Méthode d'audit du Système d'Information

Guide complet

Yann-Eric DEVARS

www.dynamap.fr
contact@dynamap.fr

Introduction 7

Phase 1 : Définir le périmètre et les objectifs de l'audit 10

1.1. Contexte et finalité de l'audit 10

1.2. Alignement sur la stratégie et l'environnement organisationnel 12

1.3. Sélection des référentiels et normes applicables 14

1.4. Délimiter précisément le périmètre technique et organisationnel 16

1.5. Détermination des objectifs de l'audit 19

1.6. Identification et rôle des parties prenantes 21

1.7. Articulation entre périmètre et risques 23

1.8. Les contraintes temporelles et budgétaires 25

1.9. Documentation de la phase initiale 26

1.10. Communication et sensibilisation en amont .. 28

1.11. Erreurs fréquentes à éviter lors de la définition du périmètre et des objectifs 29

1.12. La pierre angulaire de l'audit 30

Phase 2 : Planifier l'audit 33

2.1. L'esprit de la planification selon l'ISO 19011 34

2.2. Construction du plan d'audit : du macro au micro 35

2.3. Analyse documentaire préalable et consolidation des informations existantes 39

2.4. Stratégie de collecte des preuves et méthodes de vérification 42

2.5. Gestion logistique : disponibilité, accès et confidentialité 44

2.6. Communication et implication des parties prenantes..... 47

2.7. Gestion des risques et facteurs critiques de succès pendant la planification 48

2.8. Validation finale et lancement officiel de l'audit 50

2.9. Les bénéfices d'une planification rigoureuse ... 52

2.10. Une étape déterminante pour la réussite de l'audit 54

Phase 3 : Collecte et analyse préliminaire des informations 57

3.1. Comprendre l'importance de la collecte et de l'analyse préliminaire 58

3.2. Les sources clés à investiguer 61

3.3. Méthodes et outils pour la collecte des informations..... 67

3.4. L'analyse préliminaire : de la synthèse documentaire à la formulation d'hypothèses 71

3.5. Facteurs de succès et écueils à éviter..... 75

3.6. Articulation avec les référentiels et normes 77

3.7. Intégration des parties prenantes et communication en phase préliminaire 80

3.8 Une fondation solide pour la suite de l'audit 82

Phase 4 : Évaluation des risques et analyse de conformité 86

4.1. Contexte et objectifs de l'évaluation des risques et de la conformité 87

4.2. Principes directeurs et cadre méthodologique. 89

4.3. Identification des risques : recueillir et classer les menaces 92

4.4. Analyse et évaluation des risques : de la matrice d'impact à la priorisation 95

4.5. Analyse de conformité : confronter la réalité aux exigences 99

4.6. Croisement entre risque et conformité : établir une vision globale 103

4.7. Techniques et outils pour consolider l'évaluation 105

4.8. Synthèse : établir une liste hiérarchisée des risques et non-conformités 107

4.9. Facteurs clés de succès et écueils à éviter 109

4.10. Un socle stratégique pour la suite de l'audit..111

Phase 5 : Vérifications et contrôles sur le terrain 114

5.1. Les objectifs clés des vérifications sur le terrain 115

5.2. Les grandes méthodes de vérification 118

5.3. Organisation pratique de la phase de vérifications 123
5.4. Exemples de vérifications ciblées par référentiel 126
5.5. Documentation et consignation des preuves ..129
5.6. Gérer les imprévus et s'adapter sur le terrain ..131
5.7. Facteurs de réussite et écueils à éviter.....134
5.8. Articulation avec la suite de l'audit 136
5.9. Étude de cas : illustration synthétique.....137
5.10. Ancrer l'audit dans la réalité opérationnelle ..139
Phase 6 : Synthèse et formulation des recommandations.....142
6.1. Contexte et importance de la synthèse 143
6.2. Structurer la synthèse : principes et formats recommandés 146
6.3. Du constat à la recommandation : les étapes clés 149
6.4. Collaborer avec les parties prenantes pour construire la synthèse 153
6.5. Rédiger et formaliser le rapport de synthèse ...156
6.6. Communiquer et valider la synthèse 159
6.7. Facteurs de réussite et écueils à éviter.....161
6.8. Exemple de livrable synthétique 162

