الشركة المركزية لإعادة التأمين
COMPAGNIE CENTRALE DE RÉASSURANCE

ALGEREASS

2ème Semestre 2020 | Bulletin de la Compagnie Centrale de Réassurance (CCR) | www.ccr.dz

Edito

ALGEREASS est une revue semestrielle, abordant les sujets d'actualité auxquels fait face le marché de l'assurance et de la réassurance.

Dans ce numéro, le premier sujet abordé porte sur la conformité dans les assurances. En effet bien que son existence remonte à plusieurs années, sa mise en œuvre requiert un savoir complexe car il s'agit d'un des volets de la Solvabilité II, qui est une réforme réglementaire européenne du monde de l'assurance.

Le déploiement de la Fonction conformité oblige les organismes d'assurance à faire évoluer leur organisation, leur stratégie et leurs méthodes de travail, et afin de prévenir le risque de sanctions et d'atteinte à la réputation de l'entreprise, ils doivent adopter une conduite appropriée vis-à-vis de leurs clients, collaborateurs et partenaires.

Par ailleurs, respecter la réglementation ne suffit plus, la Conformité s'inscrit dans une démarche proactive et nécessite d'anticiper les exigences à venir. Les acteurs qui sauront relever ce défi avec le niveau d'ambition adéquat en tireront, un avantage concurrentiel indéniable. Ce numéro détaille les enjeux et finalités de la Fonction conformité dans les assurances.

Aussi, voilà déjà une année depuis l'apparition du coronavirus «Covid-19», générant un arrêt presque de l'économie mondiale. Le marché financier et les assurances ont été, parmi les premiers, à subir les effets de cette crise sanitaire.

Les conséquences sur la croissance, l'emploi, le commerce et autre, tant national qu'international, sont telles que plusieurs pays, sur les cinq continents, ont vu leurs indicateurs économiques se détériorer. Cette crise a donné lieu à des faillites en série.

Cependant, d'autres risques se sont vu accroître, il s'agit là du Cyber-risque. En effet, il faut croire que la crise sanitaire a été un terrain propice pour l'accroissement des risques liés à la sécurité des particuliers et notamment des entreprises via une utilisation accrue d'internet avec une faible sécurisation des réseaux. L'alternative choisie par les entreprises, à savoir le télétravail, en a été la première cause. L'article en question relate les différentes techniques de piratage ainsi que les solutions auxquelles peuvent recourir les sociétés afin d'amorcer les pertes.

Deux sujets distincts, mais dont le but est le même, à savoir améliorer les performances du marché de l'assurance, seront à l'honneur dans ce numéro.

Bonne lecture !

Vous pouvez retrouver l'ensemble des publications de la CCR sur le site : www.ccr.dz

LA FONCTION CONFORMITÉ DANS LES ASSURANCES

1/ Finalité

La fonction conformité dans une entreprise consiste à réaliser une gestion optimale des risques de non-conformité aux dispositions légales nationales et supranationales applicables en identifiant et évaluant ces risques.

Les risques de non-conformité peuvent être résumés à travers les catégories suivantes :

- Risque judiciaire (poursuites et/ou condamnation) ;
- Risques de pertes financières (amendes, compensations...) ;
- Risques de réputation (perte de clientèle).

Ces catégories de risques peuvent se présenter, dans la réalité, séparément ou cumulées.

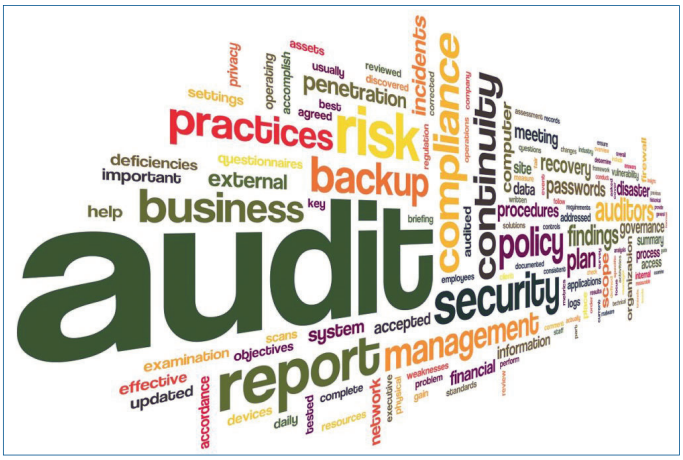
Dans le domaine des assurances et s'agissant d'une activité réglementée, la fonction conformité est intégrée, pour la partie métiers, dans le dispositif du Contrôle de l'État prévu par l'ordonnance 95-07 modifiée et complétée relative aux assurances.

