🎯 Audit de sécurité : ce moment gênant où l'on découvre l'envers du décor 🎭🔎

5 juillet 2025

Table des matières

🤔 Pourquoi faire un audit de sécurité ?

Parce que « chez nous, tout va bien » est souvent le plus grand mensonge depuis « j'ai lu les CGU ». Parce que croire que son SI est sécurisé **sans jamais l'avoir vérifié**, c'est un peu comme prendre l'autoroute à contresens… en espérant que les autres freineront.

Un audit de sécurité n'est pas une punition. Ce n'est pas un stress-test pour faire pleurer l'admin système ou faire transpirer le DSI. C'est un **examen de santé numérique** (complet, parfois douloureux, mais salutaire) qui permet :

✅ D'identifier les failles connues (et méconnues)
✅ De voir si les bonnes pratiques sont vraiment appliquées
✅ De vérifier que ce qui est écrit dans la PSSI n'est pas que littérature
✅ D'éviter de se retrouver en Une de *BleepingComputer*

En bref : un audit, c'est **l'occasion rêvée de se remettre en question avant que les cybercriminels ne s'en chargent**.

🥷 L'audit de sécurité, ce n'est PAS un pentest

Oui, le pentest est sexy. Il y a du scan, des scripts, des alertes qui clignotent, des consultants avec des pseudos de films d'action. Mais **ce n'est qu'une partie de l'audit**, pas l'audit lui-même.

Un **audit de sécurité**, c'est plus large :
🗂️ On regarde les processus,
🖥️ On inspecte les configurations,
👥 On analyse les rôles et responsabilités,
📄 Et on lit vos logs, vos documents, vos procédures (oui, même les vieux .doc de 2015).

C'est **structuré**, **documenté**, **argumenté**.
Le pentest, c'est le tir de sniper. L'audit, c'est la cartographie complète du champ de bataille, les bottes dans la boue.

🧭 I.A – Définir le périmètre (et éviter le flou artistique façon brouillard de guerre)

Avant même de parler de tests, de méthodes ou de livrables, il faut commencer par la base : **savoir ce qu'on audite**.
Ça paraît évident ? 🧐 Pas tant que ça.

📌 Le périmètre, ce n'est pas « le SI dans son ensemble » (merci, mais non merci)

Quand un DSI te dit :

« Vous pouvez auditer tout le système d'information, hein, on est transparents ici ! »

…ça sent généralement soit l'impro, soit le piège.
Un **audit sans périmètre clair**, c'est comme demander à un plombier de « vérifier toute la plomberie du pays ».
Tu risques un audit long, confus, frustrant… et inexploitable. Ou pire : tu oublies justement les zones les plus critiques.

🧱 Délimiter, c'est sécuriser… l'audit lui-même

Un bon périmètre, c'est :

- Une **liste claire des systèmes, applications, sites, réseaux** concernés
- Les **environnements concernés** : prod ? préprod ? les deux ?
- Les **technos cibles** : cloud, legacy, API, IoT, postes de travail ?
- Les **règles du jeu** : heures d'intervention, tests autorisés ou non, zones à exclure, etc.

Et ce périmètre doit être **formalisé noir sur blanc** : un mail, c'est gentil. Un doc signé, c'est mieux.

🔎 Ce qu'il ne faut JAMAIS faire :

- ❌ Dire « on verra au fil de l'audit » → traduction : on n'a aucune idée de ce qu'on veut.
- ❌ Oublier une brique critique (genre… Active Directory, le Wi-Fi invité ou la plateforme RH cloud).
- ❌ Négocier les exclusions *après* avoir trouvé une faille embarrassante.
- ❌ Laisser l'auditeur découvrir seul le périmètre (spoiler : il va le trouver… et vous ne serez pas ravis).

🎯 Pourquoi c'est crucial

Un périmètre mal défini, c'est :

- Une **perte de temps** pour tout le monde
- Des **résultats biaisés** (ça donne l'illusion d'un SI nickel alors qu'on n'a audité que la partie « jolie »)
- Un **risque juridique** si l'auditeur touche à une zone hors cadre, en production par exemple (et fait tomber un service essentiel 🧨)

💡 Astuce de vétéran

Toujours commencer par un **schéma d'architecture simplifié** (même dessiné sur un tableau). Identifier :

- Les briques critiques (AD, ERP, cloud, sauvegardes)
- Les interfaces sensibles (VPN, extranet, liens inter-sites)
- Les zones à haut risque (IoT, applis maison, Shadow IT…)

Et de là, définir **un périmètre utile et exploitable**. Quitte à faire plusieurs audits en plusieurs phases, **plutôt qu'un seul audit bancal et indigeste**.

🧨 I.B – Évaluer les risques cyber (et pas juste ce qui fait peur aux ComEx)

Ah, les risques cyber… Ce moment magique où tout le monde a une opinion : le DSI voit des ransomwares dans chaque coin d'e-mail, le RSSI ne dort plus à cause des accès partagés, et le DG s'inquiète uniquement pour le phishing "parce qu'un copain s'est fait avoir".