6.9. Un pont entre l'audit et l'amélioration continue 165

Phase 7 : Validation, rapport final et suivi du plan d'actions 167

7.1. Importance et objectifs de la validation finale.168

7.2. Contenu et structure du rapport final 170

7.3. Le plan d'actions : engager la dynamique de remédiation.....173

7.4. Suivi et contrôle de la mise en œuvre 175

7.5. Communication autour de la clôture et du suivi 178

7.6. Retour d'expérience et intégration dans l'amélioration continue 180

7.7. Cas particuliers et ajustements contextuels...181

7.8. Facteurs de réussite et risques d'échec dans l'étape finale.....183

7.9. Exemple concret de validation et suivi.....185

7.10. Un tremplin vers l'amélioration continue 187

Le mot de la fin.....190

Introduction

Le système d'information joue un rôle déterminant pour la compétitivité et la performance d'une organisation, l'audit du système d'information est donc devenu une étape incontournable.

Il ne s'agit plus simplement d'identifier des vulnérabilités techniques, mais bien d'apprécier l'ensemble des mécanismes de gouvernance, de gestion des risques et de conformité, en lien avec la stratégie et les besoins métiers.

Un audit réussi doit donc prendre en compte toutes les dimensions :

- La définition précise du périmètre
- La planification rigoureuse des interventions
- La collecte et l'analyse méthodique d'informations
- La vérification concrète des processus et configurations
- L'évaluation approfondie des risques
- La formulation de recommandations ciblées
- La mise en place d'un plan de suivi effectif

C'est dans cette logique que s'inscrit la démarche présentée ici qui propose un cadre cohérent et structuré pour réaliser un audit SI de bout en bout.

Cette méthode, bien que s'appuyant sur les

principales normes et référentiels n'est pas destinée à une certicication mais à s'inscrire dans une démarche de performance globale.

Libre à vous de vous appuyer dessus afin de préparer une certification future.

La première phase souligne l'importance de bien délimiter le périmètre et de fixer des objectifs clairs, afin de garantir la pertinence et l'efficience de la mission.

La deuxième se concentre sur la planification, étape nécessaire pour maîtriser la logistique, la répartition des ressources et la coordination des acteurs.

La troisième phase aborde la collecte et l'analyse préliminaire des informations, indispensable pour cerner les processus et procédures en place avant de descendre sur le terrain.

La quatrième phase décrit l'évaluation des risques et l'analyse de conformité : cette phase permet de mettre en lumière les menaces, vulnérabilités et exigences légales ou normatives, tout en hiérarchisant les priorités.

La cinquième phase se consacre aux vérifications et contrôles sur le terrain, moment où la théorie est confrontée à la pratique, grâce à l'observation directe, aux entretiens et aux tests techniques.

La sixième phase explique comment structurer la synthèse et formuler des recommandations concrètes,

tenant compte des réalités organisationnelles et du degré de maturité existant.

La septième phase décrit la validation, la finalisation du rapport d'audit et, surtout, le suivi du plan d'actions : c'est cette dynamique d'amélioration continue qui assure la pérennité et la valeur réelle de l'audit.

Ce parcours méthodologique, fondé sur les référentiels et bonnes pratiques reconnus (ISO 19011, COBIT, ISO 27001, ITIL, etc.), se veut à la fois complet et adaptable.

Chaque organisation peut en effet l'ajuster en fonction de ses besoins, de sa taille, de son secteur d'activité et de sa culture interne.

