° 575/2013 susvisé, et les risques liés au modèle ».

du risque opérationnel dans les années 2000 a constitué une avancée dans la mesure où un traitement qualitatif (gestion du risque et contrôle interne) puis quantitatif (exigence en fonds propres) sont venus compléter les risques « métier » et couvrir les différents évènements liés au support des métiers (dont la fonction informatique). Les travaux nombreux et approfondis conduits vers 2005 sur la continuité d'activité ont également visé à renforcer les dispositions applicables à ce sujet pour garantir une meilleure résistance aux pannes, mais n'ont pas modifié le cadre général du risque opérationnel. Mais en l'état, hormis une définition large et englobante, le risque opérationnel reste décrit selon une catégorisation (indicative) en sept classes, dont aucune individuellement, ni plusieurs réunies, ne couvrent les différents aspects du risque informatique [16].

L'intensification récente des travaux sur le risque informatique marque donc une évolution notable. Elle consiste à reconnaître ce risque plus explicitement compte tenu de son importance grandissante et transversale pour tous les métiers. Toutefois, s'il est unanimement rangé par les régulateurs dans les risques opérationnels, des éléments de définition et de traitement du risque informatique tardent à être formulés. Les établissements sont donc laissés libres de les formuler et doivent justifier qu'ils traitent toutes les dimensions du risque informatique en accord avec les dispositions applicables au risque opérationnel. Cet effort n'est pas des plus aisés. Depuis longtemps, les établissements des secteurs de la banque et de l'assurance, comme toute entreprise, s'appuient sur les principes de bonne gestion informatique produits par les organismes de standardisation internationaux, comme l'International Standardisation Organisation (ISO), auxquels certains textes bancaires faisaient eux-mêmes parfois référence [17]. Or, ces standards, produits par des professionnels de l'informatique, ne procèdent pas du cadre conceptuel établi par les instances de réglementation bancaire et financière. Les concepts de gestion du risque, pour être analogues, ne correspondent pas complètement et ne s'appuient par exemple pas sur le dispositif de contrôle interne.

Ces standards ne s'articulent pas non plus avec le dispositif attendu par les instances de réglementation bancaire et financière pour la gouvernance d'entreprise des établissements. Dorénavant, les autorités de supervision veillent à ce que les établissements n'aient pas un cadre de gestion des risques informatiques entièrement décidé et déployé uniquement par les directions informatiques mais demandent que ce cadre soit correctement intégré au cadre général en vigueur pour le risque opérationnel. Cela doit ainsi conduire les établissements à organiser leur maîtrise du risque informatique selon le modèle dit des « trois lignes de défense » [18]. Dans une telle organisation, la fonction informatique, en charge des différents processus opérationnels liés au système d'information, a la responsabilité en tant que « première ligne de défense » de mettre en œuvre ces processus avec précaution. Elle agit sous le contrôle de la « deuxième ligne de défense », qui est généralement la fonction de gestion des risques, et conformément aux politiques de gestion du risque décidées par celle-ci. Enfin, la fonction d'audit interne agit comme une « troisième ligne de défense » en contrôlant les actions des premières lignes et en évaluant l'efficacité du dispositif de gestion des risques

16 CRR, article 324 : fraude interne ; fraude externe ; pratiques en matière d'emploi et sécurité au travail ; clients, produits et pratiques commerciales ; dommages occasionnés aux actifs matériels ; interruption de l'activité et dysfonctionnement des systèmes ; exécution livraison et gestion des processus.

17 EBA (2011) : « *Guidelines on internal governance* » (GL44), septembre, point E.30.2

18 BCBS (2011) : « *Principles for the sound management of operational risk* », juin, et EBA (2017) : « *Guidelines on internal governance under Directive* 2013/36/EU », septembre.

2 La démarche de définition et de catégorisation du risque informatique au sein de l'ACPR

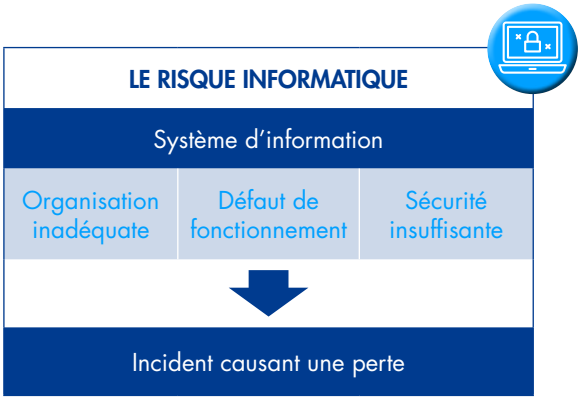
Le secrétariat général de l'ACPR s'est engagé dans des travaux visant à préciser la définition et le traitement du risque informatique. Ces travaux ont été conduits de façon transversale, à la fois pour les secteurs de la banque et de l'assurance, par le réseau des experts informatiques. Ils ont pris la forme d'une définition et d'une catégorisation du risque informatique afin de pouvoir en couvrir l'ensemble des dimensions. Ces éléments ont vocation à contribuer aux réflexions des différentes instances internationales, notamment dans la perspective des travaux du Comité de Bâle sur la révision des principes de saine gestion du risque opérationnel [19] et de la révision des principes de contrôle du secteur de l'assurance (*Insurance Core Principles*) de l'AICA.

Définition du risque informatique

Il est apparu en premier lieu important de disposer d'une définition claire du risque informatique, qui soit à la fois pertinente du point de vue des activités informatiques et aussi des concepts habituels d'analyse du risque opérationnel. Une telle définition n'existe pas encore dans la réglementation des secteurs de la banque et de l'assurance. L'AICA se réfère à une définition des professionnels du secteur de l'assurance (CRO Forum [20]). L'ABE en a adopté une en 2014, dans ses lignes directrices relatives au « processus de surveillance et d'évaluation prudentielle » (*Supervisory Review and Evaluation Process*, SREP) [21], mais celle-ci devrait être complétée, compte tenu de l'évolution des expériences et des connaissances sur ce sujet.

Pour garantir son exhaustivité, la définition élaborée dans ce document vise à couvrir le risque attaché à l'ensemble des processus de gestion du système d'information d'un établissement. Ces processus sont regroupés en trois grands ensembles qui sont l'organisation et la gouvernance, le bon fonctionnement et la qualité, ainsi que la sécurité du système d'information. Le risque informatique est pris en compte globalement, et la définition ne préjuge pas de l'organisation choisie par l'établissement, qui peut consister à confier à la direction informatique la charge tout entière du système d'information, ou à laisser les métiers en gérer directement la partie qui les concerne. Est vue comme un facteur de risque informatique toute sorte de défaillance affectant les processus de gestion du système d'information d'un établissement et qui causerait une perte, directe ou indirecte.

Ainsi, la définition retenue par l'ACPR vise à couvrir toutes les dimensions de risque, y compris celles liées à la gouvernance et à l'organisation du système d'information.



Cette définition est la suivante. **Le « risque informatique » correspond au risque de perte résultant d'une inadéquation ou d'une défaillance des processus d'organisation, de fonctionnement, ou de sécurité du système**

19 BCBS (2011) : « *Principles for the sound management of operational risk* », juin.

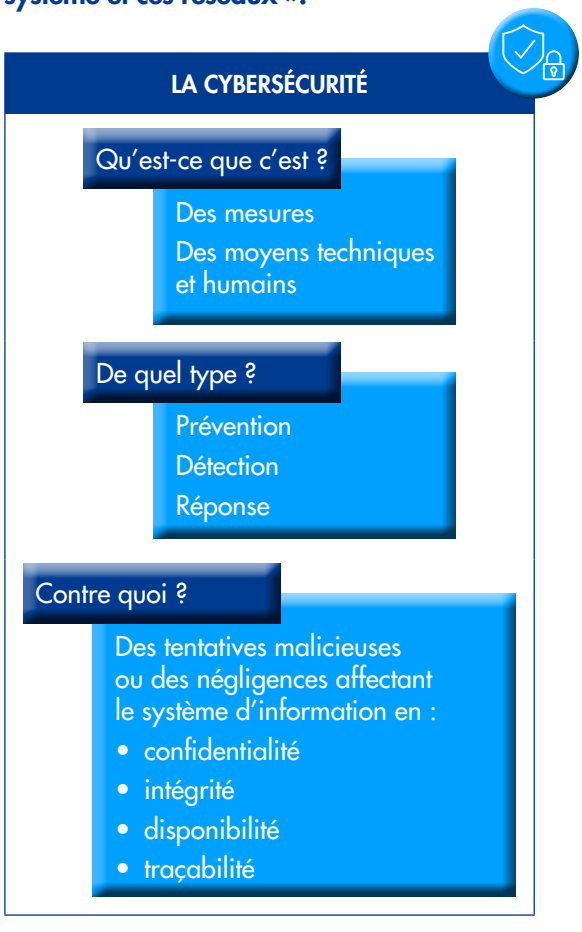
20 « *Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments* ».

21 EBA SREP GL (2014) : « *Information and communication technology (ICT) risk » means the current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which can compromise the availability, integrity, accessibility and security of such infrastructures and of data.*

d'information, entendu comme l'ensemble des équipements systèmes et réseaux, des logiciels et des données, ainsi que des moyens humains contribuant au traitement de l'information de l'institution. La définition s'inscrit dans la logique du risque opérationnel, puisque le risque se matérialise par une perte (ou une quasi-perte, un coût d'opportunité, un gain indu ou des surcharges de coût). Elle ne préjuge pas des causes, c'est-à-dire des facteurs de risque, dont une catégorisation est donnée dans la suite de ce document en suivant les trois processus de gestion du système d'information. Elle n'inclut pas le risque d'image, qui ne lui est pas spécifique, mais, comme pour tout risque opérationnel, le risque informatique peut aussi s'aggraver d'un risque d'image. À dessein, la définition retenue a une portée large, étendue au système d'information dans son ensemble c'est-à-dire à la fois les dispositifs techniques et les moyens d'organisation, ainsi que les ressources humaines intervenant pour le traitement de l'information. Cela permet de neutraliser les variations de vocabulaire (risque du système d'information, risque des « technologies de l'information et de la communication – TIC » ou risque informatique). Pour des raisons de commodité, l'expression usuelle de « risque informatique » est choisie et couvre ces différents vocables. De plus, le système d'information visé par la définition fait référence à ce qui est mis en œuvre par la direction informatique, mais aussi à ce qui est géré en dehors de son contrôle par les métiers utilisateurs et qui est communément appelé « *shadow IT* ».

Cette définition inclut la cybersécurité, mais ne s'y limite pas. En effet, la cybersécurité correspond à une démarche de protection et de réaction face à des attaques touchant tout ou partie du système d'information, et ne traite donc pas l'ensemble des risques informatiques. Ainsi, il y a lieu de positionner la cybersécurité comme une démarche contenue dans le traitement du risque informatique et non l'inverse. Pour ses travaux, l'ACPR utilise la définition de la cybersécurité telle qu'établie par la BCE.

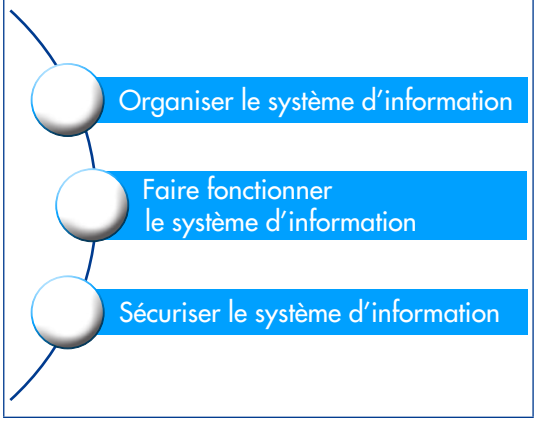
Selon cette définition, **« la cybersécurité est l'ensemble des contrôles et des mesures d'organisation ainsi que des moyens (humains, techniques, etc.) utilisés pour protéger les éléments du système d'information et des réseaux de communication contre toutes attaques logiques, que celles-ci soient conduites par le biais de brèches de sécurité physique ou logique. Ces contrôles et mesures incluent la prévention, la détection et la réponse à toute activité informatique malicieuse ou à toute négligence, qui pourrait affecter la confidentialité, l'intégrité ou la disponibilité des systèmes et des données, de même que la traçabilité des opérations effectuées sur ce système et ces réseaux ».**



Catégorisation du risque informatique

La catégorisation du risque informatique proposée regroupe de manière ordonnée l'ensemble des facteurs de risque identifiés pour les trois macro-processus informatiques, c'est-à-dire l'organisation, le fonctionnement (y compris le développement) et la sécurité du système d'information. Pour chacun de ces trois macro-processus, on identifie des facteurs de risque informatique principaux et secondaires. Ces facteurs peuvent éventuellement se cumuler.

LES PROCESSUS INFORMATIQUES ET LEURS RISQUES



Ceux liés à l'organisation regroupent les situations de décision et de pilotage global insuffisant, pouvant conduire à une mauvaise gestion informatique, à un support insuffisant des besoins des métiers, voire à une mauvaise gestion du risque informatique en général.

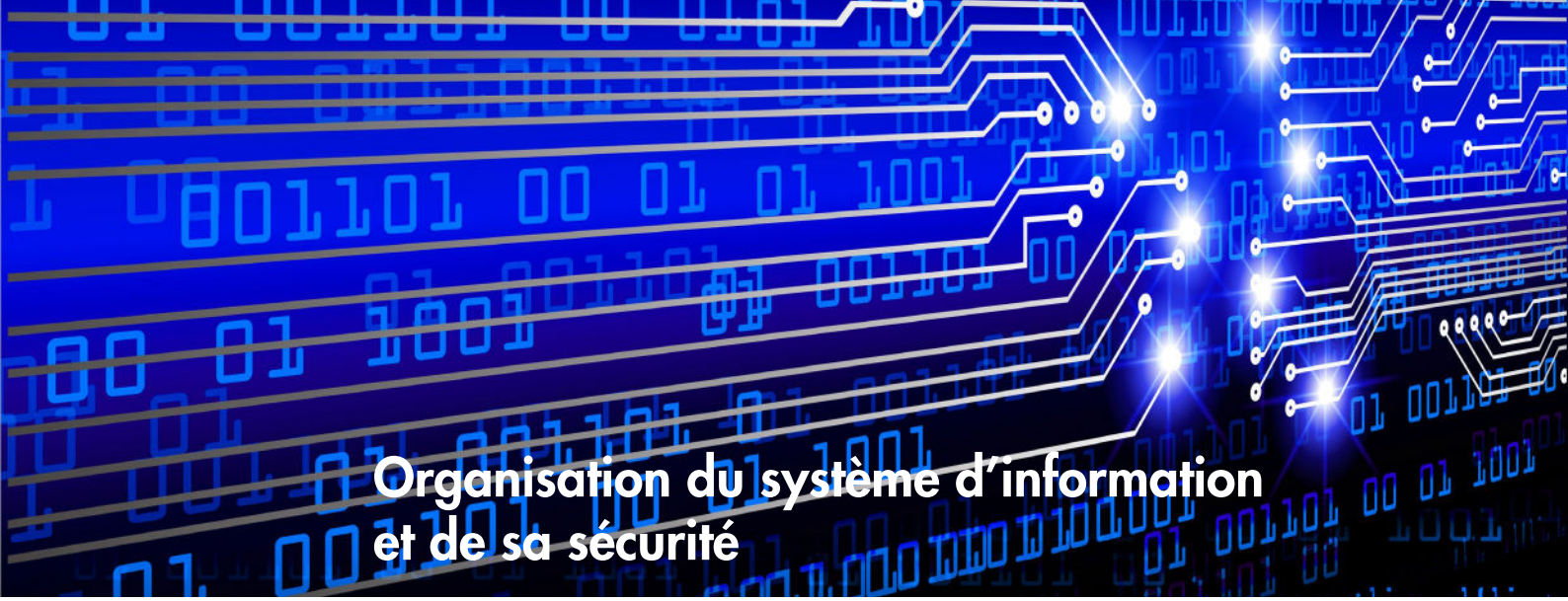
Ceux liés au fonctionnement sont compris au sens large, c'est-à-dire en incluant l'exploitation et les projets, la continuité d'activité et la qualité des données. Ils ont en commun de viser tout ce qui peut porter atteinte au bon fonctionnement du système d'information et altérer ainsi la capacité d'un établissement à réaliser ses activités. En particulier, la catégorisation retient les risques de mauvais pilotage des projets et des changements, d'atteinte à la continuité de l'exploitation, et de qualité insuffisante des données (données relatives aux clients, rapports devant être communiqués au régulateur ou propres aux établissements et n'ayant pas vocation à être diffusés).

