N° 168 - 2025 Analyses et synthèses

Synthèse de l'enquête déclarative de 2024 sur la gestion de la sécurité des systèmes d'information des organismes d'assurance

SYNTHÈSE GÉNÉRALE

Avertissement au lecteur : contexte et limites

Le Secrétariat général de l'ACPR a lancé en 2024 une enquête par questionnaire portant à la fois sur la qualité des données et la sécurité du système 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 20 mai au 1er juillet, a permis de recueillir les réponses de 224 organismes.

Cette autoévaluation fait suite à celles de 2015, 2017, 2019 et 2022 qui portaient sur la qualité des données (QDD), le système d'information (SI) et sa sécurité (SSI). L'occurrence 2024 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. Dans la suite, sous le vocable « les organismes », sera désignée la population des organismes ayant répondu à l'enquête.

Synthèse

L'enquête SSI de 2024 illustre à nouveau la progression des organismes, en termes de prise de conscience de certains enjeux liés à la sécurité de l'information. Elle matérialise également des voies d'amélioration, voire des faiblesses persistantes, en particulier en ce qui concerne l'opérationnalisation des processus structurants de sécurité. Pour la première fois, le questionnaire a comporté un volet sur l'état de préparation à l'entrée en vigueur du cadre DORA[1], pour lequel les réponses ont pu paraître optimistes au regard des constats de terrain.

La progression se poursuit en particulier pour les aspects conceptuels de stratégie et de gouvernance liés à la sécurité des systèmes d'information (SSI), avec cependant une réserve persistante concernant le positionnement de la fonction SSI qui doit être indépendante et consultée lors des décisions clés.

Le dispositif de gestion des risques SSI connait également des progrès en termes de mise en place – définition du profil de risque, intégration à la cartographie des risques SSI, contrôle interne - mais les actions les plus structurantes comme la définition de la tolérance aux risques ou la prise en charge de la criticité révèlent encore certaines faiblesses et le besoin de progresser en maturité sur le sujet.

La sensibilisation au cyber risque apparait largement ancrée dans les processus internes. Il reste toutefois une proportion substantielle (24%) d'organismes de taille plus ou moins modeste qui n'a pas encore déployé d'actions de sensibilisation à destination du personnel ou des instances de gouvernance, d'une part ou des assurés d'autre part.

La gestion opérationnelle de la sécurité poursuit une relative progression, qui se manifeste au travers de la gestion des mises à jour des actifs informatiques, ou l'identification des vulnérabilités et via certains dispositifs d'identification et d'analyse proactive des cyber-menaces (« *threat intelligence* »). Des points de vigilance demeurent concernant la mise à jour au fil de l'eau des actifs SI, intégrant leur niveau de version – information essentielle en termes de sécurité –, l'extension du périmètre d'analyse à l'intégralité du SI, ou la réalisation des scans de vulnérabilités.

La démarche de continuité d'activité demeure globalement adoptée par les organismes d'assurance mais des points de maitrise restent clairement à approfondir pour rendre pertinents les dispositifs adoptés à cette fin : restauration des sauvegardes, preuve de réalisation et plus encore, réalisation d'une étude d'impact métier (BIA) et tests en conditions réelles.

Dans un contexte de généralisation du recours à l'externalisation, avec notamment l'utilisation massive de services en nuage (*cloud*) à l'origine de nouveaux risques, le déploiement de l'intégralité des processus de suivi et de maitrise conserve toute sa pertinence. En l'espèce, le bilan reste contrasté avec des progrès qui se poursuivent en matière de contractualisation ou de recensement des prestataires, mais la persistance de points d'attention pour

[1] Le règlement européen (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier sur la résilience opérationnelle numérique du secteur financier (*Digital Operational Resilience Act* ou DORA) établit des règles en matière de cybersécurité et de gestion des risques informatiques pour un grand nombre d'entités financières. Il entrera en application le 17 janvier 2025.

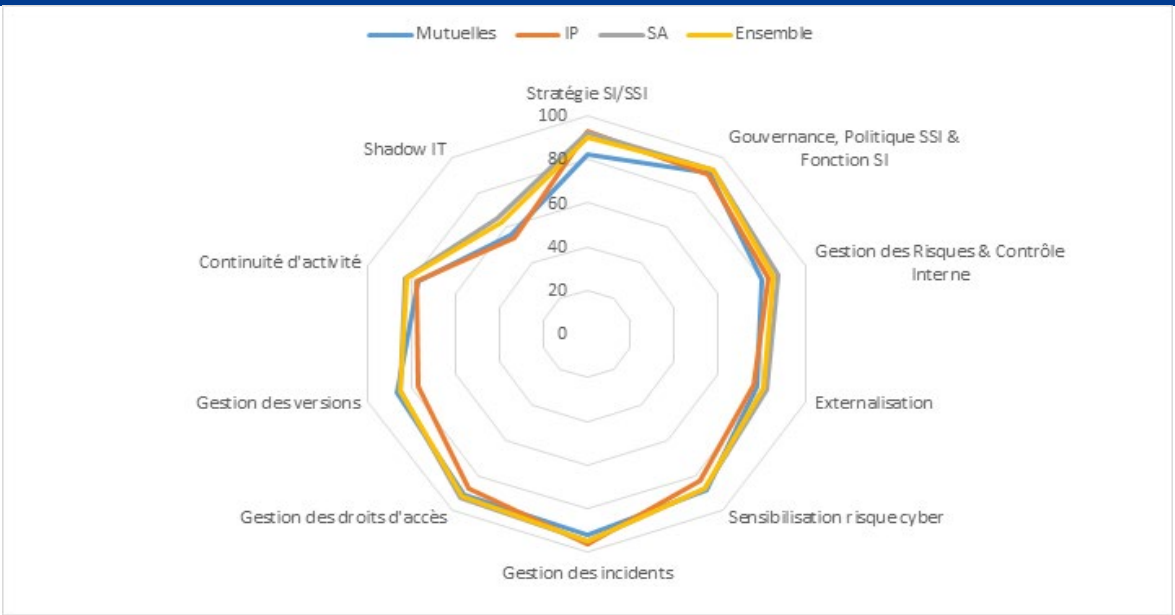
des sujets plus structurants, comme la maitrise de la substituabilité/réversibilité ou la définition de dispositifs de sécurité spécifiques au *cloud*.

La maitrise du *shadow IT*, c'est-à-dire l'utilisation de systèmes, d'appareils, de logiciels, d'applications et de services informatiques qui n'ont pas reçu l'approbation explicite de la fonction SSI, dont l'incidence augmente avec l'usage du *cloud*, reste un sujet sur lequel la maturité des organismes, notamment les plus petits, doit encore progresser, même s'il faut reconnaitre une prise de conscience depuis la dernière enquête.

Enfin, la préparation à l'entrée en vigueur du cadre réglementaire DORA a été évoquée, pour la première fois, dans cette enquête avec des réponses qui ont pu paraitre volontaristes, voire optimistes au regard des premiers constats de terrain. Cela étant, ce nouveau cadre de résilience numérique suppose une implication renforcée de la gouvernance et de la comitologie, une structuration fine du cadre de gestion des risques, un net renforcement de la gestion du risque de tiers (lié aux prestataires), l'organisation de la qualification et de la déclaration des incidents, et l'instauration de tests de résilience. Le déploiement de ces changements majeurs sera suivi attentivement ; par les services de contrôle et occasionnera une refonte du contenu des prochaines enquêtes à venir.

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

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



Source ACPR

Étude réalisée par le Pôle Qualité des données et Systèmes d'Information de la Direction des Contrôles Spécialisés et Transversaux de l'ACPR[2].

SOMMAIRE

[2] Ont contribué à cette étude Julia Faure, Florence Ruffin, Jérôme Jusot, Paul Monchauzou, Fabrice Offret, Victor Peglion et Edwin Scheer.

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

TYPOLOGIE DES REPONDANTS

Les résultats de cette enquête sont établis sur la base des réponses de 224 organismes (contre 239 en 2022). La couverture de marché des organismes ayant répondu à cette nouvelle enquête représente 84 % du chiffre d'affaires réalisé par les organismes d'assurance et de réassurance agréés en France. Dans la suite, sous le vocable « les organismes », sera désignée la population des organismes ayant répondu à l'enquête.

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 également été définie selon le chiffre d'affaires des organismes (primes ou cotisations) en 2023 :

- Premier quartile, primes entre 0 et 82 MEUR : « Petits organismes » ;
- Second quartile, primes entre 82 MEUR et 427 MEUR : « Organismes moyens » ;
- Troisième quartile, primes entre 427 MEUR et 1 250 MEUR : « Organismes importants » ;
- Dernier quartile, primes supérieures à 1 251 MEUR : « Organismes majeurs ».

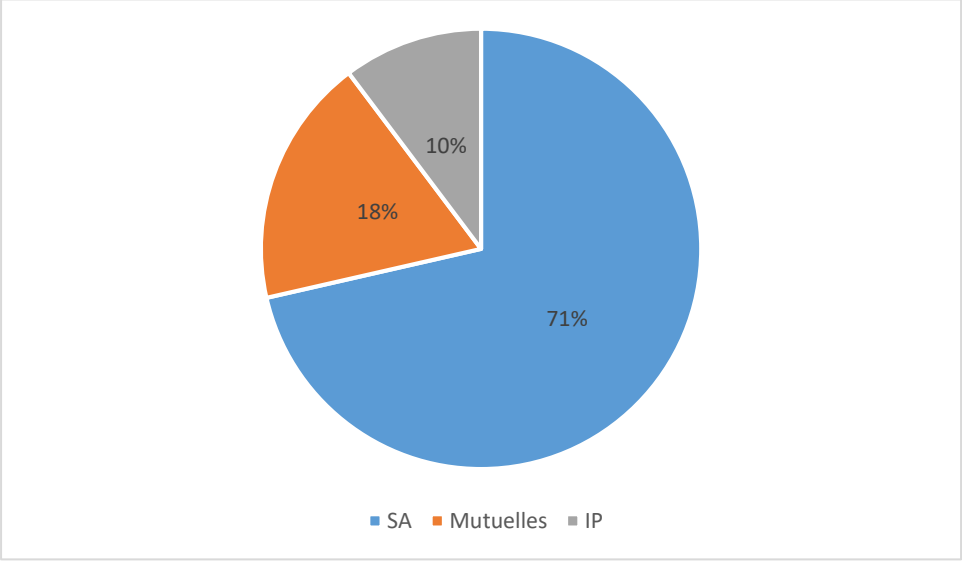
Les résultats sont parfois également présentés dans cette étude en fonction de la forme juridique des organismes, selon qu'ils relèvent du code des assurances[3], du code de la mutualité[4] ou du code de la sécurité sociale[5]. Par convention, dans la suite du document, les 3 groupes ainsi constitués 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 66 % d'organismes de taille modeste tandis que le groupe des sociétés de (ré)assurance est constitué à 57 % d'organismes « importants » et « majeurs ». En particulier, l'évolution de la composition des groupes entre les enquêtes 2022 et 2024 peut interférer dans l'interprétation de l'évolution des résultats.