L'enjeu est de doter les décideurs, la direction informatique et les équipes opérationnelles d'une feuille de route fiable pour évaluer, sécuriser et faire évoluer le SI dans le sens des objectifs stratégiques.

L'accent sera mis sur bonne gouvernance et d'une communication fluide entre l'ensemble des parties prenantes.

Car l'audit n'est pas une fin en soi : c'est un moyen pour faire progresser l'organisation, anticiper les risques et renforcer la confiance de ses clients, partenaires et collaborateurs.

Phase 1 : Définir le périmètre et les objectifs de l'audit

Dans toute démarche d'audit, la première étape consiste à cerner avec précision ce que l'on souhaite examiner et pour quelles raisons.

Avant même de mobiliser des ressources techniques ou humaines, il est indispensable d'investir le temps nécessaire dans la définition du périmètre et des objectifs.

Cette phase initiale conditionne la pertinence, la cohérence et la crédibilité de l'ensemble de l'audit.

Les référentiels tels que l'ISO 19011, COBIT, ISO 27001, ITIL ou encore ISO 20000 insistent tous, à des degrés divers, sur l'importance de clarifier en amont ce que l'on cherche à vérifier, contrôler ou améliorer.

Cette phase détaille donc, point par point, les éléments clés à considérer pour réussir cette première étape, en s'appuyant sur ***les meilleures pratiques reconnues.***

1.1. Contexte et finalité de l'audit

L'audit ne peut être mené de manière efficace si l'on ne comprend pas le **pourquoi** de la démarche.

Dans certains cas, il s'agit de satisfaire à une exigence légale ou réglementaire : par exemple, les entreprises

traitent toutes des données personnelles et sont donc soumises à des contrôles de conformité en vertu du Règlement Général sur la Protection des Données (RGPD).

D'autres audits sont dictés par une politique interne de gouvernance, suivant les recommandations de **COBIT** (Control Objectives for Information and Related Technologies), qui prône une gestion rigoureuse et alignée des ressources IT sur la stratégie d'entreprise.

Parfois, la finalité de l'audit peut simplement être l'amélioration continue, dans le cadre d'une démarche de progrès inspirée d'**ITIL** (IT Infrastructure Library) ou de l'**ISO 20000** pour la gestion des services informatiques.

Afin d'éviter toute confusion ultérieure, il est primordial de formuler clairement la finalité de l'audit : cherche-t-on à évaluer la sécurité des données, l'efficacité des processus, la qualité des services informatiques, la résilience du système d'information, ou plusieurs de ces dimensions à la fois ?

Cette clarification oriente non seulement les contrôles à mettre en place, mais aussi la sélection des parties prenantes qui seront associées à la démarche.

Par exemple, un audit purement technique sur la cybersécurité pourra s'appuyer davantage sur les référentiels **ISO 27001** et **NIST SP 800-53**, tandis qu'un

audit de gouvernance et de management se référera plutôt à **COBIT** et **ISO 38500**.

Dans la plupart des référentiels, il est recommandé de documenter la raison d'être de l'audit dans un document formel.

L'**ISO 19011**, qui est un guide reconnu pour l'audit des systèmes de management, conseille de mentionner explicitement les objectifs dans le plan d'audit.

Il ne s'agit pas uniquement d'une formalité : cette étape rend le projet compréhensible pour tous les acteurs, et facilite l'obtention d'un soutien au plus haut niveau de la direction.

Dans le cas où l'audit serait imposé par un organisme externe (organisme certificateur, autorité de tutelle, client, etc.), la description du contexte peut également inclure les exigences contractuelles ou règlementaires qui pèsent sur l'organisation.

1.2. Alignement sur la stratégie et l'environnement organisationnel

La définition du périmètre et des objectifs ne peut être dissociée du **contexte stratégique** de l'entreprise ou de l'institution.

En effet, un audit mené en silos, sans considération pour la stratégie globale, risque fort de déboucher sur des

recommandations peu adaptées ou difficiles à mettre en œuvre.

