
Projet TER :

Manuel d'utilisation de l'outil

Groupe :
Rim AMSAF
Imane KOUHHIZ Ahmed
Taha EL ABIAD
Mahamoud ROUKEH Abdi
Zakaria HANAI

Encadrante :
Mme DJOUDI Chahinda

*Parcours : Master 1 Fiabilité et sécurité
informatique*

Table des matières

1.	Introduction à l'outil d'évaluation.....	3
1.1	Objectif général.....	3
1.2	Débuter avec l'outil : choisir un référentiel	3
1.3	Présentation de la feuille d'évaluation :	3
2.	Echelles :.....	5
2.1	Échelle de maturité (CIS Controls & ANSSI)	6
2.2	Échelle de conformité (DORA)	6
3.	Dashboard	7
3.1	Dashboard CIS	7
3.2	Dashboard ANSSI	9
3.3	Dashboard DORA	10
4.	Conseils de bonnes pratiques.....	11

1. Introduction à l'outil d'évaluation

1.1 Objectif général

L'outil développé dans le cadre de ce projet permet d'évaluer le niveau de maturité en cybersécurité d'un organisme, en s'appuyant sur trois référentiels reconnus :

- ✓ Le guide d'hygiène informatique de l'ANSSI
- ✓ Les CIS Critical Security Controls
- ✓ Le cadre réglementaire européen DORA

Chaque référentiel est intégré de manière autonome dans le fichier Excel, permettant à l'auditeur de choisir celui qui correspond le mieux à son contexte ou à ses besoins spécifiques.

1.2 Débuter avec l'outil : choisir un référentiel

Dès l'ouverture du fichier, l'auditeur est invité à sélectionner le référentiel avec lequel il souhaite travailler.

Le choix du référentiel conditionne les questions à remplir et les résultats qui seront affichés dans le tableau de bord correspondant.

Guide d'hygiène de l'ANSSI | CIS Critical Security Controls | DORA

1.3 Présentation de la feuille d'évaluation :

Une fois le référentiel choisi, l'utilisateur accède à une feuille contenant un tableau à compléter.

Chaque référentiel présente les informations différemment, mais le principe reste le même : indiquer le niveau de maturité atteint pour chaque exigence.

Voici comment se présente la feuille d'évaluation pour chaque référentiel :

○ CIS Critical Security Controls :

L'onglet dédié au référentiel **CIS Controls** permet d'évaluer chaque sous-contrôle à partir d'un tableau unique. Ce tableau regroupe toutes les informations nécessaires, qu'elles soient informatives ou à remplir par l'utilisateur.

Contrôle CIS	ID	Sous-Contrôle CIS	Détail du contrôle CIS	Type d'actif	Fonction sécurité	Référence de base	Groupe de mise en œuvre
I. Inventaire et contrôle des actifs de l'entreprise	1	Établir et maintenir un inventaire détaillé des actifs de l'entreprise	Il faut établir et maintenir à jour un inventaire complet de tous les actifs capables de stocker ou traiter des données (appareils, réseaux, IoT, serveurs, cloud). Chaque actif doit être identifié avec des informations précises (adresse réseau, MAC, nom, propriétaire, service, autorisation réseau). Les outils MDM peuvent aider à gérer les appareils mobiles. L'inventaire doit être mis à jour au moins deux fois par an.	Équipements	Identifier	Système d'inventaire et de découverte des actifs	IG1
	2	Gérer les actifs non autorisés	Mettre en place un processus hebdomadaire pour détecter et gérer les actifs non autorisés, en les supprimant, en bloquant leur accès réseau ou en les plaçant en quarantaine.	Équipements	Protéger	Système d'inventaire et de découverte des actifs	IG1
	3	Utiliser un outil de découverte active	Utiliser un outil de découverte active pour identifier les actifs connectés au réseau de l'entreprise. Configurer cet outil de découverte active pour qu'il s'exécute quotidiennement, ou plus fréquemment.	Équipements	Déetecter	Système d'inventaire et de découverte des actifs	IG2

