ÉTUDES DE CAS FINAL

RAPPORT D'AUDIT

Audit de sécurité informatique : est-il essentiel à votre entreprise ?

Entreprises auditées

CYBERSHIELD

NETSECURE ISP

AGRONUTRITECH

GROUPE 2

- Rayane Lattari
- Cynthia Hached
- Massilva Ouaked
- Nabil Battata
- Amine Idres
- Massinissa Brahimi

Table de matières

Contexte d'audit

Ce rapport d'audit est élaboré dans le cadre d'un exercice visant à évaluer la conformité et la mise en œuvre des bonnes pratiques en matière de sécurité de l'information dans différents contextes organisationnels. Nous devons auditer trois sociétés :

- **Société n°1** : Société de conseil spécialisée en sécurité des systèmes d'information
- **Société n°2** : Fournisseur d'accès Internet
- **Société n°3** : Entreprise d'agro-alimentaire

L'objectif principal de cet exercice est d'évaluer l'application des exigences de sécurité de l'information spécifiées dans des référentiels internationaux tels que **l'ISO 27001** et **l'ISO 27002**, tout en proposant des actions concrètes pour améliorer la posture de sécurité de l'entreprise.

Étude de Cas - Société n°1 : **Cybershield**

1. Contexte de l'Entreprise

1.1. Présentation de l'Entreprise

- **Nom :** CyberShield.
- **Secteur :** Cybersécurité / ESN spécialisée dans les solutions de sécurité des systèmes d'information.
- **Taille :** 200 collaborateurs organisés en équipes spécialisées.
- **Clientèle :** Banques, industries, PME technologiques, et administrations publiques.
- **Mission :** Protéger les entreprises contre les cybermenaces grâce à des solutions innovantes et sur mesure.

1.2. Activités principales

- **Gestion de SOC (Security Operations Center) :**
  Surveillance en temps réel et réponse aux incidents de sécurité pour des infrastructures critiques.
- **Audit et conformité :**
  Évaluation de la posture de sécurité des clients et accompagnement dans la mise en conformité avec les normes ISO 27001, RGPD et NIS2.
- **Développement de solutions :**
  Création de plateformes sur mesure pour la gestion des accès, la surveillance des menaces, et la protection des données.
- **Formation :**
  Sensibilisation et formation des collaborateurs aux meilleures pratiques en cybersécurité.

- **Gestion des crises :**
  Assistance et récupération après cyberattaques, avec simulations régulières pour améliorer la résilience.

1.3. Pourquoi cet audit ?

Cette étude a pour but d'analyser les pratiques de sécurité de Cybershield à travers des exigences clés (*ISO 27001, RGPD*) et de proposer des recommandations applicables pour optimiser leur conformité et leur efficacité opérationnelle.

2. Méthodologie

2.1. Sources d'Informations

Pour chaque exigence, nous collectons des données via trois méthodes distinctes :

1. **Revue documentaire :** Analyse des politiques, procédures, rapports, logs et tout document pertinent.
2. **Revue technique :** Inspection et validation des systèmes techniques tels que les configurations, résultats de scans, et logs.
3. **Entretiens humains :** Discussions avec les parties prenantes (RSSI, équipes IT, RH, chefs de projet) pour comprendre les pratiques réelles.

2.2. Actions d'Audit

Pour chaque exigence, des actions spécifiques sont menées pour valider les informations issues des sources ci-dessus. Ces actions consistent à :

- Examiner les processus en place pour vérifier leur application pratique.
- Collecter des preuves concrètes via des logs, des configurations ou des tests.
- Identifier les écarts ou points à améliorer.

3. Analyse des Exigences :

3.1. Tableau d'applicabilité des exigences

Exigence	Applicable	Justification
5.8	Oui	Les projets de *Cybershield* impliquent des données sensibles des clients, nécessitant une intégration systématique des exigences de sécurité dans les méthodologies de projet.
8.1	Oui	Les collaborateurs utilisent des appareils mobiles pour travailler chez les clients ou à distance, exposant l'organisation à des risques de vol ou d'accès non autorisé.

8.30	Partiellement	*Cybershield* externalise ponctuellement des développements spécifiques (outils internes, portails clients). Cette exigence s'applique uniquement pour ces projets externalisés.
5.27	Oui	L'exploitation des incidents est essentielle pour améliorer la sécurité interne et fournir des recommandations pertinentes aux clients.
6.1	Oui	Les consultants manipulent des données critiques des clients, rendant impérative la vérification rigoureuse des antécédents pour les postes sensibles.
7.2	Oui	Bien que *Cybershield* travaille principalement en mode dématérialisé, ses locaux (serveurs, SOC) contiennent des infrastructures critiques nécessitant un contrôle physique strict.
8.8	Oui	La gestion proactive des vulnérabilités est cruciale pour sécuriser les systèmes internes et pour maintenir la crédibilité des recommandations faites aux clients.
5.35	Oui	En tant que société de conseil, *Cybershield* doit démontrer qu'elle respecte les standards qu'elle impose à ses clients via des audits internes et externes réguliers.

3.2. Détails des exigences

Exigence 5.8 : Intégration de la sécurité dans la gestion de projet

Revue documentaire

Analyse des méthodologies de gestion de projet utilisées (*Scrum, Agile, Waterfall*).
Vérification des plans de projet pour identifier :
- Les étapes liées à la sécurité (*analyse des risques, tests*).
- Les rôles et responsabilités assignés à la gestion de la sécurité.

Collecte des rapports de projet récents pour examiner si des analyses de sécurité ou des tests ont été réalisés.

Revue technique

Inspection des outils de gestion de projet (ex. : *Jira, Trello*) pour vérifier :
- Si des tickets spécifiques à la sécurité sont créés.
- Si des automatisations ou des intégrations (ex. : *scanners de vulnérabilités*) sont mises en place.

Validation des résultats des tests de sécurité réalisés sur les livrables (*via des outils comme SonarQube*).

Entretiens humains

Questions aux chefs de projet :

Quels types de projets sont réalisés et quelles méthodologies sont utilisées ?

Intégrez-vous des étapes spécifiques à la sécurité (ex. : *évaluation des risques*) ?

Discussions avec le RSSI :

Quels outils et processus de suivi sont en place pour garantir la sécurité des projets ?