Enfin, ceux liés à la sécurité visent en général toutes les atteintes malveillantes à la disponibilité, à la confidentialité et à l'intégrité des données et systèmes gérés par l'établissement. Il s'agit notamment des facteurs de risque liés à la mauvaise identification et protection des actifs du système informatique, ceux liés à des systèmes de détection insuffisants, ou à une capacité de réaction aux attaques trop faible.

La catégorisation ainsi proposée figure en détail en annexe à ce document. Plus granulaire que l'actuelle catégorisation du Comité de Bâle du risque opérationnel, elle a vocation à permettre de la compléter. Les établissements sont libres d'utiliser leur propre catégorisation ou de choisir celle proposée. Dans tous les cas, il convient de couvrir l'entièreté du champ des risques identifiés, sauf à ce que leur organisation ou leur modèle économique ne le justifie pas. À cet égard, il est utile de souligner que lorsque tout ou partie du système d'information d'un établissement est sous-traité, cela ne signifie pas que l'établissement n'est plus exposé à ces risques informatiques. Il doit en conséquence continuer à les identifier et les maîtriser dans le cadre de sa gestion du risque opérationnel et de son dispositif de contrôle interne.

Dans la suite du document, sont exposés les facteurs de risque retenus dans la catégorisation proposée ainsi que les mesures

qui paraissent utiles ou nécessaires à leur maîtrise. Ces facteurs de risque s'entendent comme des événements ou des situations susceptibles d'accroître la probabilité du risque informatique. Les mesures de maîtrise de ces facteurs de risque qui sont indiquées dans la suite du document ne sont bien évidemment pas exhaustives ou impératives. Leur présentation vise avant tout à donner un socle commun de compréhension à tous les établissements de façon à permettre leur bonne maîtrise des risques. Elle peut aussi servir aux services de l'ACPR à contribuer aux travaux des différentes instances internationales auxquelles ils participent.



Organisation du système d'information et de sa sécurité

Ce qui est désigné ici comme l'organisation du système d'information est le macro-processus qui rassemble l'ensemble des actions de décision (parfois désignées comme la « gouvernance »), de pilotage (comme la définition d'une « stratégie » et l'allocation de moyens y afférents), l'allocation des responsabilités au sein de l'entité, ainsi que les politiques et les actions consistant à veiller à la bonne gestion du système d'information (par exemple en réduisant sa complexité), à la maîtrise du recours à l'externalisation, et au respect de la conformité des outils informatiques aux dispositions juridiques que doit respecter l'établissement. Enfin, une organisation saine et prudente fait l'objet d'un dispositif de maîtrise des risques comportant une dimension de contrôle interne. Ces actions d'organisation visent également la sécurité du système d'information.

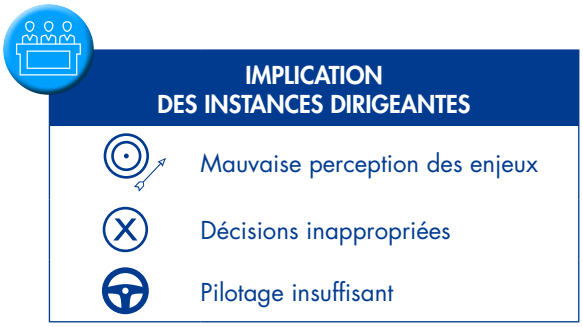
Les paragraphes suivants expliquent les facteurs de risque principaux et secondaires susceptibles d'affecter l'organisation du système d'information et de sa sécurité, ainsi que les principales mesures de maîtrise de ces risques.



1 Implication des instances dirigeantes

En raison de sa technicité, ou pour des raisons culturelles, les instances dirigeantes, entendues à la fois comme les organes exécutifs et délibérants, pourraient se désintéresser de l'activité informatique et préférer se reposer entièrement sur des responsables informatiques [22]. Pourtant, le risque est que ces responsables informatiques perçoivent mal les enjeux de l'entreprise, ou qu'ils soient mal encadrés, et ne délivrent donc pas des services informatiques soutenant l'activité de l'établissement de manière appropriée. Il est donc important que les principes de gouvernance d'entreprise, affirmant la responsabilité des dirigeants et privilégiant des processus de décision clairs et transparents, soient appliqués également aux activités informatiques. Autrement dit, les instances dirigeantes, responsables de la bonne marche de l'établissement, doivent s'impliquer dans les décisions relatives au système d'information et veiller à maîtriser les risques informatiques.

Les experts informatiques de l'ACPR distinguent trois facteurs de risque d'un défaut d'implication des instances dirigeantes.



Mauvaise perception des enjeux

Entretenir et faire évoluer un système d'information nécessitent d'anticiper sur les besoins futurs des métiers et des fonctions de support ou de contrôle, afin que ceux-ci disposent des apports technologiques au moment opportun. La qualité et la maîtrise du système d'information doivent également être des éléments pris en compte dans les choix d'orientation. Une mauvaise perception de l'ensemble de ces enjeux par les instances dirigeantes peut conduire à des retards d'adaptation ou à des situations de perte de maîtrise du système d'information.

Il est donc crucial que les dirigeants exécutifs et les administrateurs comprennent les enjeux liés à l'évolution et la maîtrise de leur système d'information pour la bonne marche de leur établissement. S'ils ne disposent pas de connaissances en la matière, il est important qu'ils y consacrent par exemple des sessions de travail dédiées et entendent des spécialistes internes et externes sur ces sujets.

Décisions inappropriées

La bonne implication des dirigeants suppose qu'ils maîtrisent les décisions relatives aux actions d'entretien et d'évolution du système d'information. À défaut, ces décisions seraient inappropriées et il en résulterait une inadaptation du système d'information.

Sans devoir être partie prenante à toute décision, il importe que les instances dirigeantes procèdent aux arbitrages liés au système d'information. Ces arbitrages devraient reposer sur une solide analyse des risques, établie en cohérence avec le dispositif de gestion des risques et l'appétit au risque qu'ils ont validé. Il paraît essentiel que les décisions majeures relatives au système d'information qui engagent les métiers ou qui pourraient générer un risque significatif, soient prises par la direction générale sous le contrôle de l'organe de surveillance.

22 Et plus largement sur la direction des Systèmes d'information (DSI).

Pilotage insuffisant

Si les instances dirigeantes n'exercent pas de réel suivi du bon fonctionnement et de la sécurité du système d'information de l'établissement, elles seront en difficulté pour agir de manière opportune en cas de dégradation de ceux-ci.

Leur bonne information sur des indicateurs de qualité, de performance, de calendrier des projets et de maintien de la sécurité est donc tout à fait essentielle pour leur permettre d'exercer leurs responsabilités. Le suivi de tels indicateurs n'est pas l'apanage des seuls responsables informatiques. Les instances dirigeantes peuvent bien sûr se concentrer sur le suivi régulier de quelques indicateurs principaux, considérés comme pertinents au regard de la stratégie définie, de la maîtrise des risques ou du suivi de telle ou telle prestation.

2 Alignement de la stratégie informatique avec la stratégie métier

Les technologies de l'information évoluent sans cesse. Ces évolutions peuvent apporter de nouvelles opportunités aux établissements en même temps qu'elles peuvent créer de nouveaux risques. La stratégie informatique, y compris en matière de sécurité, s'inscrit dans la stratégie globale des établissements. Elle vise à satisfaire les besoins des métiers et des fonctions support, mais elle est également de plus en plus au cœur de la stratégie des établissements pour conserver, voire acquérir un avantage compétitif vis-à-vis de la concurrence, par le recours à des évolutions technologiques. Si l'établissement ne définit pas de stratégie informatique ou si celle-ci n'est pas alignée sur les besoins des métiers, le système d'information risque à terme de ne pas répondre aux besoins de l'établissement, ce qui pourrait compromettre la bonne réalisation de ses objectifs commerciaux et financiers. Les facteurs de risque identifiés sont les suivants :

Manque d'anticipation des besoins métier et des évolutions/ enjeux/usages technologiques

Les évolutions informatiques requièrent souvent plusieurs années et doivent être correctement anticipées. À défaut d'être fondé sur une stratégie propre qui combine les différents besoins et prévoit les évolutions technologiques, le développement du système d'information risque d'être erratique, voire de ne pas être capable de soutenir les besoins de l'établissement au moment opportun.

C'est pourquoi il est important que les responsables informatiques formalisent, en accord avec les métiers et sous la validation des instances dirigeantes, une véritable stratégie informatique qui s'intègre dans les objectifs stratégiques de l'établissement. Pour être pertinente, la stratégie informatique anticipe les besoins et les évolutions à moyen terme et fixe des objectifs concrets permettant d'y conduire. Elle résulte normalement d'un processus formalisé, comprenant des consultations des métiers et des fonctions sur leurs besoins, ainsi qu'elle tient compte de la maîtrise des risques informatiques (par exemple ceux relatifs à la complexité, l'obsolescence et la sécurité). Sa mise en œuvre fait ensuite l'objet d'un pilotage fin pour s'assurer de la réalisation des objectifs fixés, anticiper toute difficulté et procéder, le cas échéant, à des ajustements. Il importe aussi de procéder à une actualisation annuelle de la stratégie pour tenir compte des besoins nouveaux. Lorsque l'établissement appartient à un groupe, il importe que sa stratégie soit cohérente avec celle de son groupe de rattachement.

Outils et niveaux de service inadéquats

S'il n'existe pas de stratégie informatique ou si celle-ci n'est pas pertinente, le risque est que les besoins des utilisateurs soient mal pris en compte par la fonction informatique et que l'établissement ne puisse pas exercer son activité de manière optimale.

Il importe donc de tenir compte, dans les éléments stratégiques, des besoins de fonctionnement des utilisateurs, par exemple concernant la disponibilité et la sécurité des environnements. Le document de stratégie n'a évidemment pas vocation à décrire dans le détail des niveaux de service à la manière des documents précis appelés « *service level agreement* » (SLA). Toutefois, il importe de procéder à une analyse globale des besoins de fonctionnement de l'établissement, pour lui-même et pour ses clients et partenaires, de façon à ne pas risquer de pénaliser son activité.

3 Pilotage budgétaire

Le processus budgétaire permet d'allouer les budgets nécessaires à la mise en œuvre de la stratégie informatique validée. Cela intègre les dépenses (matériel, licences, prestations, formation, etc.), les ressources humaines (ressources internes ou externes, y compris de maîtrise d'ouvrage). Un suivi de l'utilisation des enveloppes allouées est ensuite nécessaire pour les ajuster si besoin, ou procéder aux recadrages qui s'imposent. Si le processus d'allocation budgétaire n'est pas clairement défini ou n'existe pas, si le budget n'est pas aligné sur la stratégie préalablement élaborée et/ou si le suivi des dépenses est insuffisamment rigoureux, les moyens financiers disponibles risquent de ne pas être utilisés à bon escient pour mener les changements informatiques attendus.

Alignement insuffisant du budget avec la stratégie

Le budget informatique doit permettre de mettre en œuvre la stratégie informatique validée par l'établissement. S'il est insuffisant ou alloué trop tardivement, la stratégie risque de ne pas être mise en œuvre ou retardée.

Il convient donc de mettre en cohérence les deux processus pour ne pas créer de décalage. Le plus souvent, les deux processus se suivent ou sont associés. Les projets et la maintenance bénéficient chacun pour leur part d'une allocation budgétaire spécifique et bien identifiée, de façon à éviter les effets d'éviction. La disponibilité des ressources doit également correspondre aux étapes de déploiement prévues par la stratégie informatique.

Allocation budgétaire absente ou insuffisamment claire

Si les ressources ne sont pas correctement allouées, la fonction informatique ne pourra pas gérer correctement le système d'information. Un processus documenté, opposable à toutes les directions de l'établissement, y compris en matière de sécurité de l'information, apparaît essentiel pour encadrer l'exercice de préparation et d'allocation des budgets informatiques.

Ce processus inclut l'identification des besoins fonctionnels et techniques liés au parc applicatif, ainsi que ceux liés à l'exploitation du système d'information et à la sécurité de l'information. Compte tenu du cycle de vie des programmes/projets informatiques [23], il importe de combiner : i) une approche pluriannuelle permettant d'allouer des enveloppes globales pour les

23 Un programme désigne ici un ensemble de projets faisant l'objet d'un pilotage commun compte tenu des fortes adhérences entre eux, ce qui n'exclut pas un pilotage individuel de chaque projet.

programmes de grande ampleur et, ii) une approche annuelle pour définir le budget de l'année à venir, constitué à la fois de la quote-part des grands programmes sur l'année considérée et des projets de taille plus modeste, mais jugés prioritaires. Il importe que tous les acteurs concernés soient associés au processus et que les arbitrages ultimes soient opérés par la direction générale.

Suivi des dépenses insuffisant

Le suivi et la maîtrise des coûts informatiques sont des éléments d'optimisation de la rentabilité de l'établissement, nécessaires pour informer les instances dirigeantes de l'avancement et des dépassements des projets et pour procéder aux ajustements nécessaires.

Une maîtrise des budgets repose sur un suivi des dépenses global, normalement exercé par la fonction financière, et un suivi par programme et par projet, tant sur une base annuelle par rapport à l'enveloppe allouée sur l'exercice que sur une base pluriannuelle par rapport à l'enveloppe globale initialement affectée, le cas échéant ajustée depuis le démarrage du programme ou projet. Il importe que les éventuels dépassements budgétaires soient justifiés et validés par la direction générale au-delà d'un certain seuil, ou soient compensés par des arbitrages. L'homogénéité des dispositifs de pilotage des dépenses, de validation des dépassements, d'arbitrage et d'information des instances exécutive et de supervision est garantie par l'existence d'un cadre procédural précis et actualisé.

4 Rôles et responsabilités des fonctions informatique et sécurité de l'information

Tout en exerçant pleinement leur responsabilité sur les questions liées au système d'information et à sa sécurité, les dirigeants exécutifs ont besoin de s'appuyer sur des responsables informatiques et leurs équipes, que l'on désigne dans ce document par les mots « fonction informatique » et « fonction sécurité de l'information ». La bonne organisation du système d'information peut être altérée si ces rôles et responsabilités ne sont pas clairement désignés et répartis, mais aussi si les profils des responsables ne sont pas adaptés et les moyens alloués sont insuffisants.

Rôles et responsabilités mal définis, mal répartis ou mal communiqués

Une répartition claire des attributions de chaque responsable est de nature à faciliter une prise en charge efficiente des activités et éviter les blocages. Comme ils l'ont fait précédemment pour d'autres domaines de l'activité de la banque et de l'assurance (fonction risque, fonction conformité), les superviseurs attendent désormais de plus en plus de pouvoir dialoguer avec des responsables informatiques disposant d'une autorité pleine et entière sur leurs sujets.

