E 44v22

Audit interne ISO 27001 version 2022

Objectif du module : Réalisation de l'audit interne selon l'ISO 19011 pour pouvoir :

- identifier des opportunités d'amélioration
- augmenter la satisfaction des parties prenantes
- évaluer la performance du SMSI ISO 27001

1 Domaine

Le mot audit vient du verbe latin « audire » = écouter.

Audit : *examen méthodique et indépendant en vue de déterminer si les activités et les résultats satisfont aux dispositions préétablies et sont aptes à atteindre les objectifs*

En général les audits sont internes ou externes.

Les audits internes, dits aussi « de première partie », sont une exigence de la norme ISO 27001 (§ 9.2).

Les audits externes, client (ou prestataire externe) et de certification, dits aussi de seconde et de tierce parties, n'entrent pas directement dans le périmètre de ce module.

L'audit interne est l'outil le plus répandu pour vérifier, évaluer et améliorer la performance d'un système de management de la sécurité de l'information (SMSI). Son objet n'est en aucun cas de trouver les points faibles du personnel. L'audit interne est entré dans la vie quotidienne de l'organisation car il est devenu indissociable de :

- tout système de management
- la communication interne
- l'amélioration quotidienne
- la culture d'entreprise

Ce n'est qu'avec les yeux des autres que l'on peut bien voir ses défauts. Proverbe chinois

Un audit interne est de type (cf. figure 1-1) :

- du système de management
- d'un processus
- d'un produit (service, projet)

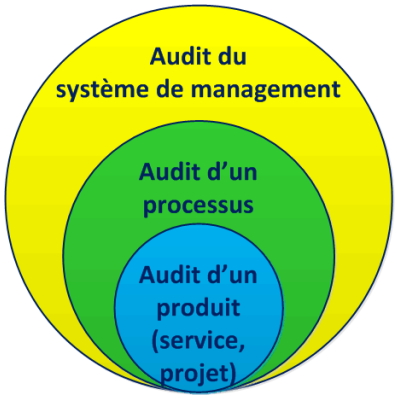


Figure 1-1. Types d'audits internes

Processus : *activités qui transforment des éléments d'entrée en éléments de sortie*

Les résultats des audits internes sont un des éléments d'entrée de la revue de direction et permettent de trouver des opportunités d'amélioration du système de management de la sécurité de l'information (SMSI) car :

Aucun système n'est parfait

Comme le montre la figure 1-2, pour le processus auditer, la direction (via la revue de direction) est considérée comme le client de l'audit avec ses besoins et attentes, eux-mêmes liés aux processus, produits et clients.