Le RSSI est-il impliqué dans la validation des livrables ?

Actions d'audit

Examiner les plans de projet et livrables des projets critiques pour identifier les étapes liées à la sécurité.

Analyser l'utilisation des outils de gestion de projet pour vérifier l'existence de tickets ou d'étapes de validation de sécurité.

Confirmer avec les chefs de projet la mise en œuvre des pratiques documentées.

Exigence 8.1 : Sécurisation des appareils mobiles

Revue documentaire

Analyse des politiques BYOD pour déterminer :

Les restrictions imposées aux appareils personnels.

Les exigences de chiffrement, VPN et MFA.

Vérification des manuels de configuration pour les solutions MDM (*Mobile Device Management*).

Examen des rapports d'incidents liés aux appareils mobiles.

Revue technique

Inspection des configurations MDM pour évaluer leur couverture :

Types d'appareils gérés (*laptops, smartphones*).

Politiques appliquées (*chiffrement, mises à jour, contrôles d'accès*).

Analyse des logs des accès mobiles aux systèmes internes pour identifier d'éventuelles anomalies ou failles.

Entretiens humains

Questions aux équipes IT :

Quels appareils sont autorisés à accéder aux systèmes internes ?

Les collaborateurs utilisent-ils leurs propres appareils ?

Discussions avec le RSSI :

- Comment les politiques BYOD sont-elles appliquées ?
- Quels mécanismes sont en place pour détecter et remédier aux incidents mobiles ?

Actions d'audit

Examiner les configurations MDM pour vérifier la couverture et les restrictions.
Analyser les logs d'accès mobiles pour détecter les comportements suspects.
Vérifier auprès des équipes IT si les appareils non conformes sont bloqués.

Exigence 8.30 : Supervision des développements externalisés

Revue documentaire

Analyse des contrats signés avec les sous-traitants pour vérifier :

- L'existence de clauses sur la sécurité des livrables.
- Les exigences d'audit ou de tests de sécurité.

Vérification de la documentation des livrables fournis (*code source, documentation technique*).

Revue technique

Inspection des livrables pour évaluer leur conformité avec les normes (ex. : *OWASP, ISO 27034*).
Analyse des résultats des tests de sécurité réalisés (*tests de pénétration, revues de code*).

Entretiens humains

Discussions avec les responsables des projets externalisés :

- Quels types de développements sont externalisés ?
- Quels processus sont en place pour valider les livrables ?

Questions aux sous-traitants (le cas échéant) :

- Quelles normes de sécurité respectez-vous ?
- Quels tests de sécurité effectuez-vous avant livraison ?

Actions d'audit

Examiner les contrats pour vérifier l'intégration des clauses de sécurité.
Vérifier les livrables externalisés et leurs rapports de test.
Confirmer avec les responsables de projet si les sous-traitants sont supervisés.

Exigence 5.27 : Exploitation des leçons issues des incidents

Revue documentaire

Analyse des registres des incidents pour identifier :
- Les causes profondes des incidents passés.
- Les actions correctives prises.

Vérification des rapports de revue post-incident.

Revue technique

Analyse des logs des incidents collectés par le SOC.
Validation des indicateurs de performance liés aux incidents (*temps de résolution, fréquence*).

Entretiens humains

Questions aux équipes SOC :
- Comment les leçons apprises sont-elles documentées ?
- Les équipes sont-elles sensibilisées aux incidents passés ?

Discussions avec le RSSI :
- Des actions correctives sont-elles mises en œuvre après chaque incident ?

Actions d'audit

Examiner les registres d'incidents pour identifier les lacunes dans la documentation.
Valider les actions correctives en vérifiant les logs.
Confirmer avec les équipes SOC la communication des leçons apprises.

Exigence 6.1 : Vérifications à l'embauche

Revue documentaire :

Analyse des politiques de recrutement pour :

Vérifier la mise en œuvre de vérifications des antécédents des candidats

Vérification des procédures internes RH pour :

S'assurer que les exigences de sécurité sont bien intégrées au processus de recrutement des employés

Revue technique :

Aucun outil spécifique requis.

Mais l'audit doit vérifier si un système de gestion des candidatures ou un logiciel RH est utilisé pour effectuer les vérifications des antécédents des candidats.

Entretiens humains :

Questions aux responsables RH :

Quelles vérifications sont effectuées lors du recrutement, en particulier pour les postes à haut risque (ex. : IT, gestion des données sensibles) ?

Les processus sont-ils systématiquement appliqués à tous les candidats, y compris ceux issus des sous-traitants ?

Discussions avec le RSSI :

Le RSSI est-il impliqué dans les décisions d'embauche pour les postes critiques en termes de sécurité ?

Actions d'audit :

Vérifier les processus de recrutement pour les employés occupant des postes sensibles afin de confirmer que des vérifications de sécurité sont systématiquement appliquées.

Vérifier la documentation RH pour s'assurer que les vérifications sont bien effectuées et que les résultats sont correctement archivés.

Exigence 7.2 : Contrôle physique des accès

Revue documentaire :

Analyse des politiques de contrôle d'accès physique aux installations sensibles de l'entreprise, notamment les centres de données, les locaux de développement et les zones de stockage de données sensibles.

Vérification des documents relatifs à la gestion des badges et des accès visiteurs, y compris les registres d'accès et les processus de gestion des clés physiques.

Revue technique :

Inspection des dispositifs de contrôle d'accès physique (ex. : lecteurs de badges, serrures électroniques, caméras de surveillance) pour vérifier qu'ils sont correctement configurés et fonctionnent efficacement.

Examen des logs d'accès physique pour identifier d'éventuelles anomalies dans les accès aux zones sensibles.

Entretiens humains :

Discussions avec les responsables de la sécurité physique :

Comment gérez-vous l'accès physique aux zones sensibles ?
Quelles sont les procédures en place pour les visiteurs et les employés temporaires ?

Discussions avec le RSSI :

Le RSSI est-il impliqué dans la définition des contrôles physiques d'accès ?
Comment gérez-vous l'accès aux zones sensibles pour les prestataires externes ?

Actions d'audit :

Vérifier l'efficacité des contrôles d'accès physiques dans les zones sensibles en menant des tests sur l'accès non autorisé.