[3] 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

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

[5] 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 organismes répondants selon leur forme juridique

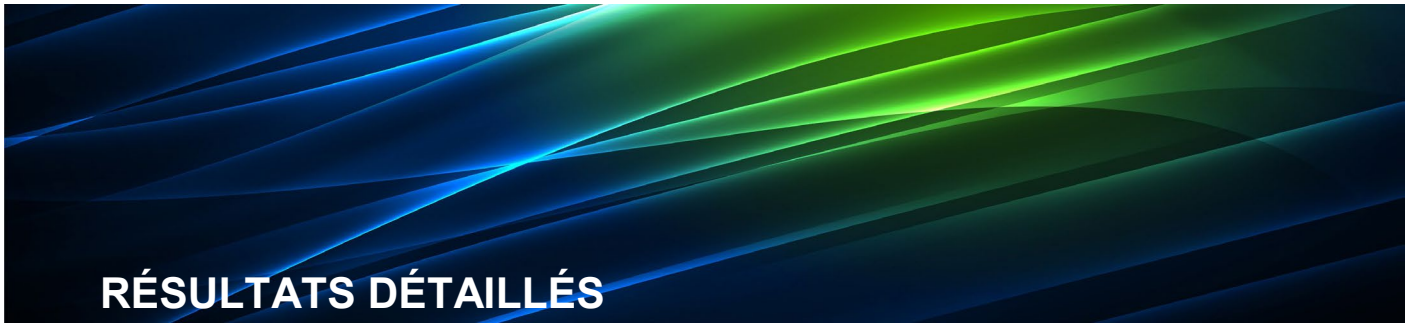


Source ACPR

Le tableau ci-dessous synthétise la distribution des répondants selon ces classes et selon le code dont ils relèvent :

		Taille d'organisme (total de primes)				Total répondants	Part (en %)	Marché 12/2023	Taux de participation
		Petits	Moyens	Importants	Majeurs				
Type d'organisme	Sociétés d'assurance et de réassurance, FRPS, succursales de pays tiers (SA)	35	34	42	49	160	71%	302	53%
	Mutuelles yc totalement substituées & MRPS (Mutuelles)	14	13	10	4	41	18%	324	13%
	Institutions de prévoyance et IRPS (IP)	7	9	4	3	23	10%	34	68%
Total répondants		56	56	56	56	224	100%	660	34%

N.B. : Les 50 plus gros organismes et/ou groupes d'assurance ont très majoritairement répondu.



1. Une normalisation de la gouvernance SSI à compléter pour la fonction SSI

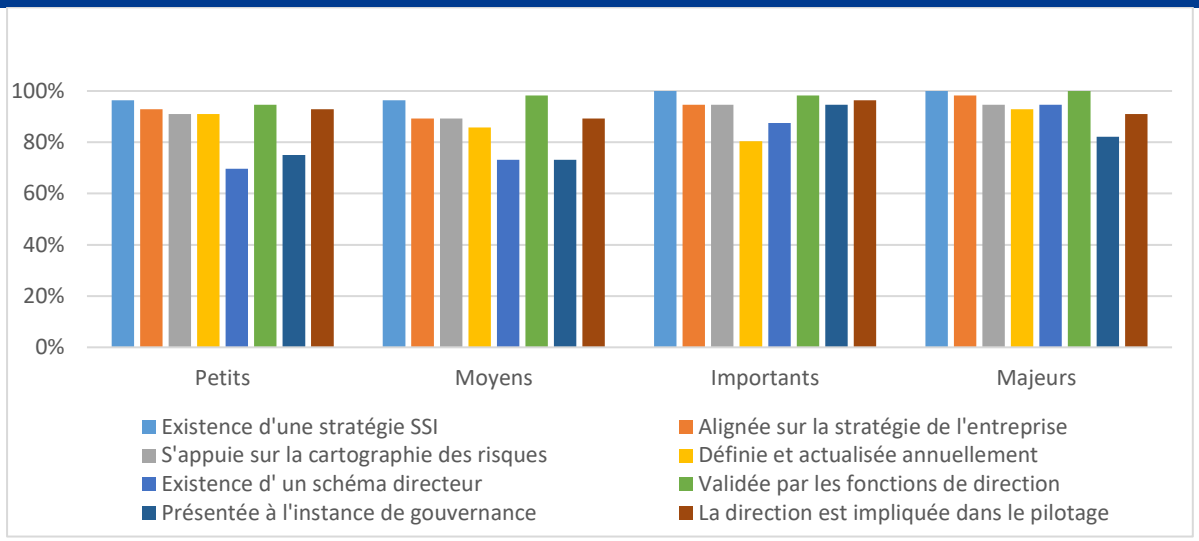
1.1 Stratégie SSI

La quasi-totalité des répondants déclare disposer d'une stratégie en matière de sécurité informatique (98%) ; il ne reste qu'une petite fraction d'organismes petits ou moyens (essentiellement mutualistes) à ne pas en disposer. Cette stratégie est très majoritairement validée par les instances de direction (98%), mais la généralisation de sa présentation aux instances de gouvernance n'est pas tout à fait acquise (81% dont 74% pour les petits et moyens).

La cohérence entre la stratégie SSI et l'exposition aux risques est très majoritairement assurée, puisque 92% des répondants s'appuient sur la cartographie des risques de sécurité SI pour établir leur stratégie SSI. Les résultats semblent stables comparés à l'enquête précédente (91% en 2022).

Enfin, la traduction opérationnelle de la stratégie SSI en schéma directeur incluant organisation, architecture, mise en œuvre et communication, puis surveillance (voir orientation 3 de la notice TIC) ,reste un enjeu pour les répondants puisque cette pratique se limite encore à 81% d'entre eux, cette proportion tombant à 70 % en moyenne pour les assureurs petits ou moyens.

Graphique 3 Caractéristiques de la stratégie SSI



Source ACPR

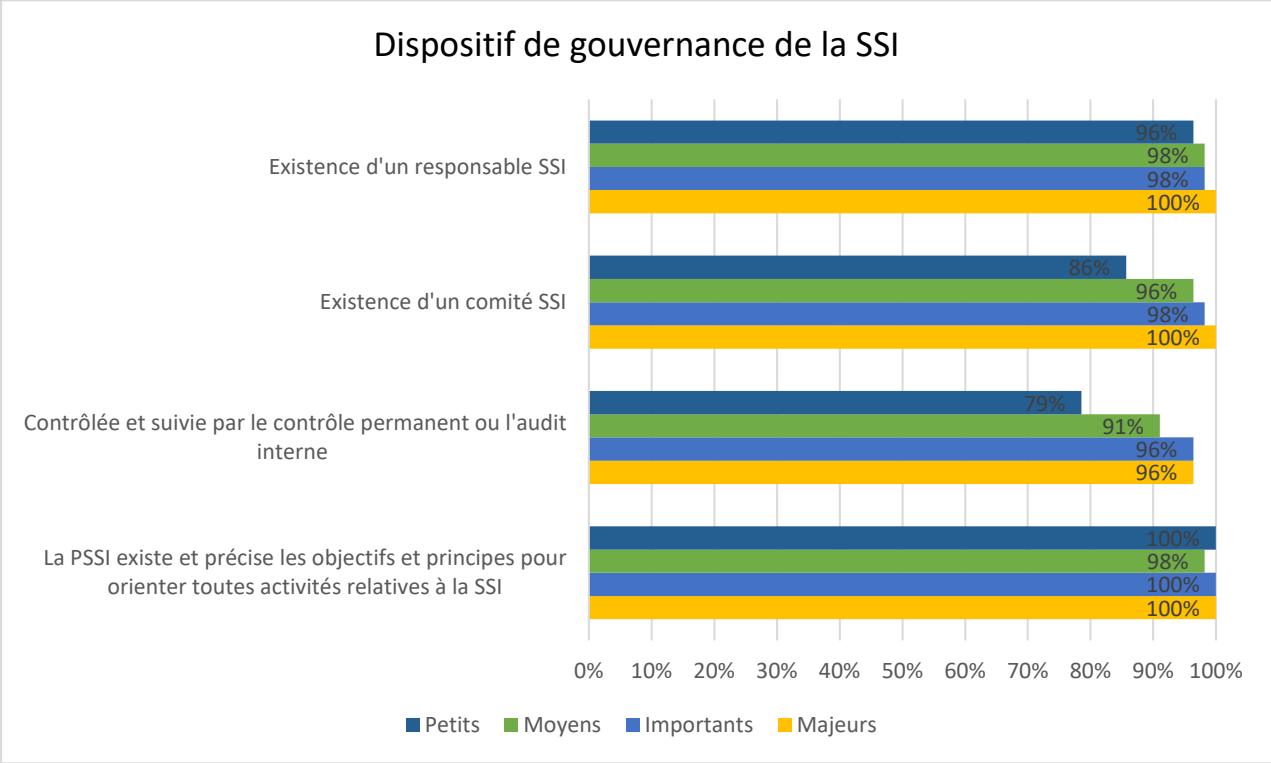
1.2 Dispositif de gouvernance SSI

Tous les répondants, sans exception, déclarent disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) encadrant la gouvernance et les activités de la sécurité des systèmes d'information (95% en 2022).

Toutefois, les instances de direction ne sont impliquées dans le processus de révision de cette politique que pour 87% des déclarants.

Par ailleurs, le contrôle de sa correcte application par le système de contrôle interne apparaît encore limité dans les organismes de taille modeste (79% contre 95% pour les organismes de tailles supérieures).

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



Source ACPR

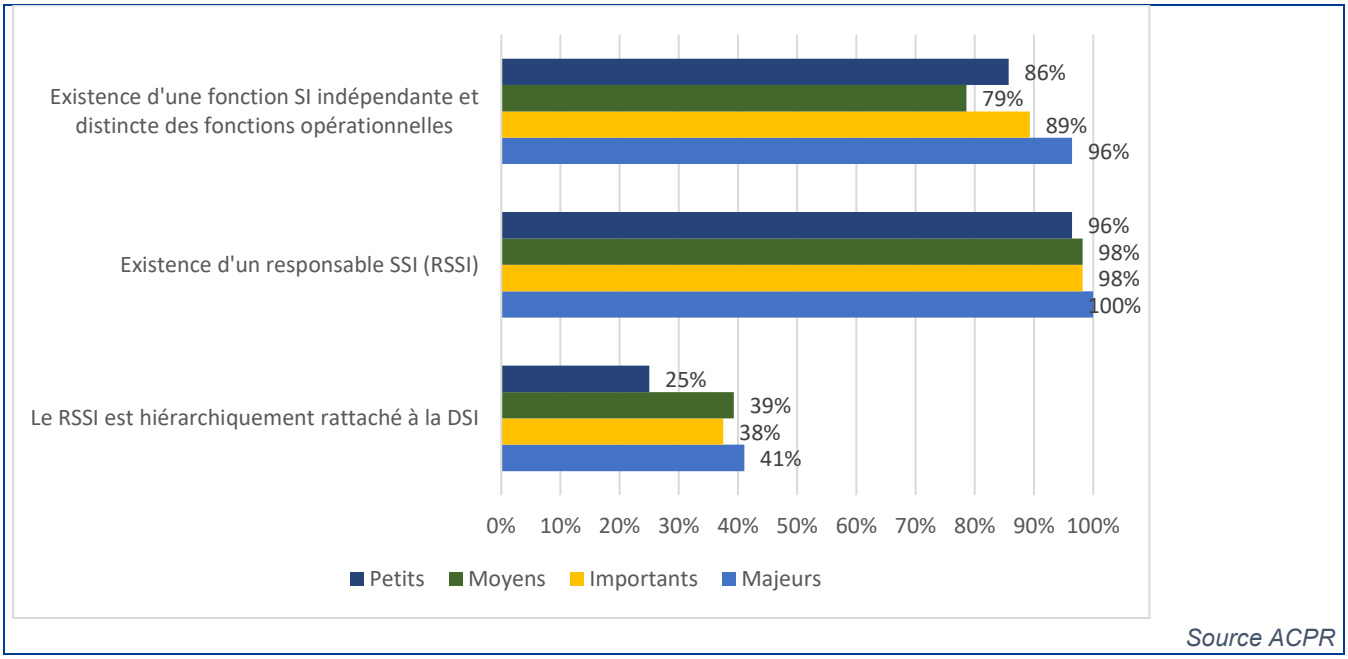
Pour animer le dispositif de sécurité des SI, 98 % des organismes répondants se sont dotés d'une fonction de responsable de la sécurité des systèmes d'information (RSSI). La fonction SSI, au sens de l'orientation 7 de la notice de l'ACPR sur la sécurité et à la gouvernance des technologies de l'information et de la communication (TIC)[6], bénéficie dans 93 % des sociétés les plus importantes d'un positionnement indépendant des fonctions opérationnelles (ce taux n'étant que de 82 % dans les organismes de petite taille ou intermédiaire).