Sauf que dans un audit sérieux, on ne travaille pas à l'instinct, **on évalue les risques avec méthode**. Fini les « ça me semble risqué », place aux analyses un peu moins au doigt mouillé. 🤭

🔍 Un risque, ce n'est pas juste une faille

Une faille technique, c'est une porte laissée ouverte.
Un risque, c'est ce qui se passe si quelqu'un passe par cette porte, chez vous, maintenant. Avec des conséquences.
Et c'est là toute la différence entre un audit utile… et un audit panique.

🎲 Évaluer les risques, ce n'est pas jouer à la roulette russe

Il faut évaluer :

- **La vraisemblance** (probabilité que ça arrive)
- **L'impact** (sur les données, la production, la réputation)
- **Le contexte** (type d'activité, exposition à internet, historique, maturité SSI…)

Et pour ça, on ne fait pas juste un tableau Excel en rouge-jaune-vert à la va-vite.
On utilise de **vraies méthodes**, comme :

- **EBIOS RM** 🇫🇷 (ANSSI) – pour cartographier menaces, événements redoutés, impacts (voir notre article)
- **NIST 800-30** 🇺🇸 – pour une approche risk-based en mode US
- **MEHARI** – pour les puristes old school

- Ou des outils maison, tant qu'ils sont logiques et documentés

---

🔥 « On a 400 vulnérabilités… mais c'est pas grave »

Une entreprise avait fait scanner tout son SI : résultat, 400 vulnérabilités.
Panique générale.
Mais à l'analyse : 80% étaient sur une appli obsolète, **isolée du réseau**, **hors service**, **non exposée**.
Impact réel ? Proche du zéro.
➡️ Le seul vrai risque identifié dans l'audit : un serveur de sauvegarde exposé en SMBv1… que personne n'avait noté car "pas critique".

Moralité : une **faille isolée et oubliée peut être bien plus dangereuse** qu'un lot de CVE bruyantes mais contenues.

🎯 Risque ≠ bruit

Évitez les effets "Wahou" :

- ❌ Un site WordPress vulnérable à XSS dans un sous-domaine oublié ≠ catastrophe
- ❌ Un port 22 ouvert dans la DMZ ≠ apocalypse (sauf si mot de passe = « 123456 »)

👉 **Un bon audit remet les risques en perspective**, en croisant technique et métier :

- Cette faille, dans CE contexte, avec CET accès, a-t-elle un vrai potentiel d'exploitation ?
- Et quelles seraient les conséquences SI elle était exploitée ?

💡 Astuce de pro

Faites toujours valider l'évaluation des risques **avec les métiers** :

- Le service finance n'a pas la même tolérance au risque que la DSI
- Une appli obsolète peut contenir des données RH oubliées
- Un poste utilisateur mal protégé peut accéder à 10 partages réseau "temporaires"

➡️ L'audit doit **croiser les mondes** : celui du technique et celui du réel. Sinon, vous ferez un super rapport… qui n'ira nulle part.

🛠️ I.C – Choisir les types et portées d'audit

(…et éviter les audits Ikea mal montés : tout est là, mais rien ne tient droit)
Dans le monde merveilleux de la cybersécurité, il existe plusieurs types d'audit. Et comme chez Ikea, si tu prends toutes les pièces sans lire la notice, tu vas finir avec un meuble bancal, un audit incomplet… et une furieuse envie de tout brûler. 🔥

🧱 L'audit, ce n'est pas un menu unique

Un **audit de sécurité**, ce n'est pas juste « on va tester un peu les failles et hop ». Il faut choisir :

- **Le type d'audit**
- **La portée fonctionnelle et technique**
- **Le niveau d'intrusivité**
- **Et surtout : la finalité**

📦 Les différents types d'audit (aka "le catalogue")

1. **Audit organisationnel** 👨‍💼
    - Revue de la gouvernance SSI, des procédures, de la PSSI, de la gestion des incidents.
    - Exemples : plan de continuité, politique des mots de passe, sensibilisation des utilisateurs.

- ➕ Souvent négligé… mais critique.

2. **Audit technique** 💻
   - Tests d'intrusion, configuration des firewalls, scan de vulnérabilités, audit de code source, sécurité des postes.
   - ➕ Le plus populaire, parce qu'il fait peur et qu'il génère des jolis rapports avec des CVE.
3. **Audit physique** 🔐
   - Accès aux salles serveurs, caméras, badges, sécurité périmétrique.
   - ➕ Rarement demandé, sauf par des paranoïaques (souvent à raison).
4. **Audit de conformité** 📜
   - Vérification des écarts entre le réel et le théorique (ISO 27001, NIS2, RGPD, HDS…).
   - ➕ Pour prouver qu'on coche les cases (ou pas).
5. **Audit applicatif** 🧩
   - Revue de sécurité des applications internes : gestion des droits, logique métier, traitement des entrées, etc.
   - ➕ À faire AVANT la mise en prod (pas après le piratage).

🧪 Portée de l'audit : vous avez dit "large" ?