- **Sous-contrôle / ID** : identifie précisément la mesure de sécurité à évaluer.
- **Détail** : description complète du sous-contrôle pour comprendre son objectif.
- **Type d'actif** : indique les ressources concernées (ex. : poste utilisateur, serveur, etc.).
- **Fonction de sécurité** : associe le contrôle à une fonction (prévention, détection, réponse...).
- **Référence** : indique le **programme ou le domaine de sécurité** auquel le sous-contrôle est rattaché (ex. : gestion des incidents, sécurité physique, gestion des audits, etc.).
- **Groupe IG** : indique si le contrôle s'applique à IG1, IG2 ou IG3, en fonction du niveau de complexité de l'organisation.

Ces colonnes **ne sont pas à modifier** : elles servent de support à l'évaluation.

IG1	IG2	IG3	Niveau de maturité	Libellé	Description	Commentaire	Axe de sécurité
X	X	X	2	Pratique informelles	L'entreprise commence à suivre une logique commune, avec des habitudes partagées issues de l'expérience. Cependant, ces pratiques restent non formalisées, et reposent sur la transmission orale ou l'usage répété plutôt que sur des procédures écrites.		Gestion_des_accès
X	X	X	2	Pratique informelles	L'entreprise commence à suivre une logique commune, avec des habitudes partagées issues de l'expérience. Cependant, ces pratiques restent non formalisées, et reposent sur la transmission orale ou l'usage répété plutôt que sur des procédures écrites.		Sensibilisation

- IG1 / IG2 / IG3** : indique à quel(s) groupe(s) de mise en œuvre s'applique le sous-contrôle
- Niveau de maturité** : à renseigner (valeurs de 1 à 5 ou "N/A").
- Libellé / Description** : ces colonnes se remplissent automatiquement selon le niveau choisi
- Commentaire** : libre à l'auditeur pour justifier sa réponse
- Axe de sécurité** : indique le domaine auquel appartient le sous-contrôle (ex. : gestion des accès, protection des données, sensibilisation).

Plan d'action	Responsable plan d'action	Priorité	Deadline	Livrables
Revoir périodiquement les droits des utilisateurs	Responsable IT / Gestionnaire des actifs	moyenne		
Revoir périodiquement les droits des utilisateurs	Responsable IT / Gestionnaire des actifs	HAUTE		

- Plan d'action** : optionnel, permet de prévoir une amélioration si nécessaire
- Responsable / Priorité / Deadline / Livrables** : aide au pilotage des actions dans le temps

Conseil : il est recommandé de parcourir l'ensemble des sous-contrôles et de compléter les champs requis ligne par ligne.

Ce tableau constitue la base de calcul automatique du tableau de bord CIS.

○ Guide d'hygiène de l'ANSSI :

L'onglet « Guide d'hygiène de l'ANSSI » propose un tableau basé sur les règles de bonne pratique du guide d'hygiène informatique de l'ANSSI.

Chaque ligne correspond à une règle à évaluer en termes de maturité.

Chapitre	N°	Règle de bonne pratique ANSSI	Description de la règle de bonne pratique	Niveau de maturité	Libellé	
I - Connaitre le système d'information	1	Former les équipes opérationnelles à la sécurité des systèmes d'informations	Les équipes techniques (administrateurs, développeurs, R&D, etc.) doivent être formées régulièrement à la sécurité informatique selon leurs missions (authentification, durcissement, fonctionnement...). Ces formations doivent être adaptées au métier de chacun et intégrées aux contrats des prestataires.	NA	Non applicable	Ce contrôle
	2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique	Tous les utilisateurs doivent être sensibilisés aux règles et comportements à adopter pour assurer leur sécurité (utilisation de mots de passe complexes, équipements personnels, vigilance...). Cette sensibilisation, à renouveler régulièrement, peut être renforcée par une charte informatique signée par tous les utilisateurs.	1	Non structuré	Aucune ou peu de pratiques
	3	Maîtriser les risques de l'infogérance	Avant d'externaliser tout ou partie du système d'information, il est essentiel d'évaluer les risques liés à l'infogérance et d'imposer des exigences de sécurité claires aux prestataires (réversibilité, audits, sauvegardes...). Ces engagements doivent être formalisés dans un plan d'assurance sécurité.	2	Pratique informelles	L'entreprise n'a pas de pratiques

