L’audit technique informatique

Alain Gbaguidi Ing.

OBJECTIFS DU COURS

•L'objectif du cours d'audit des systèmes d'information est de permettre aux participants d'acquérir les fondements de l'audit des systèmes d'information en s'initiant aux principaux concepts généraux liés à l'audit dans le domaine informatique. Et d'une manière spécifique, ce cours vise à :

- Présenter les différentes facettes de l'audit des systèmes d'information en se basant sur la démarche à suivre, le modèle à prendre en considération, ainsi que la catégorie de l'audit à utiliser lors du processus de l'évaluation des systèmes d'information ;

OBJECTIFS DU COURS

- Appréhender les principaux généraux de l'audit des systèmes d'information, aux moyens des règles, de l'éthique et déontologie et des erreurs à éviter ainsi qu'élucider les éléments de la politique de la sécurité de l'audit informatique ;

- Faire maitriser les normes professionnelles et les référentiels nécessaires à la réalisation de l'audit des systèmes d'information ;

- Fournir les concepts relatifs aux processus de planification et d'organisation de l'élaboration du plan de l'audit des systèmes d'information.

LE SYSTME INFORMATIQUE

- **Définition** : Le *système système d'information*, (noté SI) représente l'ensemble des logiciels et matériels participant au stockage, à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation.

- **Les Ambitions stratégiques d'un SI**
  - Le SI doit créer une valeur croissante pour ses utilisateurs. À cet effet, les directions métiers doivent mieux s'appuyer sur les systèmes d'information pour optimiser les processus de fonctionnement de l'administration, augmenter la performance de celle-ci et la qualité du service rendu par les agents publics. Le système d'information doit être mieux structuré et utilisé pour développer les relations numériques entre les métiers et les usagers.

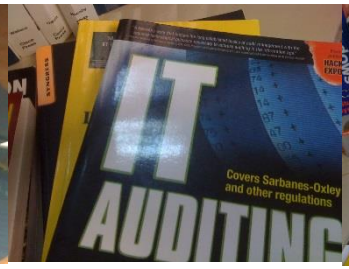
  - Le SI doit être construit de façon efficiente. Parallèlement aux investissements d"innovation qui créent de la valeur pour les utilisateurs du SI, les coûts non justifiés des composantes de ce SI doivent être réduits.

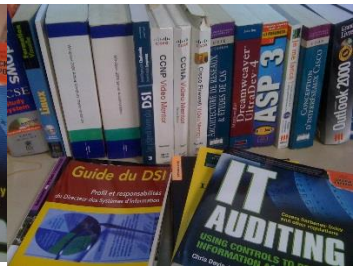
LE SYSTME INFORMATIQUE

- **Les Ambitions stratégiques d'un SI**

  – La fonction SI doit être pilotée. Les visions stratégiques des SI, et particulièrement leur alignement avec la stratégie des métiers, doivent s'appuyer sur une vision transversale du système d'information de afin de concilier enjeux métiers et enjeux globaux des politiques publiques. En particulier, certains enjeux d'organisation et de politique publique de long terme constituent des chantiers essentiels pour la réussite de l'évolution du système d'information, au-delà de visions trop locales

  – Le SI doit être construit de façon efficiente. Parallèlement aux investissements d"innovation qui créent de la valeur pour les utilisateurs du SI, les coûts non justifiés des composantes de ce SI doivent être réduits.





vision de la dynamique du système d'information

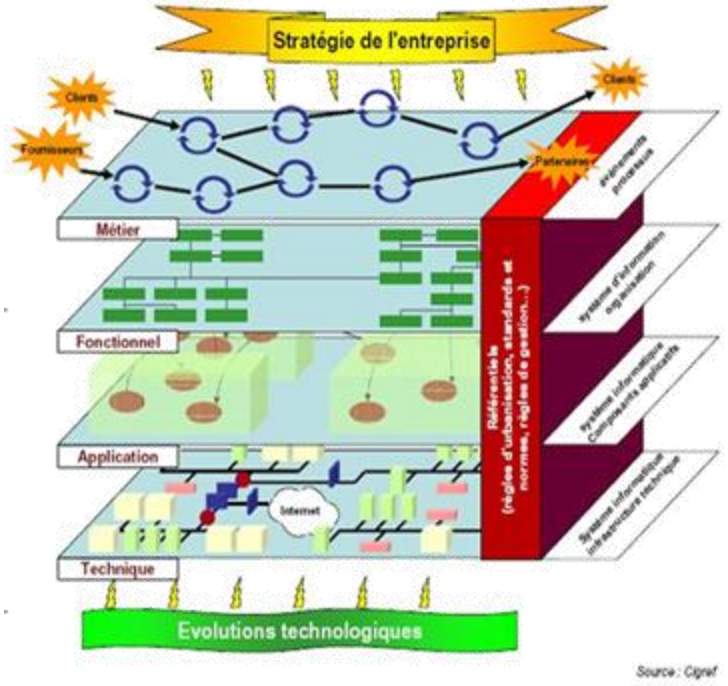
4 couches d'architecture

1 MODÈLE OPÉRATIONNEL ET PROCESSUS MÉTIER
- Fonctions métier
- Processus
- KPIs
- Procédures / acteurs
- Modèle de maturité

2 ARCHITECTURE FONCTIONNELLE / INFORMATIONS
- Domaines fonctionnels
- Fonctions
- Entité Métier (Information)
- Urbanisation

3 ARCHITECTURE APPLICATIVE / COMPOSANTS
- Domaines Applicatifs
- Applications / composants
- Services Métier/Micro Services
- Gestion des données

4 INFRASTRUCTURE
- Serveurs / Cloud
- Réseaux / Réseaux étendus
- Services de sécurité



La démarche urbanisée permet de:
- Fédérer les briques du SI cible autour d'une architecture d'ensemble et de principes qui lui permettent d'acquérir la souplesse et la réactivité nécessaires pour s'adapter aux contraintes ainsi qu'à l'évolution de l'environnement
- Maîtriser l'évolution du système d'information à travers une démarche permettant d'atteindre la cible en passant par paliers correspondants à des états stables
- Orienter les développements et les investissements sur les fonctionnalités à forte valeur ajoutée

DEFINTION ET CONTEXTE D'ETUDES

•*L'audit informatique* (*aussi appelé « audit des systèmes d'information ou de l'anglais Information Technology audit »*) consiste à une intervention réalisée par une personne indépendante et extérieure au service audité, qui permet d'analyser tout ou une partie d'une organisation informatique, d'établir un constat des points forts et des points faibles et dégager ainsi les recommandations d'amélioration. Autrement dit, L'audit informatique peut aussi être défini l'évaluation des risques des activités informatiques, dans le but d'apporter une diminution de ceux-ci et d'améliorer la maîtrise des systèmes d'information.

•*L'audit informatique* a pour objectif d'identifier et d'évaluer et déterminer ***les risques*** (*opérationnels, financiers, de réputation…)* associés aux activités informatiques d'une entreprise ou d'une administration.

DEFINTION ET CONTEXTE D'ETUDES

•À cette fin, pour sa mise en place effective, un processus de l'audit des systèmes d'information va se baser sur trois (3) aspects indispensables :

- *le cadre réglementaire du secteur d'activité d'un pays donné* ;
- *les référentiels de bonnes pratiques existants* (*exemple le référentiel* ***CobiT***, **ITIL, VAL IT** …) ;
- les ***benchmarks***5 à disposition et sur l'expérience professionnelle de l'auditeur impliqué.

DEFINTION ET CONTEXTE D'ETUDES

- De même, l'audit des systèmes d'information requiert deux grandes caractéristiques pour sa mise en place effective :

▪ *La première caractéristique* – comporte les évaluations globales d'entités durant lesquelles toutes les activités ayant trait aux systèmes d'informations sont évalués.

▪ *La seconde caractéristique* – correspond aux évaluations correspondantes aux audits thématiques, ayant pour objectif la revue d'un thème informatique au sein d'une entité (*la gestion de projet, la sécurité logique par exemple*).

DEFINTION ET CONTEXTE D'ETUDES

Processus de l'audit informatique

L'audit informatique est une mission, qui ne demande pas de simples auditeurs, puisque ces derniers doivent avoir de fortes connaissances en informatique, car des notions, ainsi que des techniques sont à cerner pour comprendre et savoir gérer un processus d'informatisation.

MODELES DE L'AUDIT DES SYSTEMES D'INFORMATION

- Un « *modèle* » est une base donnée pour servir de référence. En conséquence, il existe 2 modèles d'audit des systèmes d'information : *le modèle de l'audit de besoin* et *le modèle de l'audit de découverte des connaissances*.

LE MODELE DE L'AUDIT DE BESOIN

- **Un « *modèle* » est une base donnée pour servir de référence. En conséquence, il existe 2 modèles d'audit des systèmes d'information : *le modèle de l'audit de besoin* et *le modèle de l'audit de découverte des connaissances.***
- De part sa définition, un « *besoin* » peut être considéré comme un élément nécessaire à l'existence (autrement dit, c'est un état qui résulte de la privation ou d'un manque du nécessaire). Le modèle de l'audit du besoin est subdivisé en 2 grandes parties : *l'analyse de l'existant* et *la détermination de la cible*.

▪ *L'analyse de l'existant* – consiste en un examen (appréciation) du terrain au terme duquel l'auditeur informatique formalise la circulation des « documents-types » d'un acteur à l'autre et le traitement que chaque acteur applique à ces documents, à l'aide de *logigrammes* (traitement sur les documents) et la représentation des *graphes relationnels* (circulation des documents) ;

▪ *La détermination de la cible* – cette seconde partie consiste à référer le mode de circulation des informations et leurs interprétations ; les différentes redondances dans les graphes ; la dispersion des infrastructures ainsi que les point de contrôle et de validation nécessaires, et le découpage en zone en sous-graphes.

LE MODELE DE L'AUDIT DE BESOIN

- **Un « *modèle* » est une base donnée pour servir de référence. En conséquence, il existe 2 modèles d'audit des systèmes d'information : *le modèle de l'audit de besoin* et *le modèle de l'audit de découverte des connaissances.***
- De part sa définition, un « *besoin* » peut être considéré comme un élément nécessaire à l'existence (autrement dit, c'est un état qui résulte de la privation ou d'un manque du nécessaire). Le modèle de l'audit du besoin est subdivisé en 2 grandes parties : *l'analyse de l'existant* et *la détermination de la cible*.

▪ *L'analyse de l'existant* – consiste en un examen (appréciation) du terrain au terme duquel l'auditeur informatique formalise la circulation des « documents-types » d'un acteur à l'autre et le traitement que chaque acteur applique à ces documents, à l'aide de *logigrammes* (traitement sur les documents) et la représentation des *graphes relationnels* (circulation des documents) ;

▪ *La détermination de la cible* – cette seconde partie consiste à référer le mode de circulation des informations et leurs interprétations ; les différentes redondances dans les graphes ; la dispersion des infrastructures ainsi que les point de contrôle et de validation nécessaires, et le découpage en zone en sous-graphes.

LE MODELE DE L'AUDIT DE DECOUVERTE DES CONNAISSANCES

Le modèle de l'audit de découverte des connaissances consiste à valoriser les données et les connaissances existantes dans l'entreprise. Généralement, ce modèle aboutit au montage d'un système d'information décisionnel (désigne les moyens, les outils et les méthodes qui permettent de collecter, consolider, modéliser et restituer les données matérielles et immatérielles d'une entreprise) mais également être le prélude (précurseur) à un système de gestion de connaissances.

Le modèle de l'audit de découverte des connaissances se pratique de la manière suivante :

- Pas d'objectifs : on ne sait pas ce que l'on va découvrir ;
- Un domaine : on sait sur quels métiers on travaille, donc sur quelles bases de données;
- une équipe intégrée : travaille in situ, trois acteurs dont un expert « métier », un expert « administration informatique » et un fouilleur de données (voir data mining) ;

LES SYSTEMES INFORMATIQUES : ENJEUX ET RISQUES

- **DEFINITION**

•Le système informatique, appelé aussi système d'information, (noté SI) représente l'ensemble des logiciels et matériels participant au stockage, à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation.

•La fonction informatique vise à fournir à ces ressources l'organisation. Elle comprend donc, outre le système informatique, les personnes, processus, ressources financières et informationnelles qui y contribuent.

•Un système informatique est constitué de ressources matérielles et logicielles organisées pour collecter, stocker, traiter et communiquer les informations. Les ressources humaines nécessaires à son fonctionnement (par exemple les administrateurs) sont parfois incluses dans ce périmètre.

LE SYSTME INFORMATIQUE

- **Les principaux facteurs clefs d'un SI performant sont les suivants** :
  - une forte implication de la direction dans la gestion du SI. Elle doit notamment superviser la gestion du SI par la mise en place des outils de pilotage suivants :
  - un schéma directeur informatique (SDI), qui définit la stratégie informatique pluriannuelle, dont la validation par la direction entérine l'adéquation entre la stratégie informatique et la stratégie de l'entité ;
  - des documents d'organisation de la gouvernance du SI, mis à jour régulièrement ;
  - des comités de pilotage informatiques réguliers (suivi des incidents, suivi des projets, suivi des budgets, etc.), au sein desquels la direction doit être représentée à bon niveau ;
  - des tableaux de bord de suivi de l'informatique ;
  - un portefeuille des projets SI et des analyses de la valeur des systèmes d'information ;
  - une politique de sécurité (voir ci-après), approuvée au plus haut niveau de la direction ;
  - des comités de sécurité réguliers, au sein desquels la direction doit être représentée à bon niveau ;
  - une cartographie des applications et systèmes informatiques à jour, incluse dans une politique

LE SYSTME INFORMATIQUE

- **Les facteurs clé d'un SI performant**

- Un SI idéal :
  - est en adéquation avec la stratégie de l'organisation et les objectifs des métiers ;
  - est en conformité avec les obligations légales ;
  - est sécurisé ;
  - est facile à utiliser ;
  - est fiable ;
  - est adaptatif ;
  - est pérenne ;
  - est disponible ;
  - est efficient ;
  - respecte le plan d'urbanisme ;

LE SYSTME INFORMATIQUE

- **Les principaux facteurs clefs d'un SI performant sont les suivants**

  – d'urbanisme informatique. Cette cartographie est fondamentale pour les auditeurs, les certificateurs ou tout autre organisme de contrôle.

  – **une politique de sécurité, qui doit être validée et soutenue par la direction de l'entité** :

  la politique de sécurité des systèmes d'information (PSSI) constitue le principal document de référence en matière de sécurité des systèmes d'information (SSI). Elle reflète la vision stratégique de l'entité et montre l'importance qu'accorde la direction à la sécurité de son SI ;

  – elle se matérialise par un document présentant, de manière ordonnée, les règles de sécurité à appliquer et à respecter dans l'organisme. Ces règles sont généralement issues d'une étude des risques SSI ;

LE SYSTME INFORMATIQUE

- **Les principaux facteurs clefs d'un SI performant sont les suivants**
  - après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires…). Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir ;
  - la PSSI est un document vivant qui doit évoluer afin de prendre en compte les transformations du contexte de l'organisme (changement d'organisation, de missions...) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux) ;
  - idéalement, il devrait exister une charte d'utilisation du système d'information, dans le but de sensibiliser les utilisateurs à la sécurité informatique, informer les utilisateurs des responsabilités qui leur incombent. Pour

LE SYSTME INFORMATIQUE

- **Les principaux facteurs clefs d'un SI performant sont les suivants**
- une meilleure efficacité, cette charte devrait être signée par tous les agents et une communication régulière sur le sujet devrait être mise en place avec le support de la direction. Cette charte contiendrait par exemple les règles de sécurité et de bon usage (protection du PC, mots de passe, confidentialité, utilisation d'Internet, de la messagerie, protection du PC, etc.), les normes relatives aux logiciels (installation, licences, etc.), une description de la traçabilité des actions sur le SI à laquelle chaque utilisateur est assujetti et les sanctions applicables en cas de non-respect des règles décrites.

LE SYSTME INFORMATIQUE

- **Les principaux facteurs clefs d'un SI performant sont les suivants**

- **le respect de la législation en matière de système d'information** :
  - la législation ne peut être appréciée en termes uniquement de contrainte. La mise en conformité du SI permet de garantir de façon raisonnable un environnement de contrôle satisfaisant de son SI ;

  - les principaux textes applicables sont la loi de sécurité financière (LSF), avec un volet informatique puisque l'objectif est de renforcer la fiabilité des informations financières des entreprises mais aussi le contrôle interne sur les aspects opérationnels (de même que la loi Sarbanes-Oxley aux États-Unis mais uniquement sur les aspects financiers) ;

LE SYSTME INFORMATIQUE

- la déclaration ADPD a, en revanche, un objectif différent puisqu'elle sert à protéger les données personnelles des individus, manipulées dans les applications informatiques.

- un paramétrage correct des droits d'accès aux applications informatiques :
  - les droits d'accès au SI doivent refléter les règles de séparation des tâches telles que définies dans l'organisation ;
- au niveau informatique, les développeurs ne peuvent pas avoir accès à l'environnement de production et le personnel d'exploitation ne peut pas avoir accès à l'environnement de développement. Par ailleurs, l'attribution de droits très élevés (« administrateurs ») doit être limitée et toute action de ces profils « sensibles » doit être tracée et revue régulièrement ;

LE SYSTME INFORMATIQUE

– au niveau des applications informatiques, les droits d'accès attribués doivent traduire de façon informatique les rôles de chacun dans l'organisation. Chaque agent n'a accès qu'aux applications qui le concernent dans sa fonction, et à l'intérieur des applications, il existe des restrictions au niveau de chaque fonctionnalité, voire au niveau des données ;

– les droits d'accès doivent faire l'objet d'une gestion rigoureuse, par un service dédié. Ainsi, les demandes d'octroi de droit d'accès doivent être formalisées et obligatoirement validées par les chefs de service. Les déblocages en cas de perte de mot de passe doivent être organisés. Enfin, la liste des habilitations, application par application, doit être revue régulièrement, et les droits d'accès supprimés en cas de départ.

LE SYSTME INFORMATIQUE

- une bonne gestion des projets de développements informatiques. La réussite d'un projet informatique nécessite *a minima* les éléments suivants :
  - une vision claire de l'objectif et des résultats attendus ;
  - l'implication de la direction générale ;
  - une définition claire des responsabilités des parties prenantes ;
  - l'implication des utilisateurs (« bureaux métiers ») ;
  - la constitution d'une équipe projet dédiée dirigée par des cadres expérimentés ;
  - des choix techniques pérennes ;
  - une gestion rigoureuse et organisée du projet ;
  - un déploiement échelonné ;
  - un suivi des risques ;
  - un accompagnement du changement.

LE SYSTME INFORMATIQUE

- une définition claire des responsabilités des parties prenantes ;
- l'implication des utilisateurs (« bureaux métiers ») ;
- la constitution d'une équipe projet dédiée dirigée par des cadres expérimentés ;
- des choix techniques pérennes ;
- une gestion rigoureuse et organisée du projet ;
- un déploiement échelonné ;
- un suivi des risques ;
- un accompagnement du changement.

LE SYSTME INFORMATIQUE

- **un SI intégré :**
  - un SI est dit intégré quand toutes les applications communiquent entre elles de façon automatique à l'aide d'interfaces. Ainsi, les informations ne sont saisies qu'une seule fois dans les systèmes (notion de base de données maîtresse) et les échanges de données font l'objet de contrôles d'intégrité automatiques. L'action humaine, source potentielle d'erreurs ou de fraude, est donc très limitée.
  - par ailleurs, la piste d'audit peut être entièrement informatisée.
  - une démarche qualité informatique : la mise en place d'une démarche qualité pour la gestion de la production et le développement informatique permet d'améliorer les performances du système d'information, de normaliser les procédures de gestion en fonction des référentiels existants et d'améliorer les compétences des acteurs du système d'information. Il existe en la matière de nombreux référentiels, dont les principaux sont les suivants :

LE SYSTME INFORMATIQUE

- **CMMI (Capability Maturity Model + Integration) pour les développements informatiques (avec plusieurs niveaux de certification de 1 à 5) ;**
  - **ITIL** (Information Technology Infrastructure Library) : plus spécifique à la gestion de la production informatique ;
  - **COBIT** (Control Objectives for Information and related Technology) : est un référentiel en matière de gouvernance informatique ;
  - **ISO 27001** (auparavant la BS7799) : présente les exigences en matière de sécurité informatique
  - le cadre stratégique commun du SI de l'État et le cadre commun d'urbanisation ;
  - méthode MAREVA 2 d'analyse de la valeur des projets SI (Forum de la performance).

LES RISQUES INFORMATIQUES

- **Les développements ci-dessous décrivent, pour chaque risque informatique, les principaux facteurs de risque et les contrôles ou procédures qui doivent être mis en place pour prévenir, réduire voire supprimer ce risque.**
- Pour mémoire, l'externalisation d'un service SI conduit à transférer les risques, sans pour autant les couvrir de manière certaine. En matière informatique, comme dans tous les autres domaines, l'externalisation d'un risque ne dispense ainsi pas une organisation de s'assurer qu'il est effectivement maîtrisé par son cocontractant et ne l'exonère en rien de sa responsabilité finale.
- Les principaux risques informatiques peuvent être regroupés en 3 domaines

  – les risques opérationnels, qui sont les plus nombreux pour le sujet traité ;
  – les risques financiers, puisque l'informatique et l'information sont des actifs ;
  – les risques légaux de non-conformité, puisque les entités sont soumises à des normes internes et externes, certaines de portée légale, concernant la gestion du SI.

LES PRINCIPAUX RISQUES INFORMATIQUES

- **Les développements ci-dessous décrivent, pour chaque risque informatique, les principaux facteurs de risque et les contrôles ou procédures qui doivent être mis en place pour prévenir, réduire voire supprimer ce risque.**
- Les principaux risques, facteurs de risques et dispositifs ou moyens de contrôles des risques informatiques sont les suivants :
  - **Inadéquation du SI avec la stratégie de l'entité et les besoins des utilisateurs**
    - Facteurs de risque :
    - manque d'implication de la direction dans la gestion de l'informatique ;
    - absence de schéma directeur ;
    - absence de gouvernance informatique ;
    - manque d'implication des utilisateurs (« bureaux métiers ») dans les projets informatiques ;
    - absence d'analyse de la valeur des SI mis en place.

LES PRINCIPAUX RISQUES INFORMATIQUES

- **Contrôles ou procédures attendus** :
  - supervision de l'informatique par la direction de l'entité ;
  - existence d'une stratégie en adéquation avec la stratégie de l'organisation, traduite par exemple dans un schéma directeur informatique ;
  - gouvernance informatique en place et validée par la direction ;
  - analyse de la valeur (par exemple par MAREVA 2) ;
  - forte implication des utilisateurs (« bureaux métiers ») dans les projets informatiques.
- **Incapacité de l'organisation à redémarrer les systèmes informatiques en cas arrêt ou destruction**
  - Facteurs de risque :
    - absence de sauvegarde régulière du SI (sauvegardes externes) ;
    - absence de plan de secours ;
    - absence de site de secours

- Contrôles ou procédures attendus :
  - mise en place d'un plan de secours (documenté, mis à jour lors de modifications majeures de l'environnement informatique, et testé au moins une fois par an) ;
  - procédure de sauvegarde quotidienne des données et programmes critiques ;
  - stockage des sauvegardes à l'extérieur de l'entité ;
  - les sauvegardes doivent être testées régulièrement ;
  - lorsqu'une activité est fortement dépendante de l'informatique, mise en place d'un site de secours
- **Sécurité du SI inadaptée au niveau de risque identifié et accepté par la direction**
  - Les facteurs de risque sont multiples car la sécurité est transversale à tous les processus de l'informatique :

- **Sécurité du SI inadaptée au niveau de risque identifié et accepté par la direction**
  - Les facteurs de risque sont multiples car la sécurité est transversale à tous les processus de l'informatique :
  - sécurité physique ;
  - sécurité logique ;
  - sécurité du réseau ;
  - sécurité de l'exploitation ;
  - sécurité des PC ;
  - sécurité des données ;
  - etc.
- **Contrôles ou procédures attendus:**
  - politique de sécurité en place, validée et supportée par la direction de l'entité ;
  - outils de surveillance du système informatique (par exemple supervision) ;
  - équipe sécurité dédiée recensant tous les incidents relatifs à la sécurité et capable d'intervenir en cas d'événement de sécurité.

- **Sécurité du SI inadaptée au niveau de risque identifié et accepté par la direction**
  - Les facteurs de risque sont multiples car la sécurité est transversale à tous les processus de l'informatique :
  - sécurité physique ;
  - sécurité logique ;
  - sécurité du réseau ;
  - sécurité de l'exploitation ;
  - sécurité des PC ;
  - sécurité des données ;
  - etc.
- **Contrôles ou procédures attendus:**
  - politique de sécurité en place, validée et supportée par la direction de l'entité ;
  - outils de surveillance du système informatique (par exemple supervision) ;
  - équipe sécurité dédiée recensant tous les incidents relatifs à la sécurité et capable d'intervenir en cas d'événement de sécurité.

- **Accès aux données et aux applications par des personnes non autorisées**
- **Facteurs de risque :**
  - absence de politique de sécurité ;
  - absence de gestion rigoureuse d'attribution des droits d'accès ;
  - absence de gestion rigoureuse des points d'accès ;
  - systèmes informatiques ne permettant pas une gestion fine des droits d'accès ;
  - gestion des mots de passe insuffisante.
- **Contrôles ou procédures attendus:**
  - politique de sécurité validée par la direction de l'entité ;
  - politique de gestion des mots de passe efficace ;
  - gestion rigoureuse des droits d'accès au système d'information en cohérence avec la séparation fonctionnelle des tâches ;
  - revue régulière de la liste des habilitations, application par application ;
  - revue régulière des points d'accès ;
  - séparation des tâches effective entre les fonctions développements et exploitation ;

- **Contrôles ou procédures attendus:**
  - supervision des profils sensibles alloués au personnel informatique ;
  - traçabilité des accès et actions sensibles.
- **Applications informatiques non fiables**
- **Facteurs de risque** :
  - erreurs dans la programmation des applications par rapport aux spécifications fonctionnelles ;
  - applications insuffisamment testées ;
  - utilisateurs insuffisamment impliqués dans les phases de développements de l'application.
  - Contrôles ou procédures attendus :
  - forte implication des utilisateurs dans les développements informatiques ;
  - bonne gestion de projet ;
  - veille environnementale ;
  - procédures de recensement des anomalies ;
  - procédures de maintenances correctives, adaptatives et évolutives.

- **Indisponibilité du système informatique**
- **Facteurs de risque** :
  - mauvaise gestion de l'environnement matériel du SI (énergie, climatisation, protection physique, etc.) ;
  - absence de convention de service ;
  - absence d'outil de surveillance de la disponibilité du SI ;
  - absence de cellule réactive en cas d'indisponibilité ;
  - absence de contrat de maintenance des matériels informatiques.
- **Contrôles ou procédures attendus :**
  - convention de service entre l'informatique et les utilisateurs, portant notamment sur des objectifs de performance du SI, tels le niveau de disponibilité des serveurs ;
  - support utilisateur performant ;
  - procédure de gestion des anomalies ;
  - procédure de maintenance corrective des applications informatiques ;
  - contrats de maintenance des matériels informatiques ;
  - environnement matériel adapté ;
  - plans de continuité et de reprise de l'activité.

- **Mauvaise utilisation du SI par les utilisateurs**
- **Facteurs de risque :**
  - applications informatiques non conviviales ;
  - utilisateurs insuffisamment formés ;
  - documentation utilisateur insuffisante et pas mise à jour ;
  - manque de contrôles bloquants dans les applications informatiques.
- **Contrôles ou procédures attendus :**
  - applications faciles d'utilisation ;
  - formation initiale des utilisateurs réalisée en temps utile et complétée par une formation au fil de l'eau ;
  - documentation utilisateur complète et mise à jour régulièrement ;
  - contrôles bloquants dans les applications ;
  - procédures de gestion des maintenances évolutives, adaptatives et correctives.