C'est tentant de dire "on va tout faire"…
Mais un audit XXL, sans découpage ni priorisation, c'est l'assurance d'avoir :

- Un rapport indigeste
- Une perte de focus
- Et un DSI qui ne lit que le résumé exécutif (et encore…)

👉 Mieux vaut cibler intelligemment :

- Par périmètre technique (cloud, AD, réseau interne…)
- Par enjeux métier (application RH, outil compta, infra critique…)
- Par niveau de maturité SSI (on commence par les zones les plus sensibles/fragiles)

🤹 Niveau d’intrusivité

Audit **interne, externe, boîte noire, boîte grise, boîte blanche**… On se croirait dans un épisode de *Masterchef*.

Petit rappel :

- **Boîte noire** : l’auditeur n’a aucune info → test d’intrusion pur, simulation réelle
- **Boîte grise** : accès limité, simule un attaquant interne ou un utilisateur
- **Boîte blanche** : accès complet → permet d’aller plus vite, plus profond, plus chirurgical

Chaque méthode a son utilité… mais il faut savoir ce qu’on cherche.
Spoiler : si on veut *vraiment* trouver les failles d’AD, mieux vaut pas y aller en mode aveugle.

🔥 “On voulait un pentest… mais on n’a rien compris au rapport”

Une entreprise commande un test d’intrusion « en mode boîte noire totale » pour évaluer la sécurité externe.
Résultat : l’auditeur n’a trouvé *aucune faille exploitable* (tant mieux ?).
Mais l’entreprise, frustrée, déclare :

« On pensait qu’il allait tout tester, même nos applis internes, notre AD, nos sauvegardes, tout ça quoi… »
🛬 Sauf que ça… ce n’était PAS dans la portée. 🤌
*Ils ont confondu **pentest externe limité** et **audit global**. Et payé 12k€ pour un rapport vide. Bravo l’effet waouh.*

💡 Astuce de survie

Avant de démarrer un audit, posez toujours :

- 📋 Les **objectifs précis** : qu’est-ce qu’on veut apprendre ?
- 🧠 Le **contexte** : technique, métier, contraintes

- 📂 Le **type d'audit adapté**
- ⛳ Et la **portée** : quoi, où, quand, comment

Sinon, vous finirez avec un rapport qui commence par :

« L'objectif de cet audit n'étant pas clairement défini… »
…et ça, c'est jamais bon signe 😅

🐜 I.D – Ne pas ignorer les vulnérabilités faibles

(…ou comment une microfaille peut ruiner ton week-end. Et celui du RSSI. Et celui du PDG.)

Quand on lit un rapport d'audit, on a tous un réflexe conditionné :
🟥 Critique ? → PANIQUE
🟧 Élevée ? → ALERTE
🟨 Moyenne ? → ON VERRA
🟩 Faible ? → *Poubelle, merci, suivant.*

➡️ Mauvaise idée. Très mauvaise.
Les petites failles, les CVE sans éclat, les « infos only » ou « low severity », ce sont souvent **les vraies bombes à retardement**.

⚠️ Une faille faible ≠ un risque faible

Une vulnérabilité « faible », c'est une **étiquette technique**.
Le **risque**, lui, dépend du **contexte** :

- Une page admin sans authentification ? Faible… sauf si elle permet d'exécuter du code.
- Une version PHP obsolète ? Faible… sauf si exposée sur Internet.
- Une erreur de configuration dans une appli interne ? Faible… sauf si l'appli est utilisée par toute la direction.

🔥 « Juste un header qui fuitait, ça va hein »

Un auditeur signale qu'un serveur expose un **bête header HTTP avec sa version Apache**.
Réponse du client :

« C'est noté, mais franchement ça, c'est du détail. Qui lit les headers ? »
➡️ Six mois plus tard : compromission via une vulnérabilité connue sur cette version-là, pile poil.
Le pirate a scanné, trouvé le header, lancé l'exploit.
Conclusion : une ligne de texte "faible", une compromission critique, et un DSI en mode Damage Control.

🔥 « Mais c'est une fausse faille ! »

Un scan automatique détecte une injection de type "reflected XSS" dans un formulaire oublié.
Le RSSI balaie ça d'un revers de main :

« C'est dans une page d'erreur d'un sous-sous-site d'une appli jamais utilisée. Aucun intérêt. »
*➡️ Sauf que ce bout de code est **encore présent en prod**, **accessible sans auth**, et utilisé par… un bot indexeur tiers.*
Résultat : le XSS a été exploité via un lien malicieux envoyé à un utilisateur interne → session volée.

Tout ça pour une « faille de test ».

👈 Pourquoi elles sont dangereuses

- Elles passent souvent sous le radar
- Elles ne déclenchent pas d'alerte immédiate
- Elles sont **idéales pour pivoter** ou préparer une attaque plus sérieuse

- Elles sont **parfaites pour les attaquants patients**, les scripts d'automatisation ou les APT

🧠 Mentalité à adopter

👉 Une vulnérabilité « faible », c'est un **point d'entrée possible**.
Et un SI bien sécurisé, ce n'est pas juste un mur épais.
C'est un mur **sans fissure**, même fine.