Signification du niveau de maturité	Commentaires
Ce contrôle ou processus n'est pas concerné ou ne peut être évalué dans le contexte actuel.	
Aucune méthode claire n'est définie. Les actions reposent uniquement sur le savoir-faire individuel, sans cadre ou standard partagé. Le succès dépend donc de chaque personne, sans véritable suivi ni cohérence.	
L'entreprise commence à suivre une logique commune, avec des habitudes partagées issues de l'expérience. Cependant, ces pratiques restent non formalisées, et reposent sur la transmission orale ou l'usage répété plutôt que sur des procédures écrites.	

- **Chapitre / N° / Règle** : identifient la bonne pratique à évaluer.
- **Description** : donne le détail et le contexte de la règle.
- **Niveau de maturité** : à remplir par l'auditeur : les valeurs vont de **1 à 5**, ou **N/A** si la règle ne s'applique pas.
La sélection remplit automatiquement les colonnes **Libellé** et **Signification**.
- **Commentaires (facultatif)** : champ libre pour justifier ou contextualiser la note.

○ DORA :

L'onglet DORA repose sur les exigences du règlement européen sur la résilience opérationnelle numérique (DORA).

Chaque ligne correspond à une exigence issue du texte officiel, à évaluer sur plusieurs dimensions.

Chapitre	Article	Identifiant de l'exigence	Exigence	Politique définie	Contrôle mis en œuvre	Contrôle automatisé	Contrôle remonté à la direction	Conformité	Description
Chapitre II : Gestion des risques liés aux TIC	Article 5 : Gouvernance et organisation	4	1.Les entités financières doivent mettre en place un cadre interne de gouvernance et de contrôle garantissant une gestion efficace et prudente des risques liés aux TIC, conformément à l'article 6, paragraphe 4, afin d'atteindre un niveau élevé de résilience opérationnelle numérique.	100%	100%	100%	100%	Entièrement conforme	Toutes les dimensions du contrôle sont pleinement satisfaites. La politique est formalisée, le contrôle est mis en œuvre, automatisé (ou techniquement imposé), et suivi au niveau de la direction.
Chapitre II : Gestion des risques liés aux TIC	Article 5 : Gouvernance et organisation	5	2.L'organe de direction de l'entité financière définit, approuve, supervise et est responsable de la mise en œuvre de l'ensemble des dispositifs liés au cadre de gestion des risques liés aux TIC mentionné à l'article 6, paragraphe 1.	50%	25%	50%	100%	Partiellement conforme	Une partie seulement des éléments du contrôle est en place. Par exemple, la politique est définie et le contrôle est appliqué, mais il n'est ni automatisé ni suivi par la direction.

- **Chapitre / Article / Identifiant** : référence réglementaire de l'exigence à évaluer.
- **Exigence** : contenu de l'obligation imposée par DORA.
- **Politique définie / Contrôle mis en œuvre / Automatisation / Suivi par la direction** : à évaluer en pourcentage (0 %, 25 %, 50 %, 100 %).
- **Conformité** : synthèse générée automatiquement (ex. : "Entièrement conforme", "Partiellement conforme" ...).
- **Description** : précisions sur l'interprétation du niveau de conformité atteint.

Le remplissage se fait sur plusieurs axes pour refléter le niveau de maturité globale de l'organisation face à l'exigence.

2. Echelles :

L'outil utilise deux types d'échelles pour évaluer le niveau de sécurité de l'organisme :

- Une **échelle de maturité** (utilisée dans les référentiels CIS Controls et ANSSI), (visible dans l'onglet "Echelles" du fichier Excel)



- Une **échelle de conformité** (utilisée pour le référentiel DORA), (visible dans l'onglet "Echelles_DORA" du fichier Excel)



2.1 Échelle de maturité (CIS Controls & ANSSI)

Chaque exigence ou sous-contrôle est évalué sur une échelle de 1 à 5, ou "N/A" si elle ne s'applique pas.