- **SI non conforme avec la législation**
  - Les lois et décrets portant sur le renforcement des procédures de contrôles internes concernent pour partie l'informatique. Les actions à mettre en place font, pour la plupart, partie des recommandations déjà citées pour couvrir certains risques informatiques comme :
  - la politique de sécurité informatique ;
  - la documentation informatique à jour ;
  - la sécurité des développements informatiques ;
  - la gestion rigoureuse des droits d'accès au SI.
  - S'agissant des déclarations CNIL, il est recommandé qu'une personne soit spécifiquement désignée dans l'organisation pour gérer ce sujet et l'anticiper. Elle doit notamment sensibiliser sur le sujet les services en charge des développements informatiques.

- **SI non pérenne**
- **Facteurs de risque** :
  - utilisation de la sous-traitance informatique sans transfert de compétence en interne ;
  - documentation informatique inexistante ou non mise à jour suite aux évolutions du SI ;
  - obsolescence de l'application et/ou de la technologie utilisée ;
  - forte dépendance vis-à-vis de personnes clés qui peuvent quitter l'entité.

- **Contrôles ou procédures attendus :**
  - le SI doit faire l'objet d'un schéma directeur informatique ;
  - la documentation informatique doit être complète et à jour, notamment dans un contexte de forte utilisation de la sous-traitance ou d'applications anciennes ;
  - des procédures de transfert de compétence entre les sous-traitants et les équipes informatiques internes doivent être mises en place.

- **SI non pérenne**
- **Facteurs de risque** :
  - utilisation de la sous-traitance informatique sans transfert de compétence en interne ;
  - documentation informatique inexistante ou non mise à jour suite aux évolutions du SI ;
  - obsolescence de l'application et/ou de la technologie utilisée ;
  - forte dépendance vis-à-vis de personnes clés qui peuvent quitter l'entité.
- **Contrôles ou procédures attendus :**
  - le SI doit faire l'objet d'un schéma directeur informatique ;
  - la documentation informatique doit être complète et à jour, notamment dans un contexte de forte utilisation de la sous-traitance ou d'applications anciennes ;
  - des procédures de transfert de compétence entre les sous-traitants et les équipes informatiques internes doivent être mises en place.

APPROCHE DE CERTAINS THEMES D'AUDIT

- **Approche de certains thèmes d'audit**
  - **L'audit des SI peut soit constituer un sous-domaine d'un audit généraliste (organisation, processus, régularité, etc.), soit être l'objet principal de la mission (application, projet, sécurité, respect de la législation, etc.).**

  - **L'AUDIT DES SI A L'OCCASION DE MISSIONS « GENERALISTES »**
  - La présente partie a pour objectif de montrer en quoi des audits ayant *a priori* peu à voir avec l'informatique doivent aborder *a minima* le domaine SI. Elle fournit **une approche des implications SI** de quelques missions-types et dresse la liste des principaux enjeux et risques associés, acteurs à rencontrer, documents à récupérer et principales questions à aborder.

- **L'audit d'une organisation**
  - Les organisations utilisent quotidiennement l'informatique. Celle-ci peut prendre la forme de simple bureautique, d'applications dédiées, les mettant, le cas échéant, en relation avec leurs cocontractants ou usagers via l'Internet, voire de systèmes informatiques plus complexes. Ces outils informatiques sont, désormais, indispensables au bon fonctionnement de l'organisation. Ils sont parfois au coeur de sa performance

  - Pourtant, les organisations n'en ont pas toujours conscience. Celles qui perçoivent l'importance de l'informatique ne maîtrisent pas toujours les arcanes de son pilotage, de sa conduite et de sa sécurité. Enfin, qu'elles disposent d'une fonction informatique en leur sein ou s'adressent à des prestataires internes ou extérieurs à l'administration, elles sont parfois peu ou mal organisées pour tirer le meilleur de ces ressources.

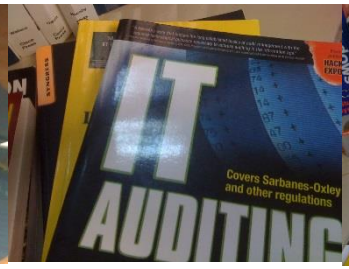
- **L'audit d'une organisation**
  - L'audit d'une organisation doit donc désormais nécessairement inclure un audit de sa relation au fait informatique. Comment définit-elle ses besoins fonctionnels, comment alloue-t-elle ses ressources humaines et financières en vue de les satisfaire, s'est-elle organisée et a-t-elle mis en place les processus lui permettant de disposer d'une informatique en phase avec ses besoins (alignement fonctionnel), réactive, sûre et efficiente ?
- **L'auditeur devra donc, à l'occasion de l'audit d'une organisation :**

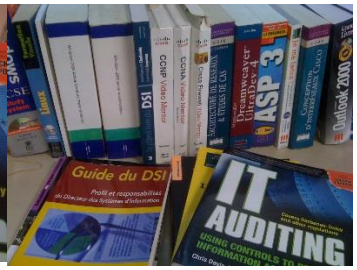
 étudier à travers les documents d'organisation et financiers les ressources organisationnelles (structures), humaines et financières qu'elle consacre à l'informatique ;

 étudier le fonctionnement de la comitologie associée au pilotage des SI ;

 se demander si ces ressources sont convenablement dimensionnées en regard de ce que d'autres organisations équivalentes consacrent à l'informatique ;

 étudier les processus stratégiques de l'organisation, inventorier les SI qui les outillent, et vérifier que l'entité s'est convenablement organisée pour garantir leur pilotage au juste niveau ;





 vérifier que l'organisation a mis en place le corpus minimal, ou décline convenablement celui fixé par le niveau supérieur (politique du SI, politique de sécurité du SI, charte d'utilisation).

- Si l'entité possède une fonction informatique dédiée (études, production, etc.), l'auditeur généraliste devra si possible solliciter les spécialistes de l'audit des SI et pourra se référer à la troisième partie du présent guide.
- L'auditeur devra rencontrer :

 la direction générale pour mesurer son degré de sensibilisation au fait informatique et l'organisation qu'elle a mise en place pour piloter ses SI ;

 une ou plusieurs directions fonctionnelles, le cas échéant les responsables de zones fonctionnelles, pour évaluer l'organisation qu'elles ont mise en place en vue de définir leurs besoins, de les exprimer et de contribuer efficacement aux processus visant à les satisfaire ;

 le cas échéant, la direction chargée des SI, pour évaluer la pertinence et les conséquences de son positionnement dans l'organisation et dans les processus de gouvernance ;

 le cas échéant, la direction chargée des achats, pour mesurer la part des SI dans son activité et vérifier la bonne prise en compte de leur spécificité ;

- le cas échéant, la direction chargée des ressources humaines, pour mesurer le poids des compétences SI (y compris indirectes,
- telles les compétences d'acheteur ou de juriste spécialisés dans le domaine SI) et des actions de formation dans le domaine.

- Il devra se procurer :

 les politiques SI et de sécurité SI de l'organisation ;

 le plan d'occupation des sols (POS) du SI et la liste des responsables de zones fonctionnelles ;

 la charte de l'utilisateur des SI à laquelle sont soumis les membres de l'organisation ;

 la liste des processus de l'organisation incluant les SI qui les supportent ;

 les comptes-rendus des comités ou groupes de travail (GT) consacrés pour tout ou partie aux SI ;

 la liste et le poids financier des principaux marchés SI en cours ;

 la politique RH et de formation.

- Au final, l'auditeur devra porter une appréciation sur la capacité de l'organisation à piloter son informatique, à apprécier ses enjeux (notamment la valeur de son patrimoine numérique) et évaluer les risques qui pèsent sur eux. Il peut aussi, si ses diligences lui fournissent une matière suffisante, évaluer l'alignement du SI sur les objectifs stratégiques de l'organisation.
- Il lui appartient de formuler les recommandations utiles en la matière.

- **L'audit des processus**
- Les processus sont désormais pour la plupart très fortement dépendants des outils informatiques. Dans le meilleur des cas, ils s'appuient sur un système informatique répondant à leurs besoins. Souvent, ils s'appuient au fil de leur déroulement sur des outils disparates, conçus dans une logique d'organisation et leur imposant des ruptures de charges. Ainsi, la performance d'un processus est intimement liée à l'alignement et à la qualité des systèmes informatiques.
- Dans une organisation pratiquant le pilotage par les processus, les projets informatiques devraient être pensés nativement dans une logique de processus.
- L'audit d'un processus doit donc inclure un audit des outils informatiques sur lesquels il s'appuie. Cet audit doit inclure l'examen des données et informations manipulées au cours du déroulement du processus, y compris celles provenant d'autres processus, des applications qui servent ou automatisent tout ou partie des tâches ou procédures qui le composent, et des infrastructures informatiques de traitement et communication qu'il utilise.

- **L'audit des processus**
  - L'auditeur devra donc, à l'occasion de l'audit d'un processus :

 étudier à travers les documents décrivant le processus et rendant compte de son fonctionnement, les données et informations manipulées, et les applications et les infrastructures utilisées. À défaut, il devra lui-même décrire le processus avant d'identifier ces éléments ;

 vérifier que les instances de gouvernance qui pilotent ce processus sont également compétentes pour orienter les SI y concourant ;

 vérifier l'alignement stratégique des outils informatiques et des processus qu'ils servent. Cette approche devra être étendue aux projets applicatifs ;

 vérifier que la sécurité physique et logique de ces données, informations, applications et infrastructures est en cohérence avec l'analyse des risques de ce processus. Il devra au préalable vérifier la pertinence de cette analyse des risques, voire procéder à sa propre analyse des risques ;

 étudier le dispositif de contrôle interne destiné à maîtriser ce processus, vérifier s'il existe qu'il est pertinent, et s'assurer que les outils informatiques y contribuent de manière efficace et efficiente ;

 vérifier que les infrastructures (particulièrement réseaux et serveurs) et les dispositifs d'assistance aux usagers de ces systèmes sont suffisants pour répondre aux besoins du processus.

- **L'audit des processus**
- L'auditeur devra rencontrer :

 la direction générale pour évaluer dans quelle mesure l'organisation pilote ses processus, voire pratique le pilotage par les processus, mesurer son degré de sensibilisation au fait informatique et vérifier que l'organisation qu'elle a mise en place pour piloter ses SI est en cohérence avec celle mise en place pour piloter les processus ;

 la ou les directions concernées par le processus audité, pour évaluer le degré de maturité de leur approche du processus, et étudier l'organisation qu'elles ont mise en place en vue de définir et exprimer des besoins en matière informatique qui soient bien alignés avec leurs processus ;

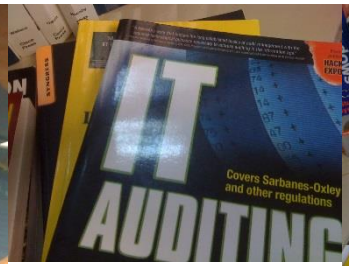
- **L'audit des processus**
- L'auditeur devra rencontrer :

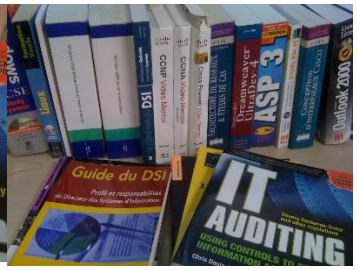
 la direction générale pour évaluer dans quelle mesure l'organisation pilote ses processus, voire pratique le pilotage par les processus, mesurer son degré de sensibilisation au fait informatique et vérifier que l'organisation qu'elle a mise en place pour piloter ses SI est en cohérence avec celle mise en place pour piloter les processus ;

 la ou les directions concernées par le processus audité, pour évaluer le degré de maturité de leur approche du processus, et étudier l'organisation qu'elles ont mise en place en vue de définir et exprimer des besoins en matière informatique qui soient bien alignés avec leurs processus ;

 s'ils existent, le pilote du processus audité et la direction chargée du pilotage des processus ou du pilotage par les processus, pour évaluer leur degré de sensibilisation au fait informatique et la qualité de leurs relations avec la direction chargée des SI ;

 la direction chargée des SI, pour évaluer la pertinence et les conséquences de son positionnement dans l'organisation et dans les processus de gouvernance vis-à-vis du processus audité.





- **L'audit des processus**
- Il devra se procurer :

 la cartographie des processus de l'organisation ;

 la description du processus audité, incluant l'inventaire des données et informations manipulées et des applications et infrastructures utilisées ;

 les tableaux de bord rendant compte de son déroulement et de sa performance ;

 la cartographie des données, informations et applications informatiques de l'organisation ;

 les politiques SI et de sécurité SI de l'organisation, et, le cas échéant, leur déclinaison à l'égard du processus audité ;

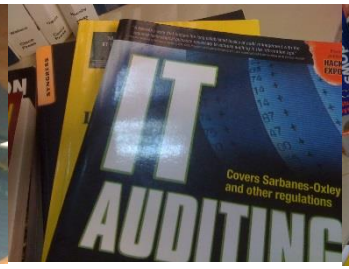
 la (ou les) charte(s) de l'utilisateur des SI à laquelle sont soumis les acteurs du processus ;

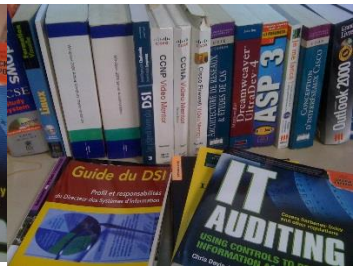
 le cas échéant, les comptes-rendus des comités ou groupes de travail consacrés pour tout ou partie au processus audité, notamment lorsqu'ils abordent le patrimoine informationnel qu'il manipule et les outils informatiques qui le servent ;

- **L'audit des processus**

 la liste des projets applicatifs en cours, principalement ceux qui ont un impact sur le processus s'ils sont identifiés selon cette clé.

Au final, l'auditeur devra porter une appréciation sur l'adaptation (efficacité, efficience, sécurité, résilience) de l'informatique aux besoins du processus audité et sur sa contribution au dispositif de contrôle interne. Il pourra le cas échéant se prononcer sur la pertinence des projets informatiques en cours, voire recommander des évolutions du système informatique.





- **L'audit de régularité**
- Les organisations s'appuient de plus en plus sur des outils informatiques. C'est à travers eux qu'elles gèrent leur ressource humaine, qu'elles exécutent leur budget et tiennent leur comptabilité, qu'elles conservent les données relatives à leurs interlocuteurs et à leurs administrés.
- Leur fonctionnement régulier est donc largement sous-tendu par la conformité aux règles de leurs systèmes informatiques, qu'il s'agisse d'inventaire des licences, de validité des règles informatiques d'exécution budgétaire et de comptabilité, de respect des normes de conservation des données personnelles, de la mise en oeuvre automatisée des règles statutaires applicables à la gestion de carrière ou au traitement des agents, etc.
- L'audit de la régularité d'une situation, qu'il s'agisse de vérifier le fonctionnement d'une entité, le déroulement d'un processus ou, plus généralement, le respect d'une norme ou d'un corpus normatif, implique donc le plus souvent l'audit des ressources informatiques qui y contribuent. L'auditeur cherchera à vérifier que les activités portées par les ressources informatiques sont en elles-mêmes régulières et à mesurer leur contribution au contrôle interne de l'entité ou du processus, par leur architecture ou les règles qu'elles portent. .

- **L'audit de régularité**
- L'auditeur devra donc, à l'occasion d'un audit de régularité :

 identifier les ressources informatiques utilisées dans le périmètre de son audit ;

 vérifier que ces ressources sont en elles-mêmes régulières (licences, respect des règles de conservation des données personnelles, respect des règles de confidentialité, etc.) ;

 vérifier que les traitements automatiques réalisés par ces ressources sont conformes au corpus normatif applicable, et évaluer leur fiabilité ;

 vérifier que la sécurité appliquée à ces ressources, outre le respect des règles de confidentialité, garantit raisonnablement qu'elles ne peuvent être utilisées à des fins frauduleuses.

- L'auditeur devra selon les cas rencontrer :

 la direction générale du périmètre auquel appartient le champ audité, pour évaluer dans quelle mesure elle est consciente de la dimension informatique de l'obligation de fonctionnement régulier qui pèse sur elle, et savoir comment cette dimension est prise en compte ;

- Il devra se procurer :

 l'inventaire des ressources informatiques utilisées dans le périmètre audité (notamment la cartographie des applications et des systèmes) ;

- **L'audit de régularité**

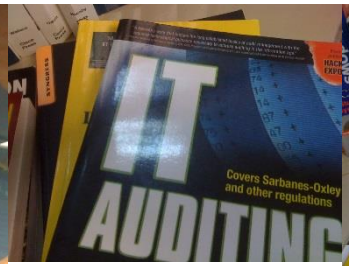
  - les contrats et inventaires de licences ;
  - les déclarations CNIL ;
  - la description du dispositif de contrôle interne incluant la part prise par l'application des règles informatiques ;
  - les rapports de vérifications issus du dispositif de contrôle interne et les bases de données répertoriant les incidents d'exploitation, pour évaluer la fiabilité des traitements informatiques ;
  - si nécessaire, les spécifications détaillées des applications concourant à la mise en oeuvre d'un corpus normatif par un traitement automatisé.

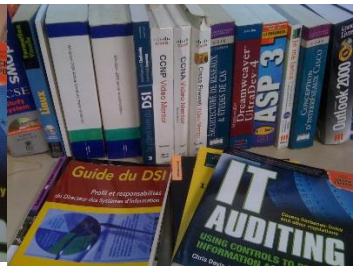
- Au final, l'auditeur devra porter une appréciation à la fois sur la valeur de la contribution de l'informatique à la régularité des opérations auditées et sur la régularité des activités informatiques elles-mêmes.
- Il lui appartient de formuler les recommandations utiles en la matière.

- **Les audits de projets non SI**
- Au-delà des projets spécifiquement informatiques (applications, infrastructures, migrations de données, etc.) qui font l'objet de développements ultérieurs, la plupart des projets contiennent une dimension informatique, qui concerne à la fois la conduite du projet et la cible visée.
- Ainsi, les ressources informatiques mises à la disposition de l'équipe projet doivent être adaptées et utilisées convenablement. Il s'agit autant d'ergonomie que de résilience et de sécurité, surtout pour un projet stratégique ou sensible.
- Par ailleurs, quel que soit le projet (organisationnel, industriel, RH, création d'un nouveau service aux administrés, etc.), la cible finale comportera très certainement une dimension informatique. Il pourra par exemple s'agir de développer les outils nécessaires à un nouveau processus, de déménager des services avec leurs ressources informatiques associées, sans rupture de la production, d'assurer la convergence entre les systèmes informatiques de deux entités fusionnées ou, au contraire, leur séparation lors d'une scission.
- Dans tous les cas, une mauvaise anticipation des opérations à réaliser sur les outils informatiques est susceptible d'avoir un impact fortement négatif sur le déroulement, voire la réussite, du projet. L'audit d'un projet devra donc en identifier les enjeux informatiques et vérifier leur correcte prise en compte.

- **Les audits de projets non SI**
- Au-delà des projets spécifiquement informatiques (applications, infrastructures, migrations de données, etc.) qui font l'objet de développements ultérieurs, la plupart des projets contiennent une dimension informatique, qui concerne à la fois la conduite du projet et la cible visée.
- Ainsi, les ressources informatiques mises à la disposition de l'équipe projet doivent être adaptées et utilisées convenablement. Il s'agit autant d'ergonomie que de résilience et de sécurité, surtout pour un projet stratégique ou sensible.
- Par ailleurs, quel que soit le projet (organisationnel, industriel, RH, création d'un nouveau service aux administrés, etc.), la cible finale comportera très certainement une dimension informatique. Il pourra par exemple s'agir de développer les outils nécessaires à un nouveau processus, de déménager des services avec leurs ressources informatiques associées, sans rupture de la production, d'assurer la convergence entre les systèmes informatiques de deux entités fusionnées ou, au contraire, leur séparation lors d'une scission.
- Dans tous les cas, une mauvaise anticipation des opérations à réaliser sur les outils informatiques est susceptible d'avoir un impact fortement négatif sur le déroulement, voire la réussite, du projet. L'audit d'un projet devra donc en identifier les enjeux informatiques et vérifier leur correcte prise en compte.

- **Les missions d'audit dont l'objet principal appartient au domaine des SI**
  - Cette sous-partie a pour objectif de montrer en quoi des audits focalisés sur l'informatique doivent s'extraire du strict périmètre de l'informatique pour aborder des dimensions ayant un impact sur le SI. Elle ne décrit bien sûr pas le cœur de la mission d'audit, objet de la troisième partie, mais donne quelques pistes pour « aller plus loin ».
  - **Les audits d'application**
- Une application n'existe que pour répondre à un besoin. Elle est conçue, réalisée, paramétrée, administrée, entretenue et utilisée par des agents appartenant ou non à l'organisation. Elle peut être utile à un ou plusieurs processus, leur être parfaitement adaptée ou au contraire être une entrave à leur bon déroulement. Elle peut s'inscrire dans une urbanisation maîtrisée ou contribuer à l'hétérogénéité, à la duplication, voire au désordre du système informatique. Elle peut donc être une source de force ou de vulnérabilité – parfois les deux – pour l'organisation.





– Les audits d'application

- Au-delà des aspects classiques d'un audit d'application en production (cf. chapitre 3), l'audit d'une application informatique peut donc nécessiter l'examen de l'urbanisation du système informatique, de la cohérence entre les logiciels et les matériels qu'ils utilisent, de l'alignement stratégique du système informatique sur les objectifs de l'organisation, voire de la gouvernance du SI, en ce qu'elle explique pour une large part les forces et faiblesses observées.
- En effet, les recommandations émises au terme de l'audit ne peuvent faire abstraction de cet environnement. Tout cela suppose une compréhension de la fonct
- Au-delà, si la correction d'une faiblesse de l'application auditée nécessite la modification d'un ou plusieurs éléments de son environnement, l'auditeur doit recommander les évolutions nécessaires.
- Ainsi, l'audit d'une application, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause : ion informatique allant très au-delà du simple objet audité.
- de l'urbanisation du système informatique ;

 de la formation des utilisateurs, y compris le personnel de la production informatique (administrateurs, soutien aux utilisateurs, etc.) ;

 de l'articulation entre les fonctions études et production ;

– **Les audits d'application**

 du ou des processus au(x)quel(s) contribue l'application, y compris le dispositif de contrôle interne mis en place pour en maîtriser les risques ;

 de l'organisation du soutien externalisé de l'application ;

 de l'organisation de la gouvernance de la fonction informatique.

- Cela vient évidemment en complément des aspects à examiner proposés en troisième partie du présent guide.
- Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas l'audit de la fonction informatique dans son ensemble mais celui d'une application bien définie. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec l'application auditée.

– Les audits des projets informatiques

- Un projet informatique n'existe que pour répondre à un besoin. Il faut donc s'assurer, au-delà du respect de la méthodologie de conduite du projet, que le besoin existe, qu'il a été convenablement recueilli et exprimé, et qu'il n'est pas perdu de vue. L'auditeur peut s'appuyer pour cela sur des outils d'analyse de la valeur1.
- L'auditeur peut se retrouver face à un projet qui, au lieu de respecter l'urbanisation en vigueur, contribue au contraire à l'hétérogénéité, voire au désordre du système informatique. Cependant, l'irrespect du cadre urbanistique par un projet ne doit pas entraîner une condamnation automatique, car cette incohérence peut révéler une urbanisation ou une organisation urbanistique inadéquates qui dans ce cas ne doivent pas nécessairement prévaloir sur le projet et ses attendus.
- Au-delà des aspects classiques d'un audit de projet (cf. chapitre 3), l'auditeur doit donc examiner la qualité de l'expression, du recueil et de la traduction du besoin, l'urbanisation du système informatique, l'inscription du projet dans cette urbanisation, voire la gouvernance du SI, en ce qu'elle explique pour une large part les forces et faiblesses observées. En effet, les recommandations émises au terme de l'audit ne peuvent faire abstraction de cet environnement. Tout cela suppose une compréhension de la fonction informatique allant très au-delà du simple objet audité.
- Au-delà, si la correction d'une faiblesse du projet audité nécessite la modification d'un ou plusieurs éléments de son environnement, l'auditeur doit recommander les évolutions nécessaires.
- Ainsi, l'audit d'un projet, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause :

– **Les audits des projets informatiques**

 des modalités d'expression et de recueil des besoins métiers ;

 du processus d'arbitrage entre projets concurrents ;

 de l'organisation de passation des marchés avec les maîtres d'oeuvres informatiques, voire avec les assistances à maîtrise d'ouvrage ;

 de la gestion des processus au sein de l'organisation, notamment du processus ayant suscité le projet audité ;

 de l'organisation de ce processus ;

 de l'organisation de la gouvernance de la fonction informatique ;

 de l'urbanisation du SI de l'organisation.

- Cela vient évidemment en complément des aspects à examiner proposés en troisième partie du présent guide.
- Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas l'audit de la fonction informatique dans son ensemble mais celui d'un projet particulier. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec ce projet.

– Les audits de sécurité

- Un dispositif de sécurité n'est pas une fin en soi. Il n'existe que pour protéger des actifs. Il faut donc s'assurer, au-delà des aspects examinés habituellement dans le cadre de l'audit de la sécurité générale informatique (cf. chapitre 3), que le dispositif de sécurité est justifié et équilibré.
- La sécurité informatique ne se résume pas à l'informatique. Elle intègre bien sûr les sécurités logique et physique de l'informatique, y compris dans leur dimension « résilience », fréquemment oubliées notamment pour les systèmes périphériques, comme les imprimantes ou téléphones en réseau, le contrôle des accès et temps de travail, l'informatique industrielle ou la gestion technique des bâtiments, mais s'étend bien au-delà. Elle s'intègre dans un dispositif global de sécurité, destiné à protéger tous les actifs de l'organisation et non seulement ses actifs informatiques ou dématérialisés, et doit être en cohérence avec les efforts réalisés en dehors du domaine informatique.

– **Les audits de sécurité**

- Elle découle d'une culture (ou inculture) de la sécurité propre à chaque organisation. Elle procède d'une identification et d'une évaluation de l'importance des actifs, d'une analyse des menaces pesant sur eux et des vulnérabilités de l'organisation, d'une décision quant à l'aversion au risque de l'organisation et aux modalités et dispositifs de sécurité qui en découlent. Elle doit aussi procéder d'une juste évaluation des contraintes normatives pesant sur l'organisation.

- Au-delà des aspects classiques d'un audit de sécurité informatique, l'auditeur doit donc examiner la qualité de l'inventaire des actifs, de l'évaluation des risques, du processus décisionnel ayant conduit à la définition d'un dispositif de sécurité et de la pertinence et la qualité de ce dispositif. En effet, les recommandations émises au terme d'un audit de sécurité ne peuvent faire abstraction de ces aspects.

– **Les audits de sécurité**

- Au-delà, si la correction d'une faiblesse du dispositif de sécurité audité nécessite la modification d'un ou plusieurs éléments de son environnement, l'auditeur doit recommander les évolutions nécessaires.
- Ainsi, un audit de sécurité, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause :

 de l'inventaire et de l'évaluation des actifs protégés par le dispositif de sécurité ;

 de l'analyse des menaces pesant sur ces actifs et des vulnérabilités devant être corrigées ;

 de la gouvernance et de la culture de la sécurité au sein de l'organisation, le cas échéant au-delà du seul périmètre informatique ;

 de l'équilibre global d'une part, entre les efforts consacrés à la sécurité informatique et ceux consacrés à la sécurité en général et, d'autre part, entre la valeur des actifs à protéger ou les normes qui leurs sont applicables et les efforts consacrés à la sécurité informatique.

– **Les audits de sécurité**

- Cela vient évidemment en complément des aspects à examiner proposés en troisième partie du présent guide.
- Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas l'audit de la sécurité dans son ensemble mais celui de la sécurité informatique. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec cette dernière.