Ainsi, la fonction informatique doit pouvoir assurer un pilotage global du système d'information de l'établissement. Habituellement, la DSI rassemble les équipes de développement et de maintenance des applications, ainsi que l'exploitation des infrastructures systèmes et réseaux. Mais, dans certains cas, les métiers ou les fonctions support disposent de leurs propres équipes de développement et de maintenance, voire de production, constituées elles-mêmes en DSI. Il importe alors qu'il y ait un responsable de la fonction informatique au sens large, c'est-à-dire de l'ensemble des équipes, qu'elles soient au sein de la DSI centrale ou des métiers et fonctions. Ce responsable

a toute autorité sur les orientations stratégiques de l'ensemble de la fonction informatique, sur le budget global, sur les normes et procédures destinées à assurer la bonne gestion et la maîtrise des risques du système d'information. Il convient que le responsable de la fonction informatique soit positionné à un niveau suffisamment élevé dans l'organigramme, idéalement avec un rattachement direct aux instances dirigeantes afin que les sujets informatiques soient correctement pris en compte au sein de l'établissement.

La fonction de sécurité de l'information doit également être clairement identifiée et disposer d'une autorité pleine et entière. Confiée à un responsable de la sécurité des systèmes d'information (RSSI), elle consistait initialement à définir la politique de sécurité de l'information, à sensibiliser les équipes à la sécurité et contribuait à la maîtrise des risques, par exemple par la conduite d'études de sécurité ou la réalisation de contrôles de deuxième niveau. Dans ses contrôles, l'ACPR a pu observer que cette fonction était souvent intégrée à la fonction informatique, alors qu'il est préférable qu'elle en soit indépendante pour pouvoir donner des avis sur la sécurité informatique en toute objectivité, ainsi que pour alerter les instances dirigeantes en cas de risque élevé. De même, les contrôles de l'ACPR ont montré que le RSSI n'avait pas toujours un positionnement hiérarchique suffisamment élevé pour lui donner l'autorité suffisante et la capacité à être entendu directement par les instances dirigeantes de l'établissement. Or, l'intensification des risques cyber rend cruciale l'alerte rapide des dirigeants et la fonction devrait être positionnée à un niveau hiérarchique élevé. L'ACPR considère que plutôt que de reposer sur une responsabilité unique, la fonction de sécurité de l'information devrait davantage être structurée selon le modèle des trois « lignes de défense » prôné par les textes internationaux.

Ainsi, les établissements devraient disposer d'équipes en charge de la sécurité des systèmes d'information au sein de la fonction informatique (1re ligne de défense), ayant à identifier les risques et définir en conséquence des procédures de sécurité, puis à en vérifier la mise en œuvre. Ils devraient également disposer au sein de la 2e ligne de défense, dans la fonction de gestion des risques, d'une équipe chargée de la sécurité de l'information afin de proposer aux dirigeants effectifs un niveau de tolérance acceptable à ces risques pour l'établissement, ainsi qu'une stratégie et des politiques de sécurité pour respecter cette tolérance, et de contrôler les vérifications effectuées par la 1re ligne de défense. Disposant de l'indépendance et de la capacité à s'exprimer devant les instances dirigeantes, le responsable de la fonction de gestion des risques devrait pouvoir alerter celles-ci en cas de situation de risque exceptionnel. Il devrait aussi pouvoir délivrer ses avis de façon indépendante et prépondérante vis-à-vis de la fonction informatique et des métiers. Ces deux lignes de défense sont l'objet d'un contrôle périodique par l'audit, disposant d'équipes spécialisées, agissant comme « 3e ligne de défense ». Une telle organisation gagnerait à être appliquée à l'ensemble des risques informatiques tels que décrits dans ce document.

Profils inadaptés ou insuffisants

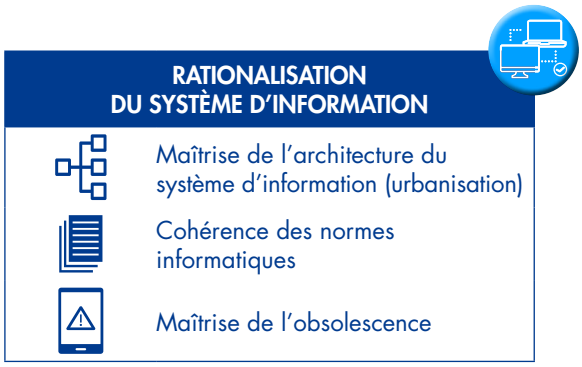
Le choix par les dirigeants exécutifs des principaux responsables au sein des fonctions informatique et de sécurité informatique est crucial pour la bonne organisation du système d'information. Ces fonctions doivent également disposer d'effectifs en nombre suffisant

ayant les compétences requises en les maintenant à jour par des formations, au risque d'être dans l'incapacité de mener leurs actions, ce qui entraverait la bonne marche et la sécurité de l'établissement.

Il importe que le choix des responsables des fonctions informatique et de sécurité informatique repose sur des critères d'expérience et d'expertise professionnelle car ces métiers comportent une forte dimension technique et managériale. Ces enjeux sont valables également pour l'ensemble des collaborateurs informatiques et il est souhaitable de formaliser la politique de gestion des ressources humaines pour ce domaine, précisant la répartition cible des effectifs internes et externes, ainsi que les fonctions clés pour lesquelles il est nécessaire de conserver en interne une expertise suffisante, y compris pour la supervision de fonctions essentielles externalisées. Elle peut être complétée par une politique de gestion des compétences définissant les objectifs de formation du personnel, en particulier via des certifications professionnelles, complétées par des formations aux évolutions technologiques et métier.

5 Rationalisation du système d'information

Au fil du temps, les systèmes d'information se développent de manière significative par la mise en place constante de nouveaux outils et le maintien, parfois partiel, des anciens. Aujourd'hui, les systèmes d'information des établissements des secteurs de la banque et de l'assurance sont constitués de vastes ensembles d'applications, systèmes et réseaux qui sont parfois difficiles à représenter en raison de leur complexité. Les facteurs de risque d'une perte de maîtrise du système d'information sont variés. Il peut s'agir d'un manque de maîtrise de l'architecture du système d'information, ou encore d'une incohérence des normes informatiques, d'un défaut de gestion de l'obsolescence.



Manque de maîtrise de l'architecture du système d'information (urbanisation)

Lorsque le système d'information devient très développé, une démarche d'architecture, parfois appelée « urbanisation » s'impose pour éviter une croissance anarchique non maîtrisable. Le principe est similaire à celui du développement des grandes villes. Les applications et systèmes fonctionnant ensemble sont regroupés de manière à simplifier et mieux maîtriser leurs interactions. Ces travaux reposent généralement sur une cartographie et un inventaire des composants du système d'information. Les architectes applicatifs et système sont chargés de veiller à ne pas multiplier les composants du système d'information de manière désordonnée. Ils peuvent identifier des zones de fragilité et préconiser une optimisation du système d'information et de son évolution.

Incohérence des normes informatiques

Un développement non-maîtrisé du système d'information peut apparaître lorsque l'action des développeurs et des

ingénieurs systèmes n'est pas suffisamment cadrée par des normes de conception, de développement et de production, voire aussi de sécurité. Ces normes visent à unifier les pratiques et à interdire le recours à des solutions non approuvées au sein de l'établissement. Il en existe pour les différents domaines d'activité : le développement d'applications, la production et la mise en œuvre des solutions réseaux. Pour jouer pleinement leur rôle, ces normes doivent être unifiées par la fonction informatique centrale de façon à éviter des pratiques hétérogènes ou incohérentes entre les différentes entités composant la fonction informatique (par exemple entre les DSI de différentes filiales au sein d'un groupe).

Défaut de maîtrise de l'obsolescence

Les technologies informatiques évoluent vite et doivent constamment être mises à jour pour éviter de faire courir le risque que le système d'information ne soit plus maintenu. Cette contrainte est très forte car elle requiert une attention élevée aux changements fréquents de versions de logiciels et de systèmes employés, ce qui suppose par exemple une gestion attentive d'inventaire. Plus fondamentalement, elle doit conduire les établissements à renouveler régulièrement les applications qui utilisent des langages de programmation anciens qui ne seraient plus connus des développeurs. Les contraintes de sécurité peuvent également justifier de mettre à jour régulièrement les technologies utilisées.

6 Maîtrise de l'externalisation

Parce que les établissements peuvent avoir besoin d'un savoir-faire ou d'une main d'œuvre qu'ils n'ont pas, les activités informatiques sont souvent confiées à des prestataires, qui peuvent appartenir au même groupe que l'établissement, ou être des sociétés tierces. Des risques de maîtrise insuffisante des activités externalisées existent si le cadre contractuel est mal défini, si la dépendance vis-à-vis du fournisseur n'est pas maîtrisée, si les niveaux de service attendus ne sont pas rigoureusement suivis et si les changements de fournisseurs ne sont pas correctement anticipés pour activer les dispositifs de réversibilité contractuels.

Cadre contractuel inadapté

Un cadre contractuel inadapté, c'est-à-dire inexistant, incomplet ou invalide, déséquilibré ou imprécis, peut mettre l'établissement en situation de ne pouvoir obtenir la prestation attendue, et donc peut-être altérer le bon fonctionnement ou la sécurité de son système d'information.

Les instances dirigeantes valident les projets importants d'externalisation en s'appuyant sur les avis des différentes fonctions de contrôle, y compris de la fonction de sécurité informatique. Le contrat et ses documents liés font référence pour définir les droits et obligations de l'établissement et du prestataire. Il est naturellement requis, même en cas d'externalisation au sein du même groupe. Il importe que le contrat détaille la nature de la prestation, les niveaux de service attendus, les contrôles permanents à effectuer, les modalités de traitement des incidents et de continuité d'activité, les besoins en matière de sécurité informatique, les conditions de réversibilité du contrat, ainsi que les rôles et responsabilités des contractants, les interlocuteurs en charge du suivi courant de la prestation, les instances de pilotage de la relation et la nature

des informations devant faire l'objet d'une information régulière de l'établissement. La sous-traitance en chaîne doit être connue, voire autorisée, par l'établissement qui doit s'assurer qu'elle ne crée pas de risque. En outre, ce dernier s'assure que le contrat inclut un droit d'audit de la prestation, et le cas échéant d'accès au site, et décrit les dispositions réglementaires qui s'imposent au prestataire. Ce droit d'audit ne doit pas être contraint par des clauses restrictives (long préavis, limitations diverses). Le contrat doit prévoir également ce droit pour les autorités de supervision de l'établissement. Des clauses types, validées par les services juridiques de l'établissement, peuvent utilement être établies pour permettre à l'établissement de toujours disposer de contrats conformes à la réglementation sur l'externalisation et préservant de manière équilibrée ses intérêts.

Dépendance forte

Lorsqu'un prestataire devient prépondérant par l'importance des activités informatiques qu'il prend en charge pour un établissement, ce dernier peut avoir des difficultés à imposer ses conditions, même en cas de dégradation de la prestation. L'externalisation à des prestataires situés à l'étranger, surtout hors du territoire européen, peut exposer un établissement à un environnement juridique mal maîtrisé.

L'élaboration d'une politique d'externalisation, soumise à la validation des instances dirigeantes, permet de définir les activités que l'établissement accepte d'externaliser et celles dont la sensibilité justifie un maintien en interne. Cette politique doit mesurer les risques juridiques liés à l'externalisation dans des juridictions étrangères, surtout hors Union européenne (par exemple quant aux règles relatives à la protection des données). La maîtrise du risque de dépendance vis-à-vis d'un ou de plusieurs fournisseurs suppose la mise en place d'un pilotage consolidé des contrats négociés avec les fournisseurs et l'implication de la direction générale dans la validation des activités externalisées au-delà de seuils de dépendance à définir. Il convient également que la politique d'externalisation détaille les conditions d'externalisation (rôles et responsabilités, processus de recherche et de sélection d'un prestataire, cadre contractuel, modalités de pilotage de la prestation).

Suivi insuffisant du respect des niveaux de service

Les niveaux de service correspondent à des engagements contractuels du prestataire vis-à-vis de l'établissement concernant la qualité et la sécurité des services informatiques. S'ils ne sont pas fixés ou si les niveaux de performance attendus sont trop bas, l'établissement ne sera pas en mesure d'exiger une prestation de bon niveau.

Il est donc essentiel que les niveaux de service soient définis contractuellement et fassent l'objet d'un suivi permanent par une équipe dédiée de l'établissement, tant via l'analyse des tableaux de bord mis en place en accord avec le fournisseur que par le traitement des événements enregistrés, qui donnent le cas échéant lieu à la définition de plans d'action. Ce dispositif est plus efficace lorsque des comités de pilotage conjoints entre l'établissement et le fournisseur permettent de veiller à la qualité de la prestation fournie. Il est souhaitable que le comité de pilotage soit présidé par un responsable dont le niveau hiérarchique est défini en fonction de la sensibilité de l'activité externalisée.

Pour les activités les plus sensibles, il peut être utile que cette instance soit présidée par le responsable de la fonction informatique, voire par la direction générale. En complément, la tenue de comités techniques à un niveau hiérarchique suffisant peut s'avérer utile. Enfin, il est nécessaire d'instaurer un processus d'escalade auprès de la fonction informatique ou de la direction générale en cas de dégradation de la qualité de service ou de la relation d'affaires.

Dispositif de réversibilité insuffisant

Le changement de fournisseur dans le domaine informatique est relativement complexe puisqu'il nécessite le plus souvent la reprise de l'existant, la garantie de continuité d'activité pour les utilisateurs avec des niveaux de service équivalents et la reprise de l'archivage sur une période longue.

Il importe donc que ce processus soit correctement anticipé, en tenant compte des contraintes budgétaires, en respectant le calendrier d'activation de la clause de réversibilité avec le fournisseur sortant et en définissant avec précision les travaux à mener. Certains seront repris par un nouveau fournisseur, ou par l'établissement en cas d'internalisation de la prestation, tandis que d'autres devront faire l'objet d'un traitement spécifique, par exemple sous la forme d'un projet à budgéter et planifier.

7 Respect des lois et règlements

Comme toute entreprise, les établissements doivent se conformer au droit régissant leur activité. En termes d'organisation, les solutions informatiques qu'ils utilisent ne peuvent donc être réalisées par les informaticiens de manière autonome et sans considération de l'environnement juridique auquel est soumis l'établissement. En effet, celui-ci risquerait d'être en situation d'infraction au droit applicable à ses activités, ce qui est inacceptable et peut en outre être très préjudiciable à ses relations avec la clientèle. La conformité du système d'information peut être altérée si l'expression des besoins des métiers ne respecte pas le droit applicable, ou si les développements informatiques ne respectent pas les préconisations juridiques demandées par les métiers, ou encore si les normes ou les techniques de production ne permettent pas de respecter le droit applicable.

Non-conformité des besoins des métiers au droit applicable

Les utilisateurs ont la responsabilité de définir leurs besoins en termes de système d'information. S'ils ne veillent pas à se conformer aux prescriptions juridiques applicables à leur activité, l'expression de leurs besoins pourra comporter des éléments non conformes qui seront ensuite mis en œuvre dans le système d'information et placeront l'établissement dans une situation de non-conformité juridique.

La prévention d'un tel risque suppose que la méthodologie de conduite de projet intègre une phase de vérification de la conformité de l'expression des besoins des métiers aux prescriptions juridiques qui s'imposent à l'établissement, ainsi qu'à ses procédures internes lorsqu'elles sont par exemple plus strictes. La direction juridique est normalement consultée pour donner son accord aux besoins formulés.

Non-conformité du système d'information aux préconisations juridiques des métiers

Les informaticiens doivent en principe se conformer aux besoins exprimés par les utilisateurs, et donc intégrer les dispositions juridiques applicables à l'activité si elles ont été correctement formulées. S'ils ne le font pas, l'établissement serait doté d'un système d'information non conforme. De même, les prescriptions juridiques peuvent évoluer au fil du temps et rendre le système d'information non conforme.

Il importe donc que toute modification du système d'information inclue des vérifications préalables et continues de la conformité au droit applicable à l'établissement, et que les manquements éventuels soient identifiés et corrigés. Ceci s'applique aussi bien aux logiciels ou services conçus en interne, qu'à ceux acquis ou loués à des prestataires externes. Les changements importants du droit applicable doivent faire l'objet de demandes d'évolution de la part des utilisateurs responsables des traitements et être mis en œuvre par les informaticiens.