Niveau de maturité	Libellé	Description	Groupe de mise en œuvre	Signification
1	Non structuré	Aucune méthode claire n'est définie. Les actions reposent uniquement sur le savoir-faire individuel, sans cadre ou standard partagé. Le succès dépend donc de chaque personne, sans véritable suivi ni cohérence.	IG1	Ce groupe s'applique aux organisations ayant peu de ressources et un niveau de risque faible. Elles doivent mettre en œuvre les contrôles de base, qui sont essentiels pour assurer un minimum de sécurité.
2	Pratiques informelles	L'entreprise commence à suivre une logique commune, avec des habitudes partagées issues de l'expérience. Cependant, ces pratiques restent non formalisées, et reposent sur la transmission orale ou l'usage répété plutôt que sur des procédures écrites.	IG2	Ce groupe concerne les structures de taille moyenne, avec plus de ressources et une exposition plus importante aux risques. Elles doivent appliquer à la fois les mesures du groupe IG1 et celles du groupe IG2 pour renforcer leur sécurité.
3	Processus défini	Des règles précises sont établies, documentées et reproductibles pour la majorité des cas. La réussite ne dépend plus des individus mais du respect des processus. Des écarts peuvent subsister, mais l'organisation sait les identifier et y remédier.	IG3	Ce groupe vise les organisations les plus développées, qui disposent de moyens importants et sont exposées à des risques plus élevés. Elles doivent mettre en place des contrôles avancés en plus de ceux des groupes IG1 et IG2, afin de mieux se protéger contre les attaques complexes.
4	Processus maîtrisé	Les processus sont suivis et mesurés de manière régulière. L'organisation adapte ses pratiques en fonction des résultats obtenus, dans une logique d'efficacité et de rentabilité. Des indicateurs sont utilisés pour piloter la performance.		
5	Amélioration continue	Les processus sont optimisés de manière continue. L'organisation adopte une démarche proactive d'amélioration, impliquant tous les collaborateurs. Les processus sont revus et adaptés en permanence pour rester performants et agiles.		
NA	Non applicable	Ce contrôle ou processus n'est pas concerné ou ne peut être évalué dans le contexte actuel.		

Signification des niveaux :

- ✓ **Non structuré** : aucune méthode formelle, actions individuelles non coordonnées
- ✓ **Pratiques informelles** : débuts de cohérence, mais sans documentation ni standard
- ✓ **Processus défini** : existence de règles claires, mais respect partiel ou variable
- ✓ **Processus maîtrisé** : suivi régulier et pilotage basé sur des indicateurs
- ✓ **Amélioration continue** : processus optimisés, révisés en continu, intégrés à une démarche qualité
- ✓ **N/A – Non applicable** : le contrôle ne concerne pas l'organisation évaluée

Le référentiel CIS Controls introduit également une notion de **groupes de mise en œuvre** :

- ✓ **IG1** : pour les organisations ayant peu de ressources et un faible niveau de risque
- ✓ **IG2** : pour les structures de taille moyenne avec des moyens plus importants
- ✓ **IG3** : pour les grandes organisations ou les entités à haut niveau de risque

Ces groupes aident à prioriser les sous-contrôles à mettre en œuvre selon le profil de l'organisation.

2.2 Échelle de conformité (DORA)

Pour DORA, l'évaluation repose sur des critères qualitatifs, combinant plusieurs dimensions (politique, mise en œuvre, automatisation, suivi).

Niveau de maturité	
Entièrement conforme	Toutes les dimensions du contrôle sont pleinement satisfaites. La politique est formalisée, le contrôle est mis en œuvre, automatisé (ou techniquement imposé), et suivi au niveau de la direction.
Partiellement conforme	Une partie seulement des éléments du contrôle est en place. Par exemple, la politique est définie et le contrôle est appliqué, mais il n'est ni automatisé ni suivi par la direction.
Non conforme	Aucun élément du contrôle n'est en place : ni politique, ni procédure, ni mise en œuvre technique.
Non applicable	L'exigence ne s'applique pas à l'entité ou au périmètre évalué (par exemple : service non utilisé, technologie non déployée, type d'activité exclu).