Analyser les logs d'accès physiques pour détecter toute activité anormale ou non conforme aux politiques de sécurité.

Exigence 8.8 : Gestion des vulnérabilités

Revue documentaire :

Examen des politiques de gestion des vulnérabilités, y compris la fréquence des scans de vulnérabilités, les types de vulnérabilités ciblées et la gestion des corrections (patches).

Vérification de la documentation des outils de gestion des vulnérabilités utilisés (ex. : Qualys, Nessus, OpenVAS), ainsi que les rapports d'analyse des vulnérabilités détectées.

Revue technique :

Analyse des résultats des scans de vulnérabilités effectués sur les systèmes de l'entreprise, y compris les délais de correction pour les vulnérabilités critiques.

Vérification des systèmes de patching pour s'assurer que les mises à jour de sécurité sont appliquées en temps opportun.

Entretiens humains :

Discussions avec les équipes IT :

Comment gérez-vous les vulnérabilités découvertes lors des scans ?
Quelle est la fréquence des tests de vulnérabilité et quelle est la politique de mise à jour des systèmes ?

Discussions avec le RSSI :

Le RSSI est-il impliqué dans le processus de gestion des vulnérabilités ?
Comment gérez-vous la correction des vulnérabilités critiques ?

Actions d'audit :

Vérifier les rapports des scans de vulnérabilités pour s'assurer que les vulnérabilités critiques sont corrigées rapidement.
Évaluer les pratiques de mise à jour pour s'assurer que les systèmes reçoivent des patchs dans les délais appropriés.

Exigence 5.35 : Audits réguliers

Revue documentaire :

Examen des politiques d'audit de sécurité de l'entreprise, y compris la fréquence des audits, les domaines audités, et les critères d'évaluation de la sécurité.
Vérification des rapports d'audit antérieurs pour s'assurer que des audits complets ont été réalisés et que des mesures correctives ont été prises pour donner suite aux conclusions des audits.

Revue technique :

Analyse des outils utilisés pour les audits internes et externes (ex. : outils GRC - Governance, Risk, and Compliance) afin de vérifier leur efficacité à détecter les écarts de sécurité.

Vérification des actions de remédiation en réponse aux résultats des audits précédents.

Entretiens humains :

Discussions avec le RSSI et l'équipe de sécurité pour comprendre la fréquence et l'étendue des audits effectués.

Questions aux auditeurs internes ou externes :

Quels sont les domaines de sécurité régulièrement audités ?
Quelle est l'approche suivie pour assurer la prise en charge des non-conformités détectées ?

Actions d'audit :

Vérifier la mise en œuvre des actions correctives identifiées lors des audits précédents.

Évaluer la couverture des audits pour s'assurer qu'ils couvrent tous les aspects critiques de la sécurité, y compris les aspects techniques et organisationnels.

Tableau 1 : implémentations proposées pour compliance

Exigence	Plan de remédiation
5.8	- Formaliser une méthodologie de gestion de projet intégrant la sécurité à chaque phase (analyse des risques, validation). - Former les chefs de projet sur les pratiques de gestion des risques et la sécurité. - Automatiser les tests de sécurité sur les livrables à l'aide d'outils comme SonarQube.
8.1	- Déployer une solution MDM (Mobile Device Management) pour gérer les appareils mobiles. - Mettre en place une politique BYOD stricte (chiffrement, segmentation des données pro/perso). - Sensibiliser les collaborateurs aux risques liés aux appareils mobiles.
8.30	- Ajouter des clauses de sécurité dans les contrats des sous-traitants (audits réguliers, tests de sécurité). - Intégrer un processus de validation technique des livrables avant leur déploiement (pipeline CI/CD). - Mettre en place un suivi des sous-traitants avec des rapports de conformité réguliers.
5.27	- Créer un registre formalisé des incidents documentant les causes et actions correctives. - Organiser des revues périodiques des incidents et des ateliers pour partager les leçons apprises avec les équipes. - Simuler des scénarios types pour former les équipes SOC.
6.1	- Mettre en place un processus de vérification des antécédents pour les postes sensibles (contrôles de casier judiciaire, clauses de confidentialité). - Automatiser les vérifications grâce à des outils dédiés pour réduire les erreurs. - Sensibiliser les recruteurs sur l'importance des vérifications pour les postes liés à la sécurité.

7.2	- Installer des contrôles d'accès physiques avancés (badges électroniques, caméras, alarmes). - Séparer physiquement les zones sensibles (serveurs, SOC) des espaces accessibles au public. - Mettre en place une surveillance vidéo avec alertes automatiques pour les intrusions.
8.8	- Déployer un outil de gestion des vulnérabilités comme Nessus ou Qualys pour identifier et corriger les failles en temps réel. - Organiser des revues trimestrielles pour évaluer l'exposition de l'organisation aux nouvelles vulnérabilités. - Former les équipes techniques à appliquer rapidement les correctifs nécessaires.
5.35	- Planifier des audits internes annuels pour suivre l'évolution des objectifs de sécurité. - Impliquer un auditeur externe pour valider la conformité aux normes ISO 27001 ou RGPD. - Introduire des mécanismes de surveillance continue pour détecter les déviations en temps réel.

Étude de Cas - Société n°2 : **NetSecure ISP**

1. Contexte de l'Entreprise

1.1 Présentation de NetSecure ISP

- **Nom :** NetSecure ISP.
- **Secteur :** Cybersécurité / ESN spécialisée dans les solutions de sécurité des systèmes d'information.
- **Taille :** 200 collaborateurs.
- **Clientèle :** Banques, industries et administrations publiques.
- **Mission :** De la gestion des infrastructures réseau à la cybersécurité.

1.2 Activités principales :

- Fourniture de services d'accès à Internet et de télécommunications.
- Gestion de SOC (Security Operations Center).

- Conseil en cybersécurité et audits (*ISO 27001*, *RGPD*, *NIS2*).
- Développement de solutions personnalisées pour la sécurité réseau.

1.3 Pourquoi cet audit ?

Les secteurs stratégiques auxquels Netsecure ISP est confronté exigent des solutions fiables, sécurisées et conformes aux normes internationales, en raison de la gestion de grandes quantités de données utilisateur et de la nécessité de maintenir des systèmes toujours opérationnels, car en tant que fournisseur d'accès à Internet, leur service doit être constamment disponible.

