AUDIT SI

ESTM – DAKAR

Année 2018 – Mamadou Boli BA

Sommaire

C’est quoi l’audit informatique

Introduction

Définition

- L’audit correspond au besoin de faire faire un diagnostic par un expert indépendant pour établir un état des lieux, définir des points à améliorer et obtenir des recommandations pour faire face aux faiblesses de l’entreprise.

- L’auditeur intervient en tant que mesureur des risques, il identifie
  - Faiblesses
  - Impacts
  - Solutions
  - Risques
- Si les mesures ne sont pas prises

Introduction

Définition

- L’audit informatique est largement utilisé mais certaines prestations réalisées sous le terme « audit informatique » sont en fait des missions de conseil.

- Le champ d’application principal de l’audit informatique doit rester l’informatique au sens large (application, matériels, ….) et de plus en plus les outils liés à l’usage des technologies de l’internet.

Introduction

Objectifs

- En termes de fiabilité de l'environnement informatique
  - L'intérêt d'un contrôle interne
  - Les acteurs de l'audit informatique
  - Les composants d'un audit de l'activité informatique
  - Les méthodes d'audit de l'activité informatique

Introduction

Objectifs

- L'intérêt d'un contrôle interne est
  - de contribuer à la maitrise de l'entreprise
- Il a pour but
  - D'assurer la protection et la sauvegarde du patrimoine et la qualité de l'information
  - De valider l'application des instructions de la direction et favoriser l'amélioration des performances
- Il se manifeste par
  - L'organisation, les méthodes et procédures

Introduction

Objectifs

- Le contrôle interne a pour objectif
  - Une bonne organisation d'ensemble de l'activité informatique
  - La mise en disposition de procédures
  - L'existence de méthodes

- La finalité du contrôle interne est
  - De réduire les risques de malveillance
  - De disposer de procédures formalisées bien comprises
  - D'améliorer l'efficacité de l'activité informatique

Introduction

Les acteurs

- Direction de l'entreprise
- Le responsable informatique
- Contrôleurs externes (commissaire aux comptes, administration fiscale, banques, …..)

Introduction

Les composants d'un audit de l'activité informatique

- Examen de l'organisation générale du service
- Examen des procédures liées au développement et la maintenance des applications
- Examen des procédures liées à l'exploitation des chaînes de traitement
- Examen des fonctions techniques

Introduction

Les méthodes d'audit de l'activité informatique

- Entretien avec le personnel et les utilisateurs du service
- Contrôle de documents ou d'états
- Outils commercialisés(progiciel)
- Méthodes (COBIT, MEHARI, ….)

Introduction

Objectifs en termes d'efficacité et de performances

- Mise en place d'un plan de secours
- Etude approfondie de la performance et du dimensionnement des machines
- adéquation aux besoins des logiciels système

En d'autres termes l'audit d'efficacité constitue une mission mandatée

- soit par la direction générale, afin de s'interroger sur le coût de son informatique,
- soit par le responsable du service de manière à vérifier la pertinence de sa configuration

Introduction

Objectifs en termes de fiabilité d'une application informatique

- Objectif premier: « se prononcer sur la qualité d'une application donnée »

- Les types de contrôles:
  - Contrôle de la fiabilité d'une application ou son utilisation
  - Contrôle de l'adéquation des logiciels développées par rapport aux spécifications fonctionnelles
  - La recherche de fraude ou erreurs
  - Le contrôle de la qualité des méthodes de développement des logiciels
  - Le contrôle de la qualité des procédures d'exploitation

Démarche

Intervenants

- Auditeur externe contractuel
  - SSII
  - FREELANCE

- Avec pour missions:
  - Examen de contrôle interne de la fonction informatique
  - Audit de la sécurité physique du centre de traitement
  - Audit de la confidentialité d'accès
  - Audit des performances

Démarche

Intervenants

- Domaines dans lesquels les auditeurs informatiques sont les plus fréquemment sollicités (source AFAI)

Domaine	Pourcentage
Sécurité logique	80%
Conduite de projets	68%
Revue environnement informatique	66%
ERP / Revue d'application	58%
Production	54%
Maitrise d'ouvrage et Cahier des charges	54%
Analyse de données	50%
Développement et rôle des études	46%
Recettes	42%
Qualité du code et réalisation	30%
Autre	20%

