n°145 - 2023

Analyses et synthèses

Synthèse de l'enquête déclarative de 2022 sur la gestion de la sécurité des systèmes d'information des organismes d'assurance

ACPR
BANQUE DE FRANCE

SYNTHÈSE GÉNÉRALE

Avertissement au lecteur : contexte et limites

Le secrétariat général de l'ACPR a lancé en 2022 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 18 mai au 30 juin, a permis de recueillir les réponses de 239 organismes.

Cette autoévaluation fait suite à celles de 2015, 2017 et 2019 qui portaient sur la qualité des données (QDD), le système d'information (SI) et sa sécurité (SSI). L'occurrence 2022 reprend les thématiques de qualité des données et de sécurité des SI des années précédentes et inclut de nouvelles questions.

Ce document présente les principaux enseignements concernant la gestion du risque informatique par les assureurs français, établis sur la base de leurs déclarations. Toutefois, certains de ces constats apparaissent optimistes au regard des situations observées lors des contrôles sur place réalisés par l'ACPR. Dans la suite, sous le vocable « les organismes », sera désignée la population des organismes ayant répondu à l'enquête.

Synthèse

L'enquête SSI de 2022 montre que les organismes ont pris conscience de certains enjeux liés à la sécurité de l'information. Cependant, nombre d'entre eux n'ont pas encore atteint un niveau de maturité suffisant leur permettant de se prémunir contre le risque cyber prégnant. En effet :

Les aspects conceptuels de stratégie et de gouvernance liés à la sécurité des systèmes d'information (SSI) semblent mieux pris en compte. Cependant, **le positionnement de la fonction Sécurité de l'Information reste un enjeu pour de nombreux organismes**, en particulier car il n'assure pas systématiquement une indépendance suffisante vis-à-vis des fonctions opérationnelles ainsi que l'accès privilégié aux instances dirigeantes. Le budget moyen alloué à la sécurité des SI apparait stable entre 2019 et 2022, s'établissant à près de 7 % du budget informatique.

Le besoin de profils spécialisés en sécurité de l'information reste élevé dans le secteur de l'assurance alors que la demande pour ce type de profil, soutenue par l'ensemble des secteurs économiques, est déjà en forte tension.

Le dispositif de gestion des risques SSI se révèle souvent incomplet et, *de facto*, ne permet pas de piloter les risques efficacement. En effet, en la matière, les contrôles de premier niveau ne sont pas systématiquement réalisés ni systématiquement revus par la seconde ligne de défense. Facteur aggravant, la périodicité erratique des missions d'audit interne ne permet pas de juger de la robustesse du dispositif de maitrise des risques SSI.

La sensibilisation au cyber risque est désormais ancrée dans les processus internes. Elle se traduit par des démarches complémentaires (charte d'utilisation du SI, formations, insertion d'une clause de responsabilité quant à l'usage du SI dans le contrat de travail, campagnes d'hameçonnage) qui se sont développées depuis 2019. Bien que les campagnes de sensibilisation ciblent encore trop peu les prestataires et encore moins les assurés, leur efficacité semble être maintenant mesurée, ce qui permet d'adapter le plan d'amélioration continue.

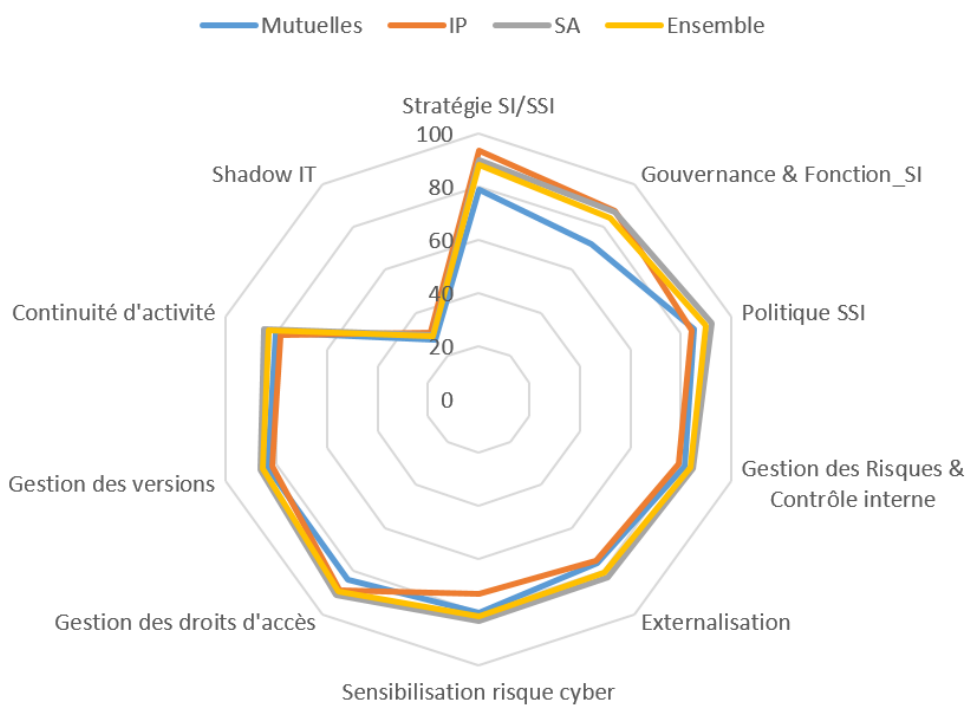
La gestion opérationnelle de la sécurité aurait progressé depuis 2019. D'une part, la gestion des mises à jour des actifs informatiques serait plus robuste et l'identification des vulnérabilités auxquelles sont soumis ces actifs se serait développée. Pour autant, **les mesures de correction opérationnelles de ces vulnérabilités restent perfectibles. Par ailleurs, les dispositifs d'identification et d'analyse proactive des cyber-menaces (« *threat intelligence* ») doivent être généralisés**. D'autre part, si la revue annuelle des habilitations est une pratique qui semble avoir significativement progressé, elle n'est pas effectuée avec la rigueur nécessaire ni sur l'intégralité des périmètres.

La démarche de continuité d'activité est globalement adoptée par les organismes d'assurance. Néanmoins, **en l'absence d'une analyse préalable des besoins métiers ainsi que de tests réguliers et opérationnels de la robustesse du PCA, cette démarche s'avère incomplète et donc inefficace**. De la même manière, les exercices de simulation de gestion de crise cyber devraient être promus et initiés par la direction générale et menés régulièrement. En effet, seule la réalisation en conditions réelles de ces tests, aussi bien pour le PCA que pour la gestion de crise, est de nature à apporter une réponse efficace en cas de sinistre informatique.

Alors que le recours à l'externalisation s'est généralisé, **l'analyse des risques, notamment sur les enjeux de sécurité des SI, n'est toujours pas systématisée**. L'utilisation massive de services en nuage (*cloud*) modifie la nature des risques auxquels les organismes sont exposés. Notamment, la réversibilité des services n'est pas systématiquement prévue et le niveau réel de sécurisation de ces services n'est pas mesuré. 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 et quelle que soit la solution (nuage ou autre) retenue.