***COBIT insiste sur le fait que la gouvernance des systèmes d'information doit être alignée sur les objectifs stratégiques de l'organisation*.**

Ainsi, avant de cadrer l'audit, il faut comprendre :

- **Les priorités de la direction générale** : par exemple, si l'entreprise vise une expansion à l'international, la question de l'interopérabilité des systèmes ou de la sécurité transfrontalière des données pourrait primer.
- **Les impératifs réglementaires** : dans certains secteurs (banques, assurances, santé…), les contraintes imposées par les régulateurs peuvent forcer la main à l'organisation pour auditer des pans spécifiques du SI.
- **Les enjeux métiers** : si l'entreprise est en pleine transformation numérique, l'audit pourra cibler les volets de l'architecture d'entreprise (TOGAF, ISO 42010) pour s'assurer de la cohérence des projets digitaux.

L'intégration de l'audit dans un cadre plus large garantit une meilleure appropriation des résultats.

Selon l'**ISO 19011**, l'auditeur doit prendre connaissance des enjeux internes et externes susceptibles d'influer sur le périmètre de l'audit.

L'audit n'est pas une fin en soi : il est un moyen d'optimiser ou sécuriser le fonctionnement de l'organisation.

Par conséquent, cette première étape doit inclure un dialogue avec les décisionnaires : directeurs généraux, directeurs informatiques, responsables métiers, etc.

C'est souvent lors de ces échanges que l'on découvre des priorités mal exprimées ou des lacunes dans la compréhension collective du rôle du système d'information.

1.3. Sélection des référentiels et normes applicables

La question du **choix des référentiels** se pose dès le début du processus, car elle va orienter les contrôles, les indicateurs et la méthode d'audit.

Plusieurs options s'offrent à l'équipe d'audit :

1. **COBIT, ISO 38500** : A privilégier lorsque la priorité porte sur la gouvernance, l'alignement stratégique et l'évaluation de la maturité des processus IT.

   COBIT propose un cadre très structuré, commençant par la gouvernance (EDM, Evaluate, Direct, monitor) et couvrant de la planification et l'organisation (APO, Align, Plan and Organize)

jusqu'à la livraison et le support (DSS, Deliver, Service and Support).

2. **ISO 27001 et le corpus 27000** : incontournable pour auditer la sécurité de l'information, la conformité aux contrôles de sécurité, la gestion des risques et la mise en place d'un SMSI (Système de Management de la Sécurité de l'Information).

   L'ISO 27001 est souvent associée à l'**ISO 27002** pour les bonnes pratiques, et l'**ISO 27005** pour le management des risques.

3. **ITIL** ou **ISO 20000** : adaptés pour évaluer la qualité des processus de gestion des services (incidents, changements, configurations, etc.).

   ITIL est un référentiel de bonnes pratiques très utilisé dans les équipes opérationnelles, tandis que l'ISO 20000 formalise des exigences permettant de se faire certifier.

4. **NIST SP 800-53** : complément utile pour ceux qui souhaitent un référentiel de contrôles de sécurité très détaillé, issu du monde anglo-saxon.

   Il est souvent mobilisé dans un contexte d'audit technique ou lorsque l'organisation opère sur le marché américain.

5. **PCI-DSS** : lorsque l'audit concerne les flux de paiements et les données de cartes bancaires, ce

référentiel est obligatoire pour nombre d'acteurs manipulant des transactions par carte.

6. **Guides ISACA** : un ensemble de guides pratiques édités par ISACA pour aider à l'évaluation spécifique des processus IT.

Le périmètre de l'audit doit refléter le choix de ces référentiels.

Il est possible d'en combiner plusieurs, par exemple COBIT pour la gouvernance globale et ISO 27001 pour la sécurité, à condition d'assurer la cohérence de la démarche.