Cette indépendance reste à renforcer : en effet dans 36% des cas, la fonction SSI est encore rattachée hiérarchiquement à la Direction des Systèmes d'Information.

Enfin, pour coordonner et piloter le dispositif SSI, 95 % des répondants ont mis en place un comité dédié à la SSI (87% en 2022).

Graphique 5 La fonction de Responsable de la SSI

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

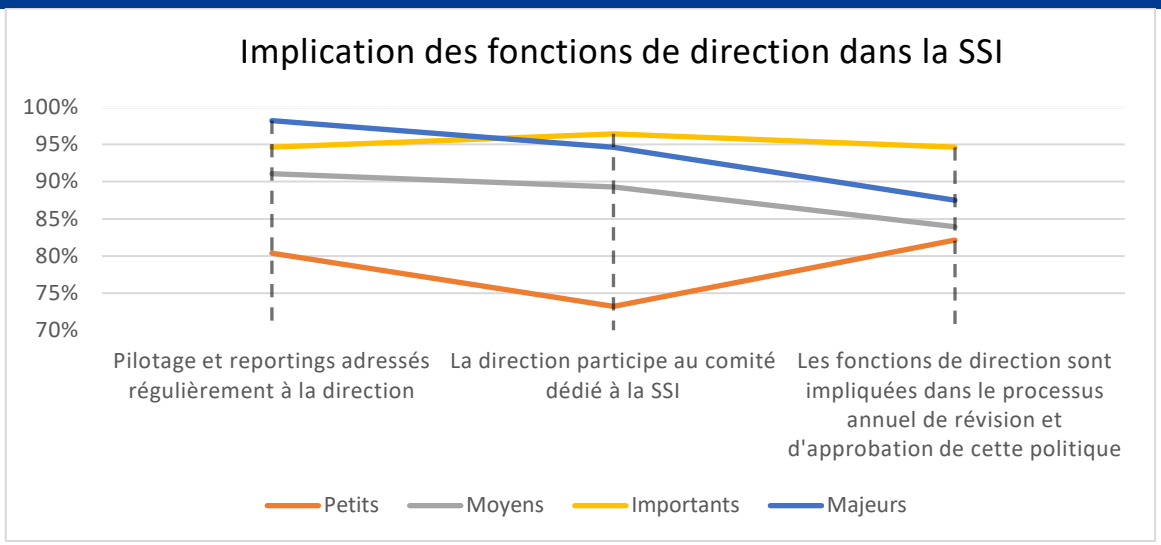


Source ACPR

Concernant l'implication des fonctions de direction dans le suivi et le pilotage des questions liées à la SSI, les organismes les plus modestes peinent encore à les impliquer. En effet, seuls 80% d'entre eux produisent un reporting interne à destination de la direction de l'organisme, pour ces mêmes organismes, seuls 73% déclarent que la direction participe au comité SSI.

Dans l'ensemble, les organismes plus importants semblent avoir davantage pris conscience de la nécessité d'impliquer les fonctions dirigeantes dans les instances et dans les thématiques liées à la SSI (voir en ce sens Orientation 3 de la notice TIC).

Graphique 6 Implication des fonctions de direction dans la sécurité des SI



Source ACPR

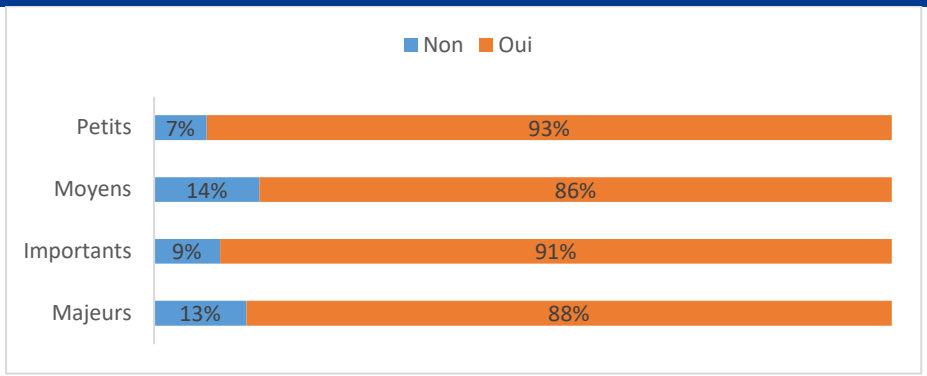
1.3 Moyens alloués à la sécurité des systèmes d'information

En matière de budget de sécurité des SI, la situation demeure stable depuis 2019 : le budget moyen s'établit à près de 7 % du budget informatique total et la valeur médiane se situe également à 7%. Au regard des moyens financiers

disponibles dans chaque organisme ou groupe d'organismes, l'effort budgétaire réalisé par les organismes de petite et moyenne taille est proportionnellement supérieur à celui des structures importantes et majeures.

De plus en plus d'organismes sanctuarisent le budget dédié aux dépenses engagées au titre de la SSI. Ainsi, 89 % en 2024 contre 84% en 2022 allouent un budget propre à la SSI. Cependant, il apparait préoccupant que 12% des organismes moyens, importants et majeurs n'allouent pas encore en 2024 un budget spécifique. Le choix d'une gestion pilotée du budget SSI est en effet une pratique à privilégier pour une vision plus fine des coûts.

Graphique 7 Organismes allouant un budget spécifique à la sécurité des SI

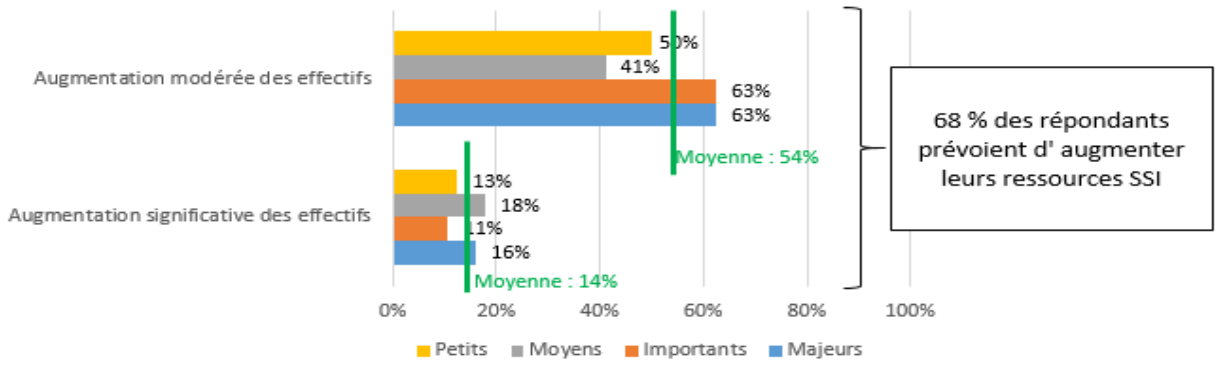


Source ACPR

Concernant les ressources humaines allouées à la sécurité des SI, la proportion de répondants prévoyant d'augmenter leurs effectifs spécialisés en sécurité est de 68 % en 2024 contre 59 % en 2022, ce qui peut notamment s'expliquer par les évolutions réglementaires (DORA) :

- ✓ Dans cette population, 14 % des organismes répondants visent une augmentation significative ;
- ✓ On note que les organismes les plus importants semblent déjà avoir fait l'effort de recrutement sur les années précédentes et qu'ils abordent le futur en augmentant modérément leurs effectifs SSI ;
- ✓ Enfin, aucun organisme ne prévoit de baisser ses effectifs SSI à l'horizon d'un an.

Graphique 8 Prévision d'augmentation des ressources SSI à horizon d'un an



Source ACPR

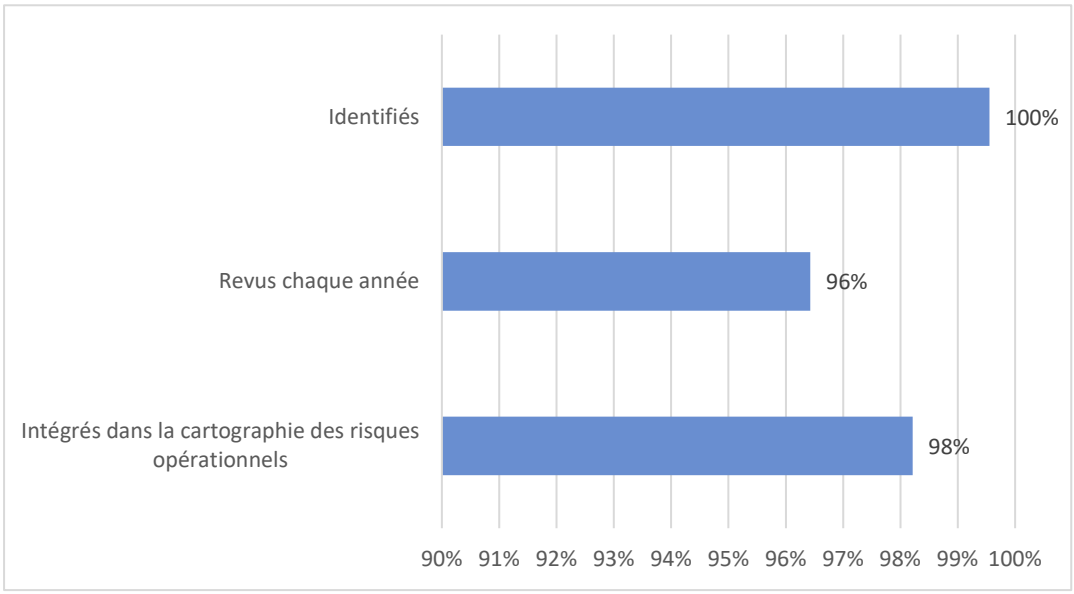
2. Des progrès – à étendre – pour le dispositif de gestion des risques et de contrôle interne en matière de SSI

2.1 Profil de risque en matière de sécurité des SI

Les organismes répondants, en intégralité désormais, déclarent identifier les risques relatifs à la sécurité des SI (ceux-ci sont nommés de façon générique « risques SSI » dans la suite). Ces risques sont intégrés à la cartographie des risques opérationnels pour 98% des organismes et ils réalisent une revue annuellement (96%).

Ces constats, basés sur les déclarations, paraissent sensiblement plus optimistes que certaines réalités rencontrées en contrôle sur place ou à l'occasion de la déclaration d'incidents cyber.