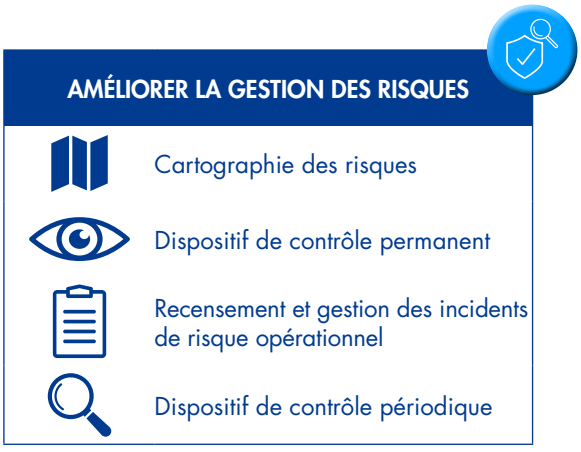
Incompatibilité des normes informatiques avec le droit applicable

Les normes informatiques, qui gouvernent les règles de programmation et d'exploitation, pourraient comporter des éléments empêchant un établissement de se conformer à ses obligations, par exemple en termes de protection des données personnelles ou de durée de sauvegarde. Ces normes ne devraient pas empêcher de respecter les besoins exprimés par les utilisateurs. Elles devraient être régulièrement adaptées à ces obligations.

Pour se prémunir contre de telles situations, l'établissement doit vérifier régulièrement la conformité de ses normes au droit applicable à son activité.

8 Gestion des risques

LLes instances dirigeantes doivent pouvoir s'appuyer sur un dispositif de gestion des risques opérationnels efficace et qui couvre l'ensemble des risques informatiques. Conformément à la réglementation, ce dispositif repose sur une cartographie et une évaluation régulière des risques, mais aussi sur des mesures de maîtrise et de suivi des risques. Au titre de ces mesures de maîtrise, il inclut un contrôle interne comportant plusieurs niveaux indépendants pour permettre des contre-vérifications. Si le dispositif de gestion du risque opérationnel prenait mal en compte les risques informatiques, il ne serait pas complet et conforme aux obligations réglementaires. Il ne refléterait pas l'entièreté des risques auxquels l'établissement est exposé et l'identification et la maîtrise des risques informatiques ne seraient pas correctement mises en œuvre. Cela pourrait se manifester par une cartographie inexistante ou partielle, ou par un dispositif de contrôle permanent insuffisant, ou une prise en compte imparfaite des incidents, ou enfin par un contrôle périodique insuffisant.



Cartographie des risques inexistante ou partielle

L'identification des risques informatiques et leur évaluation régulière sont un préalable à l'adoption de mesures de maîtrise des risques. À défaut, celles-ci peuvent manquer ou se révéler inappropriées, plaçant dès lors l'établissement en situation d'impréparation et donc en risque plus élevé.

Il est essentiel que l'établissement identifie et définisse une cotation de ses risques informatiques inhérents et résiduels, tant au sein des métiers que des fonctions support, y compris la direction informatique. Il apparaît nécessaire que ce recensement porte sur l'ensemble des actifs physiques (centres informatiques, bureaux, agences, etc.) et logiques (banque en ligne ou sur *smartphone*, *cloud*, etc.), des activités (métier ou support), des publics (salariés, clients, prestataires, partenaires) et des outils (applications, réseaux, etc.), et soit cohérent avec l'appétit au risque de l'établissement validé par les instances dirigeantes. Il est important d'inclure dans cette cartographie les liens possibles avec les clients, prestataires et partenaires pour tenir compte des risques de contagion d'un évènement de risque. L'élaboration d'une cartographie des processus des métiers et des fonctions support constitue un préalable à l'identification et l'actualisation au moins annuelle de ces risques. Il importe que la cartographie des processus et des risques, idéalement informatisée pour en faciliter la mise à jour, la consolidation et l'exploitation, s'accompagne de la définition de mesures de réduction des risques, qu'elles soient organisationnelles, techniques ou reposent sur des contrôles. En complément, il convient d'identifier les risques de nature transversale et de les inclure dans les cartographies de chaque activité. La définition des responsabilités entre la fonction informatique et les autres activités est également essentielle dans la mesure où certains risques informatiques sont subis par les métiers ou fonctions support, alors que leur traitement relève de la fonction informatique.

Défaut dans l'analyse de risque

Une analyse des risques informatiques, y compris ceux relatifs à la sécurité, doit normalement précéder l'adoption de nouveaux produits, l'engagement de nouvelles activités, tout projet informatique, ou encore le recours à des prestations externalisées. Celle-ci est cruciale pour éviter à l'établissement de s'engager dans une situation non maîtrisée. Cette analyse concourt à la bonne information des instances dirigeantes afin d'éclairer leur prise de décision. Pratiquée habituellement sur les sujets liés à la sécurité des systèmes d'information, l'analyse de risque a vocation à s'appliquer à l'ensemble des sujets de risque informatique tels que les reconnaît l'ACPR.

En complément des analyses éventuelles faites par la fonction informatique, il importe que la fonction de gestion des risques formule un avis préalable avant l'adoption, par les métiers utilisateurs ou par la fonction informatique, de nouveaux produits, projets ou activités impliquant le système d'information. Agissant pour la maîtrise des risques informatiques, y compris ceux relatifs à la sécurité du système d'information, la fonction de gestion des risques délivre un avis indépendant. Celui-ci doit avoir une valeur suffisamment contraignante pour pouvoir éviter l'engagement dans des situations porteuses d'un niveau de risque

élevé pour l'établissement, sa clientèle ou ses partenaires. Un processus d'arbitrage par les instances dirigeantes doit pouvoir être actionné en cas de désaccord du métier ou de la fonction informatique sur l'avis remis par les fonctions de contrôle. Les conditions formulées par ces fonctions de contrôle sont tracées à des fins de suivies et leur levée procède d'un examen attentif des mesures de réduction de risque mises en œuvre.

Dispositif de contrôle permanent insuffisant

Un dispositif de contrôle permanent comportant deux niveaux indépendants de contrôle est destiné à éviter des situations de risque. Ce contrôle permanent a vocation à englober les différents processus de mise en œuvre et de gestion du système d'information pour éviter que ceux-ci fassent l'objet de défaillances qui ne seraient pas détectées à temps.

Il importe que le contrôle permanent des risques informatiques, y compris de sécurité de l'information, s'insère dans le plan de contrôle permanent de l'entreprise. Ce plan doit couvrir l'ensemble des risques identifiés et être actualisé périodiquement. Le contrôle de premier niveau est assuré par les opérationnels de la fonction informatique constituant la « première ligne de défense ». Le contrôle de deuxième niveau est réalisé par des équipes de la fonction de gestion des risques, indépendantes de la fonction informatique, constituant la « deuxième ligne de défense ». La périodicité des contrôles, a minima annuelle, est adaptée au niveau de risque. Des plans d'action sont initiés pour pallier les insuffisances relevées lors des contrôles. Un outil recense le plan de contrôles et les résultats des contrôles afin d'en faciliter le suivi et l'information des instances dirigeantes.

Recensement et gestion insuffisants des incidents de risque opérationnel

Le suivi des incidents de risque opérationnel sert à mesurer les pertes d'un établissement et à mettre en place des mesures palliatives. Les incidents informatiques ont vocation à être recensés à ce titre s'ils rentrent dans les critères de définition du risque opérationnel [24]. Si les incidents informatiques, y compris de sécurité, ne sont pas inclus dans le suivi du risque opérationnel, celui-ci sera évalué de manière incomplète. Ceci pourrait altérer la qualité des mesures de réduction du risque et fausser le montant des fonds propres retenus pour y faire face.

Ainsi, il est attendu d'intégrer dans la base des incidents opérationnels tous les incidents informatiques qui en respectent les critères. Si besoin, un seuil de déclaration des incidents peut être défini, mais il importe qu'il soit suffisamment bas pour pouvoir recenser les incidents significatifs. Le recensement agrégé d'incidents similaires multiples de faible ampleur est une bonne pratique permettant d'identifier et de corriger certains dysfonctionnements avant la survenance d'un incident majeur. De plus, il importe que ces incidents donnent lieu à des plans d'action et qu'une information sur les incidents les plus significatifs et les plans d'action associés soit adressée régulièrement aux instances dirigeantes.

Dispositif de contrôle périodique insuffisant

Le contrôle périodique de l'établissement agit comme troisième niveau de contrôle sur l'ensemble des processus mis en œuvre. S'il n'inclut pas complètement les processus

24 Générer un gain ou une perte financière, matérialisé(e) ou non (manque à gagner, quasi-perte), ou non financière (par exemple, jours/hommes consacrés au rétablissement du service après une panne informatique).

relatifs au système d'information, les instances dirigeantes pourraient ne pas disposer d'informations indépendantes sur l'état des risques et des mesures de remédiation mises en œuvre en la matière.

Il est donc essentiel que les risques informatiques, y compris en matière de sécurité de l'information, soient couverts par le plan d'audit de l'établissement et traités par des auditeurs spécifiquement formés, soit dans le cadre de missions générales, soit à l'occasion de missions dédiées. Il convient également que les constats donnent lieu à l'émission de recommandations suivies de plans d'action, dont les plus critiques sont validés et suivis par la direction générale. Les instances dirigeantes doivent disposer des informations suffisantes, régulièrement actualisées, sur les risques informatiques évalués par le contrôle périodique.

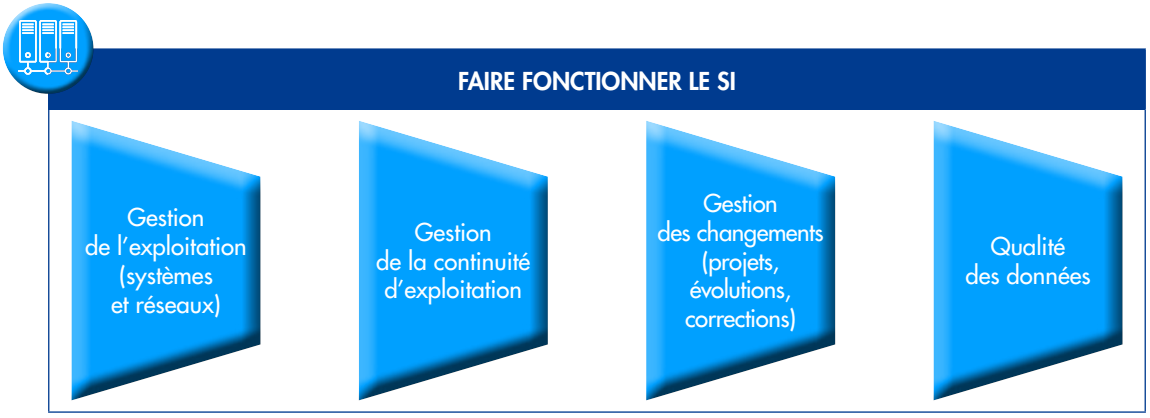


Fonctionnement du système d'information

Cette partie traite des risques portant sur le macro-processus « fonctionnement du système d'information », qui comprend l'ensemble des actions d'utilisation et d'exploitation du système en place, mais aussi les actions d'évolution pour des nouveaux services ou équipements (projets), ou plus simplement pour des corrections ou des changements modérés (maintenance corrective et évolutive). La conduite opérationnelle des services existants est parfois appelée « *run* » et la délivrance de nouveaux services (projet applicatif, installation d'infrastructures) parfois appelée « *change* ».

Dans l'ensemble de ces actions, c'est le bon fonctionnement du système d'information installé qui est en jeu, c'est-à-dire le fait de rendre le service attendu par les utilisateurs, notamment en termes de qualité, de fiabilité et de disponibilité. Les mêmes enjeux s'appliquent aux actions de « *change* », pour lesquelles le risque est de ne pas réussir à fournir correctement les services attendus. Une attention particulière est également apportée depuis quelques années à la qualité des données.

Les paragraphes suivants expliquent les facteurs de risque principaux et secondaires susceptibles de créer des perturbations dans les processus d'exploitation, de gestion de la continuité, de gestion des changements et de qualité des données. Les principales mesures de maîtrise de ces risques sont également indiquées.



1 Gestion de l'exploitation (systèmes et réseaux)

L'exploitation informatique, encore appelée « production », consiste à faire fonctionner les ordinateurs sur lesquels sont installées les applications. Ces ordinateurs, ainsi que leurs équipements de connexion, sont appelés environnements systèmes et réseaux. Une gestion déficiente de l'exploitation de ces systèmes et réseaux peut causer des perturbations plus ou moins graves, susceptibles d'altérer la qualité du service rendu aux utilisateurs.

Les experts informatiques de l'ACPR distinguent plusieurs facteurs de risques pouvant entraîner une mauvaise gestion de l'exploitation. Il peut s'agir d'insuffisances affectant les moyens de production, le processus de détection des erreurs et anomalies, ou de résolution des incidents et des problèmes. Il s'agit aussi du risque de non-respect des niveaux de service attendus par les utilisateurs.

Insuffisance des moyens de production

Les moyens de production fournissent les ressources nécessaires au bon fonctionnement du système d'information. S'ils ne sont pas correctement dimensionnés, par exemple avec des équipements suffisants en nombre et en puissance, le système d'information risque de ne pas pouvoir bien fonctionner, notamment en période de pic d'activité. De même, si les configurations de ces équipements ne sont pas à jour ou ne sont pas adaptées aux besoins, des perturbations peuvent apparaître ou la sécurité être altérée.

Il importe donc que le choix des matériels pour constituer l'environnement d'exploitation soit correctement apprécié avant de mettre en production des nouvelles solutions. Les caractéristiques techniques et notamment la puissance du matériel doivent être adaptées aux besoins de fonctionnement dictés par les niveaux de service attendus par les utilisateurs. Ensuite, la capacité des ressources utilisées doit être surveillée pour permettre leur augmentation suffisamment à l'avance et ne pas compromettre la croissance de l'usage du système d'information (nombre d'utilisateurs pouvant se connecter, puissance de calcul, espace de stockage par exemple).

La bonne gestion des moyens de production repose sur des inventaires à jour. La gestion des inventaires consiste à référencer et à centraliser l'ensemble des matériels et logiciels du système d'information, pour disposer d'une vision complète et vérifier l'adéquation des équipements installés avec les besoins identifiés. Les détails associés à chaque équipement sont décrits, notamment les numéros de version, les licences installées, les spécificités techniques des différents composants. Ainsi, la conformité aux standards techniques est facilitée et la gestion de l'obsolescence des composants en fin de vie est optimisée.

Insuffisance dans la détection des erreurs ou anomalies

Les erreurs ou anomalies de traitement perturbent le bon fonctionnement du système d'information en altérant sa disponibilité (retards, arrêts) ou la qualité des données. Leur détection rapide est donc cruciale.

Les actions de détection sont une des tâches premières du personnel d'exploitation en charge du suivi de la production. Ils peuvent de plus en plus s'appuyer sur des outils de détection, répertoriant par exemple des anomalies déjà rencontrées, afin de bénéficier d'une surveillance plus automatique. Des équipes spécialisées peuvent également être

en charge de ces actions pour une meilleure capacité de réaction. Il est préférable que les outils de détection des erreurs soient installés à différents niveaux du système d'information pour permettent d'identifier tous types de dysfonctionnements techniques, avant même la survenance d'un incident. Ainsi, repérer des temps de réponse anormalement longs permet d'anticiper une interruption du système d'information. Les outils de détection doivent couvrir l'ensemble des équipements afin de garantir un pilotage exhaustif.