- ✓ **Entièrement conforme** : toutes les dimensions sont satisfaites
- ✓ **Partiellement conforme** : certaines dimensions sont absentes
- ✓ **Non conforme** : aucun élément du contrôle n'est en place
- ✓ **Non applicable** : exigence non pertinente dans le contexte évalué

3. Dashboard

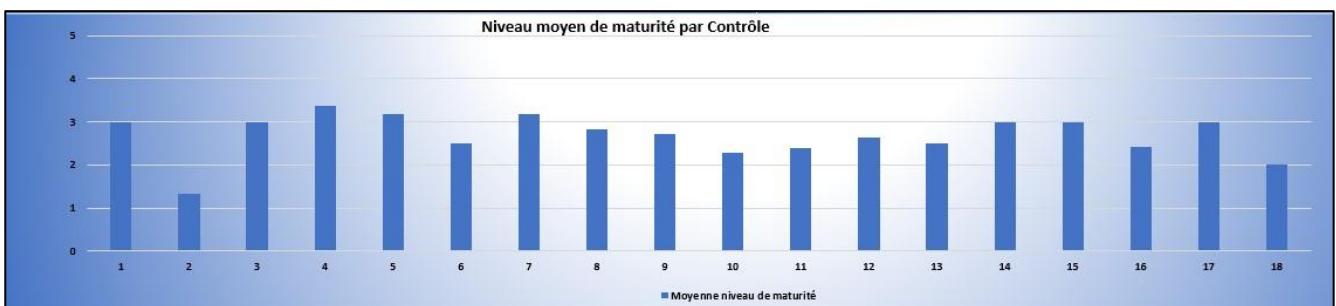
Une fois les données remplies dans les feuilles d'évaluation, l'outil génère automatiquement des tableaux de bord pour chaque référentiel.

3.1 Dashboard CIS

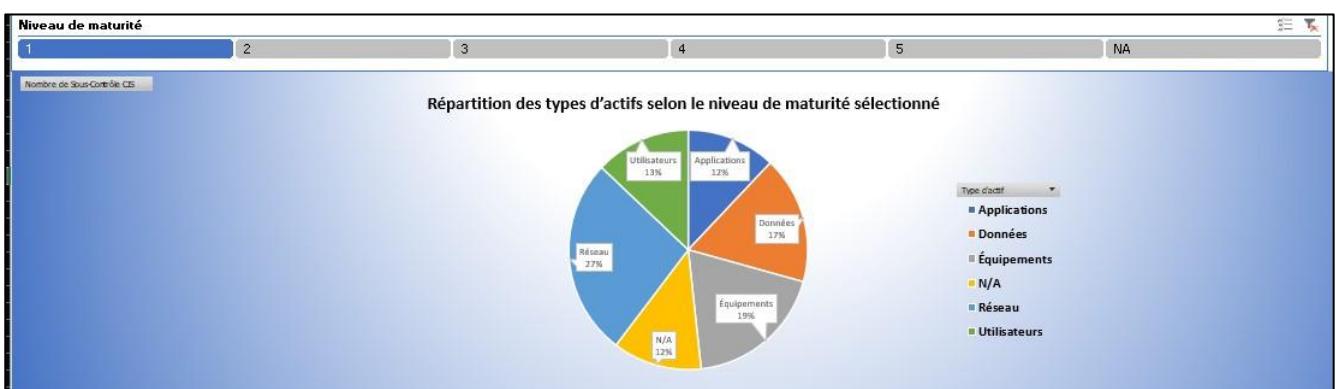
Le Dashboard affiche le résultat des différentes analyses des données sur les niveaux de maturité précédemment renseignés. On y retrouve plusieurs vues pour mieux visualiser les données.



