OCM
OFFICE DE CONTRÔLE
DES MUTUALITÉS

DOMAINES ET INDICATEURS D'APPLICATION POUR L'EVALUATION DE L'EXERCICE 2026

Dans le cadre de la responsabilisation des organismes assureurs sur le montant de leurs frais d'administration, qui est d'application en vertu des dispositions de l'arrêté royal du 10 avril 2014, onze domaines ont été fixés dans le chef de l'Office de contrôle, en regard de l'évaluation de l'exercice 2026.

Ces domaines, classés par processus visés à l'article 3 de l'arrêté royal précité, sont repris au tableau ci-après. Dans la seconde colonne du tableau sont indiqués les coefficients de pondération attribués par l'Office de contrôle auxdits domaines.

Processus et domaines	Pondération au sein du processus [1]
Processus 1	
➢ Domaine 2026/P1/OCM/D1 : La gestion des plaintes.	1
Processus 3	
➢ Domaine 2026/P3/OCM/D1 : La circulation rapide des moyens de paiement.	1
➢ Domaine 2026/P3/OCM/D2 : Le paiement rapide des tiers-payants.	1
Processus 4	
➢ Domaine 2026/P4/OCM/D1 : La détection et la récupération des paiements subrogatoires.	1
Processus 5	
➢ Domaine 2026/P5/OCM/D1 : La qualité du contrôle interne et de l'audit interne des unions nationales et mutualités.	2
➢ Domaine 2026/P5/OCM/D2 : La mise en œuvre des contrôles de validité définis à la nomenclature des soins de santé en regard d'une catégorie de prestations – Premier thème de l'année sous-revue.	1
➢ Domaine 2026/P5/OCM/D3 : La mise en œuvre des contrôles de validité définis à la nomenclature des soins de santé en regard d'une catégorie de prestations – Deuxième thème de l'année sous revue.	1
➢ Domaine 2026/P5/OCM/D4 : Audit gestion IT.	0

[1] A titre d'exemple, un chiffre 2 signifie qu'au sein du processus concerné, ce domaine aura le double du poids des domaines dotés du chiffre 1.

Processus 7 ➢ Domaine 2026/P7/OCM/D1 : Le suivi adéquat des soldes comptables présentés par les comptes de l'assurance obligatoire. ➢ Domaine 2026/P7/OCM/D2 : L'imputation des dépenses en soins de santé et en indemnités aux modèles de dépenses ad hoc. ➢ Domaine 2026/P7/OCM/D3 : Le dépôt des comptes annuels de l'assurance obligatoire.	2 3 1

Remarques générales

- Il est à noter que, dans la présente note, chaque mention du terme « union nationale » fait également référence à la Caisse des soins de santé de HR Rail, excepté en ce qui concerne les domaines afférents au secteur des indemnités pour lequel la Caisse n'est pas concernée.
- Le libellé 'assurance obligatoire' vise partout l'assurance obligatoire fédérale.

Domaine 2026/P1/OCM/D1 : La gestion des plaintes

A. Justification du domaine

Afin d'offrir une prestation de services de qualité et être en mesure de s'améliorer, les organismes assureurs doivent, dans la mesure où elles sont fondées, prendre en considération les insatisfactions éventuelles rencontrées par leurs membres, mais également par tout autre tiers avec lesquels ils sont appelés à collaborer.

B. Indicateur

L'indicateur afférent à ce domaine se présente sous la forme des réponses apportées par l'ensemble des entités mutualistes, à une batterie de 16 questions établies par l'Office de contrôle.

C. Données visées

Les procédures de travail et la mise en œuvre de celles-ci, relatives aux aspects suivants :
- réception des plaintes ;
- traitement des plaintes ;
- analyse des plaintes et rapport ;
- révision permanente des procédures.

D. Approche suivie

L'Office de contrôle a établi une liste de 16 questions et octroie à chacune de celles-ci un poids de 5,00% ou de 7,50%, en fonction de l'importance du point concerné. Ces questions sont ensuite soumises à l'ensemble des entités mutualistes afin qu'elles fournissent en regard de chacune de celles-ci une réponse en indiquant selon le cas « oui », « non » ou « partiellement ». En cas de réponse positive, il est demandé aux entités mutualistes de fournir une information probante afin de justifier leur réponse, tels que par exemple un formulaire de plaintes normalisé, la description de la procédure de plaintes, un dépliant, etc. En cas de réponse « partiellement », les entités mutualistes sont invitées à expliciter leur réponse.

Le questionnaire sous revue doit être introduit pour le 31 janvier 2026, de telle manière à pouvoir être vérifié sur place par les inspecteurs de l'Office de contrôle, lors des visites de contrôles effectuées en 2026.

Le questionnaire concerné est le suivant :

1. <u>Réception des plaintes</u>

		Oui	Non	Partiellement [1]	Pondération
1	Existe-t-il un coordinateur désigné pour centraliser les plaintes[2]? ➢ *Si "oui", veuillez donner les coordonnées du coordinateur, ainsi qu'un organigramme.*				5,00%
2	Existe-t-il une description des procédures internes de gestion des plaintes ? ➢ *Si "oui", veuillez joindre cette description.*				7,50%
3	Cette procédure a-t-elle été validée par le conseil d'administration de l'organisme assureur[3] ou par des personnes physiques auxquelles ou par l'organe auquel cette compétence a été déléguée par le conseil d'administration? ➢ *Si la procédure a été validée, veuillez en fournir la preuve.* ➢ *Si le conseil d'administration de l'organisme assureur a délégué la compétence de valider la procédure, en application de l'article 23, alinéa 2 de la loi du 6 août 1990, veuillez en fournir la preuve.*				5,00%
4	Cette procédure a-t-elle été communiquée à tous les collaborateurs? ➢ *Si "oui", veuillez joindre une description de la manière de communiquer, ainsi que, en cas de communication par écrit, une copie de cette communication.*				7,50%
5	L'existence de la procédure de traitement des plaintes et l'endroit où cette procédure peut être consultée (site web ou agence) sont-ils communiqués et mis particulièrement en évidence dans cette communication au moins une fois par an aux assurés et ce, soit à l'occasion d'une communication écrite individuelle soit par l'intermédiaire d'un média écrit d'information aux membres ? ➢ *Si "oui", veuillez joindre un exemple d'une communication écrite.*				7,50%
6	Existe-t-il un formulaire de plaintes normalisé ? ➢ *Si "oui", veuillez joindre ce formulaire.*				5,00%
7	La procédure de plaintes est-elle expliquée sur votre site internet ? ➢ *Si "oui", veuillez joindre la référence à la page concernée du site web.*				5,00%
8	Existe-il un dépliant mis à disposition des assurés expliquant la procédure de gestion des plaintes ? ➢ *Si "oui", veuillez joindre cette brochure.*				5,00%

[1] En cas de réponse « partiellement », veuillez expliciter votre réponse.

[2] On entend par « *plainte* » « *Une réaction formulée ou confirmée par écrit d'un assuré/stakeholder qui a fait usage d'un produit ou d'une prestation de services par l'OA et qui n'est pas satisfait d'un acte, d'une prestation ou d'un service presté. Il s'agit d'une réaction dont l'utilisateur attend que l'OA en fasse quelque chose. Il faut entendre par « stakeholder », un prestataire de soins, une institution de soins et un citoyen qui n'est pas affilié ou inscrit à l'organisme assureur* ». Cette définition vise également les plaintes relatives au contenu de la réglementation.

[3] Pour ce qui concerne les mutualités, lisez "organisme assureur" comme « union nationale ».

2. Traitement des plaintes

		Oui	Non	Partiellement [1]	Pondération
1	Chaque plainte est-elle enregistrée[2] **et** obtient-elle un numéro unique[3]? ➢ *Si "oui", veuillez joindre une description de la procédure d'enregistrement, ainsi qu'un aperçu des plaintes enregistrées avec leur numéro unique au cours des mois d'octobre, novembre et décembre 2025.*				5,00%
2	Un accusé de réception est-il envoyé systématiquement dans les 8 jours calendrier à la personne ayant introduit une plainte ? ➢ *Si "oui", veuillez joindre un exemplaire d'accusé de réception.* ➢ *Si "non", veuillez joindre une liste des cas où un accusé de réception est oui ou non envoyé, un exemplaire de la notification de réception qui est envoyée dans certains cas, ainsi que la raison pour laquelle une notification de réception n'est dans certains cas pas envoyée[4].*				5,00%
3	Dans la réponse définitive, est-il précisé qu'en cas d'insatisfaction de la manière dont la plainte a été gérée par la mutualité, il existe une possibilité de s'adresser au service compétent de l'union nationale ou à l'ombudsman de l'union nationale ? ➢ *Si "oui", veuillez joindre un exemple de réponse définitive.*				5,00%
4	La description des procédures internes pour le traitement des plaintes prévoit-elle un délai de 45 jours calendrier ou moins pour l'octroi d'une réponse définitive **et** ce délai est-il respecté [5]? *(voir ci-dessous pour quelques modalités pratiques)*				7,50%

3. Analyse des plaintes et rapport

		Oui	Non	Partiellement [1]	Pondération
1	Les plaintes sont-elles analysées **et** un rapport d'analyse[6] est-il transmis au conseil d'administration au moins une fois par an? ➢ *Si "oui", veuillez joindre le dernier rapport d'analyse qui a été transmis au conseil d'administration.*				7,50%
2	Un plan d'actions ayant pour but d'éviter les plaintes récurrentes est-il rédigé au moins une fois par an ? ➢ *Si "oui", veuillez joindre le dernier plan d'actions qui a été établi concernant les plaintes récurrentes.*				7,50%

[1] En cas de réponse « partiellement », veuillez expliciter votre réponse.
[2] Il peut s'agir d'un enregistrement papier ou sur support électronique.
[3] Si chaque contact avec les membres (questions, plaintes…) reçoit un numéro unique, il n'est pas indispensable que les numéros qui sont attribués aux plaintes se suivent.
[4] A documenter par l'entité mutualiste.
[5] Compte tenu de la suspension de ce délai tant que l'intéressé ou un organisme tiers n'a pas donné une suite complète à des renseignements demandés par l'entité mutualiste qui sont nécessaires à la prise d'une décision.
[6] Etant donné que chaque mutualité peut avoir une procédure de traitement des plaintes différente, un rapport d'analyse doit être établi par mutualité. L'établissement d'un rapport consolidé pour l'union nationale dans son ensemble est toutefois exigé également.

4. Révision permanente des procédures

		Oui	Non	Partiellement [1]	Pondération
1	Le système de gestion des plaintes est-il (auto-)évalué au moins une fois par an **et** un rapport d'évaluation est-il transmis au conseil d'administration [2]? ➢ *Si "oui", veuillez joindre le dernier rapport de cette (auto)-évaluation qui a été transmis au conseil.*				7,50%
2	Si une (auto)évaluation du système de gestion des plaintes est réalisée, et que des recommandations sont formulées en vue d'améliorer la qualité de la gestion des plaintes[3], des mesures ont-elles été prises afin de satisfaire aux recommandations émises ?[4] ➢ *Si "oui", veuillez joindre une description des mesures prises.*				7,50%

Pour ce qui concerne les 4 questions afférentes au point 2 « Traitement des plaintes », il est à noter que les points concernés seront vérifiés lors d'un contrôle sur place sur la base d'un échantillon de 20 dossiers de plainte. Dans le cadre de l'évaluation des aspects concernés, un seuil de tolérance de 5% est prévu. Ainsi, par exemple pour la question 2.4., un « oui » est octroyé si une réponse définitive a été donnée dans les 45 jours calendrier pour 19 ou 20 des 20 dossiers examinés. Si la population à examiner est plus petite que 20 dossiers, un seuil de tolérance de 1 dossier est également prévu pour l'obtention d'un « oui ». Par ailleurs, si le point concerné n'est pas satisfait pour plus de 50% des dossiers examinés, un « non » est octroyé.

[1] En cas de réponse « partiellement », veuillez expliciter votre réponse.

[2] Etant donné que chaque mutualité peut avoir une procédure de traitement des plaintes différente, un rapport d'évaluation doit être établi par mutualité. L'établissement d'un rapport consolidé pour l'union nationale dans son ensemble est toutefois exigé également.

[3] Etant donné que chaque mutualité peut avoir une procédure de traitement des plaintes différente, un plan d'action doit être établi par mutualité. L'établissement d'un plan d'action consolidé pour l'union nationale dans son ensemble est toutefois exigé également.