2. Méthodologie

2.1 Sources d'informations

Pour chaque exigence, les données seront collectées via les trois méthodes suivantes :

1. **Revue documentaire** :
   - Analyse des politiques, procédures, rapports, journaux système et autres documents pertinents.
2. **Revue technique** :
   - Inspection et validation des systèmes techniques, telles que les configurations réseau, résultats de scans de sécurité, et journaux d'accès.
3. **Entretiens humains** :
   - Entretiens avec les parties prenantes (RSSI, équipes IT, RH, chefs de projet, techniciens réseau) pour comprendre les pratiques appliquées.

2.2 Actions d'Audit

Pour chaque exigence, les actions suivantes seront entreprises :

- Vérification des processus documentés pour garantir leur mise en œuvre pratique.
- Collecte de preuves tangibles (rapports de sécurité, configurations réseau, logs).
- Identification des écarts ou des points à améliorer pour chaque exigence.

3. Analyse des exigences :

3.1. Tableau d'applicabilité des exigences

Exigence	Applicable	Justification
5.8	Oui	Les projets de *NetSecure ISP*, tels que la mise en œuvre d'infrastructures réseau ou de nouvelles offres client, impliquent des données sensibles et des systèmes critiques, nécessitant une intégration systématique des exigences de sécurité dans la gestion des projets.

8.1	Oui	Les équipes techniques de *NetSecure ISP* utilisent des appareils mobiles (tablettes, smartphones) pour intervenir sur les réseaux des clients ou accéder aux systèmes internes, exposant l'organisation à des risques de vol ou d'accès non autorisé.
8.30	Partiellement	*NetSecure ISP* externalise occasionnellement le développement d'applications clients ou d'outils de gestion interne. Cette exigence s'applique spécifiquement aux projets externalisés.
5.27	Oui	L'exploitation des incidents réseau ou liés à la sécurité est cruciale pour améliorer les performances des infrastructures et réduire les interruptions de service pour les clients.
6.1	Oui	Les techniciens et ingénieurs de *NetSecure ISP* ont accès à des infrastructures sensibles (centres de données, équipements clients), rendant la vérification rigoureuse des antécédents indispensable.
7.2	Oui	Les locaux de *NetSecure ISP*, hébergent des infrastructures critiques, les points d'accès ainsi que les autres points vulnérables à une intrusion non autorisée, doivent être contrôlés de manière stricte.
8.8	Oui	La gestion proactive des vulnérabilités techniques est essentielle pour sécuriser les réseaux et services fournis aux clients, ainsi que pour protéger l'infrastructure interne.
5.35	Oui	En tant que fournisseur d'accès, *NetSecure ISP* doit démontrer sa conformité via des audits internes et externes réguliers pour garantir la fiabilité et la sécurité de ses services, conformément aux attentes des clients.

3.2. Détails des exigences :

Exigence 5.8 : Intégration de la sécurité dans la gestion de projet

Revue documentaire

- Analyse des méthodologies de gestion de projet utilisées (*Scrum, Agile, ITIL*).
- Vérification des plans des projets stratégiques de *NetSecure ISP* pour identifier :
  - Les étapes liées à la sécurité (*analyse des risques, tests de pénétration*).
  - Les rôles et responsabilités assignés à la sécurité dans chaque projet.

- Examen des rapports de projets récents pour vérifier si des évaluations de sécurité ont été menées.

Revue technique

- Inspection des outils de gestion de projet (par exemple : *Microsoft Project*) pour :
  - Identifier la présence de tickets ou d'étapes spécifiques à la sécurité.
  - Vérifier l'intégration d'outils de sécurité automatisés (*analyse de code, scanner de vulnérabilités*).
- Analyse des résultats des tests de sécurité réalisés sur les livrables des projets critiques.

Entretiens humains

- Questions aux chefs de projet :
  - Quels types de projets sont réalisés, et quelles méthodologies sont suivies ?
  - Intégrez-vous des étapes spécifiques pour traiter les risques liés à la sécurité ?

- Discussion avec le RSSI :
  - Quels outils et mécanismes sont en place pour superviser la sécurité des projets ?
  - Comment le RSSI valide-t-il les livrables ?

Actions d'audit

- Examiner les plans des projets critiques pour vérifier l'intégration des étapes de sécurité.
- Confirmer l'utilisation des outils de gestion pour suivre les mesures de sécurité.
- Valider avec les chefs de projet l'application pratique des mesures de sécurité.

Exigence 8.1 : Sécurisation des appareils mobiles

Revue documentaire

- Analyse de la politique BYOD (B*ring Your Own Device*) pour évaluer :
  - Les restrictions sur les appareils personnels des collaborateurs.
  - Les exigences en termes de chiffrement, VPN et authentification multifactorielle (*MFA*).
- Vérification des manuels de configuration des solutions de gestion des appareils mobiles (*MDM*).
- Examen des incidents liés à l'utilisation des appareils mobiles.

Revue technique

- Inspection des configurations MDM pour évaluer :
  - Les types d'appareils gérés (*smartphones, tablettes, ordinateurs portables*).

    - Les politiques appliquées : chiffrement, mises à jour automatiques, contrôle des accès.
- Analyse des journaux d'accès mobile pour identifier des anomalies ou des failles de sécurité.

Entretiens humains

- Questions aux équipes IT :
    - Quels types d'appareils sont autorisés à accéder aux systèmes internes ?
    - Utilisez-vous un processus pour autoriser ou bloquer les appareils non conformes ?
- Discussion avec le RSSI :
    - Comment sont appliquées les politiques BYOD ?
    - Quels mécanismes permettent de détecter et de corriger les incidents liés aux appareils mobiles ?

Actions d'audit

- Examiner les configurations MDM pour vérifier leur efficacité.
- Analyser les journaux des connexions mobiles pour détecter les anomalies.
- Valider les actions prises par les équipes IT en cas d'incident.

Exigence 8.30 : Supervision des développements externalisés

Revue documentaire

- Vérification des contrats des sous-traitants pour identifier :
    - Les clauses spécifiques liées à la sécurité des livrables.
    - Les exigences de tests ou d'audits de sécurité.
- Analyse des livrables (*code source, documentation*) pour évaluer leur conformité.