Graphique 9 Caractéristiques de la gestion des risques SSI



Source ACPR

Pour 67 % des répondants, l'identification et la qualification du risque SSI ne s'accompagne pas de la définition d'un niveau de tolérance en matière de risque SSI, pourtant de nature à garantir que leur dispositif de maitrise du risque est en adéquation avec le niveau de risque maximum admis (voir en ce sens orientation 4 de la notice TIC).

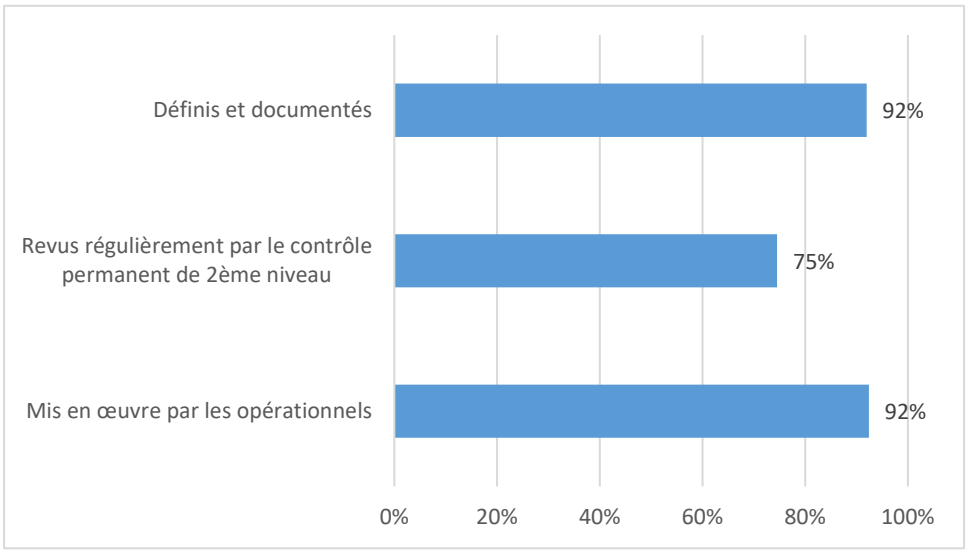
Ce constat, qui souligne la nécessité d'une évolution en termes de maturité sur la qualification du risque SSI, est autant pertinent pour les organismes de petite et moyenne taille (63 %) que pour les organismes importants et majeurs (71 %).

Par ailleurs, 87% des organismes déclarent réaliser une analyse de risques SSI pour chaque nouveau projet SI. Ce résultat est en légère augmentation par rapport à 2022 (81%).

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

La définition et la documentation des contrôles associés à la SSI sont acquises pour 92% des déclarants. Leur mise en œuvre par les opérationnels parait largement répandue (92%) et leur revue régulière par le contrôle de 2ème niveau assez largement opérée (75%).

Graphique 10 Caractéristiques des contrôles SSI



Source ACPR

De manière plus globale, pour 95% des répondants, le profil de risque étudié dans le cadre de l'ORSA[7] est réputé tenir explicitement compte de la thématique SSI dans la catégorie « risques opérationnels » et 75%[8] des entreprises déclarent tester 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.

Cela étant, les rapports ORSA examinés au cours des récentes missions de contrôle sur place laissent apparaitre que les informations relatives aux risques SSI ne sont pas encore systématiquement évoquées dans ces rapports ou qu'elles peuvent se révéler trop succinctes.

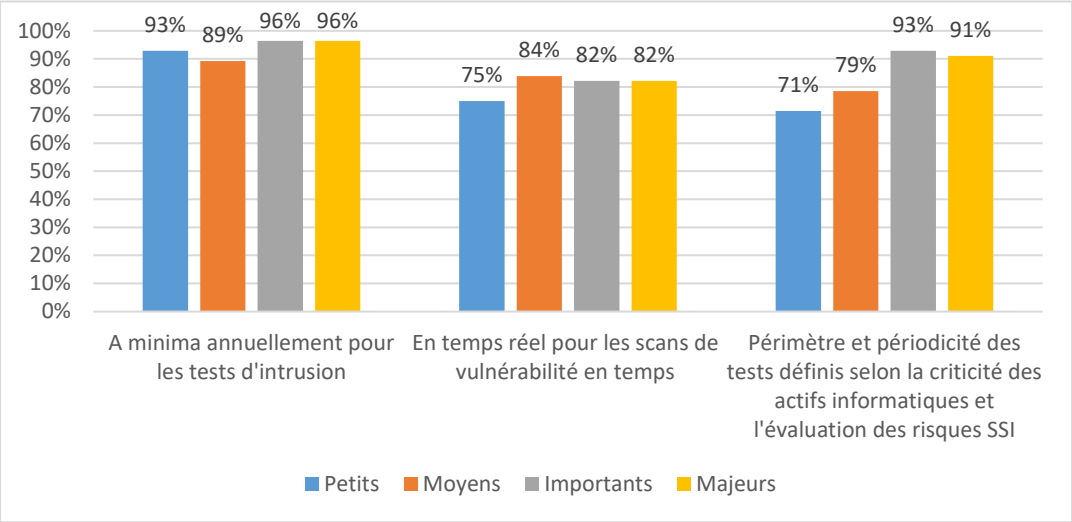
S'agissant des tests de sécurité, leur réalisation en temps réel pour les scans de vulnérabilité se développe avec un effort un peu plus marqué pour les organismes importants ou majeurs (82%) que pour les organismes plus modestes (75%).

Par ailleurs, le périmètre et la périodicité des tests de sécurité doivent être définis selon la criticité des actifs informatiques et selon l'évaluation des risques SSI. Si les organismes importants ou majeurs ont largement intégré cette dimension (91% et 93%), une marge d'amélioration persiste pour les organismes de taille plus modeste (71%).

Graphique 11 Réalisation de tests de sécurité

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

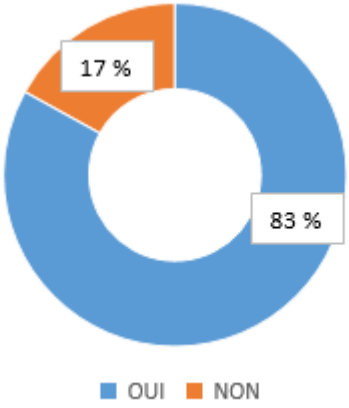
[8] ce taux variant (respectivement) de 95% des acteurs majeurs à 61% des acteurs les plus modestes.



Source ACPR

Enfin, la proportion des organismes qui procèdent à une mission d'audit sur la sécurité SI au moins tous les deux ans progresse de 72% en 2022 à 83% désormais.

Graphique 12 Réalisation d'une mission d'audit sur la sécurité SI au moins tous les 2 ans



Source ACPR

3. Les mesures concourant à la maîtrise du risque SSI en progression

3.1 Prise en compte de la sécurité dans les projets informatiques

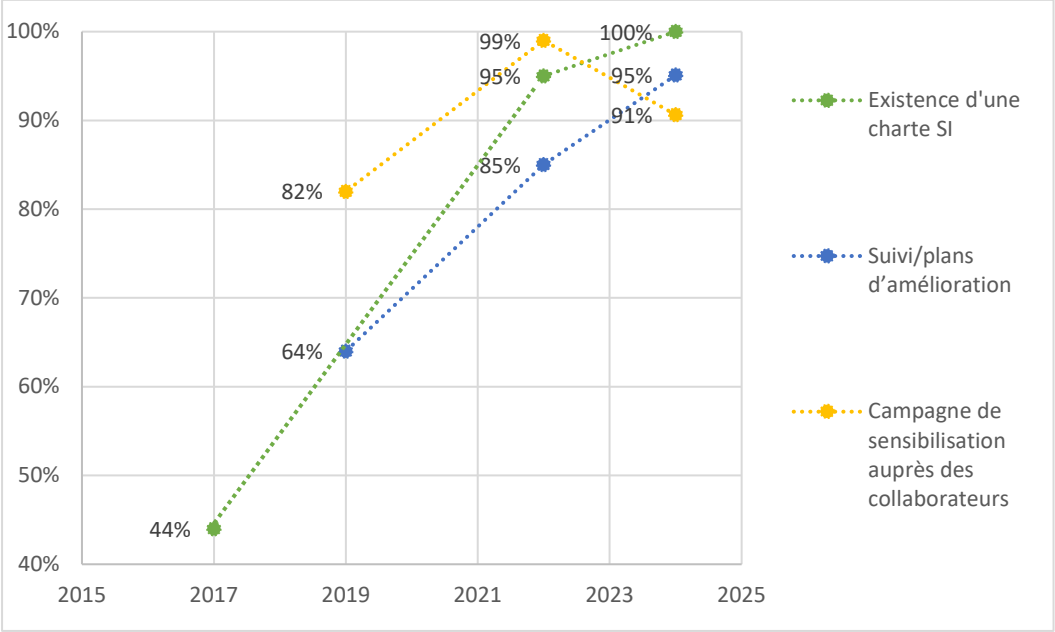
L'inclusion des analyses de risques de non sécurité dans la gestion de projets informatiques continue de s'améliorer : la population qui n'intègre pas encore cette dimension dans la réalisation de ces projets se réduit progressivement (13%, versus 19 % en 2022 et 26 % en 2019).
Cette fraction reste cependant élevée pour les petits et moyens organismes (17%), probablement en raison d'une relative faiblesse de l'acculturation à la sécurité informatique (voir en ce sens l'orientation 16 de la notice TIC).

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

La mise en œuvre de mesures de sensibilisation et de formation à la thématique du risque cyber demeure assez largement pratiquée depuis 2022 :

- La mise en place d'une charte d'utilisation du SI que chaque collaborateur s'engage à appliquer : cette pratique est maintenant institutionnalisée à 100% ;
- Un dispositif intégrant le risque cyber dès l'arrivée des collaborateurs (clause de responsabilité dans le contrat de travail et session de sensibilisation) : une légère baisse est à noter 91 % des répondants qui ont adopté ce dispositif (contre 93 % en 2022) ;
- Les campagnes de sensibilisation, notamment par test d'hameçonnage (*phishing*), se généralisent à l'ensemble du marché ;
- La fraction des collaborateurs de la (ou des) DSI ayant des formations spécifiques sur la SSI adaptées à leur activité reste plutôt stable. Cependant, nous notons de manière étonnante une légère baisse chez les organismes majeurs passant de 88% en 2022 à 82% en 2024.

Graphique 13 Évolution des actions de sensibilisation relative à la sécurité des SI



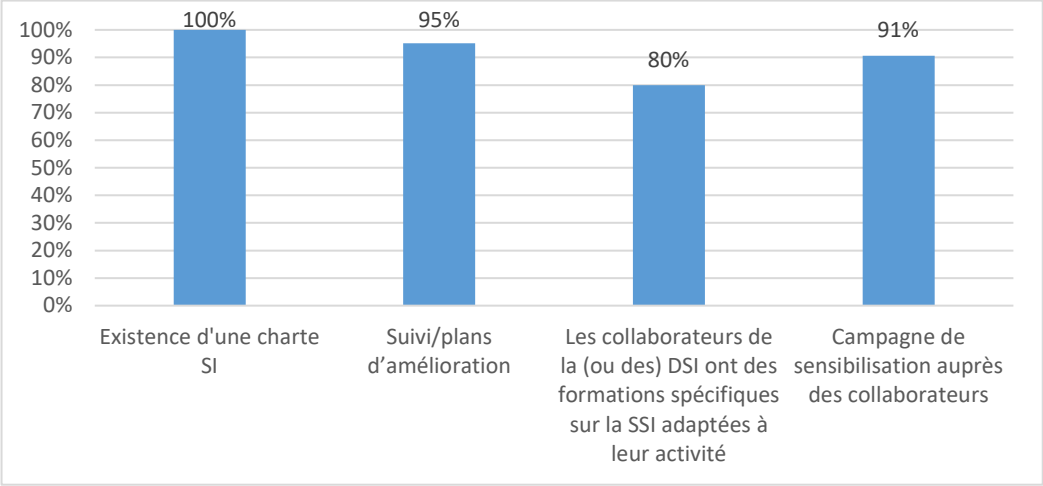
Source ACPR

Les campagnes de sensibilisation sont peu à peu étendues aux membres des instances de gouvernance[9], surtout dans les organismes de taille importante ou majeure. Et dans une moindre mesure aux collaborateurs prestataires de service. Les actions de sensibilisation auprès des assurés restent encore un axe à développer.