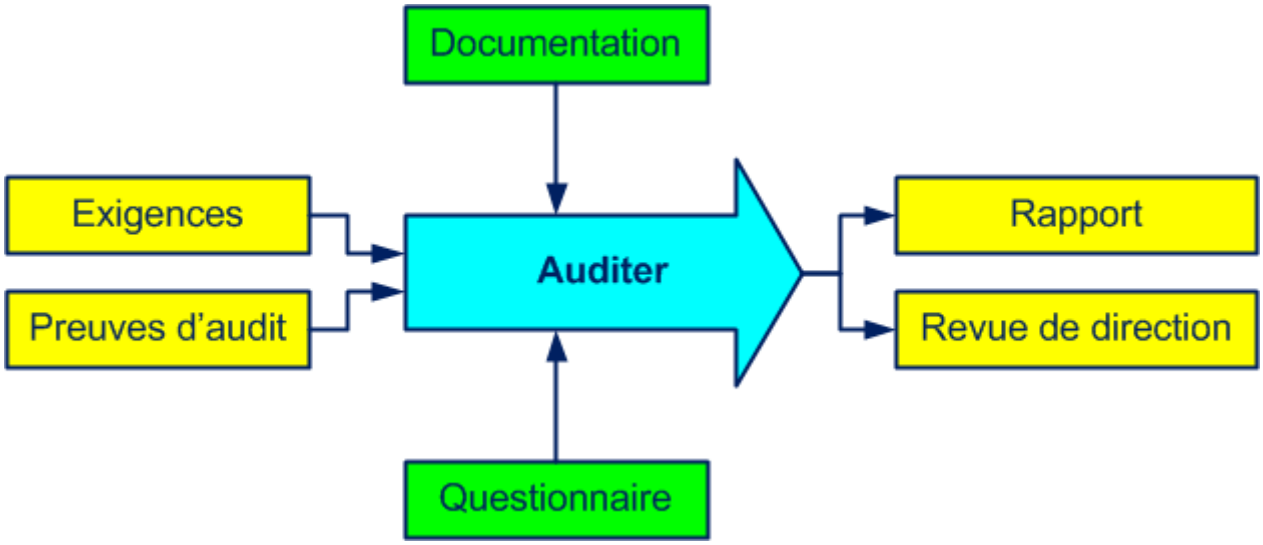


Figure 1-2. Le processus auditer

Dans les années 80 les audits internes étaient surtout documentaires – avez-vous écrit ce que vous faites ?

Plus tard, le début des années 2000, les audits internes étaient plutôt de conformité – ce que vous faites respecte-t-il les exigences de la norme ?

Maintenant les audits internes sont essentiellement d'efficacité – comment améliorez-vous votre performance ?

2 Normes

Les conseils que donne le document ISO 19011 se résument dans les domaines d'applications suivants :

- les principes de l'audit – chapitre 4
- le programme d'audit - chapitre 5
- la réalisation d'audit- chapitre 6
- la compétence des auditeurs- chapitre 7

Une bonne connaissance de la norme ISO 27001 est indispensable pour comprendre et suivre ce module.

N'hésitez pas à revenir sur les exigences de la norme ISO 27001 version 2022, cf. page ad hoc.

 Le présent module est basé sur les normes génériques et internationales suivantes :

- ISO 19011 (2018) : Lignes directrices pour l'audit des systèmes de management
- ISO 27000 (2018) : Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire
- ISO 27001 (2022) : Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information – Exigences

Toutes ces normes et beaucoup d'autres peuvent être commandées sur le site de l'AFNOR (Association française de normalisation) dans la rubrique boutique catalogue normes.

Plus de 28 000 normes (en anglais et autres langues) sont disponibles gratuitement sur le site Public.resource.Org.

3 Définitions

Le début de la sagesse est la définition des termes. Socrate

Quelques termes et définitions des systèmes de management et des audits :

Accident *: événement non désiré causant la mort ou des dommages*
Action corrective *: action pour éliminer les causes d'une non-conformité ou tout autre événement indésirable et empêcher leur réapparition*
Amélioration continue : *processus permanent permettant d'améliorer les performances globales de l'organisation*
Audité *: celui qui est audité*
Auditeur *: celui qui est formé pour effectuer des audits*
Client : *celui qui reçoit un produit*
Client de l'audit : *celui qui demande un audit*
Compétence *: aptitudes, connaissances et expériences personnelles*
Conformité *: satisfaction d'une exigence spécifiée*
Conclusion d'audit : *résultat d'un audit*
Constatation d'audit *: tout écart des critères d'audit*
Danger *: situation pouvant conduire à un incident potentiel*
Direction : *groupe ou personnes chargées de la gestion au plus haut niveau de l'organisation*
Document (information documentée) : *tout support permettant le traitement d'une information*
Ecart *: non-respect d'un seuil déterminé*
Enregistrement : *document fournissant des preuves tangibles des résultats obtenus*
Environnement de travail : *ensemble des facteurs humains et physiques dans lesquels le travail est réalisé*
Exigence *: besoin ou attente implicite ou explicite*
Fournisseur (prestataire externe) : *celui qui procure un produit*
Maîtriser *: garantir la conformité aux critères spécifiés*
Non-conformité *: non-satisfaction d'une exigence spécifiée*
Organisation (entreprise) : *structure qui satisfait un besoin*
Partie prenante : *personne, groupe ou organisation pouvant affecter ou être affecté par une organisation*
Problème *: écart qu'il faut réduire pour obtenir un résultat*
Produit (ou service) *: tout résultat d'un processus ou d'une activité*
Produit fini *: tout résultat final d'un processus ou d'une activité*
Procédure : *ensemble d'actions à entreprendre pour effectuer un processus*
Qualité : *aptitude à satisfaire des exigences*
Revue *: examen d'un dossier, d'un produit, d'un processus afin de vérifier l'atteinte des objectifs fixés*
Risque *: vraisemblance d'apparition d'une menace ou d'une opportunité*

