n°117 - 2020

Analyses et synthèses

Synthèse de l'enquête déclarative de 2019 sur la gestion de la sécurité des systèmes d'information des assureurs

ACPR
BANQUE DE FRANCE

SYNTHÈSE GÉNÉRALE

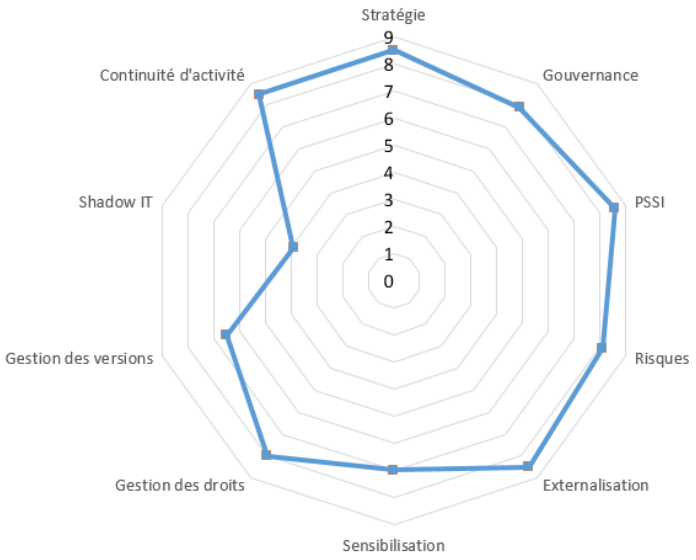
Avertissement au lecteur : contexte et limites

Le secrétariat général de l'ACPR a lancé fin 2019 une enquête par questionnaire portant à la fois sur la qualité des données et sur la sécurité des systèmes d'information auprès des acteurs opérant sur le marché français de l'assurance, sollicités soit directement soit par l'intermédiaire des fédérations professionnelles. Le questionnaire en ligne, ouvert du 16 septembre au 8 novembre, a permis de recueillir les réponses de 193 organismes représentant 84 % du chiffre d'affaires du marché de l'assurance et de la réassurance en France[1].

Ce questionnaire fait suite à ceux de 2015 et 2017 qui portaient, pour le premier sur la qualité des données (QDD), le système d'information (SI) et sa sécurité (SSI) et, pour le second, uniquement sur le volet SI/SSI. L'occurrence 2019 reprend de manière plus approfondie les thématiques de qualité des données et de sécurité des SI.

Ce document présente les principaux enseignements concernant la gestion du risque informatique des assureurs français, établis sur la base de leurs déclarations. Cependant, certains de ces constats apparaissent optimistes au regard des situations observées lors des contrôles sur place réalisés par l'ACPR.

Graphique 1 Notation des principaux processus impliqués dans la gestion de la SSI



Source ACPR

Par rapport aux précédents questionnaires, les aspects conceptuels de stratégie et de gouvernance liée à la sécurité des systèmes d'information (SSI) seraient aujourd'hui très majoritairement pris en compte de manière plus satisfaisante :

- la réalisation de la cartographie des risques SI semble une pratique plus répandue ;
- qui permet de bâtir une stratégie SSI, celle-ci participant et soutenant la stratégie globale de l'entreprise ;
- une politique de sécurité des systèmes d'information (PSSI) est définie et mise en œuvre ;

[1] Sur la base du chiffre d'affaires du marché de l'assurance et de la réassurance en France en 2018

- la proportion de responsables de la sécurité des systèmes d'information (RSSI) indépendants du directeur des systèmes d'information (DSI) est en augmentation ;
- la comitologie évolue : le dialogue s'instaure *via* la mise en place plus courante de comités dédiés à la sécurité des SI.

Les risques associés à la SSI seraient également mieux compris. Pour autant, les actions opérationnelles concourant à leur maitrise ne sont que partiellement en place et les deuxième et troisième lignes de défense s'investissent encore trop peu dans ces sujets : certaines pratiques de vérification de la sécurité se sont démocratisées comme les tests d'intrusion sur les sites web accessibles depuis l'extérieur, ce qui n'est pas encore le cas pour le réseau interne. En revanche, leurs conclusions restent cantonnées aux équipes techniques et sont encore peu partagées avec le top management et les instances de contrôle interne (contrôle permanent, audit interne, comité des risques et de l'audit…).

Les campagnes de sensibilisation au sein des organismes se développent : la proportion d'assureurs ayant mis en place des actions de sensibilisation de leurs collaborateurs est en augmentation. De plus, ces actions de sensibilisation sont mieux ancrées dans l'environnement de travail[2] et sont plus sophistiquées qu'auparavant : les campagnes sont adaptées en fonction de l'actualité de la menace cyber et s'appuient sur des mises en situation (phishing, clés USB…). Toutefois, en l'absence de bilan des résultats, ces campagnes ne s'inscrivent pas encore dans un plan global de sensibilisation à long terme des collaborateurs.