[9] Les fonctions de direction constituent l'une des principales populations ciblées par les cybercriminels.

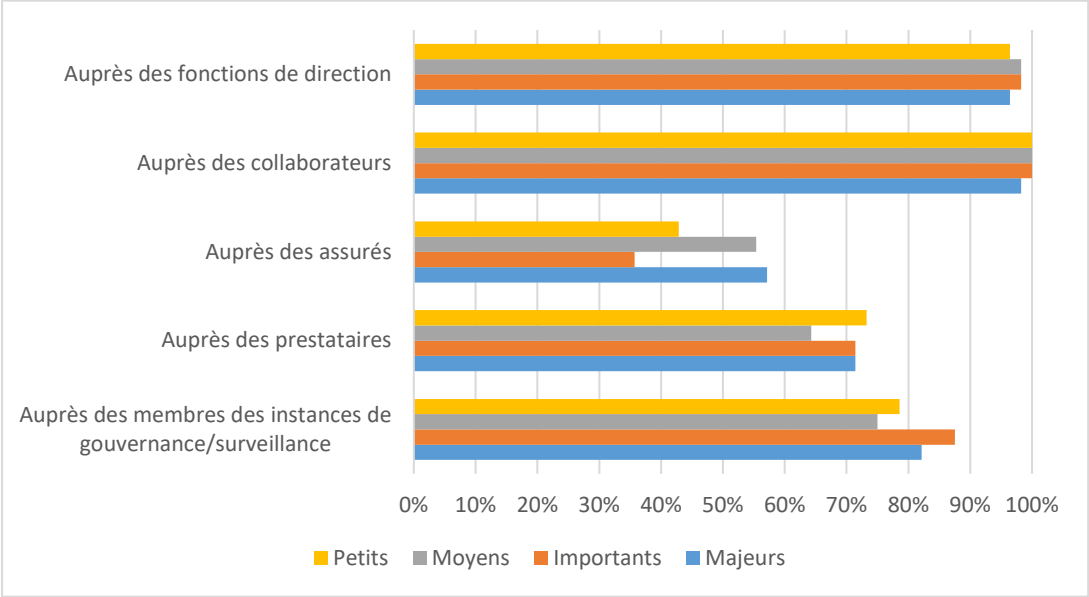
De plus, la mesure de l'efficacité des campagnes de sensibilisation est désormais intégrée, ce qui est un préalable nécessaire à l'établissement de plans d'amélioration. Les organismes de petite et moyenne taille quant à eux continuent leur progression (75% en 2022 à 84% en 2024 ; 92% en 2022 à 98% en 2024).

Graphique 14 Actions de sensibilisation relative à la sécurité des SSI



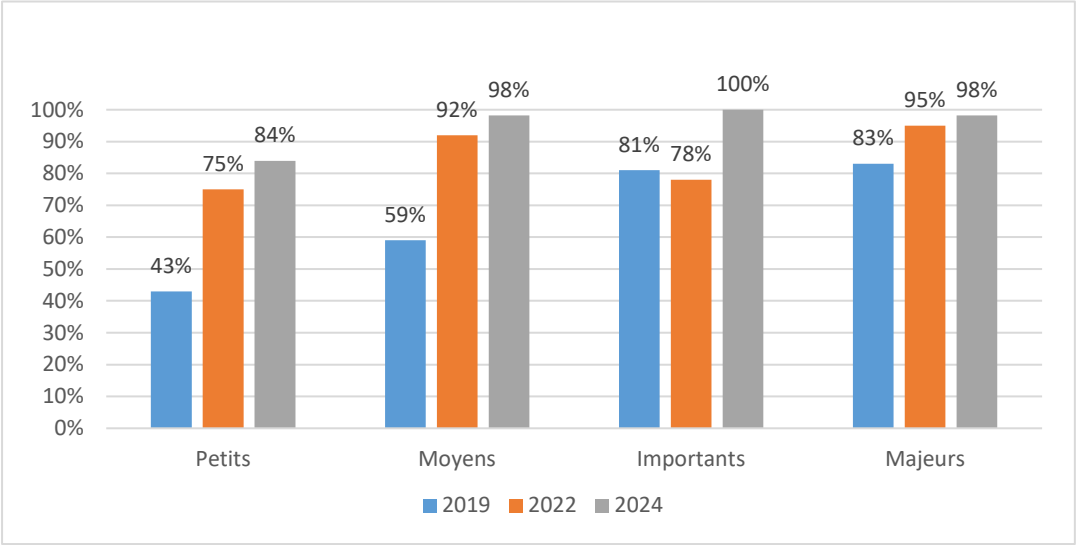
Source ACPR

Graphique 15 Campagnes de sensibilisation aux risques de sécurité des SI



Source ACPR

Graphique 16 Suivi et plan d'amélioration des campagnes

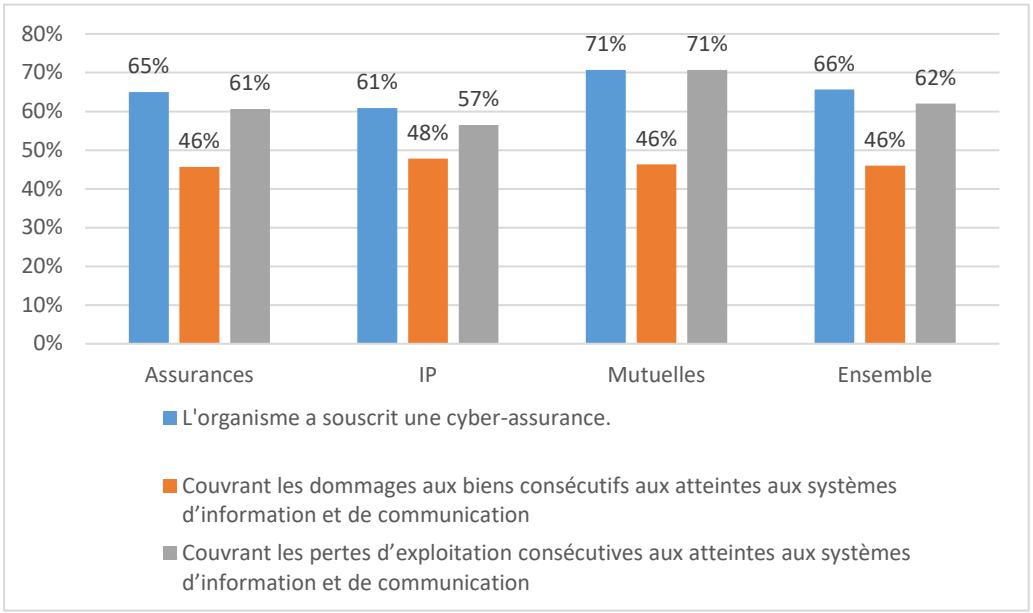


Source ACPR

3.3 Couverture d'assurance

Comme en 2022, de nombreux organismes déclarent avoir souscrit une assurance cyber mais cette assez large majorité est en érosion notable (66% en 2024 contre 85% en 2022).

Graphique 17 Cyber-assurance en France en 2024



Source ACPR

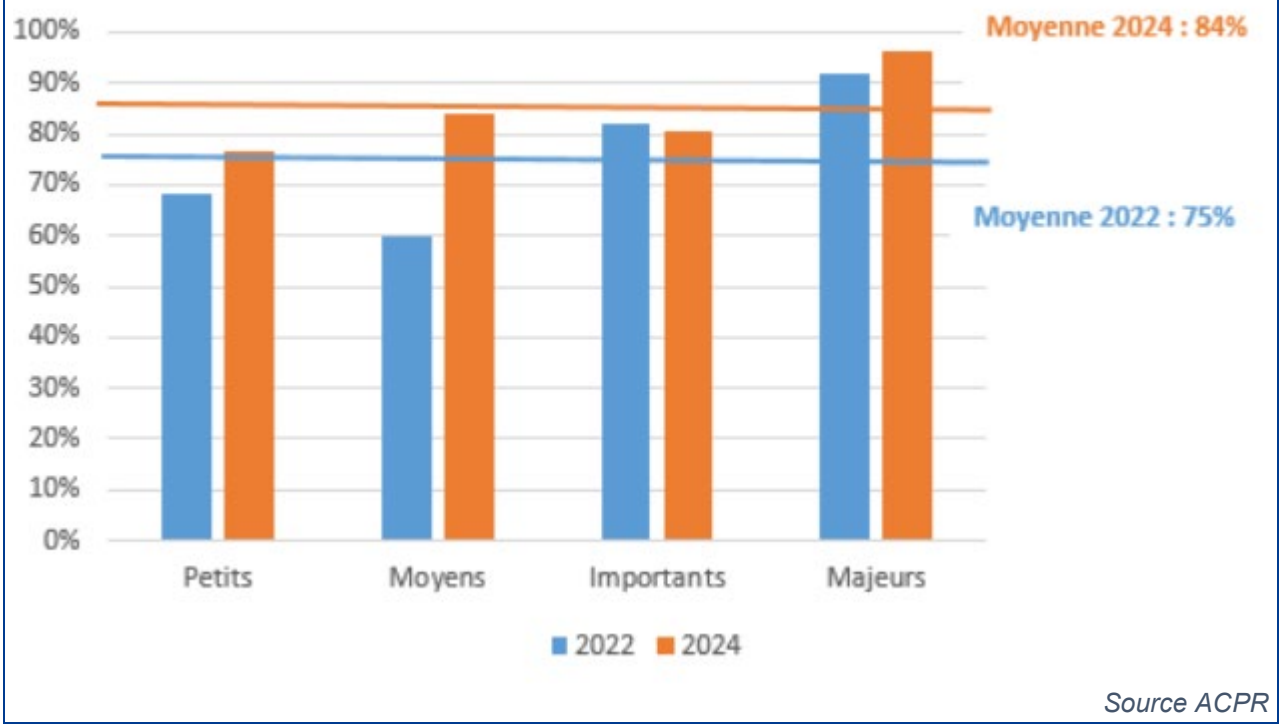
4. Des mesures opérationnelles de gestion du risque SSI à approfondir

4.1 Inventaire des actifs et gestion des vulnérabilités

Concernant la maitrise des inventaires, les résultats de cette enquête 2024 sont assez contrastés. En effet, les résultats sont globalement meilleurs avec une mise à jour régulière de l'inventaire des actifs pour 99 % des répondants (contre 89 % en 2022) mais pour autant, la mise à jour au fil de l'eau intégrant le niveau de version des actifs SI chute de 76 % à 69 % sur la même période, ce qui signifie une faiblesse dans la précision de ces inventaires.