Exemples de parties prenantes : investisseurs, clients, prestataires externes, employés, organisations sociales, politiques, publiques

Dans la terminologie des systèmes de management ne pas confondre :

- anomalie, défaut, défaillance, dysfonctionnement, gaspillage, non-conformité et rebut :
  - l'anomalie est une déviation par rapport à ce qui est attendu
  - le défaut est la non-satisfaction d'une exigence liée à une utilisation prévue
  - la défaillance c'est quand une fonction est devenue inapte
  - le dysfonctionnement est un fonctionnement dégradé qui peut entraîner une défaillance

    - le gaspillage c'est quand il y a des coûts ajoutés mais pas de valeur
    - la non-conformité est la non-satisfaction d'une exigence spécifiée en production
    - le rebut est un produit non conforme qui sera détruit
- audit, audité et auditeur
    - l'audit est un processus de vérification et d'amélioration du SMSI
    - l'audité est celui qui est audité
    - l'auditeur est celui qui effectue l'audit
- auditer et inspecter
    - auditer c'est améliorer le SMSI
    - inspecter c'est vérifier la conformité d'un processus ou produit
- cartographie et organigramme
    - la cartographie est la présentation graphique des processus et leurs interactions dans une organisation
    - l'organigramme est la présentation graphique des départements et leurs liens dans une organisation
- client et prestataire externe
    - le client reçoit un produit
    - le prestataire externe
- efficacité et efficience
    - l'efficacité est le niveau d'obtention des résultats escomptés
    - l'efficience est le rapport entre les résultats obtenus et les ressources utilisées
- indicateur et objectif
    - l'indicateur est l'information de la différence entre le résultat obtenu et l'objectif fixé
    - l'objectif est un engagement recherché
- maîtriser et optimiser
    - la maîtrise est le respect des objectifs
    - l'optimisation est la recherche des meilleurs résultats possibles
- procédure, processus, procédé, produit, activité et tâche :
    - la procédure écrite est un document précisant la manière d'effectuer un processus ou une activité (qui, quand, où, comment)
    - le processus est l'ensemble d'activités de transformation d'éléments d'entrées en éléments de sortie (quoi, pourquoi)
    - le procédé est la façon d'exécuter une activité
    - le produit est le résultat d'un processus
    - l'activité est un ensemble de tâches
    - la tâche est une suite d'opérations élémentaires
- programme et plan d'audit
    - le programme d'audit est la planification annuelle des audits
    - le plan d'audit est le descriptif des activités d'un audit
- revue et suivi
    - la revue est l'analyse de l'efficacité d'une activité
    - le suivi est la vérification de l'atteinte des résultats d'une action

Remarque 1 : chaque fois que vous utiliserez l'expression « opportunité d'amélioration » à la place de non-conformité, problème, souci, dysfonctionnement ou défaillance vous gagnerez un peu plus la confiance de l'audité.

Remarque 2 : le mot anglais « control » a plusieurs sens. Il peut être traduit par maîtrise, autorité, commande, gestion, contrôle, surveillance, inspection. Pour éviter des malentendus notre préférence est pour maîtrise et inspection au détriment de contrôle.

Remarque 3 : le client peut être aussi l'usager, le bénéficiaire, le déclencheur, le donneur d'ordres, le consommateur.

Remarque 4 : entre processus et procédé notre préférence est pour processus (en anglais « process »). 

Remarque 5 : l'utilisation des définitions de l'ISO 19011 et de l'ISO 27000 est recommandée. Le plus important est de définir pour tous dans l'organisation un vocabulaire commun et sans équivoque.