Revue technique

- Inspection des livrables fournis pour vérifier leur conformité avec les normes (ex. *OWASP, ISO 27034*).
- Analyse des résultats des tests de sécurité réalisés (ex. *tests de pénétration, revues de code*).

Entretiens humains

- Questions aux responsables des projets externalisés :
    - Comment la conformité des sous-traitants est-elle suivie ?
    - Quels mécanismes sont en place pour superviser leurs livrables ?
- Discussion avec les sous-traitants :
    - Quels tests effectuez-vous avant la livraison ?
    - Respectez-vous des normes spécifiques (ex. *ISO 27034*) ?

Actions d'audit

- Vérifier l'inclusion de clauses de sécurité dans les contrats.
- Examiner les livrables externalisés et leurs rapports de test.
- Confirmer auprès des responsables que les sous-traitants sont bien supervisés.

Exigence 5.27 : Exploitation des leçons tirées des incidents

Revue documentaire

- Analyse des rapports d'incidents pour identifier les actions correctives prises.
- Vérification des leçons documentées issues des incidents précédents.

Revue technique

- Analyse des journaux du SOC pour valider :
  - Les indicateurs de performance (temps de réponse, fréquence des incidents).
  - La traçabilité des actions post-incidents.

Entretiens humains

- Questions aux équipes SOC :
  - Documentez-vous les leçons apprises après chaque incident ?
  - Comment les actions correctives sont-elles communiquées aux parties concernées ?
- Discussion avec le RSSI :
  - Les processus d'amélioration continue sont-ils appliqués après chaque incident majeur ?

Actions d'audit

- Vérifier les registres d'incidents pour s'assurer que les leçons apprises sont documentées.
- Valider l'application des actions correctives en analysant les logs.

Exigence 6.1 : vérifications préalables (screening)

Revue documentaire

- Les politiques de vérification des antécédents pour les nouveaux employés doivent être vérifiées pour s'assurer de leur conformité avec les lois et règlements.
- Les descriptions de poste doivent être analysées pour évaluer leur alignement avec le niveau d'accès et la sensibilité des informations.
- Les enregistrements des processus de vérification des candidats, tels que les antécédents criminels, les références et la vérification des diplômes, doivent être examinés.

- La documentation pour les exceptions au processus de vérification doit être validée.

Revue technique

- Les outils RH automatisés utilisés pour gérer les dossiers de vérification doivent être inspectés.
- La sécurisation et le stockage des informations sensibles des candidats doivent être vérifiés (par exemple, chiffrement ou contrôles d'accès).
- Les journaux d'accès aux données de vérification doivent être analysés.

Entretiens humains

- Des questions doivent être posées aux équipes RH concernant les processus de vérification :
    - Quels types de vérifications sont effectués ?
    - Comment les exceptions sont-elles gérées ?
- Une discussion doit être menée avec le RSSI pour comprendre comment les données sensibles des candidats sont protégées.

Actions d'audit

- Les dossiers doivent être vérifiés pour confirmer que les vérifications préalables ont été effectuées conformément aux politiques.
- Les données collectées pendant le processus de vérification doivent être validées pour leur conformité avec les exigences réglementaires.

Exigence 7.2 : contrôle des points d'accès physiques

Revue documentaire

- Les politiques de sécurité des périmètres physiques, notamment celles relatives aux zones de livraison et de chargement, doivent être examinées.
- Les plans et procédures pour isoler les points d'accès non autorisés doivent être analysés.
- Les incidents documentés liés aux accès non autorisés aux locaux doivent être consultés.

Revue technique

- Les systèmes de contrôle d'accès physique (ex. : badges, caméras de surveillance, capteurs de mouvement) doivent être inspectés.
- Les journaux d'accès physiques pour les zones sensibles doivent être vérifiés.
- Les mécanismes utilisés pour isoler les zones critiques des moyens de traitement de l'information doivent être analysés.

Entretiens humains

- Des questions doivent être posées aux responsables de la sécurité physique :
    - Quelles zones sont particulièrement sensibles et comment sont-elles protégées ?
    - Quels sont les processus pour détecter et réagir aux accès non autorisés ?
- Une discussion doit être menée avec les employés pour évaluer leur compréhension des politiques de sécurité physique.

Actions d'audit

- Les zones sensibles doivent être validées comme étant isolées et sécurisées.
- Les journaux d'accès et les rapports d'incident doivent être vérifiés pour leur complétude et leur exactitude.

Exigence 8.8 : gestion des vulnérabilités techniques

Revue documentaire

- Les politiques et procédures pour la gestion des vulnérabilités techniques doivent être analysées.
- Les rapports de scan de vulnérabilités réalisés doivent être examinés.
- Les registres des incidents de sécurité liés à des vulnérabilités non corrigées doivent être consultés.

Revue technique

- Les outils de gestion des vulnérabilités (ex : scanners de vulnérabilités comme Nessus) doivent être inspectés.
- Il doit être vérifié que les patchs critiques sont appliqués dans les délais recommandés.
- Les journaux des systèmes doivent être analysés pour détecter des attaques exploitant des vulnérabilités connues.

Entretiens humains

- Les équipes IT doivent être interrogées pour comprendre leur processus de gestion des vulnérabilités :
    - Comment les vulnérabilités sont-elles identifiées ?
    - Quel est le délai moyen pour appliquer des correctifs ?
- Une discussion doit être menée avec le RSSI pour comprendre la supervision des processus de remédiation.

Actions d'audit

- Il doit être validé que les vulnérabilités techniques sont identifiées et corrigées en temps opportun.
- Les rapports de scan de vulnérabilités doivent être vérifiés, et des actions de suivi doivent être mises en œuvre.

Exigence 5.35 : revue indépendante de la sécurité de l'information

Revue documentaire

- Les rapports d'audits indépendants passés sur la gestion de la sécurité doivent être consultés.
- La revue des objectifs de sécurité, politiques et mesures doit être vérifiée comme effectuée régulièrement.
- Les plans d'actions correctives mises en œuvre à la suite des audits doivent être examinés.