Insuffisance dans la gestion des incidents et des problèmes

Une fois détectés, les incidents [25] sont gérés afin de restaurer aussi vite que possible le bon fonctionnement du système d'information et minimiser les interruptions de service. Complémentaire à la gestion des incidents, la gestion des problèmes [26] consiste à diagnostiquer la cause d'incidents répétitifs ou difficiles à résoudre, à mettre en place les mesures pour éviter leur réapparition et à minimiser l'incidence de ceux qui ne peuvent être évités. L'efficacité de ces deux processus est donc essentielle pour minimiser les dégradations de service et la perte de confiance des utilisateurs.

Ces processus gagnent à être formalisés par des procédures opérationnelles. Les différentes étapes de traitement des incidents et des problèmes, depuis leur identification à leur résolution, font appel à des équipes spécialisées et sont tracées pour vérifier leur bon achèvement. Un échelonnage selon le niveau de sensibilité permet d'affecter des priorités. La gestion des problèmes est étroitement liée à la gestion des incidents, avec des outils, des critères de catégorisation et de priorité similaires. La résolution est généralement facilitée par l'existence de cartographies et d'inventaires des installations, des flux d'informations et des services critiques. La résolution des incidents et problèmes est suivie par des comités chargés de surveiller la qualité du service. Elle fait l'objet de rapports synthétiques aux instances dirigeantes pour permettre la bonne mobilisation des équipes et l'allocation de moyens suffisants.

Non-respect des niveaux de service

Les niveaux de service définissent les attentes des utilisateurs en termes de fonctionnement du système d'information (plages d'ouverture, délais d'interruption possible, rythme des sauvegardes, passage en secours notamment). Il en existe pour les conditions d'exploitation et, plus largement, pour la performance globale du service. Indépendamment de tout incident ou problème, ou même d'une mauvaise configuration du matériel, une mauvaise gestion de l'exploitation peut se caractériser par l'incapacité des administrateurs des systèmes et réseaux à tenir les engagements envers les utilisateurs.

Les traitements d'exploitation des systèmes et réseau sont normalement formalisés par des procédures opérationnelles permettant aux administrateurs des plates-formes de suivre de manière rigoureuse les différentes opérations en situation de service normal et de service dégradé. Par ailleurs, il importe que les niveaux de service soient formalisés dans des conventions de service avec les métiers utilisateurs. Celles-ci précisent les critères de suivi et le niveau de satisfaction attendu pour ces services, à la fois pour la qualité du service et sa disponibilité. La contractualisation des niveaux de service attendus est utile pour mesurer l'atteinte des besoins des utilisateurs. Des indicateurs permettent de suivre les engagements et de prendre des actions de correction.

25 Au sens du référentiel ITIL (*Information Technology Infrastructure Library*), un incident est compris comme « une interruption non prévue d'un service des technologies de l'information (TI) ou une réduction de la qualité d'un service des TI ».

26 Au sens du référentiel ITIL, un problème est la cause d'un incident.

2 Gestion de la continuité informatique

La continuité informatique désigne les mesures et moyens mis en œuvre pour garantir la disponibilité du système d'information selon les besoins exprimés par les utilisateurs au titre de la « continuité d'activité ». Les services fonctionnent généralement selon des plages d'ouverture qui varient selon la nature des activités, sauf dans certains cas où aucune interruption n'est tolérée. En tout état de cause, l'exploitation doit garantir une disponibilité parfaite des systèmes et réseaux pendant les plages d'ouverture pour que les applications puissent fonctionner et disposer de bons temps de réponse. À défaut, le système est indisponible ou sujet à des ralentissements et l'activité des utilisateurs est perturbée.

Les risques d'indisponibilité du système d'information peuvent survenir lorsque l'établissement n'a pas une bonne organisation en place pour gérer son dispositif de continuité d'activité, ou lorsqu'il n'a pas correctement identifié les différents scénarios d'indisponibilité, lorsque les moyens de production ou de secours sont insuffisamment protégés contre les accidents, ou lorsque son dispositif de continuité informatique est insuffisant ou ne correspond pas avec celui prévu pour les utilisateurs, ou enfin lorsqu'il n'est pas suffisamment testé.

Mauvaise organisation de la continuité

Les établissements doivent s'être organisés pour gérer leur dispositif de continuité d'activité, qui répond à des obligations réglementaires. Ce dispositif est double et comprend un volet propre à la poursuite de l'activité des utilisateurs (locaux de repli) et un volet de secours informatique (passage sur site de secours). Ce dispositif comporte une description des actions à mener pour assurer la continuité des processus métiers considérés comme essentiels, et les moyens nécessaires à mettre en œuvre en cas de crise. Cela permet de réduire le risque d'interruption d'activité ou de dysfonctionnements du système d'information à un niveau acceptable pour l'établissement. Si l'organisation mise en œuvre n'est pas adéquate, l'établissement risque de ne pas pouvoir réellement disposer de moyens de secours en cas de panne de ses équipements principaux.

Il importe donc que l'organisation mise en œuvre pour gérer la continuité d'activité s'appuie sur des politiques et des procédures formalisées de coordination, de pilotage, et de prise de décision. Cela suppose que les rôles et les responsabilités pour les situations de gestion de crise soient clairement définis. L'implication et la validation des dirigeants garantissent l'alignement de la continuité avec la stratégie, la mise à disposition de moyens budgétaires et humains suffisants, l'engagement des salariés et de leur encadrement. Une méthodologie, une structure de gestion de crise efficace et une politique de communication adaptée complètent normalement le dispositif. L'établissement dispose d'un plan de continuité qui comporte un plan de secours informatique (PSI).

Insuffisance dans l'identification des scénarios d'indisponibilité

Les plans de continuité sont normalement fondés sur des scénarios de perte de ressources, comprenant des dysfonctionnements de systèmes et de réseaux pour des durées plus ou moins longues. Le PSI a vocation à décrire les modalités d'activation des moyens de secours selon ces différents scénarios. Si les scénarios définis n'identifient pas l'ensemble des perturbations possibles ou en

évaluent mal les conséquences, le dispositif de gestion de la continuité risque de mal répondre à une situation de panne imprévue, ce qui empêchera les utilisateurs de pouvoir continuer leur activité.

Pour s'en prémunir, il convient de réaliser des analyses d'impact pour les métiers utilisateurs (notamment sur les plans réglementaire, juridique, commercial, financier ou de réputation) selon différents scénarios d'indisponibilité des locaux, des systèmes d'information, du personnel, de l'énergie et des télécommunications et des fournisseurs clés. Ces analyses d'impact permettent de définir la « durée maximale d'interruption admissible » (DMIA) et la durée de « perte de données maximale admissible » (PDMA). Sur cette base, des objectifs sont fixés aux équipes de production en termes de délai maximal de reprise (« *recovery time objective* » – RTO) et de durée maximale admise entre un incident et la date de sauvegarde des données la plus récente (« *recovery point objective* » – RPO).

Non-alignement de la continuité informatique avec la continuité métier

Le plan de secours informatique décrit les modalités de continuité pour la production informatique. Il s'insère dans le plan de continuité global de l'établissement qui décrit par ailleurs les moyens de repli pour les utilisateurs. Le PSI doit donc être cohérent avec le plan de continuité sinon le risque est qu'il ne soit pas suffisant pour permettre la continuité des applications essentielles ou critiques.

Pour éviter tout écart conduisant à une inadéquation des moyens de secours informatiques, le PSI doit découler d'analyses d'impact sur les métiers utilisateurs, et les délais de rétablissement du service (exprimés en RTO et RPO) doivent correspondre aux DMIA et PDMA définis par eux. Les écarts qui résulteraient d'une incapacité connue des moyens de secours doivent être portés à la connaissance des instances dirigeantes pour un éventuel arbitrage sur les besoins utilisateurs ou l'allocation de moyens supplémentaires.

Protection insuffisante des moyens de production et de secours contre les accidents

Les centres informatiques sont particulièrement exposés aux accidents et détériorations pouvant affecter le matériel et ainsi provoquer des perturbations pour le bon fonctionnement du système d'information. Ces sites sont très dépendants en électricité pour alimenter les matériels, et aussi en eau pour la climatisation. Toutes sortes d'accidents ou d'évènements naturels peuvent sévèrement les affecter (incendie, inondation, tremblement de terre, écrasement d'un avion, pollution chimique, pollution électromagnétique, etc.).

Il importe ainsi que les établissements soient rigoureux dans le choix des emplacements pour leurs centres informatiques, en évitant toute zone exposée à des risques naturels (zone inondable ou sismique par exemple) ou de voisinage (aéroport, site chimique, etc.). Il convient également qu'ils équipent leurs centres de dispositifs visant à détecter les accidents et à atténuer au maximum les détériorations potentielles. Cela vaut particulièrement pour le risque d'incendie (détection, extinction) et pour le risque de fuite d'eau dans le circuit de climatisation. Ces dispositifs doivent être correctement dimensionnés, régulièrement testés et maintenus en bon état de marche. Ces protections sont non seulement nécessaires dans les plateaux hébergeant le matériel informatique mais aussi

dans les pièces dédiées au matériel électrique et aux serveurs de télécommunication. Il est également préférable de concevoir une politique globale de sécurité prévoyant par exemple d'éviter d'entreposer des matières inflammables comme des cartons dans les salles de machines ou les locaux alentours.

Insuffisance des dispositifs de continuité

Conformément au plan de secours informatique, l'établissement doit pouvoir basculer l'exploitation de son système d'information sur une infrastructure de secours lorsque son système principal est indisponible. S'il a mal dimensionné ses équipements de secours, il risque de ne pas pouvoir faire fonctionner des applications dont il a pourtant besoin. Si ses sauvegardes sont trop anciennes, il risque de perdre beaucoup de données importantes.

C'est pourquoi les équipements des infrastructures de secours doivent être correctement dimensionnés pour pouvoir faire fonctionner les applications et fonctionnalités identifiées comme essentielles et critiques par le plan de continuité. Ces infrastructures doivent être opérationnelles pour faciliter le basculement de la production dans des délais réduits correspondants aux exigences des utilisateurs (RTO et RPO). Les sauvegardes doivent être suffisamment fréquentes et protégées. Les bascules doivent pouvoir être déclenchées, soit en totalité pour l'ensemble du système d'information, soit par partie ou application. Si l'exploitation est répartie sur au moins deux sites fonctionnant en partage de charge (mode « actif-actif »), il importe que chacun des sites puisse supporter la charge totale de fonctionnement en cas d'indisponibilité d'un ou de plusieurs sites. De plus, les désastres régionaux doivent être pris en compte, en particulier par des distances suffisantes entre environnement de production et environnement de secours. À cet égard, il importe tout particulièrement que le site de secours dispose d'approvisionnements électriques provenant d'une source de production différente de celle qui dessert le site principal et qu'il ne soit pas exposé aux mêmes risques naturels que le site principal (crue fluviale, proximité avec un même aéroport ou site industrialo-chimique, etc.). Si tel est le cas, un troisième site est nécessaire pour permettre de disposer de réelles capacités de production dans tous les scénarios d'indisponibilité.

Tests insuffisants

L'efficacité et la pertinence des plans de continuité métiers et de secours informatique dépendent de tests de mise en œuvre suffisamment réguliers. Les tests des dispositifs techniques et organisationnels permettent d'évaluer la solidité des solutions prévues, conformément aux niveaux de service validés par les utilisateurs.

Il importe que les plans de continuité soient testés sur un périmètre exhaustif à l'aide d'une méthodologie éprouvée, donnant une assurance raisonnable sur leur qualité et leur efficacité, notamment quant au respect des exigences des utilisateurs. La pertinence des tests de secours n'est démontrée que lorsque ceux-ci incluent le basculement de la production de l'environnement principal vers l'environnement de secours. Cet environnement de secours doit ainsi être utilisé en situation réelle par les équipes métiers pendant une période suffisamment significative et sur un périmètre représentatif de leurs activités critiques (notamment pour permettre le déroulement des travaux de fins de période comme une fin de semaine ou de mois). Les environnements de secours doivent permettre

une production alternée sur au moins un des sites de secours. Les résultats sont suivis au niveau adéquat et font l'objet des mesures correctives nécessaires.

3 Gestion des changements (projets, évolutions, corrections)

On appelle « changements » en informatique l'ensemble des modifications effectuées sur un système, soit pour le corriger ou le faire évoluer (maintenance), soit pour le changer ou le compléter (projet). Cela peut concerner les logiciels et les équipements. Il s'agit évidemment de processus délicats puisque devant s'insérer dans une production existante. Une mauvaise gestion des changements entraîne des dysfonctionnements. En la matière, les facteurs de risques à prendre en compte sont que les normes relatives à la gestion des changements soient inappropriées, que les changements ou les projets soient mal organisés ou gérés avec incompétence, que les exigences fonctionnelles et techniques soient mal prises en compte, que les nouveaux éléments soient insuffisamment testés, ou encore que le changement soit mal exécuté.

Insuffisance dans la définition ou l'application des normes relatives à la gestion des changements

Étant un processus délicat, la gestion des changements est habituellement un processus normé par des politiques et des procédures opérationnelles. De telles politiques prévoient par exemple que les mises en production sont regroupées en lot plutôt qu'exécutées unitairement. Une mise en production qui ne serait pas correctement normée serait plus exposée au risque de mauvaises manipulations.

Des politiques et procédures complètes et adaptées sont donc recommandées. Elles sont mises en œuvre par des équipes spécialisées et formées à cet effet au sein des entités. Les différentes typologies de changements sont définies, dont les changements standards et les changements urgents, pour corriger les anomalies graves de fonctionnement. La description des traitements distingue les différentes phases, notamment l'enregistrement, l'évaluation des impacts, la classification, la priorisation, les étapes de validation, la planification, les tests, les conditions de retour arrière. La gestion des versions (« *releases* ») est également comprise dans ces processus.

Mauvaise organisation dans la conduite de projets

La réussite des processus de gestion de changements, et tout particulièrement de conduite de projet, dépend largement de la mise en œuvre d'une organisation solide et de la compétence des équipes en charge. L'utilisation d'une méthodologie de travail aide également à encadrer le processus. Le défaut de maîtrise des travaux peut conduire à des retards ou des surcoûts, voire à une réduction des fonctionnalités attendues.

Il convient notamment de définir clairement les rôles et les responsabilités de chacun des participants pour disposer d'une organisation solide. Des comités assurant le suivi des travaux et favorisant la coordination des acteurs facilitent le suivi des délais, des coûts et de la qualité ainsi que la prise de décision. Les projets importants sont suivis par un sponsor chargé de veiller à leur bon déroulement. Un dispositif de communication auprès des différents acteurs réduit les incompréhensions qui peuvent être source d'erreurs ou de retards. L'utilisation d'une méthodologie de

conduite de projets est bénéfique car elle permet de garantir le bon enchaînement des différentes étapes de réalisation après vérification de la qualité des livrables. Enfin, le choix des collaborateurs est crucial et il convient de vérifier leur compétence pour l'exercice des différentes tâches.

Mauvaise prise en compte des exigences fonctionnelles et techniques

Les applications et logiciels doivent répondre aux besoins des utilisateurs. Ceux-ci doivent donc être formellement exprimés pour être correctement pris en compte. Par ailleurs, il existe aussi des exigences techniques imposées par les prescriptions de sécurité, de production ou d'exploitation réseau. Il est également possible de faire travailler les utilisateurs et les développeurs informatiques de façon rapprochée et interactive pour une bonne prise en compte des besoins (ex : méthode de développement « agile »). Cela s'applique aussi aux développements informatiques qui pourraient être réalisés par les utilisateurs (« *shadow IT* »), surtout quand ceux-ci sont utilisés pour produire des informations de gestion importantes.

Il convient de suivre une méthodologie partagée par l'ensemble des parties prenantes pour recueillir et valider les exigences fonctionnelles formulées par les utilisateurs. Les exigences techniques qui imposent des contraintes à la prise en compte des besoins fonctionnels doivent être connues des utilisateurs et admises par eux. Les exigences techniques propres à l'exploitation des systèmes et réseaux doivent être prises en compte par les administrateurs techniques au plus tôt dans la conception et la réalisation de nouveaux équipements.