L'important est de ne pas tomber dans un millefeuille de normes qui embrouillerait l'équipe d'audit et les audités.

Cette sélection doit être justifiée dans la documentation de lancement d'audit, pour que chacun sache sur quels standards et bonnes pratiques les contrôles seront basés.

1.4. Délimiter précisément le périmètre technique et organisationnel

Une fois que le contexte et les référentiels sont clarifiés, il faut matérialiser **ce qui entre** et **ce qui ne rentre pas** dans le champ de l'audit.

L'**ISO 27001**, dans sa section 4.3, insiste fortement sur la nécessité de définir le périmètre du SMSI pour éviter toute ambiguïté.

On parle ici non seulement de périmètre technique (serveurs, applications, bases de données, réseaux), mais également de périmètre organisationnel (les filiales, les services internes, les rôles et responsabilités).

Voici quelques points essentiels à clarifier :

- **Le périmètre géographique** : s'agit-il d'un audit limité au siège de l'entreprise ou incluant des filiales, des data centers, des bureaux régionaux ?

  Les référentiels comme COBIT s'appliquent à l'ensemble de l'organisation, mais on peut décider de restreindre l'audit à certaines entités pour des raisons de faisabilité ou de calendrier.

- **Le périmètre fonctionnel** : par exemple, un audit peut se focaliser sur la fonction support (service desk, gestion des incidents, exploitation), ou bien inclure l'ensemble des processus IT (développement, tests, mise en production, etc.).

  ITIL propose une vision transverse des services, alors qu'ISO 27001 se concentre plutôt sur la protection de l'information à travers tous les processus.

- **Le périmètre applicatif** : dans certains cas, l'audit vise une ou plusieurs applications critiques (ERP, CRM, e-commerce), notamment pour vérifier la conformité aux règles de sécurité, de disponibilité ou de confidentialité.

  Lorsque l'on aborde les questions de protection des données personnelles, la CNIL ou l'**ISO 27701** (extension de l'ISO 27001 pour la protection de la vie privée) peuvent entrer en jeu.

- **Le périmètre organisationnel** : est-il prévu d'auditer la fonction RH, la fonction achats, la direction financière, la direction des opérations ?

  Cela peut sembler secondaire au premier abord, mais beaucoup de failles de sécurité ou de dysfonctionnements organisationnels proviennent d'une mauvaise coordination entre services.

Dans cette étape, il est judicieux de dresser un **inventaire** ou un **diagramme** représentant les entités, les systèmes et les processus inclus.

Un tel schéma facilite la compréhension collective du périmètre et offre une base pour répartir les responsabilités.

L'**ISO 19011** invite à mentionner dans le plan d'audit toute contrainte qui pourrait limiter le champ de l'audit (période de l'année, accès restreint à certains systèmes sensibles, etc.).

Cette transparence permet d'éviter que l'audit ne soit décrié par la suite comme incomplet ou partiel.

1.5. Détermination des objectifs de l'audit

Définir un périmètre est indispensable, mais cela doit s'accompagner d'une liste claire d'objectifs opérationnels.

Selon l'**ISO 19011**, un audit peut avoir plusieurs finalités : vérifier la conformité à un standard, évaluer l'efficacité d'un processus, identifier les risques pour proposer des actions correctives, etc.

Dans le domaine des technologies de l'information, on retrouve souvent les objectifs suivants :

1. **Évaluer la conformité à un référentiel** : par exemple, vérifier que l'organisation respecte les exigences de l'ISO 27001 (contrôles A.5 à A.18), ou que les processus IT respectent les bonnes pratiques d'ITIL.
2. **Mesurer la maturité des processus** : en se basant sur les grilles de maturité proposées par COBIT ou par des modèles comme CMMI, l'objectif est de situer l'organisation sur une échelle de performance.
3. **Identifier et prioriser les risques** : la sécurité de l'information étant un enjeu majeur, l'audit peut viser à dresser une cartographie des menaces et