L'attribution d'un score aux réponses individuelles permet de mesurer et visualiser la maturité moyenne du marché sur les différentes thématiques abordées dans l'enquête et de constater d'éventuels écarts entre les différentes populations d'organismes :

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



Source ACPR

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

Étude réalisée par le Pôle Qualité des données et Systèmes d'Information de la Direction des Contrôles Spécialisés et Transversaux de l'ACPR[1].

[1] Ont contribué à cette étude Jérôme JUSOT, Paul MONCHAUZOU, Edwin SCHEER, Charles SLOMSKI et Valérie PIQUET

SOMMAIRE

TYPOLOGIE DES RÉPONDANTS

Les résultats de cette enquête sont établis sur la base des réponses de 239 organismes (contre 198 en 2019). Les organismes ayant répondu à cette nouvelle enquête totalisent 88 % du chiffre d'affaires réalisé en 2021 par les sociétés d'assurance et de réassurance agréées en France.

Les résultats peuvent être visualisés selon 2 types de répartition des répondants. Ils sont principalement détaillés en fonction de la taille des organismes. À cet effet, une segmentation a été définie selon le chiffre d'affaires des organismes (primes ou cotisations) en 2021 :

- Premier quartile, primes entre 0 et 68 MEUR : « Petits organismes » ;
- Second quartile, primes entre 68 MEUR et 383 MEUR : « Organismes moyens » ;
- Troisième quartile, primes entre 383 MEUR et 1 200 MEUR : « Organismes importants » ;
- Dernier quartile, primes supérieures à 1 200 MEUR : « Organismes majeurs ».

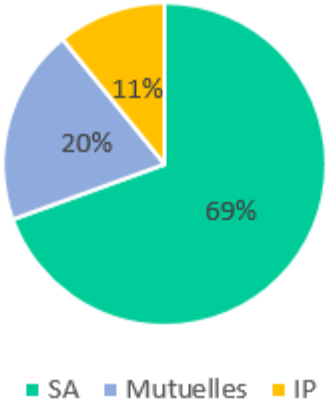
Les résultats sont parfois également présentés en fonction de la forme juridique des organismes, selon qu'ils relèvent du code des assurances[2], du code de la mutualité[3] ou du code de la sécurité sociale[4]. Par convention, dans la suite du document, les 3 groupes ainsi constitués seront respectivement nommés SA, Mutuelles et IP. Même si les effectifs des trois populations sont déséquilibrés (*cf. infra*), cette classification permet d'observer les éventuelles disparités entre elles : cette classification a vocation à « personnaliser » les résultats de l'enquête selon les 3 grandes populations opérant sur le marché de l'assurance en France mais peut avoir moins de sens du point de vue économique. Notamment, leur composition selon le critère de la taille est hétérogène : par exemple, le groupe des mutuelles comprend 76 % d'organismes de taille modeste tandis que le groupe des sociétés de (ré)assurance est constitué à 59 % d'organismes « importants » et « majeurs ». En particulier, l'évolution de la composition des groupes entre les enquêtes 2019 et 2022 peut interférer dans l'interprétation de l'évolution des résultats.

[2] Les organismes relevant du code des assurances sont les sociétés d'assurance et de réassurance, les fonds de retraite professionnelle supplémentaire (FRPS) et les succursales de pays tiers

[3] Les organismes relevant du code de la mutualité sont les mutuelles et les mutuelles et unions de retraite professionnelle supplémentaire (MRPS)

[4] Les organismes relevant du code de la sécurité sociale sont les institutions de prévoyance (IP) et institutions de retraite professionnelle supplémentaire (IRPS)

Graphique 2 Répartition des répondants selon leur forme juridique



Source ACPR

Le tableau ci-dessous synthétise la distribution des répondants selon les quartiles définis et selon le code dont ils relèvent :

		Taille d'organisme (total de primes)				Total répondants	Part (en %)	Marché 12/2021	Taux de participation
		Petits	Moyens	Importants	Majeurs				
Type d'organisme	Sociétés d'assurance et de réassurance, FRPS, succursales de pays tiers (SA)	29	39	52	46	166	69%	284	58%
	Mutuelles vc totalement substituées & MRPS (Mutuelles)	24	12	5	6	47	20%	350	13%
	Institutions de prévoyance et IRPS (IP)	6	9	3	8	26	11%	34	76%
Total répondants		59	60	60	60	239	100%	668	36%

N.B. : les 50 organismes de plus grande taille du marché français ont tous participé à l'enquête

RÉSULTATS DÉTAILLÉS

1. Vers une normalisation de la gouvernance SSI

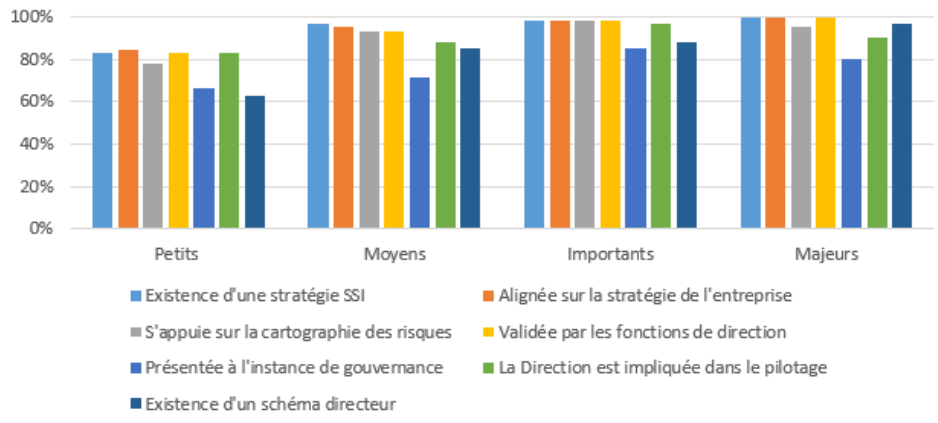
1.1 Stratégie SSI

Les répondants ont défini, dans leur grande majorité (95 % d'entre eux), une stratégie en matière de sécurité informatique, alignée sur les ambitions stratégiques de l'entreprise et validée par les fonctions de direction[5] qui la présentent dans une moindre mesure (76 %) aux instances de gouvernance/surveillance. De plus, les fonctions de direction ne s'impliquent pas systématiquement (90 %) dans le pilotage des axes majeurs de cette stratégie.

La cohérence entre la stratégie SSI et l'exposition aux risques semble plus recherchée qu'auparavant puisque 91 % des répondants (contre 83 % en 2019) s'appuient sur la cartographie des risques de sécurité SI pour établir leur stratégie SSI.

La traduction opérationnelle de la stratégie SSI en schéma directeur reste un enjeu pour les répondants hors acteurs majeurs puisque cette pratique ne concerne pour l'heure que 79 % d'entre eux, cette proportion tombant à 63 % pour les assureurs les plus modestes.