Défaut dans les logiciels

Les logiciels utilisés par l'établissement ne doivent évidemment pas souffrir de défauts de fonctionnement qui altéreraient la fiabilité des informations produites, ou ralentiraient et compliqueraient la gestion des processus. Cela est bien sûr applicable aux applications développées spécifiquement pour l'établissement et aux logiciels de marché. Cela s'applique aussi aux développements informatiques qui pourraient être réalisés par les utilisateurs (« *shadow IT* »), surtout quand ceux-ci sont utilisés pour produire des informations de gestion importantes.

Des recettes fonctionnelles et techniques sont destinées à vérifier l'adéquation des applications et logiciels. Il importe qu'elles soient exhaustives et formalisées, ainsi qu'elles donnent lieu à des comptes rendus partagés entre les parties prenantes. Des actions correctives sont mises en place si des anomalies importantes sont détectées. Les anomalies mineures peuvent être déclarées non-bloquantes pour le démarrage et faire l'objet de corrections ultérieures.

Insuffisance des tests

Les tests permettent de s'assurer de la conformité des changements avec les besoins validés, aussi bien en termes fonctionnels que techniques.

Des tests de non-régression sont systématiquement réalisés à l'occasion de changements pour éviter les effets de bord non désirés. Un environnement de pré-production, très similaire à celui de production, permet de vérifier l'adéquation des nouveaux composants (fonctionnalités, performance).

Défauts dans l'exécution des changements

La mise en production des changements est tout particulièrement délicate car si elle n'est pas correctement réalisée, elle peut causer des perturbations sur le système en place, avec potentiellement des conséquences très dommageables lorsqu'il est difficile de faire un retour-arrière.

Il importe donc de suivre un processus de mise en production très rigoureux. Ainsi, la planification des déploiements logiciels et matériels s'appuie sur des procédures formalisées qui visent à garantir un niveau satisfaisant de disponibilité. Ces procédures incluent des méthodes de retour-arrière en cas de défaut. Un calendrier de changement est normalement mis en œuvre avec l'objectif de les regrouper sur des périodes où le personnel expérimenté est présent et en dehors des périodes normales de services (week-end par exemple). Le cas échéant, des experts qualifiés sont mobilisables en astreinte et des responsables sont joignables en cas d'anomalie.

4 Qualité des données

Une des exigences primordiales qui s'impose à un système d'information est que ses données soient justes, c'est-à-dire qu'elles correspondent aux données attendues en entrée et/ou que leurs transformations tout au long des calculs réalisés par le système d'information ne créent pas d'erreurs. Cela s'impose tout particulièrement aux systèmes d'information des établissements des secteurs de la banque et de l'assurance qui tiennent notamment des données personnelles et des avoirs financiers. L'exigence prend également de l'importance concernant les données de calcul des risques, qui sont utilisées par les instances dirigeantes pour piloter l'activité et par les superviseurs pour la surveiller. Ainsi, la mauvaise qualité des données peut être particulièrement dommageable, à la fois pour la conduite de l'activité si l'établissement n'utilise pas des données fiables, et pour le suivi des risques si les indicateurs en la matière sont erronés. La qualité des données peut être en défaut lorsque la normalisation des données et des référentiels est insuffisante, ou lorsque le système d'information utilise ou produit des données erronées. Un défaut de contrôle peut encore expliquer un problème de qualité des données.

Insuffisance de normalisation des données

Les systèmes d'information des établissements des secteurs de la banque et de l'assurance sont souvent composés de multiples applications. Si elles ont été conçues à des périodes différentes et pour des besoins chaque fois nouveaux, les notions qu'elles utilisent (« emprunteur », « assuré » par exemple) peuvent ne pas toujours être définies de la même manière, de sorte qu'il est difficile de les comparer ou de les agréger. Normalement, les notions les plus utilisées sont gérées sous forme de « référentiels » uniques, pour l'usage commun des différentes composantes de l'établissement. De même, une démarche de « normalisation » des données consiste à rapprocher et même unifier lorsque c'est possible, les définitions de notions similaires utilisées dans l'ensemble du système d'information. Si l'établissement ne recourt pas à des référentiels pour ses données les plus partagées, ou s'il n'a pas engagé de démarche de normalisation, ses différentes composantes de son système d'information risquent d'utiliser des données non comparables ni cumulables, au détriment d'une vision consolidée de son activité et de ses risques.

C'est pourquoi il convient de privilégier l'élaboration de référentiels de données pour les notions les plus couramment utilisées par l'entreprise. Les différentes applications utilisatrices de ces données peuvent ainsi disposer d'une source unique et fiabilisée. Une fonction ou un métier est désigné comme responsable de ces référentiels et en assure la mise à jour et la pertinence des définitions des données. De même, pour réduire l'hétérogénéité entre les différentes applications qui utilisent des données approchantes et faciliter leur agrégation, l'établissement a intérêt à engager une démarche de normalisation des données. Cette démarche concerne les métiers et fonctions utilisateurs, mais aussi la fonction informatique, qui est gardienne de la rationalisation du système d'information dans son ensemble. Cette normalisation peut utilement s'appuyer sur des dictionnaires de données, donnant leur définition et leur syntaxe, et s'imposant à l'ensemble des entités utilisatrices.

Utilisation ou production par le système d'information de données erronées

Si le système d'information utilise des données fausses en entrée, il est probable qu'il produira des données inexactes en sortie. Mais indépendamment de la qualité des données source, s'il existe dans le système des erreurs de calcul, les données produites seront erronées. Les erreurs de données ne sont pas seulement liées à des problèmes d'exactitude. Elles peuvent également résulter de données inappropriées ou incomplètes, ou tout simplement indisponibles au moment du calcul. Le risque d'erreurs est aussi plus grand lorsqu'un processus automatisé fait l'objet de retraitements manuels.

Le caractère approprié de la donnée est testé par les utilisateurs avant la mise en production, puis régulièrement vérifié. Des pistes d'audit permettent de restituer les traitements et les étapes de modifications apportées, pour une compréhension de la transformation de l'information de son origine à sa forme finale. Les traitements manuels sont limités au maximum et font l'objet de vérifications approfondies et régulières. Les incidents de production sont analysés pour vérifier leur incidence sur la qualité des données produites. Les indicateurs de risque produits pour les instances dirigeantes et les superviseurs sont fondées le plus possibles sur des indicateurs calculés automatiquement plutôt que sur des valeurs d'approximation. Enfin, il importe que les données soient disponibles avec des niveaux de détail suffisants et avec les critères d'agrégation demandés, pour couvrir tous les besoins significatifs des utilisateurs.

Défaut de contrôle de qualité des données

La qualité des données doit faire l'objet de contrôles réguliers et approfondis par les utilisateurs et les fonctions de contrôle. À défaut, l'établissement pourrait ne pas détecter une situation d'utilisation ou de production de données erronées.

Ainsi, la vérification des données tout au long de leur cycle de vie, ainsi que des rapports d'activité ou de suivi du risque, doit s'appuyer sur des contrôles automatisés et manuels, permettant d'identifier les éventuelles anomalies et de mettre en place les plans d'actions pour les corriger.



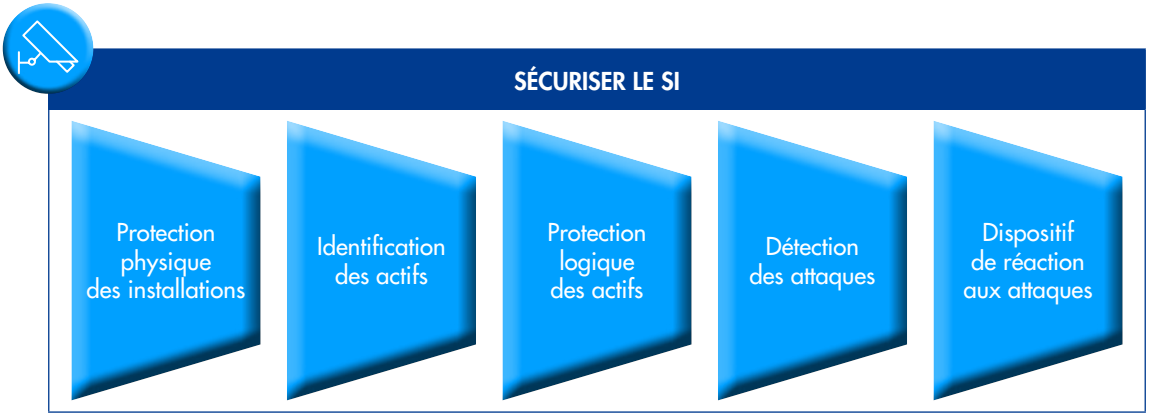
Sécurité du système d'information

Cette partie traite des risques pouvant affecter le macro-processus « sécurité du système d'information », qui rassemble les différentes actions de prévention et de réaction destinées à contrecarrer les atteintes à la sécurité. Il est habituel de présenter ces atteintes comme étant celles faites à la disponibilité, à l'intégrité, à la confidentialité, et à la preuve ou à la traçabilité des données et des opérations.

La sécurité du système d'information a pris une importance croissante face aux cybermenaces mais il s'agit en réalité d'une préoccupation ancienne. À l'origine, elle englobait à la fois les menaces d'origine accidentelle (pannes, évènements naturels) ou malveillante. Aujourd'hui, il est plus aisé de prendre en compte les menaces accidentelles au titre du macro-processus de « fonctionnement du système d'information » comme cela a été fait ci-dessus, et de recentrer celui de « sécurité du système d'information » sur la prévention et la réaction face aux attaques malveillantes, y compris lorsqu'elles bénéficient de négligences.

Les préconisations liées à la sécurité ne doivent pas être lues en isolation de celles présentées précédemment en matière d'organisation et de gouvernance.

Les paragraphes suivants présentent les principaux facteurs de risques pouvant affecter la sécurité du système d'information dans son ensemble (production, développement, test et secours) et, pour chacun d'eux, des exemples de mesures de réduction du risque pouvant être mises en œuvre. Les facteurs de risque retenus sont ceux qui résulteraient d'insuffisances affectant la protection physique des installations et



facilitant une intrusion, l'identification des actifs informatiques (c'est-à-dire les différents biens qui constituent le système d'information comme les équipements matériels, les logiciels et les données), la protection de ces actifs, la détection des attaques, ou encore la réaction à ces attaques.

1 Protection physique des installations

La protection des bâtiments contre l'intrusion malveillante a pris un tour plus important ces dernières années pour tenir compte de nouveaux types d'attaques, soit violentes, soit discrètes. Une intrusion dans les locaux peut conduire au vol et à la destruction d'actifs physiques, voire à faciliter une intrusion logique dans le système d'information en permettant l'introduction de programmes malveillants (« *malwares* ») qui peuvent espionner, saboter ou substituer des informations appartenant à l'institution, à ses clients ou à ses partenaires. De telles intrusions sont possibles si les mesures de protection des bâtiments ou d'accès aux équipements informatiques sont insuffisantes.

Protections insuffisantes contre l'intrusion dans les bâtiments

Des mesures de protection sont cruciales pour les locaux hébergeant les infrastructures systèmes et réseaux (centres informatiques). Elles peuvent également être nécessaires pour les locaux commerciaux ou administratifs qui, même s'ils ne présentent pas la même criticité, hébergent néanmoins les postes de travail, les accès réseaux et la documentation de l'établissement.

Il est préférable de ne pas identifier les centres informatiques par des signes visuels pouvant révéler la finalité et l'appartenance des locaux. Leur accès est aussi limité à un nombre réduit de personnes afin de limiter les risques. Des procédures strictes encadrent les conditions d'accès aux installations, y compris pour les prestataires en charge de la maintenance des équipements. Ces procédures restreignent les accès aux seules personnes dûment annoncées, identifiées et accréditées. La protection des locaux repose généralement sur des dispositifs de protection périmétrique (clôtures, barrières, sas d'entrée, contrôle par badge, etc.) et de détection d'intrusion (vidéo-surveillance, alarmes, etc.). Ces équipements doivent être régulièrement testés et maintenus en capacité. Des mesures de contrôle d'accès différenciées par zone complètent utilement le dispositif à l'intérieur de l'enceinte en restreignant l'accès aux locaux selon le besoin reconnu, appelé « besoin d'en connaître », des personnels. Les dispositifs de sécurité sont synchronisés pour permettre la corrélation d'évènements. Les journaux d'évènements de ces dispositifs sont conservés pendant une durée suffisante pour pouvoir mener à bien toutes les investigations utiles.

Protections insuffisantes des équipements informatiques

Les mesures de protection du matériel complètent celles destinées à empêcher les intrusions. Les actifs physiques critiques, tels que les serveurs, les consoles d'administration, les équipements réseaux, les équipements électriques, les clés, etc., requièrent une protection renforcée par des dispositifs de sécurité complémentaires et spécifiques (ex : cage autour des serveurs, fermeture des baies, vidéo-surveillance spécifique).

2 Identification des actifs

Une mauvaise connaissance des actifs informatiques est de nature à entraver la gestion de la sécurité du système d'information car elle peut aboutir à ne pas appliquer préventivement des mesures de sécurité homogènes et appropriées ou à entraver les actions de riposte à une attaque. Les facteurs de risque sont des défaillances dans l'inventaire ou dans la classification des actifs.

Défaillances dans l'inventaire des actifs

Le recensement des actifs informatiques est nécessaire pour identifier les actifs les plus critiques pour les métiers utilisateurs ou les plus exposés aux cyberattaques. Ce recensement prend la forme d'un inventaire qui comprend les actifs « métiers » (ex. : applications, données) et « support » (ex. : locaux, équipements). Cet inventaire est tenu à jour. Il contient tous les éléments utiles à l'identification, la localisation, la fonction et la propriété de chaque actif. Il permet également de mettre en relation les actifs pour identifier rapidement les interactions et interdépendances, informations utiles en cas de gestion crise.

Défaillances dans la classification des actifs

La classification consiste à définir le niveau de sensibilité des actifs, ce qui sert, d'une part, à déterminer les mesures de protection à implémenter et, d'autre part, à identifier rapidement les actifs à isoler et à préserver en cas d'attaque. La classification vise en premier lieu les données et les applications qui les gèrent. Cela permet ensuite d'accorder un niveau de sensibilité correspondant aux équipements systèmes et réseaux utilisés pour ces applications, ainsi qu'aux sites sur lesquels ils sont installés. Il en résulte une vision globale, à la fois aux plans logique et physique, de ce que l'établissement doit protéger en priorité.

Pour que la classification soit complète et pertinente, elle doit couvrir l'ensemble des actifs logiques ainsi que l'ensemble des actifs physiques qui les supportent. Elle doit résulter d'une analyse formalisée et validée par les propriétaires des actifs concernés. Il importe qu'elle soit périodiquement réexaminée. La classification des actifs se fait selon leur sensibilité au regard des critères de disponibilité, d'intégrité, de confidentialité, de traçabilité, ou des contraintes légales ou réglementaires. L'impact financier ou en matière de réputation peut également servir à cette évaluation.