La gestion de la sécurité en profondeur reste à renforcer : la revue des habilitations est un des piliers de la sécurité en profondeur. Pourtant, la revue annuelle des droits d'accès aux applications n'est pas systématique : une partie des assureurs n'en réalise toujours pas (cependant, leur proportion a diminué depuis l'enquête de 2017). Quand la procédure de revue existe, on constate une absence de discipline dans la régularité du cycle de mise en œuvre. De plus, la revue des comptes est mal, voire pas effectuée. On constate par ailleurs que le contrôle permanent n'est pas ou peu impliqué dans ces sujets.

La gestion de l'inventaire du parc informatique et la gestion des versions sont absolument nécessaires. Si la première est maintenant bien ancrée dans les processus, des progrès doivent être faits concernant la seconde. De surcroît, en l'absence d'une politique de gestion des versions proactive et prospective, la réalisation accrue de tests de vulnérabilité n'est pas totalement efficace.

Le plan de continuité/de reprise d'activité (PCA/PRA) est devenu un pilier de la stratégie d'entreprise et les sociétés sont désormais plus attentives à le tester régulièrement, en simulant des *scenarii* de crise dans lesquels il serait pertinent d'intégrer un scenario de cyber-attaque. En outre, la conception du PCA prend encore trop peu en compte les attentes et contraintes des métiers qui devraient pourtant logiquement orienter les objectifs de la reprise.

Par ailleurs, les contraintes de sécurité liées à l'externalisation paraissent de mieux en mieux intégrées. Pour autant, l'analyse de risques, notamment sur les enjeux de sécurité des SI, auxquels cette sous-traitance exposerait l'organisme d'assurance n'est pas systématique, notamment dans les organismes de taille plus modeste. Le renforcement des aspects contractuels, de la prise en compte des objectifs de sécurité dans les engagements de service et l'identification des risques liés à l'externalisation doivent rester un objectif fort quelle que soit la taille des organismes qui souhaitent y avoir recours.

[2] Notamment dans le processus d'accueil par l'inclusion dans le contrat de travail d'une clause de responsabilité quant à l'usage approprié du SI, par la signature d'une charte d'utilisation du SI…

Le recours à des solutions externes au système d'information (le *shadow IT*[3]) et l'usage des EUC[4] sont encore trop peu surveillés par les organismes malgré les risques de sécurité qu'ils représentent. Il en va ainsi de l'usage de solutions Cloud, parfois plus ergonomiques ou plus facilement accessibles que les solutions validées par les Directions informatiques, démultipliant les risques de fuites de données pour l'organisme. De même, la généralisation du télétravail doit s'accompagner de réflexions sur la sécurité des usages dans des environnements informatiques domestiques.

Enfin, le budget alloué à la sécurité des SI a légèrement augmenté depuis l'enquête 2017. Mais une part encore importante des organismes ne s'oblige pas à sanctuariser ce budget même si des actions de sécurité sont effectivement réalisées, ce qui *in fine* ne leur permet pas d'en pérenniser l'existence ni de suivre les dépenses de sécurité réellement engagées.

N.B. Les résultats ci-après sont le plus souvent présentés selon une segmentation du marché de l'assurance/réassurance en 4 catégories : petits, moyens, grands et très grands organismes, correspondant aux quartiles définis en fonction du chiffre d'affaires.

Mots-clés : risque cyber, stratégie SI, plan de continuité d'activité, gestion des risques, gestion des droits et des habilitations, gestion des versions

[3] Outils - systèmes d'information et de communication - sous toutes leurs formes (appareils personnels, logiciels, applications, services web, programmes…) qui sont développés/achetés/utilisés directement par leurs utilisateurs sans l'approbation ni la supervision de la direction informatique
[4] *End-User Computing* - programmes ou services non gérés par la DSI

Étude réalisée par le Pôle Qualité des données et Systèmes d'Information de la Direction des Contrôles Spécialisés et Transversaux de l'ACPR[5].

SOMMAIRE

[5] Ont contribué à cette étude Philippe BLAIRON, Jérôme JUSOT, Philippe LAM et Valérie PIQUET