Suite page 2

Sommaire

Suite de la page 1

En effet, celle-ci produit les normes qui doivent régir les contrats d'assurance, l'organisation et la solvabilité financière des organismes d'assurance et de réassurance.
Par rapport à ce dispositif, il existe un mécanisme de surveillance qui repose principalement sur un reporting périodique (trimestriel ou annuel) et un contrôle sur la place.
Pour répondre aux exigences de ce dispositif légal relatif à leur activité, les sociétés d'assurance agréées sont en principe dotées des moyens et ressources pour contrôler, suivre et rendre compte de leur conformité.
Cependant, l'exploitation d'une société d'assurance implique des actes, des engagements et des influences internes et externes, qui ne sont pas régies par la réglementation d'assurance mais par d'autres sources juridiques (Droit économique et social, Droit sur les données numériques, réglementation des changes, réglementation anti-blanchiment, codes de déontologie…etc.).
Les implications possibles de l'action de l'entreprise en interne et en externe du non-respect des dispositions prévues par les références juridiques précitées, ne font pas forcément l'objet d'une prise en charge fonctionnelle normée au niveau des sociétés d'assurance.
A notre sens, la fonction conformité vient combler cet espace du contrôle interne en fournissant aux sociétés d'assurance et aux autorités de contrôle, les instruments d'une couverture globale des obligations légales incombant à ces dernières et induites par leurs statuts et activités.



II/ Organisation de la fonction conformité

A notre sens, la fonction conformité dans une entreprise fait partie du dispositif du contrôle interne. Elle embrasse tous les processus opérationnels de l'entreprise d'assurance.

En ce sens, le support organisationnel de son exercice devrait être analogue et intégré à celui des autres fonctions du contrôle interne (audit interne, gestion des risques, contrôle de gestion, actuariat… etc.).
L'idée de l'intégration de la vérification de la conformité au dispositif du contrôle interne, est justifiée par sa finalité qui est de gérer un type de risques liés à l'exploitation de l'entreprise, en l'occurrence les risques de non-conformité à la législation et la réglementation en vigueur. Elle représente un élément qui complète ce dispositif.

Sur cette base, l'organisation de la fonction conformité est définie par les responsabilités, les compétences et les reportings rattachée à la fonction :

Responsabilités

Cette fonction est assumée par un responsable de haut rang directement rattachée aux organes dirigeants de la compagnie (Direction générale et Conseil d'administration). Il est indépendant de toute structure ou fonction opérationnelles.

Compétences

Les ressources humaines assumant cette fonction devrait présenter un profil professionnel et des qualifications leur permettant à la fois de maîtriser les techniques de contrôle interne et le dispositif légal qui régit ou qui peut impacter l'activité de l'entreprise d'assurance.

Reportings

Le responsable chargé de la fonction conformité rend compte aux organes dirigeants de la compagnie (Directeur Général, Conseil d'administration). Il peut, aussi, livrer des reportings à l'autorité de supervision, périodiquement ou à la demande de celle-ci.

III/ Périmètre d'intervention de la conformité

Sur un plan théorique, la conformité doit embrasser tous les domaines légaux (lois, décrets, arrêtés, décisions, instructions... et conventionnelles (chartes, codes de déontologie, directives...) qui peuvent impacter l'entreprise dans les situations de non-conformité.
Mais en pratique et dans un souci d'efficacité opératoire, il est admis d'impliquer la conformité dans ces différents domaines avec une intensité variable.
Par exemple, le domaine légal traité par la réglementation d'assurance ou le droit classique des affaires, ne présentent pas une priorité de la conformité, parce qu'ils sont déjà couverts par le dispositif du contrôle interne existant mais aussi par la supervision de l'autorité de contrôle des assurances.

En revanche, les domaines liés aux relations clientèle, la protection des données, les règles anti-blanchiment et la fraude, par exemple, constituent le cœur du travail de vérification de la conformité.