APPROCHE THEMATIQUE ET TECHNIQUE DES PRINCIPAUX DOMAINES D'AUDIT DES SI

– Audit du pilotage des systèmes d'information

- La notion de maturité d'une organisation dans le domaine des systèmes d'information est une notion importante dans la compréhension et l'évaluation du rôle et de la performance de l'informatique dans l'organisation. Cette maturité se décline d'abord sur les plans fonctionnel et technologique, puis sur le plan organisationnel et managérial.
- L'objectif de l'audit est d'évaluer la « maturité » informatique de l'Organisation et l'adéquation du rôle, du positionnement et des objectifs de la DSI avec les enjeux de l'Organisation.

– **Audit du pilotage des systèmes d'information**

Points de contrôle

1. Rôle et positionnement de l'informatique dans l'organisation

1.1. La DSI est-elle rattachée à la DG et présente au COMEX ?

1.2. Vérifier l'existence d'une charte informatique ou de tout autre document définissant le rôle et le périmètre de responsabilité de la DSI :

- s'assurer que la DSI est limitée à son rôle de MOE (versus MOA), comprenant notamment : la conception, réalisation, mise en œuvre et l'exploitation des solutions, la responsabilité des choix d'architecture et des solutions techniques afin de garantir la cohérence d'ensemble, la (co)responsabilité des achats informatiques, ...
- vérifier que la DSI est une force de proposition et de conseil dans le domaine des technologies de l'information.

– **Audit du pilotage des systèmes d'information**

1.3. Évaluer le degré d'implication et de maîtrise de la DG dans les systèmes d'information de l'Organisation : • systèmes d'information et innovations technologiques intégrées dans le Projet de service ? • prendre connaissance des communications interne et externe.
1.4. Vérifier qu'ont été créés des Comités « informatique » (stratégique, pilotage,..) regroupant les différentes directions de l'Organisation en charge de recenser les besoins et les opportunités, gérer les priorités et suivre les projets : • évaluer le rôle et le « poids » exacts de ce comité. Prendre connaissance de ses objectifs, de sa composition et des comptes-rendus de ses réunions.
1.5. Vérifier que les métiers assurent leur rôle de MOA, en prenant en charge des aspects suivants : • le pilotage du SI et des projets ainsi que la responsabilité des budgets ; • la définition des processus et l'analyse des besoins, notamment dans le domaine de la sécurité (classification des données en termes de disponibilité, d'intégrité et de confidentialité) ; • la gestion du changement, la gestion des évolutions de l'application (gestion des demandes, arbitrages, priorités, budget) et son administration ; • la validation des traitements et la recette des nouvelles versions.

– **Audit du pilotage des systèmes d'information**

1.6. Vérifier en pratique que le leadership des grands projets : • informatiques de l'Organisation est assuré par une équipe compétence sous le contrôle et l'autorité des directions générales et métiers et que le modèle de coopération maîtrise d'œuvre / maîtrise d'ouvrage est mature et opérant.
2. Planification stratégique
2.1. Périmètre fonctionnel (couverture, ouverture et dépendance des SI).
2.2. Prendre connaissance du schéma directeur de l'Organisation (ou de ses axes stratégiques et ses grands projets) et analyser le plan informatique et la feuille de route du SI ministériel : • analyse des processus d'élaboration et de validation du plan (contenant) ; • analyse de la pertinence du plan (contenu) et de son alignement stratégique ; • analyse de l'adéquation des compétences et des ressources aux objectifs du plan.

– **Audit du pilotage des systèmes d'information**

2.4. Prendre connaissance des documents d'urbanisme de l'Organisation : • analyse des processus d'élaboration et de validation du document (contenant) ; • analyse de la pertinence du document (contenu), notamment de la délimitation des zones fonctionnelles ; • analyse des schémas directeurs des zones fonctionnelles.
2.5 Analyse des procédures de pilotage et de mise à jour du plan d'occupation des sols (POS) : • analyse des dispositifs de pilotage et de suivi de la réalisation du plan ; • analyse du rôle des comités et des procédures de mise à jour du plan (périodicité annuelle minimum) ; • analyse du positionnement dans l'Organisation et du rôle des responsables de zones fonctionnelles, de quartiers fonctionnels et de blocs fonctionnels.

– **Audit du pilotage des systèmes d'information**

2.6. Cohérence & homogénéité des technologies (homogénéité des OS, SGBD, postes de travail, langages, rationalisation des plateformes, standardisation des configurations,...).
2.7. Intégration et fiabilité des applications.
2.8. Unicité des référentiels (clients, fournisseurs, articles,...) et des saisies.
3. Budgets et coûts informatiques
Prendre connaissance et évaluer l'organisation et les processus : • analyse du processus d'élaboration et de validation du budget (qui, quand, comment) ; • analyse du périmètre du budget (géographique et organisationnel, charges et investissement,...) et évaluation de son caractère exhaustif ; • analyse de l'organisation du contrôle de gestion informatique (existence d'un contrôleur de gestion dédié au sein de la DSI ?) ;

– **Audit du pilotage des systèmes d'information**

• analyse des outils et procédures de suivi analytique, de contrôle des coûts, d'analyse des écarts et le cas échéant de refacturation des utilisateurs ; • analyse des tableaux de bord et des procédures de *reporting* (cf. chapitre Mesure et suivi de la performance).
3.2. Établir des ratios et des éléments de *benchmark* (interne et/ou externe, ratio coûts/CA, ...). Attention : à manier avec précaution, les ratios de coûts IT ne sont qu'un élément d'évaluation parmi d'autres et les benchmarks doivent être fiables pour être utilisés.
4. Mesure et suivi de la performance informatique
4.1. Des objectifs de court, moyen et long termes ont-ils été assignés à la DSI (approche BSC ?) et ces objectifs sont-ils déclinés au sein des organisations ?
4.2. Existe-t-il un comité informatique regroupant les différentes directions de l'organisation et dont les principaux objectifs sont : • le recensement des opportunités, la gestion des priorités, la validation des investissements et la politique de sécurité (stratégie) ; • le suivi et le contrôle des performances, de la qualité de la prestation et de l'atteinte des objectifs fixés (pilotage).

– **Audit du pilotage des systèmes d'information**

4.3. Vérifier l'existence et la couverture des engagements de service / *Service Level Agreement* (SLA) par application. La qualité de service, pour l'utilisateur, se mesure sur les critères de :

- disponibilité et continuité d'exploitation (disponibilité moyenne de l'application, durée maximum d'indisponibilité, perte maximum de données,..) ;
- performance (temps de réponse TP, traitement batch, Interfaces...) ;
- support (help desk et assistance utilisateur : couverture horaire et linguistique, délais de résolution des incidents, formation....) ;
- sécurité (confidentialité, intégrité des données, authentification, non répudiation,..) ;
- coûts (coûts d'évolution, coûts récurrents de fonctionnement,...).

4.4. Évaluer la pertinence des indicateurs de qualité et de performance ainsi que les moyens et outils de mesure...

– **Audit du pilotage des systèmes d'information**

4.5. La DSI tient-elle un tableau de bord (idéalement de type BSC) permettant un suivi consolidé de la performance (opérationnelle et financière) et de la qualité des prestations informatiques ? • suivi global de l'avancement du plan informatique et suivi détaillé projet par projet ; • suivi des indicateurs de performance (SLA) par application, analyse des taux de conformité, suivi de l'évolution de la performance, etc. ; • suivi des coûts (mois, YTD) rapprochés du budget ; • suivi d'indicateurs « internes » (taux d'utilisation des CPU, espace disque, analyse du portefeuille des demandes utilisateurs, productivité des études, formation et gestion des compétences internes, etc.) ; • enquête périodique de satisfaction auprès des utilisateurs, etc.
4.6. Est-il systématiquement effectué un bilan après chaque projet et notamment un bilan économique (bilan rapproché des prévisions de

– **Audit du pilotage des systèmes d'information**

l'étude préalable) ?
5. Organisation et structure de la DSI
5.1. Vérifier l'existence d'un organigramme à jour de la DSI.
5.2. Existe-il une définition de fonction et un partage clair des rôles et des responsabilités pour chaque poste figurant sur l'organigramme ?
5.3. Vérifier que l'ensemble des composantes d'une fonction informatique est convenablement pris en compte, notamment la veille technologique, la sécurité informatique, la fonction qualité & méthodes, la gestion des ressources humaines, le contrôle de gestion, le support utilisateurs (de proximité et à distance), l'administration des serveurs…
5.4. Évaluer l'adéquation des effectifs aux besoins et aux enjeux : • analyse de la couverture fonctionnelle et géographique de l'informatique ; • benchmarks internes et externes, ratios effectifs/CA et Budget IT/CA, … • analyse du recours à la sous-traitance ; • analyse de la charge du personnel informatique : horaires pratiqués, portefeuille des demandes utilisateurs, …

– **Audit du pilotage des systèmes d'information**

5.5. Évaluer l'adéquation des qualifications du personnel avec les fonctions qu'ils occupent :

- prendre en compte la stratégie de l'organisation, ainsi que le marché local de l'emploi ;
- remettre en perspective le rôle, les objectifs et les attentes vis-à-vis de l'informatique ;
- prendre en compte le niveau de risque (risque inhérent à l'activité, dépendance de l'organisation vis-à-vis de son système d'information, ...).

5.6. L'expression des besoins, les spécifications fonctionnelles et la recette des applications sont-elles effectuées par les utilisateurs ?

5.7. Les tâches, les locaux et les environnements relatifs aux fonctions études et exploitation, qu'ils soient assurés ou fournis en interne, ou externalisés, sont-ils séparés ?

- Vérifier que les accès aux bibliothèques de production (données et programmes) sont interdits aux études (y compris sous-traitants).

– **Audit du pilotage des systèmes d'information**

5.8. Vérifier l'existence d'une procédure de mise en production : • évaluer sa pertinence et son niveau d'application.
5.9. Lorsque les organisations le permettent, vérifier que les différentes tâches d'administration des bases de données -DBA- sont séparées entre les études et l'exploitation : • gestion du contenu : architecture des bases, dictionnaire de données ; • gestion du contenant : gestion des configurations et des performances.
5.10. La séparation des tâches est-elle maintenue et assurée lors de la rotation des équipes, des vacances et du départ d'un personnel ?
5.11. Évaluer le caractère « raisonnable » du turn-over de la DSI (5 à 15% / an).
5.12. Évaluer la capacité de l'Organisation à gérer les carrières des informaticiens : • prendre connaissance des évolutions sur les trois dernières années.

– **Audit du pilotage des systèmes d'information**

5.13. Vérifier l'adéquation du niveau de rémunération du personnel informatique et évaluer le « moral » des équipes : • évaluer les mesures prises par la DSI ou par les RH pour s'assurer de la cohérence vis-à-vis du marché (étude annuelle, *benchmarking*,...).
5.14. Évaluer la dépendance de l'Organisation vis-à-vis d'une ou plusieurs personnes. Éléments à prendre en compte : • développements internes versus progiciel, âge des applications et technologies mises en œuvre, taille des équipes, niveau de la documentation...
5.15. Les contrats des informaticiens contiennent-ils des clauses spécifiques de confidentialité et de non-concurrence ?
5.16. Les informaticiens sont-ils dispensés de préavis en cas de rupture brutale du contrat de travail ?
5.17. Existe-il un plan de formation nominatif pour l'ensemble des informaticiens ?
5.18. L'effort de formation est-il adapté, suffisant et s'inscrit-il dans la durée ? • 5 à 10 jours par an, sur les trois dernières années. Formation individualisée qui répond aux souhaits de l'employé et aux besoins de l'organisation.

– **Audit du pilotage des systèmes d'information**

6. Cadre législatif et réglementaire Français
6.1. Vérifier que les prescriptions légales découlant de la loi « Informatique et Libertés » sont connues (procédures de déclaration, documentation, règles de confidentialité) et respectées : • prendre connaissance et évaluer la démarche et les procédures mises en œuvre au sein de l'organisation (information, inventaire,...).
6.2. Vérifier que la loi sur la fraude informatique est connue et que des mesures préventives ont été prises : • les bannières d'accueil aux routeurs et aux serveurs d'accès distant (de type " Bienvenue.. ", " *Welcome* ",...) sont-elles bannies et remplacées par des messages d'avertissement ? • prendre connaissance de la nature et de la pertinence de la communication interne sur le sujet.
6.3. Vérifier que les lois sur l'usage de moyens de chiffrement et de la signature électronique sont connues et, le cas échéant, respectées.

– **Audit du pilotage des systèmes d'information**

6.4. Vérifier que la loi sur le contrôle fiscal des comptabilités informatisées est connue et, dans la mesure du possible, respectée : • contrôler les procédures annuelles de sauvegarde et d'archivage des données et des programmes des applications concernées ; • vérifier l'existence de documentations études, exploitation, utilisateurs et d'une procédure de mise à jour de cette documentation ; • s'assurer que ces obligations fiscales sont contractuellement prises en compte avec les fournisseurs concernés : sous-traitance d'un développement (documentation), ASP ou infogérance (mise à disposition de l'administration), ...
6.5. Vérifier que la loi sur la propriété intellectuelle / logiciel « pirate » est connue et rigoureusement respectée : • vérifier l'existence d'un inventaire des configurations logicielles ; • évaluer/valider la procédure de mise à jour de cet inventaire

– **Audit du pilotage des systèmes d'information**

(une procédure automatique doit être privilégiée) ;

- effectuer des contrôles sur un échantillon de postes de travail ;
- sur la base de l'inventaire fourni, contrôler les justificatifs de licences.

Audit de sécurité des systèmes d'information

L'information est un actif précieux de l'Organisation. À ce titre, il faut la protéger contre la perte, l'altération et la divulgation. Les systèmes qui la supportent doivent quant à eux être protégés contre l'indisponibilité et l'intrusion. La sécurité est une démarche globale de l'Organisation organisée autour d'une politique de sécurité. Il faut donc considérer les systèmes dans leur globalité et l'ensemble des acteurs.

Points de contrôle
1. Facteurs clés de succès
1.1. Une politique de sécurité est définie et correspond à l'activité de l'Organisation.
1.2. Une démarche de mise en œuvre de la gestion de la sécurité est adoptée et compatible avec la culture de l'Organisation.
1.3. La direction assure un soutien total et un engagement visible.
1.4. Les exigences de sécurité et les risques sont compris et évalués.
1.5. L'ensemble des responsables et des employés sont sensibilisés et informés.
1.6. Les lignes directrices de la politique de sécurité et des normes de sécurité de l'information sont distribuées à tous les employés et à tous les fournisseurs.
1.7. Les acteurs de la sécurité sont formés de manière appropriée.
1.8. Un système de mesure complet et mis en place afin d'évaluer l'efficacité de la gestion de la sécurité de l'information et pour collecter les suggestions d'amélioration.

Audit de sécurité des systèmes d'information

2. Politique de sécurité
2.1. Il existe une politique de sécurité formalisée avec une implication de la direction générale et une définition claire des responsabilités.
2.2. La communication se fait à tous les utilisateurs sous une forme pertinente, accessible et compréhensible au lecteur.
2.3. Une revue régulière de la politique est réalisée afin de vérifier son adéquation avec : • les évolutions des activités de l'organisation et donc des risques ; • les changements technologiques ; • l'historique des incidents.
2.4. La démarche de sécurité inclut la totalité de l'informatique et non les seuls réseaux, serveurs et applications. Les imprimantes et téléphones sous IP, l'informatique technique et industrielle, l'informatique de gestion technique des bâtiments, celle de gestion des accès et temps de travail, etc. bénéficient sans exception ni zone d'ombre du dispositif de sécurité.

Audit de sécurité des systèmes d'information

3. Organisation de la sécurité
3.1. Il existe une structure dédiée à la gestion de la sécurité de l'information : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité dans les unités.
3.2. Il y a une attribution claire des responsabilités.
3.3. Un propriétaire est désigné, il est responsable de la mise en œuvre et du suivi des évolutions à apporter.
3.4. Il existe des procédures d'autorisation de nouveaux matériels ou logiciels.

Audit de sécurité des systèmes d'information

3.5. Il existe des procédures applicables à l'accès aux informations de l'organisation par des tiers :

- les accès par des tiers aux infrastructures de traitement de l'information sont contrôlés ;
- une analyse des risques a été menée ;
- des mesures de protection de l'information ont été établies et sont acceptées contractuellement par le tiers : clause de confidentialité, transfert de propriété, responsabilités, règles d'accès physique et logique, restitution ou destruction de l'information confiée, remplacement de collaborateur....

3.6. En ce qui concerne les modalités de protection de l'information confiée à des sous-traitants, il faut vérifier :

- la prise en compte des exigences de sécurité dans les conditions contractuelles : mesures prises pour sécuriser les données pendant l'échange et pendant la conservation par le sous-traitant, modalité de restitution ou de destruction de l'information confiée, possibilité pour le sous-traitant de faire appel à de la sous-traitance, plan de continuité, clause d'audit ;
- le respect des lois pour les données personnelles et la propriété intellectuelle.

Audit de sécurité des systèmes d'information

3.7. Vérifier qu'il existe des modalités de réaction aux incidents de sécurité et aux défauts de fonctionnement : • signalement rapide des incidents de sécurité ; • signalement des failles de sécurité ; • signalement du fonctionnement défectueux de logiciels ; • capitalisation sur la résolution d'incidents ;
• processus disciplinaire.
3.8. Il existe une revue régulière de la sécurité des audits aussi bien internes qu'externes.
4. Classification et contrôle des actifs
4.1. Vérifier que les actifs sont inventoriés et hiérarchisés par valeur pour l'organisation.
4.2. Vérifier que pour tout actif important, un propriétaire est désigné et informé de ses responsabilités.
4.3. Vérifier qu'il existe un système de classification qui définit un ensemble approprié de niveaux de protection.
4.4. Vérifier que chaque actif a fait l'objet d'une étude visant à déterminer son niveau de classification.

Audit de sécurité des systèmes d'information

5. Sécurité du personnel
5.1. Vérifier que les postes et les ressources sont définis : • inclusion de la sécurité dans les responsabilités des postes ; • sélection du personnel et politique de recrutement ; • accords de confidentialité ;
5.2. Vérifier que les utilisateurs sont formés.
6. sécurité : gestion des communications et des opérations
6.1. Vérifier la documentation des procédures et les responsabilités opérationnelles.
6.2. Contrôler les modifications opérationnelles.
6.3. Vérifier l'établissement de procédures de gestion des incidents.
6.4. Vérifier la séparation des fonctions et des infrastructures.
6.5. Vérifier l'étude de sécurité en cas de gestion externe des infrastructures.

Audit de sécurité des systèmes d'information

6.6. Vérifier les mesures de protection contre les infections logiques.
6.7. Vérifier les sauvegardes des données : • réalisation régulière des copies de sauvegarde des données, des applications et des paramètres ; • distinguer sauvegarde et archivage ; • déterminer les périodes de conservation des données ; • conserver plusieurs générations de sauvegardes ; • stocker les sauvegarde en lieu sûr ; • tester régulièrement les supports de sauvegarde ; • tester régulièrement les procédures de restauration.
6.8. Vérifier les modalités de gestion des supports de données : • tenir en lieu sûr tous les supports amovibles ; • effacer de manière sécurisée le contenu des supports à réutiliser hors de l'organisation ; • établir une procédure de mise au rebut des supports prévoyant leur destruction ; • établir des procédures de manipulation des supports adaptées au niveau de sensibilité de l'information contenue.

Audit de sécurité des systèmes d'information

6.9. Vérifier les mesures de sécurisation des échanges de données :

- définition d'accords portant sur les échanges d'informations et de logiciels entre les organisations ;
- sécurité du courrier électronique.

7. Conformité

7.1. Vérifier la conformité aux exigences légales et réglementaires :

- protection des données personnelles ;
- respect de la propriété intellectuelle ;
- conservation de l'information.

7.2. Effectuer des audits de sécurité réguliers :

- internes et externes ;
- revue systématique et tests empiriques (exemple : test d'intrusion) ;
- protection des outils d'audit des systèmes ;
- protection des rapports d'audit de sécurité.

Audit de sécurité des systèmes d'information

8. Gestion des identifiants et des mots de passe
8.1. Vérifier qu'il y a un seul utilisateur par identifiant.
8.2. Vérifier que les identifiants inutilisés pendant un certain délai sont révoqués.
8.3. Vérifier que les règles de bases sont connues et mises en place : • utilisation systématique ; • le titulaire doit être le seul à connaître son mot de passe ; • changement périodique ; • règles de composition ; • procédures en cas d'inactivation ou de perte.
9. Contrôle des accès
9.1. Vérifier la définition et la documentation de la politique de contrôle d'accès : • exigences de sécurité des applications individuelles de l'organisation ; • politiques de dissémination de l'information et d'autorisation d'accès ("besoin d'en savoir") ainsi que les niveaux de

Audit de sécurité des systèmes d'information

sécurité et la classification de l'information ;

- obligations contractuelles concernant la protection de l'accès aux données ;
- profils d'accès standard des utilisateurs pour les catégories communes de travail ;
- distinction des règles obligatoires et des recommandations facultatives ;
- établissement de règles "tout est interdit sauf" plutôt que "tout est permis sauf" ;
- règles devant être validées par un responsable (séparation des fonctions).

9.2. Vérifier la gestion des accès utilisateurs :

- identification unique des utilisateurs (tous les utilisateurs) ;
- vérification que l'utilisateur a été autorisé par le propriétaire des informations ;
- suppression des droits d'accès d'un utilisateur ayant changé de poste ou quitté l'organisation ;

Audit de sécurité des systèmes d'information

- contrôle périodique et suppression des codes d'identification utilisateurs redondants et des comptes qui ne sont plus utilisés ;
- non-réaffectation des codes d'identification ;
- attribution des privilèges aux individus sur la base de leurs "besoins minimum" par rapport à la fonction qu'ils remplissent ;
- examen régulier des droits d'accès utilisateur.

9.3. Vérifier l'utilisation de mots de passe et de systèmes de déconnexion automatique :

- tout compte utilisateur doit être protégé par un mot de passe ;
- engagement des utilisateurs à :
  - ne pas divulguer leur mot de passe ;
  - ne pas écrire leur mot de passe de façon trop évidente ;
  - ne pas stocker leur mot de passe dans une procédure automatique ;
  - changer leur mot de passe dès qu'ils le soupçonnent

Audit de sécurité des systèmes d'information

- contrôler que le système impose un changement régulier du mot de passe ;
- contrôler que le système impose le choix de mots de passe robustes ;
- discipline utilisateur pour la déconnexion ;
- la déconnexion doit être automatique en cas d'inactivité prolongée.

9.4. Vérifier le contrôle des accès aux réseaux :

- authentification des utilisateurs pour les connexions externes ;
- protection des ports de diagnostic à distance et de télémaintenance ;
- contrôle des flux (*firewalls*) ;
- cloisonnement.

Audit de sécurité des systèmes d'information

9.5. Vérifier le contrôle de l'accès aux systèmes d'exploitation :

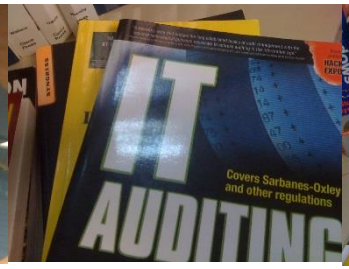
- identification / authentification des utilisateurs ;
- limitation du nombre de tentatives infructueuses ;
- enregistrement des tentatives infructueuses ;
- limitation des jours et heures de connexion ;
- affichage de la dernière connexion ;
- protection de l'accès aux utilitaires.

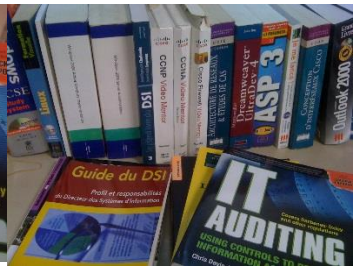
9.6. Vérifier le contrôle de l'accès aux applications :

- restriction des accès à l'information ;
- isolation des systèmes critiques.

9.7. Vérifier la surveillance des accès aux systèmes et leur utilisation :

- consignation des événements :
  - constitution des journaux d'audit :
    - ✓ qui, quand, quoi, d'où ;
- surveillance de l'utilisation des systèmes activités sensibles (opérations privilégiées, modification de la sécurité) ;
- alertes sur incident (violation, tentatives infructueuses, notification de *firewall* ou de sdi) ;
- utilisation anormale ou atypique des ressources ;
- auditabilité des journaux ;
- revue régulière des journaux ;
- synchronisation des horloges :
  - assure l'exactitude des journaux d'audit (éléments de





preuve) ;
9.8. Vérifier la gestion de l'informatique mobile : • contrôle d'accès aux ordinateurs portables ; • protection des données stockées (chiffrement) ; • protection contre les virus ; • sauvegardes ; • connexions automatiques à distance ; • sensibilisation du personnel doté d'ordinateurs portables : ▪ confidentialité du travail dans les lieux publics ou moyens de transport ; ▪ surveillance du matériel contre le vol ; ▪ espionnage industriel.
9.9. Vérifier les suites données aux incidents : • vérifier les réactions des possesseurs des ordinateurs incidentés ; • vérifier les modalités effectives de remontée de l'information sur l'incident, ses délais, son parcours, son format ; • vérifier les mesures d'isolement du ou des ordinateurs incidentés ; • vérifier l'effectivité des mesures de communication d'alerte ; • vérifier l'effectivité des mesures d'enquête et de l'exploration menée pour identifier les failles du système ayant permis l'incident. • vérifier les modalités et le contenu de la communication des rappels vers les utilisateurs à l'issue de la crise, ou des nouvelles consignes.

Audit de sécurité des systèmes d'information

10. Développement et maintenance des systèmes

10.1. Exigences de sécurité des systèmes :

- expression des besoins, contrôle interne, piste d'audit, sécurité ;
- spécification détaillée des besoins, contrôle interne, piste d'audit, sécurité ;
- audit des spécifications ;
- recette des fonctionnalités de contrôle interne, piste d'audit, sécurité ;
- audit de la recette ;
- audit "post mise en place".

10.2. Sécurité des systèmes d'application :

- validation des données d'entrée : type, limites de valeur, liste de valeurs possibles ;
- contrôle des traitements : contrôles de sessions séquentielles, totaux de contrôle ;
- exhaustivité des traitements ;

10.3. Protocole de recette :

- tests systématiques avant le passage en production ;
- utilisation d'un environnement différent de l'environnement de production ;
- participation des utilisateurs à la recette ;
- documentation de la recette et archivage ;
- séparation des fonctions développement/exploitation ;
- procédure de passage en production lors des maintenances correctives urgentes (journalisation des actions).

10.4. Sécurité des fichiers :

- contrôle des logiciels opérationnels : mise à jour uniquement par bibliothécaire, uniquement code exécutable, journal d'audit des versions ;
- protection des données d'essai des systèmes : banalisation des données de production, garder une copie pour rejouer les tests dans les mêmes conditions ;
- contrôle de l'accès aux bibliothèques de programmes sources : hors de la production, accès réservé aux développeurs autorisés, gestion des versions et conservation de l'historique des modifications.

Audit de sécurité des systèmes d'information

Informations à collecter

Organisation :

- politique de sécurité ;
- normes et standards en vigueur ;
- personnes et équipes impliquées dans l'exploitation du réseau et du parc micro (administration, maintenance, sécurité, support utilisateur ; définition des responsabilités) ;
- procédures appliquées ou prévues (mode dégradé) ;
- plans (de sauvegarde, d'archivage, de secours, de reprise, etc.) ;
- interlocuteurs pour l'audit (informatique et utilisateurs).

Audit de sécurité des systèmes d'information

Volumétrie :

- nombre d'utilisateurs ;
- volumes de données transmises ;
- taille des données sauvegardées.

Matériels :

- serveurs ;
- stations de travail ;
- équipements réseau (commutateurs, routeurs), firewalls ;
- matériel d'environnement (imprimantes, scanner et photocopieurs en réseau, téléphones IP).