Une stratégie et une gouvernance de la SSI qui se renforcent

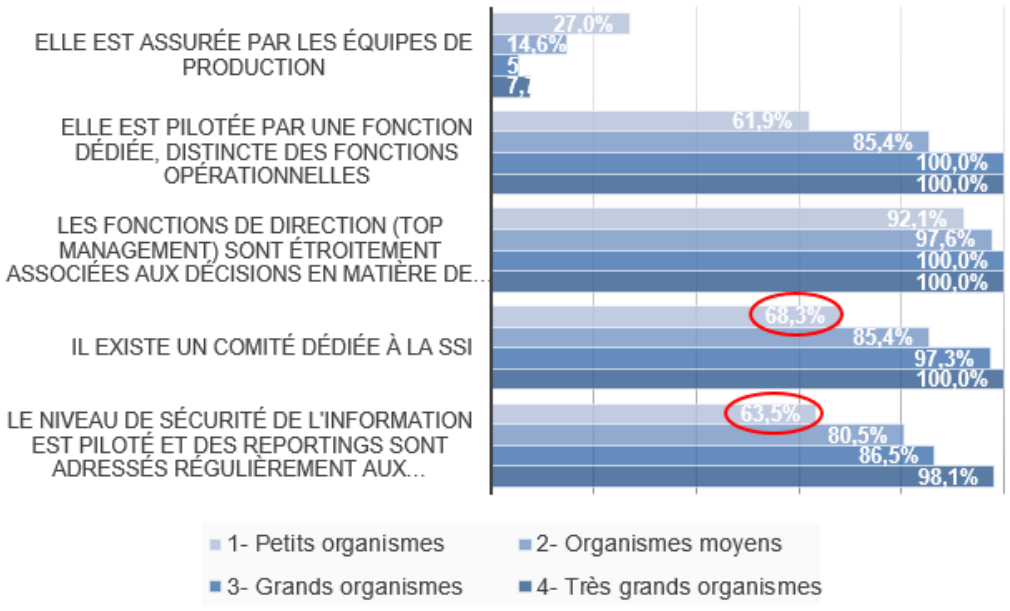
1. Stratégie SSI

La grande majorité des assureurs (93 % des répondants), quelle que soit leur taille, déclare avoir défini une stratégie en matière de sécurité des SI (SSI) formalisée dans une politique (PSSI) contre 59 % en 2017. Ce taux atteint 100 % pour les grands organismes.

Dans 83 % des cas, la stratégie SSI s'appuierait sur la cartographie des risques de sécurité SI et serait alignée pour 86 % des organismes avec leur stratégie d'entreprise. Cependant la stratégie SSI dans les organismes de taille modeste reste un enjeu pour l'avenir puisque :

- 32 % n'ont pas mis en place de comité dédié à la SSI ;
- 36 % ne disposent pas d'un reporting à transmettre régulièrement aux fonctions de direction.

Graphique 2 Les caractéristiques de la gouvernance SSI



Source ACPR

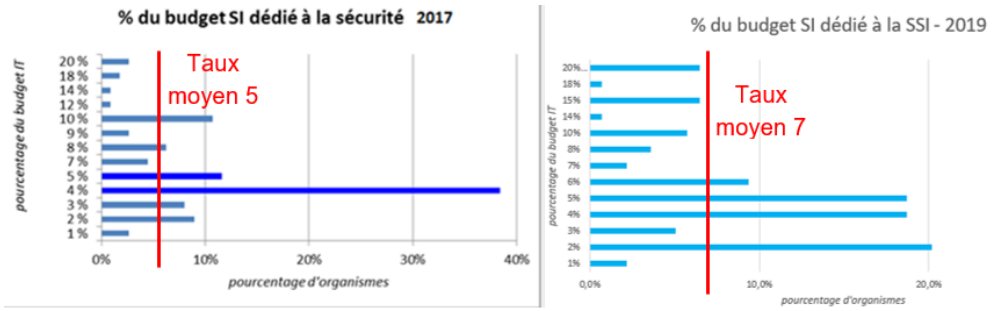
2. Politique SSI

Une politique (PSSI) est définie au sein de 93 % des répondants. Pour autant, le contrôle de sa correcte application par la 2ème et/ou 3ème ligne de défense demeure trop limité pour les petits organismes (73 % d'entre eux seulement).

3. Budget SSI

En matière de budget de sécurité des SI : la situation a évolué entre 2017 et 2019 : Le budget moyen est passé de 5 à 7 % du budget total SI, quand la valeur médiane s'est déplacée de 4 à 6 %. Par ailleurs, 25 % des organismes ne réservent pas de budget spécifique pour les dépenses engagées au titre de la SSI. Ce choix de gestion financière globalisée présente des inconvénients puisqu'il ne permet pas d'objectiver le budget consacré à la sécurité des systèmes d'information, qu'il permet des arbitrages entre activités de nature différentes et ne garantit pas la pérennité de l'allocation budgétaire dédiée à la sécurité. Il est souvent l'un des symptômes caractérisant un pilotage de la sécurité peu mature.