[4] Dans le cas où il a été répondu « non » à la question 4.1, ainsi que dans le cas où une (auto)évaluation est réalisée mais n'entraîne pas l'émission de recommandations, le poids afférent à cette question est ajouté à la question précédente (question 4.1).

Domaine 2026/P3/OCM/D1 : La circulation rapide des moyens de paiement

A. Justification du domaine

Les moyens financiers mis à la disposition des organismes assureurs par l'INAMI ont pour but de permettre auxdits organismes d'assurer le paiement, dans les délais, des prestations de soins de santé, ainsi que des indemnités d'incapacité de travail. A cet égard, le respect des dispositions légales et réglementaires constitue l'un des fondements de l'assurance maladie - invalidité.

B. Indicateur

L'indicateur afférent à ce domaine correspond à la valeur du coefficient de liquidité, qui exprime le rapport entre la moyenne des disponibilités journalières et les dépenses financières des organismes assureurs. Ledit coefficient est corrigé via la prise en considération du solde du compte courant avec l'assurance complémentaire.

C. Données visées et période concernée

Le coefficient de liquidité corrigé susmentionné sera calculé sur la base de l'information contenue dans les documents T20 et T21, afférents à l'exercice 2026. Sont également nécessaires les listes des intérêts financiers obtenus en 2026, par les différents organismes assureurs dans le cadre de l'assurance obligatoire. Ces listes sont communiquées à l'Office de contrôle par l'INAMI. La rente moyenne des fonds d'Etat à longue échéance (OLO linéaire) pour l'exercice 2026 constitue également une donnée nécessaire dans le cadre de l'évaluation du domaine sous revue.

D. Approche suivie

L'évaluation des liquidités des organismes assureurs est basée sur la prise en considération des aspects suivants qui sont traités de manière conjointe :

- la rapidité avec laquelle les paiements sont effectués ;
- le maintien au minimum de la trésorerie ;
- le rendement de la trésorerie ;
- la rapidité avec laquelle une dette éventuelle de l'assurance complémentaire envers l'assurance obligatoire est apurée.

Étant donné que « la rapidité avec laquelle les paiements sont effectués » va de pair avec « le maintien au minimum de la trésorerie », les deux éléments d'évaluation sont groupés et évalués à l'aide du coefficient de liquidité, qui exprime le rapport entre la moyenne des disponibilités journalières et les dépenses financières des organismes assureurs. Le « rendement de la trésorerie » est également fonction du coefficient de liquidité.

La « rapidité avec laquelle une dette éventuelle de l'assurance complémentaire envers l'assurance obligatoire est apurée » est traitée lors du calcul du coefficient de liquidité, via la prise en considération du solde du compte courant avec l'assurance complémentaire. Le cas échéant, une indemnité d'intérêt dont le calcul se base sur la rente moyenne des fonds d'État à longue échéance (OLO linéaires de l'exercice 2026) est imputée à charge des organismes assureurs accusant un solde moyen débiteur sur leur compte courant avec l'assurance complémentaire. Le coefficient de liquidité ainsi obtenu pour chaque organisme assureur est ensuite évalué en fonction de l'échelle reprise au guide opératoire.

Enfin, une mesure corrective est appliquée afin de tenir compte du montant des intérêts débiteurs encourus par les organismes assureurs sur leurs comptes financiers et décomptés vis-à-vis du régime de l'assurance obligatoire. Cette mesure consiste à ôter de la quote-part octroyée aux unions nationales sur base du coefficient de liquidité corrigé précité, le montant des intérêts créditeurs dont l'assurance obligatoire n'a pu bénéficier en 2026 du fait de la compensation réalisée avec les intérêts débiteurs. Le montant de cette mesure corrective représente en fait 80% des intérêts débiteurs concernés[(1)].

[(1)] En application de l'article 195, § 3, de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, et conformément aux conditions prévues par l'arrêté royal du 12 avril 1984, les frais d'administration des organismes assureurs sont majorés de 20% du montant des intérêts générés au départ des moyens financiers mis à la disposition des organismes assureurs dans le cadre de l'assurance obligatoire.

Domaine 2026/P3/OCM/D2 : Le paiement rapide des tiers-payants

A. Justification du domaine

L'article 4, §1, de l'arrêté royal du 18 septembre 2015 portant exécution de l'article 53, §1, de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, ainsi que les différentes conventions nationales enregistrées entre les prestataires de soins et les organismes assureurs, précisent les délais dans lesquels les paiements tiers-payants doivent avoir lieu. Le non-respect de ces modalités serait susceptible de remettre en cause le système du régime tiers-payant.

B. Indicateur

L'indicateur afférent à ce domaine correspond à la valeur du ratio annuel, résultant du rapport entre les dettes tiers-payants en souffrance et les paiements tiers-payants effectués.

C. Données visées et période concernée

Le ratio susmentionné est calculé sur base de l'information contenue dans les documents T20 afférents à l'exercice 2026.

D. Approche suivie

Ce domaine traite spécifiquement de la rapidité avec laquelle les organismes assureurs exécutent les paiements en faveur des tiers-payants et est évaluée au moyen du ratio annuel résultant du rapport entre les dettes tiers-payants en souffrance et les paiements tiers-payants effectués. Le calcul dudit ratio exclut expressément les montants afférents aux douzièmes des hôpitaux et ce, de façon à neutraliser en la matière les facteurs sur lesquels les organismes assureurs ne sont pas en mesure d'exercer une influence.

En cas de dépassement par l'INAMI de son objectif budgétaire et d'épuisement du « compte courant excédents de liquidité » d'un ou de plusieurs organismes assureurs, une procédure corrective prévoit en outre que la valeur du coefficient retenu soit fixée en diminuant le ratio initialement obtenu, pour le ou les organismes assureurs concernés, du pourcentage de dépassement de l'objectif budgétaire arrondi à l'unité supérieure. Par exemple, dans l'hypothèse où le coefficient d'un organisme assureur qui aurait épuisé son « compte courant excédents de liquidité » serait de 1,04, et que l'INAMI aurait enregistré un dépassement de son objectif budgétaire de 2,35%, la valeur du coefficient utilisée dans le cadre de l'évaluation dudit organisme assureur, serait diminuée de 0,03 et ainsi portée de 1,04 à 1,01.

Domaine 2026/P4/OCM/D1 : La détection et la récupération des paiements subrogatoires

A. Justification du domaine

L'article 136, §2, de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, fixe les dispositions applicables en matière de récupération des montants payés à titre subrogatoire.

B. Indicateur

L'indicateur afférent à ce domaine se présente sous la forme des réponses apportées par les réviseurs à une batterie de 33 questions établies par l'Office de contrôle et reprises ci-après, ainsi qu'à la circulaire 17/03/D1 du 30 juin 2017, afférente au « Rapport à établir par les réviseurs dans le cadre de la responsabilisation des organismes assureurs sur le montant de leurs frais d'administration - Domaine examiné dans le cadre du processus défini à l'article 3, 4°, de l'arrêté royal du 10 avril 2014: La détection et la récupération des paiements subrogatoires ».

C. Données visées et période concernée

Dans le cadre des paiements subrogatoires, les procédures de travail et la mise en œuvre de celles-ci au cours de l'exercice 2026, relatives aux aspects suivants :

- détection des prestations à récupérer ;
- procédures de suivi.

D. Approche suivie

Les dispositions reprises à la circulaire précitée fixent les modalités à respecter par les réviseurs dans le cadre de leur mission. Il est à noter qu'en raison du nombre important des procédures de travail visées par le questionnaire sous revue, le Conseil de l'Office n'a pas souhaité prédéterminer une méthode d'échantillonnage à suivre et a souhaité laisser les réviseurs libres de fixer eux-mêmes les méthodes concernées permettant d'obtenir, sur le plan de la théorie statistique, un taux de fiabilité suffisant.

Les procédures de détection des cas y sont distinguées de celles appliquées en matière de suivi des récupérations. Le réviseur est appelé à vérifier auprès de chaque mutualité la bonne application des procédures définies par l'union nationale. A l'issue de ses examens, le réviseur donne ensuite son appréciation par rapport aux 33 questions qui lui sont soumises en précisant si les points concernés sont « rencontrés », « pas rencontrés » ou « partiellement rencontrés ». Il est à noter que certaines questions ne sont pas applicables à la Caisse des soins de santé de HR Rail et que dans ce cas, le poids des questions concernées sera reporté sur les autres questions.

Dans l'exécution de leurs travaux, les réviseurs ne feront pas usage de l'assistance directe du service d'audit interne telle que définie dans l'ISA 610.

Conformément aux dispositions de la circulaire précitée, le rapport du réviseur doit être communiqué à l'Office de contrôle pour le 15 mars 2027.

Les questions concernées sont les suivantes :

1.1 Procédures de détection

A. Accidents

(Par accidents, sont visés les accidents du travail, les accidents de la route, les accidents de responsabilité civile, les agressions et les erreurs médicales présumées)

Réception des documents d'hospitalisation	Oui	Non	Part.	Poids
✓ L'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que les informations reprises aux documents 721bis, 723 et 727 soient examinées afin de déterminer si l'hospitalisation concernée ne résulte pas d'un accident ?				3,03%
✓ Dans l'affirmative, lorsque sur la base de l'examen des informations contenues auxdits documents, il y a une suspicion suffisante d'accident, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à l'envoi d'une déclaration d'accident au membre ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

Réception du certificat d'incapacité de travail	Oui	Non	Part.	Poids
✓ L'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que les informations reprises aux certificats d'incapacité de travail soient examinées afin de déterminer si l'incapacité concernée ne résulte pas d'un accident ?				3,03%
✓ Dans l'affirmative, lorsque sur la base de l'examen des informations contenues auxdits documents, il y a une suspicion suffisante d'accident, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à l'envoi d'une déclaration d'accident au membre ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

Réception des feuilles de renseignements indemnités	Oui	Non	Part.	Poids
✓ L'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que les informations reprises aux feuilles de renseignements "indemnités" soient examinées, afin de déterminer si l'indemnisation concernée ne résulte pas d'un accident ?				3,03%
✓ Dans l'affirmative, lorsque sur la base de l'examen des informations contenues auxdits documents, il y a une suspicion suffisante d'accident, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à l'envoi d'une déclaration d'accident au membre ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

Réception d'informations du membre (guichet, courrier, mail, téléphone, …)	Oui	Non	Part.	Poids
✓ Lorsque sur la base d'informations communiquées par un membre, il y a une suspicion suffisante d'accident, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que ces informations soient avec certitude, communiquées au service "accidents" ?				3,03%

✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

Intervention de l'assurance complémentaire	Oui	Non	Part.	Poids
✓ Dans le cadre des prestations accordées en assurance complémentaire, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à détecter une suspicion d'accident ?				3,03%
✓ Dans le cas d'une suspicion suffisante, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à l'envoi d'une déclaration d'accident au membre ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

Envoi et réception de la déclaration d'accident	Oui	Non	Part.	Poids
✓ En l'absence de réponse du membre à l'envoi d'une déclaration d'accident, des rappels sont-ils transmis endéans un délai : - de deux mois, pour le 1er rappel (électronique ou papier) ? - de quatre mois, pour le 2e rappel (électronique ou papier) ? - de six mois, pour le 3e rappel (électronique ou papier)? Ce troisième envoi n'est cependant pas obligatoire lorsque le montant total concerné est inférieur au montant fixé en vertu des dispositions de l'article 326, §3, de l'arrêté royal du 3 juillet 1996.				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

B. Maladies professionnelles

	Oui	Non	Part.	Poids
✓ Préalablement à la réception d'une décision du FEDRIS, si le Médecin-conseil a lié l'intervention de l'assurance maladie-invalidité à une potentielle maladie professionnelle, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que cette information soit enregistrée et qu'un listing provisoire des indemnités d'incapacité de travail octroyées dans le cadre de cette maladie soit établi en prévision d'une récupération future éventuelle ?				3,03%
✓ La procédure de travail précitée est-elle appliquée de manière correcte et systématique ?				3,03%

1.2 <u>Procédures de suivi</u>

A. Généralités

	Oui	Non	Part.	Poids
✓ L'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que les dossiers de subrogation non clôturés et qui ne sont pas bloqués par une procédure judiciaire en cours, soient revus au minimum 1 fois par an ?				3,03%

✓ L'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à établir, au moins une fois par an, un inventaire exhaustif des dossiers en cours ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,04%

B. Accidents

(Par accidents, sont visés les accidents du travail, les accidents de la route, les accidents de responsabilité civile, les agressions et les erreurs médicales présumées)