Revue technique

- Les outils utilisés pour suivre et superviser les audits indépendants doivent être vérifiés.
- Les preuves d'évaluation des mesures de sécurité (rapports, journaux) doivent être analysées.

Entretiens humains

- Les auditeurs internes ou externes doivent être interrogés :
  - Quelle est la fréquence des audits indépendants ?
  - Quels aspects de la sécurité sont priorisés ?
- Une discussion doit être menée avec la direction pour comprendre comment les résultats des audits sont utilisés pour améliorer les pratiques.

Actions d'audit

- Il doit être confirmé que des audits indépendants sont réalisés régulièrement.
- Les recommandations des audits doivent être validées comme étant suivies et mises en œuvre.

Tableau 1 : implémentations proposées pour compliance

Exigence	Plan de remédiation
5.8	- Formaliser une méthodologie de gestion de projet intégrant la sécurité à chaque phase (*analyse des risques, validation*). - Former les chefs de projet sur les pratiques de gestion des risques et la sécurité. - Automatiser les tests de sécurité sur les livrables à l'aide d'outils comme SonarQube.
8.1	- Déployer une solution MDM (*Mobile Device Management*) pour gérer les appareils mobiles. - Mettre en place une politique BYOD stricte (*chiffrement, segmentation des données pro/perso*). - Sensibiliser les collaborateurs aux risques liés aux appareils mobiles.

8.30	- Ajouter des clauses de sécurité dans les contrats des sous-traitants (audits réguliers, tests de sécurité). - Intégrer un processus de validation technique des livrables avant leur déploiement. - Mettre en place un suivi des sous-traitants avec des rapports de conformité réguliers.
5.27	- Créer un registre formalisé des incidents documentant les causes et actions correctives. - Organiser des revues périodiques des incidents et des ateliers pour partager les leçons apprises avec les équipes. - Simuler des scénarios types pour former les équipes SOC.
6.1	- Mettre en place un processus de vérification des antécédents pour les postes sensibles (*contrôles de casier judiciaire, clauses de confidentialité*). - Automatiser les vérifications grâce à des outils dédiés pour réduire les erreurs. - Sensibiliser les recruteurs sur l'importance des vérifications pour les postes liés à la sécurité.
7.2	- Installer des contrôles d'accès physiques avancés (*badges électroniques, caméras, alarmes*). - Séparer physiquement les zones sensibles (*serveurs, SOC*) des espaces accessibles au public. - Mettre en place une surveillance vidéo avec alertes automatiques pour les intrusions.
8.8	- Déployer un outil de gestion des vulnérabilités comme Nessus ou Qualys pour identifier et corriger les failles en temps réel. - Organiser des revues trimestrielles pour évaluer l'exposition de l'organisation aux nouvelles vulnérabilités. - Former les équipes techniques à appliquer rapidement les correctifs nécessaires.
5.35	- Planifier des audits internes annuels pour suivre l'évolution des objectifs de sécurité.

	- Impliquer un auditeur externe pour valider la conformité aux normes ISO 27001 ou RGPD. - Introduire des mécanismes de surveillance continue pour détecter les déviations en temps réel.

Étude de Cas - Société n°3 : **AgroNutriTech**

1. Contexte de l'Entreprise

1.1 Présentation de l'Entreprise

- **Nom** : AgroNutriTech
- **Secteur** : Agroalimentaire – Production et distribution de produits alimentaires biologiques.
- **Taille** : 120 collaborateurs répartis dans plusieurs pôles.
- **Clientèle** : Grandes surfaces bio, détaillants spécialisés, e-commerce.

1.2 Activités principales

- **Transformation des matières premières biologiques** : Transformation des fruits et légumes locaux en confitures, purées et jus bio.
- **Développement de nouvelles recettes** : Recherche et développement pour l'élargissement de la gamme de produits.
- **Distribution via des chaînes logistiques connectées** : Gestion des stocks et traçabilité via un ERP centralisé.
- **Conformité aux normes ISO 22000** : Engagement à respecter les standards de sécurité alimentaire et la protection des données personnelles des consommateurs.

2. Méthodologie

2.1 Sources d'Informations

1. **Revue documentaire** :
    a. Politiques de sécurité de l'information, rapports d'incidents, logs ERP.
    b. Contrats avec les sous-traitants, politiques RH.
2. **Revue technique** :
    a. Analyse des configurations ERP, tests de sécurité sur les logiciels et systèmes industriels (*SCADA, IoT*).
    b. Inspection des logs des systèmes industriels connectés pour s'assurer de la conformité.
3. **Entretiens humains** :
    a. Discussions avec le RSSI, chefs de projet, responsables IT et production pour obtenir des insights sur les pratiques et processus en place.

2.2 Actions d'Audit

- Identifier les écarts entre les politiques documentées et leur mise en œuvre réelle.
- Valider les configurations techniques et les preuves d'application des exigences.
- Confirmer avec les parties prenantes la compréhension et l'utilisation des bonnes pratiques.

3. Analyse des Exigences

3.1 Tableau d'applicabilité des exigences dans un contexte agroalimentaire

Exigence	Applicable	Justification
5.8 : Sécurité dans les projets	Oui	Nécessaire pour garantir que les projets (ex. nouveaux processus de production, logiciels de suivi qualité) intègrent la sécurité dès leur conception.
8.1 : Sécurité mobile	Oui	Les appareils mobiles sont utilisés pour accéder à l'ERP et surveiller la production ou les stocks en temps réel.
8.30 : Externalisation	Oui	Les prestataires gèrent certaines parties critiques comme le transport, la traçabilité ou les audits qualité.
5.27 : Retours incidents	Oui	Important pour éviter des incidents critiques comme la contamination alimentaire ou des interruptions de production.
6.1 : Vérifications à l'embauche	Oui	Garantit que les personnes accédant aux informations sensibles ou aux zones critiques sont fiables.
7.2 : Contrôle physique	Oui	Indispensable pour sécuriser les zones sensibles comme les laboratoires, chambres froides ou zones de stockage des matières premières.
8.8 : Gestion vulnérabilités	Oui	Permet de réduire les risques de cyberattaques ciblant les systèmes d'automatisation ou la traçabilité.

5.35 : Audits réguliers	Oui	Essentiel pour garantir la conformité réglementaire et la sécurité des données critiques (traçabilité, qualité).