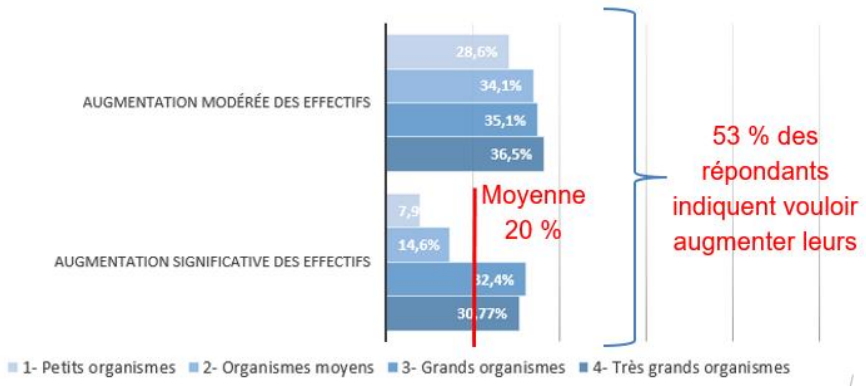
Graphique 3 Évolution du budget SI consacré à la sécurité entre 2017 et 2019



Source ACPR

En complément, concernant la gestion RH des compétences en matière de SSI, 14 % des organismes annonçaient en 2017 vouloir augmenter significativement leurs effectifs spécialisés en sécurité. Cette ambition est toujours de mise puisque cette proportion atteint 20 % en 2019. Comme en 2017, ce besoin accru de spécialistes est davantage identifié par les organismes importants et très importants. Cette demande portée par l'ensemble des secteurs économiques engendre une forte tension sur le marché de l'emploi des spécialistes en sécurité. En l'absence de recrutement, les organismes d'assurance optent soit pour la sous-traitance d'une partie des activités, soit pour leur réalisation partielle en reportant le résiduel.

Graphique 4 Prévisions de mouvements RH de spécialistes en sécurité du SI à horizon un an



Source ACPR

La gestion des risques SSI s'est étoffée mais s'appuie sur un dispositif de contrôle interne incomplet

1. Inventaire des actifs et identification des risques SSI

97 % des répondants indiquent réaliser un inventaire des actifs SI, sa mise à jour étant effectuée au fil de l'eau par 80 % des organismes. Pour mémoire, en 2017, l'inventaire et la cartographie des SI étaient encore partiels pour 39 % des organismes dont plus de la moitié (55 %) n'était pas en capacité d'identifier les zones du SI à isoler en cas de cyber-attaque.

En parallèle de cette apparente amélioration concernant la connaissance des composants du SI, l'identification des risques SSI est réalisée par 98 % des répondants. Chez ceux-ci, ces risques sont intégrés dans la cartographie des risques opérationnels et font l'objet d'une revue annuelle.

2. Prise en compte des risques SSI dans le dispositif de contrôle interne

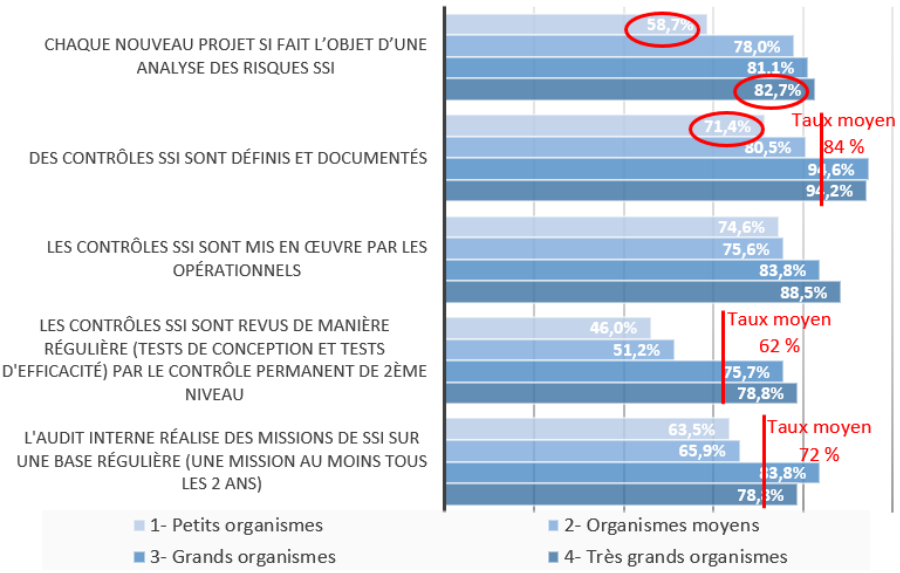
L'identification des risques n'engendre pas pour autant leur prise en compte automatique dans le plan de contrôle SSI. En effet, les contrôles relatifs à a sécurité des SI ne sont définis et documentés que par 84 % des organismes ayant répondu, ce taux baissant à 71 % pour les plus petites structures. Par ailleurs, les revues de ces contrôles SSI en collaboration avec les équipe du contrôle permanent (2ème niveau/2ème ligne de défense) ne sont effectuées régulièrement que par 62 % des participants.

Ainsi, la compréhension conceptuelle du risque SSI semble avoir progressé alors que les actions de contrôle permettant d'en assurer une maitrise opérationnelle pertinente semblent être en retrait.

S'agissant des actions portées par la 3ème ligne de défense, encore 28 % des répondants (contre 55 % en 2017) réalisent, en moyenne, moins d'une mission d'audit de sécurité tous les deux ans.