	Oui	Non	Part.	Poids
✓ Suite à la réception du flux "période acceptée d'incapacité", l'organisme assureur a-t-il, sur la base de cette information, arrêté une procédure de travail visant à éviter les risques de double paiement ?				3,03%
✓ Dans le cas d'un accident de la route avec tiers responsable, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail qui vise à ce qu'un courrier soit adressé au membre afin de l'informer qu'elle va exercer son droit de subrogation et que si le membre conclut une transaction, cette dernière n'est pas opposable à l'entité mutualiste sans l'accord de cette dernière [(1)] ?				3,03%
✓ En cas d'accident de la route sans tiers responsable, c'est-à-dire soit un accident où le tiers responsable ne s'est pas fait connaître ou a fait un délit de fuite, soit un accident où le conducteur responsable n'est pas assuré ou encore, si l'assurance du tiers responsable est en faillite ou sans agrément, l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à ce que les débours soient adressés au Fonds Commun de Garantie Belge (FCGB) ?				3,03%
✓ Lorsqu'elle réceptionne une déclaration d'accident qui met en cause la responsabilité civile d'un tiers (la date de réception doit donc être attestée, par exemple via l'apposition d'un cachet), l'entité mutualiste a-t-elle mis en œuvre une procédure de travail visant à informer la compagnie d'assurance du tiers responsable au plus tard dans un délai de deux mois de la date à laquelle elle est en possession des coordonnées de ladite compagnie ?				3,03%
✓ L'entité mutualiste a-t-elle mis en œuvre une procédure interne de travail visant à faire en sorte que la liste des débours à transmettre au tiers responsable ou à la compagnie d'assurance de celui-ci, soit la plus complète possible ?				3,03%
✓ Dans le cadre des récupérations de montants payés à titre subrogatoire, en cas de procédure judiciaire, l'entité mutualiste a-t-elle mis en œuvre une procédure qui vise à ce que des intérêts de retard soient réclamés ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

[(1)] Article 136, §2, de la loi coordonnée du 14 juillet 1994 relative à l'assurance obligatoire soins de santé et indemnités.

C. Maladies professionnelles

	Oui	Non	Part.	Poids
✓ Lorsqu'une décision positive du FEDRIS est réceptionnée par une mutualité par l'intermédiaire de l'union nationale, la mutualité a-t-elle mis en œuvre des procédures de travail visant à vérifier l'existence des débours (indemnités) à récupérer auprès de cet organisme ?				3,03%
✓ A la réception d'une décision positive du FEDRIS concernant une indemnisation pour maladie professionnelle, et si l'indemnité proposée ne fait pas l'objet d'une quelconque contestation, la mutualité a-t-elle mis en œuvre une procédure de travail visant à renvoyer au FEDRIS, le document MP5 dûment complété endéans les deux mois ?				3,03%
✓ Suite à une décision positive du FEDRIS concernant une incapacité permanente, la mutualité a-t-elle mis en œuvre des procédures de travail visant à adapter immédiatement les indemnités octroyées au membre concerné en fonction des indemnités que le FEDRIS va désormais verser à ce membre ?				3,03%
✓ Suite à une décision positive du FEDRIS concernant une maladie professionnelle, la mutualité a-t-elle mis en œuvre des procédures de travail visant à récupérer les indemnités liées à cette maladie qu'elle aurait déjà payées ?				3,03%
✓ Les procédures de travail précitées sont-elles appliquées de manière correcte et systématique ?				3,03%

Domaine 2026/P5/OCM/D1 : La qualité du contrôle interne et de l'audit interne des unions nationales et mutualités.

A. Justification du domaine

Conformément aux dispositions de l'article 31 de la loi du 6 août 1990, « chaque union nationale doit disposer d'un système de contrôle interne et d'audit interne qui porte sur l'ensemble de ses activités, ainsi que sur celles des mutualités qui lui sont affiliées ». La qualité du système de contrôle interne et d'audit interne est l'un des éléments fondamentaux du bon fonctionnement des organismes assureurs et la condition nécessaire à l'exécution correcte des missions qui leur sont confiées. Par la circulaire 10/11/D1 du 18 octobre 2010, entretemps remplacée par la circulaire 24/04/D1 du 2 juillet 2024, l'Office de contrôle a fixé le modèle COSO-ERM comme base lors de l'identification des risques et lors de leur évaluation et gestion afin de réaliser les objectifs posés.

B. Indicateur

L'indicateur afférent à ce domaine se présente sous la forme des réponses apportées par les réviseurs à une liste de 84 questions qui sont classées selon les 8 composantes fixées par le modèle COSO-ERM (5 de ces questions ne concernent pas la Caisse des soins de santé de HR Rail). Ledit questionnaire, qui figure en annexe 1, sera à compléter par les réviseurs désignés par les différents organismes assureurs en regard de l'assurance obligatoire. A chaque question, il est attribué un poids identique, soit 1,1905% (100%/84) pour les cinq unions nationales et 1,2658% (100%/79) pour la Caisse des soins de santé de HR Rail.

C. Données visées et période concernée

Les questions concernées portent sur la situation constatée par les réviseurs au cours de l'exercice 2026.

D. Approche suivie

En regard de chaque question et après examen de celle-ci, le réviseur est invité à indiquer à son rapport l'une des réponses suivantes :

- NON (si rien n'a été fait) ;
- Plutôt NON (si le point n'est pas rencontré, sans que l'on puisse dire que rien n'a été fait) ;
- Plutôt OUI (si le point est dans une grande mesure rencontré, mais que de nouvelles étapes sont néanmoins encore à réaliser) ;
- OUI (si le point est rencontré).

- pour les questions où le réviseur estime que la réponse à apporter est « NON », « Plutôt NON » ou « Plutôt OUI », il est demandé au réviseur de reprendre un commentaire étayant son appréciation. Dans ce cas, le réviseur se doit également d'indiquer si ladite appréciation est ou non extrapolable à l'ensemble de l'organisme assureur concerné. Dans l'hypothèse où certaines remarques ne concerneraient pas toutes les mutualités, le rapport devra mentionner explicitement l'appréciation attribuée à chacune de celles-ci ;

- préalablement à l'examen qui sera réalisé par les réviseurs, chaque entité mutualiste devra réaliser une auto-évaluation sous la forme d'un questionnaire complété, et dont les réponses seront suffisamment circonstanciées et documentées. Il est à noter que le questionnaire complété par les soins de l'entité mutualiste sera destiné exclusivement à l'usage des réviseurs et ne sera pas communiqué à l'Office de contrôle. Le rapport transmis à l'Office de contrôle reprendra uniquement le questionnaire complété par le réviseur à l'issue de son examen ;

- compte tenu du fait que chaque organisme assureur dispose de sa propre structure organisationnelle, il appartiendra à chaque réviseur de juger si la question traitée doit seulement être examinée au niveau de l'union nationale ou si elle doit également faire l'objet d'un examen en regard de chacune des mutualités de celle-ci. Lorsqu'une question nécessite un examen auprès des mutualités, il est impératif que ledit examen soit réalisé auprès de toutes les mutualités affiliées à l'organisme assureur concerné ;

- un rapport unique doit être présenté par organisme assureur, lequel concernera néanmoins toutes les mutualités qui lui sont affiliées. Dans l'hypothèse où les mutualités examinées ne seraient pas toutes soumises au contrôle du même réviseur, il appartient au réviseur désigné par le secrétariat national pour l'assurance obligatoire de centraliser l'ensemble des informations dans un rapport unique.

Le rapport du réviseur doit être communiqué à l'Office de contrôle pour le 15 mars 2027.

Domaine 2026/P5/OCM/D2 : La mise en œuvre des contrôles de validité définis à la nomenclature des soins de santé en regard d'une catégorie de prestations – Premier thème de l'année sous revue

A. Justification du domaine

Les contrôles de validité et le respect des règles définies à la nomenclature des soins de santé sont essentiels afin d'assurer un remboursement correct des prestations et un usage adéquat des fonds de l'assurance obligatoire. Le thème avancé par l'INAMI est celui afférent aux prestations relevant de la spécialité en cardiologie visées à l'article 20, §1er, e), de la nomenclature des soins de santé.

B. Indicateur

L'indicateur afférent à ce domaine correspond à la manière dont sont exécutés les contrôles de validité dans le domaine des prestations relevant de la spécialité en cardiologie dont l'INAMI a indiqué qu'ils doivent être réalisés a priori.

C. Données visées et période concernée

Les données utilisées pour l'évaluation de ce domaine sont les montants des dépenses fournies par les organismes assureurs, en regard des prestations retenues par l'Office de contrôle et introduites dans les modèles N par les organismes assureurs au cours du premier semestre 2026.

D. Approche suivie

En concertation avec l'INAMI, une catégorie de prestations reprise à la nomenclature des soins de santé est choisie annuellement par le Conseil de l'Office de contrôle. Ensuite, et toujours en concertation avec l'INAMI, l'Office établit une liste de codes de la nomenclature en regard desquels des contrôles de validité doivent être en principe réalisés par les organismes assureurs dans le but de procéder au remboursement correct des prestations concernées.

Sur la base de la liste précitée, l'Office de contrôle attribue un poids à chaque code de la liste en fonction du rapport existant entre d'une part, la somme des dépenses afférentes au code concerné, et d'autre part, le total des dépenses enregistrées pour l'ensemble des codes repris à la liste. Le poids attribué à chaque code est ensuite proportionnellement réparti entre les contrôles de validité qui le concernent.

L'Office de contrôle transmet ensuite aux organismes assureurs la liste des codes de la nomenclature retenus et les invite à compléter cette liste en indiquant en regard de chacun des codes si les contrôles de validité concernés sont exécutés. Dans l'affirmative, il leur est également demandé de mentionner si ces contrôles ont eu lieu au moment de la tarification des prestations concernées (contrôles a priori) ou ultérieurement à celle-ci (contrôles a posteriori). Il va de soi que pour les prestations retenues visées à l'article 20, §1er, e), de la nomenclature, ce contrôle ne doit être exécuté qu'a priori. En outre, il leur est demandé d'opérer une distinction selon que :

- les contrôles de validité a priori sont bloquants ou signalétiques ; ces derniers se définissant comme des contrôles dont la seule fonction est de signaler au tarificateur qu'une règle est à vérifier relativement à une prestation donnée mais qui ne présentent pas un caractère bloquant ;
- les contrôles de validité a posteriori sont réalisés annuellement (depuis au moins deux ans) ou dans un délai de trois mois qui suit la date d'introduction de la demande de remboursement auprès de l'organisme assureur.

Les informations ainsi communiquées par les organismes assureurs font ensuite l'objet de vérifications effectuées sur place par les inspecteurs de l'Office de contrôle. A cette occasion, il est également tenu compte des pourcentages de cas fautifs en regard des contrôles a priori bloquants, a priori signalétiques et a posteriori, qui ne sont pas strictement rencontrés.

Domaine 2026/P5/OCM/D3 : La mise en œuvre des contrôles de validité définis à la nomenclature des soins de santé en regard d'une catégorie de prestations – Deuxième thème de l'année sous revue

A. Justification du domaine

Les contrôles de validité et le respect des règles définies à la nomenclature des soins de santé sont essentiels afin d'assurer un remboursement correct des prestations et un usage adéquat des fonds de l'assurance obligatoire. Le thème avancé par l'INAMI est celui afférent aux prestations relevant de la compétence des opticiens visées à l'article 30 de la nomenclature des soins de santé.

B. Indicateur

L'indicateur afférent à ce domaine correspond à la manière dont sont exécutés les contrôles de validité dans le domaine des prestations relevant de la compétence des opticiens dont l'INAMI a indiqué qu'ils doivent être réalisés a priori.

C. Données visées et période concernée

Les données utilisées pour l'évaluation de ce domaine sont les montants des dépenses fournies par les organismes assureurs, en regard des prestations retenues par l'Office de contrôle et introduites dans les modèles N par les organismes assureurs au cours du premier semestre 2026.

D. Approche suivie

En concertation avec l'INAMI, une catégorie de prestations reprise à la nomenclature des soins de santé est choisie annuellement par le Conseil de l'Office de contrôle. Ensuite, et toujours en concertation avec l'INAMI, l'Office établit une liste de codes de la nomenclature en regard desquels des contrôles de validité doivent être en principe réalisés par les organismes assureurs dans le but de procéder au remboursement correct des prestations concernées.

Sur la base de la liste précitée, l'Office de contrôle attribue un poids à chaque code de la liste en fonction du rapport existant entre d'une part, la somme des dépenses afférentes au code concerné, et d'autre part, le total des dépenses enregistrées pour l'ensemble des codes repris à la liste. Le poids attribué à chaque code est ensuite proportionnellement réparti entre les contrôles de validité qui le concernent.