Périmètres indicatifs d'intervention de la conformité

Domaines prioritaires	Domaines secondaires
Relations clientèle	Réglementation d'assurance
Protection des données	Droit des sociétés
Anti-Blanchiment	Procédures de gestion
Lutte contre la fraude	Normes comptables
Responsabilité des Dirigeants	Fiscalité
Relations de travail	Droit immobilier
Responsabilité sociale et environnement	Communication financière

Il est important de souligner que, par définition, le champ d'intervention de la conformité n'est pas figé, puisque la source des risques dont elle en charge (dispositif légal et jurisprudence) est évolutive.

IV/ Gestion opérationnelle de la conformité

La vérification de la conformité est une discipline du contrôle interne dont l'objet est la gestion des risques de non-conformité aux dispositifs réglementaires en vigueur au double national et international. Les modalités de mise en œuvre sont celles du Risk Management, à savoir :

- Identification des risques par domaine juridique ;
- Évaluation de l'impact des risques identifiés ;
- Mesures d'atténuation des risques ;
- Indicateurs des risques ;
- Plan des actions correctives.

Ainsi et par cette approche, la fonction produit une cartographie des risques (ou registre des risques) et recommande, le cas échéant, des mesures de réduction des risques de non-conformité.

Schématiquement et sur un cycle annuel, le déroulement de la fonction conformité marque trois temps :

► Le premier correspond à l'établissement (pour la première année) ou à la revue (pour les années ultérieures) du registre des risques de non-conformité par domaine ou catégorie ;

► L'élaboration du plan des recommandations du responsable chargé de la conformité et sa soumission pour adoption au comité de la conformité ;

► La livraison d'un reporting périodique aux organes de gestion de l'entreprise (Direction Général et Conseil d'administration) et éventuellement, à l'autorité de contrôle.

V/ Conformité et prévention

La prévention en matière de conformité consiste à déployer toute action de nature à réduire la probabilité de réalisation des risques de non-conformité auxquels la compagnie d'assurance peut être confrontée.

Dans ce sens, il existe au moins deux moyens de prévention à déployer par la compagnie d'assurance :

- La diffusion de la culture de la conformité, par la formation et l'information des services gestionnaires de la compagnie. Il s'agit de développer le réflexe d'un retour régulier aux références réglementaires régissant les opérations pour s'assurer de leur conformité.
- La veille réglementaire, qui consiste à suivre l'évolution avérée ou probable des règles auxquelles l'activité de la compagnie est soumise et de prévoir les mesures à entreprendre pour minimiser les risques de non-conformité qui peuvent survenir.

Conclusion

La vérification de la conformité est une fonction relativement nouvelle en Algérie. Elle est encore quasiment inexistante dans le secteur des assurances. Alors que les risques de non- conformité aux différentes réglementations et codes de déontologie, sont réels sinon avérés.

L'absence de la fonction conformité dans les modelés de management des compagnies algérienne d'assurance (à l'exception probablement des filiales des groupes internationaux), est liée nous semble-t-il au vide juridique entourant cette fonction.

Aussi, nous pensons, qu'il serait indiqué de produire une matière réglementaire du contrôle interne dans les compagnies d'assurance en incluant la conformité. A notre sens, cette mesure serait de nature à renforcer les dispositifs de contrôle de la conformité dans le secteur des assurances et favoriserait une participation active de celui-ci à la gestion des risques auxquels sont exposées les institutions financières algériennes notamment la lutte contre le blanchiment d'argent.

M. Hadj Mohamed SEBA
Président Directeur Général

LES CYBER-RISQUES AU TEMPS DU COVID-19

Depuis Février 2020, le monde fait face aux conséquences d'une crise pandémique du nom de Covid-19. Tous les secteurs confondus ont été touchés, certains plus sévèrement que d'autres où des business ont dû être fermés. Ces conséquences ont également impacté le secteur des assurances, à travers le développement de risques auxquels les assureurs n'étaient pas entièrement préparés.

On parle déjà depuis quelques temps du cyber-risk, comme risque émergeant, pour lequel les assureurs ont mis en place une couverture adaptée, non encore répandue partout dans le monde, elle devrait se généraliser peut-être suite aux conséquences de la crise sanitaire actuelle.

En effet, Afin d'assurer la continuité des activités, toutes les entreprises ont eu recours au télétravail, du moins, pour les sociétés qui se sont déjà organisées et préparées pour la mise en place de cette solution.