En complément, 17 % des très grands organismes et 41 % des plus modestes engagent des projets informatiques sans en faire une analyse de risque de sécurité préalable, ce qui illustre là-encore un manque de maturité par rapport à la problématique de sécurité.

Graphique 5 Caractéristiques du dispositif de contrôle interne en matière de risques SSI



Source ACPR

3. Actions de prévention : sensibilisation des collaborateurs

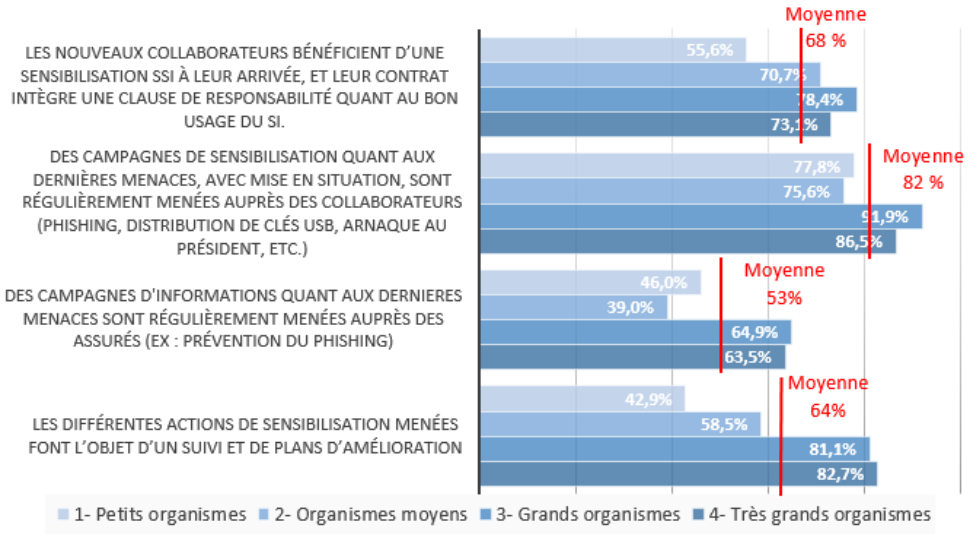
Lors du sondage de 2017, les organismes mobilisaient encore trop peu de moyens pour sensibiliser leurs utilisateurs/collaborateurs à la cyber-sécurité. En effet, à l'époque, 44 % d'entre eux se contentaient de la signature d'une charte d'utilisation du SI. Celle-ci est signée dans 68 % des organismes ayant répondu en 2019.

De plus, 82 % des organismes lancent aujourd'hui (contre 29 % en 2017) des campagnes de sensibilisation spécifiques à la cyber-sécurité, reflétant les dernières menaces avec une mise en situation (phishing, distribution de clés USB, arnaque au président, etc.).

Cependant, deux axes doivent encore faire l'objet d'améliorations :

- le premier concerne la sensibilisation auprès des assurés que seuls 53 % des répondants mettent en œuvre ;
- le second concerne l'évaluation de l'efficacité desdites campagnes, complétée d'un suivi dans le temps des plans d'action mis en place : pour l'heure, 64 % des organismes déclarent effectuer ce suivi.

Graphique 6 Les différentes actions de sensibilisation à la SSI



Source ACPR

La gestion de l'externalisation se développerait et les aspects contractuels se renforceraient

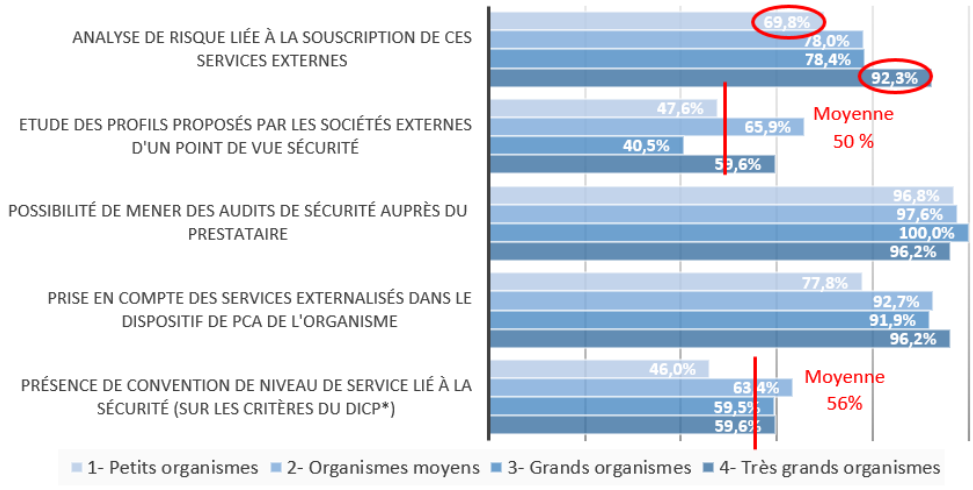
Le recours à des prestataires externes pour la réalisation ou la gestion d'activités de l'organisme d'assurance ne le soustrait pas aux responsabilités qui y sont attachées.