L'Office de contrôle transmet ensuite aux organismes assureurs la liste des codes de la nomenclature retenus et les invite à compléter cette liste en indiquant en regard de chacun des codes si les contrôles de validité concernés sont exécutés. Dans l'affirmative, il leur est également demandé de mentionner si ces contrôles ont eu lieu au moment de la tarification des prestations concernées (contrôles a priori) ou ultérieurement à celle-ci (contrôles a posteriori). Il va de soi que pour les prestations retenues visées à l'article 30 de la nomenclature, ce contrôle ne doit être exécuté qu'a priori. En outre, il leur est demandé d'opérer une distinction selon que :

- les contrôles de validité a priori sont bloquants ou signalétiques ; ces derniers se définissant comme des contrôles dont la seule fonction est de signaler au tarificateur qu'une règle est à vérifier relativement à une prestation donnée mais qui ne présentent pas un caractère bloquant ;
- les contrôles de validité a posteriori sont réalisés annuellement (depuis au moins deux ans) ou dans un délai de trois mois qui suit la date d'introduction de la demande de remboursement auprès de l'organisme assureur.

Les informations ainsi communiquées par les organismes assureurs font ensuite l'objet de vérifications effectuées sur place par les inspecteurs de l'Office de contrôle. A cette occasion, il est également tenu compte des pourcentages de cas fautifs en regard des contrôles a priori bloquants, a priori signalétiques et a posteriori, qui ne sont pas strictement rencontrés.

Domaine 2026/P5/OCM/D4 : Audit gestion IT

A. Justification du domaine

Les organismes assureurs dépendent fortement, pour l'exécution de leurs tâches, du bon fonctionnement de la gouvernance informatique et de la sécurité informatique. Prendre les mesures nécessaires qui garantissent la qualité de la gouvernance informatique et de la sécurité informatique est par conséquent essentiel pour la bonne exécution des missions confiées aux organismes assureurs.

B. Indicateur

L'indicateur afférent à ce domaine se présente sous la forme d'une évaluation de la maturité informatique de l'organisme assureur, réalisée par un partenaire externe spécialisé en audit IT accompagné de plusieurs inspecteurs de l'Office de contrôle, au moyen d'un questionnaire (cf. annexe 2) divisé en quatre domaines de risque :

- Gouvernance informatique ;
- Planification & stratégie informatiques ;
- Processus, services et actifs informatiques ;
- Sécurité de l'information et cybersécurité.

Chaque domaine de risque est ensuite divisé en sous-domaines de risque et chaque sous-domaine de risque comporte plusieurs questions. Sur la base des réponses à ces questions et de la documentation fournie, un score de maturité est attribué à chaque sous-domaine de risque.

Puisque la même criticité ne s'applique pas à tous les sous-domaines de risque, le niveau de criticité a été déterminé pour chacun d'entre eux. Quatre niveaux de criticité ont été définis, avec un poids allant de 0,9 (non critique) à 1,1 (essentiel), et ont été associés aux sous-domaines de risque de manière à ce que le poids moyen pour l'ensemble des sous-domaines de risque soit de 1.

Sur la base des scores de maturité ainsi déterminés par sous-domaine de risque, adaptés au niveau de criticité, un score final est calculé, qui est la moyenne des scores obtenus par sous-domaine de risque. Ce score final est exprimé sous la forme d'un nombre, avec deux chiffres après la virgule. L'objectif est un score de maturité de 3 pour l'ensemble du questionnaire.

C. Données visées et période concernée

L'évaluation en question du questionnaire se fait sur la base de la situation constatée dans le courant de l'année 2026.

D. Approche suivie

Pour chaque question, l'organisme assureur doit, pour une date à déterminer, mettre à disposition les documents/preuves justificatives nécessaires pour l'audit sur une plateforme numérique. Après examen préalable par les auditeurs, ces documents/pièces justificatives seront discuté(e)s plus en détail lors d'un atelier organisé par organisme assureur et dans le cadre duquel chaque organisme assureur aura l'occasion de fournir des précisions supplémentaires et d'éventuel(le)s documents/pièces justificatives supplémentaires.

Lorsque tou(te)s les documents/pièces justificatives reçu(e)s auront été analysé(e)s de manière approfondie par les auditeurs, chaque sous-domaine de risque se verra accorder un score de maturité entre 0 et 5, qui correspond aux niveaux de maturité suivants :

- Niveau 1 : un score de maturité de 0,00 à 1,24 ;
- Niveau 2 : un score de maturité de 1,25 à 2,24 ;
- Niveau 3 : un score de maturité de 2,25 à 3,24 ;
- Niveau 4 : un score de maturité de 3,25 à 4,24 ;
- Niveau 5 : un score de maturité de 4,25 à 5.

Sur la base du fichier Excel élaboré à cet effet, la valeur de l'indicateur est déterminée.

Domaine 2026/P7/OCM/D1 : Le suivi adéquat des soldes comptables présentés par les comptes de l'assurance obligatoire

A. Justification du domaine

L'article 10, § 1er, de l'arrêté royal du 21 octobre 2002 portant exécution de l'article 29, §§ 1er et 5, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités, dispose que « *Toute entité mutualiste procède, une fois l'an au moins, avec bonne foi et prudence, aux opérations de relevé, de vérification, d'examen et d'évaluation nécessaires pour établir avant la clôture de chaque exercice comptable un inventaire complet de ses avoirs et droits de toute nature, de ses dettes, obligations et engagements de toute nature relatifs à chacune de ses activités et des moyens propres qui y sont affectés.* »

B. Indicateurs

Il existe ici deux indicateurs qualitatifs, à savoir :
- la présence d'un inventaire exhaustif et détaillé pour chacun des comptes présentant un solde à la clôture de l'exercice ;
- la présence de « montants anciens » au sein des soldes des comptes afférents aux droits et obligations des membres dans le cadre des prestations et des cotisations à décompter avec l'INAMI.

C. Données visées et période concernée

Les soldes des comptes examinés sont ceux arrêtés à la clôture de l'exercice 2024.

D. Approche suivie

La collecte des données nécessaires à l'évaluation de ce domaine est réalisée dans l'ensemble des mutualités et unions nationales de mutualités, ainsi qu'auprès de la Caisse des soins de santé de HR Rail, par les inspecteurs de l'Office de contrôle. Le poids accordé au domaine sous revue est réparti de façon égale sur les deux indicateurs précités.

Présence d'un inventaire exhaustif et détaillé.

Sur la base des inventaires tenus par chaque entité mutualiste dans le cadre de l'assurance obligatoire, les inspecteurs de l'Office de contrôle vérifient la présence d'un inventaire exhaustif et détaillé pour chacun des comptes présentant un solde à la clôture de l'exercice examiné, conformément aux dispositions de la circulaire de l'Office 21/01/D1 du 30 avril 2021.

En ce qui concerne la présence d'un inventaire détaillé, le nombre de comptes pour lesquels l'entité mutualiste n'a pu fournir un inventaire complet et exhaustif servira de base à l'évaluation.

Présence de "montants anciens" au sein des soldes précités.

Par « montants anciens », il y a lieu de considérer la présence au sein des soldes des comptes afférents aux droits et obligations des membres dans le cadre des prestations et des cotisations à décompter avec l'INAMI (comptes repris sous les codes comptables « 40 – Créances résultant de prestations et cotisations A.M.I. », « 42 – Dépenses A.M.I. à traiter », « 44 – Dettes A.M.I. à un an au plus » et « 49 – Comptes de régularisation et comptes d'attente », à l'exception toutefois des comptes 490 à 493), de montants qui aux termes des délais résultant des dispositions légales et réglementaires de l'assurance maladie-invalidité ou des principes généraux de la comptabilité, ne devaient plus figurer à ces comptes. Les montants anciens détectés sont distingués selon l'exercice au cours duquel ils ont acquis ce caractère.

Domaine 2026/P7/OCM/D2 : L'imputation des dépenses en soins de santé et en indemnités aux modèles de dépenses ad hoc

A. Justification du domaine

Ce domaine d'action porte sur le respect des délais quant à l'imputation aux modèles de dépenses des prestations de soins de santé et d'indemnités comptabilisées. L'imputation des dépenses doit en effet, pour les soins de santé, se référer à un mois comptable déterminé, tandis que pour les indemnités, ladite imputation doit se référer à un trimestre déterminé. Tout déplacement des dépenses entre des mois ou des trimestres aurait pour effet de rendre inexacts les modèles de dépenses introduits par les organismes assureurs auprès de l'INAMI. L'importance de tels déplacements est particulièrement aiguë en cas de déplacements entre des mois ou des trimestres appartenant à des exercices différents.

B. Indicateur

L'indicateur afférent à ce domaine correspond aux montants des dépenses de soins de santé et d'indemnités d'incapacité de travail non imputés respectivement au mois ou au trimestre ad hoc.

C. Données visées et période concernée

Tant en ce qui concerne les dépenses de soins de santé, que celles d'indemnités, les contrôles portent sur la totalité des dépenses imputées sur la période courant du premier trimestre au quatrième trimestre de l'exercice 2025.

D. Approche suivie

Le « respect des délais applicables en matière de soins de santé » se voit assigner un poids de 90%, le second aspect « respect des délais applicables en matière d'indemnités » se voit quant à lui octroyer un poids de 10%.

Les contrôles sont réalisés par les inspecteurs de l'Office à l'aide du logiciel Galvanize (ACL), conformément aux dispositions reprises à la circulaire de l'Office de contrôle 12/10/D1 du 14 décembre 2012. L'impact chiffré des déplacements constatés, représentent les indicateurs de ce domaine.

Les déplacements concernés sont distingués selon qu'ils ont eu pour effet de réaliser un transfert de dépenses entre :

1. deux mois (ou deux trimestres s'il s'agit d'indemnités) appartenant à un même exercice ;
2. deux mois (ou deux trimestres s'il s'agit d'indemnités) n'appartenant pas à un même exercice.

Domaine 2026/P7/OCM/D3 : Le dépôt des comptes annuels de l'assurance obligatoire

A. Justification du domaine

En application de l'article 30bis de la loi du 6 août 1990, inséré par la loi du 17 juillet 2015 portant des dispositions diverses en matière de santé, les comptes annuels doivent être déposés à la BNB dans les trente jours suivant l'approbation par l'assemblée générale / le comité de gestion, en même temps que la liste des administrateurs et réviseurs et le rapport du (des) réviseur(s) sur ces comptes annuels. L'arrêté royal du 6 septembre 2016, qui fixe les modalités de ce dépôt, a rendu cette obligation applicable à partir des comptes annuels de l'exercice 2015. Cette obligation a été instaurée en vue de favoriser la transparence du secteur mutualiste.

B. Indicateurs

L'évaluation est réalisée au moyen des trois questions reprises dans le tableau ci-dessous. Ces questions concernent le respect du délai, ainsi que la qualité du dépôt. L'administration répondra par « oui » ou « non » à chacune de ces questions. Le poids de chaque question est indiqué dans la deuxième colonne du tableau ci-après.

	Poids
1. Les comptes annuels ont-ils été déposés dans le délai lors du premier dépôt pour un exercice déterminé (les dépôts suivants ne sont pas pris en considération), c'est-à-d. dans les trente jours suivant l'approbation de l'assemblée générale / du comité de gestion, et ce premier dépôt a-t-il été réalisé dans la version correcte (version BNB de MutWeb) et avec les pages correctes des comptes annuels? *La réponse à cette question ne tient pas compte du caractère exhaustif ou non des informations visées à la question 2, ni de la présence ou non du rapport visé à la question 3.*	0,70
2. Lors du premier dépôt, la liste des administrateurs et du (des) réviseur(s) a-t-elle été complétée sur la page de garde (nom, prénoms et fonction) ?	0,10
3. Lors du premier dépôt, le rapport du réviseur à l'assemblée générale / au comité de gestion a-t-il été joint (rapport adéquat, rapport complet, ...) ?	0,20

C. Données visées et période concernée

L'évaluation est réalisée sur les comptes annuels de l'assurance obligatoire qui ont été approuvés pendant la période du 2 décembre 2025 au 1er décembre 2026 inclus par l'assemblée générale / le comité de gestion du dernier des six organismes assureurs qui a fait approuver ses comptes annuels.

Dans l'hypothèse où pendant la période sous revue plusieurs comptes annuels auraient été approuvés par l'organisme assureur dont l'assemblée générale s'est réunie en dernier lieu, le montant total octroyé pour ce domaine sera scindé selon le nombre d'exercices pour lesquels le dépôt doit être évalué.