Remarque 6 : le document ISO 19011 version 2018 utilise conjointement les termes procédure, enregistrement et information documentée. Notre préférence est pour procédure ( *) et enregistrement (*  *).*

Pour d'autres définitions, commentaires, explications et interprétations que vous ne trouvez pas dans ce module et dans l'annexe 06 vous pouvez consulter :  

- Plateforme de consultation en ligne (OBP) de l'ISO
- Electropedia de l'IEC
- Bernard Froman, Christophe Gourdon, Dictionnaire de la qualité, AFNOR, 2003

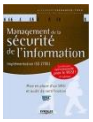
Quand je pense à tous les livres qu'il me reste encore à lire, j'ai la certitude d'être encore heureux. Jules Renard

 Pour aller plus loin quelques livres sur les audits :

-  Paul Gagnon, L'audit sécurité, AFNOR, 2005
-  Spencer Pickett, The Essential Handbook of Internal Audit, John Wiley & Sons, 2005 (Le livre essentiel de l'auditeur interne)
-  Michel Jonquières, Manuel de l'audit des systèmes de management, AFNOR, 2006
-  Henri Mitonneau, Réussir l'audit des processus, AFNOR, 2006
-  Geneviève Krebs, Yvon Mougin, Les nouvelles pratiques de l'audit qualité interne, AFNOR, 2007
-  Christophe Villalonga, L'audit qualité interne, Dunod, 2007

-  Solange Faucher et al, Vade-mecum de l'auditeur QSEDD, AFNOR, 2009
-  Pierre Vandeville, L'audit qualité, sécurité, environnement, AFNOR, 2009
-  Geneviève Krebs, La relation auditeur – audité, AFNOR, 2009
-  David Hoyle, John Thompson, ISO 9000 Auditor Questions, Transition Support, 2009 (Questions auditeurs ISO 9000)
-  Christophe Villalonga, Le Guide du parfait auditeur interne, Lexitis, 2011
-  Claude Pinet, L'audit de système de management, Lexitis, 2012
-  Yvon Mougin, Les nouvelles pratiques de l'audit de management QSEP (Qualité, Santé et sécurité, Environnement, Performance), AFNOR, 2013
-  Pascal Weber, Luc Villedieu, La sécurité de l'information: Mettre en pratique les exigences ISO 27001 : 2013, CreateSpace Independent Publishing Platform, 2014
-  Jacques Renard, Théorie et pratique de l'audit interne, Eyroles, 2016
-  Alexandre Fernandez Toro, Comprendre et mettre en œuvre la norme ISO 27001: Conseils pratiques d'implémentation, CreateSpace Independent Publishing Platform, 2016
-  Alexandre Fernandez Toro, Sécurité opérationnelle : Conseils pratiques pour sécuriser le SI, Eyrolles, 2016
-  Richard Chambers, Quelques leçons d'audit interne : Les conseils d'un grand professionnel, Eyroles, 2016
-  Alan Calder, Iso27001/Iso27002: Un guide de poche, It Governance, 2017
-  Alan Calder, Neuf étapes vers le succès: Un aperçu de la mise en œuvre de la norme ISO 27001:2013, IT Governance, 2017

- 

Michel Cattan, Guide des processus, AFNOR, 2018
- 

Alexandre Fernandez-Toro, Management de la sécurité de l'information: Présentation générale de l'ISO 27001 et de ses normes associées - Une référence opérationnelle pour le RSSI, Eyrolles, 2018
- 

Guillaume Litvak, Sébastien Allaire, Guide de l'audit interne : Défis et enjeux - Théorie et pratique, Vuibert, 2019
- 

Anne Lupfer, Gestion des risques en sécurité de l'information, Mise en œuvre de la norme ISO 27005, Eyrolles, 2021 (2010)

4 Principes

4.1 Principes de management

Les sept principes de management de la qualité (cf. figure 4-1) nous aiderons à obtenir des performances durables (cf. ISO 9001 : 2015, § 0.2).