Pour autant, l'analyse des risques liés au transfert d'activités n'est toujours pas systématisée, notamment dans les petits organismes (où seuls 70 % déclarent le faire contre 92 % pour les plus grands). De plus, l'étude du profil de sécurité SI des sociétés approchées dans le cadre d'une potentielle sous-traitance n'est pas encore une pratique largement répandue (1 répondant sur 2 déclare le faire). On note toutefois une progression puisqu'en 2017, la sécurité du SI n'était considérée comme un critère de sélection des prestataires que par 32 % des organismes répondants, et parmi eux, un quart n'identifiaient pas les interdépendances de leur SI avec celui des partenaires.

En 2019, l'identification et le pilotage des prestataires critiques seraient quasi-systématiques dans la population des répondants. Ils auraient par ailleurs significativement renforcé les contrats de sous-traitance en se ménageant la possibilité de réaliser des audits chez le prestataire, en incluant des clauses sur la localisation des données et sur la réversibilité des services externalisés. Ils auraient en outre élargi l'horizon de leur plan de continuité (PCA – *Cf. infra*) pour intégrer les services externalisés.

Cependant, la sécurité ne constitue pas encore un élément incontournable des contrats de service (SLA) : seuls 56 % des répondants indiquent inclure la sécurité dans les conventions de service. En termes de risques, on peut souligner que pour l'organisme qui sous traite, ceci nuit à l'efficacité du pilotage de sa SSI envisagée dans sa globalité.

Graphique 7 Caractéristiques de la contractualisation de prestations externes / services externalisés



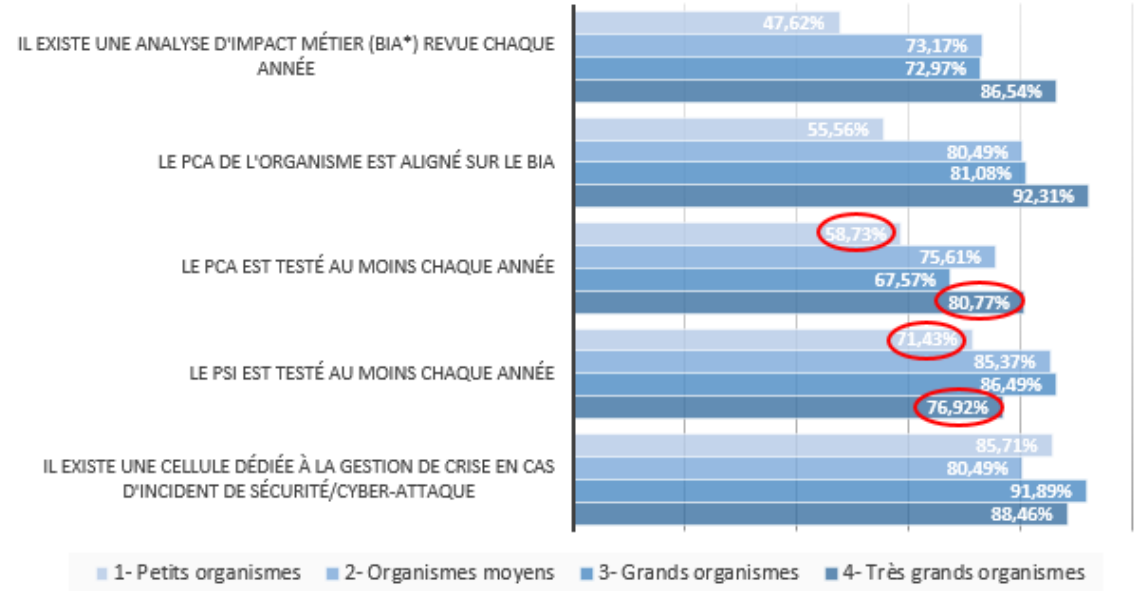
Source ACPR

Le plan de continuité est devenu un pilier de la stratégie d'entreprise, pour autant il doit être mieux aligné avec les besoins métiers

Alors que l'inventaire des processus critiques et le plan de continuité d'activité (PCA) incluant le plan de secours informatique (PSI) sont des éléments quasi-systématisés d'après les répondants à l'enquête de 2019, ceux-ci ne s'obligent pourtant pas à les tester annuellement[6]. Ce constat concerne encore 19 % des répondants de grande envergure et est encore plus aigu chez les plus petits organismes répondants, dont 41 % seulement n'éprouvent pas ou pas régulièrement la robustesse de leur PCA. On note toutefois la progression globale du marché vis-à-vis de cette pratique puisqu'en 2017, 10 % des participants avaient déclaré ne pas disposer d'un plan de gestion de crise documenté et régulièrement revu pour faire suite à une cyber-attaque et parmi les répondants qui s'en étaient dotés, 46 % déclaraient ne jamais le tester en simulant notamment le scenario de cyber-attaque.