En clair :

*« Ce n'est pas critique aujourd'hui » ne doit **jamais** signifier « ce n'est pas à traiter ».*

💡 Astuce pour le rapport d'audit

Quand vous traitez les vulnérabilités faibles :

- ✅ Mentionnez le **scénario d'exploitation possible**
- ✅ Indiquez les **conditions d'exploitation** (accès, prérequis, enchaînements)
- ✅ Mettez en lien avec d'autres failles potentielles (effet domino)

➡️ Ça aide à comprendre que le **danger vient souvent de la combinaison** de plusieurs faiblesses.

🧰 I.E – Ne pas ignorer les contraintes et limites d'un audit

(spoiler : l'auditeur n'est pas Dieu… et encore moins technicien polyvalent en CDI chez vous)

Faire un audit de sécurité, c'est essentiel. Mais croire qu'un auditeur va tout voir, tout tester, tout comprendre et corriger *en bonus*, c'est un peu comme appeler un

médecin pour un check-up et lui demander d'opérer à domicile… avec une cuillère.

⚖️ L'audit, c'est un état des lieux, pas une réparation

L'audit :

- Observe 🧐
- Analyse 🧠
- Signale 📣
- Propose 📄

Mais il ne **corrige pas**, **ne garantit pas**, et **ne promet pas de tout découvrir**.
Et surtout, il **ne remplace pas les équipes internes**.

Si vous attendez qu'il redémarre vos serveurs après avoir signalé une mauvaise conf, vous allez attendre longtemps.

🤖 L'auditeur n'a pas de super-pouvoirs

L'auditeur travaille avec ce qu'on lui donne :

- Des accès (ou pas)
- Des documents (parfois vieux de 10 ans)
- Des interlocuteurs (parfois très très absents)
- Et un délai (souvent très très court)

⚠️ Résultat :

S'il n'a pas les accès aux logs, il ne les lira pas.
S'il n'a pas de doc réseau, il ne devinera pas la topologie.
Et s'il découvre seul une VM oubliée, ce n'est pas de la magie, c'est de la négligence côté client.

🔥 « Vous n’avez pas trouvé cette faille ?! »

Client outré en fin d’audit :

“Vous êtes passés à côté d’un serveur Windows vulnérable, exposé en 3389 !”

Sauf que… ce serveur :

- Était **dans une DMZ non déclarée**
- Était **hors périmètre**
- N’apparaissait **nulle part dans la doc fournie**

Réponse de l’auditeur :

“Désolé, je n’ai pas la licence de clairvoyance dans mon forfait.” 🧙‍♂️

🔥 « On pensait que vous alliez corriger les failles »

Lors d’un audit technique, l’équipe sécurité reçoit le rapport et demande :

“OK, donc vous corrigez tout ça maintenant ?”
Non.
L’audit n’est pas une prestation de remédiation.
“Mais vous les avez trouvées, donc vous savez les corriger, non ?”
*Peut-être. Mais l’auditeur, lui, n’est **ni votre admin**, **ni votre prestataire de patching**, **ni votre assistant RSI**.*

🧩 Ce qu’un audit NE PEUT PAS faire :

- 🔮 Prédire toutes les failles futures
- 🧰 Remplacer une politique de sécurité
- 👷 Réparer les erreurs de conf

- 📡 Scanner ce qui est caché, non déclaré ou « oublié dans un coin »
- 🤐 Se substituer à vos responsabilités internes

👉 Il **vous aide à voir clair**, pas à faire le ménage à votre place.

💡 Astuce pro : poser des limites claires

Un bon audit, c'est aussi un audit **bien cadré** :

- Délais définis
- Périmètre verrouillé
- Contraintes techniques listées (accès VPN, environnement sensible, maintenance en cours…)
- Risques acceptés (tests en prod ? simulateur ou réel ? outils actifs ou passifs ?)

Et surtout : **des attentes réalistes**.
Ce n'est pas le grand nettoyage de printemps, c'est l'inspection avec lampe torche et mètre ruban.

🚫 II – Ce qu'un audit de sécurité n'est PAS

(…et autres mythes qu'on devrait inscrire sur les mugs des comités SSI)

❌ 1. Un audit, ce n'est pas une chasse aux sorcières 🧙

L'objectif n'est pas de :

- Trouver LE coupable
- Humilier l'admin qui a oublié de patcher un Windows 2012
- Ou imprimer un rapport rouge écarlate à faire signer au PDG sous Lexomil

Un audit bien mené, c'est :
✅ Une **photographie à l'instant T**
✅ Une **aide à la décision**
✅ Et surtout, **un outil de pilotage**, pas une séance de blâme publique.

Et si votre RSSI utilise l'audit pour régler ses comptes avec l'équipe infra, c'est que vous avez un problème d'équipe… pas de sécurité.

❌ 2. Ce n'est pas une certification magique 🪄

« Ah super, on a fait un audit ! Donc on est sécurisés, non ? »
Non. Non. Et encore non.

Faire un audit ≠ être conforme
Faire un audit ≠ être protégé
Faire un audit ≠ avoir corrigé quoi que ce soit

C'est juste **le début** du travail.
Et parfois, c'est même le moment où l'on découvre que le travail va être… long.
Très long.