3.2 Détails des exigences :

Exigence 5.8 : Intégration de la sécurité dans la gestion de projet

Revue documentaire :

- Vérifier l'intégration des étapes de sécurité dans les projets spécifiques à l'agroalimentaire, tels que le développement de nouvelles recettes ou l'intégration de la traçabilité dans l'ERP.
- Analyser les plans de projet pour s'assurer que la sécurité est prise en compte tout au long du cycle de vie des projets.
- Vérifier si des étapes spécifiques à la sécurité alimentaire (*respect des normes ISO 22000*) sont incluses dans les projets de transformation et de développement de nouveaux produits.

Revue technique :

- Inspecter les outils de gestion de projet utilisés (*Jira, Trello*) pour vérifier la création de tickets liés à la sécurité des projets.
- Analyser les résultats des tests de sécurité réalisés sur les livrables (*utilisation d'outils comme SonarQube ou des scanners de vulnérabilités*).

Entretiens humains :

- **Questions aux chefs de projet** :
  - "Comment la sécurité est-elle intégrée dans vos projets agroalimentaires ?"
  - "Quels tests de sécurité sont réalisés avant la mise en production des nouvelles recettes ?"
- Discussions avec le **RSSI** pour comprendre son rôle dans la validation des livrables et de la traçabilité des produits.

Actions d'audit :

- Examiner les plans de projet récents pour vérifier les étapes de sécurité, notamment dans la production alimentaire et la gestion des données des consommateurs.
- Valider la mise en œuvre des pratiques via des tests concrets sur les projets critiques, comme l'implémentation de nouvelles gammes ou l'amélioration du système de gestion des stocks via ERP.

Exigence 8.1 : Sécurisation des appareils mobiles

Revue documentaire :

- Vérifier la politique BYOD et les exigences de chiffrement, VPN et MFA, en particulier pour les employés mobiles travaillant dans les zones de production ou dans le laboratoire de R&D où des informations sensibles (*comme les recettes ou les analyses de produits*) sont manipulées.
- Examiner les manuels MDM pour comprendre la gestion des appareils mobiles et des terminaux connectés à l'ERP.

Revue technique :

- Analyser les configurations MDM (*Mobile Device Management*) pour évaluer les politiques de sécurité appliquées (*chiffrement des appareils, mises à jour régulières, contrôles d'accès*).
- Inspecter les logs d'accès aux systèmes ERP depuis les appareils mobiles pour détecter d'éventuelles anomalies ou violations de sécurité.

Entretiens humains :

- **Questions aux équipes IT** :
  - "Quels appareils mobiles ont accès aux systèmes ERP et à la gestion des stocks ?"
  - "Comment les appareils personnels des employés sont-ils sécurisés ?"
- Discussions avec le **RSSI** pour comprendre comment les politiques BYOD sont appliquées dans les zones sensibles comme la production et la logistique.

Actions d'audit :

- Examiner les configurations MDM pour vérifier les restrictions sur les appareils mobiles et les dispositifs de sécurité appliqués.
- Tester l'accès aux systèmes depuis des appareils non conformes pour évaluer les contrôles de sécurité en place.

Exigence 8.30 : Supervision des développements externalisés

Revue documentaire :

- Examiner les contrats des sous-traitants (*en particulier ceux pour le développement ERP et la gestion des données clients*) pour vérifier les clauses de sécurité, notamment sur la gestion des données sensibles (*données des clients, recettes de produits*).
- Vérifier la documentation des livrables (*code source, rapports de tests de sécurité*) fournis par les prestataires externes.

Revue technique :

- Inspecter les livrables pour évaluer leur conformité aux normes de sécurité (*par exemple, OWASP pour les applications web, ISO 27034 pour les pratiques de développement sécurisé*).
- Analyser les résultats des tests de pénétration réalisés sur les logiciels livrés par les prestataires pour s'assurer qu'ils répondent aux exigences de sécurité.

Entretiens humains :

- Discussions avec les responsables des projets externalisés :
  - "Quels processus sont en place pour garantir la sécurité des livrables ?"
- **Questions aux sous-traitants** :
  - "Quelles normes de sécurité respectez-vous dans le développement des logiciels, notamment pour les systèmes ERP utilisés dans l'agroalimentaire ?"

Actions d'audit :

- Examiner les contrats pour s'assurer que les exigences de sécurité sont clairement spécifiées, en particulier pour la gestion de la traçabilité et des informations sensibles.
- Réaliser une revue de code des livrables externes ou un test de pénétration si nécessaire.

Exigence 5.27 : Exploitation des leçons issues des incidents

Revue documentaire :

- Analyser les registres **des incidents** pour vérifier les **causes profondes** des incidents passés, notamment ceux liés à des failles de sécurité dans les systèmes de traçabilité ou la gestion des stocks.
  - Vérifier les **actions correctives** prises après chaque incident et la mise à jour des processus pour éviter leur récurrence.
- Vérifier la documentation des **revues post-incident** pour s'assurer que les **leçons apprises** sont bien partagées à travers l'entreprise.

Revue technique :

- Inspecter les **logs d'incidents** collectés par le SOC (*Security Operations Center*) pour identifier les incidents liés à des vulnérabilités dans les systèmes ERP ou industriels (*IoT, SCADA*).
- Valider les **indicateurs de performance** des incidents (*temps de résolution, fréquence*) pour déterminer si les actions correctives ont été efficaces.

Entretiens humains :

- **Discussions avec les équipes SOC et IT** pour comprendre comment les incidents sont gérés, documentés et analysés.
- **Questions au RSSI** pour savoir comment les **leçons tirées des incidents** sont communiquées et intégrées dans les pratiques de sécurité de l'entreprise.

Actions d'audit :

- Examiner les **rapports d'incidents** pour vérifier que les actions correctives ont été suivies et mises en œuvre.
- Confirmer que des **mécanismes de retour d'expérience** sont en place pour éviter la récurrence d'incidents similaires.

Exigence 6.1 : Vérifications à l'embauche

Revue documentaire :

- Analyser les politiques RH et les pratiques actuelles en matière de recrutement pour s'assurer qu'elles incluent des vérifications de base (*antécédents criminels, qualifications, expériences*).
- Valider que les employés manipulant des données sensibles ou travaillant dans des zones critiques (*ERP, R&D*) font l'objet de vérifications supplémentaires adaptées aux risques.