Par ailleurs, la réalisation d'une étude d'impact métier (BIA[7]), étape préalable à l'élaboration d'un PCA qui garantit la prise en compte des besoins des métiers dans les objectifs du PCA, ne constitue pas encore une pratique systématisée : ainsi, un tiers des répondants n'en dispose toujours pas (cette proportion montant à plus de 50 % pour les petits organismes).

Graphique 8 Usages en matière de plan de continuité d'activité



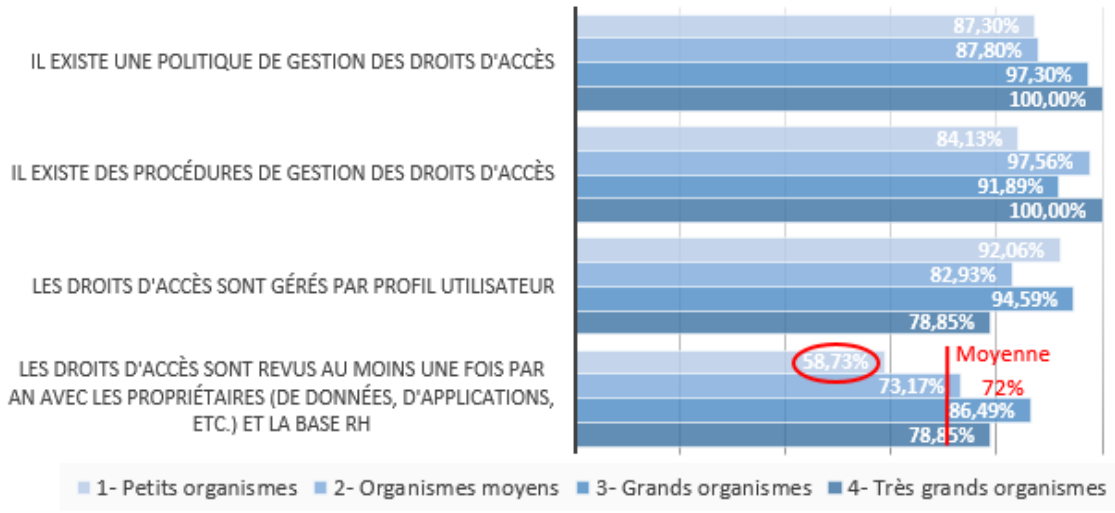
Source ACPR

[6] qui est la fréquence minimale recommandée
[7] Business Impact Analysis

La gestion opérationnelle et la sécurité en profondeur doivent être renforcées

La revue des habilitations est un des piliers de la sécurité en profondeur. Si les organismes semblent s'être dotés d'une politique et de procédures de gestion des droits, sa mise en œuvre n'est pas encore totale : la revue annuelle des droits n'est toujours pas effectuée par 28 % des organismes répondants (à noter qu'ils étaient 34 % à déclarer ne pas le faire au moins annuellement en 2017) et ce chiffre monte à 41 % pour les plus petites structures.

Graphique 9 Caractéristiques de la gestion des droits

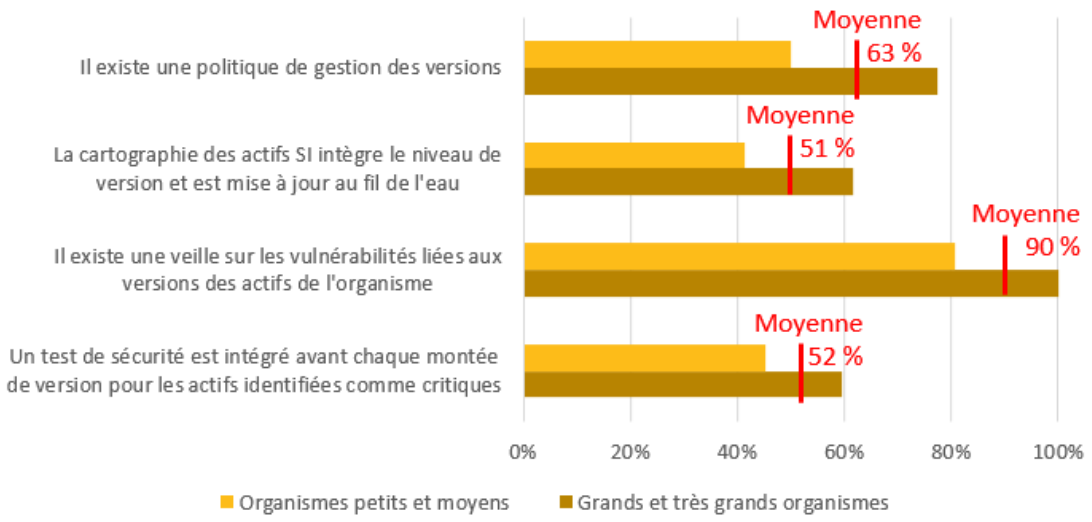


Source ACPR

De même, l'attention portée à la gestion des comptes à privilège ainsi que le respect des principes de ségrégation des rôles et de moindre privilège semblent ne pas être systématisés et constituent un axe majeur d'amélioration de la gestion des droits d'accès.