Logiciels :

- systèmes d'exploitation ;
- middleware ;
- principales applications utilisées.

Communications :

- architecture du réseau (topologie) ;
- plan de câblage ;
- connexions avec l'extérieur.

Audit de la production informatique

Un audit de la fonction production consiste à analyser la capacité de l'organisation à exploiter les systèmes dans des conditions répondant aux besoins opérationnels définis par les directions utilisatrices.

Il s'agit d'analyser l'adéquation des moyens humains, matériels, logiciels et organisationnels (procédures d'exploitation, de sauvegardes, …) mis en œuvre pour répondre aux enjeux de l'organisation en termes de disponibilité de ses applications, d'intégrité et de confidentialité de ses données et enfin de conformité aux besoins opérationnels des utilisateurs (notion de qualité de service).
Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2.
Les points de contrôle proposés ci-dessous leur sont complémentaires.

Audit de la production informatique

Points de contrôle
1. Enjeux, engagements de service et suivi de la performance
1.1. S'assurer que les niveaux de services sur lesquels s'engage la production sont en adéquation avec les enjeux de disponibilité, d'intégrité et de confidentialité des différents systèmes.
1.2. S'assurer que les moyens organisationnels (ex : escalade), humains (ex : nombre et compétences des personnels d'astreinte), et matériels (ex : architecture redondante) permettent un respect des engagements de service.
1.3. Vérifier que les niveaux de service assurés par la production font l'objet de conventions de service comportant des indicateurs mesurables : valider le contenu des conventions de services. S'assurer que les principaux attributs de la prestation font l'objet d'indicateurs de mesure de la performance et d'objectifs quantifiés. Juger la pertinence des indicateurs et l'ambition des objectifs au regard des enjeux.
1.4. S'assurer que le suivi de la performance est un process continu : demander les derniers comptes-rendus à l'attention des utilisateurs. En cas de non-respect des objectifs de la convention de service, valider la pertinence des actions correctives entreprises.

Audit de la production informatique

Vérifier que les tableaux de bords de production font l'objet d'un suivi adéquat :
se faire communiquer les tableaux de bords de production et juger de leur pertinence aussi bien que de leur complétude ;
s'assurer de l'existence de procédures permettant à l'équipe de production de remédier aux éventuels problèmes identifiés par l'intermédiaire des tableaux de bords.

2. Organisation de la fonction production

2.1. S'assurer que la ligne de partage entre études et production est clairement définie et documentée.

2.2. Vérifier que l'organisation de la production correspond à une réponse adaptée aux besoins opérationnels de l'organisation :

- comprendre la structuration du service production. Identifier les modalités de découpage des rôles et responsabilités (découpage par application, par technologie, par niveau de support ...) et s'assurer qu'ils permettent de répondre de manière adéquate aux enjeux de disponibilité, de sécurité et d'intégrité ;
- valider l'indépendance de la production par rapport aux études ;
- vérifier l'existence de convention de service par application ;

Audit de la production informatique

- vérifier l'existence de moyens de communication normalisés entre production et autres acteurs de l'organisation ;

2.3. Vérifier que les technologies opérées sont suffisamment maîtrisées :

- identifier les différentes technologies utilisées, valider l'existence pour chacune d'entre elles des compétences suffisantes tant d'un point de vue qualitatif que quantitatif et, si la taille du service de production le justifie, des grilles croisées compétences / individus ;
- revoir les budgets formation et l'adéquation des formations avec les technologies actuelles et celles induites par le déroulement du plan informatique.

2.4. Vérifier qu'il existe une bonne maîtrise des différentes missions de la production :

- identifier le périmètre couvert par la production et en dériver les principales missions assumées ;
- valider la couverture de ces différentes missions dans les descriptions de postes ;
- se focaliser sur les aspects autres que l'opération des systèmes : ex : production d'indicateurs de pilotage, *capacity planning*, veille technologique, revue qualité, ...

Audit de la production informatique

3.3. Vérifier que le dimensionnement des architectures actuelles permet de répondre aux engagements de services (indicateurs de pilotage et de mesure de la performance).

3.4. Vérifier que les infrastructures ne sont pas manifestement surdimensionnées en regard des besoins actuels et prévisibles.

3.5. Vérifier que les configurations matérielles (redondance matérielle et réseau, architecture disques, *clustering* CPU, média de sauvegarde, ...) permettent de garantir le niveau de disponibilité sur lequel la production s'engage.

Type de questions :

- les systèmes de disques ou de stockage d'information (SAN, ...) prémunissent-ils contre des pertes d'information ?
- les sauvegardes, leur périmètre, et les temps de restauration sont-ils adaptés et en ligne avec les engagements de la production ?
- les accès réseaux sont-ils doublés et les architectures sont-elles doublées ?

Audit de la production informatique

4. Livraisons en production

4.1. Vérifier les conditions et procédures de livraisons en production. Valider la démarche de contrôle des livraisons en production et *a minima* les points de contrôles suivants :

- recette fonctionnelle entre études et utilisateurs (PV de recette) ;
- réalisation de tests d'intégration ;
- test des procédures et des packages de livraisons, y compris retour arrière ;
- sauvegarde des environnements impactés avant livraison ;
- livraison effectuée à un moment où un retour arrière est possible sans impacter le service client (le soir, le week-end, ...) ;
- recette d'exploitation entre études et production (PV de recette).

4.2. Vérifier les conditions et procédures de livraisons en production. Valider le niveau de responsabilité de la production par rapport aux livraisons des études :

- la production a-t-elle un pouvoir de veto si elle estime qu'il n'y a pas de garantie quant au risque relatif à la livraison (tests non effectués, sources non fournies, livraison non packagée et non documentée, ...) ;
- les études mettent-elles à disposition dans un environnement étanche les sources et la production prend-elle le relais pour les opérations ultérieures (compilations, paramétrage, ...).

4.3. Vérifier la nature des tests effectués par la production. S'assurer que les machines et les environnements disponibles permettent de réaliser le cas échéant les tests suivants :

- test de montées en charge (volumétrie pour du transactionnel[2] et exploitabilité pour des traitements asynchrones) ;
- intégration technique portant non seulement sur de l'intégration au niveau du système mais aussi au niveau de l'interaction avec l'ordonnanceur de production et le

Audit de la production informatique

- intégration technique portant non seulement sur de l'intégration au niveau du système mais aussi au niveau de l'interaction avec l'ordonnanceur de production et le système de remontée d'alerte ;
- tests d'interface avec d'autres applications ;
- intégration dans l'architecture réseau (filtrage de ports TCP/IP par un *firewall* par exemple).

Audit de la production informatique

5. Exploitation et gestion des incidents

5.1. Vérifier le découpage de la journée de production en tâches clairement délimitées permettant la mise en œuvre de points d'arrêt. S'assurer que les traitements s'inscrivent dans la logique suivante :

- tout traitement impactant des données sensibles peut faire l'objet d'un retour arrière (*archivelog*, sauvegarde, *roll back*[3], *timestamp*[4]) ;
- un traitement modifiant des données commence par analyser la validité des données (syntaxe, *timeliness*, ...) avant d'effectuer une mise à jour et permet de rejeter selon des règles connues les transactions ou les lots comportant des anomalies ;
- tout rejet possible par le système génère une alerte et est dûment couvert par une procédure de recyclage ;
- l'échec d'un traitement isolé n'empêche pas de respecter les délais de déroulement de la journée de production (temps de réalisation d'un traitement très inférieur aux marges de sécurité).

Audit de la production informatique

5.2. Vérifier la validité des assertions suivantes :

- les alertes sont remontées en temps réel à la console d'administration (système de gestion d'alerte - pull et push : la console vérifie le statut d'un système, un traitement peut remonter une alerte) ;
- les applications et les systèmes opérés génèrent des fichiers d'erreurs exploitables (*tracelog*, ...) ;
- l'ordonnanceur de production ou les outils utilisés (batch d'exécution) permettent l'arrêt du déroulement des traitements en cas d'erreur grave ;
- le niveau d'automatisation de la production permet de décaler des jobs non critiques et de mesurer l'impact sur le chemin critique (i.e. le chemin critique de production et les marges de sécurité sont identifiés) ;
- les outils systèmes offrent des garanties comme intégrité et *timeliness* des fichiers intermédiaires (puits de données --> *Cortex Sink*) et capacité de retour arrière (*Roll Back* automatique de SGBD) si non pris en compte dans le chemin d'exploitation (sauvegarde intermédiaire) ou dans les traitements.

Audit de la production informatique

5.3. Vérifier le patrimoine documentaire utilisé par l'exploitation :
existe-t-il des guides de production par application ?

- le séquencement des tâches de production est-il correctement documenté (dans le robot ou sur papier) ?
- les différents points de reprise sont-ils clairement identifiés ?
- existe-t-il une main courante de production traçant tout événement anormal intervenu et les actions correctives entreprises ?
- existe-t-il un référentiel listant typologies d'incidents et actions de résolution à entreprendre ? (alimenté sur la base des anomalies résolues dans le passé).

Audit de la production informatique

5.4. Analyser les procédures d'exploitation :

- existe-t-il une typologie claire de gravité d'incident ?
- existe-t-il une procédure d'escalade décrivant spécifiquement quels sont les moyens de résolution des problèmes (*troubleshooting*) à mettre en œuvre par chaque niveau et les délais régissant l'escalade. La procédure d'escalade permet-elle le respect des engagements de disponibilité (SLA) ?
- les actions à entreprendre en fonction du type d'incident sont-elles documentées (ex : fermer le transactionnel, faire une sauvegarde, générer un cliché (*snapshoot*) sur un environnement pour faire du débogage, vérifier un certain nombre d'éléments, ...) ?
- les astreintes sont-elles explicites ? Couvrent-elles uniquement le support production ou incluent-elles les études ? Sont-elles en adéquation avec les engagements de disponibilité ?
- les compétences disponibles au sein de la production permettent-elles un support adéquat de tous les environnements ?

Audit de la production informatique

6. Procédure de sauvegarde et de reprise

6.1. Identifier les différentes sauvegardes effectuées et les croiser avec les besoins existants. Valider que toute sauvegarde répond à un besoin précis et que tous les besoins sont couverts :

- peut-on faire repartir l'exploitation à partir de sauvegarde sur site avec des caractéristiques de rechargement intégrant des besoins de forte réactivité (*mirroring*[3], *dump* (sauvegarde en masse) de données, ...) ?
- gère-t-on un archivage spécifique pour répondre aux obligations de la loi de finances pour 1990 sur les comptabilités informatisées ?
- gère-t-on des sauvegardes externalisées permettant de se prémunir contre une perte de tout ou partie du SI ?
- les périmètres incorporés dans les sauvegardes permettent une reconstruction complète d'un système (OS, programmes, données).

Audit de la production informatique

6.2. Valider que les éléments suivants font partie intégrante des procédures de sauvegarde :

- plan de sauvegarde identifiant par serveur / application, le périmètre de sauvegarde (fichiers, programmes, paramètres, os,..) et la cyclicité ;
- acteurs (homme, système de sauvegarde) en charge de la réalisation et du contrôle des sauvegardes ;
- plannings prévisionnels de tests de restauration ;
- clauses de révision des procédures de sauvegardes et des périmètres (nouvelle livraison applicative, migration serveur, ...) ;
- règle de remplacement et stockage des medias de sauvegarde.

Audit de la production informatique

6.3. Vérifier le bon suivi des procédures de sauvegarde :

- consulter les comptes rendus de sauvegardes et valider la prise en compte de tout incident mentionné ;
- vérifier les bordereaux d'entrée / sortie des media supportant les sauvegardes externalisées ;
- s'assurer que le dernier changement des media de sauvegarde est en ligne avec ce que préconise la procédure ;
- rapprocher le planning des livraisons en production et valider que les éventuelles modifications de périmètre ont bien été incorporées dans les procédures.

6.4. Se focaliser sur les aspects de restauration :

- s'assurer qu'il existe des procédures de restauration précisant les modalités selon lesquelles on peut remonter partiellement ou totalement un système en partant des sauvegardes.

6.5. Valider le suivi du planning prévisionnel de tests de restauration :

- consulter les comptes rendus des derniers tests de restauration ;
- regarder l'effectivité du plan d'action déroulant du résultat des tests de restauration ;
- rapprocher le planning de livraison applicative avec les procédures de restauration et valider que ces dernières sont

Audit de la production informatique

7. La maintenance du matériel et du logiciel de base

7.1. Valider la complète couverture des matériels critiques et logiciels de base par des contrats de maintenance adaptés. Vérifier les engagements de disponibilité et les contrats de maintenance hardware ainsi que les clauses d'exclusion de garantie :

- est-ce que tous les serveurs critiques sont couverts ? Si non, le fabriquant assure-t-il encore la maintenance de ce matériel ?
- en est-il de même pour les baies de disques et les éléments actifs de réseau ?
- les délais contractuels d'intervention et de réparation sont-ils en adéquation avec les engagements de disponibilité ? Les clauses de pénalités financières sont-elles réalistes et applicables ?
- les conditions physiques de stockage du matériel sont-elles susceptibles de faire appliquer les clauses de dégagement de responsabilité ? (température, poussière, hygrométrie,..) ?

7.2. Vérifier les engagements de disponibilité et les contrats de maintenance des logiciels de base ainsi que les clauses d'exclusion des garanties contractuelles :

- est-ce que tous les OS utilisés sont couverts par un contrat de maintenance ? Si non, l'éditeur assure-t-il encore la maintenance de la version utilisée et cette version est-elle compatible avec d'éventuels « *upgrades* » matériels ?
- en est-il de même pour les SGBD, robot d'exploitation et autres outils d'administration (remontée d'alerte,

Audit de la production informatique

administration réseau, ...)

- les délais contractuels d'intervention et de réparation sont-ils en adéquation avec les engagements de disponibilité ? Les clauses de pénalité financière sont-elles réalistes et applicables ?

Audit des Applications informatiques en service

Une application informatique (« application software ») est un logiciel accompagnant, automatisant, ou se substituant à un processus ou une partie de processus de l'organisation.

Une application comprend:

- des programmes, des données, des paramètres, une documentation mais aussi des habilitations pour gérer les accès aux données et aux transactions de l'application.

L'audit d'une application peut avoir deux visées distinctes : l'audit de fiabilité et de sécurité ou l'audit d'efficacité et de performance. Un audit complet couvrira ces deux périmètres.

L'audit de fiabilité et de sécurité a pour objectif d'émettre une appréciation motivée sur la fiabilité de l'outil informatique, c'est-à-dire sur la qualité du contrôle interne de l'application et la validité des données traitées et restituées. Ce type d'audit permettra de mettre en évidence d'éventuelles failles dans la chaîne de contrôle composée de contrôles programmés effectués par la machine et de contrôles manuels restant à la charge des utilisateurs.

L'audit d'efficacité et de performance a pour objectifs d'apprécier l'adéquation de l'application aux besoins et aux enjeux de l'organisation, d'évaluer sa contribution à la création de valeur, d'évaluer sa performance et sa rentabilité et enfin d'évaluer sa pérennité et sa capacité d'évolution.

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires

Audit des Applications informatiques en service

Points de contrôle
1. Audit de la sécurité et de la fiabilité : analyse des risques associés à l'organisation
1.1. Existe-t-il un comité informatique, présidé par la direction générale et au sein duquel les directions utilisatrices sont représentées et influentes (stratégie, contrôle et pilotage,..) ?
1.2. Existe-il, au sein de l'organisation, une « politique » relative aux applications, connue, partagée et mise en œuvre : • couvrant l'ensemble du cycle de vie de l'application (conception, exploitation) ; • favorisant la responsabilisation et l'appropriation par les utilisateurs de leur système d'information ? La notion de « propriété » d'application est-elle utilisée ?
1.3. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application sont-ils clairement identifiés et couvrent-ils l'analyse des risques, la définition des besoins de sécurité, la gestion des changements et des évolutions, l'administration de l'application ?
1.4. A-t-il été réalisé une analyse des risques, spécifique à l'application, qui a débouché sur la définition des besoins de sécurité (classification formelle des données et des traitements en termes de disponibilité,

Audit des Applications informatiques en service

d'intégrité et de confidentialité) ?

1.5. Dans le prolongement de l'analyse des risques et de l'expression des besoins de sécurité, a-t-il été mis en œuvre un contrat de service (SLA) entre l'informatique et la direction utilisatrice ?

1.5. Indépendamment de l'application :

- prendre connaissance et analyser le niveau de contrôle interne et de séparation des tâches au sein de la direction utilisatrice ;
- évaluer le niveau de sensibilité des utilisateurs à la sécurité ainsi que le niveau de « maturité » de l'organisation vis-à-vis de ses systèmes d'information.

1.7. Existe-il un manuel d'administration de l'application, à jour et maîtrisé, comprenant notamment : mode d'emploi du manuel,

Audit des Applications informatiques en service

1.8. Vérifier l'existence de procédures formalisées imposant l'accord du « propriétaire » de l'application pour tout changement sur :

- les programmes de l'application (maintenance corrective et évolutive) ;
- la planification des traitements informatiques (batch, clôture, ...) ;
- l'environnement technologique de l'application ;

Vérifier que l'administration est bien assurée par les utilisateurs.

1.9. Le « propriétaire » dispose-t-il d'un compte-rendu (*reporting*) mensuel « intelligible » de la performance de l'application, dans le respect du contrat de service ?

Audit des Applications informatiques en service

1.10. Existe-il un guide utilisateurs / manuel de procédures, diffusé, à jour et maîtrisé, comprenant notamment : • mode d'emploi du manuel, présentation de l'application, mode opératoire, règles de gestion, écrans et zones de saisie, liste des messages d'erreurs, états de contrôle et d'exception, documentation des pistes d'audit ; • description des contrôles programmés et des contrôles manuels compensatoires à chaque phase du traitement (mode opératoire, procédure d'escalade et/ou de recyclage des anomalies, délais de mise en œuvre, ...).
2. Audit de la sécurité et de la fiabilité : Analyse des risques associés à l'application
2.1. L'accès aux ressources de l'application (données et transactions) est-il restreint par un système de gestion d'accès ?
2.2. Existe-t-il une procédure de gestion des profils utilisateurs de l'application placée sous la responsabilité du propriétaire de l'application (procédure de création / modification et suppression des droits d'accès) ? Un dispositif de SSO est-il mis en œuvre ?

Audit des Applications informatiques en service

2.3. Chaque utilisateur possède-t-il un identifiant qui lui est propre ? Vérifier qu'il n'existe pas de compte « générique » et que l'informatique (chef de projet) n'a que des accès en lecture au même titre que d'éventuels sous-traitants et éditeurs.

2.4. Le mot de passe associé à l'identifiant permet-il d'assurer une protection d'accès efficace (7 caractères minimum, gestion de l'historique des mots de passe sur 2 ans, contrôle de « trivialité », changement trimestriel des mots de passe, etc.) ?

2.5. Les tentatives de connexions infructueuses à l'application sont-elles enregistrées et contrôlées par le propriétaire de l'application? Sont-elles limitées ?

2.6. L'accès aux données et aux transactions de l'application peut-il être correctement paramétré en fonction des tâches des utilisateurs ou le système de confidentialité est-il basé sur le contrôle d'accès aux données ?

2.7. La séparation des tâches est-elle respectée dans le paramétrage des profils ?

- comparer les droits d'accès avec les fonctions des utilisateurs ;
- vérifier l'adéquation entre les droits et les profils ;
- vérifier que toutes les personnes ayant des droits d'accès sont toujours dans le service / l'organisation.

2.8. La piste d'audit sur le système d'administration de l'application est-elle assurée et régulièrement contrôlée ?

2.9. Tous les documents servant de base à la saisie sont-ils préparés, préformatés, complets et approuvés avant saisie ?

Audit des Applications informatiques en service

2.14. Les opérations effectuées sur des données sensibles sont-elles l'objet d'une piste d'audit suffisante et régulièrement analysée ?

- identité de l'auteur de l'opération ;
- entité / fichier /donnée sur laquelle l'opération a été effectuée ;
- date et heure des événements ;
- valeur avant et après l'opération.

Objectifs de contrôle de la piste d'audit :

- évaluation de la qualité des pistes (couverture, exploitabilité, ...) ;
- évaluation de la sécurité des pistes (sécurité de ses constituants : OS, SGBD, ...) ;
- évaluation de la gestion des pistes (procédures de contrôle, archivage, ...).

2.15. Les procédures de transmission de fichiers en entrée assurent-elles l'exhaustivité et l'exactitude des informations transmises (contrôles systèmes) ?

Audit des Applications informatiques en service

2.16. Les contrôles mis en œuvre lors de l'intégration des données par fichiers à l'application sont-ils suffisants et identiques à ceux mis en œuvre dans le cadre d'une saisie transactionnelle (contrôles applicatifs) ?
2.17. Le système prévoit-il de conserver toutes les données rejetées dans un fichier d'anomalies protégé et de les éditer en vue d'un contrôle et d'un recyclage ?
2.18. Les données rejetées sont-elles analysées et corrigées dans des délais raisonnables et compatibles avec les délais de validation des traitements ?
2.19. Les corrections des données rejetées subissent-elles les mêmes contrôles que les données initiales, et jouissent-elles d'une piste d'audit suffisante ?

Audit des Applications informatiques en service

2.20. Toutes les opérations de mise à jour des données sensibles sont-elles journalisées (transactions, traitements batch) ?
2.21. Toutes les opérations de mise à jour des données sensibles sont-elles journalisées (transactions, traitements batch) ?
2.21. Rapproche-t-on les totaux de contrôle de fin de journée et la différence est-elle analysée au travers des transactions journalisées ?
2.22. Des contrôles automatiques périodiques, notamment de vraisemblance, sont-ils effectués afin de vérifier l'intégrité des montants gérés par l'application (niveau applicatif ou base de données) ?
2.23. La couverture, le contenu et la distribution des états de sortie de l'application sont-ils adaptés aux enjeux et à l'organisation de l'organisation ?
2.24. Effectuer une revue détaillée des états disponibles et de leur destinataire et vérifier que chaque nouvel état de sortie fait l'objet d'une procédure de recette.
2.25. Chaque utilisateur dispose-t-il du bon niveau d'information et de moyen de contrôle adapté ?
2.26. La distribution des états de sortie est-elle sous contrôle (existence d'une procédure permettant l'identification et la validation formelle des destinataires) et leur niveau de confidentialité assuré ?
2.28. Les contrôles utilisateurs des états de sortie font-ils l'objet de procédures formalisées (guide de procédures), connues et appliquées ?

Audit des Applications informatiques en service

2.29. Les procédures de validation des résultats (Qui, Quand, Comment), de classement et d'archivage des états produits sont-elles adaptées, formalisées, connues et appliquées ?

- existence d'une procédure, identification des responsables, délai de mise à disposition des états et délai de validation, procédures à suivre en cas d'incident.

2.30. Lorsque l'application est la juxtaposition de plusieurs modules, l'homogénéisation des codifications et des règles de gestion a-t-elle été assurée ?

2.31. L'intégrité et l'exhaustivité des données transmises entre les différents modules de l'application et/ou à des applications en aval sont-elles assurées ?

Audit des Applications informatiques en service

3. Audit de la sécurité et de la fiabilité : analyse des risques associés à la fonction informatique
3.1. Au sein du service informatique, les tâches relatives au développement et à l'exploitation de l'application sont-elles séparées ? • Prendre connaissance de l'organigramme de la DSI, des descriptions de travaux (*Job description*) et de la procédure de mise en production.
3.2. L'accès aux bibliothèques de production (données et programmes) est-il interdit aux analystes-programmeurs ? • Sans réelle étanchéité des environnements de développement et de production, la séparation des tâches reste toute théorique. Analyser les droits d'accès. Un accès en lecture pour les chefs de projets est généralement admis.
3.3. La séparation des tâches est-elle maintenue et assurée en cas d'absence d'un salarié (maladie, vacances,..) ?
3.4. L'équipe actuelle en charge de la maintenance (interne ou externe) a-t-elle une maîtrise suffisante de l'application et les moyens de la faire évoluer ?
3.5. Existe-t-il une procédure formalisée et standard de maintenance de l'application validée par l'informatique et la maîtrise d'ouvrage concernée ?

Audit des Applications informatiques en service

3.6. Les nouvelles versions (développement interne, progiciel) sont-elles systématiquement testées puis recettées dans un environnement dédié avant d'être livrées à l'exploitation ?
3.7. Existe-t-il une procédure formalisée de transfert des programmes entre les environnements de recette et d'exploitation ?
3.8. La documentation de l'application est-elle systématiquement mise à jour après chaque intervention de maintenance ?
3.9. Les corrections effectuées en urgence sur les programmes sont-elles effectuées dans un cadre bien défini et formalisé ? Font-elles l'objet d'un rapport systématiquement revu par la direction informatique ?
3.10. Un logiciel de contrôle de programmes sources et de programmes exécutables est-il utilisé pour identifier et tracer toute modification effectuée (piste d'audit) ?
3.11. Les travaux batch de l'application, qu'ils soient périodiques ou à la demande, sont-ils systématiquement planifiés et formellement validés par le responsable d'exploitation et par le responsable utilisateur ?
3.12. Existe-t-il une procédure de contrôle des traitements batch et d'archivage des comptes-rendus d'exécution ?
3.13. La gestion des incidents en général et les procédures d'urgence en particulier sont-elles définies et correctement documentées ?
3.14. La documentation d'exploitation est-elle à jour, dupliquée, protégée et inclut-elle les procédures de gestion des incidents et de reprise / redémarrage ?

Audit des Applications informatiques en service

3.15. Vérifier l'existence et l'application d'un Contrat de Service (SLA) pour l'application :

- vérifier que le SLA couvre les besoins de disponibilité, d'intégrité et de confidentialité de l'application et de ses données ;
- valider que les engagements de service sont en adéquation avec l'analyse des risques.

3.16. Vérifier que les moyens organisationnels (ex : escalade, astreintes, procédures et *reporting*, ...), humains (effectif, compétences des personnels), matériels et logiciels (ex: architecture redondante, outil de mesure, ...) permettent le respect des engagements de service et la mesure rigoureuse du niveau de service.

3.17. Évaluer le niveau de service par l'analyse des tableaux de bord.

3.18. Les procédures de sauvegarde et de reprise de l'application sont-elles satisfaisantes et répondent-elles aux enjeux de l'application et aux engagements de service de l'informatique ?

3.19. Une partie des sauvegardes est-elle stockée à l'extérieur de l'organisation (banque, société spécialisée) selon une périodicité adaptée aux enjeux ?

Audit des Applications informatiques en service

3.20. En cas de sinistre grave, existe-t-il un plan de secours en adéquation avec les besoins et les enjeux (plan d'urgence, plan de repli, plan de reprise) ? • vérifier le dimensionnement des moyens mis en place ; • déterminer les faiblesses du plan de secours existant (axes d'analyse : étude d'impact financier, sites de repli, plan de secours informatique, plan de secours télécom, sauvegardes des documents, procédures, organisation, logistique).
3.21. Ce plan est-il périodiquement testé et mis à jour ?
3.22. L'organisation dispose-t-elle d'un responsable sécurité et d'une politique formalisée en matière de sécurité informatique, conforme à la réglementation ? Cette politique couvre-t-elle la fonction informatique ?
3.23. Les accès aux commandes système, aux bibliothèques et bases de données de production sont-ils protégés (logiciel de contrôle) et limités au personnel d'exploitation ?
3.24. Les accès aux logiciels de base et utilitaires sensibles sont-ils contrôlés et systématiquement "tracés" ?
3.25. Existe-t-il des procédures de contrôle périodique des accès aux ressources de l'application (analyse des « logs[6] » par le responsable de la sécurité) ?