Cependant, une mise en œuvre non-maîtrisée du télétravail peut augmenter considérablement les risques de sécurité pour les entreprises ou organisations qui y recourent. Il peut même représenter une source de danger pour leurs activités face à une montée de la cybercriminalité qui profite de cette nouvelle opportunité pour frapper davantage.

La plupart des entreprises du secteur financier utilisent déjà des systèmes d'accès à distance aux données, mais les capacités installées ne permettent pas forcément à la majorité des employés de s'en servir en même temps, ce qui a pour effet d'accroître les risques pour la sécurité.

Les départements informatiques sont soumis à une pression pour améliorer rapidement les capacités en perfectionnant ou en remplaçant les systèmes existants, ce qui leur laisse peu de temps pour effectuer des tests de sécurité poussés. Certaines failles dans les infrastructures et les protocoles d'accès à distance peuvent passer inaperçues et servir de cibles lors de cyber-attaques.

Néanmoins, à la suite d'une crise d'une telle ampleur, des leçons sont à tirer et les implications en termes de cyber-risques et de cyber-assurances ne se limitent pas uniquement à une augmentation des risques.
Selon le rapport publié par l'ONUDC (Organisation des Nations Unies contre la drogue et le crime), cette crise a fait émerger plusieurs menaces qui y sont directement liées, Il va sans dire que ces menaces ciblent toute personne utilisant la technologie en ligne.

E-mails malveillants

Le courrier électronique est, et continuera d'être, le principal vecteur de menace pour les particuliers et les organisations. Les cybercriminels utilisent depuis longtemps des événements majeurs et largement médiatisés dans des campagnes d'hameçonnage pour améliorer l'efficacité de leurs attaques, et la pandémie actuelle ne fait pas exception.
Différents thèmes sont utilisés dans ces courriels, cela peut aller des rapports sur la pandémie aux conseils de santé provenant de sources gouvernementales officielles.

Une fois cliqué sur, ces virus peuvent inclure divers dommages à un système qui peuvent aller de rançon-giciel, enregistreurs de frappe et autres types de collecte d'informations personnelles. Les criminels envoient des vagues de ces campagnes qui peuvent inclure plus de 150.000 à 175.000 courriels envoyés à la fois, plusieurs campagnes sont observées quotidiennement. Le volume actuel de leurres de courrier électronique liés aux coronavirus représente de loin le plus grand nombre d'attaques que le cyberespace ait connues.

Domaines malveillants

Au mois de mars, les cybercriminels ont créé tous les jours jusqu'à 5.000 noms de domaines malveillants liés au Coronavirus. Bien plus que le nombre de nouveaux sites fiables sur ce thème, alertent les chercheurs bénévoles regroupés depuis peu au sein de la Cyber Threat Coalition (CTC).
Ces sites Web malveillants disposent d'une grande variété d'attaques :

- Usurpation de l'identité d'un site-web officiel ;
- Diffusion de logiciels malveillants ;
- Fausses campagnes.

Désinformation

Les concepts de fausses nouvelles ne sont pas nouveaux. De toute évidence, la situation actuelle a facilité la diffusion de ces informations sur toutes les plateformes sociales. Une très grande partie des utilisateurs d'Internet sont confinés à la maison et utilisent Internet à une capacité accrue, ce qui permet de publier, de republier et d'ajouter des informations erronées sur tous les médias.

Généralement, l'intention est d'induire en erreur afin de nuire à une agence, une entité ou une personne et / ou d'obtenir un avantage financier ou politique, il peut également être utilisé pour le sensationnalisme, la malhonnêteté ou les gros titres fabriqués pour augmenter le lectorat. À une époque où le nombre d'abonnés ou de lecteurs peut devenir une source de gain financier, nous pouvons facilement comprendre les raisons des efforts déployés pour la désinformation ces dernières années.

En ce qui concerne cette pandémie spécifique, comme c'est le cas dans tous les titres à travers le monde, les créateurs de désinformation mènent des campagnes malveillantes et secrètes en créant des histoires et des erreurs dans tous les secteurs et toutes les plateformes sociales pour atteindre leur objectif.