❌ 3. Ce n'est pas un outil marketing (en tout cas pas tout de suite) 📣

Oui, certaines boîtes aiment afficher :

"Audit de sécurité réalisé en 2024 – Conforme aux standards de l'industrie 🏅"

Mais :

- Est-ce que les vulnérabilités ont été corrigées ?
- Est-ce que l'audit a couvert tous les systèmes ?
- Est-ce que le plan d'action est suivi ?

- Est-ce que ça a été revérifié depuis ?

Sinon, c'est du **greenwashing numérique** : on a passé un scan, on a lu le rapport, et on a rangé ça avec les factures.

❌ 4. Ce n'est pas un outil de flicage interne 👮

Non, un audit n'a pas vocation à :

- Surveiller les utilisateurs
- Fliquer les admins
- Pister "qui a cliqué sur le lien de phishing en 2019"

C'est un **processus structuré, bienveillant (en théorie)**, qui vise à **élever le niveau global de sécurité**, pas à faire peur à tout le monde.

Et puis entre nous : si l'auditeur a vraiment envie de jouer les flics, il finira chez la CNIL, pas dans votre SI.

❌ 5. Ce n'est pas une solution miracle 🙏

« On a des problèmes de sécurité, faisons un audit. »
Très bien.
Mais ensuite ?

« Ah… il faut lire le rapport ? Et appliquer les recommandations ? Et suivre un plan d'action ? Et refaire un audit plus tard ? »

➡️ Oui.
Un audit, c'est comme aller chez le médecin :
Il t'annonce que tu fumes, que tu manges mal, et que tu dors 4h par nuit… mais c'est **à toi de changer tes habitudes**.

🔥 “Le rapport ? Non, on ne l’a pas encore lu…”

Une entreprise fait un audit complet.
Trois mois plus tard, l’auditeur appelle pour savoir si les recommandations ont été appliquées.
Réponse :

“Ah, on ne vous a pas payé pour la restitution ? Le rapport doit encore traîner dans la boîte mail du DSI.”

➡️ Le PDF est resté non lu. Zéro correction. Et deux mois plus tard : ransomware.
Moralité : **le meilleur audit du monde ne sert à rien si on l’enterre dans une armoire virtuelle.**

💡 Résumé rapide (à imprimer sur un mug) :

Cliché	Réalité
“L’audit va nous sécuriser”	Non, il va vous alerter
“L’auditeur va tout voir”	Non, il voit ce qu’on lui montre
“On est bons, c’est vert partout”	Non, vous êtes bons là où on a regardé
“C’est pour accuser les gens”	Non, c’est pour faire mieux, ensemble
“On fera les actions plus tard”	Non, vous ferez les attaques plus tôt 😬

🔪 III. Gouvernance, procédures et documentation : le vrai terrain de l'audit

🧠 L'audit, ce n'est pas "juste" de la technique

Certains s'imaginent que l'audit, c'est du hacking en semi-clair, quelques scripts lancés depuis Kali ou Burp Suite, un scanner Nessus, et un rapport coloré.
Mais **le vrai révélateur**, celui qui met le doigt là où ça fait mal,
c'est **l'organisation** : la manière dont on structure la sécurité **au quotidien**.

Il y a un piège dans l'imaginaire collectif (surtout chez les techs barbus et les Comex pressés) :

L'audit, c'est juste un mec qui cherche des failles.
Et si on a un bon antivirus et une équipe réactive, c'est bon.

Eh bien non.
Un audit, c'est aussi vérifier si **les processus de gestion du risque cyber existent… et fonctionnent.**
Et là, on entre dans le monde merveilleux de la **documentation**, des **rôles**, des **procédures**, et du **pilotage de la SSI**. Oui, ce monde où les fichiers Excel vivent plus longtemps que certains serveurs. 🧟

En clair :

Pas besoin de failles zero-day quand une entreprise n'a aucun plan, aucune procédure, et zéro suivi.

🧾 Ce que l'auditeur veut voir (et que vous redoutez parfois de lui montrer)

🔥 *1. Une procédure de gestion des incidents*

🛑 Qui fait quoi quand la merde arrive ?
Un bon audit va chercher s'il existe une procédure :

- Déclenchement (qui déclare l'incident ?)
- Investigation (qui centralise ? qui isole ?)
- Communication interne/externe (RSSI, Com, DG, DPO…)
- Retour d'expérience (post mortem documenté ou simple pizza-partie ?)

➡️ Sans cette procédure, vous improvisez. Et en cybersécurité, l'impro… ça finit rarement bien.

🔄 *2. Un PRA/PCA clair, testé, documenté*

Le PRA (Plan de Reprise d'Activité) et le PCA (Plan de Continuité) sont des piliers :

- En cas de ransomware ou d'incident majeur
- En cas de panne, incendie, vol, ou attaque ciblée
- Pour éviter que l'activité ne s'arrête… ou que le DG panique en direct à la radio

Un audit va chercher :

- Les **scénarios testés**
- Les **RTO/RPO documentés**
- La **liste des services critiques**
- La **date du dernier test réel** (pas la réunion où on a dit "on devrait tester un jour")

💣 Anecdote véridique : entreprise attaquée → PCA de 2020 non mis à jour, responsable absent, test jamais réalisé = chaos total pendant 4 jours. L'audit suivant a été… corsé.