Par ailleurs, même si la gestion de l'inventaire des actifs SI est devenue une pratique incontournable (97 % des réponses – *cf. supra*), la gestion des versions des équipements n'est pas encore ancrée dans les pratiques et les inventaires ne sont implémentés de la version des actifs que dans 51 % des cas.

Graphique 10 Pratiques en matière de gestion des versions des applications



Source ACPR

À ce jour, seuls 63 % des répondants possèdent une politique de gestion des versions. Celle-ci doit notamment leur permettre d'appréhender de manière homogène et efficace les trains de version et de définir une réelle stratégie quant aux montées de version en agissant de manière proactive et non réactive face aux annonces des éditeurs (obsolescence/fin de support, alertes/failles de sécurité…). Cette proportion baisse à 55 % dans les structures plus modestes.

Pour autant, la veille sur les vulnérabilités des versions en place semble avoir progressé. En effet, 90 % des répondants indiquent effectuer cette veille qui représente la première action de maitrise à inscrire dans une (future) politique de gestion des versions.

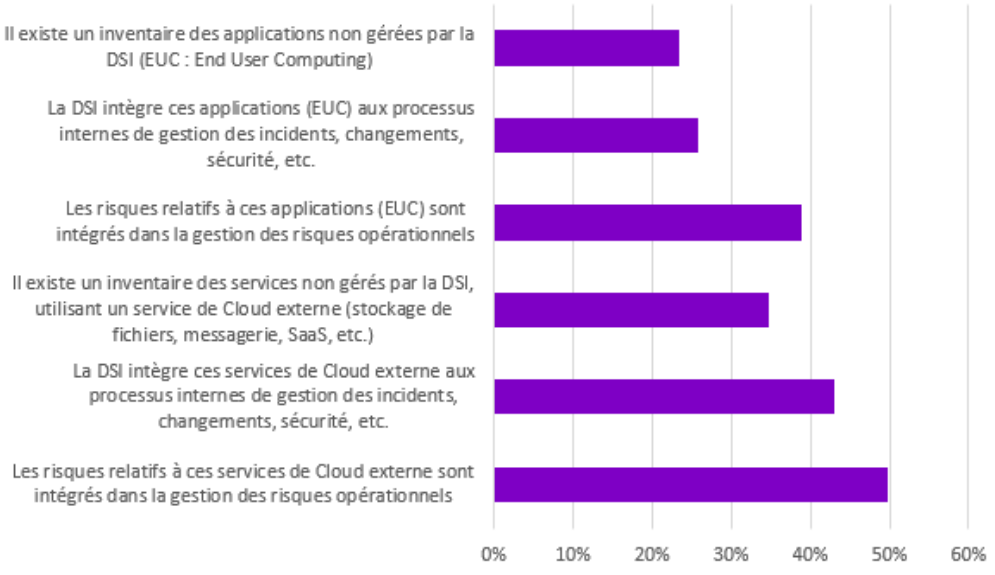
De plus, la pratique des tests de sécurité sur les équipements considérés comme critiques est intégrée de façon très contrastée dans les organismes : ils sont réalisés par 60 % des répondants parmi les organismes les plus importants et par 45 % parmi les moyens et modestes.

Une gestion du « shadow IT » encore lacunaire

La thématique « Shadow IT » n'avait pas été abordée lors de la précédente enquête en 2017. Ce terme recouvre les outils - systèmes d'information et de communication - sous toutes leurs formes (appareils personnels, logiciels, applications, services web, programmes…) qui sont développés/achetés/utilisés directement par leurs utilisateurs sans l'approbation ni la supervision de la direction informatique.

À ce jour, peu d'organismes (23 % des répondants indépendamment de leur taille) référencent et intègrent la gestion des EUC (*End-User Computing* - programmes ou services non gérés par la DSI). Cependant, 39 % des répondants déclarent prendre en compte les risques opérationnels liés à ces EUC, ce qui reste insuffisant.

Graphique 11 Prise en compte du Shadow IT



Source ACPR

Les services de type *Cloud Computing* semblent en revanche davantage pris en considération que les applications « internes » -, leur identification par les services techniques étant facilitée par les validations à obtenir dans le cadre de procédures d'achat et de facturation. Pour autant, l'inventaire de ces services, leur intégration dans les processus internes de gestion, notamment sous l'angle de la sécurité et des risques opérationnels, sont loin de constituer des pratiques systématiques, et ce, y compris chez les organismes de taille importante (moins de 50 % des répondants).