Graphique 3 Caractéristiques de la stratégie SSI



Source ACPR

1.2 Dispositif de gouvernance SSI

Le cadre de gouvernance de la sécurité des systèmes d'information s'appuie pour 95 % des répondants sur une Politique de Sécurité des Systèmes d'Information (PSSI). Toutefois, celle-ci ne donne pas systématiquement lieu (pour 5 % de cette population) à une traduction en procédures opérationnelles sur les thèmes spécifiques de la SSI. Par ailleurs, le contrôle de sa correcte application

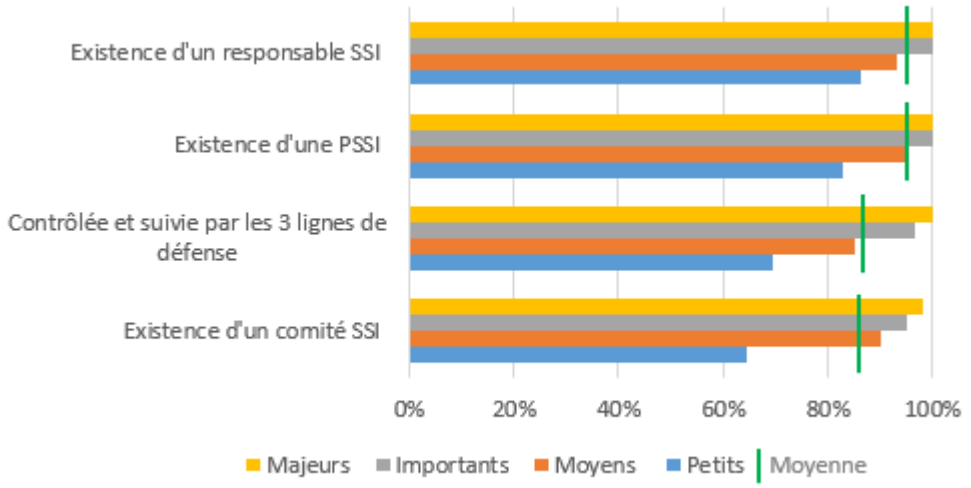
[5] Ce taux atteint 100 % pour les organismes majeurs

par le système de contrôle interne apparaît encore limité dans les organismes de taille modeste (69 % parmi les organismes de petite taille et 85 % parmi les organismes de taille moyenne).

Pour animer le dispositif de sécurité des SI, 95 % des organismes répondants se sont dotés d'un responsable de la sécurité des systèmes d'information (RSSI) - 10 % des organismes de petite et de moyenne taille n'en disposent pas. La fonction SI (au sens de l'orientation 7 de la Notice TIC[6]) bénéficie dans 84 % des sociétés d'un positionnement indépendant des fonctions opérationnelles (ce taux n'étant que de 66 % dans les organismes les plus modestes), cette indépendance étant renforcée dans 57 % des cas par le fait que cette fonction n'est pas rattachée hiérarchiquement à la Direction des Systèmes d'Information.

Enfin, pour coordonner et piloter la sécurité SI, 87 % des répondants ont mis en place un comité dédié à la SSI (resp. 64 % des petits organismes).

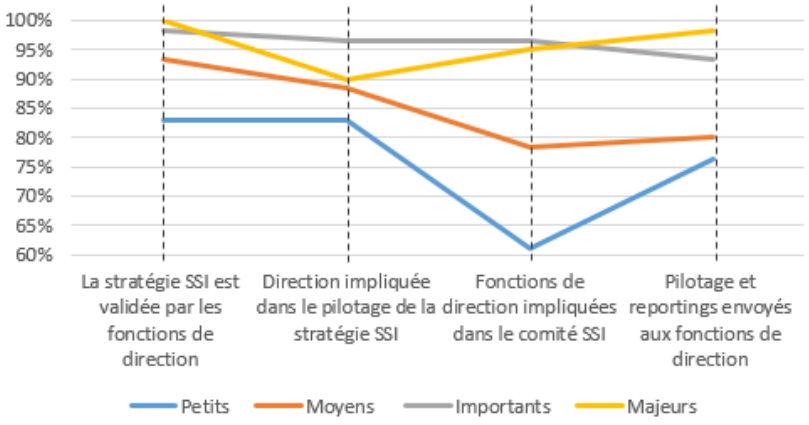
Graphique 4 Dispositif de gouvernance de la sécurité des systèmes d'information



Source ACPR

Quelle que soit la taille des répondants, les fonctions de direction semblent s'impliquer plus clairement dans la définition et le pilotage de la stratégie SSI que dans le pilotage de la sécurité à proprement parler.

Graphique 5 Implication des fonctions de direction dans la sécurité des SI



Source ACPR

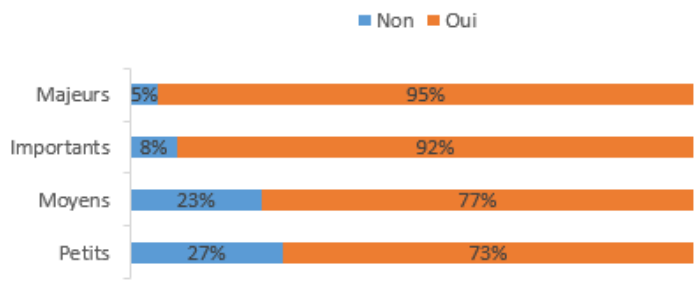
[6] https://acpr.banque-france.fr/sites/default/files/media/2021/07/02/20210702_notices_orientations_aeapp.pdf

1.3 Moyens alloués à la sécurité des systèmes d'information

En matière de budget de sécurité des SI, la situation est restée stable entre 2019 et 2022 : le budget moyen s'établit à près de 7 % du budget informatique total (5 % en 2017) et la valeur médiane à presque 6 %. Au regard des moyens financiers disponibles dans chaque groupe d'organismes, l'effort budgétaire réalisé par les organismes de petite et moyenne taille est supérieur à celui des structures importantes et majeures (resp. budget de 7,5 % contre 5,8 %).

De plus en plus d'organismes sanctuarisent le budget dédié aux dépenses engagées au titre de la SSI. Ainsi, 84 % en 2022 contre 75 % en 2019 allouent un budget propre à la SSI. Le choix d'une gestion pilotée du budget SSI est une pratique à privilégier puisqu'elle offre une vision plus fine des coûts et permet un meilleur pilotage financier.