« En cas de ransomware, combien de temps mettez-vous à redémarrer l'activité ? »

Souvent :

- « Ça dépend… »
- « On a des sauvegardes ! » (🤦)
- « On n'a jamais testé, mais normalement ça devrait marcher. On prie ?!! «

📋 3. Une cartographie des actifs (pas juste dans la tête du sysadmin)

Si personne ne sait :

- Quels sont les serveurs critiques
- Où se trouvent les bases de données sensibles
- Quel est le périmètre du cloud
  ➡️ … l'auditeur le saura avant vous. Et il ne sera pas content.

🧟 Anecdote : "On ne savait pas que ce serveur existait encore." — Phrase prononcée dans 70% des audits, au moment où l'auditeur tombe sur une machine oubliée, exposée, non patchée depuis 2017. (Elle tourne très bien… pour l'attaquant.)

👑 4. Une vraie gouvernance SSI

L'auditeur cherche :

- Qui est responsable (RSSI ? DSI ? prestataire ?)
- Qui décide ?
- Qui arbitre ?

- Qui priorise ?
- Et… qui rend des comptes ?

Sans ça, c'est la jungle. Un audit sans interlocuteur clair, c'est un cauchemar, et souvent un symptôme d'un **SI livré à lui-même**.

📂 *5. Une PSSI documentée ET appliquée*

La **Politique de Sécurité des Systèmes d'Information**, c'est le "code de la route" interne.
Elle doit exister, être communiquée, comprise et… appliquée.

Un audit sérieux va regarder :

- Si la PSSI est à jour
- Si elle est diffusée aux équipes
- Si elle est **alignée avec la réalité** (pas juste une collection d'intentions pieuses)
- Et si elle est **vérifiée** (audit interne, KPI, suivi)

Sinon ? PSSI = PDF poussiéreux.

🧱 *6. Une gestion de projet SSI structurée*

Oui, la sécurité se pilote comme un projet :

- Objectifs clairs (maturité NIST/ISO/NIS2 ?)
- Roadmap SSI (avec priorités, jalons, budgets)
- Plans d'action issus d'audits précédents
- Indicateurs de suivi (patching, MFA, sensibilisation…)

➡️ Un bon audit ne se contente pas de pointer les failles. Il évalue aussi **votre capacité à piloter la sécurité au quotidien.**

Un audit efficace, c'est aussi un **audit de votre capacité à piloter la sécurité comme un projet** :

- Existe-t-il une feuille de route SSI ?
- Y a-t-il un suivi des plans d'action post-audit ?
- Des jalons ? Des budgets ? Des indicateurs ?
- Une stratégie à 6 mois, 1 an, 3 ans ?

➡️ L'auditeur ne vient pas juste constater l'état du SI, il vient **voir comment vous en prenez soin**.

🧠 Conclusion : pas de paperasse = pas de sécurité

"Chez nous, on est agiles, on documente peu."
→ Traduction : "on est désorganisés, et on prie très fort pour que personne ne tombe malade ni ne parte en vacances."

La sécurité, c'est de la **rigueur**, de la **traçabilité**, de la **préparation**, et **de la mémoire**.
Tout ce qu'un audit vient mesurer **au-delà des outils**.

📉 "Mais pourquoi auditer nos documents ? Ce sont juste des papiers !"

Lors d'un audit organisationnel, le client n'avait ni PRA, ni procédure de gestion des incidents, ni journalisation des accès, mais :

"On est à jour techniquement, ça suffit largement."

➡️ 6 mois plus tard, attaque par ransomware.
Sans plan, sans communication, sans gouvernance :

- Les sauvegardes n'étaient pas accessibles
- Les admins étaient injoignables
- Le DG a annoncé publiquement "nous ne sommes pas touchés"… 3h avant que la prod ne s'arrête

👉 Résultat : audit réclamé par les assureurs, réputation ternie, coût x10.

❌ IV. Les erreurs à ne pas commettre

(…ou comment saboter son audit en 10 leçons – sans même s'en rendre compte)

🕳️ 1. Ne pas définir clairement le périmètre

Audit flou = audit foutu.
Si vous laissez l'auditeur "voir ce qu'il peut regarder", vous aurez :

- Un audit partiel
- Un rapport inutile
- Et potentiellement une non-conformité majeure… sur *ce que vous avez justement oublié d'auditer*

➡️ À éviter absolument : "Auditez tout ce que vous voulez, sauf ce qu'on préfère ne pas voir."

🧠 2. Ne pas faire d'analyse de risque en amont

Aller auditer sans avoir fait de cartographie des risques, c'est comme envoyer un pompier sans lui dire où se trouve le feu.
Résultat : un audit hors sol, un plan d'action pas priorisé, et du budget mal investi.

➡️ Le risque, ce n'est pas une note Nessus. C'est un scénario réel, dans VOTRE contexte.

⚒️ 3. Choisir le mauvais type d'audit

Commander un pentest quand on a besoin d'un audit organisationnel.
Lancer un scan de vulnérabilités et appeler ça un "audit ISO 27001".

➡️ Résultat : un rapport joli, mais totalement inutile.
Et un RSSI qui soupire, encore.