Utilisation accrue des médias sociaux

Alors que de plus en plus de personnes dépendent des médias sociaux pour obtenir des informations, communiquer avec leurs amis et leur famille, travailler, faire des achats en ligne et plus encore, l'utilisation de tous les médias sociaux a connu une croissance exponentielle à la suite de la crise du COVID-19. L'un des résultats statistiques les plus importants résultant de l'utilisation des médias est l'augmentation du temps d'appel en groupe, qui a bondi à plus de 1000% au cours du dernier mois, comme l'a rapporté Facebook Messenger. Cela indique qu'une grande partie du monde maintient correctement la distanciation sociale.

La région MENA est la région où les attaques de cybercriminalité ont le plus proliféré. En effet, de par leurs situations socio-économiques, les cybercriminels profitent du fait que les autorités sont plus concentrées sur comment éviter que la pandémie ne dégénère en une situation incontrôlable.
L'infrastructure bancaire et gouvernementale, les médias sociaux, les attaques sur les visioconférences, et les campagnes d'hameçonnage sont les principaux risques liés au cyberespace dans la zone MENA.

A côté de la mise en place d'une campagne de sensibilisation à la cybercriminalité et de plus de déploiement d'ef-

forts de la part des autorités, l'assurance peut, elle aussi, atténuer les cyber-risques. En effet, le renforcement des mesures de sécurité du réseau et de la surveillance est essentiel pour lutter contre ce cyber-risque accru.

Il est également important que les entreprises réfléchissent à mettre en place des mesures pour atténuer leurs expositions à ce genre de risque, et de prime à bord, la souscription d'une assurance pour la couvrir, et dans ce contexte, il est nécessaire de comprendre les différents types d'assurance que l'on veut avoir (si ce n'est pas déjà acquis) ou de revoir afin de s'assurer qu'elle correspond aux risques actuels auxquels l'entreprise est confrontée.

Commencez par une assurance «cyber» dédiée, qui n'est pas un produit standardisé mais qui se présente plutôt sous de nombreuses formes et appellations différentes, les cyber-politiques incluent souvent plusieurs couvertures qui pourraient intervenir dans un incident lié au COVID-19, à la fois pour la responsabilité civile et les pertes de première partie, telles que la couverture pour :

- Responsabilité découlant d'une défaillance ou d'une violation de la sécurité du réseau ;
- Responsabilité découlant de l'utilisation, de la divulgation, de l'accès ou de la destruction non autorisés d'informations protégées ;
- Les frais de responsabilité et de défense découlant d'une procédure réglementaire alléguant des actes, des erreurs ou des omissions qui entraînent la violation de la loi régissant les informations protégées ou la violation d'une loi sur les avis de violation ;
- Interruption des activités dans le cas où le réseau du preneur d'assurance est arrêté ou rendu inutilisable en raison d'une cyber-attaque ;
- Coûts pour engager un consultant en criminalistique informatique pour enquêter sur une violation et évaluer la divulgation d'informations protégées ;
- Les coûts pour minimiser les atteintes à la réputation en cas de violation ;
- Les sommes versées en réponse à une demande de cyber extorsion dans laquelle un pirate informatique menace d'attaquer ou de perturber le réseau ou le site Web du preneur d'assurance ou de divulguer des informations protégées.

Une autre question importante se pose dans l'environnement actuel, celle de savoir si les employés utilisent leurs ordinateurs personnels (hors entreprise) à des fins professionnelles.

Si tel est le cas, où un ordinateur personnel est impliqué dans un piratage, cela pourrait créer un problème de couverture. La couverture dépendra du libellé spécifique de votre cyber-police et des faits spécifiques de l'événement.

Aussi, il existe d'autres assurances potentiellement applicables, en plus de la cyber-couverture, on retrouve la police contre la criminalité, cette dernière couvre généralement, entre autres, la fraude informatique, qui comprend la prise ou le transfert frauduleux d'argent, de titres ou de biens via un piratage ou une autre utilisation du réseau du preneur d'assurance. A titre d'exemple, cette couverture peut intervenir si l'entreprise est victime d'une usurpation d'identité ou d'une autre attaque d'ingénierie sociale dans laquelle un employé est amené à transférer des fonds de l'entreprise à un pirate informatique au lieu du destinataire légitime.

D'autres couvertures peuvent également être sollicitées, selon la nature de la responsabilité qui découle d'un cyber incident. Par exemple, si un tiers fait valoir une atteinte à la vie privée découlant d'une violation, consultez la politique de responsabilité générale. Aujourd'hui, les polices de responsabilité générale contiennent une ou plusieurs exclusions relatives aux données électroniques et autres, mais le libellé d'une telle exclusion doit être analysé à la lumière des circonstances spécifiques pour évaluer la couverture potentielle.