Les résultats reflétant la maitrise des processus de remédiation de vulnérabilité et d'acquisition de dispositifs d'analyse proactive de la menace (*threat intelligence*) sont eux en évolution croissante sur l'ensemble des segments (94% de gestion des vulnérabilités, et 84% pour la *threat intelligence* contre 75 % en 2022).

Graphique 18 Évolution de la *threat intelligence*



Source ACPR

Ces résultats globalement positifs restent à relativiser car de nombreux organismes ne procèdent pas à la détection de leurs vulnérabilités sur l'intégralité des périmètres SI (détection souvent limitée aux parties exposées sur Internet, sans couvrir l'intégralité du SI, et excluant fréquemment la partie historique dite « *legacy* »).

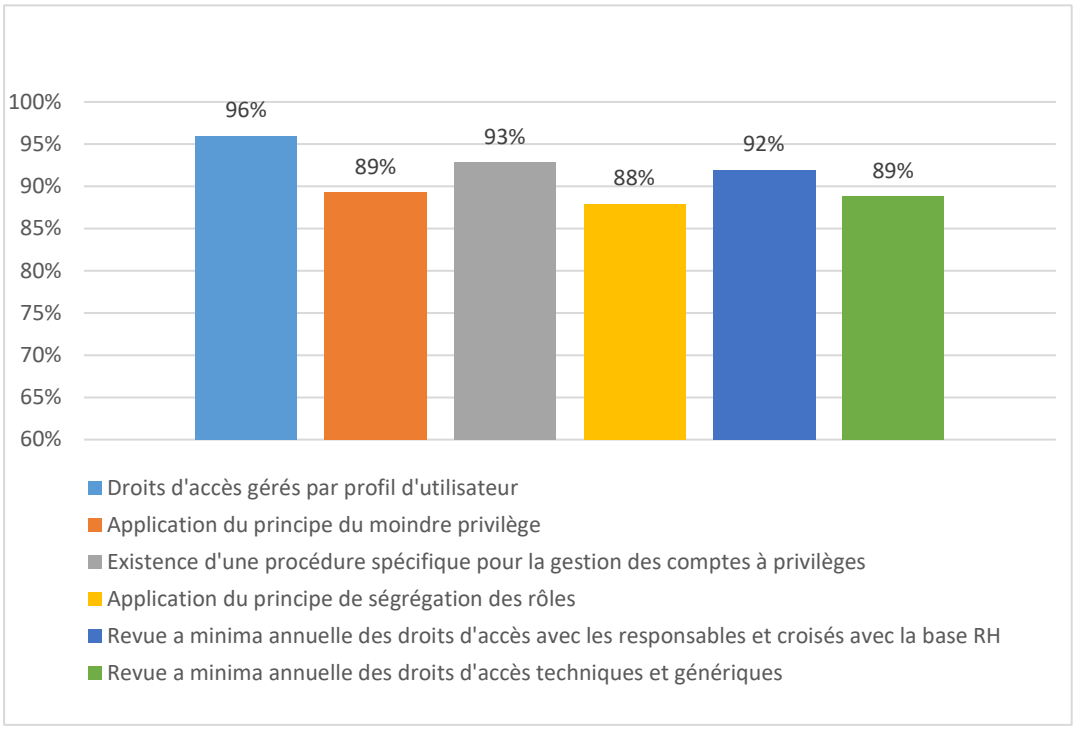
Par ailleurs, l'analyse de la menace est souvent confiée à des prestataires externes, dotés d'outils automatisés qui ne tiennent pas réellement compte des caractéristiques techniques spécifiques à chaque système d'information, faute de connaissance approfondie de l'organisme considéré.

La connaissance et la maitrise de l'exposition des organismes au risque cyber demeurent des sujets de progrès pour les organismes et d'attention pour le superviseur.

4.2 Gestion des droits d'accès

La progression du taux de réalisation de revue annuelle des droits (habilitations) se poursuit : 92 % des répondants déclarent effectuer cette opération aujourd'hui (87 % en 2022, et 72 % en 2019).

Graphique 19 Gestion des droits d'accès



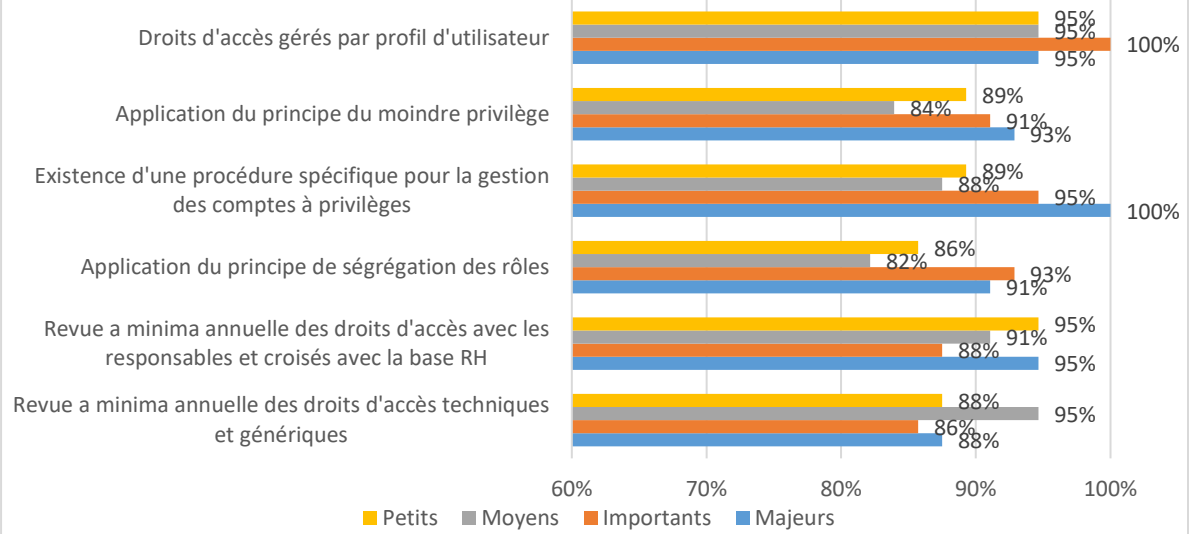
Source ACPR

Les revues annuelles de droits d'accès techniques et génériques sont généralisées pour 89 % des répondants (versus 84 % en 2022) et l'application du principe de moindre privilège est elle aussi très suivie.

Les statistiques des organismes les plus modestes ont fortement augmenté concernant les revues annuelles par les responsables métier, en passant à 95 % de réponse favorable sur cette exercice.

Cela étant, en dépit des chiffres élevés relevés à travers cette enquête déclarative, il est encore fréquemment constaté lors des contrôles que certains périmètres de droits applicatifs ne sont pas intégrés au processus de revue et que la complexité du processus mis en œuvre peut parfois limiter son efficacité (périmètre, fréquence et réactivité).

Graphique 20 Gestion des droits d'accès

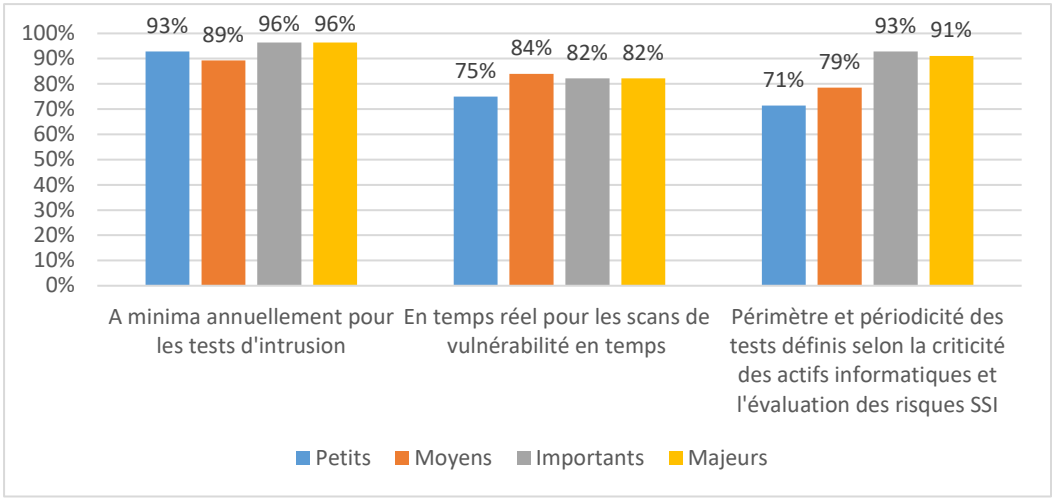


Source ACPR

4.3 Réalisation de tests de sécurité

94% des organismes indiquent réaliser des tests de sécurité (test d'intrusion, scans, etc.) sur une base au moins annuelle (-1 point ; en moyenne 91% pour les organismes petits et moyens) mais les scans de vulnérabilité en temps réel ne sont pas déployés pour 20% des déclarants. Il en va de même (pour 22 % des organismes) pour la définition du périmètre et de la périodicité des tests selon la criticité des actifs informatiques ou selon l'évaluation des risques SSI. Faute d'une définition adaptée, la pertinence et l'intérêt des tests s'en trouvent nettement amoindris pour l'appréciation du niveau de sécurité de l'organisme.

Graphique 21 Réalisation de tests de sécurité

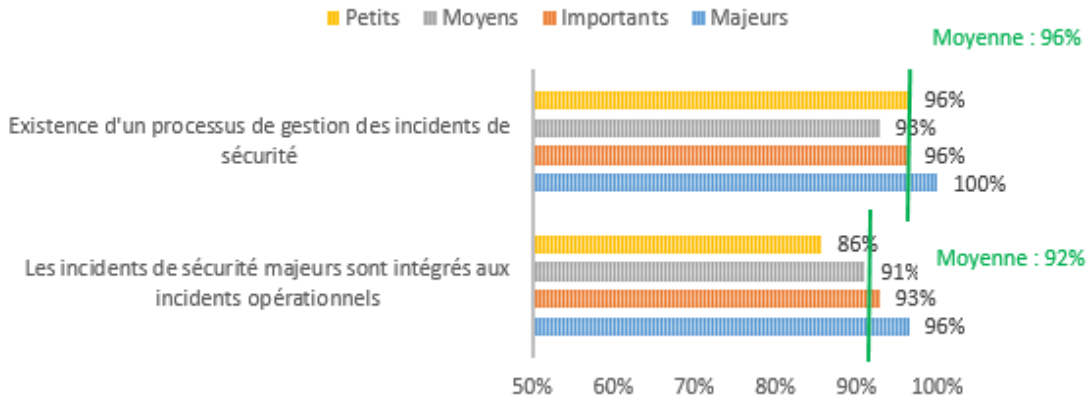


Source ACPR

4.4 Gestion des incidents de sécurité et opérationnels

L'existence d'un processus de gestion des incidents de sécurité apparait généralisée pour 96 % des répondants et, pour 92 % d'entre eux, ce processus prévoit l'intégration des incidents de sécurité majeurs dans le registre des incidents opérationnels. Cette thématique est intégrée pour la grande majorité des organismes, avec une nette progression pour les petits (86 % versus 76 % en 2022).