🐜 4. Ignorer les vulnérabilités « faibles »

C’est juste un XSS dans un formulaire oublié ? Un FTP sans mot de passe ?
➡️ Félicitations, vous venez d’offrir une porte d’entrée parfaite pour un attaquant malin.

Un audit sérieux analyse l’exploitabilité, **pas seulement la gravité CVSS**.

📦 5. Ne pas poser les limites de l’audit

Lancer un audit sans informer la prod, sans préciser ce qui est critique, sans définir les heures d’intervention, c’est jouer à la roulette russe avec un bazooka.

➡️ Problèmes en prod, perte de données, crise interne… et audit suspendu dans le chaos.

🙈 6. Cacher des éléments à l’auditeur

Les zones « qu’on ne veut pas montrer » sont souvent les plus pourries.
L’auditeur le sait. Il les verra.
Et il le mettra dans le rapport, en gras, souligné, avec capture d’écran.

➡️ L’audit n’est pas là pour “piéger” : il est là pour que vous sachiez ce qui vous menace *avant que ce soit trop tard*.

🗃️ 7. Négliger la documentation

Pas de procédure d'incident. Pas de PRA. Pas de registre des accès.
Mais tout le monde est sûr que "ça va".

➡️ Non. Ça ne va pas.
Et en audit, **l'absence de preuve = absence de maîtrise**. Peu importe si "tout est dans la tête de Bernard".

👑 8. Ne pas désigner de pilote

Si l'auditeur parle à 8 personnes différentes, avec 8 versions des faits, il ne pilote pas un audit : il fait un escape game.

➡️ Un audit doit avoir **un interlocuteur identifié**, capable de centraliser, arbitrer, transmettre, et valider.

📩 9. Ne pas lire le rapport… ou ne rien en faire

Rien n'est pire qu'un super rapport rangé dans un dossier "à traiter un jour".
Et si le plan d'action est lancé *après* l'incident, c'est trop tard.

➡️ Un audit est utile **uniquement si les recommandations sont traitées, suivies et revérifiées**.

📆 10. Penser que c'est "one-shot"

"On a fait un audit l'année dernière, donc c'est bon."
Spoiler : non.

➡️ Un audit doit être régulier, intégré à une démarche d'amélioration continue.
Parce que les failles changent. Les équipes changent. Les usages changent.
Et les attaquants, eux, **ne prennent pas de vacances**.

💬 Bonus : La mauvaise foi en mode expert

Mauvaise réaction	Traduction réelle
"Ce n'est pas critique."	"On n'a pas envie d'y toucher."
"On n'a pas le temps pour ça."	"On n'a pas compris les priorités."
"On verra ça plus tard."	"On ne le fera jamais."
"C'est comme ça depuis des années."	"On a toujours mal fait, pourquoi changer maintenant ?"
"Mais personne ne l'utilise…"	"…sauf le hacker qui l'a trouvé hier."

🧩 V. Conclusion

Un bon audit ne sécurise pas votre SI… il vous aide à le faire.

Faire un audit de sécurité, ce n'est pas une fin en soi. Ce n'est pas une opération cosmétique, ni une case à cocher pour faire plaisir au Comex, au DPO ou à l'assureur cyber.

C'est un **révélateur**.
Un miroir sans filtre sur l'état réel de votre sécurité numérique.
Et parfois… ça pique. Fort. 💉

🎯 L’audit, c’est :

✅ Un **bilan complet** : technique, organisationnel, documentaire
✅ Une **prise de recul structurée**, par des yeux extérieurs
✅ Un **déclencheur d’actions concrètes** : correctifs, refonte, sensibilisation, priorisation
✅ Un **outil de gouvernance** : il permet de justifier des choix, des budgets, des arbitrages
✅ Et parfois un **électrochoc salutaire** (celui qui évite le vrai choc, celui de la compromission)

❌ Ce que l’audit ne fera *jamais* :

❌ Corriger à votre place
❌ Remplacer une stratégie de sécurité
❌ Déjouer une attaque future tout seul
❌ Compenser une absence de culture SSI
❌ Sauver un SI mal géré par la grâce d’un PDF de 40 pages

🔄 Ce qu’il faut faire après l’audit :

1. Lire le rapport (vraiment) 📖
2. Prioriser les actions selon les risques identifiés 🎯
3. Établir un plan d’action clair (qui fait quoi, pour quand) 🛠️
4. Communiquer (aux équipes, à la direction, aux prestataires) 📣
5. Réévaluer régulièrement (audit interne, contrôle, suivi) 🔁
6. Refaire un audit plus tard pour mesurer les progrès (et pas juste cocher une case ISO) 🔍
7.

📌 Et surtout…

L'audit est une **photo à l'instant T**. Mais la sécurité, elle, est **un film en temps réel**, où chaque acteur doit être réveillé, briefé, et équipé pour jouer son rôle. (Voir notre article)

🧠 *En cybersécurité, on ne gagne pas avec un audit.*
On gagne avec une culture, une organisation, une vigilance… et un peu d'humilité.