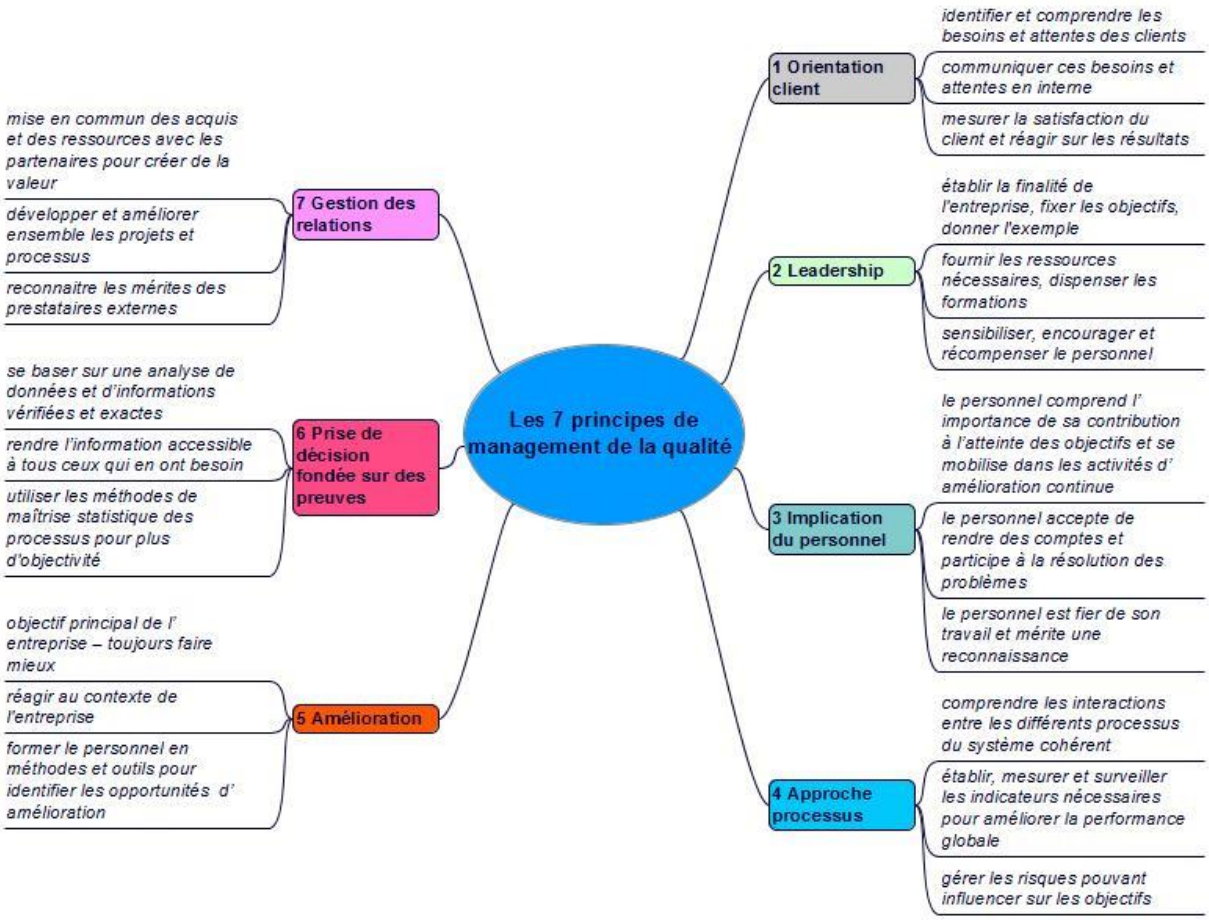


Figure 4-1. Les 7 principes de management de la qualité

4.2 Principes de l'audit

Pour que l'audit soit un outil à valeur ajoutée il faut respecter certains principes.