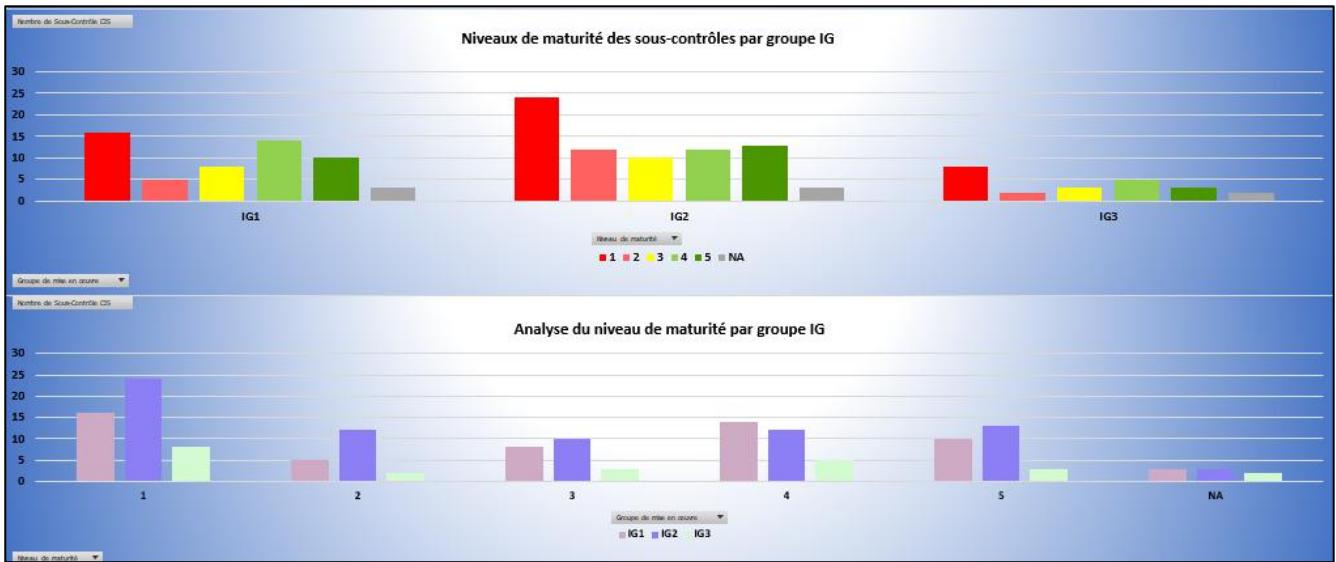
- Ce graphique présente la **répartition des sous-contrôles par niveau de maturité**, sous deux formes complémentaires :
 - **À gauche**, un **radar** met en évidence les niveaux les plus représentés, pour visualiser rapidement les écarts de maturité.
 - **À droite**, un **diagramme circulaire** illustre la part de chaque niveau dans l'ensemble des sous-contrôles évalués.



- Ce graphique en barres affiche le **niveau moyen de maturité atteint pour chaque contrôle principal** du référentiel CIS . Il permet d'identifier facilement les domaines les plus avancés et ceux qui nécessitent une attention particulière.