🧠 Postface – Le mot du RSSI (qui en a vu d'autres)

Par : Un Responsable de la Sécurité des Systèmes d'Information, fonctionnaire semi-pyromane et survivant d'audits depuis 2008

J'ai vu des audits "fast & furious", torchés en deux jours, sans accès, sans interlocuteur, sans périmètre.
J'ai vu des DSI me dire "on est bons là-dessus", juste avant que l'auditeur trouve un accès RDP ouvert à tout l'internet.
J'ai vu des responsables métiers pleurer quand on leur a demandé ce qu'il advenait de leurs données en cas de crash serveur.
J'ai vu des directeurs mettre en signature :

"Notre SI est audité régulièrement par des experts"
…alors qu'ils n'avaient même pas lu la synthèse exécutive.

Et pourtant… je continue d'y croire.

Pourquoi ?
Parce que **le bon audit**, celui qu'on prend au sérieux, qu'on digère, qu'on discute en équipe, qu'on transforme en plan d'action **concret**, c'est une bénédiction.

C'est ce qui m'a permis de :

- Prouver à la direction que "le budget sécurité" ne servait pas à acheter des claviers RGB
- Rattraper une dette technique avant qu'elle ne devienne une brèche

- Former les équipes aux bons réflexes
- Éviter un drame RH en découvrant un accès partagé non tracé
- Dormir (parfois) un peu mieux la nuit

Alors oui, c'est contraignant.
Oui, ça fait ressortir des trucs qu'on aurait préféré ne pas voir.
Oui, parfois ça donne envie de changer de métier et d'ouvrir un food truck.

Mais un audit bien mené, c'est **un outil d'alignement** :

- Alignement entre technique et métier
- Entre ambition et réalité
- Entre promesses PowerPoint et systèmes en prod

Et dans un monde où les attaques sont de plus en plus rapides, sophistiquées et ciblées, on ne peut plus se contenter de "ça tiendra bien encore quelques mois".

Alors faites vos audits. Les vrais.
Les utiles.
Les douloureux mais honnêtes.
Et surtout… faites quelque chose avec.

Parce que la vraie faille, ce n'est pas une CVE.
C'est **de croire qu'on n'en a pas**.

Bien à vous,
Un RSSI (pas encore interné, mais ça viendra)

✅ Checklist finale : Êtes-vous prêt pour un audit de sécurité ?

Spoiler : si vous cochez moins de 10 cases, il est temps de paniquer (ou d'appeler à l'aide).

📍 Avant l'audit : cadrage & préparation

- 📦 **Périmètre défini** et validé par tous les acteurs (DSI, RSSI, métiers, prestataires)
- 🎯 **Objectifs clairs** de l'audit (technique, organisationnel, conformité, etc.)
- 📋 **Contrat d'audit ou lettre de mission** signé avec les règles du jeu (accès, horaires, limites)
- 📎 **Liste des accès et comptes techniques** préparée et testée
- 🗺️ **Cartographie du SI à jour** (même approximative, mais pas de plan de 2013)
- 📚 **Documents clés rassemblés** (PSSI, PRA, PCA, procédures incidents, sensibilisation, etc.)
- 🤝 **Référents désignés** (interlocuteur technique, fonctionnel, SSI…)

🧪 Pendant l'audit : transparence & organisation

- 💬 Les équipes sont **prévenues** (pas de scan surprise en pleine prod critique)
- 📞 Les contacts sont **disponibles** pour répondre aux questions de l'auditeur
- 🔎 Les **écarts sont assumés**, pas cachés ou minimisés
- 🧠 L'auditeur a accès aux bonnes personnes (technique, métier, gouvernance)
- 🗂️ Une **trace des échanges** est conservée (pour les actions post-audit)

📊 Après l'audit : exploitation & plan d'action

- 📖 Le rapport est **lu en entier** (oui, même les annexes)

- 🚦 Les **recommandations sont priorisées** selon le risque réel, pas juste la “sévérité CVSS”
- 🛠️ Un **plan d’action formalisé** est lancé (avec échéances, pilotes, jalons)
- 📣 Une **communication claire** est faite aux équipes concernées
- 🔁 Une **revue régulière** du plan d’action est mise en place
- 📅 Le **prochain audit est planifié** (parce que la cybersécurité, c’est pas une fois tous les 4 ans)

🧠 Checklist bonus : documents et procédures à produire ou mettre à jour

📂 Document ou procédure	Statut
📄 PSSI à jour, connue, appliquée	[ ]
📋 Procédure de gestion des incidents	[ ]
🔁 PRA (reprise) et PCA (continuité)	[ ]
🔐 Politique de gestion des accès et des rôles	[ ]
👨‍💻 Procédure d’onboarding/offboarding utilisateurs	[ ]
🗄️ Cartographie des données sensibles	[ ]
🧰 Journalisation et politique de logs	[ ]

📂 Document ou procédure	Statut
👨‍⚖️ Registre des traitements (si RGPD)	[ ]
📡 Politique de sécurité des fournisseurs	[ ]
📚 Plan de sensibilisation cybersécurité	[ ]
🎩 Rôles et responsabilités SSI formalisés	[ ]
📅 Roadmap ou feuille de route SSI	[ ]