Audit des Applications informatiques en service

4. Audit d'efficacité et de performance: adéquation de l'application aux besoins
4.1. Le projet s'inscrit-il dans le schéma-directeur du système d'information et ce dernier est-il aligné avec le schéma directeur de l'organisation ?
4.2. Évaluation de l'alignement stratégique de l'application : • vérifier l'existence d'une maîtrise d'ouvrage « forte » et impliquée ; • vérifier que la direction générale a participé à l'étude préalable et a validé le projet et notamment l'analyse coûts/bénéfices ; • vérifier que le cahier des charges de l'application prend en compte tous les aspects du problème posé et du domaine fonctionnel considéré ; dans le cas contraire, vérifier que le management avait connaissance de ces lacunes lors de la validation des spécifications ; vérifier que les choix effectués ne compromettent pas l'intégration des fonctionnalités complémentaires dans une phase ultérieure ;

Audit des Applications informatiques en service

4. Audit d'efficacité et de performance: adéquation de l'application aux besoins
4.1. Le projet s'inscrit-il dans le schéma-directeur du système d'information et ce dernier est-il aligné avec le schéma directeur de l'organisation ?
4.2. Évaluation de l'alignement stratégique de l'application : • vérifier l'existence d'une maîtrise d'ouvrage « forte » et impliquée ; • vérifier que la direction générale a participé à l'étude préalable et a validé le projet et notamment l'analyse coûts/bénéfices ; • vérifier que le cahier des charges de l'application prend en compte tous les aspects du problème posé et du domaine fonctionnel considéré ; dans le cas contraire, vérifier que le management avait connaissance de ces lacunes lors de la validation des spécifications ; vérifier que les choix effectués ne compromettent pas l'intégration des fonctionnalités complémentaires dans une phase ultérieure ;

Audit des Applications informatiques en service

- vérifier que le projet s'intègre de façon satisfaisante dans le système d'information existant (intégration technique et fonctionnelle) et que l'unicité des référentiels de l'organisation est assurée (bases clients, produits, entités, fournisseurs, référentiel comptable, ...) ;
- sur la base du bilan de projet (lorsque qu'il existe), vérifier que le projet a atteint ses objectifs et couvre tous les aspects du domaine fonctionnel ; le cas échéant, analyser les écarts et vérifier qu'ils ont été portés à la connaissance de la

Audit des Applications informatiques en service

direction générale.
4.3. Les utilisateurs ont-ils été suffisamment associés à la définition des spécifications ou au choix de la solution puis aux évolutions successives ?
4.4. Les utilisateurs réalisent-ils toutes leurs tâches dans l'application (évaluation du taux d'automatisation des opérations) ?
4.5. Sinon, maintiennent-ils des systèmes parallèles (ancien système, tableurs) en dehors de l'application ? Existe-t-il des saisies multiples ?
4.6. Adéquation aux besoins des utilisateurs : • la totalité des fonctionnalités de l'application est-elle utilisée et maîtrisée par les utilisateurs ? • l'ergonomie de l'application est-elle satisfaisante ? Par exemple, la saisie d'une transaction récurrente est-elle suffisamment productive (nombre d'écrans optimisé, saisie assistée, temps de réponse acceptable, ...) ? • les rapports issus du système répondent-ils convenablement aux besoins des utilisateurs ? En particulier chaque niveau de management dispose-t-il de l'information qui lui est nécessaire (adéquation à l'organisation) ? • le support utilisateur (technique et fonctionnel) est-il satisfaisant et adapté aux utilisateurs et aux enjeux ? • la documentation utilisateur est-elle adaptée, complète, accessible et permet-elle une utilisation optimale de l'application ?

Audit des Applications informatiques en service

• la formation des utilisateurs est-elle suffisante, adaptée et périodique, notamment pour une activité où le « turn-over » est important ? • existe-t-il des enquêtes périodiques de satisfaction auprès des utilisateurs ? À l'aide ou non de ces enquêtes, évaluer le
niveau de satisfaction des utilisateurs (performance de l'application, appropriation et maîtrise, qualité de la formation et du support, absence de phénomène de rejet, ...) ?
5. Audit d'efficacité et de performance : analyse de la performance et de la rentabilité
5.1. Une évaluation de la rentabilité de l'investissement a-t-elle été établie préalablement au développement ou à l'acquisition de l'application ?
5.2. Cette évaluation a-t-elle intégré les coûts de déploiement mais aussi les coûts d'exploitation/charges récurrentes ?
5.3. A-t-on étudié sérieusement les offres du marché (progiciel) avant de se lancer dans un développement spécifique ?
5.4. Les délais de mise en œuvre de l'application sont-ils « raisonnables » (impact d'un éventuel « effet tunnel ») et conformes au planning initial ?

Audit des Applications informatiques en service

5.5. Un bilan post-projet a-t-il été effectué afin de mesurer l'atteinte des objectifs ?
5.6. La réduction des charges (notamment de personnel et d'exploitation) et/ou des délais (délais de traitements, délais de clôture, ...) est-elle conforme à la réduction attendue lors de l'étude préalable ?
5.7. A-t-on constaté des améliorations non quantifiables, définies ou pas lors de l'étude préalable (amélioration de la sécurité, du service client, ...) ?
5.8. A-t-on réalisé une réingénierie des processus (*Business Process Reengineering* (BPR) ou une étude d'organisation préalablement à la rédaction du cahier des charges ?
5.9. Les processus métiers sont-ils performants et optimisés (rechercher toute source d'amélioration possible) ?
5.10. Les traitements sont-ils performants et les données cohérentes et fiables (voir guide d'audit « Fiabilité et Sécurité d'une application ») ?
5.11. L'architecture technique est-elle adaptée et optimisée, notamment les bases de données (bon dimensionnement des configurations, gestion des évolutions techniques, personnalisation (*tuning*) des bases de données, ...) ?

Audit des Applications informatiques en service

5.12. A-t-on mis en place des indicateurs de performance et un contrat de service adaptés aux enjeux entre l'informatique et les utilisateurs : • disponibilité de l'application, le cas échéant par plage horaire ; • temps de réponse, le cas échéant par transaction et traitement sensibles ; • gestion des incidents et du support utilisateurs, fiabilité des traitements par lots (*batch*) ; • gestion des demandes de maintenance et gestion des droits d'accès ; • continuité d'exploitation et site de back-up.
5.13. Les outils de mesure de la performance et les tableaux de bord sont-ils adaptés aux besoins et aux indicateurs, sans contestation possible ?
6. Audit d'efficacité et de performance : analyse de l'évolutivité/pérennité de l'application
6.1. Les technologies utilisées sont-elles conformes aux standards de l'organisation ?
6.2. Le logiciel est-il de conception récente et fondé sur des technologies portables, non obsolètes et évolutives (matériel, OS, SGBD, outils de développements, ...) ?
6.3. Les technologies utilisées sont-elles matures et suffisamment répandues sur le marché (Linux, J2EE, .net,..) ? Les compétences existent-elles sur le marché notamment dans le contexte d'un déploiement à l'international ?
6.4. Les technologies utilisées ont-elles suffisamment de marge pour faire

Audit des Applications informatiques en service

face à un nombre croissant d'utilisateurs et de transactions (cf. Business Plan) ?

6.5. L'application est-elle techniquement et fonctionnellement intégrée dans le SI ?

6.6. L'application est-elle modulaire, paramétrable et conceptuellement adaptée aux éventuelles évolutions de l'activité, notamment :

- capacité d'adaptation à une internationalisation (multilingue, multidevise et multiprotocole, ...)?
- capacité d'intégrer une nouvelle entité juridique, un nouveau produit, un nouveau métier, ... ?
- capacité de « filialiser » un métier de l'Organisation ou de décentraliser certaines activités ?
- capacité d'un déploiement massif (client léger versus client lourd, ...) ?

6.7. L'application évolue-t-elle régulièrement par versions successives ?

6.8. Le volume des demandes de maintenance évolutive est-il « normal » (en fonction de l'âge de l'application) et de maintenance corrective « raisonnable » (20-25% max de la maintenance dans les 2 premières années) ?

Audit des Applications informatiques en service

6.9. Si l'application est de conception ancienne, la structure en charge de la maintenance (interne ou externe) offre-t-elle des garanties suffisantes de pérennité de l'application (niveau de documentation, taille, ancienneté et compétence des équipes, solidité financière du sous-traitant, ...) ?
6.10. Le niveau de dépendance vis-à-vis de cette structure est-il raisonnable ?
6.11. L'éditeur a-t-il des références significatives dans le même secteur d'activité et dans des organisations de taille et de complexité équivalente ?
6.12. La version du progiciel installée dans l'organisation est-elle mature et utilisée dans un nombre significatif d'organisations ?
6.13. A-t-on procédé à des développements spécifiques limités qui ont respecté les points d'interface et les normes préconisées par l'éditeur ? En particulier, les sources du progiciel, n'ont-ils pas été modifiés ?
6.14. Existe-il un club utilisateurs où l'Organisation est présente et influente ?
6.15. A-t-on souscrit un contrat de maintenance avec l'éditeur ?
6.16. Les redevances de maintenance sont-elles régulièrement payées ?
6.17. Le contrat prévoit-il une clause dite d' « *Escrow Agreement* » permettant de disposer des sources, auprès d'un tiers de confiance, en cas de défaillance de l'éditeur ?
6.18. Les montées de versions sont-elles régulièrement effectuées ?
6.19. Dispose-t-on d'un engagement ou d'une visibilité suffisante de la pérennité du progiciel (notamment en cas de gel des évolutions ou de l'état technique) ?

Introduction à l'audit des systèmes informatiques et cadre de références (Cobit/Itil)

- **Définition** : L'audit informatique est l'évaluation des risques des activités informatiques, dans le but d'apporter une diminution de ceux-ci et d'améliorer la maîtrise des systèmes d'information

- **Les besoins et les nécessités d'audit informatiques**

  – c'est le cadre du prolongement du développement de la théorie de la révision comptable le contrôle des systèmes d'informatique de gestion ont vu le jour.

  – Les dirigeants ressentent, le besoin d'audit informatique afin de connaitre l'impact du changement dû aux introductions de systèmes informatisé dans l'environnement du travail ;

  – Le besoin de connaître les chiffres et le retour des investissements (ROI) avec divers coût et les risques encourus.

référentiels

- **Définition** : L'audit informatique est l'évaluation des risques des activités informatiques, dans le but d'apporter une diminution de ceux-ci et d'améliorer la maîtrise des systèmes d'information

  - **Il y a fondamentalement deux référentiels à la mode pour la gouvernance IT:**

    - **Cobit (Control Objectives for Informations and Technologie)**

    - **Itil (Information Technology Infrastructure Library)**

Cobit

- C'est un cadre de contrôle qui vise à aider le management à gérer les risques (sécurité, fiabilité, conformité) et les investissements.
  - CobiT est une approche orientée processus,
    - 4 domaines:
      - planification organisation, Acquisition et mise en place, Distribution et Support, Monitoring
      - 34 processus distincts
      - 215 activités

Processus de Cobit

planification & Organisation	**PO1**	Définir un plan informatique stratégique
	PO2	Définir l'architecture de l'information
	PO3	Determiner la direction technologique
	PO4	Définir l'organisation IT et ses relations
	PO5	Gérer l'investissement informatique
	PO6	Communiquer les objectifs du management
	PO7	Gérer les resources humaines
	PO8	S'assurer de la conformité avec les pré requis externes
	PO9	Evaluer les risques
	PO10	Gérer les projets
	PO11	Gérer la qualité

Processus de Cobit/ domaine

Acquisition & Implementation	**AI1**	Trouver des solutions informatiques
	AI2	Acquisition et maintenance des Applications
	AI3	Acquisition et maintenance des infrastructures technologiques
	AI4	Développer et maintenir les procedures
	AI5	Installer les systemes et les valider
	AI6	Gérer les changements

Processus de Cobit/ domaine

Delivery & Support	**DS1**	Définir et gérer le niveau de service
	DS2	Gérer des services tiers
	DS3	Gérer les performances et la capacité
	DS4	Assurer la continuité de service
	DS5	Assurer la sécurité des systèmes
	DS6	Identifier et allouer les coûts
	DS7	Instruire et former les utilisateurs
	DS8	Assister et conseiller les utilsateurs
	DS9	Gérer les configurations
	DS10	Gérer les problèmes et incidents
	DS11	Gérer les données

Objectifs Cobit:

- répondre aux besoins de l'entreprise
  - **Le management** pour lequel il offre un moyen d'aide à la décision
  - **Les utilisateurs** pour lesquels il permet d'apporter des garanties sur la sécurité et les contrôles des services informatiques
  - **Les auditeurs** auxquels il propose des moyens d'interventions reconnus internationalement

Structure : six notions fondamentales

- **1 Synthèse**
- **2 Cadre de référence**
- **3 Outils de mise en œuvre**
- **4 Guide de management**
- **5 Objectifs de contrôle**
- **6 Guide d'audit**

Synthèse

- **La synthèse est un résumé des principaux concepts de Cobit.**
  - **<u>Rôle</u>:**
    - **Aider à sensibiliser les managers à l'organisation de l'audit et du contrôle.**

Cadre de référence

- **La synthèse est un résumé des principaux concepts de Cobit.**
  - **<u>Rôle</u>:**
    - **Aider à sensibiliser les managers à l'organisation de l'audit et du contrôle.**
- **Un enjeu majeur pour Cobit est la pertinence de l'information elle est déterminée à partir de sept critères :**
  - L'efficacité : qualité et pertinence de l'information, distribution cohérente
  - L'efficience : rapidité de la délivrance
  - La confidentialité : accessibilité à la demande et protection
  - La conformité : respect des règles et lois
  - La fiabilité : exactitude des informations transmissent par le management

Cadre de référence

– **Un enjeu majeur pour Cobit est la pertinence de l'information elle est déterminée à partir de sept critères :**

- **L'efficacité** : qualité et pertinence de l'information, distribution cohérente
- **L'efficience :** rapidité de la délivrance
- **La confidentialité** : accessibilité à la demande et protection
- **L'intégrité**: exactitude de l'information
- **La disponibilité**: accessibilité à la demande et protection (sauvegarde)
- **La conformité** : respect des règles et lois
- **La fiabilité** : exactitude des informations transmissent par le management

Outils de mise en œuvre

- **Le guide outils de mise en œuvre décrit:**
  - **comment augmenter, convaincre et influencer les personnes clés dans l'entreprise.**

- **On peut résumer en 11 arguments clés la globalité du dispositif**

Guide de management

- **Le guide de management COBIT permet de:**
- **Situer le niveau de maturité des 34 processus par rapport à un modèle de maturité**
- **Définir les facteurs clefs de succès de chaque processus**
- **Mesurer l'accomplissement des objectifs**
- **Définir des indicateurs de performance**
- **Le modèle de maturité de COBIT**
- **Le guide outils de mise en œuvre décrit:**
  - **comment augmenter, convaincre et influencer les personnes clés dans l'entreprise.**

Guide de management

- **Le modèle de maturité de COBIT**
  - **5 niveaux de maturité**

Niveau	Nom	Description
0	Inexistant	Les processus de gestion ne sont pas appliqués
1	Initialisé	Les processus sont ad hoc et des organisés
2	reproductible	Les processus suivent un modèle répétable
3	défini	Les processus sont formalisés et communiqués
4	Géré	Les processus sont surveillés et mesurés
5	Optimisé	L'amélioration du processus est gérée

Guide de management

- **Le modèle de maturité permet de définir:**
  - **La situation actuelle de l'organisation**
  - **La situation des entreprises dans un domaine métier équivalent**
  - **Les standards internationaux**
  - **La stratégie d'amélioration de l'entreprise, là où elle souhaite aller**

Guide de management

- **Les facteurs clefs de succès (FCS)**
  - Les FCS décrivent les points et actions les plus importantes permettant à la direction de renforcer le Contrôle sur les processus de gestion.

  - Les FCS décrivent les choses les plus importantes à faire pour que les processus de gestion des TI atteignent leurs objectifs en ce qui concernent:
    - La stratégie,
    - La technique,
    - L'organisation,
    - Les processus et procédures

Le guide d'audit

- Les objectifs de l'audit sont définis dans Cobit de la façon suivante:
  - Déceler, analyser, et expliquer les failles d'un système d'information et les risques qui en découlent.
  - Apporter les solutions permettant d'ajuster le SI au regard des besoins de l'entreprise
  - Garantir de façon fiable l'atteinte des objectifs de contrôle pour le management dans le cas d'une utilisation de Cobit

Le guide d'audit

Acquérir une bonne compréhension de la situation

Evaluer les étape de contrôle

Evaluer les étapes de contrôle

Justifier le risque

Classification générique des types d'audit

- Typologie d'audit informatique:
  - **Trois types d'audits classés en rapport avec le degré de finalité d'importance et de difficulté:**
    - Audit diagnostic: l'auditeur doit porter un jugement sur un SI en projet, ou existant qui fonctionne mal
      - Résultats attendu: analyse des contres performances, recommandations
    - Audit de régularité (conformité): l'auditeur vérifie l'application des procédures informatique et la régularité des transaction ou la cohérence des données
    - Audit d'efficacité: analyse approfondie des méthodes et moyens
      - Doit faire appel à des experts ou des externes.

Les divers phases d'une mission d'audit

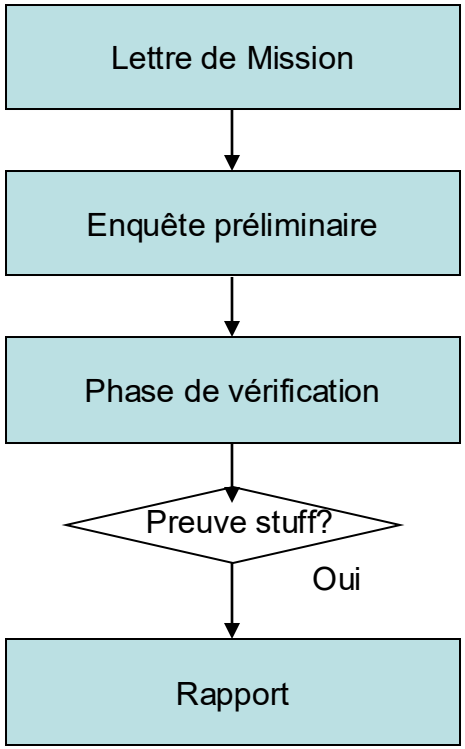


Schéma global d'une mission d'audit

Les divers phases d'une mission d'audit

Les divers phases d'une mission d'audit

- **L'enquête préliminaire**
  - définition des objectifs claires, précis et en harmonie avec la demande
    - En aucun cas les objectifs ne pourront être déviés
  - La durée de cette phase de quatre à cinq jours environs
    - L'ensemble de l'équipe doit participer à cette mission
  - Modèle d'une équipe d'audit
    - Chef de mission ou superviseur
    - Auditeur spécialiste informatique
    - Auditeur généraliste
    - Le chef du service d'audit
  - **Quatre phases dans cette étape**:
    - Analyse et définition des objectifs
    - La préparation (documentation élaboration de questionnaires)
    - Prise de contact avec les audités
    - Enquête préliminaire proprement dite

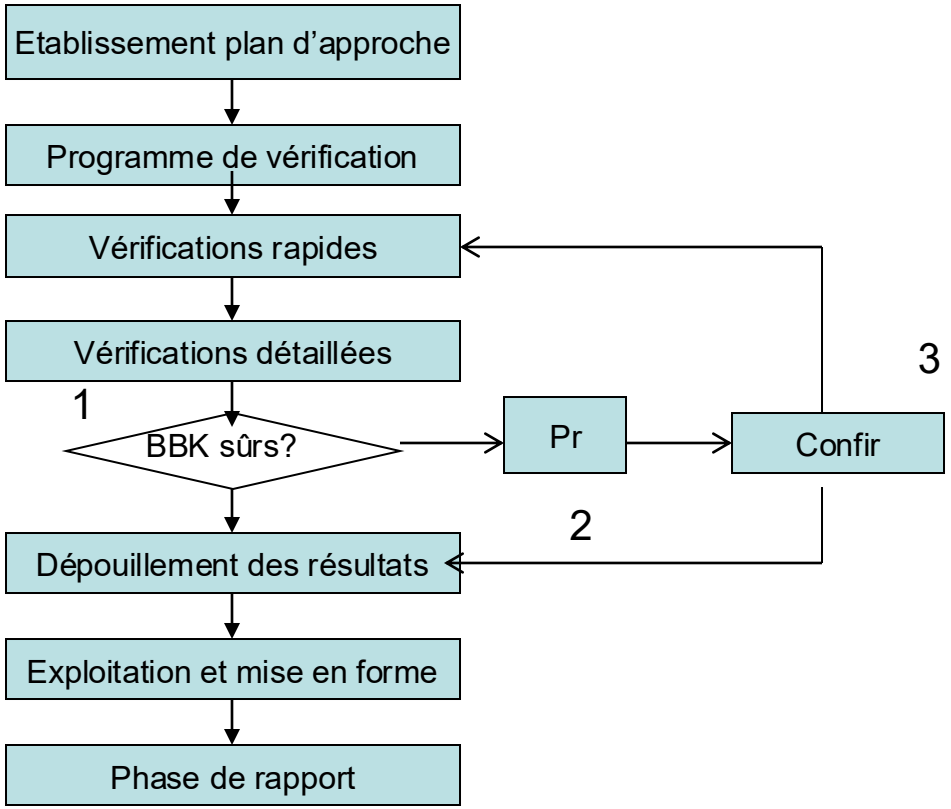
L'enquête préliminaire proprement dite

- **But:**
  - Collecter des informations afin de pouvoir dresser un plan de travail
  - Etudier la faisabilité par rapport à l'ordre de mission des objectifs
  - Possibilité de remettre en cause les objectifs
  - **Modèle d'une équipe d'audit**
    - Chef de mission ou superviseur
    - Auditeur spécialiste informatique
    - Auditeur généraliste
    - Le chef du service d'audit

Phase de vérification

- **décomposition**
  - Etablissement du programme de vérification
  - Vérification sur le terrain, recherche de preuve de défaillance
  - Dépouillement et compilation des résultats obtenus
  - Exploitation des résultats première mise en forme et classement pour le rapport futur
  - **Deux types de vérification**
    - La vérification rapide: les entretiens, l'examen de la documentation, les procédures, la preuve physique de l'existence de procédures ou documents
    - Vérifications approfondies: chiffrement des dégâts réels ou potentiels

Les divers phases d'une mission d'audit



BBK black Blue Key: bilan bref mettant en valeur les points forts et les points faibles

Phase de restitution et du rapport

- **Consiste à:**
  - préparer, rédiger, éditer le rapport:
    - Rédaction d'un projet de rapport
      - Présentation du projet, examen des incohérences ou points faibles
      - Mise en accord avec les audités
      - Elaboration définitive des recommandations (faire un fichier de suivi)
      - Rédaction du rapport définitif
      - Notification et envoie aux intéressés
      - Envoie du fichier de suivi et de la lettre de clôture

Phase de restitution et du rapport

- **Qualités d'un bon rapport:**
  - neutralité, objectivité, critiques constructives:
    - **Neutralité**: ne jamais faire transparaitre ses sentiments
    - **Objectivité**: ne pas être théorique mais très pratique
    - **Critiques constructives**: ne pas critiquer sans proposer une solution
    - Le rapport est technique mais lisible et compréhensible par un profane
    - En face de chaque point faible une recommandation
    - Tenir compte des points de désaccord lors de la présentation du pré-rapport

Phase de restitution et du rapport

volume, clarté, concision :

- **volume**: pas de règle mais ne jamais produire un rapport de moins de 25-30 pages
- **clarté**: rédiger en français simple et bien ponctué
- **concis**: se souvenir que c'est un rapport et non une dissertation
- **Tableau récapitulatif**: il est bon de faire un tableau récapitulatif des points forts et faibles d'après les preuves ou d'après l'intime conviction

Exemples et démarches pour les audits qualité d'un service de support

- **Mission** : Ayant reçu des plaintes d'utilisateurs concernant les services rendus, la direction générale mandate un audit sur le processus de support de la division informatique.

- **La lettre de mission**: est envoyée simultanément à la division informatique et au responsable d'audit (au mois de Mars de l'année N). L'audit était planifié et sera exécuté après les vacances d'été.

RESOLUTION

- Nous développons les éléments correspondants à chaque phase du processus d'audit après la réception de la lettre de mission :

  - L'enquête préliminaire
  - La phase de vérification
  - la phase de rapport.

RESOLUTION

- Proposition des deux points importants suivants :

- -acceptation de la mission
- -utilisation du référentiel du service audité s'il existe, dans le cas contraire, les auditeurs s'appuieront sur la norme Cobit, en particulier pour la vérification concernant le support :
- -vérifier le processus de l'équipe de support
- -le processus de gestion de configuration des logiciels utilisés par le support ;
- -le processus d'assurance de la qualité de service ;
- -le processus de revue de ce service ;
- -le processus de résolution de problèmes du personnel support.

Les autres référentiels de la gouvernance des TI

- le COSO et le Balanced Scorecard (BSC).
- **Le COSO**

- Le COSO *(Committee of Sponsoring Organizations of the Treadway Commission)* a publié en 1992 un cadre de référence pour le contrôle interne afin d'aider les entreprises à évaluer et à améliorer leur système de contrôle interne. Le contrôle interne y est décrit comme un processus étant sous la responsabilité d'une instance constituée dans le but d'assurer la réalisation d'objectifs regroupés dans les domaines suivants :
  - • efficacité et efficience des opérations ;
  - • fiabilité des rapports financiers ;
  - • conformité aux lois et règlements.

Les autres référentiels de la gouvernance des TI

- En ce qui concerne la gouvernance des TI, il existe de nombreux cadres de référence, chacun avec leur point de vue.

- Ainsi, chaque cadre de référence offre un niveau de détail approprié dans son domaine. L'une des difficultés de la gouvernance des TI est bien de faire coexister les approches terrain, forcément détaillées et spécialisées, et les synthèses de pilotage stratégique. Ce chapitre présente les principaux référentiels en matière de pilotage global, de pilotage des services, des projets et de la sécurité des TI.

Les autres référentiels de la gouvernance des TI

- En 2004, le COSO a publié le document *Management des risques dans l'entreprise*
- (*Enterprise Risk Management* ou ERM) qui élargit le périmètre du contrôle
- interne. L'ERM englobe :
    - la notion de portefeuille de risques ;
    - une structuration en quatre catégories d'objectifs (opérations, reporting, conformité et objectifs stratégiques) ;
    - le niveau de prise de risque décidé de façon stratégique par l'entreprise ;
    - les événements qui impactent les risques ;
    - les quatre catégories de réponse aux risques (éviter, réduire, partager et
    - accepter) ;
    - le périmètre de l'information et de la communication ;
    - les rôles et les responsabilité des acteurs en charge de la sécurité mais aussi des directeurs *(board)*.

Les autres référentiels de la gouvernance des TI

- **Le Balanced Scorecard (BSC)**

- Le Balanced Scorecard (BSC), ou tableau de bord prospectif, est une représentation qui permet de clarifier la vision et la stratégie d'une entreprise, et de la traduire en plans d'action. Il donne aussi bien le retour sur le fonctionnement des processus internes que des contraintes externes

Les autres référentiels de la gouvernance des TI

- **Le management de la sécurité**
- Plusieurs normes, méthodes et référentiels de bonnes pratiques en matière de sécurité des systèmes d'information sont disponibles.

  – Ils constituent des guides méthodologiques ainsi que les moyens de garantir une démarche de sécurité cohérente.

Les autres référentiels de la gouvernance des TI

- **Le management de la sécurité**
  - la norme ISO/IEC 27000 présente le vocabulaire et les définitions du domaine de la sécurité, applicables à chacun des standards ;
  - la norme ISO/IEC 27001 décrit la politique du management de la sécurité des systèmes d'information au sein d'une entreprise qui sert de référence à la certification ;
  - la norme ISO/IEC 27002 constitue le guide de bonnes pratiques de la sécurité des SI ;
  - la norme ISO/IEC 27003 a pour vocation d'être un guide d'implémentation
  - la norme ISO/IEC 27004 sera un nouveau standard pour le pilotage des indicateurs et des mesures dans le domaine de la sécurité des SI ;
  - la norme ISO/IEC 27005 sera un nouveau standard sur le management des risques pour la sécurité des SI ;
  - la norme ISO/IEC 27006 résume les exigences applicables aux auditeurs externes dans leur mission de certification sur l'ISO 27001.