Démarche

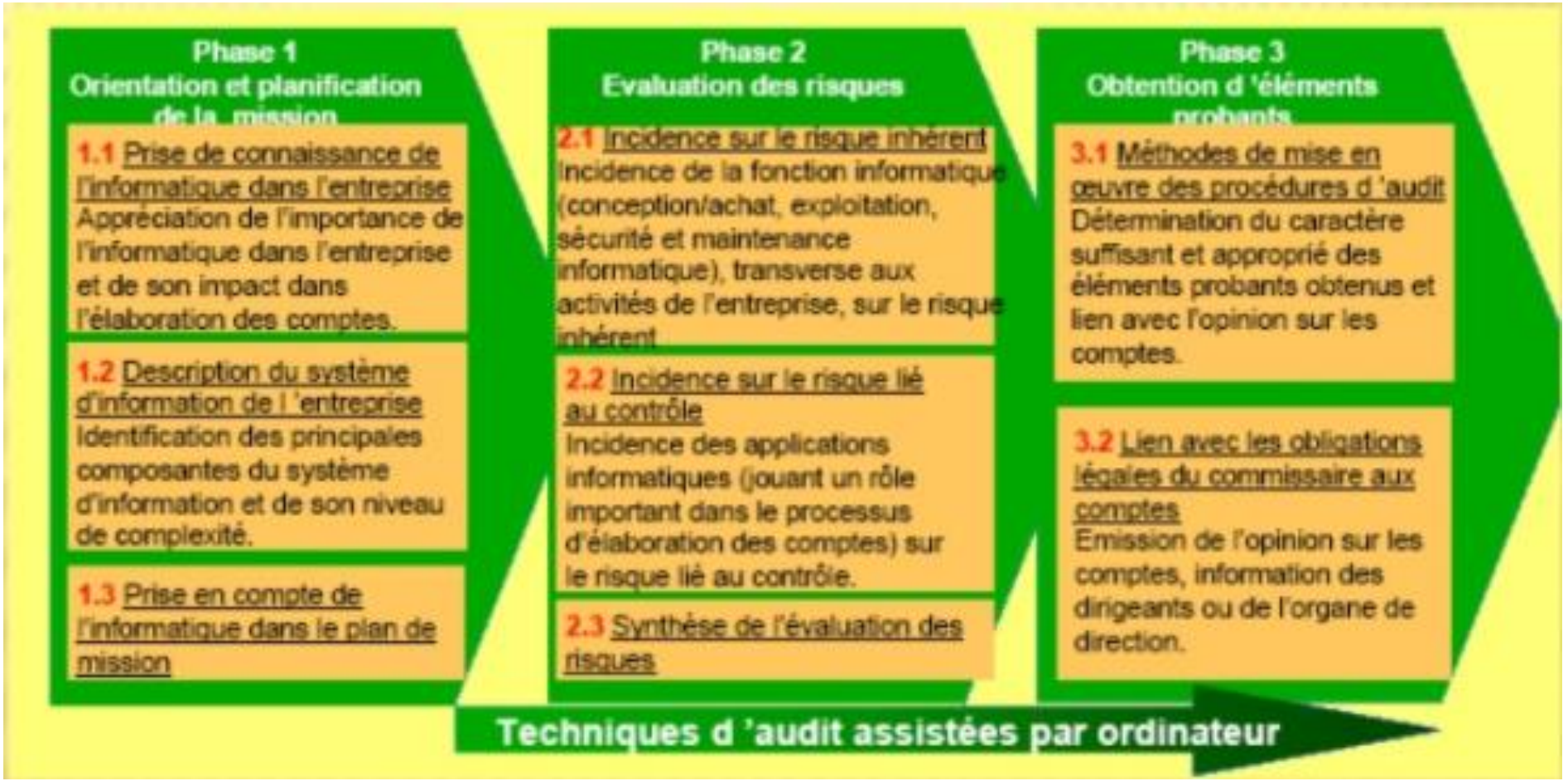
Les auditeurs internes

- Les missions susceptibles d'être confiées à l'auditeur interne ont à priori les mêmes que celles susceptibles d'être confiées à l'auditeur externe

- Cependant l'auditeur interne qui dépend soit de la direction générale soit d'un service d'audit est souvent confronté à un problème de délai (couvrir la demande dans un délai raisonnable)