Revue technique :

- Aucun outil spécifique requis, mais vérifier si une liste standardisée des vérifications nécessaires est utilisée dans les systèmes RH.

Entretiens humains :

- Discussions avec le département RH pour comprendre les processus de vérifications actuels et leur fréquence.

Actions d'audit :

- Intégrer une politique formelle pour les vérifications d'antécédents, spécifiquement pour les postes IT, logistique et R&D.

Exigence 7.2 : Contrôle physique

Revue documentaire :

- Vérifier la présence de politiques décrivant les accès aux zones sensibles (*labo R&D, entrepôts*).
- S'assurer qu'une liste des zones sensibles est documentée et régulièrement mise à jour.

Revue technique :

- Inspecter les dispositifs physiques en place : lecteurs de badges, caméras, serrures électroniques.
- Tester les accès non autorisés en tentant d'entrer dans une zone critique sans badge valide.

Entretiens humains :

- Discussions avec les responsables logistique et sécurité pour comprendre les procédures en place (*gestion des badges, accès visiteurs*).

Actions d'audit :

- Renforcer les contrôles en ajoutant des caméras intelligentes avec détection de mouvement dans les zones critiques.
- Mettre en place des audits réguliers pour s'assurer que les accès sont révisés périodiquement.

Exigence 8.8 : Gestion des vulnérabilités

Revue documentaire :

- Examiner les politiques de gestion des vulnérabilités, incluant les processus de détection, d'évaluation et de correction des failles.
- Valider que des cycles réguliers de mises à jour et de patching sont documentés.

Revue technique :

- Vérifier l'utilisation d'outils tels qu'OpenVAS, Nessus ou Qualys pour scanner les infrastructures internes et exposées.
- Évaluer la fréquence et la portée des scans, ainsi que le délai moyen de correction des vulnérabilités identifiées.

Entretiens humains :

- Discussions avec l'équipe IT et le RSSI sur les processus d'identification et de correction des failles.

Actions d'audit :

- Automatiser les scans hebdomadaires pour l'ensemble du réseau interne et des systèmes ERP.
- Prioriser les vulnérabilités critiques avec un délai de correction maximum de 72 heures.

Exigence 5.35 : Audits réguliers

Revue documentaire :

- Vérifier si un plan d'audit annuel est en place, couvrant les aspects techniques, organisationnels et physiques.
- S'assurer que les audits incluent une évaluation de conformité réglementaire (*ISO 22000, RGPD*).

Revue technique :

- Aucun outil spécifique, mais évaluer si des outils de suivi des non-conformités (*par exemple, des trackers ou solutions GRC*) sont utilisés.

Entretiens humains :

- Discussions avec le RSSI pour comprendre la fréquence et la méthodologie des audits internes et externes.

Actions d'audit :

- Instituer une revue semestrielle pour les zones critiques comme l'ERP et les dispositifs de traçabilité.
- Documenter systématiquement les écarts et assigner des responsabilités claires pour les actions correctives.

Tableau 1 : Plan de remédiation spécifique à l'agroalimentaire

Exigence	Plan de Remédiation
5.8 : Sécurité dans les projets	- Formaliser une méthodologie de gestion de projet intégrant la sécurité agroalimentaire à chaque phase (ex. *analyse des risques sur la chaîne de production*). - Former les chefs de projet sur les normes ISO 22000 et les pratiques de gestion des risques agroalimentaires. - Automatiser les tests de sécurité IT spécifiques aux systèmes d'automatisation industriels.
8.1 : Sécurité mobile	- Déployer une solution MDM (*Mobile Device Management*) pour sécuriser les terminaux mobiles utilisés pour surveiller les stocks et la production. - Implémenter une politique BYOD stricte incluant le chiffrement des données sensibles (ex. *recettes, analyses de production*). - Former les collaborateurs sur les risques liés à l'accès mobile aux applications critiques (*ERP, suivi qualité*).

8.30 : Externalisation	- Ajouter des clauses spécifiques dans les contrats des sous-traitants pour assurer la conformité avec les normes agroalimentaires (ex. *audits réguliers de sécurité IT et physique*). - Valider les systèmes externalisés liés à la traçabilité et à la logistique via un pipeline CI/CD sécurisé. - Mettre en place un reporting régulier des sous-traitants sur la conformité et les mesures correctives.
5.27 : Retours incidents	- Mettre en place un registre centralisé des incidents liés à la sécurité des données sur les matières premières ou les produits finis. - Organiser des revues trimestrielles avec les équipes qualité et IT pour discuter des incidents. - Simuler des scénarios d'incidents critiques (ex. *rupture de chaîne de froid, failles dans le suivi de traçabilité*).
6.1 : Vérifications à l'embauche	- Mettre en place un processus de vérification des antécédents pour les postes sensibles (ex. *gestion des stocks, R&D*). - Automatiser les vérifications des dossiers des nouveaux employés. - Former les équipes RH sur l'importance des vérifications pour les postes impactant la chaîne de production.
7.2 : Contrôle physique	- Installer des contrôles d'accès renforcés dans les zones critiques (*chambres froides, laboratoires, zones de stockage*). - Séparer physiquement les zones R&D (*recettes, données sensibles*) des espaces de production accessibles. - Implémenter un système de surveillance vidéo avec alertes automatiques en cas d'intrusion.
8.8 : Gestion des vulnérabilités	- Déployer un outil comme Nessus pour surveiller en continu les systèmes industriels (*SCADA, ERP*). - Planifier des revues trimestrielles des vulnérabilités spécifiques aux logiciels d'automatisation et de contrôle qualité. - Former les équipes IT et qualité à appliquer rapidement les correctifs de sécurité sur les équipements critiques.

5.35 : Audits réguliers	- Organiser des audits internes annuels pour évaluer la sécurité des données sur la traçabilité et la conformité aux normes ISO 27001 et ISO 22000. - Solliciter un auditeur externe pour vérifier la robustesse des systèmes IT dans le contexte de la chaîne d'approvisionnement. - Mettre en place un système de surveillance continue pour identifier rapidement les écarts de conformité.