Les autres référentiels de la gouvernance des TI

- **Les normes ISO/IEC 17799 et ISO/IEC 27002**

- La norme ISO/IEC 17799 de 2005, renommée ISO/IEC 27002, spécifie une politique de la sécurité des systèmes d'information qui se présente comme un guide de bonnes pratiques.

- De façon schématique, la démarche de sécurisation du système d'information doit passer par quatre étapes de définition.

    1. Périmètre à protéger (liste des biens sensibles).
    2. Nature des menaces.
    3. Impact sur le système d'information.
    4. Mesures de protection à mettre en place.

Les autres référentiels de la gouvernance des TI

- **Les normes ISO/IEC 17799 et ISO/IEC 27002**

- La norme ISO/IEC 27002 fournit des exemples et des indications sur les niveaux 1 à 3, et liste pour le niveau 4 une série de mesures à mettre en place. Elle comporte 39 catégories de contrôle et 133 points de vérification répartis en 11 domaines.
  - Politique de sécurité.

  - Organisation de la sécurité :
    - organisation humaine, implication hiérarchique ;
    - notion de propriétaire d'une information et mode de classification ;
    - évaluation des nouvelles informations ;
    - mode d'accès aux informations par une tierce partie ;
    - cas de l'externalisation des informations.

  - Classification et contrôle des biens.

  - Sécurité du personnel.

Les autres référentiels de la gouvernance des TI

- **ITIL : le management des services**
- Développé par l'OGC pour le gouvernement britannique, ITIL *(Information Technology Infrastructure Library)* se présente comme une série de livres décrivant les bonnes pratiques pour le management des services TI. Son approche est davantage orientée sur le « quoi faire » que sur le « comment faire ».
- Les principes qui sous-tendent ITIL sont l'orientation client, la prise en compte, en amont de tout projet, des exigences de services et l'approche processus. ITIL est devenu un standard de fait, au moins pour le périmètre des centres d'assistance et des opérations.

• Organisation de la sécurité :
  – organisation humaine, implication hiérarchique ;
  – notion de propriétaire d'une information et mode de classification ;
  – évaluation des nouvelles informations ;
  – mode d'accès aux informations par une tierce partie ;
  – cas de l'externalisation des informations.

• Classification et contrôle des biens.

• Sécurité du personnel.

Les autres référentiels de la gouvernance des TI

- **ITIL : le management des services**
- Développé par l'OGC pour le gouvernement britannique, ITIL *(Information Technology Infrastructure Library)* se présente comme une série de livres décrivant les bonnes pratiques pour le management des services TI. Son approche est davantage orientée sur le « quoi faire » que sur le « comment faire ».
- Les principes qui sous-tendent ITIL sont l'orientation client, la prise en compte, en amont de tout projet, des exigences de services et l'approche processus. ITIL est devenu un standard de fait, au moins pour le périmètre des centres d'assistance et des opérations.

• Organisation de la sécurité :
  – organisation humaine, implication hiérarchique ;
  – notion de propriétaire d'une information et mode de classification ;
  – évaluation des nouvelles informations ;
  – mode d'accès aux informations par une tierce partie ;
  – cas de l'externalisation des informations.

• Classification et contrôle des biens.

• Sécurité du personnel.

Les autres référentiels de la gouvernance des TI

- **ITIL : le management des services**
- Développé par l'OGC pour le gouvernement britannique, ITIL *(Information Technology Infrastructure Library)* se présente comme une série de livres décrivant les bonnes pratiques pour le management des services TI. Son approche est davantage orientée sur le « quoi faire » que sur le « comment faire ».
- Les principes qui sous-tendent ITIL sont l'orientation client, la prise en compte, en amont de tout projet, des exigences de services et l'approche processus. ITIL est devenu un standard de fait, au moins pour le périmètre des centres d'assistance et des opérations.

• Organisation de la sécurité :
  – organisation humaine, implication hiérarchique ;
  – notion de propriétaire d'une information et mode de classification ;
  – évaluation des nouvelles informations ;
  – mode d'accès aux informations par une tierce partie ;
  – cas de l'externalisation des informations.

• Classification et contrôle des biens.

• Sécurité du personnel.

Les autres référentiels de la gouvernance des TI

- **ITIL : le management des services**
- • Le domaine Soutien des services se focalise sur le quotidien et comprend :
- – le centre de services *(Service Desk)* ;
- – la gestion des incidents ;
- – la gestion des problèmes ;
- – la gestion des configurations ;
- – la gestion des changements ;
- – la gestion des mises en production.

- **les cinq domaines couverts par ITIL V2 ne faisant pas l'objet de**
- certification sont :

• ***Business Perspective***, qui concerne les questions d'organisation (organisation de la production, relations entre les différentes rôles, fonctions et responsabilités, relations avec les fournisseurs et prestataires externes) ;

• ***Application Management*,** qui concerne la gestion des relations entre études et exploitation (support applicatif, changement logiciel, mise en production) ;

• ***ICT Infrastructure Management***, qui concerne le cycle de vie de l'infrastructure (automatisation, maintenance, installation) ;

• ***Security Management***, qui concerne le pilotage de la sécurité informatique ;

• ***Planning to Implement Service Management***, qui concerne la mise en place d'une orientation « client » au sein de la DS

Différents types de contrôles internes

Le contrôle peut être:

- préventif,
- Détective (inspection)
- réactif

Types	implémentation
Préventif	Administrative
Détective	Technique
Réactif	Physique

Exemple de contrôle interne

changements sur les logiciels:

- **Contrôle d'intégrité**: cas de code non testé ni homologué
  - Risque: la logique erroné dans le code perte de confiance sur les résultats du SI, doute sur les résultats produits par le SI.
- **Quels sont les contrôles interne pour minimiser ce risque?**
  - S'assurer que le programmeur n'a pas un l'accès logique pour mettre à jour les codes en production.
  - S'assurer que les personnes qui peuvent faire les mises à jour en production ne peuvent pas le faire sans test

Exemple de contrôle interne

Accès au système:

- **Accès inappropriés**: des droits d'accès accordés aux personnes inutilement.
  - Risque: les données peuvent être changé, ajoutées, effacées
  - **Quels sont les contrôles interne pour minimiser ce risque?**
  - Exiger un nom d'utilisateur et un mot de passe pour accéder au système.
  - Avoir un nombre limité d'Administrateurs de sécurité des applications avec les droits d'ajouter les nouveaux utilisateurs
  - S'assurer de l'expertise de ces administrateurs à discerner qui à besoin de quoi réellement

Exemple de contrôle interne

Plan de Backup et recouvrement de données après sinistre:

- **Perte de données**: en cas de problèmes disques, carte etc.
  - Risque: indisponibilité du SI
  - **Quels sont les contrôles interne pour minimiser ce risque?**
  - Exiger le backup du système périodiquement suivant la criticité des données et la rapidité de changement d'état.
  - Ne pas stocker les secours sur le site de production
  - Documenter le plan de restauration et de retour à la normale

Déterminer quoi auditer

Guide:

- **Risques élevé**: orienter son travail sur les domaines identifiés à haut risque
- **Importance:** regarder de prêt les processus importants pour le domaine audité
- **Valeur ajouté**: concentrer ces efforts là où vous pouvez apporter une réelle ajoutée à l'entreprise.

Déterminer quoi auditer

Créer l'univers d'audit:

- **Comment**?
  - répertorier les fonctions IT qui sont centralisées
  - Placer chacune de ces fonctions comme point intéressant de votre audit
    - » Exemple: vous avez une fonction d'administrateur central quoi d'intéressant pour l'audit?
    - » Faire une revue de l'environnement d'administration
    - » Gestion des comptes
    - » Gestion des changements
    - » Gestion des problèmes, gestion des patchs,
    - » suivi de la sécurité
    - » Tout ce qui peut concerner l'ensemble du SI
    - » Revue de la sécurité de déploiement des machines serveurs

Déterminer quoi auditer

Administration de serveur Unix et linux	Support centralisé
Administration de serveur Windows	Gestion de bases de données
Sécurité de réseau sans fil	Téléphonie voix sur IP
Gestion des Switch et routeurs	Mobilité
Gestion de firewall/DMZ	Les règles de sécurité IT

Liste de choses intéressantes à auditer en environnement centralisé

Créer l'univers d'audit

- **Fonctions IT centralisées**: déterminer les fonctions IT qui sont centralisées.
  - Sur un domaine Windows par exemple se pencher sur la fonction d'administrateur de domaine est bien un bon choix.
- **Fonctions IT décentralisées :** regarder de prêt les IT qui sont sous la responsabilité des sites. Par exemple la sécurité physique et environnementale.
- **Application métier**: prévoir l'audit de chacune des applications métiers.
  - Il est bon de classer l'application en audit financier ou technique
- **Conformité**: il faut accorder une place à la réglementation

Faire un classement de l'univers d'audit

Guide de classement de l'univers:

- **Les problèmes connus dans le domaine**: si vous savez qu'il y a des problèmes dans le domaine il est bon de faire un audit sur ces problèmes

- **Les risques inhérents au domaine :** est un indicateur qui vous pousse par expérience à auditer un domaine

- **Intérêt d'auditer ce domaine**: cela est personnel à l'auditeur qui pense qu'auditer ce processus apportera une valeur ajoutée à l'entreprise

Audité les contrôles au niveau entité

Les étapes de test:

- **I - Faire une revue de la structure IT de l'organisation et s'assurer qu'elle a une mission bien définie et qu'elle à les pouvoirs sur l'ensemble des opérations et que ses tâches sont bien définies**
  - comment?
  - Revue de l'organigramme pour savoir à qui l'IT se rapporte
  - Evaluer tous les points de confusion dans la prise de décision
  - Evaluer la division des responsabilités IT:
    - » Les informaticien ne doivent pas faire de la saisie de donnée (à analyser selon la compagnie)
    - » Les programmeurs ne doivent pas être capable de mettre les application en production
    - » Les fonctions de développeur, support et maintenance doivent être bien séparées
    - » Il doit y avoir un responsable de la sécurité du SI

Audité les contrôles au niveau entité

Les étapes de test:

- **II - Faire une revue du planning des processus stratégique de l'IT et s'assurer de son alignement sur la stratégie de l'entreprise. Evaluer les progrès des processus IT par rapport au plan stratégique de l'entreprise** comment**?**
  - Revue des objectifs à court moyen et long terme de la stratégie IT
  - Faire l'adéquation avec les priorités de l'entreprise
  - S'assurer que le management IT est impliqué au niveau management de l'entreprise
    - » La participation CODIR
    - » Consultation sur les grands projets de l'entreprise
    - » Budget de fonctionnement existant et bien maitrisé
    - » Evaluer les processus qui sont mis en place pour le suivi des projets IT par rapport aux priorités de la direction

Audité les contrôles au niveau entité

Les étapes de test:

- **III – Déterminer s'il existe une stratégie pour l'évolution de la technologique et celle des applications et si un plan existe, évaluer les processus techniques dont le planning dure dans le temps.**

  comment?

  - Rechercher les processus informatique dont le planning dur dans le temps
  - Rechercher les applications et les technologies commandées et s'assurer qu'il existe un support à long terme pour chacune d'elles
  - S'assurer qu'il y a un suivi des changements sur l'ensemble des acquisitions de l'entreprise
  - Voir s'il n'est pas possible de migrer vers de nouvelles technologies

Audité les contrôles au niveau entité

Les étapes de test:

- **IV – faire la revue des indicateurs de performance et d'évaluation de l'IT, s'assurer qu'il y a des procédures en place pour mesurer les performances des activité journalières et surtout pour suivre la performance par rapport au niveau de service, du budget.**
- comment**?**
  - Obtenir une copie des mesure faites par l'IT périodiquement sur les activités
  - Déterminer le role de chaque métrique
  - S'assurer que la métrique satisfait bien aux besoin ciblé
  - Voir en cas de contreperformance si le problème a été analysé
  - Voir si des mesure de correction ont été prise en cas de contreperformance
  - Faire une revue de tous les services level-agreement SLA
  - S'assure qu'il existe une procédure budgétaire pour le département IT

Audité les contrôles au niveau entité

Les étapes de test:

- **V – faire la revue des processus IT qui approuvent et font la priorisation des nouveaux projets. Déterminer si une acquisition ou la mise en place d'un projet ne peut avoir lieu sans être approuvée. S'assurer qu'il existe un suivi de l'ensemble des projet IT importants tout au long de leur cycle.**
- **Comment?**
  - Faire une revue des documents des projets et voir en cours et l'accord de mise en œuvre
  - Prendre le planning projet de l'IT et voir si il existe une priorisation

Audité les contrôles au niveau entité

Les étapes de test:

- **VI – s'assurer de l'existence de procédures sur la sécurité IT et qu'elle assure une sécurité pour l'environnement. Déterminer comment la procédure est diffusée et comment sa mise en application est contrôlée et opposable à tous.**
- **Comment?**
  - Demander une copie de la politique de sécurité du SI
  - Regarder si elle couvre l'ensemble des risque de l'entreprise au minimum
    - » La classification de la documentation, leur rétention, leur destruction
    - » Un usage acceptable des moyens IT à la disposition des employés pour leur besoins personnels
    - » Connections à distance
    - » Mots de passe
    - » Sécurité des serveurs
    - » Sécurité des clients
    - » Accès logique

Audité les contrôles au niveau entité

Les étapes de test:

- **VIII– Revue et évaluation des processus de contrôle de l'accès logique des personnes étrangères**
- **Comment?**
  - S'assurer que la procédure qui donne l'accès des visiteurs prévoit l'approbation d'un employé
  - Avoir un profil pour visiteur dans le système
  - Avoir une procédure connue par les visiteurs
  - S'assurer que les données confidentielles de l'entreprise ne tombent pas dans la main des visiteurs.
  - S'assurer que dans la procédure des personnes étrangères les avertissements pour violation sont bien inscrites

Audité les contrôles au niveau entité

Les étapes de test:

- **IX– s'assurer que les règles de transport, le stockage et la réutilisation des médias sont bien définies dans la procédure de sécurité du SI**
- **Comment?**
  - Faire obligation de crypter toute donnée sensible à transporter
  - Toute bande magnétique doit être mise en lambeau au cas où on s'en sépare
  - Les média optiques et papier doivent aussi être mise en lambeau.

Audité les contrôles au niveau entité

Les étapes de test:

- **X– Vérifier que dans la politique de sécurité du système d'information l'ensemble des suivis est bien formalisé.**
- **Comment?**
  - Observer la documentation sur l'architecture du SI et s'assurer de sa capacité à anticiper sur les besoins d'évolution
  - Les procédures de suivi doivent avoir une attention particulière sur les limites du système
  - La surveillance des Log doit inclure les limites des éléments constituants du SI
  - Le rapport sur la disponibilité du SI en terme de ressources

Audité les Data Centers et reprise après désastre

Contrôles de base:

- **Contrôle d'accès**
  - Faire la revue du contrôle d'accès (on peut avoir des technologies comme: la biométrie qui lit votre empreinte digital, la forme de vos mains, la rétine tec..) pour identifier toute personne qui a accès data center
  - Noter la présence de Sas s(a) *etatium, tamis*
- **Système d'alarme**
  - Feux, eau, chaleur extrême et niveau d'humidité,
  - variation de l'énergie électrique
  - Gaz inhabituel.

Audité les Data Centers et reprise après désastre

Contrôles de base:

- **Extinction de feu**
  - S'assurer de la présence en nombre suffisant d'extincteurs
  - Voir si le positionnement est adapté à chaque endroit (tech. Eau ou gaz)
- **Alimentation**
  - Alimentation redondante,
  - UPS
  - Générateur.

Audité les Data Centers et reprise après désastre

Contrôles de base:

- **chauffage ventilation et climatisation**
  - S'assurer de la redondance de la climatisation et de la ventilation
  - Une capacité double est exigée
- **Connectivité réseau**
  - Redondance niveau réseau .

Audité les Data Centers et reprise après désastre

Les étapes de test:

- **Inspecter l'éclairage extérieur, l'orientation du bâtiment, le voisinage pour identifier les facteurs de risque, signalétique**
- **Comment?**
  - **Signalétique** anonyme
  - **Voisinage** le mieux est que le datacenter soit dans un immeuble isolé pas de voisin immédiat
  - **éclairage extérieur** suffisamment éclairé pour être vu à une distance raisonnable

Audité les Data Centers et reprise après désastre

Les étapes de test:

- **Inspecter les entrée externes et les murs pour s'assurer de leur capacité à protéger le data center correctement**
  - **Faux plafond et faux planché** passage facile dans certaines conditions
  - **Sas** s'assurer du bon fonctionnement la première porte doit se fermer avant l'ouverture de la deuxième porte

Audité les Data Centers et reprise après désastre

Les étapes de test:

- **évaluer physiquement les équipements d'authentification et voir s'ils sont appropriés pour l'utilisation qui en est fait et leur bon fonctionnement**
  - **Étudier le log des équipement pour s'assurer qu'il enregistre vraiment**
    - » User id.
    - » L'heure de la demande d'accès
    - » Échec ou succès de la demande

Audité les Data Centers et reprise après désastre

Les étapes de test:

- **Vérifier que la mise à la terre existe pour protéger le système**
- **S'assurer que l'alimentation est conditionnée pour prévenir la perte de données**
- **Vérifier que pendant les coupures momentanées l'ups fournit le courant**
- **S'assurer aussi que pour une coupure prolongée le générateur prend effectivement le relai**

Audité les Data Centers et reprise après désastre

Système d'alarme:

- **s'assurer de la protection du data center par une alarme de type burglar contre les intrusions physiques**
- **Vérifier qu'il existe une alarme de détection de feu dans le data center**
- **S'assurer qu'une alarme de détection d'eau est configurée dans le data center**
- **S'assurer qu'une alarme de détection d'humidité est configurée dans le data center**
- **Faire une revue du suivi des alarmes et s'assurer que les logs sont étudiés**

Audité la reprise après désastre

Résilience du système:

- **s'assurer que la redondance matérielle est assurée pour une haute disponibilité du système**
- **s'assurer qu'il existe un site de secours avec le même niveau de sécurité au point disponibilité**
- **S'assurer dans ce cadre de comment les données sont répliquées sur le site de secours ex: base de données**
  - » **Electronic vaulting: -** à base d'un batch qui fait périodiquement la copie du site de production sur le site de secours
  - » **Remote journaling**: - fournit un processus parallèle en temps réel par une connexion sur le réseau
  - » **Database shadowing**: fournit un processus parallèle en temps réel par une ou plusieurs connexions sur le réseau

Audité la reprise après désastre

Backup et restauration:

- **s'assurer que les procédures de backup sont appropriées pour chaque système**
- **Vérifier que le système peut réellement être restaurer à partir des médias de backup**
- **S'assurer que les médias de backup peuvent être restaurer promptement sur le site de secours**

Audité les Switch, routeurs, et par feu

Planning de reprise après désastre:

- **S'assurer qu'il existe des contrôles appropriés pour les vulnérabilités connues de la version de l'équipement. Ce contrôle doit inclure la mise à jour logicielle et le suivi des changements**
- **Vérifier que tous les services qui ne sont pas nécessaires sont désactivés**

Audité les Switch, routeurs, et par feu

Service Name	Comments	Config File Entry
TCP Small Servers	RFC specified services for TCP (chargen, daytime, etc)	`no service tcp-small-servers`
UDP Small Servers	RFC specified services for UDP (chargen, daytime, etc)	`no service udp-small-servers`
Finger	Gives away information about the device and users; should be disabled or at least blocked from external networks	`no service finger` *or* `no ip finger`
HTTP Server	Used to manage the router via HTTP; disable if not in use; restrict access via ACLs if in use; typically not used at TI	`no http server` `no ip http secure-server`
Proxy ARP	Use only when absolutely necessary to support legacy architectures; not really a big deal unless the interface is an end-user subnet	`no ip proxy-arp` (on each interface)
DNS	Disable entirely or enable with specific server(s)	`no ip domain-lookup` (to disable) `ip name-server addresses` (for specific servers)
DHCP	Assumes you have other DHCP servers on your network	`no ip dhcp-server`
bootp	Bootstrap Protocol	`no ip bootp server`
identd	Identifies the user of a particular TCP connection	`no ip identd`
CDP	Cisco Discovery Protocol: Information sent through CDP is cleartext and unauthenticated	`no cdp run` (disables globally) `no cdp enable <interface>` (disables per interface)

Audité les Switch, routeurs, et par feu

- **S'assurer qu'il existe une bonne politique de gestion du protocole SNMP** (Simple network management Protocol)
- **revoir et évaluer la procédure de création des comptes utilisateurs, s'assurer que les comptes créé sont réellement pour les besoins professionnels. Surveiller aussi la validité des comptes.**
  - » **Il faut prévoir une politique de durcissement des mots de passe**
  - » **Ne jamais accepter que les administrateurs partagent le même compte**
- **S'assurer que les contrôles appropriés sont utilisés pour les mots de passe**

Audité les Switch, routeurs, et par feu

- **vérifier qu'un Protocol de gestion sécurisé est utilisé là où cela est possible**
  - telnet envoie en clair toutes ces informations un sniffer peut donc lire le mot de passe
  - **Priorisé l'utilisation de SSH et autres protocole sécurisés**
- **Vérifier que les copies des configurations existes**
- **Vérifier que l'authentification est activé et envoyé à un système centralisé**
- **Evaluer l'utilisation de NTP**
  - » **Ntp server <ip address> key <key>**
- **S'assurer qu'une convention de nommage standard existe pour tous les équipements réseaux**

Audité les Switch, routeurs, et par feu

- **Vérifier qu'il existe une documentation standard pour la mise en production d'un équipement réseau**
- **Vérifier que l'administrateur ne s'amuse pas à utiliser VLAN I**
- **Evaluer l'utilisation de TRUNK AUTONEGOTIATION si possible assigner le trunk inteface à un VLAN natif autre que le VLAN I**
  - » Ne pas utiliser *Dynamic Trucking Protocol*
  - switch(config)# int f 0/1
  - switch(config-if)#switchport mode trunck
  - switch(config-if)# switchport mode trunck native vlan 998

Audité les Switch, routeurs, et par feu

- **Vérifier qu'il existe une documentation standard pour la mise en production d'un équipement réseau**
- **Vérifier que l'administrateur ne s'amuse pas à utiliser VLAN I**
- **Evaluer l'utilisation de TRUNK AUTONEGOTIATION si possible assigner le trunk inteface à un VLAN natif autre que le VLAN I**
  - » Ne pas utiliser *Dynamic Trucking Protocol*
  - switch(config)# int f 0/1
  - switch(config-if)#switchport mode trunck
  - switch(config-if)# switchport mode trunck native vlan 998

Audité les Switch, routeurs, et par feu

- **Mettre toutes les interfaces qui ne sont pas dans un trunk dans le mode nontrunking sans autonégotiation**
  - switch(config)# int f 0/1
  - switch(config-if)#switchport mode access
  - switch(config-if)# switchport nonegociate

- **Mettre toutes les interfaces qui sont dans un trunk dans le mode trunking permanent sans autonégotiation**
  - switch(config)# int f 0/1
  - switch(config-if)#switchport mode trunk
  - switch(config-if)# switchport nonegociate

Audité les Switch, routeurs, et par feu

- **lister tous les VLAN qui sont dans le trunk**
  - switch(config)# int f 0/1
  - switch(config-if)#switchport trunk allowed vlan 6, 10, 20, 101
- **Utiliser un unique vlan natif pour chaque trunk sur le switch**
  - switch(config)# int f 0/1
  - switch(config-if)#switchport trunk native vlan 998
  - switch(config)# int f 0/2
  - switch(config-if)#switchport trunk native vlan 997

Audité les Switch, routeurs, et par feu

- **évaluer l'utilisation des vlans sur le réseau**
  - Les vlan sont utilisés pour cinder les domaines de brodcast et pour diviser les ressources avec différents niveaux de sécurité
- **Désactiver tous les ports inutilisés et les mettre dans un vlan inutilisé**
- **Evaluer l'utilisation du protocole VTP (vlan trunking protocol) dans l'environnement**
- **Vérifier que des seuils existent qui limitent les trafiques brodcast/multicast sur les ports**

Audité les Switch, routeurs, et par feu

- **Vérifier que les interfaces inactives sur le routeur sont désactivés**
- **Vérifier que tous les dumps des routeurs sont sauvegardé**
- **Vérifier que tous les mise à jour de la table de routage sont authentifées**
- **Vérifier que ip source routing et ip direct broadcat sont désactivés**

Audité les Switch, routeurs, et par feu

- **Vérifier que tous les paquets sont refusés par défaut**
- **S'assurer que les adresses ip inappropriées internes et externes sont filtées**
- **Vérifier que tous les mise à jour de la table de routage sont authentifées**
- **Vérifier que ip source routing et ip direct broadcat sont désactivés**

Outils et technologie

- **outils d'audit de routeur (RAT): www.cisecurity.org**
- **Firemon: www.securepassage.com**
- **Wireshark: www.wireshark.org**
- **Nmap: http://insecure.org**
- **TeraTeam Pro: http://hpvector.co.ip/authors/VA002416/teraterm.html**
- **Top 100 security tools: http://sectools.org**

Liste à cocher pour l'audit routeur switch, parfeu

	Examen des contrôles autour du développement et de la maintenance des configurations.
	Veiller à ce que les contrôles appropriés sont en place pour toutes les vulnérabilités associées à la version actuelle du logiciel. ces contrôles peuvent inclure des mises à jour de logiciels, les changements de configuration, ou d'autres contrôles compensatoires.
	Vérifiez que tous les services inutiles sont désactivés.
	Veiller à ce que les bonnes pratiques de gestion SNMP sont suivies.
	Examiner et évaluer les procédures de création des comptes d'utilisateurs et s'assurer que les comptes sont créés seulement quand il y a un besoin commercial légitime. Également examiner et évaluer les processus afin de s'assurer que les comptes sont supprimés ou désactivés dans les meilleurs délais en cas de cessation ou de changement d'emploi.
	Veiller à ce que les contrôles de mots de passe appropriés soient utilisés.
	Vérifiez que les protocoles de gestion sécurisés sont utilisés lorsque cela est possible

Liste à cocher pour l'audit routeur switch, parfeu

	Veiller à ce que les sauvegardes actualisés ou à jour existent pour les fichiers de configuration le cas échéant.
	Vérifiez que l'enregistrement des évènements est activé et envoyé à un système centralisé de sauvegarde.
	Évaluer l'utilisation du protocole Network Time Protocol (NTP).
	Vérifiez qu'une bannière est configurée pour mettre au courant, tous les utilisateurs se connectant au système, de la politique de d'utilisation et de surveillance des systèmes de l'entreprise.
	Veiller à ce que les contrôles d'accès sont appliquées au port console.
	Veiller à ce que tous les équipements réseaux sont stockés dans un endroit sûr.
	Veiller à ce qu'une convention de nommage standard est utilisé pour tous les appareils
	Vérifiez que des processus standard et documentés existent pour l'assemblage des équipements réseau.

Audité les Switch, routeurs, et par feu

Switch

1.Vérifiez que les administrateurs n'utilisent pas le VLAN 1.

2.Évaluer l'utilisation de l'auto-négociation des trunk

3.Vérifier que les processus d'atténuation d'attaques sur Spanning-Tree Protocol sont activés.

4.Évaluer l'utilisation des VLANs sur le réseau.

5.Désactivez tous les ports inutilisés, et les placer dans un VLAN inutilisé.

6.Évaluer l'utilisation du VLAN Trunking Protocol (VTP).

7.Vérifier qu'il existe des seuils qui limitent le traffic des broadcast/multicast sur les ports.