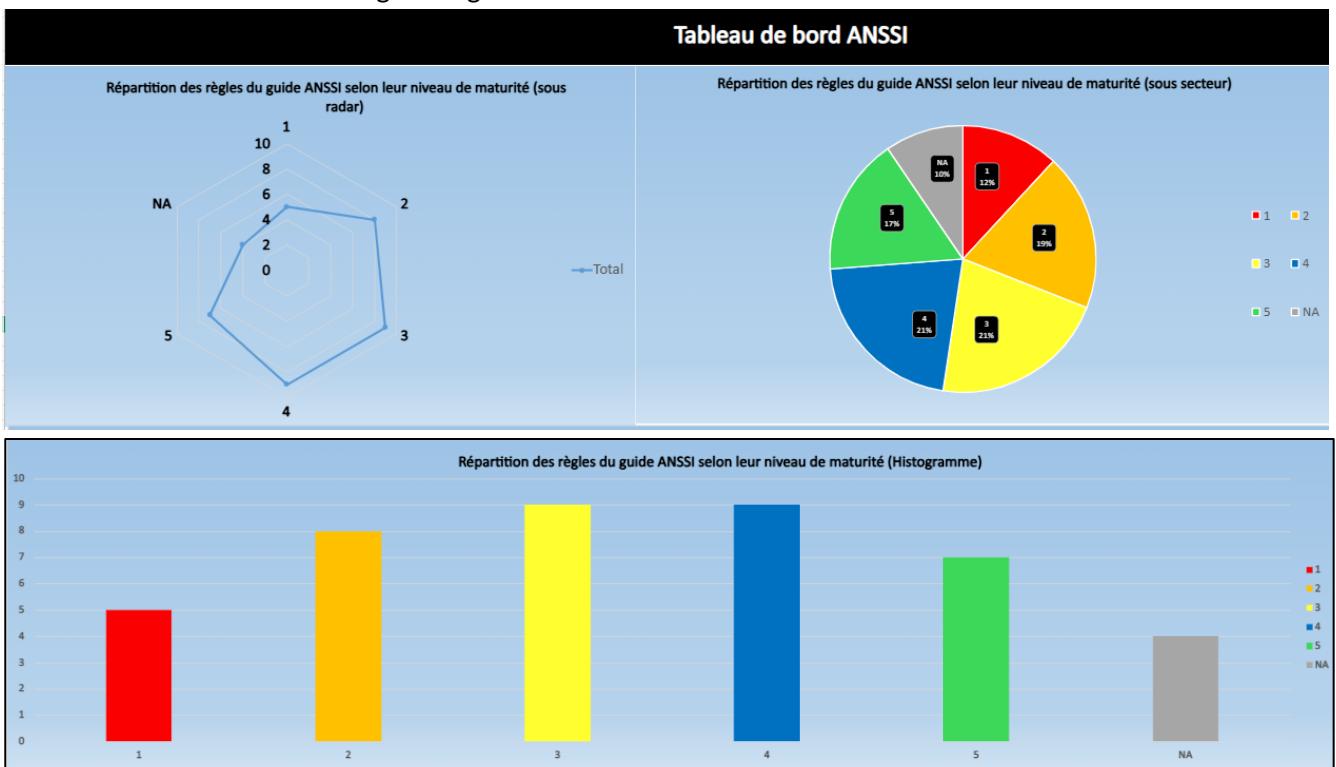
- Ce diagramme circulaire montre la **répartition des types d'actifs** (applications, équipements, réseau, etc.) pour un **niveau de maturité donné**. L'auditeur peut sélectionner un niveau (1 à 5 ou N/A) pour voir quels types d'actifs sont les plus concernés par ce score.



- Ces deux graphiques permettent d'analyser les niveaux de maturité en fonction des groupes de mise en œuvre (IG1, IG2, IG3) du référentiel CIS :
 - En haut : répartition des sous-contrôles par niveau de maturité au sein de chaque groupe IG, ce graphique aide à repérer les écarts de maturité à l'intérieur de chaque groupe (ex. : trop de niveau 1 dans IG2).
 - En bas : analyse croisée des niveaux de maturité atteints par groupe IG, chaque niveau est réparti par groupe, ce qui permet de comparer leur avancement global.

3.2 Dashboard ANSSI

Le tableau de bord ANSSI fournit plusieurs représentations visuelles de la répartition des niveaux de maturité attribués aux règles du guide.



➤ Ces trois graphiques affichent la même donnée sous différents angles :