Dans l'hypothèse où aucun organisme assureur n'aurait fait approuver de comptes annuels pendant la période concernée, la totalité du montant à attribuer sera accordée compte tenu du principe fixé au guide opératoire et selon lequel un domaine non évalué, sans mise en cause de la responsabilité des organismes assureurs, est attribué à 100%.

D. Méthode de travail suivie

Un score de 100 % est octroyé à une réponse « Oui », et un score de 0 % à une réponse « Non ».

Le pourcentage à octroyer est calculé au moyen de la formule suivante, dans laquelle il est tenu compte du poids de chaque question :

$X\ (\%) = (A_1 * 0{,}70) + (A_2 * 0{,}10) + (A_3 * 0{,}20)$

A_1, A_2, et A_3 étant les scores pour respectivement les questions 1 à 3.

Annexe 1

Questions à examiner par les réviseurs en regard du domaine afférent la qualité du contrôle interne et de l'audit interne

Composante COSO	Thème	Thème n°	n° question	Descriptif question	Réponses réviseur(s) (NON/Plutôt NON/Plutôt OUI/OUI)	Observations réviseur(s)
Environnement interne	Politique en matière de gestion des risques	1	1	L'union nationale a-t-elle défini une politique en matière de gestion des risques concrétisée par une charte ?		
			2	Le Comité d'Audit, le Conseil d'administration et la direction effective suivent-ils de manière périodique les activités concrètes permettant l'application de cette politique de gestion des risques ?		
	Appétence au risque	2	3	L'appétence aux risques a-t-elle été clairement définie et formalisée par rapport aux objectifs ?		
			4	Existe-t-il un organigramme dans lequel les fonctions sont clairement définies ?		
			5	Le principe de séparation des fonctions incompatibles au sein de l'entité mutualiste est-il assuré pour toutes les fonctions-clés qui ont été définies comme telles par l'entité mutualiste ?		
			6	Le principe de surveillance mutuelle, notamment par la mise en œuvre de doubles signatures ou de contrôles croisés, est-il appliqué au sein de l'entité mutualiste ?		
			7	Les règles à suivre et les responsabilités des organes de gouvernance sont-elles définies dans une charte ou dans un autre document ?		
	Comité d'audit: sa composition, son rôle	3	8	La composition du comité d'audit est-elle conforme à celle définie au règlement ? C'est-à-dire qu'elle compte au moins 4 membres, dont la moitié au moins appartient au conseil d'administration de l'union nationale et n'assume aucune responsabilité dans la gestion journalière de ladite union ou de ses mutualités.		
			9	Le Comité d'audit a-t-il, via le service d'audit, la capacité d'obtenir tout renseignement ou document et de procéder à toute investigation qu'il juge nécessaire ?		
			10	Le Comité d'audit a-t-il la possibilité de prendre connaissance des rapports d'activité et du résumé des principales recommandations individuelles formulées par le service d'audit interne, ainsi que de l'état de la situation quant à la suite qui leur est donnée ?		
			11	Le Comité d'audit fait-il au moins une fois par an rapport au Conseil d'administration ?		
			12	Les modalités des rapports que le Comité d'audit doit adresser au Conseil d'administration ont-elles été clairement définies par le Conseil d'administration ?		
	Service d'audit interne, plan d'audit et méthode de travail	4	13	La fonction d'audit interne est-elle exercée par un service autonome, agissant par délégation et pour le compte de la direction effective de l'union nationale ?		
			14	L'indépendance du service d'audit interne au sein de l'organisation est-elle garantie par les dispositions de la charte d'audit ?		
			15	Le service d'audit interne se situe-t-il réellement en dehors de l'élaboration, de la mise en place et de l'exécution des mesures d'organisation et de contrôle interne ?		
			16	Le service d'audit interne a-t-il accès à tous les documents, fichiers et informations de l'entité mutualiste, en ce compris l'information en matière de gestion et les procès-verbaux des organes consultatifs et décisionnels, et ce dans la mesure requise pour l'exercice de sa mission ?		
			17	Les membres du service d'audit interne ont-ils les bonnes compétences au bon moment, par la formation permanente et/ou est-il fait, si nécessaire, appel à de l'expertise externe ?		
			18	Les missions du service d'audit font-elles l'objet de la part de ce service de l'établissement d'un plan d'audit ?		
			19	Les plans validés par le comité d'audit sont-ils respectés ?		
			20	Les documents de travail sont-ils établis selon une méthode déterminée préalablement, permettant de vérifier si la mission a été effectuée dans son intégralité, et la manière dont elle a été réalisée ?		
			21	Les documents afférents aux missions qui ont été réalisées, reflètent-ils suffisamment les contrôles effectués et étayent-ils assez les appréciations formulées au rapport d'audit ?		
			22	La mise en œuvre des plans d'audit s'appuie-t-elle sur des échantillons représentatifs de la population étudiée ?		

Environnement interne (suite)	Structure organisationnelle	5	23	La direction de l'union nationale exerce-t-elle un suivi régulier des activités, entre autre pour tout ce qui se rapporte aux éventuelles "opérations décentralisées" ?		
			24	Vu l'importante décentralisation des activités au sein du secteur mutualiste, il est essentiel que les règles de traitement administratif, comptable et informatique soient rigoureusement uniformes. Est-ce le cas ?		
			25	Vu l'importance, au sein du secteur mutualiste, de l'application des dispositions légales et réglementaires diverses (entre autres de l'INAMI et de l'Office de contrôle), l'entité mutualiste a-t-elle mis au point des procédures visant à assurer le respect desdites dispositions ?		
			26	Existe-t-il une politique de congés obligatoires pour les personnes en charge de fonctions-clés ?		
			27	La structure de protection du système d'information (sécurité physique ou logique: accès au paramétrage, initiation et modification des transactions) est-elle appropriée à la structure de l'entité mutualiste ?		
			28	Le Conseil d'administration, la Direction effective et le Comité d'audit sont-ils autonomes et compétents pour leur domaine de décision ?		
			29	La communication entre le Conseil d'administration, la Direction effective et/ou le Comité d'audit, et les auditeurs internes ou externes (fréquence, qualité) est-elle considérée comme adéquate ?		
			30	Les réunions, sujets abordés avec la Direction effective, et actions décidées par le Conseil d'administration et/ou le Comité d'audit sont-ils appropriés ? (examen des thèmes, participation à la préparation du reporting financier)		
			31	Les recommandations du Comité d'audit (y compris les recommandations internes et externes) sont-elles prises en compte et rapportée par la Direction effective ?		
	Principes d'intégrité et de valeurs éthiques	6	32	Les valeurs éthiques et principes d'intégrité ont-ils été formalisés dans un code de conduite ?		
			33	Le code de conduite a-t-il été communiqué à chaque membre du personnel ?		
			34	Le Conseil d'administration dispose-t-il d'une procédure permettant de s'assurer des compétences et de l'honorabilité des membres ?		
			35	Les dépenses des membres de la direction font-elles l'objet d'une procédure indépendante d'approbation ?*		
			36	Un comité de rémunération a-t-il été instauré ?*		
			37	La composition du comité de rémunération est-elle adéquate ?*		
			38	Le comité de rémunération fonctionne-t-il de façon indépendante ?*		
			39	Les procédures standard d'embauche, de formation, de motivation, d'évaluation, de rémunération, de transfert ou de licenciement du personnel sont-elles adaptées ?*		
	Environnement de contrôle interne	7	40	La surveillance de la Direction effective par le Conseil d'administration et le Comité d'audit est-elle adéquate ? (à savoir: absence de limitation volontaire de la communication et absence de domination excessive des organes de direction par une personne ou un nombre limité de personnes).		
			41	Les choix des principes comptables, d'estimations comptables et d'imputations sont-ils économiquement justifiés et conformes aux directives de l'OCM ?		
			42	Le management a-t-il une connaissance suffisante de l'activité, de la planification (plan stratégique, plans d'actions opérationnels, budget ...), du suivi de l'activité, et/ou de la prise de décisions ?		
			43	Le management a-t-il suffisamment de connaissances relatives au respect des obligations légales et réglementaires (prise en compte des spécificités sectorielles) ?		
Définition des objectifs	Objectifs stratégiques	8	44	Les objectifs stratégiques sont-ils clairement définis ?		
			45	Les objectifs stratégiques sont-ils liés à la mission/vision de l'union nationale ?		
			46	Les objectifs stratégiques ont-ils été communiqués à tous les niveaux de l'union nationale ?		
			47	Les objectifs stratégiques ont-ils été formalisés et approuvés ?		
			48	Les objectifs stratégiques ont-ils été intégrés dans la gestion des risques ?		
	Tolérance et appétence au risque	9	49	L'union nationale a-t-elle identifié son niveau de tolérance au risque, les indicateurs pouvant la mesurer ainsi que les variations acceptables par rapport à l'atteinte des objectifs ?		
Identification des événements	Niveau de l'identification des événements	10	50	L'inventaire des risques a-t-il été formalisé ?		
	Techniques d'identification des risques	11	51	Des gestionnaires en matière de risques ont-ils été identifiés au sein de l'union nationale ?		
			52	Ces gestionnaires en matière de risques ont-ils été formés ?		
			53	Des techniques qualitatives et quantitatives d'identification des risques sont-elles mises en œuvre ?		
			54	L'audit interne s'assure-t-il de la mise à jour de l'inventaire des risques?		

*** Ces questions ne sont pas applicables dans le cadre de l'évaluation de la Caisse des soins de santé HR Rail.**

Identification des événements	**Gestion du risque de fraude**	**12**	55	La Direction effective a-t-elle mis en place des mesures préventives pour couvrir les risques de tout type de fraude interne et externe ?		
			56	En cas de fraude, la Direction effective prend-elle des mesures correctives ?		
Evaluation des risques	**Méthodologie d'évaluation des risques**	**13**	57	L'évaluation des risques repose-t-elle sur des échelles d'évaluation de probabilité et d'impact ?		
			58	L'audit interne s'assure-t-il de la mise à jour de l'évaluation des risques ?		
	Facteurs de risque opérationnels	**14**	59	Les évolutions significatives ont-elles été prises en compte dans le cadre de l'analyse des risques (changements concernant le management, le système d'information, les prestations, les avantages, la structure en général, ...) ?		
			60	En matière de blanchiment d'argent, des politiques et procédures ont-elles été mises en place afin de limiter les risques liés à l'activité avec des ressortissants de pays tiers et/ou des pays où les pratiques sont opaques ?		
			61	Des politiques et procédures ont-elles été mises en place afin d'identifier les transactions inhabituelles ?		
	Facteurs de risque financiers et comptables	**15**	62	Des politiques et procédures ont-elles été mises en place afin de réduire les risques liés aux éventuelles difficultés de financement de l'activité (capacité à maintenir des ressources suffisantes) ?		
			63	Des politiques et procédures ont-elles été mises en place afin de réduire le risque lié au financement des frais d'administration mis à disposition par l'INAMI en application des dispositions légales ?		
Traitement des risques	**Réponses aux risques**	**16**	64	Des mesures ont-elles été prises suite aux risques identifiés dans l'inventaire des risques ?		
			65	L'audit interne s'assure-t-il des actions prises pour répondre aux risques soulevés ?		
			66	La responsabilité et la date prévue de mise en œuvre des mesures de contrôle interne planifiées sont-elles définies ?		
			67	Le risque résiduel a-t-il été réduit à un niveau acceptable dans le cadre de l'appétence aux risques définie par le Conseil d'administration, ou sinon des actions sont-elles en cours ?		
Activités de contrôle	**Activités de contrôle**	**17**	68	Le type/nature de contrôle a-t-il été intégré dans l'inventaire des risques et/ou dans les autres outils de gestion des risques s'il en existe ?		
			69	Le moment du contrôle (a priori ou a posteriori) a-t-il été intégré dans l'inventaire des risques et/ou dans les autres outils de gestion des risques s'il en existe ?		
			70	La fréquence du contrôle (a priori ou a posteriori) a-t-il été intégré dans l'inventaire des risques et/ou dans les autres outils de gestion des risques s'il en existe ?		
			71	Des manuels de procédures récents existent-ils ?		
			72	Les systèmes automatisés d'information électroniques sont-ils suffisamment fiables ?		
			73	Le système de contrôles internes est-il adaptée à la taille et la nature des activités de l'entité ?		
			74	Les politiques de développement et de modification des systèmes comptables et des contrôles comptables sont-elles adaptées ?		
Informa-tion et commu-nication	**Information et communication**	**18**	75	Les systèmes de traitement de l'information, tant automatisés que non automatisés, disposent-ils de la capacité de délivrer l'information financière et comptable, dans des délais raisonnables, aussi bien vers les utilisateurs opérationnels que vers la Direction effective ?		
			76	L'union nationale a-t-elle élaboré un plan de communication relatif à la gestion des risques ?		
Surveillance et monitoring	**Surveillance et monitoring**	**19**	77	L'union nationale dispose-t-elle d'un système de surveillance continue de ses risques dans ses activités normales d'exploitation ?		
			78	L'audit interne rapporte-t-il sur l'évaluation du fonctionnement du contrôle interne établi par la Direction effective ?		
			79	Le suivi des procédures de contrôle interne, notamment pour les activités décentralisées, est-il suffisant ?		
			80	L'audit interne fait-il l'objet d'une évaluation par le Comité d'audit, et à défaut, par le Conseil d'administration ?		
			81	La direction effective de l'union nationale évalue-t-elle au moins une fois par an le contrôle interne ?		
			82	La direction effective de l'union nationale informe-t-elle au moins une fois par an le Conseil d'administration du fonctionnement du contrôle interne ?		
			83	Les procès-verbaux, tant de la direction effective que du conseil d'administration, font-ils mention des délibérations concernant l'état du système de contrôle interne ainsi que de son évaluation ?		
			84	Les modalités des rapports que la direction effective doit adresser au Conseil d'administration ont-elles été clairement définies par le Conseil d'administration ?		