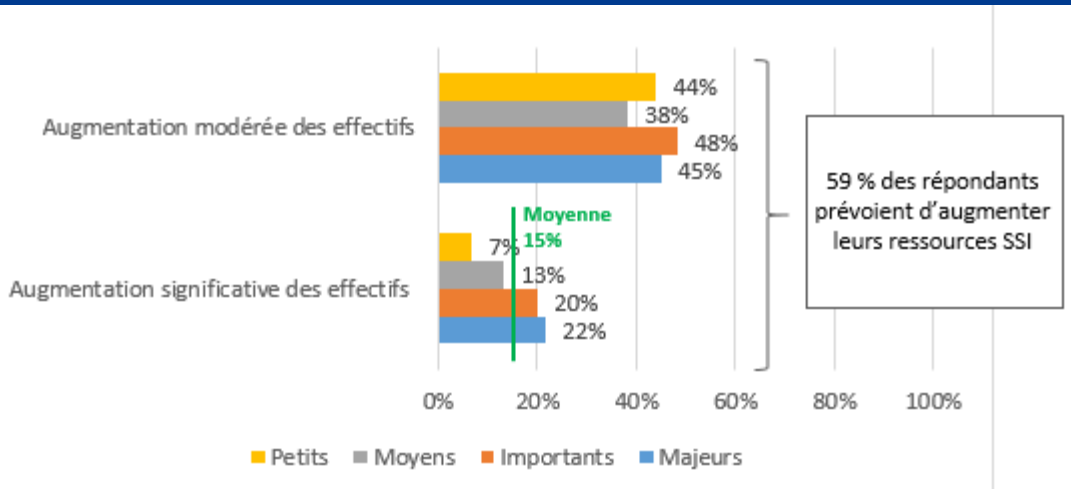
Graphique 6 Organismes allouant un budget spécifique à la sécurité des SI



Source ACPR

Concernant les ressources humaines allouées à la sécurité des SI, la proportion de répondants prévoyant d'augmenter leurs effectifs spécialisés en sécurité est de 59 % en 2022 contre 53 % en 2019. Dans cette population, un quart (15 % des organismes répondants) visent une augmentation significative (soit un taux proche du niveau de 2017 après le « pic » à 20 % en 2019). Comme en 2020, les ambitions fortes sur le niveau de ressources SSI sont portées par les organismes de taille importante et majeure.

Graphique 7 Prévisions d'augmentation des ressources SSI à horizon d'un an



Source ACPR

La demande de ressource spécialisée en SSI, portée par l'ensemble des secteurs économiques, reste à un niveau très élevé et engendre *de facto* une forte tension sur le marché de l'emploi pour les profils en question. En l'absence de recrutements, les organismes d'assurance optent pour la sous-traitance de tout ou partie des activités faisant appel à ce type d'expertise.

2. Le dispositif de gestion des risques et de contrôle interne en matière de SSI n'est pas encore totalement déployé

2.1 Profil de risque en matière de sécurité des SI

L'ensemble des organismes répondants (99 %) déclarent identifier les risques relatifs à la sécurité des SI (nommés de façon générique « risques SSI » dans la suite), les intégrer à la cartographie des risques opérationnels (97 %) et en réaliser une revue chaque année.

Cette apparente identification et qualification du risque générique SSI n'entraine pourtant pas systématiquement (seulement 65 % des répondants) de décision des entreprises sur le niveau de maitrise souhaité et, par déduction, sur le niveau de tolérance en la matière. Autrement dit, les entreprises qui ne s'obligent pas à définir leur tolérance au risque SSI ne sont pas en capacité de garantir que leur dispositif de maitrise du risque est en adéquation avec le niveau de risque maximum auquel elles admettent de rester exposées. Si la moindre maturité sur cette thématique est compréhensible s'agissant des organismes de petite et moyenne taille (43 %), elle l'est bien moins pour les organismes importants (27 %) et majeurs (18 %).

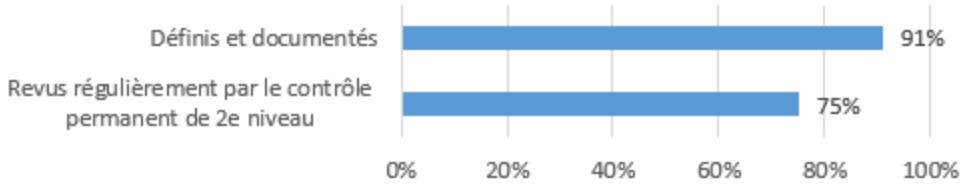
Pour 91 % des répondants, le profil de risque étudié dans le cadre de l'ORSA[7] tient explicitement compte de la thématique SSI dans la catégorie « risques opérationnels » et 76 %[8] des entreprises testeraient les impacts sur leur profil de risque de scenarii conduisant à l'indisponibilité du SI (en conséquence d'une cyber-attaque, d'une panne…) ou à des fuites de données. Or, l'examen des rapports ORSA délivrés jusqu'à présent à l'ACPR révèle d'une part que très peu d'entre eux fournissent des informations relatives aux risques SSI et, d'autre part, quand le sujet est abordé, que ces informations sont extrêmement succinctes.

2.2 Dispositif de contrôle interne en matière de risque de non sécurité des SI

Bien que les risques soient identifiés et reportés dans la cartographie des risques de l'entreprise, ils ne sont pas encore automatiquement associés à des contrôles opérationnels (dits de niveau 1). En effet, malgré une amélioration par rapport à 2019, 19 % des plus petites structures et 15 % des structures de taille moyenne (contre resp. près de 29 % et 20 % en 2019) déclarent ne pas définir de contrôles opérationnels SSI. Quand les contrôles de 1er niveau sont définis, ils sont quasi-systématiquement mis en œuvre.

Par ailleurs, le contrôle permanent de 2ème niveau ne réalise pas régulièrement de revue de conception et d'efficacité des contrôles de 1er niveau dans 25 % des organismes ayant répondu (en amélioration de 13 points par rapport à 2019), cette proportion allant de 8 % dans les organismes majeurs à 42 % dans les organismes de petite taille.

Graphique 8 Caractéristiques des contrôles SSI



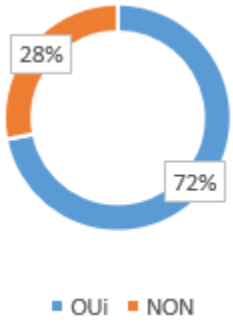
Source ACPR

[7] *Own Risk and Solvency Assessment* ou évaluation interne des risques et de la solvabilité

[8] ce taux variant (respectivement) de 88% des acteurs majeurs à 64 % des acteurs les plus modestes

Enfin, les pratiques de l'audit interne en matière de risque SSI n'ont pas évolué depuis 2019, et ce, au sein de chaque groupe de taille : ainsi, pour une proportion encore très importante (28 %) des organismes répondants, la fréquence des missions d'audit portant sur la sécurité des SI est inférieure à une tous les 2 ans.