3 Protection logique des actifs

La sécurité des actifs repose en premier lieu sur un ensemble de mesures de protection informatiques (dites « logiques »), destinées à prévenir toute compromission du système d'information. Les motivations des attaquants sont de tous ordres, qu'elles visent à tirer un bénéfice direct (fraude, vol, rançon, espionnage), ou à nuire (perturbation du bon fonctionnement, sabotage, atteinte à la réputation). Mais quelles que soient ces motivations, les perturbations qu'elles provoquent porteront sur la disponibilité (ex : blocage d'un système), l'intégrité (manipulation d'un actif), la confidentialité (lecture ou vol d'une donnée par exemple), ou l'altération du système de traçabilité (effacement des changements de droits par exemple). Les mesures de protection doivent donc couvrir ces différents types de perturbations et être adaptées à la sensibilité de chaque actif. Ces mesures ne se conçoivent

plus isolément. Il est de bonne pratique désormais de les multiplier à différents niveaux du système d'information (par exemple en filtrant les communications non seulement à l'entrée mais aussi plus avant dans le système) de façon à ralentir la progression d'un attaquant. C'est le concept de « défense en profondeur ». Si la protection logique des actifs est insuffisante, le risque est qu'un attaquant puisse pénétrer dans le système d'information et le compromettre. Cela peut être en raison de défaillances dans les dispositifs de sécurité périmétrique, de protection contre les logiciels malveillants, de gestion des identités et des droits d'accès, d'authentification des collaborateurs, de protection de l'intégrité et de la confidentialité des systèmes et données, de protection de leur disponibilité, de gestion des correctifs de sécurité, de revue de la sécurité, de sécurisation des solutions externalisées ou de sensibilisation à la sécurité des systèmes d'information.

Défaillances dans les dispositifs de sécurité périmétrique

La sécurité périmétrique consiste à protéger le système d'information vis-à-vis de l'extérieur ou à isoler des zones internes. Comme il existe de nombreuses communications avec des contreparties externes, la sécurité périmétrique va consister à rassembler les flux de communication sur un nombre limité de points de passage, puis à filtrer et analyser les flux entrants et sortants pour en vérifier le contenu. Ces dernières années, cette protection a pu être décriée au motif qu'elle devenait quasiment impossible face à la multiplication des canaux et flux d'échange. Pourtant, la sécurité périmétrique reste un atout primordial pour une protection efficace du système d'information, même s'il convient par ailleurs de la compléter par d'autres mesures, notamment de détection à l'intérieur du système.

Il est donc attendu que des dispositifs assurant la sécurité périmétrique du système d'information soient mis en œuvre pour empêcher toute tentative d'accès illégitime au système d'information, ou à tout le moins aux applications et données identifiées comme sensibles. Des mécanismes de filtrage du trafic réseau (pare-feu par exemple), comportant des règles d'analyse et de blocage sont déployés, et les actifs les plus sensibles sont logiquement isolés au sein du système d'information, ou même coupés de celui-ci. L'efficacité des dispositifs de protection périmétrique est régulièrement réévaluée et adaptée.

Défaillances dans les dispositifs de protection contre les logiciels malveillants

Les logiciels malveillants sont le plus souvent le vecteur des cyberattaques. Ils peuvent servir à capter des informations pouvant faciliter une intrusion future (collecte d'informations techniques, organisationnelles ou procédurales), compromettre l'intégrité des systèmes ou données (défiguration de sites, chiffrement de données suivi d'une demande de rançon), perturber la disponibilité des applications (sabotage), ou plus directement pour dérober des informations confidentielles (espionnage). Si l'établissement ne met pas en œuvre des mesures de protection contre ces logiciels, la sécurité de son système d'information peut être gravement compromise.

Il importe donc de déployer des dispositifs anti-malwares sur l'ensemble des équipements matériels, voire logiciels : passerelles de messagerie (analyse des pièces-jointes, détection de fichiers exécutables), passerelles

d'accès à Internet, points d'accès réseau avec les partenaires, etc. Ces dispositifs doivent être activés et tenus à jour. S'il existe des dérogations, elles doivent être formalisées et validées. Les dispositifs de protection sont protégés contre toute tentative de désactivation ou de désinstallation par les utilisateurs. L'emploi de plusieurs suites de sécurité distinctes au sein du système d'information permet d'éviter l'exploitation d'une faiblesse ou d'une faille d'un outil particulier.

Défaillances dans les dispositifs de gestion des identités et des droits d'accès

Les droits d'accès au système d'information sont normalement accordés aux utilisateurs selon le principe du « besoin d'en connaître ». Ils protègent l'usage légitime du système. Ils sont liés à la gestion de l'identification des utilisateurs. C'est la reconnaissance par l'entreprise du statut et de la fonction de ses collaborateurs qui doit guider l'attribution de droits d'accès. Ainsi, l'embauche, le départ ou le changement d'affectation du collaborateur doivent normalement déclencher une mise à jour des droits d'accès. Des principes analogues devraient prévaloir pour les composants du système d'information gérés par des prestataires externes. Si tel n'est pas le cas, ou si les droits sont tout simplement trop largement attribués ou mal mis à jour, un attaquant pourra plus facilement les usurper et évoluer dans le système d'information.

Pour permettre l'imputation de toute action sur le système d'information à une personne donnée, l'identification des collaborateurs internes et externes est nominative. L'utilisation de comptes génériques pour accéder aux serveurs, applications et données est restreinte et formellement encadrée. Les collaborateurs disposant de comptes à privilèges (administrateurs par exemple) disposent également de comptes ordinaires pour effectuer leurs tâches courantes (accès à la messagerie d'entreprise, navigation sur Internet, etc.). Une gestion efficace des droits d'accès suppose l'utilisation de profils (métiers et techniques) pour uniformiser et faciliter l'attribution de droits unitaires. Toute attribution d'un droit d'accès unitaire complémentaire, hors profil, doit ainsi être justifiée, formalisée et validée. De façon générale, les droits d'accès à un actif sont validés par le propriétaire de cet actif, directement ou par délégation. Il importe que les droits d'accès soient en adéquation constante avec les fonctions occupées. En particulier, toute mutation ou départ d'un collaborateur se traduit par une suppression des habilitations accordées dans un délai raisonnablement court. Les meilleures pratiques en la matière consistent à réaliser une synchronisation entre les systèmes de gestion des droits d'accès et des systèmes de gestion des ressources humaines (ou des contrats de prestation le cas échéant). Les droits accordés font l'objet de réexamens réguliers pour s'assurer de leur légitimité. La fréquence de ces revues est adaptée à la sensibilité des droits accordés. De la même façon, la définition des profils est revue périodiquement pour en évaluer la pertinence.

Défaillances dans les dispositifs d'authentification des collaborateurs

L'authentification consiste à apporter la preuve de son identité, par exemple pour accéder à un équipement ou une application. En informatique, le mécanisme le plus fréquent est le mot de passe mais sa sécurité peut être insuffisante pour empêcher une usurpation.

Il importe donc que des mécanismes d'authentification adaptés à la sensibilité des

actifs accédés soient en place. Des moyens d'authentification à double facteur et/ou dynamiques sont à privilégier pour l'accès aux actifs les plus critiques. Le cas échéant, des règles de complexité des secrets d'authentification choisis par les collaborateurs sont normées et adaptées à leur fonction. Le respect de ces règles est régulièrement contrôlé. L'attribution de facteurs d'authentification temporaires est formellement encadrée et sécurisée (changement du mot de passe à la première connexion par exemple). Lorsqu'ils sont statiques, les facteurs d'authentification (mots de passe, *tokens*, etc.) doivent être renouvelés périodiquement. Tout accès au système d'information réalisé hors des locaux fait normalement l'objet de procédures d'authentification renforcées (collaborateur ou prestataire externe). Les secrets d'authentification doivent enfin être correctement protégés.

Défaillances dans les dispositifs de protection de l'intégrité des systèmes et des données

Des mesures de protection de l'intégrité des systèmes et des données sont nécessaires pour empêcher qu'un attaquant puisse réaliser des modifications des composants du système d'information qui en altéreraient son bon fonctionnement (y compris sa fiabilité) ou sa sécurité. Il pourrait s'agir par exemple de modification des configurations d'un système, ou de ses droits d'accès, afin de réaliser une attaque. Il pourrait aussi s'agir d'une modification de données au profit de l'attaquant, ou encore un chiffrement en vue de demander une rançon.

Pour renforcer la sécurité des systèmes et pouvoir détecter toute altération de configuration, qu'il s'agisse de l'ajout d'un programme ou de la modification de paramètres systèmes ou applicatifs, il est d'usage de limiter strictement les droits d'exécution de logiciels sur les machines – serveurs et postes de travail – et de faire une prise d'empreinte des fichiers « clés » des serveurs. De plus, une manière de réduire le risque de compromission d'un matériel consiste à réduire au strict nécessaire les logiciels qui l'équipent ainsi que ses fonctionnalités. Cette technique appelée « durcissement » permet de réduire mécaniquement le nombre de failles logicielles qui pourraient être exploitées par un attaquant. Concernant les données, mais aussi les applications qui les utilisent, la protection contre toute tentative d'altération peut recouvrir plusieurs formes distinctes. Il est ainsi préférable que les applications soient conçues de manière sécurisée en incluant des contrôles automatiques pour la création, la modification et la suppression des données sensibles. De même, les applications peuvent être organisées de façon à comporter une double validation (principe des « quatre-yeux ») pour les opérations importantes (validation d'un paiement par exemple). Lors du transport et du stockage des données, leur intégrité peut être protégée par des mécanismes techniques et applicatifs de « scellement » permettant de vérifier qu'elles n'ont pas été altérées. Le sceau est classiquement calculé par une fonction dite de « hachage » après ajout éventuel d'un « sel » pour éviter les attaques par « dictionnaire » (« *rainbow tables* »). Ces mécanismes, s'ils sont mis en œuvre, doivent toutefois être conformes aux recommandations en vigueur de l'ANSSI [27] pour être pleinement efficaces et sûrs. Enfin, et de façon spécifique aux services offerts par une entité sur Internet, des mécanismes de protection spécifiques au risque de défiguration – « *web defacement* » – peuvent être appliqués aux sites Internet.

27 Voir annexe B1 du *Référentiel Général de Sécurité de l'ANSSI* (*https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/*).

Défaillances dans les dispositifs de protection de la confidentialité des données

Les mesures de protection de la confidentialité des données, qu'elles soient relatives aux applications (base de données des clients par exemple) ou aux matériels (données de configuration par exemple), visent à empêcher une prise de connaissance illégitime (lecture) ou un vol (copie). Dans les deux cas, les conséquences peuvent être désastreuses pour l'établissement, notamment aux plans juridique (manquement aux obligations réglementaires) et financier (réparation des dommages, sanction), ainsi qu'en termes de réputation.

Pour éviter toute divulgation ou vol de données, il convient de protéger les données de production et de limiter leur dissémination sur d'autres environnements. Ainsi, les environnements de production peuvent être ségrégués ou isolés logiquement des autres environnements pour réduire tout accès incontrôlé depuis un environnement de développement ou de test, généralement moins protégé. De façon similaire, les données accessibles depuis les environnements de tests ou de développement peuvent être rendues anonymes ou, mieux encore, être purement fictives pour réduire tout risque de divulgation de données réelles. Pour minimiser les risques d'accès aux données à des tiers non autorisés, la possibilité de consulter ou de manipuler des données de production doit être encadrée et les accès tracés. Cette mesure concerne notamment les prestataires tels que les hébergeurs, info-gérants, éditeurs de solutions logicielles, qui peuvent disposer de droits étendus sur les environnements de production sans que l'entité ne sache précisément qui a accès à ses données. Par ailleurs, les données les plus sensibles doivent être protégées tout au long de leur cycle de vie : lors de la saisie et de l'affichage (en étant par exemple masquées partiellement ou en totalité), mais aussi lors du stockage et du transport (en étant chiffrées). Il peut également être pertinent de chiffrer de bout en bout les communications réseau, c'est-à-dire à la fois sur les réseaux publics et les réseaux internes (entre applications). Dans tous les cas, les différents mécanismes cryptographiques mis en œuvre doivent, là encore, être conformes aux recommandations en vigueur de l'ANSSI pour être totalement efficaces et sûrs.

Le matériel hébergeant les données ou permettant un accès à ces données doit lui aussi être protégé. C'est notamment le cas des dispositifs nomades (ordinateurs) et mobiles (téléphones, tablettes) qui peuvent se voir appliquer des mesures spécifiques telles que le chiffrement des supports internes de stockage ou, quand c'est possible, la mise en place d'un mot de passe pouvant empêcher le démarrage du matériel et l'accès à son contenu. De façon plus générale, en fin de cycle de vie, une bonne pratique est d'avoir des procédures de mise au rebut des équipements qui consistent à détruire logiquement et/ou physiquement toute information en mémoire. Enfin, au niveau applicatif, les applications disponibles publiquement (applications et services Internet, applications mobiles, etc.) peuvent utilement bénéficier de mesures visant à empêcher toute tentative de rétro-ingénierie. Cette pratique vise à récupérer sous une forme exploitable le code source d'un logiciel dans le but de le contrefaire (atteinte à la propriété intellectuelle) ou d'en comprendre le fonctionnement (par exemple pour ensuite l'attaquer).

Défaillances dans les dispositifs de protection de la disponibilité

Des attaques externes peuvent rendre le système d'information indisponible, soit en empêchant totalement d'y accéder, soit simplement en le ralentissant. Des cyberattaques de ce type, appelées « *Denial of Service* » – DoS [28], consistant à saturer les accès externes à un système, ont été très nombreuses ces dernières années. Immédiatement pénalisantes pour les utilisateurs, ces attaques peuvent porter atteinte à la réputation des établissements des secteurs de la banque et de l'assurance.

La protection du système d'information contre les atteintes à sa disponibilité repose en premier lieu sur les mêmes dispositifs de gestion de la continuité que ceux évoqués à propos du maintien du bon fonctionnement du système d'information. De manière spécifique pour les attaques DDoS, l'établissement peut utilement recourir à des solutions de filtrage permettant de reconnaitre les flux légitimes. En cas d'attaque d'un site web utilisé par la clientèle, il peut également être utile de pouvoir activer un site distinct, copie du premier ou destiné seulement à diffuser de l'information, et qui est accessible à une autre adresse que celle faisant l'objet de l'attaque.

Défaillances dans les dispositifs de gestion des correctifs de sécurité

Les cyberattaques consistent souvent à exploiter des failles de sécurité sur les logiciels ou les matériels. Les éditeurs mettent normalement très rapidement à niveau leurs solutions informatiques lorsque des failles de sécurité sont découvertes. Si l'établissement n'est pas lui aussi rapide à changer ses versions pour bénéficier des correctifs de sécurité, il reste exposé à des attaques. Cette démarche est facilitée par l'existence d'un inventaire des actifs à jour.

La protection du système d'information contre les attaques logiques requiert une mise à jour rapide des correctifs de sécurité, pour l'ensemble des actifs concernés. Une veille est organisée pour identifier les vulnérabilités pouvant affecter le système d'information et apporter au plus vite les correctifs. Elle s'appuie sur les informations de configuration disponibles dans l'inventaire des actifs pour vérifier l'ampleur des vulnérabilités et déterminer un plan de mise à jour. Ce plan tient compte du niveau de sensibilité des actifs. Pour éviter de créer toute nouvelle vulnérabilité, les nouveaux équipements à installer le sont dans des versions supportées par leurs constructeurs ou éditeurs, et à jour des correctifs de sécurité.

Défaillances dans les dispositifs de revues de sécurité

On désigne par revues de sécurité les mesures consistant à tester l'efficacité des défenses mises en œuvre (« test d'intrusion ») ou à vérifier l'existence de vulnérabilités en observant les configurations du matériel et des logiciels (« scans de vulnérabilités » et « revues de code applicatif »). Les établissements ont de plus en plus recours à ces techniques pour compléter leurs mesures de protection. Cela offre l'avantage de tester les possibilités qu'aurait un attaquant à contourner les défenses. À défaut, l'établissement pourrait considérer à tort que les mesures qu'il a mises en œuvre sont suffisantes.

Il est donc recommandé de procéder à la réalisation régulière de revues de sécurité afin de vérifier l'absence de failles

28 Lorsque l'attaquant parvient à utiliser un grand nombre d'appareils tentant de se connecter au système, l'attaque est appelée « *Distributed Denial of Service* » – DDoS.

exploitables sur les actifs informatiques. Cela devrait comporter des campagnes de scans de vulnérabilités périodiques sur les équipements connectés à Internet, par définition plus exposés, mais également sur les équipements internes (serveurs). Des tests d'intrusion ciblés viennent compléter ces scans pour éprouver la sécurité des équipements et des applications nouvellement installés ou faisant l'objet d'évolutions. Pour obtenir des résultats objectifs et fiables, ces campagnes sont conduites par des experts externes ou des tiers indépendants, en utilisant des approches et des méthodologies variées. Enfin, des audits de code axés sur la sécurité sont menés pour identifier et corriger au plus tôt toute faille potentielle.