Audité les Switch, routeurs, et par feu

Routeur

1.Vérifiez que les interfaces inactives sur le routeur sont désactivées.

2. Assurez-vous que le routeur est configuré pour enregistrer tous les "core dump".

3. Vérifiez que tous les routing updates (mises à jour de routage) sont authentifiés.

4. Vérifier que les IP source routing et les IP directed broadcasts sont désactivés.

==========

Audit des Firewalls:

1.Vérifiez que tous les paquets sont refusés par défaut
2. Veiller à ce que les adresses IP inappropriée aussi bien externes qu'internes sont filtrées.

Audité l'OS WINDOWS

Tests sur Windows server:

- **Vérifier l'OS et les versions du service pack (psinfo sur http://sysinternals.com/Utilities/Pstolls) est un outils qui peut vous aidez**
- **Vérifier que le firewall utiliser est celui procuré par la compagnie l'outils pslist**
- **S'assurer que l'antivirus est bien celui que l'entreprise a fourni**

Audité l'OS WINDOWS

Tests sur windows server:

- **S'assurer que tous les patchs approuvés sont déployés et que la procédure de déploiement de patch existe (**psinfo –s**)**
- **Faire une revue et vérifier les informations de démarrage**
- **Faire une revue des services, des applications installées et des tâches programmées**
  - » Déterminer les services qui sont activés et valider leur nécessité
  - » Évaluer ses services sur les vulnérabilités connues et assurer les patchs

Audité l'OS WINDOWS

Outils	Description	Ou se les procurer
netstat	Fournit les informations réseau	Command windows
psservice	Donne la liste des informations sur les services	www.sysinternals.com
sc	Outils d'interrogation sur les services	Command windows
DumpSec	Ligne de commande pour la configuration de la sécurité	www.somarsoft.com
tcpvcon	CLI montre les processus mappé sur le port	www.sysinternals.com
tcpview	GUI montre les processus mappé sur le port	www.sysinternals.com

Audité l'OS WINDOWS

Services inutiles

Alerter	Network DDE
Application Layer gateway Service	Network DDE DSDM
Clipbook	Printspooler
Error Reporting Service	Routing and Remote Access
Fax Service	Telephony
IMAPI CD-Burning COM Service	Telnet
Indexing Services Wireless	Upload Manager
Windows Messenger Service	Windows Image acquisition (WAI) Configuration
Netmeeting Remote Desktop Sharing	

Audité l'OS WINDOWS

Tests sur windows server:

- **S'assurer que les applications sur la machines sont celles approuvées par la procédure de management serveur** psinfo- s
  - **Rechercher les conflits entre applications**
  - **Les dépendances**
  - **Un nombre élevé d'applications signifie probabilité de compromission**
- **S'assurer que toutes les tâches en attentes sont toutes approuvées** schtasks

Audité l'OS WINDOWS

Gestion des compte et contrôle de mot de passe:

- **Revoir et évaluer la procédure des comptes utilisateurs et s'assure de la justification professionnelle de l'ensembles des comptes créés**
- **Revoir et évaluer la procédure d'habilitation sur les comptes d'utilisateurs ayant changés de statut**
- **S'assurer que les utilisateurs sont créés dans le domaine et clairement annoté dans active directory. Chaque utilisateur doit faire partie d'un groupe bien défini** compmgm.msc ou DumpSec.exe

Audité l'OS WINDOWS

Gestion des comptes et contrôle de mot de passe:

- **Revoir et évaluer les groupes, et déterminer les restrictions de chaque groupe. S'assurer que les restrictions fonctionnent**
- **Revoir et évaluer la dureté des mots de passe**
  - » Chaque compte doit avoir un mot de passe
  - » Crack mot de passe pwdump6 www.foofus.net/fizzgig/
  - » http://openwall.com/passwords/microsoft-windows-nt-2000-xp-2003
- Evaluer les politiques de sécurités des mots de passe
  - » Vieillissement
  - » Longueur
  - » Complexité
  - » Historique
  - » verrouillage

Les cracker de mot de passe:

cracker	coût	commentaire
Jonh	gratuit	Sur le site www.openwall.com force brut cracker. Supporte des lignes de commande
rcrack	gratuit	www.antsight.com/zsl/rainbowcrack. cet outil se trouve dans caïen et abel www.oxid.it
ophcrack	gratuit	http://ophcrack.sourceforge.net
Proactive Password Auditor	300-2500$	www.elcomsoft/ppa.html
SAMIside	$40	www.insidepro.com

Règles sur les comptes:

Règle	**Configuration**
Age minimum d'un mot de passe	1 jour
Age maximu d'un mot de passe	90-180 jours
Nombre de caractères minimum	8 caractères
Mot de passe complexe	Activé
Historique du mot de passe	10-20 en mémoire
Maximum d'essaie pour un mot de passe	10-20 essais
Durée de verrouillage de compte	10-30 mn

Audité l'OS WINDOWS

Revue options sécurités et droits utilisateurs:

- **l'installation par défaut windows 2003 à 39 droits d'utilisateurs et 70 options de sécurité**
- **Revoir et évaluer l'utilisation des droits d'utilisateurs et les options de sécurité accordées aux éléments dans la configuration des sécurités**
  - » **Les usages:**
  - » **Renommer les comptes utilisateurs et administrateurs**
  - » **Désactiver le compte invité**
  - » **Choisir de ne pas afficher le nom d'utilisateur de la dernière session**
  - » **Avertir l'utilisateur pour qu'il change sont mot de passe avant la date d'expiration**

Audité l'OS WINDOWS

Sécurité réseau et contrôles:

- **Revoir et évaluer l'utilisation de la connexion à distance et sa nécessité, RAS, FTP, Telnet, SSH, VPN et autres méthodes**
- **S'assurer qu'une bannière existe et s'affiche quand on se connecte au système**
- **Faire une revue des partages sur le système**
- **S'assure que l'audit est activé sur le serveur et que cette pratique est inscrite dans la procédure IT**
- **Évaluer les procédure de surveillance de la sécurité du SI**

Audité l'OS WINDOWS

Sécurité réseau et contrôles:

- **Revoir toute documentation sur le suivi de la sécurité du SI**
- **Faire attention à la fréquence du monitoring**
- **Regarder comment le monitoring de la détection d'intrusion se fait**
  - » **Outils: Tripwire et autre outils de monitoring des log**
- **Passer le système au scanner de vulnérabilité réseau**
- **Passer la machine au scanner de vulnérabilité**

Audité l'OS WINDOWS

Client Windows:

- **Déterminer si le client utilise le firewall de l'entreprise** Netsh

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\0008>netsh firewall show config

Domaine configuration du profil :
-------------------------------------------------------------------
Mode d'opération = Activer
Mode d'exception                    = Activer
Mode réponse multidiff/transmission = Activer
Mode de notification = Activer

Configuration de service pour le profil Domaine :
Mode     Personnalisé Nom
-------------------------------------------------------------------
Activer  Non          Partage de fichiers et d'imprimantes

Configuration des programmes autorisés pour le profil Domaine :
Mode     Nom / programme
-------------------------------------------------------------------
Activer  Assistance à distance / C:\WINDOWS\system32\sessmgr.exe

Configuration de port pour le profil Domaine :
Port   Protocole Mode     Nom
-------------------------------------------------------------------
139    TCP       Activer  Service de session NetBIOS
445    TCP       Activer  SMB sur TCP
137    UDP       Activer  Nom du service NetBIOS
138    UDP       Activer  Service de datagramme NetBIOS

Standard configuration du profil :
-------------------------------------------------------------------
Mode d'opération = Activer
Mode d'exception                    = Activer
Mode réponse multidiff/transmission = Activer
Mode de notification = Activer

Configuration de service pour le profil Standard :
Mode     Personnalisé Nom
-------------------------------------------------------------------
Activer  Non          Partage de fichiers et d'imprimantes