Graphique 9 Réalisation d'une mission d'audit sur la sécurité SI au moins tous les 2 ans



Source ACPR

3. Les mesures concourant à la maitrise du risque SSI ont fait l'objet d'efforts significatifs

3.1 Prise en compte de la sécurité dans les projets informatiques

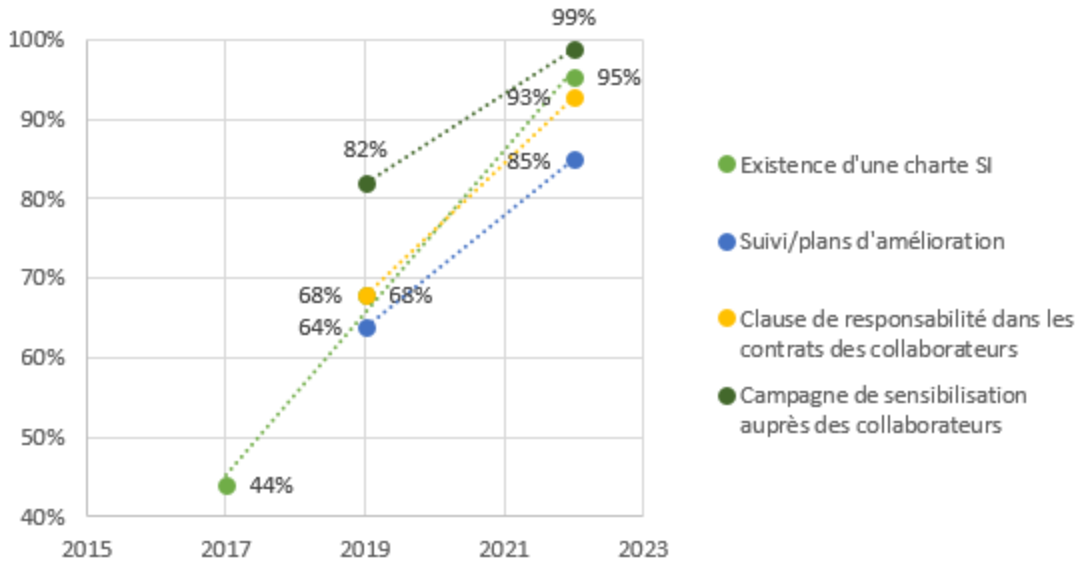
L'inclusion des analyses de risque de non sécurité dans les processus de projets informatiques semble s'être développée. Toutefois, la population (19 % des organismes en 2022 contre 26 % en 2019) qui déclare ne toujours pas en réaliser comporte des organismes de grande taille (resp. 7 % des acteurs majeurs et 15 % des acteurs importants). Les organismes de taille modeste semblent avoir adopté cette bonne pratique de façon significative (76 % en 2022 contre 59 % en 2019).

3.2 Sensibilisation au risque de non sécurité des systèmes d'information

Les mesures mises en œuvre concernant la sensibilisation et la formation à la thématique du risque cyber ont été significatives depuis 2019. Elles se traduisent par différentes initiatives :

- la mise en place d'une charte d'utilisation du SI que chaque collaborateur s'engage à appliquer : cette pratique, observée dans moins de la moitié des répondants en 2017 est maintenant presque institutionnalisée (95 %) ;
- un dispositif intégrant le risque cyber dès l'arrivée des collaborateurs (clause de responsabilité dans le contrat de travail et session de sensibilisation) : en moins de 3 ans, ce sont maintenant 93 % des répondants (contre 68 % en 2019) qui ont adopté ce dispositif ;
- les campagnes de sensibilisation, notamment par test d'hameçonnage (*phishing)*, se généralisent à l'ensemble du marché.

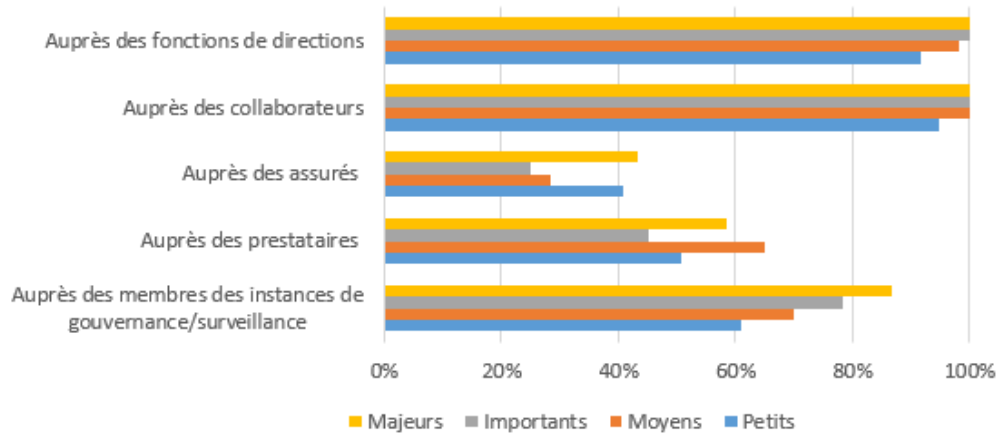
Graphique 10 Évolution des actions de sensibilisation relative à la sécurité des SI



Source ACPR

Sur le dernier point des campagnes de sensibilisation, les collaborateurs y compris occupant des fonctions de direction constituent la principale population ciblée et les organismes étendent peu à peu les campagnes de sensibilisation aux membres des instances de gouvernance/surveillance (surtout dans les organismes majeurs) et dans une moindre mesure aux collaborateurs prestataires de service. Les actions de sensibilisation auprès des assurés restent un axe à développer.

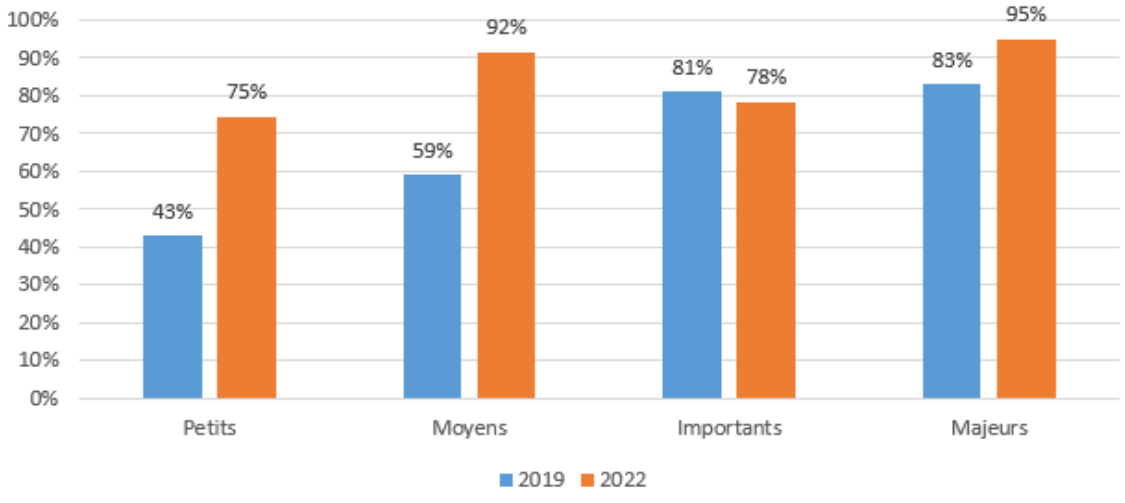
Graphique 11 Campagnes de sensibilisation aux risques de sécurité des SI



Source ACPR

De plus, la mesure de l'efficacité des campagnes de sensibilisation fait maintenant partie du processus et permet d'établir un plan d'amélioration de celles-ci dans 95 % des organismes (contre 83 % en 2019), les organismes de petite et moyenne taille ayant fourni des efforts conséquents.

Graphique 12 Suivi et plan d'amélioration des campagnes



Source ACPR

3.3 Couverture d'assurance

En 2022, 85 % des organismes ont indiqué avoir souscrit une assurance en cas de sinistre d'origine cyber.

