# Annexe C : Plan de surveillance

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Plan de surveillance ISO/IEC 27001:2013** | | | | | | |
| **1** : Audit initial  **2 :** Audit de surveillance 1  **3** : Audit de surveillance 2  **4** : Audit de recertification | | | **Plan** | | | |
| **1**  **(202X)** | **2**  **(202X)** | **3**  **(202X)** | **4**  **(202X)** |
| **Articles d’ISO/IEC 27001:2013** | | | | | | |
| **4 Contexte de l’organisme** | | | | | | |
| **4.1** | Compréhension de l’organisation et de son contexte | |  |  |  |  |
| **4.2** | Compréhension des besoins et des attentes des parties intéressées | |  |  |  |  |
| **4.3** | Détermination du domaine d’application du système de management de la sécurité de l’information | |  |  |  |  |
| **4.4** | Système de management de la sécurité de l’information | |  |  |  |  |
| **5 Leadership** | | | | | | |
| **5.1** | Leadership et engagement | |  |  |  |  |
| **5.2** | Politique | |  |  |  |  |
| **5.3** | Rôles, responsabilités et autorités au sein de l’organisation | |  |  |  |  |
| **6 Planification** | | | | | | |
| **6.1** | Actions liées aux risques et opportunités | |  |  |  |  |
| **6.2** | Objectifs de sécurité de l’information et plans pour les atteindre | |  |  |  |  |
| **7 Support** | | | | | | |
| **7.1** | Ressources | |  |  |  |  |
| **7.2** | Compétence | |  |  |  |  |
| **7.3** | Sensibilisation | |  |  |  |  |
| **7.4** | Communication | |  |  |  |  |
| **7.5** | Informations documentées | |  |  |  |  |
| **8 Fonctionnement** | | | | | | |
| **8.1** | Planification et contrôle opérationnels | |  |  |  |  |
| **8.2** | Appréciation des risques de sécurité de l'information | |  |  |  |  |
| **8.3** | Traitement des risques de sécurité de l’information | |  |  |  |  |
| **9 Évaluation des performances** | | | | | | |
| **9.1** | Surveillance, mesure, analyse et évaluation | |  |  |  |  |
| **9.2** | Audit interne | |  |  |  |  |
| **9.3** | Revue de direction | |  |  |  |  |
| **10 Amélioration** | | | | | | |
| **10.1** | Non-conformité et actions correctives | |  |  |  |  |
| **10.2** | Amélioration continue | |  |  |  |  |
| **Objectifs et mesures de référence** | | | | | | |
| **A.5** | Politiques de sécurité de l’information | |  |  |  |  |
| **A.6** | Organisation de la sécurité de l’information | |  |  |  |  |
| **A.7** | Sécurité des ressources humaines | |  |  |  |  |
| **A.8** | Gestion des actifs | |  |  |  |  |
| **A.9** | Contrôle d’accès | |  |  |  |  |
| **A.10** | Cryptographie | |  |  |  |  |
| **A.11** | Sécurité physique et environnementale | |  |  |  |  |
| **A.12** | Sécurité liée à l’exploitation | |  |  |  |  |
| **A.13** | Sécurité des communications | |  |  |  |  |
| **A.14** | Acquisition, développement et maintenance des systèmes d’information | |  |  |  |  |
| **A.15** | Relations avec les fournisseurs | |  |  |  |  |
| **A.16** | Gestion des incidents liés à la sécurité de l’information | |  |  |  |  |
| **A.17** | Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité | |  |  |  |  |
| **A.18** | Conformité | |  |  |  |  |
| **Exigences supplémentaires** | | | | | | |
|  | Utilisation du logo et de la marque déposée | |  |  |  |  |
|  | Liste des documents inclus dans le SM audité | |  |  |  |  |
| **Notes et commentaires :** | |  | | | | |

*Pour les visites terminées, marquez « X » dans la case pour chaque article/processus couvert.*

*Pour les visites planifiées, marquez « O » dans la case pour chaque article/processus à couvrir.*