Défaillances dans les dispositifs de sécurité des solutions externalisées

Il est fréquent qu'une partie, voire la totalité parfois, d'un système d'information soit gérée par un ou plusieurs prestataires pour l'établissement. Ces prestataires peuvent appartenir au même groupe que l'établissement ou ne pas lui être liés. Dans tous les cas, les prestataires agissent au nom et pour le compte de l'établissement et celui-ci reste responsable de la gestion de son système d'information, ce qui inclut donc sa sécurité.

La protection de la sécurité du système d'information suppose donc que les parties externalisées soient protégées à l'égal du reste. Pour cela, avant la mise en œuvre de la sous-traitance, l'entité cliente mène une analyse de risques à laquelle prennent part les fonctions de contrôle, dont la fonction de sécurité de l'information. Les instances dirigeantes se prononcent sur les projets d'externalisation en tenant compte des conditions de sécurité. L'analyse de risque identifie le caractère sensible des activités concernées, et s'assure de l'existence de solutions garantissant la confidentialité des informations (par exemple, en ayant recours au chiffrement) et de capacités de repli. Une fois en place, les services externalisés répondent aux mêmes exigences de sécurité que s'ils étaient conduits en propre par l'établissement : les dispositions contractuelles relatives à l'externalisation impliquent que les conditions de sécurité appliquées par le prestataire respectent les politiques de sécurité de l'établissement. Ce dernier suit dans le temps la performance des services sous-traités, y compris les éventuels incidents. L'établissement dispose d'un droit d'audit contractuel et celui-ci n'est pas affecté par des conditions restrictives (préavis long). Dans le cas d'une externalisation sous la forme d'une prestation de *Cloud computing*, l'ACPR a présenté en juillet 2013 un certain nombre de bonnes pratiques liées à la sécurité des données et des systèmes, que les établissements sont appelés à respecter [29], de même que les recommandations de l'ABE publiées en décembre 2017 [30].

Défaillances dans les dispositifs de sensibilisation à la sécurité des systèmes d'information

La sensibilisation du personnel et des instances dirigeantes à la sécurité des systèmes d'information est une action nécessaire pour faciliter l'émergence d'une culture du risque sur ces sujets. Elle peut contribuer à lutter efficacement contre les attaques malveillantes, qui visent souvent des collaborateurs, voire des dirigeants, pour les manipuler en vue de s'introduire dans le système (clé USB ou message électronique infecté par exemple) ou de réaliser une fraude (ingénierie sociale). Elle vise aussi à réduire le risque de négligence de la part de ces utilisateurs, qui pourrait permettre la réalisation d'une action malveillante d'un tiers.

29 ACPR (2013) : « Les risques associés au *Cloud computing* », juillet. *https://acpr.banque-france.fr/search-es?term=201307+Risques+associes+au+Cloud+computing*

30 *https://www.eba.europa.eu/documents/10180/1712868/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf*

Pour s'en prémunir, des actions de sensibilisation sont souhaitables. Elles complètent les procédures en vigueur en informant sur les risques et en diffusant les bonnes pratiques en matière d'utilisation et de protection du système d'information. Des campagnes de formation spécifiques aux collaborateurs disposant de privilèges élevés (administrateurs) ou exerçant des fonctions sensibles (développeurs) sont régulièrement organisées par ailleurs. Les actions de sensibilisation sont, dans la mesure du possible, étendues aux collaborateurs externes, partenaires et clients. L'efficacité de chaque action conduite est évaluée et ajustée si nécessaire.

4 Détection des attaques

La sécurité ne peut plus reposer uniquement sur des mesures de protection. La survenance de cyberattaques « silencieuses » [31] montre à quel point les attaquants peuvent réussir à s'introduire de manière discrète dans un système d'information pour en comprendre l'organisation et causer des dommages sérieux. La protection peut donc ne pas suffire et doit se doubler d'une détection. Cette détection comporte habituellement deux grands axes. L'un consiste à collecter et analyser les événements (« traces ») enregistrés par les matériels, et l'autre consiste à repérer des comportements anormaux d'utilisateurs. En l'absence de tels outils de détection, ou lorsque ceux-ci sont incomplets, l'établissement risque de ne pas détecter ni bloquer des intrusions dans son système d'information.

Défaillances dans les dispositifs de recueil et d'analyse des traces

Il existe des outils [32] de collecte, de centralisation et de corrélation des événements (« traces ») enregistrés par les différents équipements matériels du système d'information (particulièrement les pare-feux, les routeurs réseau, les sondes de détection, mais aussi les systèmes de production) qui sont utilisés pour surveiller ces équipements. Cette surveillance permet de repérer des intrusions ou simplement des tentatives d'intrusion dans le système d'information et ainsi d'alerter le plus tôt possible.

Les bonnes pratiques, notamment à des fins de cybersécurité, requièrent aujourd'hui de disposer d'outils automatiques de recueil et d'analyse de traces ainsi que d'une équipe de surveillance pour les exploiter (telle un « *Security Operating Centre* » – SOC), idéalement mobilisée 24 heures sur 24 et 7 jours sur 7, toute l'année. Ces systèmes de type SIEM couvrent au mieux la totalité du système d'information, ou du moins ses éléments communiquant avec Internet et ses composants classés comme sensibles. Les traces recueillies sont horodatées, archivées, et protégées contre toute tentative de modification. Les alertes les plus graves sont prises en charge par une équipe de veille, qui se tient en permanence informée des nouvelles modalités d'attaque ou failles exploitées [33]. L'organisation en place permet le partage d'informations sur les incidents rencontrés par les différentes unités internes. Des échanges avec les établissements pairs et les autorités sont également institués.

Défaillances dans les dispositifs de surveillance des comportements anormaux des utilisateurs

Les utilisateurs externes (clients se connectant en ligne par exemple) et internes (collaborateurs réalisant des opérations, personnels informatiques) mettent en œuvre les fonctionnalités du système d'information qui sont prévues pour leur usage. Un comportement malintentionné de leur part, ou de

31 On désigne ainsi les attaques qui ne provoquent pas immédiatement de perturbation, mais qui consistent à progresser discrètement dans le système d'information pour mieux l'attaquer

32 Ex. : outils de type SIEM (*Security Incident Event Management*).

33 Cette fonction peut être prise en charge par le SOC.

la part d'attaquants usurpant leurs droits, va se traduire par un usage anormal des fonctionnalités. Si des dispositifs de surveillance des comportements anormaux des utilisateurs ne sont pas mis en place, le système d'information de l'établissement risque d'être détourné à l'insu de celui-ci.

Les bonnes pratiques consistent à mettre en œuvre une surveillance des transactions suspectes dans les applications, les outils d'administration, les bases de données ou tout autre environnement sensible au sein de l'organisation. Cette surveillance mérite d'être réalisée en temps réel pour permettre une plus grande réactivité face aux attaques. Les connexions inhabituelles au système d'information sont surveillées (connexions à des horaires ou dates inhabituels comme des vacances, ubiquité des connexions, accès depuis des machines ou des adresses internet nouvelles etc.). Les anomalies lors de l'authentification des utilisateurs externes (clients, prestataires) et internes sont tracées et analysées (tentatives répétées par exemple). Les comportements anormaux des clients utilisant des sites transactionnels (gestion de compte en ligne par exemple) sont détectés. Les opérations de décaissement de valeurs sont surveillées et des mécanismes de blocage peuvent éventuellement être activés pour éviter des sorties de valeurs en nombre ou en montant élevés. Les fonctions de copie ou de suppression de masse sur les bases de données sensibles sont surveillées, voire bloquées, de même que les fonctions d'élévation de privilèges sur les systèmes et bases.

5 Dispositif de réaction aux attaques

Comme l'indiquent les principes de gestion de la cybersécurité, la sécurisation du système d'information suppose, outre des mesures de protection et de détection, de mettre en place également une organisation et une démarche de réaction aux attaques et de rétablissement du système d'information. Plusieurs étapes sont nécessaires, depuis le contingentement des composants du système qui ont été touchés, puis l'éradication des logiciels malveillants, avant la remise en service en mode dégradé, et ensuite la reconstitution d'un système d'information sain et complètement opérationnel. Ces différentes opérations requièrent une organisation de gestion de crise, qu'il est bien sûr utile d'avoir préconstituée. Les facteurs de risque pouvant empêcher une bonne réaction aux attaques sont donc liés à des défaillances de ces différents processus, soit de gestion de crise, soit de contingentement des attaques, ou de reprise des opérations.

Défaillances dans les dispositifs de gestion de crise

Une organisation de gestion de crise repose sur des procédures indiquant, selon différents scénarios affectant le bon fonctionnement de l'établissement, les modes opératoires à mettre en œuvre pour en contenir les impacts et rétablir l'activité. Les rôles et responsabilités des décideurs et des personnels clés sont précisés et ceux-ci ont les moyens (locaux, matériels, communications) de se rassembler pour diriger les opérations. Ce type d'organisation est requis dans les établissements de la banque et de l'assurance, notamment pour faire face à des pertes de ressources (bâtiments, collaborateurs, systèmes informatiques, prestataires externes). Si l'organisation de gestion de crise n'est pas étendue aux différents scénarios d'atteinte à la sécurité du système d'information, les établissements pourraient ne pas être en mesure de les gérer efficacement.

C'est pourquoi, il importe que des procédures de gestion de crise adaptées au risque cyber existent et soient régulièrement testées et ajustées. Ces procédures couvrent les différents scénarios de cyberattaques et leurs conséquences en disponibilité, confidentialité, intégrité et traçabilité. Elles prévoient des actions coordonnées avec les parties prenantes externes (partenaires, clients) et, le cas échéant, les autorités compétentes. Elles incluent un volet communication (médias, partenaires, clients) et information (instances dirigeantes, superviseurs).

Défaillances dans les dispositifs de contingentement des attaques

Le contingentement des attaques consiste à en stopper la propagation, y compris à des tiers, puis d'éradiquer les vecteurs d'attaque comme les malwares utilisés par l'attaquant. Cette démarche est un préalable à la reprise des opérations afin d'éviter une propagation incontrôlée de l'attaque.

Des équipes opérationnelles et dédiées sont en charge de la réponse aux incidents, telles les *Computer Security Incident Response Team* – CSIRT. Elles ont la responsabilité d'endiguer les attaques et d'en éradiquer les effets. Elles disposent de l'expertise et de l'autorité requises pour, le cas échéant, identifier les applications à arrêter et les réseaux à déconnecter. Ces équipes s'appuient en cas de besoin sur une expertise externe complémentaire et contractualisée. Idéalement, ces équipes sont capables de mettre en place des leurres pour détourner l'attention ou affaiblir l'attaquant durant les opérations de sécurisation du système d'information.

Défaillances dans les dispositifs de reprise des opérations

Le rétablissement du système d'information consiste à le remettre en service. Généralement, cette démarche est progressive. Les opérations peuvent d'ailleurs, le cas échéant, être réalisées par des procédures manuelles dégradées le temps de l'attaque, c'est-à-dire sans recourir à l'informatique. Lorsque les vecteurs d'attaque sont éradiqués, une reprise partielle du système d'information est possible, en utilisant les composants non-atteints. Ensuite, l'intégrité du système est reconstruite pour permettre un fonctionnement plein et normal du système d'information.

Le rétablissement du système d'information affecté par une attaque repose sur des procédures préparées à l'avance, régulièrement testées et revues. Ces procédures permettent de prioriser les actions de reprise et de garantir l'intégrité des systèmes et données restaurés.

Annexe : catégorisation du risque informatique

Macro processus	Facteurs principaux de risque informatique	Facteurs secondaires de risque informatique
Organiser le SI et sa sécurité	Implication insuffisante des instances dirigeantes	• Mauvaise perception des enjeux • Décisions inappropriées • Pilotage insuffisant
	Stratégie IT insuffisamment définie ou alignée avec la stratégie métier	• Manque d'anticipation des besoins métier, et des évolutions/enjeux/usages technologiques • Outils et niveaux de service inadéquats
	Pilotage budgétaire défaillant	• Allocation budgétaire insuffisamment alignée avec la stratégie • Allocation budgétaire absente ou insuffisamment claire • Suivi des dépenses insuffisant
	Rôles et responsabilités de la fonction informatique et de la fonction de sécurité informatique inadéquats	• Rôles et responsabilités mal définis, mal répartis ou mal communiqués • Profils inadaptés ou insuffisants
	Rationalisation insuffisante du SI	• Manque de maîtrise de l'architecture (urbanisation) • Incohérence des normes informatiques • Manque de maîtrise de l'obsolescence
	Insuffisante maîtrise de l'externalisation	• Cadre contractuel inadapté • Dépendance forte • Suivi insuffisant des niveaux de service • Dispositif de réversibilité insuffisant
	Non-respect des lois et règlements	• Non-conformité des besoins des métiers au droit applicable • Non-conformité du système d'information aux préconisations juridiques des métiers • Incompatibilité des normes informatiques avec le droit applicable
	Gestion des risques insuffisante	• Cartographie des risques inexistante ou partielle • Défaut dans l'analyse de risque • Dispositif de contrôle permanent insuffisant • Recensement et gestion insuffisants des incidents • Dispositif de contrôle périodique insuffisant

Macro processus	Facteurs principaux de risque informatique	Facteurs secondaires de risque informatique
Faire fonctionner le SI	Mauvaise gestion de l'exploitation (systèmes et réseaux)	• Insuffisance des moyens de production • Insuffisance dans la détection des erreurs ou anomalies • Insuffisance dans la gestion des incidents/problèmes • Non-respect des niveaux de service
	Mauvaise gestion de la continuité informatique	• Mauvaise organisation de la continuité • Insuffisance dans l'identification des scénarios d'indisponibilité • Non alignement de la continuité informatique avec la continuité métier • Protection insuffisante des moyens de production et de secours contre les accidents • Insuffisance des dispositifs de continuité • Tests insuffisants
	Mauvaise gestion des changements (projets, évolutions, corrections)	• Insuffisance dans la définition ou l'application des normes relatives à la gestion des changements • Mauvaise organisation dans la conduite de projets • Mauvaise prise en compte des exigences fonctionnelles et techniques • Défaut dans les logiciels • Insuffisance des tests • Défauts dans l'exécution des changements
	Mauvaise qualité des données	• Insuffisance de normalisation des données • Utilisation ou production par le système d'information de données erronées • Défaut de contrôle de qualité des données
Sécuriser le SI	Insuffisance dans la protection physique des installations	• Protections insuffisantes contre l'intrusion dans les bâtiments • Protection insuffisante des équipements informatiques
	Défaut d'identification des actifs	Défaillances dans : • l'inventaire des actifs • la classification des actifs
	Insuffisance dans la protection logique des actifs	Défaillances dans les dispositifs de : • Sécurité périmétrique • Protection contre les logiciels malveillants • Gestion des identités et des droits d'accès • Authentification des collaborateurs • Protection de l'intégrité des systèmes et des données • Protection de la confidentialité des données • Protection de la disponibilité • Gestion des correctifs de sécurité • Revues de sécurité • Sécurité des solutions externalisées • Sensibilisation à la sécurité des systèmes d'information
	Insuffisance dans la détection des attaques	Défaillances dans les dispositifs de : • Recueil et d'analyse des traces • Surveillance des comportements anormaux des utilisateurs
	Insuffisance du dispositif de réaction aux attaques	Défaillances dans les dispositifs de : • Gestion de crise • Contingentement des attaques • Reprise des opérations

819017 Bdf Dircom Studio Création - 01/2019