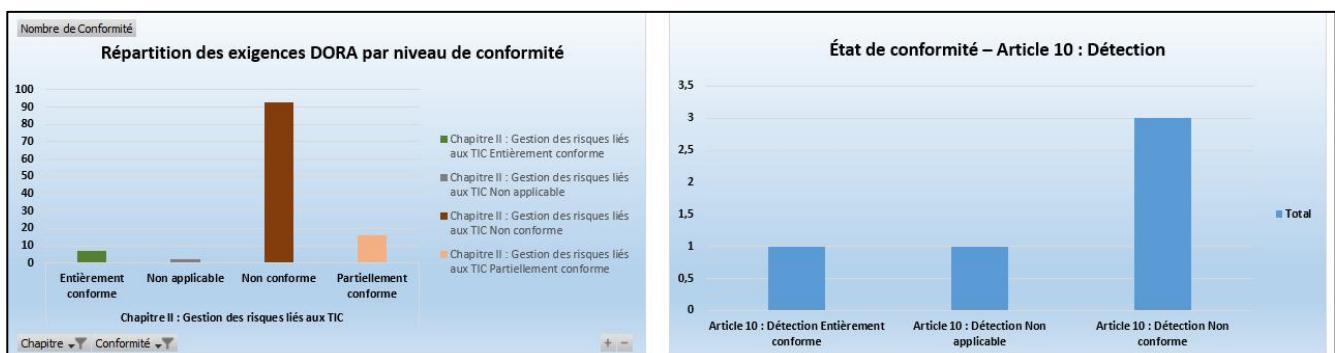
- Radar : met en évidence l'équilibre ou les déséquilibres dans la répartition des niveaux.
- Diagramme circulaire : offre une lecture rapide et intuitive des proportions (ex. : 21 % au niveau 3, 12 % au niveau 1...).
- Histogramme : permet une comparaison visuelle directe entre les quantités de règles évaluées à chaque niveau.

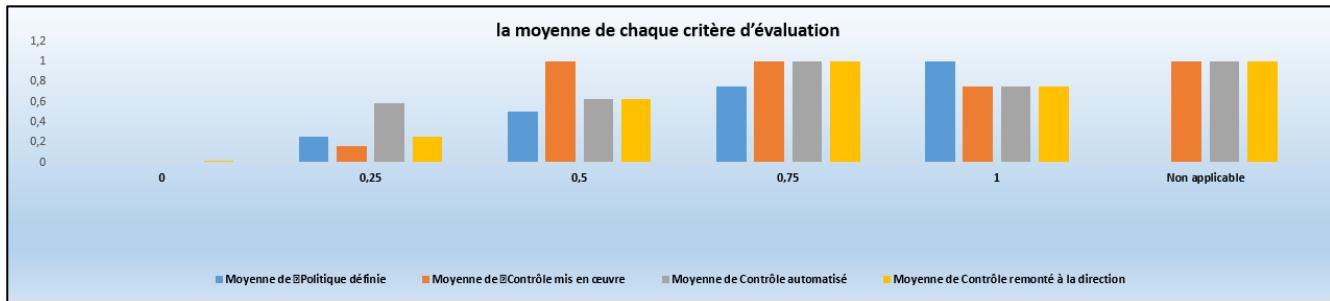
Ces représentations permettent d'évaluer rapidement l'état général de maturité des règles d'hygiène et d'identifier les niveaux les plus fréquents.



➤ Ce graphique montre la **répartition globale des règles ANSSI selon leur niveau de maturité**, avec la possibilité de filtrer par chapitre.

3.3 Dashboard DORA





- En haut à gauche, **la répartition globale des exigences par niveau de conformité** permet d'identifier immédiatement les zones critiques. Les exigences sont classées selon qu'elles sont entièrement conformes, partiellement conformes, non conformes ou non applicables.
- En haut à droite, **l'analyse de l'article 10 “Détection”** met en évidence le niveau de conformité pour chacune de ses exigences. Cette représentation permet d'examiner plus précisément un article en particulier, et d'identifier les points à corriger.
- Enfin, en bas, **la visualisation des moyennes par critère d'évaluation** permet d'analyser les dimensions les plus avancées ou les plus à renforcer. On y retrouve les scores moyens obtenus pour chaque critère : politique définie, contrôle mis en œuvre, automatisation, et remontée à la direction.

4. Conseils de bonnes pratiques

- ✓ Réaliser l'autoévaluation en équipe (informatique, SSI, direction métier...) pour croiser les points de vue.
- ✓ Attribuer les niveaux de maturité de manière honnête, même si cela révèle des faiblesses. Le but est l'amélioration continue.
- ✓ Ajouter des commentaires pour justifier les notes et noter les actions à envisager.
- ✓ Réévaluer les contrôles tous les 6 à 12 mois pour suivre les progrès et ajuster les priorités