Graphique 22 Gestion des incident de sécurité des SI



Source ACPR

5. L'effectivité et l'opérationnalisation des plans de continuité d'activité à renforcer

L'existence de plans de continuité ayant paru acquise lors des précédentes enquêtes, les questions ont été approfondies, avec en résultats, la mise au jour de quelques faiblesses :

- Certes, la gestion de la sauvegarde stockée sur un ou plusieurs sites éloignés du site principal parait largement répandue (98 % à 100 %) ;
- Mais, s'agissant de la restauration des sauvegardes testée (85 %, sans prime particulière au bénéfice des organismes majeurs) ainsi que sur les preuves de réalisations (79 % dont 62 % pour les petits), les organismes apparaissent moins matures.
- Par ailleurs, il reste des efforts à accomplir en termes de conservation des preuves de réalisation des tests (seule manière de matérialiser la piste d'audit ; 21% non conformes)

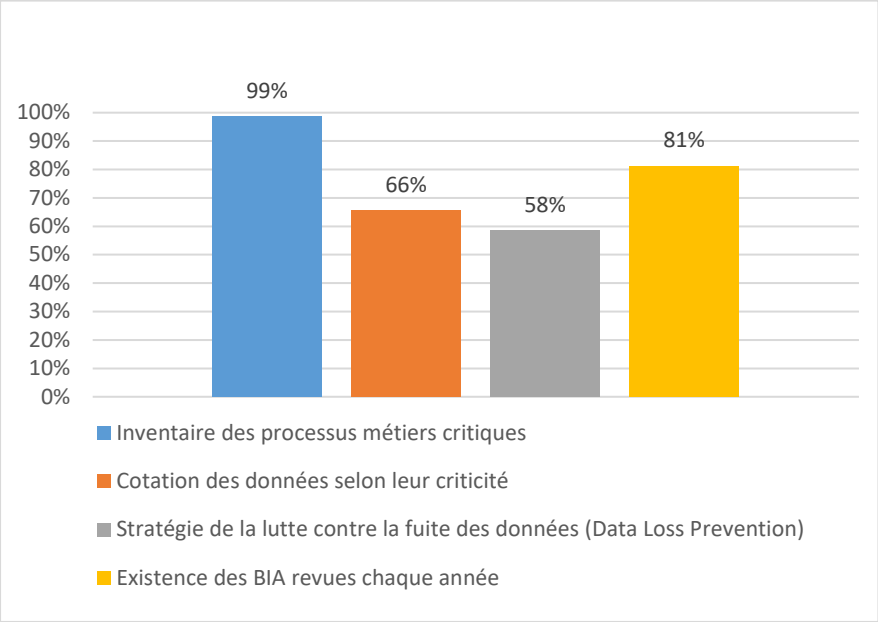
L'inventaire des processus critiques métiers et le plan de continuité d'activité (PCA) sont également généralisés (99 %) mais des limites sont également constatées, notamment :

- les organismes encore réfractaires à la réalisation – pourtant nécessaire – d'une étude d'impact métier (BIA[10]), décrivant leurs besoins en terme de reprise d'activité, restent trop nombreux (19 % contre 26 % en 2022 ;
- plus préoccupant, les tests en conditions réelles du PCA ne progressent pas : en effet, 27 % des organismes ne testent pas leur PCA annuellement. Or, dans un contexte d'augmentation et d'aggravation des cyberattaques, les organismes de la place devraient urgemment prendre ce sujet en considération ;

- enfin, l'ensemble des organismes déclarent posséder un plan de secours informatique, mais un tiers des organismes n'ont pas aligné le PSI aux besoins métier. Le PSI est revu et testé de façon annuelle par 84 % des organismes, ce qui est un progrès.

[10] *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

Graphique 23 Caractéristiques de la gestion de la continuité d'activité



Source ACPR

6. Des efforts à approfondir en matière d'externalisation

Le recours à l'externalisation en matière de technologies de l'information et de la communication (TIC), dite aussi « infogérance », présente de nombreux avantages pour les organismes d'assurance : pallier l'absence ou la faiblesse d'une compétence en interne, disposer d'une expertise spécifique, permettre une rationalisation des coûts…). Mais ce recours s'accompagne de risques opérationnels pour les données et le pilotage de la sécurité des systèmes d'information qu'il convient d'identifier, d'analyser et de maitriser. Or, il est important de souligner que s'appuyer sur l'externalisation pour la réalisation ou la gestion de certaines activités ne soustrait pas les organismes aux obligations qui y sont attachées.

Le bilan en la matière apparaît toujours contrasté.

L'enquête précédente avait permis de mettre en évidence des progrès en matière de contractualisation. Les données déclarées en 2024 confirment cette tendance en particulier, en ce qui concerne les clauses relatives à la localisation des données, et ce, sur l'ensemble des organismes, quelle que soit leur taille.

En revanche, s'agissant des clauses afférentes à l'efficacité des PCA du prestataire (tests et audit), les organismes petits et moyens ne les incluent pas encore suffisamment dans les contrats (86% pour les premiers et 88% pour les seconds). Enfin, l'intégration des services externalisés critiques dans le dispositif de PCA (y compris celui du prestataire) est une mesure qui doit être renforcée, quelles que soient la forme juridique et la taille des organismes.

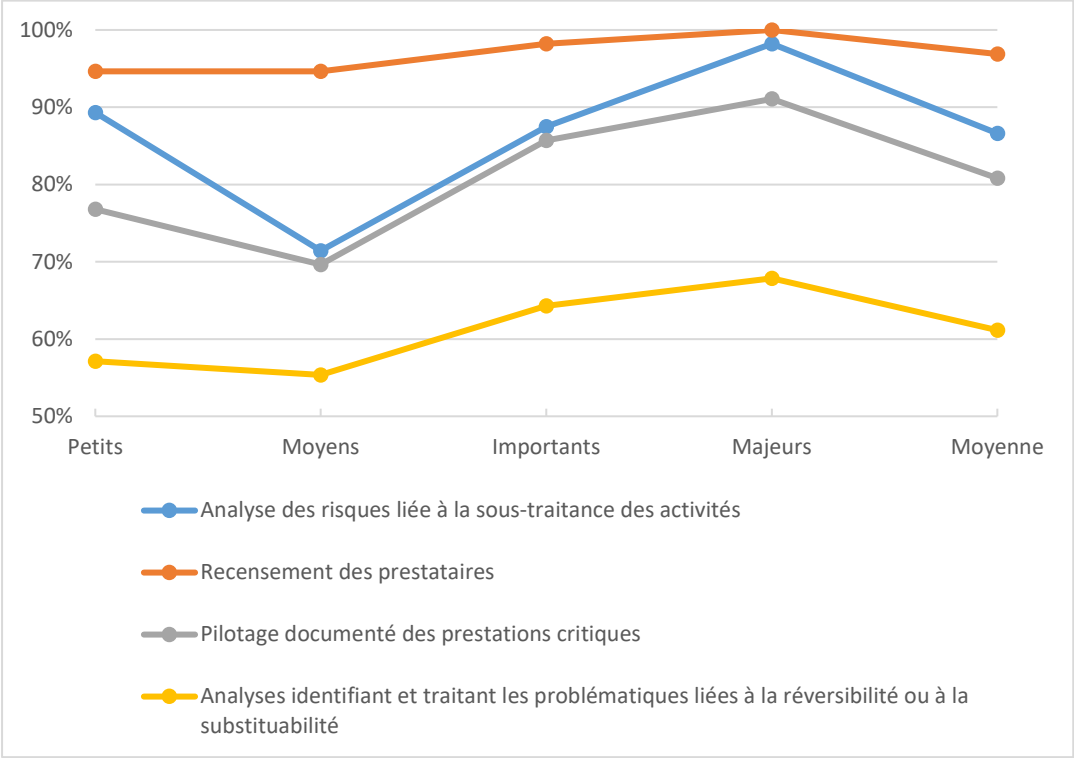
Le recensement des prestataires est une pratique plus ancrée, mais la définition d'exigences et d'indicateurs liés à la sécurité pour les prestations externalisées critiques prévue au contrat est insuffisante, quelles que soient la taille ou la forme juridique des organismes ayant participé à l'enquête.

De même, la réalisation d'une analyse de risque liée à la sous-traitance des activités externalisées apparait plus faible pour les organismes de taille moyenne.

Le pilotage documenté des prestations critiques est en progression, même si un point de vigilance demeure pour les organismes de taille moyenne et les institutions de prévoyance (70 % le prévoient).

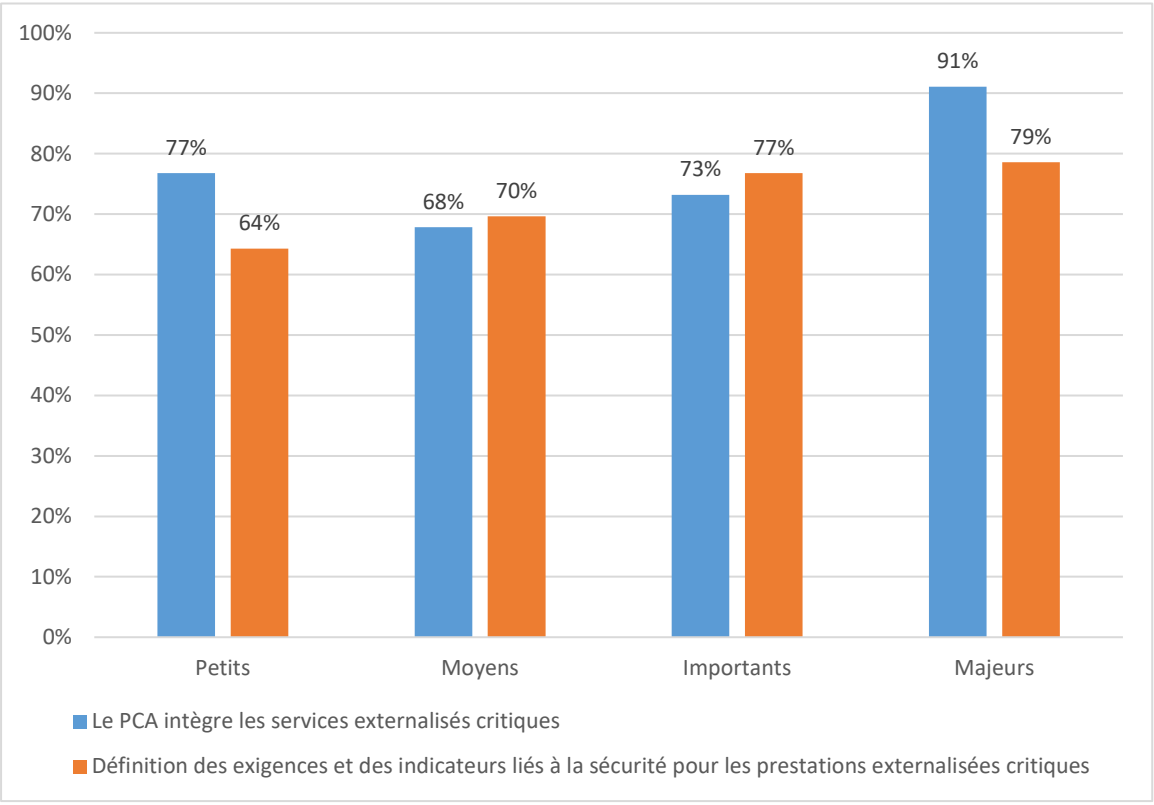
Enfin, la stratégie de retrait mise en place par les organismes d'assurance demeure un point préoccupant. Corollaires de l'externalisation, la réversibilité (reprise des prestations par l'organisme) et la substituabilité (transfert de l'activité à un prestataire tiers) sont très insuffisamment prises en compte et analysées par l'ensemble des organismes répondants, et plus particulièrement chez les mutuelles (43%). Cette fraction des organismes ne parait pas en capacité d'organiser la fin d'une relation contractuelle, quelle qu'en soit la cause.