4. Les mesures opérationnelles de gestion du risque SSI doivent être systématisées

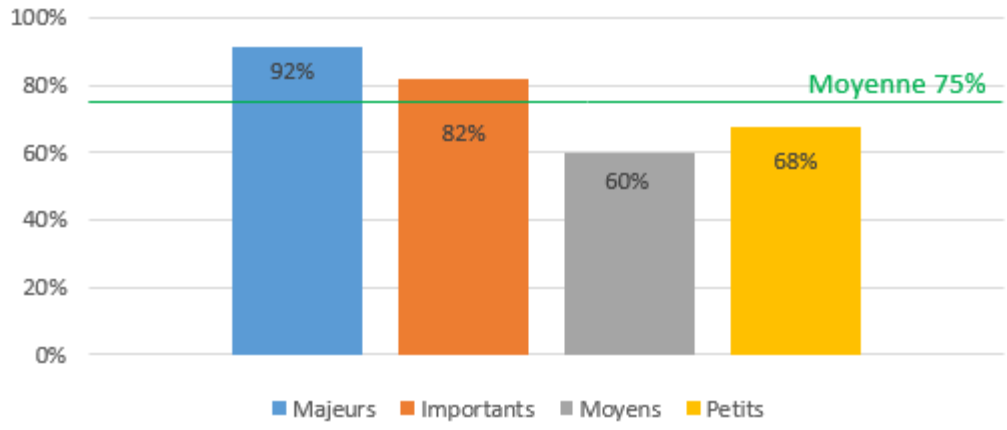
4.1 Inventaire des actifs et gestion des vulnérabilités

En 2022, 89 % des organismes indiquent mettre l'inventaire des actifs SI à jour régulièrement (en amélioration de 9 points par rapport à 2019). De plus, 76 % des répondants précisent que cet inventaire intègre le niveau de version et que ce dernier est mis à jour au fil de l'eau. L'ancrage de cette pratique est central pour la maitrise du parc informatique et constitue un prérequis incontournable pour le déploiement de la gestion des correctifs (*patch management*) qui s'appuie sur la connaissance de l'environnement interne.

Concernant plus spécifiquement la gestion des vulnérabilités, les organismes ont pris des mesures concernant l'identification des vulnérabilités auxquelles sont soumis leurs actifs. Ainsi, 90 % des répondants indiquent disposer d'un processus d'identification, de documentation et de remédiation des vulnérabilités (98 % pour les majeurs). À noter que le processus opérationnel de remédiations se révèle hautement perfectible et constitue un véritable défi pour de nombreux organismes.

Afin d'optimiser la connaissance et la protection de leur exposition au risque cyber, les organismes semblent s'être lancés massivement dans les dispositifs d'analyse proactive des menaces (*threat intelligence*) puisque cette pratique rassemble 75 % des répondants. Un effort reste toutefois nécessaire pour de nombreux organismes qui ne se sont pas encore dotés de cette analyse.

Graphique 13 Existence d'un dispositif de *threat intelligence*



Source ACPR

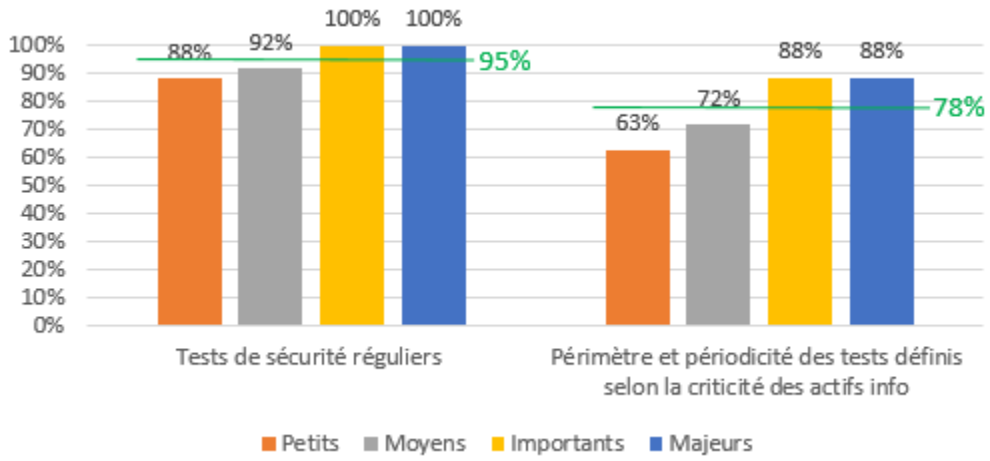
4.2 Gestion des droits d'accès

La revue des habilitations, un des piliers de la sécurité en profondeur, est une pratique en nette progression. En effet, 87 % des répondants déclarent réaliser cette revue au moins annuellement contre 72 % en 2019. Parmi les organismes les plus modestes, 27 % n'effectuent toujours pas une revue annuelle des droits d'accès. De plus, 84 % des organismes revoient *a minima* annuellement les droits d'accès techniques et génériques.

Par ailleurs, les organismes indiquent très majoritairement (95 % et ce, toutes tailles confondues) appliquer des procédures accordant des droits d'accès par profil utilisateur en respectant le principe de moindre privilège, en nette amélioration par rapport à 2019. Enfin, les plus petites structures ont plus de difficultés à assurer une complète ségrégation des rôles, déclarant mettre en œuvre cette pratique pour 78 % d'entre elles, contre 87 % pour l'ensemble des organismes.

4.3 Réalisation de tests de sécurité

Graphique 14 Réalisation de tests de sécurité

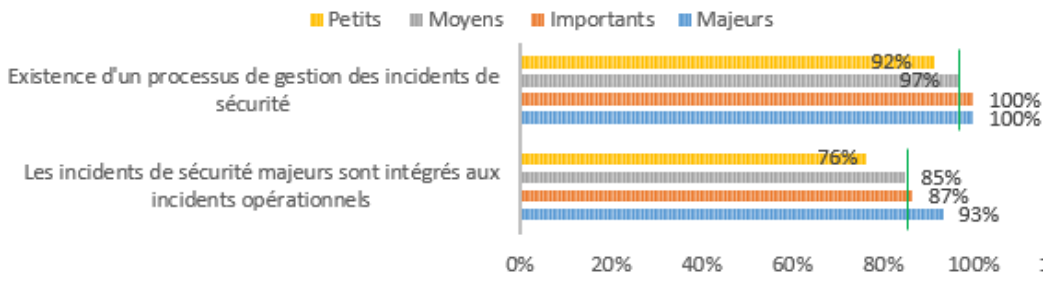


Source ACPR

95% des organismes indiquent réaliser des tests de sécurité (test d'intrusion, scans, etc) sur une base régulière. Cependant, pour 22 % des organismes, le périmètre et la périodicité des tests ne sont pas systématiquement définis selon la criticité des actifs informatiques ni selon l'évaluation des risques SSI, ce qui, au-delà de la question des frais engagés, limite leur pertinence et leur intérêt pour l'appréciation du niveau de sécurité de l'organisme.