#	Questions	Informations générales
1	**Gouvernance informatique**	
1.1	Mission	
1.1.1	L'organisation dispose-t-elle d'un cadre de gouvernance informatique bien défini et documenté qui comprend des politiques, des processus et des contrôles visant à garantir que les décisions liées à l'informatique soient alignées sur la stratégie, les objectifs et l'appétence aux risques de l'entreprise ?	Un cadre de gouvernance informatique consiste en un ensemble de structures, de processus et de pratiques qui guident et contrôlent la gestion de l'informatique au sein d'une organisation. Il fournit un cadre pour la prise de décisions, la responsabilité et la gestion des risques en lien avec l'informatique. Les éléments clés généralement inclus dans un cadre de gouvernance informatique sont les suivants : 1) structure de gouvernance informatique définissant les rôles, les responsabilités et l'organisation hiérarchique pour la gouvernance informatique (par ex. comité de pilotage informatique) ; 2) politiques et procédures informatiques décrivant les attentes et les besoins de l'organisation en matière de gestion informatique, couvrant des domaines tels que la sécurité de l'information, la confidentialité des données, la gestion des actifs informatiques... ; 3) gestion des risques informatiques, qui se concentre sur l'identification, l'évaluation et la gestion des risques liés à l'informatique ; 4) mesure des performances, qui implique la définition d'indicateurs clés de performance (KPI) et de métriques pour évaluer l'efficacité et le rendement des opérations informatiques, ainsi que l'établissement de rapports à leur sujet ; 5) gestion des investissements et des ressources informatiques, qui se concentre sur la gestion efficace des investissements et des ressources informatiques, par exemple en contrôlant les budgets et les dépenses informatiques. Une charte de gouvernance informatique est un document formel qui décrit les principes, les objectifs et les responsabilités liés à la gouvernance informatique au sein d'une organisation. Il s'agit d'un document fondateur qui définit la structure, les processus et les contrôles en matière de gouvernance informatique.
1.1.2	L'organisation dispose-t-elle d'un ensemble complet de politiques et de procédures écrites relatives à la gouvernance informatique qui sont décrites dans une charte de gouvernance informatique ou un document équivalent ?	
1.1.3	L'organisation dispose-t-elle d'une matrice RACI (Responsible, Accountable, Consulted and Informed) et d'un cadre de délégation d'autorité bien définis et documentés pour les processus décisionnels et la remontée vers la hiérarchie, étayés par des organigrammes et des descriptions de postes ?	
1.2	Alignement Entreprise & Informatique	
1.2.1	Existe-t-il des mécanismes ou des processus établis pour mesurer et évaluer la satisfaction des parties prenantes à l'égard des performances de l'organisation informatique ? Il peut s'agir de méthodes telles que des enquêtes de satisfaction, des séances sur les leçons tirées à la fin d'un projet ou une participation active de l'entreprise aux groupes de travail informatiques.	Une collaboration et une communication efficaces entre les parties prenantes de l'informatique et les parties prenantes de l'entreprise sont cruciales pour un alignement réussi. Il est par conséquent recommandé d'établir des canaux de communication réguliers, de favoriser les relations et de veiller à ce que l'informatique comprenne les besoins de l'entreprise et y réponde.

1.2.2	Des processus ou des mécanismes sont-ils mis en place pour faciliter une communication et une collaboration régulières entre les parties prenantes de l'informatique (internes et externes) et la direction afin de garantir l'alignement des activités informatiques sur les objectifs et les priorités de l'entreprise ?	
1.3	Gestion de portefeuille	
1.3.1	Des processus sont-ils mis en place pour établir et maintenir l'alignement entre le portefeuille informatique et la vision de la stratégie informatique de l'organisation ? Il peut s'agir de procédures documentées pour la gestion de portefeuille, d'examens réguliers visant à garantir l'alignement et de mécanismes permettant de traiter tout écart ou changement dans la vision de la stratégie informatique.	Le portefeuille informatique d'une organisation comprend tous les projets, programmes et services informatiques, et la gestion efficace de ce portefeuille joue un rôle important dans la gouvernance informatique et la gestion efficace des ressources informatiques. Il s'agit d'identifier, de sélectionner, de prioriser et de superviser les projets et les programmes informatiques afin d'assurer leur alignement sur les objectifs stratégiques de l'organisation et de maximiser la valeur. Ceci inclut la définition de critères d'investissement, l'évaluation et la catégorisation des initiatives informatiques, la réalisation d'analyses coûts-avantages et le suivi des performances et de l'avancement des projets et des programmes.
1.3.2	Des critères clairs et cohérents ont-ils été définis pour évaluer et prioriser les investissements informatiques ? Ces critères peuvent inclure l'alignement stratégique, la viabilité financière, l'évaluation des risques, la disponibilité des ressources et les avantages potentiels.	
1.3.3	Un processus est-il mis en place pour suivre et évaluer les résultats des investissements informatiques, en tenant compte à la fois des rendements financiers (par ex. le RSI) et non financiers (par ex. l'alignement stratégique, l'efficacité opérationnelle et la satisfaction des clients) ?	
1.3.4	Un processus est-il mis en place pour suivre les performances et l'avancement des projets et programmes informatiques au sein du portefeuille ? Il s'agit notamment de suivre les indicateurs clés de performance (KPI), d'évaluer la santé des projets et de s'assurer que les initiatives fournissent les bénéfices escomptés.	
1.3.5.	Un processus est-il mis en place pour identifier et gérer les risques associés aux initiatives informatiques au sein du portefeuille ? Il s'agit d'évaluer et d'atténuer les risques afin de minimiser les impacts négatifs potentiels sur l'organisation. En outre, un processus décisionnel clair a-t-il été établi pour la sélection, l'approbation et la priorisation des investissements informatiques ? Ce dernier permet de s'assurer que les décisions soient prises sur la base de critères objectifs et en conformité avec les objectifs stratégiques de l'organisation.	
1.4	Gestion des risques informatiques	

1.4.1	L'organisation a-t-elle mis en place un cadre ou un processus formel de gestion des risques informatiques, qui permet d'identifier et d'évaluer régulièrement les risques informatiques, ainsi que de les communiquer et d'en faire état à la direction et au conseil d'administration ?	La gestion des risques informatiques est le processus consistant à identifier, évaluer et atténuer les risques associés aux systèmes, à l'infrastructure et aux opérations informatiques au sein d'une organisation. Il s'agit de comprendre les menaces et les vulnérabilités potentielles, d'évaluer leur impact potentiel sur les objectifs de l'entreprise et de mettre en place des contrôles pour gérer et réduire ces risques. Les éléments clés du processus sont l'identification, l'évaluation, l'atténuation, le suivi, la communication et le reporting des risques. En outre, établir une culture de conscience des risques au sein de l'organisation est crucial. Il s'agit de sensibiliser et de responsabiliser tous les niveaux de l'organisation à la gestion des risques informatiques, de favoriser une approche proactive de la gestion des risques et d'encourager l'amélioration continue. Enfin, la gestion des risques informatiques devrait s'aligner sur les exigences réglementaires, les normes du secteur et les cadres de gouvernance internes. Le respect de la législation et de la réglementation applicables contribue à atténuer les risques juridiques et de réputation. Globalement, la gestion des risques informatiques vise à protéger les actifs d'information de l'organisation, à préserver la confidentialité, l'intégrité et la disponibilité des données, et à assurer la continuité des opérations informatiques. Elle aide les organisations à prendre des décisions en connaissance de cause, à allouer les ressources de manière efficace et à gérer les risques de manière proactive afin d'atteindre les objectifs de l'entreprise.
1.4.2	Comment les risques informatiques sont-ils priorisés et classés en fonction de leur impact potentiel et de leur probabilité ?	
1.4.3	Des stratégies et des contrôles documentés en matière d'atténuation des risques sont-ils mis en place pour les risques informatiques identifiés ? Le cas échéant, un processus est-il mis en place pour garantir que l'acceptation des risques par la direction soit documentée et formellement approuvée ?	
1.4.4	Comment l'organisation veille-t-elle à ce que la gestion des risques informatiques soit alignée sur les exigences réglementaires et les bonnes pratiques du secteur ? Il convient de prendre en considération les nouvelles technologies émergentes, comme l'IA, l'automatisation et la robotique.	
1.4.5	Comment l'organisation gère-t-elle les risques liés aux tiers et s'assure-t-elle que les fournisseurs et les partenaires adhèrent aux pratiques appropriées de gestion des risques ?	
1.4.6	Un processus est-il mis en place pour veiller à ce que des audits informatiques soient régulièrement réalisés ?	
1.5	Politique & Conformité informatiques	
1.5.1	Des politiques et procédures informatiques sont-elles formellement définies, approuvées et documentées ? Dans l'affirmative, un processus est-il mis en place pour garantir leur révision et leur mise à jour régulières ?	La section intitulée « Politique & Conformité informatiques » se concentre sur la mise en place et le maintien de politiques et de procédures visant à garantir que les activités informatiques s'alignent sur les objectifs de l'organisation et soient conformes aux lois, à la réglementation et aux normes applicables. Cette section fournit des conseils pour l'élaboration et la mise en œuvre de politiques informatiques, la définition des rôles et des responsabilités et la mise en place de processus de contrôle et d'application de la conformité. Elle couvre également des domaines tels que la gestion des risques, la sécurité, la confidentialité et le respect de la législation et des dispositions réglementaires. L'objectif est de s'assurer que des pratiques de gouvernance et de gestion informatiques soient mises en place pour gérer efficacement les risques liés à l'informatique et garantir le respect des exigences applicables.
1.5.2	Comment les politiques informatiques sont-elles communiquées et appliquées dans l'ensemble de l'organisation ? Les employés bénéficient-ils d'une formation appropriée et de programmes de sensibilisation sur la politique et la conformité informatiques ?	
1.5.3	Comment l'efficacité de la politique informatique et des mesures en matière de conformité est-elle mesurée et évaluée ? Une personne ou une équipe est-elle chargée de superviser la politique et la conformité informatiques ? Existe-t-il un processus de contrôle et de reporting en matière de conformité informatique ?	
1.5.4	Existe-t-il un processus permettant d'assurer de manière appropriée l'identification (en temps utile) des lois, de la réglementation et des normes du secteur applicables à l'organisation (aux opérations informatiques de l'organisation) ?	
1.5.5	Des politiques et procédures documentées sont-elles mises en place pour garantir le respect de la législation et de la réglementation applicables ? Comment l'organisation évalue-t-elle et documente-t-elle sa conformité aux prescriptions légales et réglementaires spécifiques ? (par ex. DORA, NIS...)	
2	**Planification & Stratégie informatiques**	
2.1	Planification	