Graphique 24 Phase d'étude et de contractualisation de l'externalisation SI/SSI



Source ACPR

Graphique 25 Prise en compte des exigences spécifiques à l'externalisation



Source ACPR

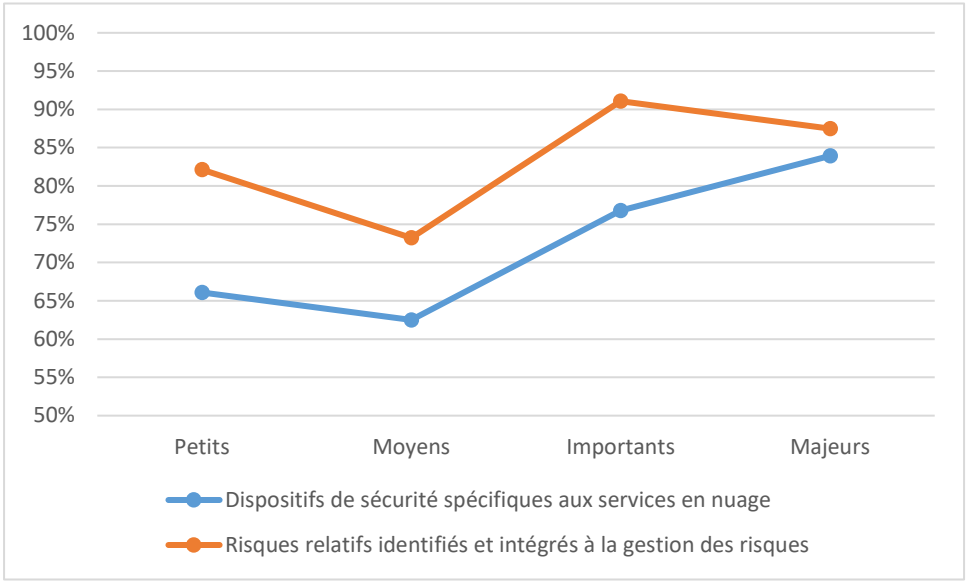
L'utilisation du *cloud* (services en nuage) s'est généralisée (96% des organismes répondants) sur la base des avantages procurés par les solutions *cloud*. Toutefois, ces recours créent également des risques spécifiques :

- augmentation de la surface d'attaque ;
- l'ouverture sur le net rend tous les services potentiellement accessibles ;
- le niveau de sécurité devient dépendant des modalités d'application des configurations par le fournisseur, ainsi que de la bonne gestion des identités, des habilitations ou des vulnérabilités.

L'enquête fait ressortir que même si les risques relatifs aux services en nuage sont mieux identifiés et analysés, la mise en place de dispositifs de sécurité spécifiques à ces services reste encore insuffisante (absence pour 44% des déclarants ; voir en ce sens les orientations de l'AEAPP - EIOPA-BoS-20-002 - relatives à la sous-traitance à des prestataires de services en nuage[11]).

Graphique 26 Dispositif de sécurité des services en nuage

[11] https://acpr.banque-france.fr/sites/default/files/media/2020/07/22/annexe_orientations_aeapp.pdf



Source ACPR

7. Une maitrise du *shadow IT* qui reste à conforter

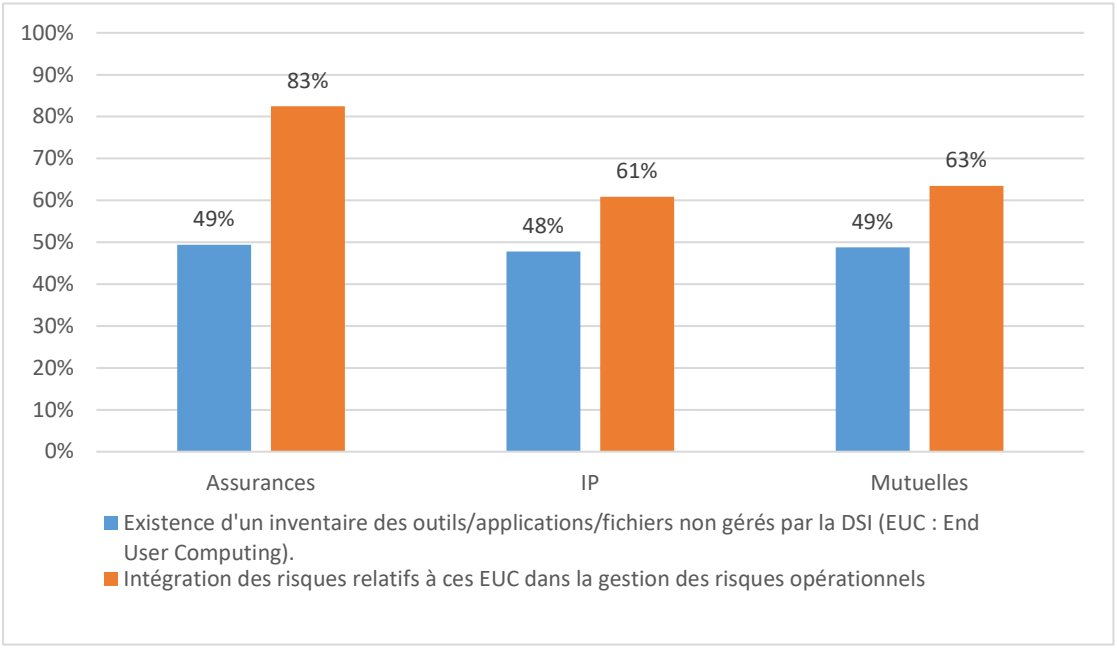
Le *shadow IT*, dont l'incidence est augmentée par l'adoption de services *cloud*, recouvre les outils informatiques sous toutes leurs formes (appareils personnels, logiciels, applications, services web, programmes, …) qui sont développés, achetés ou utilisés par des utilisateurs appartenant à l'organisme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

Même si cette pratique peut répondre à des besoins spécifiques, elle peut avoir des conséquences graves vis-à-vis de la protection des données sensibles, de la conformité ou de la sécurité. En effet, si certains outils peuvent apparaitre relativement inoffensifs, nombre d'entre eux comportent des fonctionnalités telles que le partage et le stockage de fichiers ou des fonctions collaboratives, qui peuvent présenter des risques importants pour une organisation et ses données sensibles.

Le référencement et la gestion des « EUC » (*End User Computing* – programmes ou services non gérés par la Direction des Systèmes d'Information) présentaient de très sévères lacunes en 2019 et en 2022 et le constat s'améliore en 2024 avec des scores en nette croissance en valeur relative (de 22% à 43% pour la réalisation d'inventaires et de 37% à 71% pour l'intégration des outils spécifiques dans la gestion des risques opérationnels). Cette progression reste relative car en valeur absolue, les scores déclarés illustrent une faiblesse persistante au regard des nombreux risques associés à la thématique, tels que l'exposition aux cyberattaques jusqu'à la perte de données hautement confidentielles.

Ainsi, malgré des progrès sensibles, les risques relatifs aux EUC sont encore insuffisamment intégrés dans la gestion des risques opérationnels, cette tendance étant particulièrement marquée chez les institutions de prévoyance (61% en moyenne sur les deux sujets) et les mutuelles (63%).

Graphique 27 Maitrise du *shadow IT*



Source ACPR

8. Préparation à l'entrée en vigueur du cadre réglementaire DORA

En prévision de l'entrée en vigueur au 17 janvier 2025 du cadre réglementaire DORA, l'enquête réalisée a intégré, cette année, quelques questions relatives à l'état de la préparation des organismes.

Près de la totalité des organismes (99,5%) déclarent avoir mis en place un dispositif de veille réglementaire (sur les textes d'application, les consultations publiques…), ce qui parait cependant optimiste au regard des actions de contrôle sur place ou des constats opérés lors du suivi des incidents cyber en 2024 ; en effet, les effets et conséquences des textes structurants concernant la définition du cadre de gestion des risques ou les prestataires de technologies de l'information et de la communication (TIC) critiques ou importants, publiés en 2024, ont alors paru, soit non identifiés, soit très insuffisamment pris en compte.

Une remarque similaire – sur les déclarations apparaissant largement volontaristes - peut être énoncée pour les réponses aux autres questions générales :

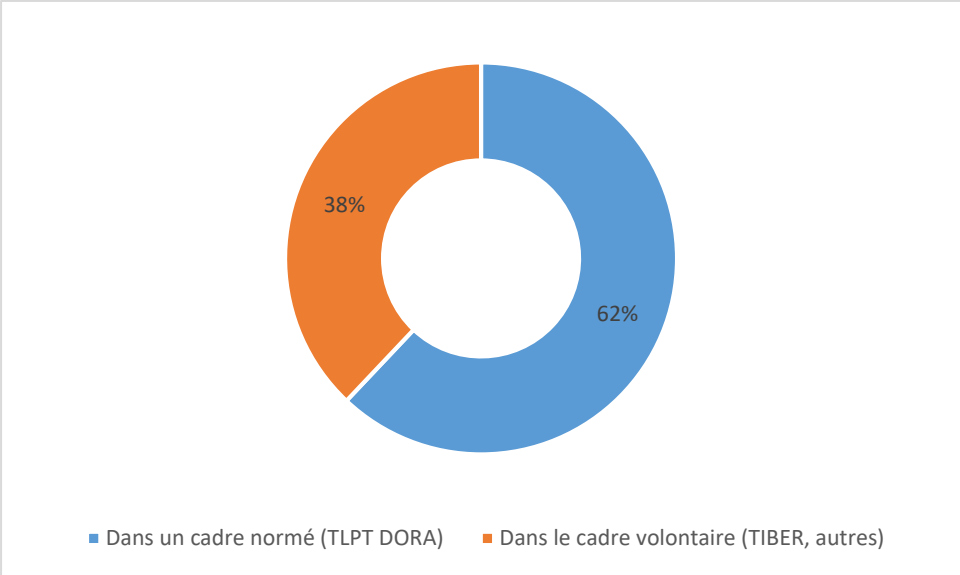
- 99,1% des déclarants énoncent que l'adaptation de la gouvernance aux cadres de gestion des risques ou de contrôle interne a été étudiée ;
- Parmi ces déclarants, de 96,4% pour les petits à 100% pour les majeurs indiquent que l'adaptation au cadre DORA du dispositif de gestion et déclaration des incidents a été étudiée ;
- De 94,6% à 100% également indiquent que le renforcement du dispositif de gestion des prestataires de services TIC critiques et non critiques a été également étudié.
- De 91,3% à 100% des organismes selon la taille ou la nature juridique déclarent renforcer leur dispositif de gestion des prestataires de services TIC, critiques et non critiques

Le dernier point du questionnaire concerne la réalisation de tests de résilience opérationnelle prévue par le règlement DORA. Il convient de ne pas confondre :

- les tests de résilience opérationnelle numérique, à l'initiative de l'entité, une fois par an *a minima* pour les systèmes gérant des fonctions critiques ou importantes et incluant annuellement les prestataires de service TIC critiques ou importants ;

- les tests d'intrusion fondés sur la menace (*threat led penetration tests* ou TLPT) qui deviendront une obligation triennale pour une sélection d'établissements dont la désignation, basée sur des critères réglementaires et sur le principe de proportionnalité, est de la compétence des autorités nationales (ACPR pour les assureurs français) ; ces établissements seront avertis de leur désignation à partir de l'entrée en application de DORA.

Graphique 28 Étude de la mise en œuvre de tests de résilience



Source ACPR