La dernière chose dont une entreprise a besoin pendant cette pandémie est d'être piratée. Les retombées économiques d'une cyber-attaque substantielle, aggravées par la pression économique imposée par la COVID-19, pourraient être dévastatrices, l'assurance peut aider à atténuer la perte, si une entreprise est victime d'une cyber-attaque pendant la pandémie, il faut passer rapidement à l'analyse de toutes les polices d'assurance potentiellement pertinentes, prévenir tous ses assureurs et respecter toutes les conditions de chaque police.

Il s'agit là d'une bonne opportunité pour travailler en étroite collaboration avec le courtier et le conseiller en couverture qualifié, à la fois pour l'obtention de polices et en cas de réclamation, pour s'assurer qu'aucun détail n'est laissé de côté et que toutes les exigences de la police sont respectées.

Yousra BAKI
Chef de service Communication

STATISTIQUES CAT NAT

Le taux de pénétration de l'assurance CAT NAT en Algérie

Le risque Immobilier

Estimation du stock de logements assujettis à Octobre 2019

8 750 969

Nombre de logements couverts en 2019

1 074 403

Taux de pénétration

12.28%

Le risque commercial & industriel

Nombre total des inscrits au registre de commerce à fin 2019

2 054 912

Nombre de polices au titre des risques commerciaux et industriels en 2019

177 937

Taux de pénétration

8.66%

Soit un taux moyen de 10,47%

Évolution du taux de pénétration de l'assurance CAT NAT

Années	Habitations	Installations industrielles et commerciales	Taux moyen
2019	12.28 %	8.66 %	10.47 %
2018	10.47 %	7.93 %	9.20 %
2017	11.48 %	8.22 %	9.85 %

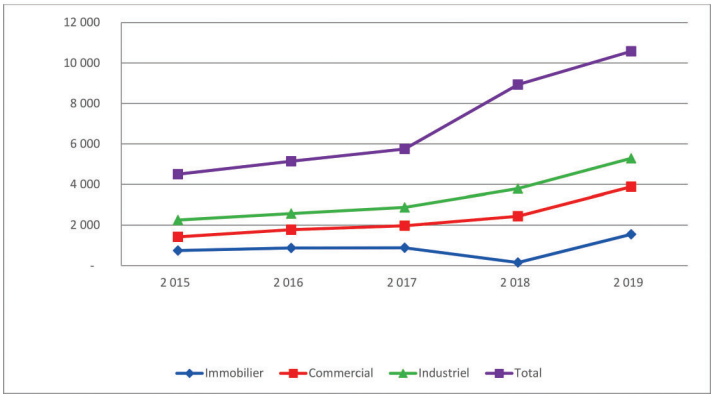
Évolution du marché CAT NAT de 2015 à 2019

Primes en Millions DA

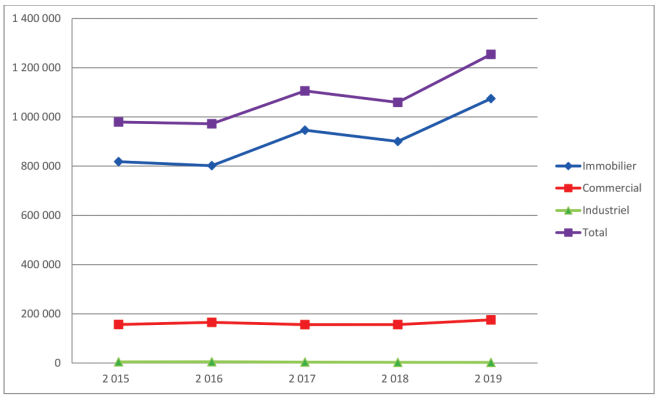
	2015		2016		2017		2018		2019	
	Primes	Nbre de risques assurés	Primes	Nbre de risques assurés	Primes	Nbre de risques assurés	Primes	Nbre de risques assurés	Primes	Nbre de risques assurés
Immobilier	743	817.926	869	801.514	880	945.964	149	900.074	1.544	1.074
Commercial	675	156.648	903	165.366	1.088	156.073	2.287	156.352	2.338	176
Industriel	832	4.677	797	5.032	906	3.746	1.357	2.665	1.405	2
Total	2.251	979.251	2.570	971.912	2.874	1.105.783	5.137	1.059.091	5.287	1.252

La production de la branche CAT NAT a atteint 5.287 DA en 2019, dont une part de 77,76 % est générée par les compagnies publiques.