Pour l'auditeur :

- la déontologie, pour garantir :
  - l'honnêteté, l'éthique et la responsabilité
  - des activités entreprises avec la compétence nécessaire
- la présentation impartiale, pour assurer :
  - des conclusions d'audit honnêtes et précises
  - des constatations et un rapport d'audit détaillés
- la conscience professionnelle, pour assumer :
  - l'importance de la tâche
  - la confiance accordée

- la confidentialité, pour traiter avec précaution les informations :
  - sensibles
  - confidentielles
- l'indépendance, pour :
  - conduire un audit impartial
  - rédiger des conclusions objectives
- l'approche fondée sur la preuve, pour obtenir des conclusions :
  - fiables, vérifiables et
  - reproductibles
- l'approche par les risques, pour atteindre les objectifs de l'audit en :
  - identifiant et diminuant les menaces
  - saisissant les opportunités

Mais aussi :

- le bon sens, c'est toujours le meilleur outil
- la curiosité, pour apprendre et réussir
- la bienveillance, pour aider l'audité à saisir des opportunités d'amélioration
- le langage abordable
- l'attitude positive, c'est valorisant pour l'audité

Pour l'audit :

- l'indépendance (l'auditeur et l'activité auditée n'ont pas de conflits d'intérêt), pour garantir :
  - l'objectivité des conclusions
  - le fondement des constatations sur des preuves tangibles
- l'approche factuelle, pour assurer :
  - que les preuves d'audit sont vérifiables
  - des conclusions d'audit reproductibles

Pour l'audité :

- rester disponible
- ne pas essayer de cacher la vérité
- ne pas avoir peur de ses réponses
- accepter objectivement les non-conformités trouvées
- être conscient de participer à l'amélioration du SMSI en étant :
  - bienveillant et
  - coopératif

Un auditeur ne peut auditer son département car :

Nul ne peut être à la fois juge et partie. Proverbe latin

 Minute de détente. Cf. blague « l'ingénieur et le berger »

4.3 Performance du SMSI

Pour un système de management de la sécurité de l'information ce qui nous intéresse est le degré d'atteinte des objectifs ou autrement dit la performance. La performance d'un SMSI est mesurée par son efficacité et surtout par son efficience (cf. figure 4-2).

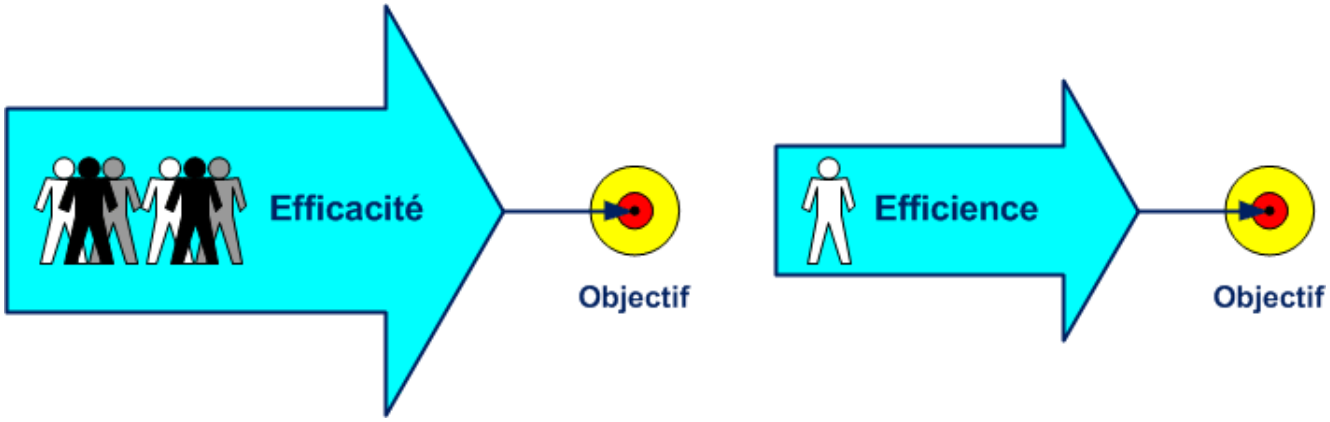


Figure 4-2. Performance d'un SMSI

Efficacité : *capacité de réalisation des activités planifiées avec le minimum d'efforts*
Efficience : *rapport financier entre le résultat obtenu et les ressources utilisées*

N.B. On peut être efficace parce que l'on a atteint son objectif, mais non efficient – on a utilisé trop de ressources, on a toléré et réalisé trop de gaspillages !