2.1.1	Une stratégie informatique (qui s'aligne sur les objectifs et les buts commerciaux généraux de l'organisation) a-t-elle été établie et formellement définie ? Il s'agit de définir l'orientation, la portée et les priorités des initiatives informatiques afin de soutenir les objectifs stratégiques de l'organisation.	La section Planification & Stratégie informatiques se concentre sur la définition de la stratégie informatique et la garantie qu'elle s'aligne sur les objectifs stratégiques de l'organisation, tout en établissant la gouvernance et les mesures de performance nécessaires pour contrôler et gérer efficacement les initiatives informatiques. Les principaux domaines traités dans cette section sont les suivants : 1) Établir la stratégie informatique : Il s'agit de comprendre la stratégie d'entreprise de l'organisation et de la traduire en une stratégie informatique qui contribue à la réalisation des objectifs de l'entreprise. Ceci implique de définir la vision, la mission et les objectifs en matière d'informatique. 2) Identifier des initiatives informatiques stratégiques : Il s'agit d'identifier et de prioriser les initiatives informatiques qui permettront à l'organisation d'atteindre ses objectifs stratégiques. Ceci implique d'évaluer les capacités informatiques actuelles, d'identifier les lacunes et de déterminer les initiatives informatiques nécessaires pour combler ces lacunes. 3) Définir des mesures de performance informatique : Il s'agit de définir des mesures et des objectifs de performance pour contrôler l'efficacité et le rendement des initiatives informatiques. Ceci implique d'établir des indicateurs clés de performance (KPI) qui s'alignent sur les objectifs stratégiques de l'organisation.
2.1.2	Les rôles et les responsabilités relatifs à la stratégie et à la gouvernance informatiques sont-ils formellement définis ?	
2.1.3	Des processus sont-ils mis en place pour vérifier si la stratégie et la planification informatiques sont respectées et si les objectifs prédéfinis sont atteints ?	
2.2	Sourcing stratégique / gestion des risques liés aux tiers	
2.2.1	Comment les fournisseurs tiers sont-ils identifiés et évalués au niveau des risques informatiques ? Des critères permettant de déterminer le niveau de risque informatique d'un fournisseur/d'un tiers ont-ils été définis ?	La gestion des risques informatiques liés aux tiers est essentielle pour les organisations afin de protéger les données sensibles, de maintenir le respect des dispositions réglementaires, de sauvegarder leur réputation, d'assurer la continuité de l'activité et de mettre en place des pratiques de gestion des fournisseurs efficaces. En gérant de manière proactive les risques liés aux tiers, les organisations peuvent atténuer les menaces et les vulnérabilités potentielles associées à leurs partenariats externes.
2.2.2	Quelle est la diligence appropriée (par ex. vérifications des antécédents, évaluations de la stabilité financière...) exercée avant de collaborer avec un fournisseur tiers ?	
2.2.3	Comment les contrats et les accords de niveau de service (ANS) sont-ils établis avec les fournisseurs tiers ? Comment est-il veillé à ce que les exigences appropriées en matière de sécurité, de confidentialité, de protection des données et/ou de réponse aux incidents soient incluses dans les accords ?	
2.2.4	Comment le contrôle et la supervision constants des fournisseurs tiers sont-ils effectués (tout au long de la relation) ? Quelles sont la fréquence et l'étendue des activités de contrôle, telles que (par exemple) les évaluations de sécurité, les analyses des vulnérabilités ou les évaluations de performance ?	
2.2.5	Comment la résiliation ou la stratégie de sortie est-elle gérée avec les fournisseurs tiers ? Des processus sont-ils mis en place pour garantir, par exemple, l'existence de plans d'urgence, de processus de récupération des données ou la suppression des droits d'accès en cas de résiliation ?	
2.3	Organisation informatique	
2.3.1	Un processus est-il mis en place pour s'assurer que la direction de l'organisation « donne le ton » et s'engage dans la gouvernance et la sécurité informatiques, par exemple en promouvant une culture de la conformité et en soutenant activement les initiatives informatiques ?	La culture informatique au sein d'une organisation fait référence aux croyances, valeurs, attitudes, comportements et normes collectifs qui façonnent l'approche qu'a l'organisation en matière de technologie et de son utilisation. Elle englobe l'état d'esprit et les comportements des individus au sein de l'organisation à l'égard des activités liées à l'informatique, telles que la gouvernance informatique, la sécurité, l'innovation, la collaboration et l'amélioration
2.3.2	Comment est-il veillé à ce que la culture informatique soit en adéquation avec les attentes de la direction ?	

		l'informatique, telles que la gouvernance informatique, la sécurité, l'innovation, la collaboration et l'amélioration continue.
2.3.3	Des processus sont-ils mis en place pour permettre une culture informatique positive, favorisant un environnement dans lequel les employés sont en mesure d'explorer les nouvelles technologies et où un esprit ouvert à l'apprentissage est encouragé ?	La culture informatique au sein d'une organisation joue un rôle crucial dans la manière dont la technologie est perçue, exploitée et gérée. Elle influence la manière dont les employés interagissent avec les systèmes informatiques, dont ils priorisent les initiatives informatiques et dont ils abordent les risques et les défis liés à l'informatique. Une culture informatique positive favorise un environnement dans lequel la technologie est adoptée, mise à profit de manière efficace et alignée sur les buts et objectifs de l'organisation.
2.3.4	Des processus sont-ils mis en place pour aider les employés à adopter les changements technologiques et à s'y adapter, facilitant ainsi la mise en œuvre réussie des initiatives informatiques et des efforts de transformation numérique ?	
2.4	Gestion d'actifs	
2.4.1	**Matériel** Un inventaire détaillé des actifs de l'entreprise a-t-il été établi et maintenu ? Un processus est-il mis en place pour garantir que l'inventaire reste à jour ? L'inventaire fait-il l'objet d'une révision régulière (annuelle par exemple) ? Cet inventaire devrait inclure tous les actifs de l'entreprise ayant le potentiel de stocker ou de traiter des données, y compris les appareils des utilisateurs finaux (appareils portables et mobiles compris), les éléments du réseau et les serveurs.	**Matériel** Gérer activement (inventorier, suivre et corriger) tous les actifs de l'entreprise (appareils des utilisateurs finaux, y compris portables et mobiles ; éléments du réseau ; appareils non informatiques/Internet des objets (IDO) ; et serveurs) connectés à l'infrastructure physiquement, virtuellement, à distance, et ceux qui se trouvent dans des environnements cloud, afin de connaître précisément l'ensemble des actifs qui doivent être contrôlés et protégés au sein de l'entreprise. Cela permettra également d'identifier les actifs non autorisés et non gérés à supprimer ou à restaurer.
2.4.2	**Matériel** Un processus est-il mis en place pour traiter les actifs non autorisés ? L'organisation peut choisir de supprimer l'actif du réseau, d'empêcher l'actif de se connecter à distance au réseau ou de mettre l'actif en quarantaine.	
2.4.3	**Logiciel** Un inventaire détaillé des logiciels a-t-il été établi et maintenu ? Existe-t-il un processus garantissant que l'inventaire reste à jour ? L'inventaire fait-il l'objet d'une révision régulière (annuelle par exemple) ? Cet inventaire devrait inclure tous les logiciels sous licence installés sur des actifs de l'entreprise.	**Logiciel** Gérer activement (inventorier, suivre et corriger) tous les logiciels (systèmes d'exploitation et applications) sur le réseau, afin que seuls les logiciels autorisés soient installés et puissent être exécutés, et que les logiciels non autorisés et non gérés soient détectés et que leur installation et leur exécution soient empêchées.
2.4.4	**Logiciel** Un processus est-il mis en place pour garantir que tous les logiciels autorisés soient actuellement supportés ? Un processus est-il mis en place pour les exceptions, par exemple pour des raisons commerciales ?	
2.4.5	**Logiciel** Un processus est-il mis en place pour traiter les logiciels non autorisés (par ex. suppression, exception documentée...) ?	
2.4.6	Existe-t-il une CMDB centrale pour gérer les actifs et ressources critiques ? Les ressources/actifs clés ainsi que leurs relations sont-ils bien documentés, y compris les informations de configuration (modèle logique des services, actifs, infrastructure et enregistrement des articles de configuration (CI), ainsi que leurs relations) ?	Une Configuration Management Database (CMDB) à jour est importante car elle fournit un répertoire centralisé d'informations sur les actifs informatiques d'une organisation, leurs relations et leurs configurations. Elle permet une gestion efficace des services informatiques, une gestion précise des changements et une meilleure prise de décision en fournissant une compréhension complète de l'infrastructure informatique et de ses dépendances.
2.4.7	Existe-t-il des procédures pour s'assurer que la CMDB soit mise à jour en temps utile ?	

2.5	Finance, budget, métriques & contrôles	
2.5.1	Un processus est-il mis en place pour s'assurer que le budget informatique soit aligné sur les objectifs stratégiques de l'organisation ? Comment est-il évalué si ce budget reflète les priorités et les buts de l'organisation, et s'il soutient la mise en œuvre d'initiatives informatiques contribuant à atteindre ces objectifs ?	La gestion des finances informatiques est importante parce qu'elle permet à l'organisation d'optimiser l'allocation des ressources financières, de prendre des décisions en connaissance de cause et de maximiser la valeur dérivée des investissements informatiques.
2.5.2	Comment le processus de planification et d'allocation du budget informatique est-il mené ? Des critères sont-ils définis pour prioriser des fonds et les allouer à différentes initiatives informatiques ? Ce processus de planification tient-il compte de facteurs tels que la gestion des risques, l'optimisation des coûts et le retour sur investissement ?	
2.5.3	Un processus est-il mis en place pour suivre et contrôler le budget informatique ? Un processus est-il également mis en place pour garantir un reporting régulier sur les performances budgétaires en matière d'informatique ?	
3	**Processus, services et actifs informatiques**	
3.1	Architecture	
3.1.1	Existe-t-il des diagrammes architecturaux clairs et à jour de l'environnement informatique ? Sont-ils facilement accessibles et effectivement communiqués aux parties prenantes concernées (par ex. les équipes informatiques, les utilisateurs finaux...) ?	Il est crucial de comprendre l'alignement entre l'architecture informatique et les objectifs de l'entreprise et de veiller à ce qu'une vue d'ensemble actualisée de l'architecture soit disponible en permanence. De plus, l'organisation doit veiller à ce que l'architecture informatique soit évolutive et flexible en évaluant des facteurs tels que les performances du système, la planification des capacités, les capacités d'intégration et la faculté d'adaptation aux technologies émergentes.
3.1.2	Comment est-il veillé à ce que l'architecture informatique puisse s'adapter à une future croissance, à des avancées technologiques ou à une évolution des besoins de l'entreprise ?	
3.2	Gestion de programmes	
3.2.1	Une approche structurée est-elle mise en place, comme un processus de gestion de portefeuilles de projets, pour évaluer et prioriser les projets et programmes informatiques sur la base de leur alignement sur les objectifs de l'entreprise, les buts stratégiques et les ressources disponibles ?	La gestion des programmes informatiques est cruciale pour les organisations puisqu'elle garantit la bonne exécution de projets et de programmes informatiques alignés sur les objectifs de l'entreprise. Elle fournit une approche structurée pour sélectionner, prioriser, planifier et réaliser des initiatives, en optimisant l'allocation des ressources et en minimisant les risques. Une gestion efficace des programmes informatiques permet aux organisations d'atteindre les résultats escomptés, de maximiser la valeur et de s'adapter à l'évolution des paysages technologiques, pour finalement générer la croissance et la réussite de l'entreprise.
3.2.2	Des méthodologies de gestion de projets, comme Waterfall ou Agile, sont-elles mises en place ? Dans l'affirmative, comment est-il veillé à ce qu'elles soient respectées ?	
3.2.3	Des mécanismes permettant de suivre et de contrôler les coûts des projets, comme la budgétisation, le reporting financier et les analyses coûts-avantages, sont-ils mis en place ?	
3.2.4	Les résultats et les bénéfices des projets sont-ils mesurés pour évaluer la réussite et la valeur apportées par les initiatives informatiques ?	

