# Règle n° 6 : Contrôler régulièrement la sécurité et exiger des résultats

## Quelles sont les bonnes pratiques de contrôle à mettre en place ?

- S'assurer que l'organisation et les processus choisis pour protéger les informations sont toujours au niveau définis : **mise en place d'un plan d'audit annuel pour vérifier la conformité des process et de l'organisation aux politiques de sécurité définies**
- S'assurer que la sécurité mise en place sur les systèmes pour protéger les informations est toujours au niveau défini : **mise en place des contrôles réguliers de la sécurité sur les systèmes les plus sensibles et les plus critiques**
- S'assurer que les systèmes sont bien protégés de toutes les failles techniques connues : **faire vérifier les failles de sécurité connues par un test annuel de vulnérabilité des systèmes les plus sensibles**
- S'assurer que les risques identifiés ont bien été pris en compte et corrigés : **Faire une revue régulière des risques identifiés et de leur plan de réduction**
- S'assurer que les systèmes suivent bien les mises à jour fournies par les principaux éditeurs **: Mettre en place des indicateurs de suivi des mises à jour des patches de sécurité des systèmes les plus sensibles**
- S'assurer de pouvoir restaurer des informations corrompues : **mettre en place des contrôles réguliers des sauvegardes**
- S'assurer d'être protégé des menaces virales : **mettre en place des contrôles réguliers sur la mise à jour antivirus sur les systèmes les plus sensibles**
- S'assurer que l'élément humain de l'organisation respecte bien les politiques de sécurité et réagisse correctement aux évènements pour protéger les informations : **mettre en place des contrôles sur la sensibilisation des collaborateurs à la sécurité par des campagnes de phishing, de vérification de bureau propre, de faux appels téléphoniques**

## Faits / exemples

**Affaire des Panama papers (2016)** : utilisation par les pirates / lanceurs d'alerte de failles de sécurité non traitées pour s'introduire dans le SI et récupérer plus de 11 millions de documents.

## Résultats attendus

Un rapport d'audit sur l'évaluation de la sécurité contenant plusieurs chapitres :

- Résultat des audits effectués sur les process
- Niveau des failles de sécurité
- Résultat test de vulnérabilité et pénétration
- Résultat des campagnes de sensibilisation des employés
- Liste de risques identifiés par le rapport
- Proposition d'un plan d'action pour améliorer la protection des informations

Un tableau de bord régulier sur les systèmes les plus critiques avec le niveau de sécurité nécessaires :

- Correctif de sécurité à jour
- Antivirus à jour
- Backup opérationnel
- Risques identifiés corrigés