Configuration des programmes autorisés pour le profil Standard :
Mode     Nom / programme
-------------------------------------------------------------------
```

Audité l'OS WINDOWS

Sécurité réseau et contrôles:

- **Regarder aussi si le poste de travail a l'antivirus de l'entreprise**
- **S'assurer que les patchs sont à jour sur le client** pslist
- **S'assurer que le client à le MBSA (microsoft baseline security analyzer)**
  - » Compte actif sans mot de passe ou un mot de passe trivial
  - » Utilisant un système de fichiers plus vieux que le NTFS
  - » Autologin activé
  - » IIS activé
  - » L'ensemble des log de connexion est activé

Audité des Serveurs Web

Gestion des comptes:

- **Vérifier que le serveur web est sur une machine dédiée et non sur une machine sur laquelle se trouve une application critique**
- **Vérifier que le serveur web est bien patché et mise à jour avec le dernier code**
- **Déterminer s'il faut des outils supplémentaire pour la protection du serveur web)**
- **Vérifier que les services et modules inutiles sont désactivés. Les services qui tournent sur la machine devront avoir le minimum de privilège**

Audité des Serveurs Web

Gestion des comptes:

- **Vérifier que seul les protocoles et ports appropriés sont autorisés sur le serveur web**
- **Vérifier que le serveur web est bien patché et mise à jour avec le dernier code**
- **Vérifier que les comptes qui ont un accès sur le serveur web sont gérés correctement et ont des mots de passe bien durcis**
- **S'assurer qu'il existe des contrôles appropriés pour les fichiers, répertoires et répertoires virtuels**
- **S'assurer que les fichiers ou répertoires suivant sont bien protégés:**
  - » **Contenu du serveur web**
  - » **Les script du site**
  - » **Fichiers système**
  - » **Les utilitaires**

Audité des Serveurs Web

Gestion des comptes:

- **S'assurer que le serveur web a les logging appropriés activés et sécurisés**
- **Vérifier la validité et l'utilisation des certificats**
- **Vérifier que toutes les entrée sont validés avant de les utiliser sur les applications web**
  - » Data type
  - » Allowed caracter set
  - » Longeur minimum et maximum
  - » Null est il admis
  - » Est-ce qu'un paramètre est obligatoire ou pas?
  - » Est-ce qu'on admet des doublons

Audité des Serveurs Web

Gestion des comptes:

- **S'assurer que le serveur web est à jour sur les patches contre les attaques overflows**
- **S'assurer que l'application web est protégé contre les attaques par injection**
- **S'assurer qu'il existe un mécanisme sécurisé de stockage**
- **Déterminer s'il existe des contrôles adéquats pour lutter contre les dénis de service**

» Utilitaire: sur http://opensourcetesting.org/performance.php

Audité des Serveurs Web

Gestion des comptes:

- **Faire les revues suivantes:**
- **S'assurer que les mailing listes sont sécurisés et que les plateformes et applications sont surveillées**
- **Les patches de sécurité sont appliqués et que la procédure d'application est écrite**
- **Une procédure permettant de scanner régulièrement de l'intérieur comme de l'extérieur existe**
- **Une procédure de la configuration de la sécurité existe**

Audité des Serveurs Web

☐	1. Vérifié que le serveur web tourne sur un système dédié pas en conjonction avec une application critique
☐	2. Vérifié que le serveur web à reçu l'ensemble des derniers correctifs rigoureusement après approbation de ceux-ci
☐	3. Déterminer si le serveur web à besoin d'outils additionnels
☐	4. vérifier que les services et modules inutiles sont désactivés. Les services qui tournent sur la machines doivent avoir le juste privilège
☐	5. Vérifier que seul les bon protocoles et ports sont autorisés à accéder au serveur
☐	6. Vérifier que les comptes qui sont autorisés à accéder au serveur web sont gérés correctement
☐	7. S'assurer que les contrôles nécessaires sont faits sur les fichiers répertoires et répertoires virtuels
☐	8. Vérifier la validité des certificats sur le serveur web

Audité des Serveurs Web

☐	1. Vérifier toutes les entrées avant de les utiliser sur le serveur web
☐	2. vérifier que les contrôles sur les autorisations sont faits
☐	3. faire une revue les vulnérabilités sur les scriptes du site
☐	4. Vérifier que le serveur est mise à jour contre tous les buffers overflows connus
☐	5. S'assurer que les applications web sont protégées contre les attaques de type injection
☐	6. S'assurer que le stockage sécurisé et l'ensemble des mécanismes de sauvegarde est correctement et proprement fait
☐	7. déterminer le contrôle adéquat pour lutter contre les dénis de service

Audité les bases de données

Type d'objet	Description
table	ensemble de données organisées sous forme d'un tableau où les colonnes correspondent à des champs et les lignes à des enregistrements, également appelés entrées
View	une instruction SELECT sur une table ou une autre vue qui crée une table virtuelle. Les vues peuvent modifier le nombre ou l'ordre des colonnes, peuvent appeler des fonctions, et peuvent manipuler des données de diverses manières
Stored procedure/function	code procédural qui peut être appelé à exécuter des fonctions complexes au sein de bases de données. Les fonctions retournent des valeurs. Les procédures ne retournent pas de valeurs. Les stored procedure ou procédures stockées sont très efficaces pour l'accès aux données.
Trigger	code procédural qui est appelée quand une table est modifiée. Un trigger peut être utilisé pour effectuer toutes sortes d'actions, y compris les modifications sur d'autres tables.
Index	Mécanisme permettant d'obtenir une recherche rapide de données. Les indices sont des objets complexes, et leur mise au point correcte est essentielle à la performance d'une base de données.

Audité les bases de données

Gestion des comptes:

- **S'assurer que les permissions sont données et retirées de façon appropriée**
- **Faire la revue des permissions accordées à un individu au lieu d'un groupe ou un rôle**
- **Vérifier s'il n'existe pas d'accès implicite qui ont été obtenu par erreur**
- **Retirer la permission PUBLIC où cela n'est pas nécessaire**
- **Restreindre l'accès à l'OS**

Audité les bases de données

- Commandes Sql (Structured Query Language):
  - **Les commandes sql sont utilisées pour extraire des données d'une base de données**

SQL commandes	Description
SELECT	Affiche un set de données d'une table
INSERT	Ajoute une nouvelle donnée dans la table
UPDATE	Modifie une donnée existante dans la table
DELETE	Enlève un set de données de la table

Audité les bases de données

- **Avant de commencer**:
- Vous devez demander un compte pour accéder à la base de données
- Si possible avoir toutes les tables dont vous avez besoin offline
- Il est bon de faire les tests offline tant que cela est possible
- Faire verrouiller le compte que vous a créer à la fin de votre mission

Audité les bases de données

Gestion des comptes:

- **Restreindre l'accès du répertoire où se trouve la base de donnée**
- **Restreindre les permissions sur les clé du registre utilisées par la base de donnée**
- **Rechercher les utilisateur par défaut et les mots de passe par défaut**
- **Rechercher les mots de passe facile comme password et secret**

Audité les bases de données

Gestion des comptes:

- **S'assurer que les capacité de gestion de mot de passe de la base de données est bien activé:**
  - » Expiration du mot de passe
  - » Réutilisation du mot de passe
  - » Verrouillage du compte
  - » Réinitialisation du mot de passe après verrouillage

Audité les bases de données

Surveillance de l'activité:

- **Il faut considérer les points suivants sur la base:**
  - » Audit de l'accès et de l'authentification
  - » Audit utilisateurs et administrateurs
  - » Audit des activités suspectes
  - » Audit des vulnérabilités
  - » Audit des changements

Audité les bases de données

Gestion des comptes:

- **S'assurer que l'audit est activé**
  - » Activé l'audit natif de la base de données
  - » Surveiller l'activité réseau pour auditer la base de données
  - » Faire une revue du logs des transactions pour avoir une piste d'audit pour la base de données
- **Vérifier que l'encryptions est mise en œuvre sur le réseau**
- **Vérifier que les derniers patches de la base de données sont installés**

Audité les bases de données

Gestion des comptes:

- **S'assurer de l'intégrité des données de la base en recherchant toute sorte d'application de corruption de données ex: trojan horses**
- **Restreindre les permissions sur les clé du registre utilisées par la base de donnée**
- **Rechercher les utilisateur par défaut et les mots de passe par défaut**
- **Rechercher les mots de passe facile comme password et secret**

Audité les bases de données

- **Vérifier que la base de données est à jour sur les patches**
- **Vérifier que la base de données est encore maintenue par le vendeur**
- **Vérifier qu'il existe une procédure en place qui alerte sur le nouveaux patches de la base de données pour leur application.**

Audité des applications

- **Usurpation d'identité**: l'usurpation d'identité est un risque important pour les applications qui ont de nombreux utilisateurs, mais qui fournissent un contexte d'exécution unique au niveau application et base de données.

- **Falsification de données**: les utilisateurs peuvent potentiellement changer les données qui leur sont livrés, et donc potentiellement de manipuler la validation côté client tels que les que les résultats de GET, POST, HTTP headers ainsi de suite. Les applications ne devraient pas envoyer des données à l'utilisateur, tels que les taux d'intérêt ou des périodes, qui sont obtenus uniquement à partir des applications elles-mêmes. L'application doit aussi vérifier soigneusement les données reçues de l'utilisateur et valider qu'elles sont saines et applicables avant de les enregistrer ou de les utiliser. Pour les applications Web et autres applications ayant un composant client, assurez- vous d'effectuer vos contrôles de validation sur le serveur et non pas le client, où les contrôles de validation pourraient être altérés.

Audité des applications

- **Rejet**: Les utilisateurs peuvent contester des transactions s'il y a un manque de vérification ou d'historique de leur activité. De préférence, l'application doit s'exécuter avec les droits ou privilèges de l'utilisateur, pas plus, mais cela peut ne pas être possible avec de nombreuses applications commerciales disponibles sur le marché.

- **Divulgation d'information professionnelle ou de données**: Les utilisateurs se méfient à juste titre de soumettre leurs informations personnelles à un système informatique. s'il est possible pour un hacker de révéler publiquement les données des utilisateurs, que ce soit de manière anonyme ou en tant qu'utilisateur autorisé, il y aura une perte immédiate de la confiance et de réputation. En conséquence, les applications doivent inclure des contrôles rigoureux pour éviter l'abus et la manipulation des users ID, surtout si elles utilisent un contexte unique pour exécuter l'application entière.

Audité des applications

- **Déni de Service**: Les concepteurs d'applications doivent être conscients que leurs applications peuvent être soumises aux attaques de type déni de service. Par conséquent, l'utilisation des ressources lourdes telles que des fichiers volumineux, des calculs complexes, les longues requêtes doit être réservé aux utilisateurs authentifiés et autorisés et ne pas être disponibles aux utilisateurs anonymes.

- **Elévation des privilèges**: Si une application dispose des rôles d'utilisateur et d'administrateur différents, il est essentiel de s'assurer que l'utilisateur ne puisse pas obtenir des privilèges supérieurs à ceux qu'il a normalement.

Audité des applications

- **Faire une revue et une évaluation des contrôles sur les données en entrée**
  - » S'assurer que les champs num n'accepte pas l'entrée des caractères alphanumériques
  - » Les champs de date et heures doivent intégrer un contrôle pour que les données soient correctement entrées
  - » Les doublons ne doivent pas être acceptés
  - » Les transactions doivent intégrer un contrôle logique de données
  - » Il faut absolument insérer des program cutoff control pour prévenir que les utilisateurs ne valide pas des données au mauvais moment
  - » L'utilisation des opérateurs de base de données (comme *, =, ou select) ne doivent pas être autorisés comme entrée.

Audité des applications

- **Faire une revue et une évaluation des contrôles en place sur les données en entrée ou en réception d'une interface du système**
- **Dans le cas où le même donnée est répartie sur plusieurs bases de données ou système, s'assurer qu'il existe un processus d'une synchronisation périodique pour détecter l'inconsistance de la donnée**
- **Revoir et évaluer les pistes d'audites présents dans le système et les contrôles sur de ces pistes d'audites**
- **S'assure que le système à les moyens de tracer les transactions ou une portion de données du début à la fin du processus**

Audité des applications

- **S'assurer que l'application fournit les mécanismes d'authentification des utilisateurs, basés au minimum, sur un identifiant unique pour chaque utilisateur et un mot de passe confidentiel**
- **Revoir et évaluer le mécanisme d'autorisation de l'application pour s'assurer que les utilisateurs ne peuvent pas accéder à des transactions ou données sensibles sans au préalable avoir reçu une autorisation du mécanisme de sécurité du système**
- **S'assurer que le mécanisme de sécurité du système possède une fonction d'administrateur avec les contrôles appropriés et les fonctionnalités**

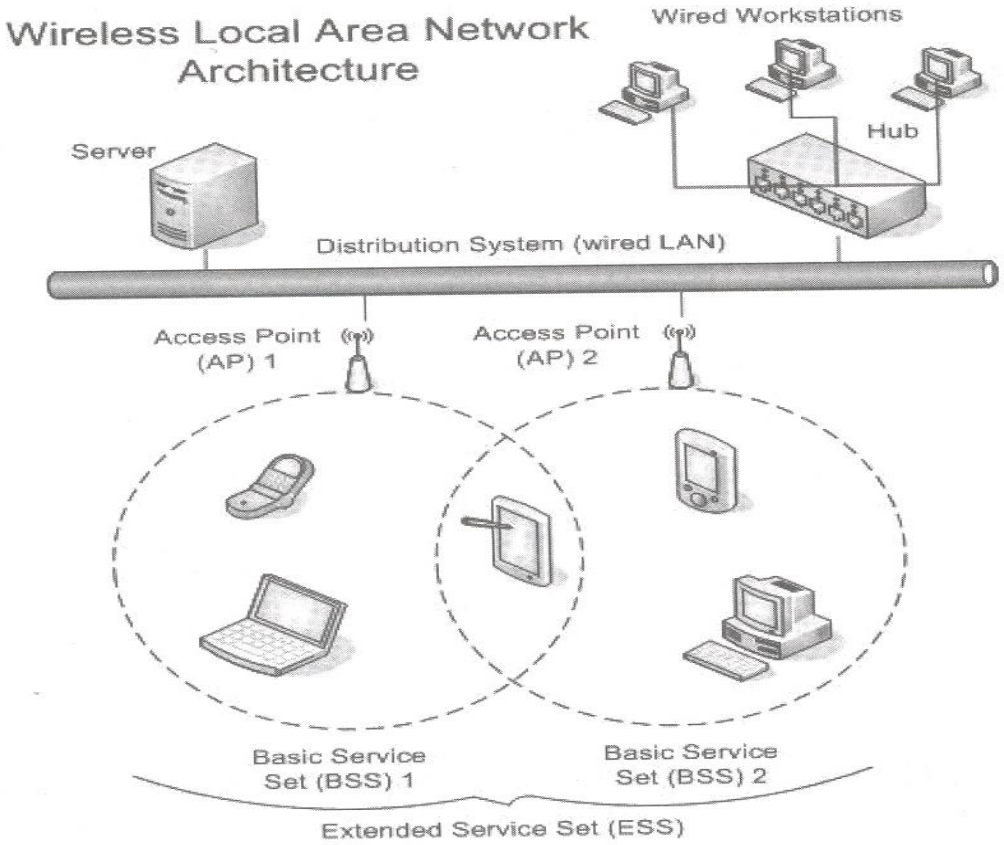
Audité des applications

- **S'assurer que les mécanismes et procédures existent pour suspendre des utilisateurs, quand ils ont changé de fonction ou quitté l'entreprise**
- **Vérifier que les contrôles sur le mot de passe de l'applications sont vraiment appropriés**
- **S'assure que les utilisateurs sont sortis automatiquement de l'application au bout d'un certain temps d'inactivité qui est configurable par l'administrateur**
- **Evaluer l'utilisation de l'encryptions de donnée par l'application pour la protection des données**

Audité des applications

- **Vérifier si les développeurs ne peuvent pas altérer les données en production**
- **S'assurer que la mise en production d'une application passe par les étapes de test, homologation avant la production**
- **Evaluer les contrôles sur le code, les modifications et le versionning**
- **S'assurer qu'il existe un contrôle du processus de backup de l'application**
- **S'assurer qu'une procédure de recouvrement de données existe et en place pour l'application**

Audite d'un WLAN et des équipements mobiles



Audite d'un WLAN et des équipements mobiles

WLAN audit technique

- **S'assurer que les points d'accès sont mise à jour avec la dernière version de logiciel**
- **Evaluer la procédure de contrôle de la gestion de l'administration centralisée**
- **S'assurer que les clients mobiles ont le minimum de protection**
  - » **Firewall**
  - » **antivirus**
- **Evaluer la sécurité de la méthode d'authentification**
  - » **EAP-TLS, PEAP, EAP-MD5**

Audite d'un WLAN et des équipements mobiles

WLAN audit technique

- **Évaluer la sécurité de la méthode de communication choisie**
- **Evaluer la procédure de surveillance de la sécurité**
- **Vérifier que des points d'accès fantômes n'existent pas sur le réseau**
- **Evaluer la procédure en place pour résoudre les demandes des utilisateurs**

Audite d'un WLAN et des équipements mobiles

WLAN audit technique

- **S'assure qu'il existe une procédure appropriée en place pour la sécurité du WLAN**
  - Vérifier l'existence des procédures et se rendre compte de leur connaissance par l'administrateur du WLAN
  - Si les procédures existent et non suivie il faut trouver les raisons de la non application
  - Toute transmission radio doit être encrypter pour prévenir contre les écoutes
  - Tous les points d'accès doivent être à jour sur le firmware
  - Seul les personne autorisées peuvent avoir un accès d'administration du réseau
  - Les mots de passe des points d'accès doivent suivre le durcissement de la compagnie
  - Le nom par défaut du réseau n'est pas admissible (ESSID)
  - Les clients doivent utiliser IPSec sur un vpn

Audite d'un WLAN et des équipements mobiles

WLAN audit technique

- **Evaluer le plan de sinistre pour du WLAN**
  - Si les procédures existent et non suivie il faut trouver les raisons de la non application
  - Toute transmission radio doit être encrypter pour prévenir contre les écoutes
  - Tous les points d'accès doivent être à jour sur le firmware
  - Seul les personne autorisées peuvent avoir un accès d'administration du réseau
  - Les mots de passe des points d'accès doivent suivre le durcissement de la compagnie
  - Le nom par défaut du réseau n'est pas admissible (ESSID)
  - Les clients doivent utiliser IPSec sur un vpn

Audité Unix et linux

répertoires usuels Unix et linux

répertoire	Description
/bin	Dossier où est logé la plupart des binaires du système
/sbin	Contient les binaires dont l'utilisation réservée aux comptes privilèges
/etc	Contient les fichiers de configuration système
/boot	Dans beaucoup de systèmes contient le noyau
/home	C'est le home directory des utilisateurs
/var	Contient les informations dont les programmes ont besoins pour tourner
/lib	Librairie système et application
Usr/	C'est un autre endroit où trouver les packages utilisateurs ; d'autres répertoires peuvent s'y trouver
/root	Le home directory du compte root y est placé
/tmp	Répertoire temporaire auquel tout utilisateur peut accéder
/mnt	Les fichiers distants peuvent être montés en cet endroit
/dev	Représente le concept que tout est fichier, on y trouvera les fichiers de périphérique, représentant les hardware du système

Audité Unix et linux

Gestion des comptes:

- **Evaluer le vieillissement des mots de passe**
- **S'assurer que tous les UserID dans fichier password sont unique**
  - » Cat /etc/passwd |awk –F: '{print $3}' | uniq –d
- **Revoir la procédure de gestion du password initial et comment il est communiqué à l'utilisateur**
- **Chaque compte doit être associé à un employé et qu'il est bien tractable**
- **Un shell invalide doit être associé à tous les comptes désactivés**

Audité unix et linux

Gestion des comptes:

- **Revoir et évaluer les procédures de création des comptes unix et linux et surtout que les utilisateurs sont désactivé s'ils ne sont plus dans l'entreprise**
- **S'assurer que tous les UserID dans fichier password sont unique**
  - » Cat /etc/passwd |awk –F: '{print $3}' | uniq –d
- **S'assurer que les mots de passe sont shodow et utiliser un hachage si possible**
  - » More /etc/ passwd (chercher dans le fichier passwd '*' ou »x »
- **Evaluer les permissions sur les fichiers de password de son ombre (shadow)**
- **Revoir et évaluer la solidité de mise en œuvre pour les mots de passe**

Audité unix et linux

Gestion des comptes:

- **Evaluer le vieillissement des mots de passe**
- **S'assurer que tous les UserID dans fichier password sont unique**
  - » Cat /etc/passwd |awk –F: '{print $3}' | uniq –d
- **Revoir la procédure de gestion du password initial et comment il est communiqué à l'utilisateur**
- **Chaque compte doit être associé à un employé et qu'il est bien tractable**
- **Un shell invalide doit être associé à tous les comptes désactivés**

Audité unix et linux

Gestion des comptes:

- **Revoir et évaluer le niveau d'accès superuser**
- **Revoir et évaluer l'usage des groupes et déterminer les restrictions associées**
- **Évaluer l'utilisation des mots de passe au niveau groupe**
- **Revoir et évaluer la sécurité des répertoires dans le chemin par défaut utilisé par l'administrateur quand il ajoute un nouvel utilisateur**
- **Revoir et évaluer la sécurité des répertoires dans le chemin root. Évaluer l'utilisation de « current directory » dans le chemin**

Audité unix et linux

Gestion des comptes:

- **Revoir et évaluer la sécurité des home directory de l'utilisateur et des fichiers de configuration. Généralement devrait avoir le droit écrire pour le propriétaire**
- **Chercher les repèrtoires open (avec une permission** drwxrwxrwx**) dans le système**
- **Revoir et évaluer la sécurité sur le noyau**
- **S'assurer que les fichiers ont un propriétaire légal dans /etc/passwd file. Examiner les atjob programmer dans le système pour s'assurer qu'il n'y a rien de suspect**

Audité unix et linux

- **Déterminer les services réseaux qui sont activés dans le système, et valider leur nécessité. Pour les services nécessaires revoir et évaluer les procédure de mise à jour des vulnérabilités connues de ces services.**
- **Exécuter un utilitaire de vulnérabilité réseau pour chercher les vulnérabilités éventuelles dans l'environnement**
- **Si les ftp anonimous sont activés s'assurer qu'ils sont bien contrôlés**
- **Si NFS est activé et vraiment nécessaire, s'assurer qu'il est proprement sécurisé.**

Audité unix et linux

- **Faire une revue de l'utilisation des protocoles sécurisés**
- **S'assurer qu'une bannière existe pour toute connexion au système**
- **Revoir et évaluer l'utilisation des protocoles sécurisés**
- **Revoir et évaluer l'utilisation de fichiers .**netrc
- **Revoir et évaluer l'utilisation des modems sur le serveur**

Panorama des solutions de secours

- **Maillons du SI:**
  - **Les serveurs (applications, fichiers, impression, messagerie, techniques, etc.);**
  - **Le réseau local**
  - **Les accès au(x) réseau(x) externe(s)**
  - **Les accès à l'internet,**
  - **Les postes utilisateurs,**
  - **La téléphonie**

Panorama des solutions de secours

- **Typologie des moyens de secours**
  - **Salles blanches (cold sites):**
  - **Salles oranges (warm sites):**
  - **Salles rouges (hot sites):**
  - **Salles miroir (mirrored sites),**

Panorama des solutions de secours

- **De la bonne distance:**
  - **Sinistre ouragan: en moyenne 150km**
- **Disponibilité:**
  - **La haute disponibilité im. (mn)**
  - **La moyenne disponibilité, qlq h. entre 6 et 24h**
  - **La faible disponibilité au-delà de 48h,**

Panorama des solutions de secours

- **Sauvegarde, restauration et disponibilité des données:**
  - **Méthode de sauvegarde:**
    - » **Sauvegarde complète**
    - » **Sauvegarde incrémentale**
    - » **Sauvegarde différentielle**
    - » **Journalisation**

POLITIQUE DE CLASSIFICATION ET DE PROTECTION DE L'INFORMATION

Contexte et Objectifs

- L'information constitue pour le Groupe Société Générale un actif qu'il importe de protéger en fonction du niveau de risque qui lui est attaché.

  L'objectif est d'assurer la protection de l'information vis-à-vis des différentes catégories de risques susceptibles de l'affecter (l'indisponibilité, l'altération, la divulgation ou l'insuffisance de moyens de preuve), et d'engendrer un préjudice -notamment financier, juridique ou d'image

- L'identification des exigences de sécurité des informations permet, après analyse des risques :
  - de classifier les informations, afin de permettre la mise en œuvre de mesures de prévention, de protection et de contrôle, ainsi que de pistes d'audit pertinentes ;
  - et de définir les moyens de sécurité adéquats selon les critères de disponibilité, d'intégrité et de confidentialité des informations, ainsi que d'existence de moyens de preuve suffisants.

POLITIQUE DE CLASSIFICATION ET DE PROTECTION DE L'INFORMATION

- **Objectif de la classification**

- Cette diapositive décrit les principes applicables en matière de politique de classification et de protection de l'information.
- Ces principes sont au nombre de cinq :
  - propriété de l'information ;
  - classification de l'information par niveau ;
  - proportionnalité et gradation des mesures de protection ;
  - marquage de l'information ;
  - évolution du niveau de classification des informations.
- Il précise en outre les règles de gouvernance applicables pour classifier les informations

POLITIQUE DE CLASSIFICATION ET DE PROTECTION DE L'INFORMATION

- **Les principes directeurs de classification et de protection de l'information**
  - **Principe 1 - Propriété de l'information**
    - Le propriétaire d'information est une personne ou une entité ayant des responsabilités de création, d'entretien, de mise à jour, de suivi et / ou d'évolution d'une information. Il s'agit, soit de l'auteur qui est, de par sa fonction ou sa mission, à l'origine des données, soit de l'entité métier ayant la charge de leur création dans le cadre de l'organisation du Groupe. Dans le cas d'une entité, son responsable assure le rôle de propriétaire.
  - **Principe 2 - Classification de l'information par niveaux**
    - Toute information traitée doit recevoir une classification de sécurité. La classification consiste à associer à chaque information un niveau de sécurité choisi parmi des niveaux prédéfinis, pour chaque critère de classification (par exemple, une information classée C3 en confidentialité doit être transmise chiffrée alors que le chiffrement n'est pas obligatoire pour la classification C1).

POLITIQUE DE CLASSIFICATION ET DE PROTECTION DE L'INFORMATION

- **Les principes directeurs de classification et de protection de l'information**
  - **Principe 2 - Classification de l'information par niveaux**
  - **Les critères de classification sont :**
  - **la disponibilité** : propriété d'être accessible et utilisable à la demande d'une personne ou d'une entité autorisée dans les délais impartis ;
  - **l'intégrité** : propriété assurant qu'une information – ou un processus automatisé de traitement de cette information – n'a pas été modifié, altéré ou détruit de façon accidentelle ou non autorisée ;
  - **la confidentialité** : propriété selon laquelle une information ne peut être divulguée ou rendue accessible à des individus, entités ou processus n'ayant pas à connaître cette information, ou non autorisés ;
  - **la preuve** : propriété d'être en mesure de prouver qu'une action ou un événement relatif à l'information a eu lieu. Elle est caractérisée par un niveau de qualité de mémorisation des différentes actions liées à l'utilisation des informations manipulées (par exemple, à travers l'existence et l'archivage de « pistes d'audit »).

POLITIQUE DE CLASSIFICATION ET DE PROTECTION DE L'INFORMATION

- **Les principes directeurs de classification et de protection de l'information**
  - **Principe 3 - Proportionnalité et gradation des mesures de protection**
  - Le principe de proportionnalité et de gradation des mesures de protection consiste à protéger chaque information et/ou chaque système en fonction de son niveau de classification dans chacun des critères de disponibilité, d'intégrité, de confidentialité et de preuve.

  - **Principe 4 - Marquage de l'information**
  - Tout support d'information, quels que soient sa forme et son niveau de classification, doit porter un marquage approprié et adapté au contexte afin d'en garantir la lisibilité, permettant d'y associer le niveau de protection adéquat (par exemple sous la forme d'un « cartouche » inséré en en-tête de chaque document, précisant un certain nombre de rubriques à renseigner, en particulier les niveaux de classification associés au document, son auteur, sa référence, etc.).

  - **Principe 5 - Évolution du niveau de classification des informations**
  - La classification est revue autant que de besoin par son propriétaire (ou dépositaire) en fonction du contexte ou d'un événement marquant (par exemple, échéance de la date limite de validité de classification, évolution des risques et des mesures de sécurité, etc.). Ce processus prend la forme d'une dé-classification si le niveau de classification diminue, de sur-classification si le niveau de classification augmente.

POLITIQUE DE CLASSIFICATION ET DE PROTECTION DE L'INFORMATION

- **Sensibilisation**
  - L'efficacité des règles de classification et de protection des informations est conditionnée par une sensibilisation de l'ensemble des acteurs concernés aux objectifs, aux enjeux et aux méthodes de classification des informations. Les actions de sensibilisation permettent ainsi de garantir une adhésion ainsi qu'une compréhension correcte et cohérente des mesures préconisées de la part de l'ensemble des personnels de l'entreprise. Chaque responsable hiérarchique doit sensibiliser ses collaborateurs à l'importance du respect de ces règles. Il convient aussi de demander aux intervenants externes (et particulièrement aux intérimaires et aux prestataires) de procéder à une sensibilisation comparable de leurs salariés mis à la disposition.
  - Un rappel régulier de ces règles doit être effectué tant auprès des agents permanents que des intervenants temporaires. Un document de sensibilisation doit être remis aux salariés nouvellement recrutés, ainsi qu'à chaque prise de poste.

Méthode et Outils

Recherche de l'information:

- C'est la première étape dans la conduite des testes de pénétration
  - A la fin de cette étape nous devons avoir un détail de l'architecture du réseau et connaitre la complexité de notre mission d'audit
  - Identifier le type de système sur le réseau, OS etc..
  - Deux types de recherche d'informations:
    - Recherche d'information passive
    - Recherche d'information active

Méthode et Outils

Recherche de l'information:

- Rechercher d'informations passives:
  - Cette étape se fait offline, elle consiste à prélever des informations sur le réseau et l'OS sans les se connecter directement aux équipements
  - Identifier à cette étape aussi les informations sur la société, la localisation du réseau et des systèmes informatiques
    - Rechercher le site internet de l'entreprise
    - Rechercher avec un moteur de recherche toute information la concernant
    - Chercher des groupes de discussion où on trouve les employés de l'entreprise cible
    - Si les employés ont un site personnel les visiter
    - Rechercher les offres d'emploi du site
    - Etc..

Méthode et Outils

Recherche de l'information:

- Rechercher d'informations passives:
  - **Web presence**: cette phase permet d'avoir les informations suivantes –santé financière de l'entreprise – informations sur les employés – le positionnement physique et logique – architecture réseau - etc.
  - Cette étape utilise les outils suivant:
    - Web browser
    - Alexa.org
    - Archive.org
    - dig
    - nslookup

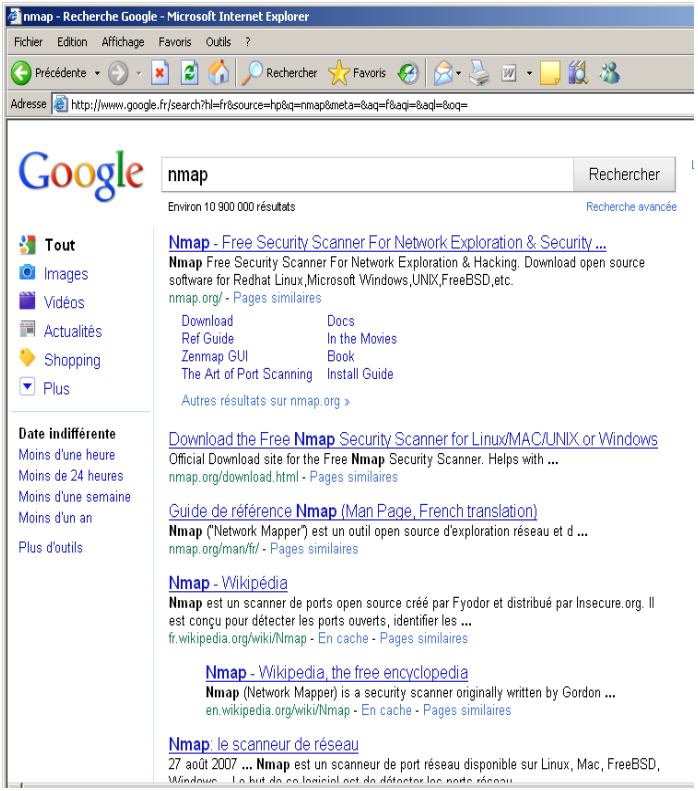
Méthode et Outils

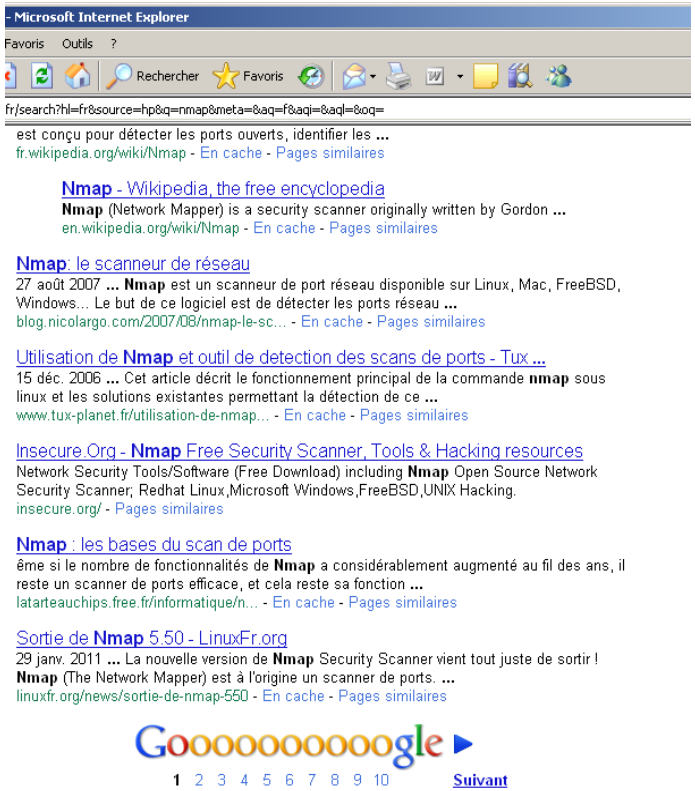
Recherche de l'information:

- Rechercher d'informations passives:
  - **Que cherche –t- on avec ces outils**: adresse site web, type de serveur web, localisation, dates dernière mises à jour, les liens internet (interne et externe), arborescence des répertoires web, les standards d'encryptions, les adresses sur le site, la possibilité d'e-commerce, les services et produits offerts

Méthode et Outils

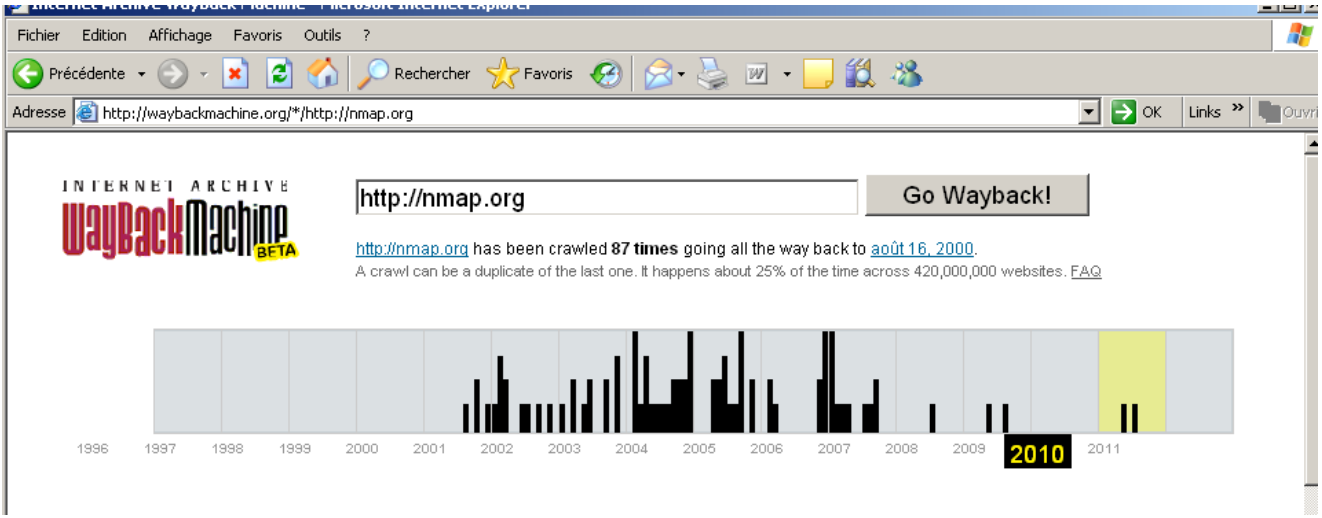
Recherche de l'information:





Méthode et Outils

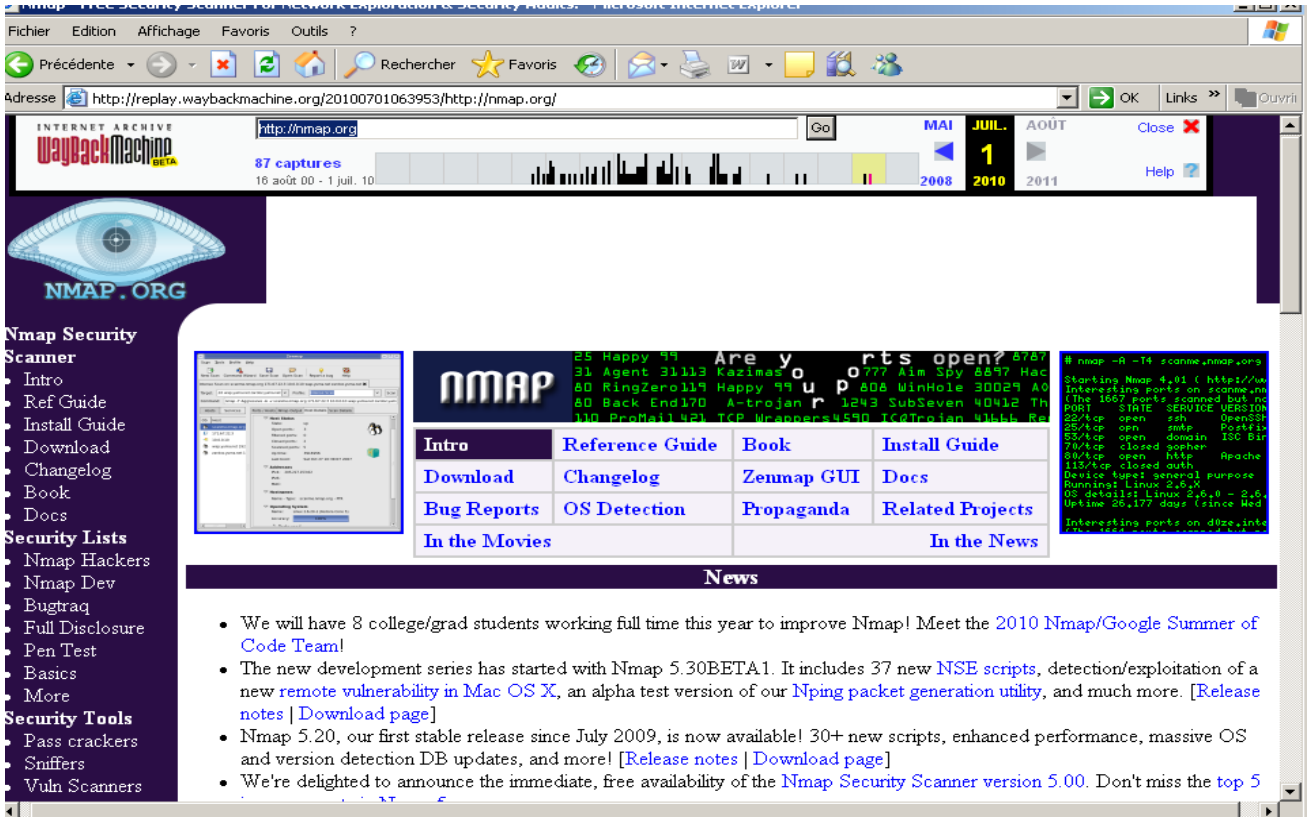
Recherche de l'information:



Ce site a changé 87 depuis aout 2010

Méthode et Outils

Recherche de l'information:



Méthode et Outils

Recherche de l'information:

Méthode et Outils

Recherche de l'information:

- Rechercher d'informations actives:
  - Cette étape se fait online, elle consiste à prélever des informations sur le réseau et l'OS en nous connectant directement aux équipements
  - Identifier à cette étape aussi les informations sur la société, la localisation du réseau et des systèmes informatiques

Méthode et Outils

Recherche de l'information:

- Rechercher d'informations actives:
  - Chercher les information sur le dns avec l'outils dig
  - Prendre les informations comme existence de serveur de messagerie
  - Chercher si une dmz existe dans l'entreprise

Exemple de plan proposé pour un programme de travail

- ***A. Rappel des objectifs***
  - **A.1. Modalité de traitement des états d'anomalies et des factures anormales**
  - **A.2. Conception des états d'anomalies**
  - **A.3. Impact des factures anormales sur les réclamations**

Exemple de plan proposé pour un programme de travail

- ***B. Etude des procédures - Mémorandum***
  - **B.1. Organisation**
  - **B.2. Traitement de l'information concourant à la facturation**
  - **B.3. Les contrôles de la facturation:**
    - » les états de sortie ;
    - » contrôle au centre de traitement (au niveau de l'exploitation informatique) ;
    - » contrôle dans les agences ou filiales pour les grandes entreprises. *BA.* Les réclamations:
    - » au centre de traitement;
    - » aux agences**.**

Exemple de plan proposé pour un programme de travail

- **C. *Principaux points forts et points faibles***
  - **Points forts et points faibles du centre de traitement.**
  - **Points forts et points faibles des agences.**
- ***D. Vérifications***
  - **Contrôle de la facturation des gros clients.**
  - **Contrôle de la facturation des clients ordinaires. - Contrôle des autres prestations facturées.**
  - **Contrôle des anomalies des états.**

Exemple de plan proposé pour un programme de travail

Introduction (avec rappel de l'ordre de mission).

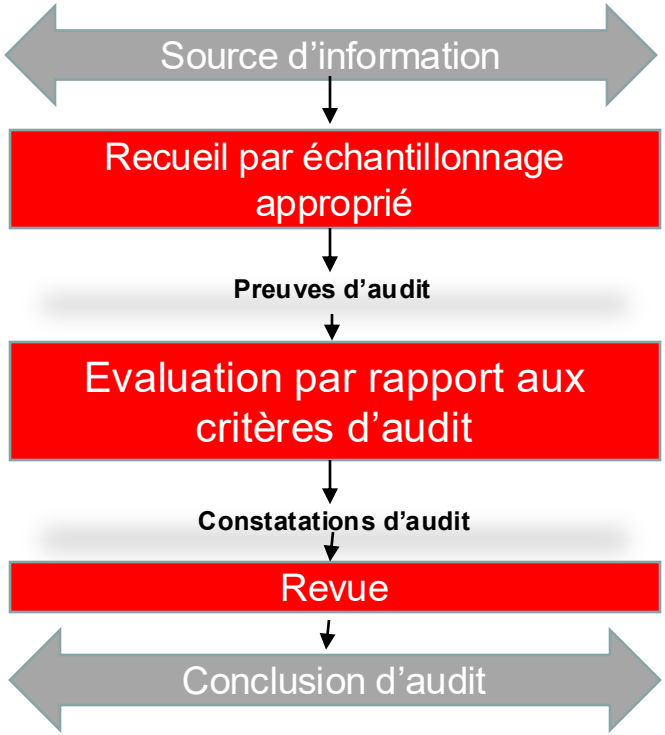
- Contexte d'exploitation du centre des serveurs.

Diagnostic et recommandations.

- *A. Système physique: architecture générale des serveurs et interfaces*
- *- Les points forts. - Les points faibles. - Recommandations.*
- *B. Systèmes logiciels et les problèmes des ports*
- *- Les points forts et les points faibles concernant les logiciels utilisés.*
- *- Les points forts et les points faibles concernant les affectations des ports.*
- *C. Les autres types de risques*
- *- Recommandations.*
- *- Conclusion: dans cette partie, les auditeurs devraient préconiser l'application stricte des recommandations compte tenu des risques encourus, ainsi qu'une mise à niveau rapide des procédures.*

Vue d'ensemble du processus d'audit

ISO 19011, Clause 6.4.7



Procédure de collecte et d'analyse de preuve

Procédure de collecte de preuves

- A. Observations
- B. Revue documentaire
- C. Entretien
- D. Analyse
- E. Vérification technique

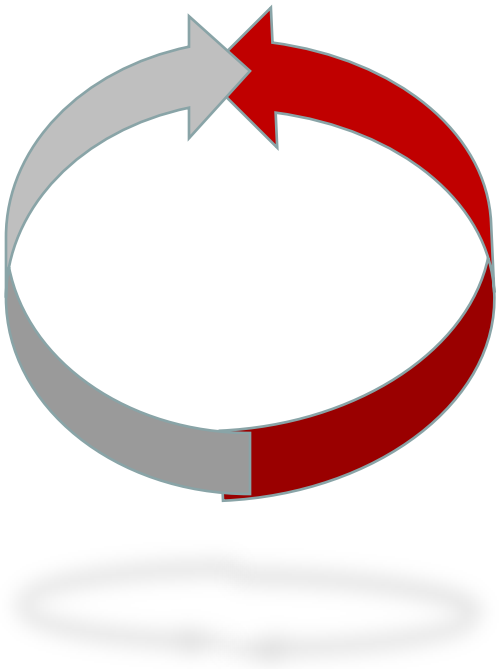
Procédure d'analyse de preuves

- F. Corroboration
- G. Evaluation

A. Les procédures d'audit: l'observation

- Dans le cas d'une observation directe, l'auditeur constate avec objectivité un phénomène à partir de ses propres sens et à l'aide de procédures appropriées
- Par exemple, l'auditeur observe:
  - Le déroulement d'un processus de mise à jour d'un logiciel
  - Les performances d'un employé
  - L'inventaire des ordinateurs
  - La présence d'un dispositif de prévention d'incendie

Types d'observation



Observation générale

- Permet de confirmer l'existence d'un processus ou d'un groupe de mesures de sécurité et d'obtenir un niveau de compréhension suffisant du fonctionnement de ceux-ci
- Exemple: l'auditeur visite le centre de traitement de données

Observation détaillée

- Permet l'obtention d'information d'informations détaillées lesquelles aident à évaluer et à déterminer si les contrôles mis en œuvre fonctionnent de manière efficace, continue et sans erreur.
- Exemple: l'auditeur écoute plusieurs appels en direct adressé au centre de service

B. Les procédures d'audit: Revue documentaire

- La revue documentaire consiste en un examen systématique et méthodique de document textuels
- L'auditeur doit évaluer la conformité des documents en fonction du:
  - contenu
  - Format
  - Gestion du processus documentaire

B. Les procédures d'audit: Revue documentaire

- L'auditeur doit documenter ses observations
- Cela peut être effectué de divers manières:
  - Prise de notes
  - Photocopie de documents
  - Prise de photos ou enregistrements audio/vidéo
  - La présence d'un dispositif de prévention d'incendie

C. Procédure d'audit l'entretien

- Entretien/interview: poser des question (orales ou écrites) aux employés et aux autres personnes appropriées (tiers) dans le but de recueillir des preuves d'audit
- Pour être efficace l'auditeur en charge de l'entretien doit:
  - Eviter d'influencer les informations
  - Prendre des notes rapidement
  - Corroborer l'information chaque fois que c'est possible