Démarche

Approche de l’audit en environnement informatique



Conduite de mission

Démarche – la lettre de mission

- Objectifs de la mission
- Périmètre de la mission
- Période d'intervention
- Contraintes à prévoir pour les services audités
- La méthode
- La constitution de l'équipe
- Les documents préparatoires

Conduite de mission

Démarche – le programme de travail

- Structure de l'entreprise concernée
- Domaines fonctionnels
- Applications informatiques
- Matériels et réseaux

Conduite de mission

Démarche – Enquête préalable

- Délimiter les besoins et analyser le SI de l'audité

- Interroger en collaboration avec l'audité les utilisateurs et les entreprises qui participent au fonctionnement actuel du SI

Conduite de mission

Démarche – Rapport d'audit

- Le rapport rédigé doit être clair et non porté sur la technique
- Dans le cas de missions d'expertise, le rapport proposera un plan d'action pour améliorer la performance

Conduite de mission

Démarche – Choisir un auditeur informatique

Trois critères à prendre en considération

- L'indépendance de l'auditeur
- Le professionnel du diagnostic
- Sa capacité à faire des recommandations

Les outils de l'auditeur

Les normes

- ISO 27002

- Généralités: Créée en 2000 (ISO 17799), Renommée en 2005
- Objet: sécurisation de l'information

=> Confidentialité, intégrité, disponibilité

- Caractère facultatif => guide de recommandations
- 4 étapes dans la démarche de sécurisation:
  - Liste des biens sensibles à protéger
  - Nature des menaces
  - Impacts sur le SI
  - Mesures de protection

Les outils de l'auditeur

Les normes

LES NORMES

- ISO 27001
  - Généralités: Créée en 2005
  - Objet: Politique du Management de la Sécurité de l'Information

=> établir un Système de Management de la Sécurité de l'Information :