3.3	Gestion des changements	
3.3.1	Un processus de gestion des changements a-t-il été formellement défini, en décrivant par exemple comment les changements sont demandés, examinés et approuvés avant leur conception ?	La gestion des changements informatiques est d'une importance capitale pour les organisations, puisqu'elle fournit une approche structurée et contrôlée pour la mise en œuvre de changements apportés aux systèmes et à l'infrastructure informatiques. Elle permet de minimiser les risques associés aux changements, en veillant à ce qu'ils soient correctement évalués, autorisés et communiqués. Une gestion efficace des changements réduit la probabilité d'interruptions de service, de violations de données et d'autres impact négatifs sur les opérations de l'entreprise. Elle contribue également à maintenir la stabilité et la fiabilité des services informatiques, en veillant à ce qu'ils répondent aux besoins de l'organisation et de ses parties prenantes. En mettant en œuvre des processus de gestion des changements, les organisations peuvent s'adapter à l'évolution des paysages technologiques, améliorer leur efficacité opérationnelle et accroître la satisfaction des clients.
3.3.2	Les rôles et les responsabilités en ce qui concerne les différentes phases du processus de gestion des changements ont-ils été définis (par ex. organe consultatif en matière de changements), ainsi que des critères clairs pour l'approbation d'un changement (avant sa mise en œuvre) ?	
3.3.3	Comment est-il veillé à ce que les exigences de l'entreprise soient incorporées durant la phase de conception d'un changement ?	
3.3.4	Existe-t-il différents environnements (pour les systèmes clés, par ex. DEV, ACC & PRD) pour permettre un développement, une acceptation et un déploiement appropriés et sécurisés des changements ?	
3.3.5	Un processus est-il mis en place pour gérer les changements non autorisés (urgence) ? *Note : Cette question vise essentiellement à déterminer les mécanismes mis en place par l'organisation pour incorporer et documenter les changements apportés en situation d'urgence, en veillant à ce qu'ils soient correctement examinés et approuvés rétrospectivement.*	
3.4	Gestion des services des tiers (s'il y a lieu)	
3.4.1	Existe-t-il un inventaire de tous les prestataires tiers de services informatiques ? Comment veillez-vous à ce que la liste soit à jour ?	La gestion des risques liés aux tiers (TPRM) fait référence au processus d'identification, d'évaluation, de suivi et d'atténuation des risques potentiels associés aux relations d'une organisation avec des tiers externes, comme des vendeurs, des fournisseurs, des sous-traitants et des partenaires, tout au long du cycle de vie. La gestion des risques liés aux tiers implique une évaluation des menaces et vulnérabilités potentielles que ces tiers peuvent présenter pour la conformité d'une organisation à la réglementation, la réputation, les opérations, la stabilité financière, la sécurité des données et d'autres aspects. L'objectif de la gestion des risques liés aux tiers est de minimiser la probabilité et l'impact de ces risques en mettant en œuvre des contrôles, politiques et procédures appropriés pour gérer efficacement les relations avec les tiers.
3.4.2	Un catalogue de services est-il défini pour décrire les services fournis par les prestataires de services informatiques pour aider l'organisation ?	
3.4.3	Existe-t-il un catalogue de services formel convenu avec l'organisation ?	
3.4.4	Des critères (ANS) sont-ils définis pour évaluer les performances et les services fournis par la partie tierce ?	
3.4.5	Les critères de performance sont-ils mesurés (KPI) ?	
3.4.6	Une procédure formelle définissant les mesures prises dans le cas où les KPI ne sont pas remplis est-elle définie ?	
3.4.7	Des réunions régulières et formelles avec l'organisation des services sont-elles prévues ?	
3.5	Gestion des incidents et des problèmes	
3.5.1	Existe-t-il un outil dédié pour enregistrer et répertorier les incidents ? Différents niveaux d'impact des incidents sont-ils définis et clairement communiqués aux équipes ?	La gestion des problèmes est une pratique centrée sur la prévention des incidents ou la réduction de leur impact. La gestion des incidents se concentre sur le traitement des incidents en temps réel.
3.5.2	Existe-t-il une équipe dédiée qui prend en charge les défaillances de service (gestion des incidents) au sein de l'équipe informatique (par ex. helpdesk) ?	

3.5.3	Une politique formelle de gestion des incidents est-elle définie ? Des KPI formels sont-ils définis en termes d'objectifs de résolution d'incidents ?	Lorsqu'une stratégie de gestion des incidents est mise en place, vous êtes en mesure de détecter une menace, de déterminer son impact potentiel et d'activer les processus adéquats pour la contenir. Chaque domaine au sein de votre organisation devrait appliquer le même seuil et le même processus pour la remontée vers la hiérarchie, afin que chaque incident se voie accorder un poids égal et cohérent dans votre réponse.
3.5.4	Une procédure formelle de gestion des problèmes est-elle définie pour veiller à ce que les causes profondes des incidents soient analysées afin d'éviter qu'ils ne se reproduisent ?	
3.5.5	Un processus de reporting formel est-il défini pour signaler les incidents majeurs à la direction ?	
4	**Sécurité de l'information et cybersécurité**	
4.1	Sécurité informatique	
4.1.1	L'organisation a-t-elle mis en œuvre un environnement de contrôle informatique et l'a-t-elle aligné sur les bonnes pratiques reconnues, comme la norme ISO 27001 en matière de gestion de la sécurité de l'information ou le cadre de cybersécurité du NIST (NIST CSF) ? Dans l'affirmative, comment l'alignement ou la conformité est-il/elle garanti(e) (par ex. via des audits internes) ?	La gouvernance de la sécurité de l'information est cruciale parce qu'elle établit le cadre et la responsabilité en matière de gestion et de protection des actifs d'information d'une organisation. Elle garantit que la sécurité de l'information soit alignée sur les objectifs de l'entreprise, que les risques soient gérés de manière appropriée et que les contrôles et processus nécessaires soient mis en place pour protéger les données sensibles et atténuer les menaces potentielles.
4.1.2	L'organisation a-t-elle mis en place un cadre de gouvernance de la sécurité de l'information qui définit les rôles, les responsabilités et l'obligation de rendre compte en matière de gestion de la sécurité de l'information ?	
4.1.3	Des politiques et procédures documentées en matière de sécurité de l'information sont-elles mises en place pour traiter des domaines clés tels que le contrôle d'accès, la classification des données, la réponse aux incidents et la confidentialité des données ?	
4.1.4	Comment l'organisation identifie-t-elle et évalue-t-elle les risques en matière de sécurité de l'information et de cybersécurité ? Un processus formel d'évaluation des risques est-il mis en place, et les risques sont-ils régulièrement évalués et mis à jour ?	
4.1.5	L'organisation a-t-elle mis en œuvre des processus de sensibilisation à la sécurité de l'information pour veiller à ce que les membres du personnel soient correctement informés et formés en ce qui concerne leurs responsabilités en matière de sécurité de l'information ?	
4.1.6	Votre organisation utilise-t-elle une technologie opérationnelle (TO) ? Dans l'affirmative, les mêmes mesures (concernant la gouvernance de la sécurité, les risques de sécurité, etc. - en référence aux précédentes questions du point 4.1) que celles mises en œuvre dans le domaine des technologies de l'information ont-elles été implémentées ?	
4.2	Gestion des identités et des accès	
4.2.1	Comment l'organisation gère-t-elle l'accès des utilisateurs aux systèmes et aux données ? Des contrôles sont-ils mis en place pour garantir un provisionnement adéquat des utilisateurs, des examens des accès et la séparation des tâches ?	

4.2.2	Un inventaire des comptes a-t-il été établi et maintenu ? L'inventaire doit contenir (au minimum) les informations suivantes : nom de la personne, nom d'utilisateur, dates de début/de fin et département. De plus, un exercice visant à vérifier si tous les comptes sont autorisés est-il régulièrement réalisé (par ex. trimestriellement pour les comptes administrateur) ?	Une gestion adéquate des identités et des accès (IAM) permet de veiller à ce que les bonnes personnes aient un accès approprié aux bonnes ressources et au bon moment. Elle aide à protéger les données sensibles, à empêcher les accès non autorisés, à rationaliser les processus de provisionnement et de déprovisionnement des utilisateurs et à maintenir la conformité aux exigences réglementaires.
4.2.3	Quels mécanismes (par ex. authentification multifacteurs, authentification unique) ou quelles mesures de sécurité (par ex. paramètres de mot de passe complexes) ont été mis en œuvre pour limiter l'authentification non autorisée ?	
4.2.4	Quelles mesures de contrôle avez-vous mises en place pour - veiller à ce que les privilèges des administrateurs soient limités aux comptes admin dédiés, et si possible, limités dans le temps ? - détecter et désactiver les comptes dormants ? - garantir une séparation adéquate des tâches ? - limiter le nombre de comptes génériques ? - restreindre de manière appropriée les comptes tiers/fournisseurs ?	
4.3	Gestion des données	
4.3.1	Un processus de gestion des données a-t-il été établi et maintenu ? Ce processus devrait traiter le caractère sensible et la propriété des données, ainsi que le traitement des données, les limites en matière de conservation des données et les exigences en matière d'élimination. De plus, comment est-il veillé à ce que les prescriptions légales (par ex. RGPD) soient respectées lorsqu'elles sont applicables ?	Une gestion des données adéquate implique de garantir l'intégrité, la disponibilité et l'accessibilité des données, pour permettre une prise de décisions en connaissance de cause, des opérations efficaces et une conformité à la réglementation en matière de confidentialité de données.
4.3.2	Un inventaire des données a-t-il été établi et maintenu ? Les données sensibles, critiques ou à caractère personnel devraient au minimum être inventoriées.	
4.3.3	Des mesures de contrôle ont-elles été mises en œuvre pour garantir le chiffrement des données sur les appareils des utilisateurs finaux, ainsi que sur les supports amovibles ?	
4.4	Gestion de la sécurité du réseau et de l'infrastructure	
4.4.1	Un processus de configuration de la sécurité pour les actifs de l'entreprise (par ex. appareils des utilisateurs finaux), les logiciels (par ex. systèmes d'exploitation, applications) ainsi que l'infrastructure de réseau (par ex. routeurs) a-t-il été établi et maintenu ? Ce processus inclut-il la gestion des comptes par défaut (par ex. racine, admin) sur les actifs et les logiciels de l'entreprise, ainsi que la désactivation des services inutiles sur les actifs et logiciels de l'entreprise ?	La gestion de la sécurité du réseau et de l'infrastructure consiste à protéger le réseau et l'infrastructure informatique de l'organisation contre les accès non autorisés, les violations et les menaces potentielles. Elle garantit la confidentialité, l'intégrité et la disponibilité des systèmes et données critiques, en protégeant contre les cyberattaques et en minimisant le risque de perturbations opérationnelles.
4.4.2	Quelles mesures de contrôle ont été déployées pour protéger le réseau contre les menaces externes (par ex. VPN, pare-feux sur les serveurs ou les appareils des utilisateurs finaux) ?	

		le risque de perturbations opérationnelles.
4.4.3	Quelles mesures de contrôle ont été mises en œuvre pour protéger les logiciels et l'infrastructure des logiciels malveillants (par ex. malware) ? Cela comprend-il des protections pour les emails et les navigateurs ?	
4.4.4	Un processus de gestion des vulnérabilités a-t-il été établi et maintenu ? Ce processus inclut-il - des scans réguliers des vulnérabilités ; - un processus de correction pour les vulnérabilités identifiées ; et - un processus de gestion des patchs pour les systèmes d'exploitation et les applications, si possible automatisé ?	
4.5	Gestion des incidents (en matière de sécurité)	
4.5.1	Un processus de réponse aux incidents a-t-il été établi et maintenu ? Ce processus prévoit-il des rôles et des responsabilités, des exigences de conformité et un plan de communication ?	La gestion des incidents est cruciale puisqu'elle permet aux organisations de répondre efficacement aux incidents de sécurité et de les atténuer, minimisant ainsi l'impact sur les opérations et réduisant le dommage potentiel. Elle garantit une approche structurée et coordonnée de la gestion des incidents, en facilitant la détection à temps, le confinement, l'examen et la restauration pour maintenir la continuité de l'activité et protéger les informations sensibles.
4.5.2	Quelles mesures de contrôle ont été mises en œuvre pour identifier et détecter les événements susceptibles de compromettre la sécurité [par ex. Centre des opérations de sécurité (OC)] ?	
4.5.3	Quelles mesures de contrôle supplémentaires ont été mises en œuvre pour garantir une gestion adéquate des incidents (par ex. évaluations post-incident, mécanismes pour la communication durant les incidents, exercices de réponse aux incidents...) ?	
4.6	Continuité de l'activité	
4.6.1	Un plan formel de continuité de l'activité et un plan de reprise des activités ont-ils été définis ?	En cas de perturbations importantes des activités habituelles, généralement causées par un incident ou une panne grave, la capacité à rétablir la distribution de ce qui compte le plus protège nos entreprises contre des dommages inacceptables en termes financiers et en termes de réputation. Une stratégie intégrée de continuité de l'activité permet de garder vos fonctions critiques opérationnelles et contribue à établir une culture de la résilience.
4.6.2	Le plan de continuité de l'activité (PCA) et le plan de reprise des activités (PRA) sont-ils périodiquement testés ?	
4.6.3	Les résultats du PCA et du PRA sont-ils formellement communiqués à la direction ?	
4.6.4	Un plan d'action formel basé sur les résultats des tests du PCA et du PRA est-il défini ?	