4.4 Gestion des incidents de sécurité et opérationnels

Graphique 15 Gestion des incidents de sécurité des SI



Source ACPR

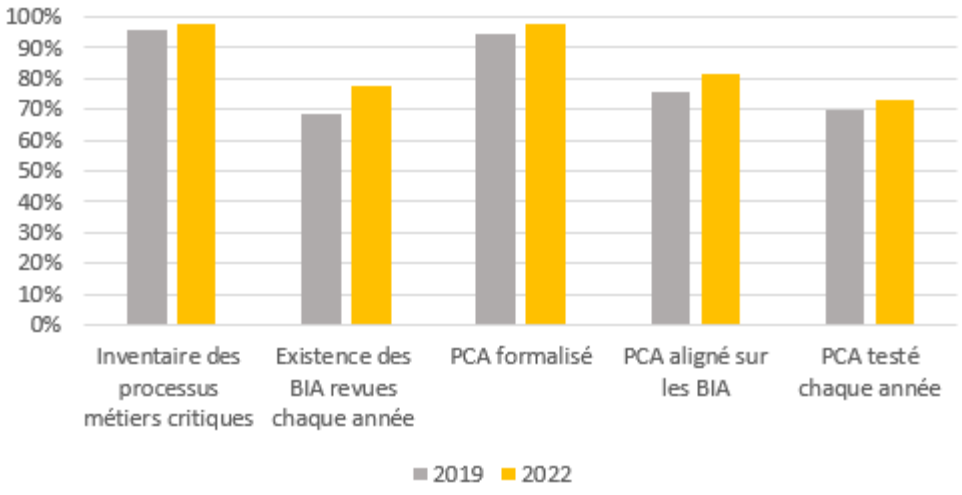
La mise en œuvre d'un processus de gestion des incidents de sécurité est généralisée (97 % des répondants). Ce processus prévoit dans 85 % des organismes l'intégration des incidents de sécurité majeurs dans le registre des incidents opérationnels. Cela permet leur prise en compte à part entière dans la gestion des risques opérationnels et constitue une source d'information essentielle pour préparer le cadre de gestion de crises provoquées par des incidents de sécurité majeurs.

5. Le plan de continuité d'activité doit être mieux aligné avec les besoins métiers

La continuité d'activité repose sur plusieurs dispositifs qui se complètent. La maturité et l'investissement des organismes dans les différents chantiers à mener apparaissent contrastés selon les thématiques et hétérogènes selon la taille des organismes. Toutefois, les organismes semblent avoir légèrement progressé depuis 2019 sur la plupart des sujets et indiquent :

- pour 97 % d'entre eux, disposer d'un inventaire des processus métiers jugés critiques,
- pour 77 % d'entre eux, mener des analyses d'impact métiers (BIA[9]) et réaliser leur revue chaque année (allant de 66 % des organismes de petite taille à 93 % des entités majeures),
- pour 71 % d'entre eux, réaliser une cotation des données selon leur degré de criticité. Cette pratique n'est pas encore systématisée dans les organismes majeurs (7 % d'entre eux ne le font pas) et constitue un axe d'amélioration future pour 43 % des organismes de petite et moyenne taille,
- pour 65 % d'entre eux, avoir mis en place une stratégie contre la fuite des données. Les organismes de taille majeure semblent largement (92 %) en avance dans le déploiement de cette pratique par rapport aux autres entités,
- pour 98 % d'entre eux, avoir formalisé un plan de continuité d'activité (PCA) qui serait revu chaque année dans 90 % des cas mais testé annuellement dans seulement 73 % des cas. Sur ce dernier point, des efforts restent à fournir dans tous les organismes quelle que soit leur taille. Enfin, les besoins métiers exprimés dans les BIA ne sont pris en compte que dans 82 % des plans de continuité.

Graphique 16 Points d'appui de la continuité d'activité



Source ACPR

À l'exception d'un cas, tous les organismes disposant d'un plan de continuité d'activité déclarent l'avoir complété en mettant en place et en formalisant un plan de secours informatique (PSI), revu chaque année dans 89 % des cas et testé annuellement par 82 % des répondants (cette proportion tombe à 64 % dans le groupe des organismes les plus petits). À nouveau, la cohérence avec les besoins

[9] *Business Impact Analyses.* Ces études visent à recueillir les besoins des métiers notamment en matière de durée maximale d'interruption des systèmes et d'indisponibilité des données. Elles constituent l'étape préalable à la conception du plan de continuité

exprimés par les métiers n'est assurée que dans 74 % des organismes et constitue un enjeu dans l'ensemble des entités. De plus, quatre organismes (l'un de taille importante et trois de taille très modeste) indiquent ne disposer ni d'un PCA formalisé ni d'un PSI formalisé.

En complément, la totalité des répondants précisent que leurs sauvegardes sont stockées sur un ou plusieurs sites éloignés du site principal. En revanche, le processus de restauration n'est pas testé annuellement par une population correspondant à 9 % d'entre eux qui inclut des organismes de taille importante et majeure.

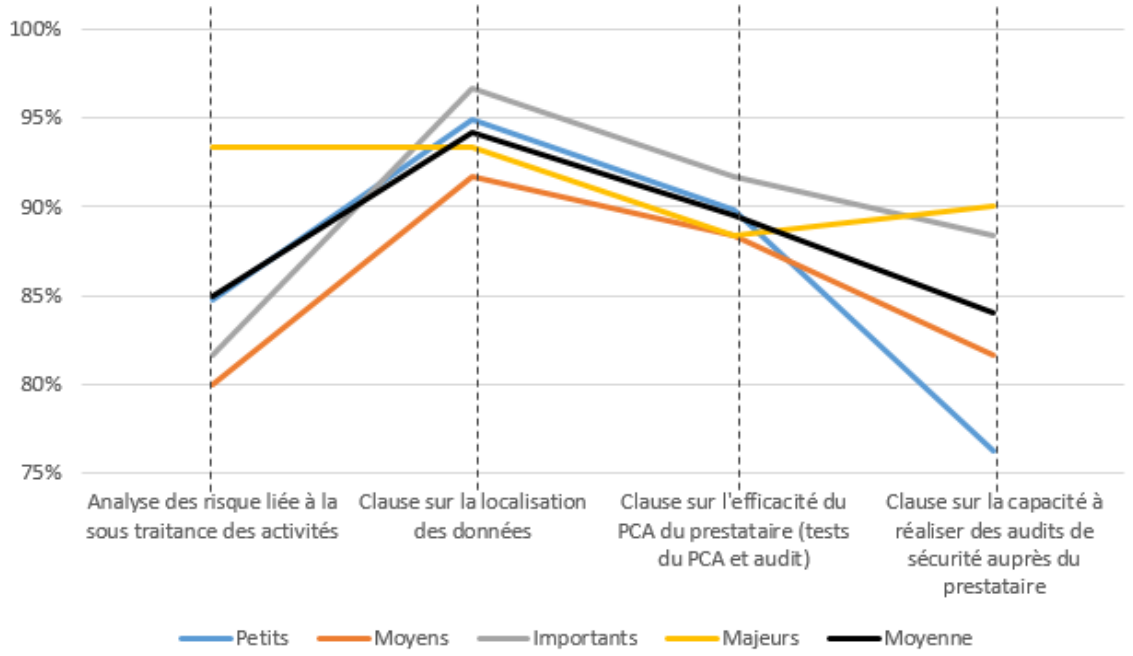
Enfin, la proportion d'organismes disposant d'une cellule de crise activable en cas de cyber attaque a crû de près de 8 points entre 2019 et 2022, et ce, tous organismes confondus.