Évolution des primes souscrites



Évolution du nombre des risques couverts



Estimation du taux de pénétration de l'assurance CAT NAT pour les biens immobiliers en 2019, par wilaya

Wilayas	Taux de pénétration	Wilayas	Taux de pénétration	Wilayas	Taux de pénétration
1. Boumerdes	35.83 %	17. El Oued	12.77 %	33. Sidi Bel Abbès	6.72 %
2. Tindouf	29.13 %	18. Jijel	11.84 %	34. Aïn Defla	6.69 %
3. Saïda	25.89 %	19. Mila	11.53 %	35. Sétif	6.35 %
4. Constantine	25.34 %	20. El Tarf	11.50 %	36. Annaba	6.16 %
5. Laghouat	22.29 %	21. Ouargla	10.78 %	37. Béjaia	5.21 %
6. Tiaret	19.78 %	22. Oran	10.45 %	38. Naâma	5.14 %
7. Alger	19.73 %	23. Tizi Ouzou	9.32 %	39. Tamanrasset	4.72 %
8. Guelma	18.35 %	24. Tissemsilt	9.12 %	40. Mascara	4.09 %
9. M'sila	17.60 %	25. Ghardaïa	9.06 %	41. Bechar	3.60 %
10. Chlef	16.67 %	26. Khenchela	8.96 %	42. Relizane	3.59 %
11. Blida	16.28 %	27. Tipaza	8.42 %	43. Djelfa	3.51 %
12. Medea	15.73 %	28. Aïn Temouchent	8.33 %	44. Oum El Bouaghi	3.31 %
13. Skikda	14.81 %	29. Batna	8.16 %	45. Souk Ahras	2.79 %
14. Bordj Bou Arreridj	14.57 %	30. Tlemcen	7.70 %	46. Tebessa	2.28 %
15. Biskra	14.45 %	31. Bouira	7.25 %	47. Illizi	1.90 %
16. El Bayadh	13.73 %	32. Mostaganem	6.78 %	48. Adrar	1.78 %

Estimation du taux de pénétration de l'assurance CAT NAT pour les biens industriels & commerciaux en 2019, par wilaya

Wilayas	Taux de pénétration	Wilayas	Taux de pénétration	Wilayas	Taux de pénétration
1. Blida	14.92 %	17. Ouargla	7.66 %	33. Ghardaïa	4.17 %
2. Boumerdes	14.85 %	18. M'sila	7.50 %	34. Tamanrasset	4.11 %
3. Alger	14.23 %	19. Bouira	7.17 %	35. Tebessa	4.01 %
4. Tipaza	13.31 %	20. Medea	6.98 %	36. Mascara	3.72 %
5. Jijel	12.72 %	21. Batna	6.75 %	37. Bechar	3.64 %
6. Annaba	12.30 %	22. Tissemsilt	6.60 %	38. Oum El Bouaghi	3.56 %
7. Biskra	12.05 %	23. Guelma	6.49 %	39. Aïn Temouchent	3.39 %
8. Constantine	10.87 %	24. Illizi	6.23 %	40. Relizane	3.21 %
9. Oran	9.94 %	25. Tlemcen	6.09 %	41. Khenchela	3.14 %
10. Mostaganem	9.53 %	26. Sétif	5.89 %	42. Adrar	2.81 %
11. Bordj Bou Arreridj	8.96 %	27. Souk Ahras	5.86 %	43. Tiaret	2.77 %
12. Tizi Ouzou	8.57 %	28. El Tarf	5.45 %	44. Sidi Bel Abbès	2.66 %
13. Aïn Defla	8.55 %	29. Béjaia	5.38 %	45. Saïda	2.56 %
14. Chlef	8.50 %	30. El Bayadh	5.12 %	44. Djelfa	2.49 %
15. Mila	8.23 %	31. El Oued	5.07 %	47. Tindouf	1.79 %
16. Skikda	7.69 %	32. Laghouat	4.57 %	48. Naâma	1.48 %