6. Des efforts d'analyse et de pilotage restent nécessaires en matière d'externalisation

Le recours à des prestataires externes pour la réalisation ou la gestion d'activités de l'organisme d'assurance ne le soustrait aucunement aux responsabilités attachées à ces activités. Dans ce contexte, il est d'autant plus crucial que l'assureur organise le processus d'externalisation afin d'en avoir la maitrise selon les différents aspects par lesquels il se traduit. Or, le bilan en la matière apparait contrasté.

Ainsi, la contractualisation des prestations semble plus aboutie qu'en 2019 s'agissant des clauses sur la localisation des données (prévues par 94 % des répondants), des attentes en matière d'efficacité du plan de continuité d'activité (tests et audit) du prestataire (explicitées par 90 % des répondants) et la capacité à mener des audits de sécurité (toutefois moins répandue parmi les organismes de petite et moyenne taille). En revanche, l'analyse des risques liés au transfert des activités n'est toujours pas systématisée (15 % des organismes, toutes tailles confondues, n'en réalisent pas).

Graphique 17 Phase d'étude et de contractualisation de l'externalisation SI/SSI



Source ACPR

Le recensement des prestataires semble être une pratique bien ancrée dans une grande majorité d'organismes (97 %). Cependant, l'exercice de collecte d'informations sur les prestataires[10] réalisé courant 2022 auprès d'une sélection d'organismes a notamment révélé un niveau de détail insuffisant pour identifier les prestataires et une appréhension limitée de leur criticité.

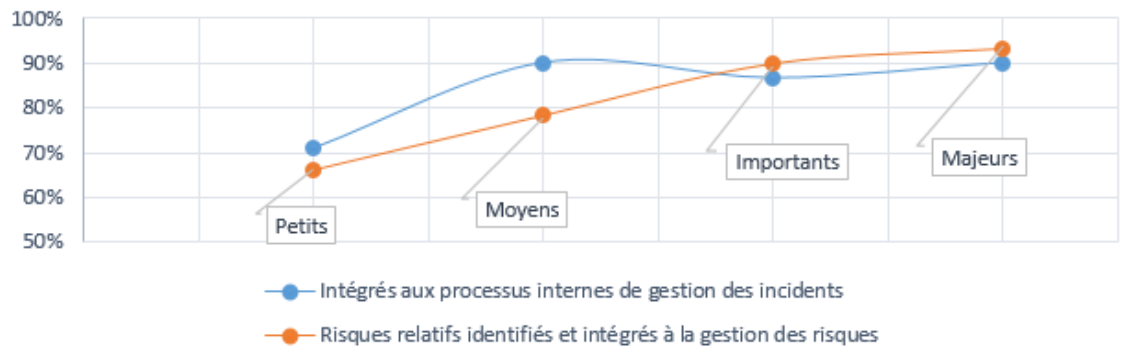
De façon préoccupante, 22 % des organismes (uniformément répartis parmi les 4 catégories de taille) indiquent ne pas réaliser de pilotage documenté des prestations critiques. De surcroit, 26 % des organismes (dont 15 % d'organismes de taille majeure et 23 % d'organismes de taille importante) ne définissent pas d'exigences ni d'indicateurs de sécurité avec leurs prestataires critiques. Enfin, 32 % des entités (dont 40 % d'importantes et majeures) n'effectuent pas d'analyse de réversibilité alors qu'il

[10] En prévision de l'obligation (issue du règlement européen sur la résilience numérique opérationnelle DORA – *Digital Operational Resilience Act*) de mettre en place et tenir à jour un registre des prestataires critiques

s'agit de l'étape préalable préparant la stratégie de sortie. En conclusion, alors qu'un suivi particulier des prestataires est nécessaire pour garantir le niveau de service et de sécurité adéquat, les organismes d'assurance semblent ne pas en avoir pris pleinement conscience et peinent à mettre les moyens pertinents en place.

Alors que la gestion de la continuité d'activité semble désormais prise en compte par la quasi-totalité des organismes (*cf*. section précédente), un tiers d'entre eux, toutes tailles confondues, déclarent toutefois ne pas intégrer les activités externalisées dans cette démarche. Or, il est nécessaire que chaque organisme tienne compte des dépendances vis-à-vis de ses fournisseurs critiques pour garantir la pleine efficacité de son dispositif de continuité et la pertinence des tests de résilience pratiqués.

Graphique 18 Services en nuage



Source ACPR

Une part prépondérante des organismes (93 %) indiquent utiliser des services en nuage (*cloud*). Pour autant, cette externalisation spécifique n'est pas totalement intégrée dans les processus internes : parmi les organismes ayant recours au nuage, 9 % n'incluent pas ces services dans les processus opérationnels internes de gestion des incidents, des changements et de la sécurité. Or l'utilisation de solutions *Cloud*, en particulier en mode « *IaaS*[11] » et « *PaaS*[12] », n'exonère pas les organismes de prendre en charge les aspects opérationnels tels que la gestion des versions et des mises à jour de sécurité. Par ailleurs, toujours dans la population de répondants utilisant le nuage, 12 % n'alimentent pas leur dispositif de gestion des risques des risques relatifs aux solutions en nuage.

[11] *IaaS : Infrastructure as a Service*
[12] *PaaS : Platform as a Service*

7. Une gestion du *Shadow IT* toujours lacunaire

Le *Shadow IT* recouvre les outils informatiques sous toutes leurs formes (appareils personnels, logiciels, applications, services web, programmes, …) qui sont développés, achetés ou utilisés par des utilisateurs appartenant à l'organisme d'assurance, sans que la direction des systèmes d'information en soit informée et donc sans supervision ni sécurisation de sa part.

La thématique *« Shadow IT »* a été abordée lors de la précédente enquête en 2019. Cette dernière a notamment révélé des lacunes dans la gestion des « EUC » (*End-User Computing* – programmes ou services non gérés par la DSI) qui représentent une des formes du *Shadow IT*. En 2022, le référencement des EUC n'a pas progressé par rapport à 2019 (22 % des organismes, de façon uniforme quelle que soit leur taille), ce qui, en dehors des aspects de supervision et de sécurisation mentionnés *supra*, est particulièrement dommageable en cas d'usage de « *Shadow SaaS*[13]», solution pouvant être contractualisée par un utilisateur sans qu'aucune analyse de risque ne soit effectuée par le RSSI. De la même façon, les risques relatifs aux applications non gérées par la DSI sont toujours aussi peu pris en compte (37 % des répondants seulement) dans la gestion des risques opérationnels.

[13] *Shadow Software as a Service*