- Choix des mesures de sécurité
- Protection des actifs

- Utilisation du modèle PDCA

PDCA, ou roue de Deming
doc. Yalta

Les outils de l'auditeur

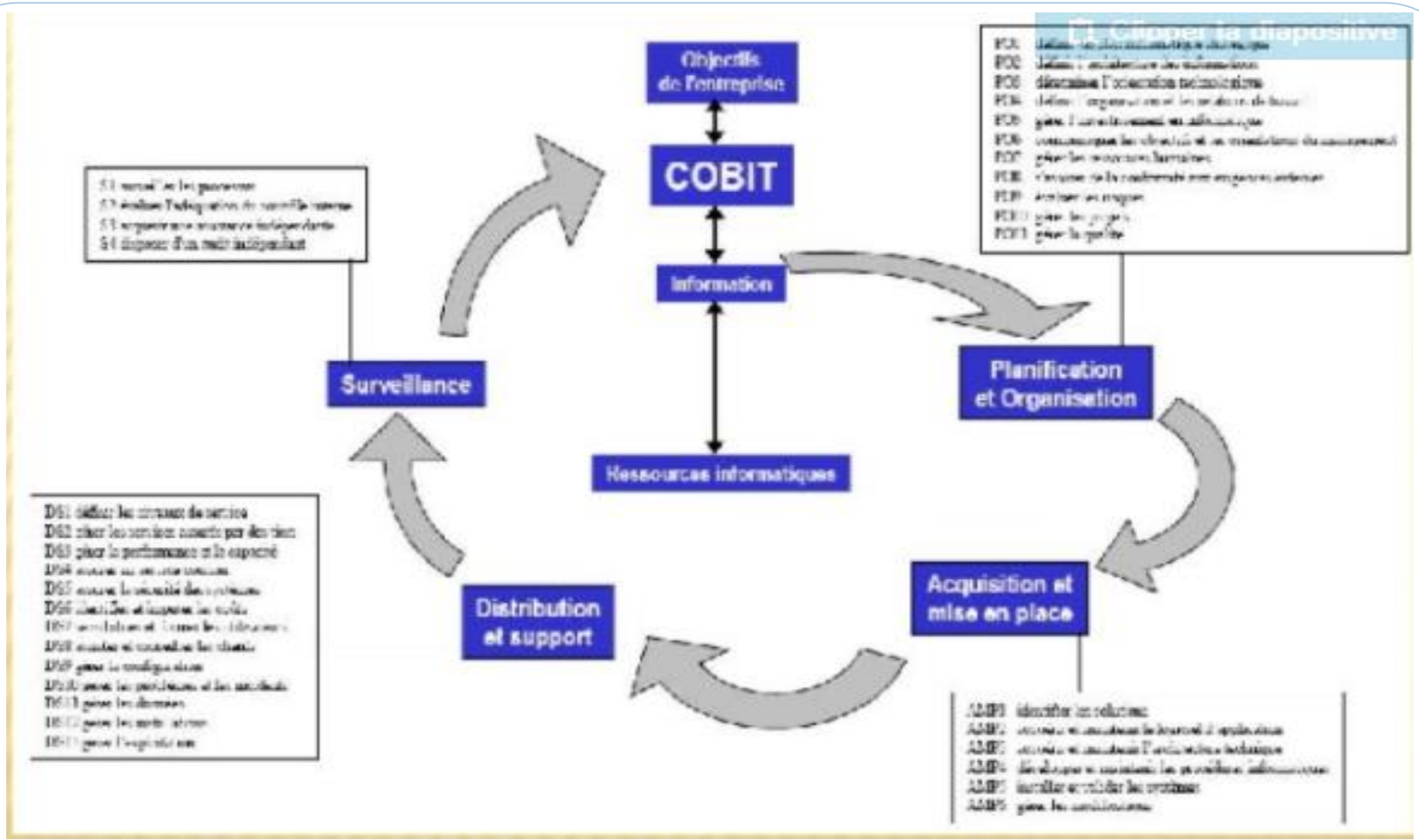
Les méthodes

- COBIT

  - Généralités : Créée en 1996 par l'ISACA / AFAI
  - Structure
  - Contenu:
    - Synthèse
    - Cadre de référence
    - Guide d'audit
    - Guide de management
    - Outils de mise en oeuvre
  - Intérêts:
    - Lien entre les objectifs de l'entreprise et ceux de technologies d'information
    - Intégration des partenaires d'affaires
    - Uniformisation des méthodes de travail
    - Sécurité et contrôle des services informatiques
    - Système de gouvernance de l'entreprise

Les outils de l'auditeur

Les méthodes

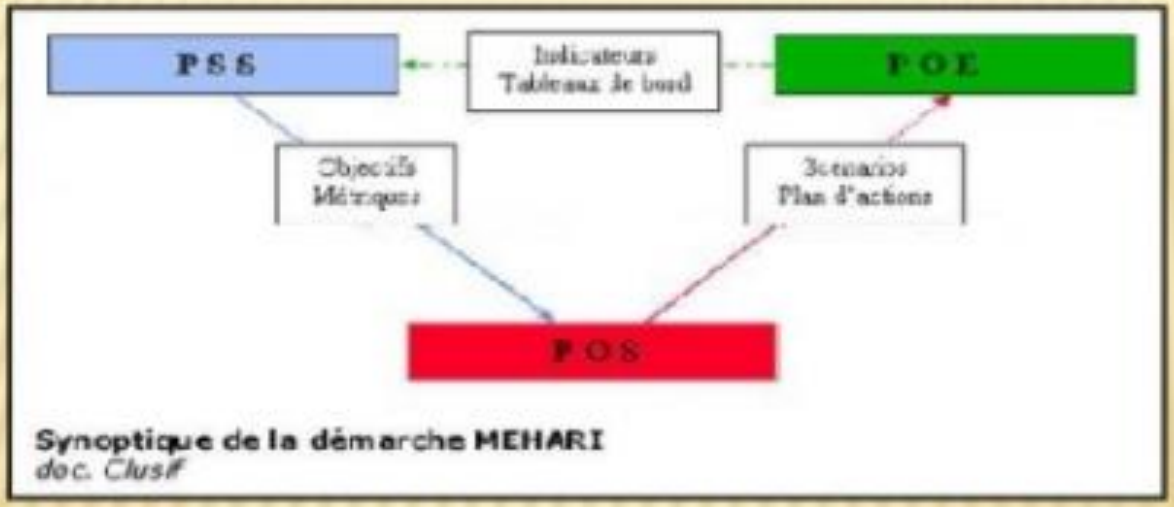


Les outils de l'auditeur

Les méthodes

MEHARI

- Généralités : Créée en 1995 par le CLUSIF, remplaçant MARION
- Structure:



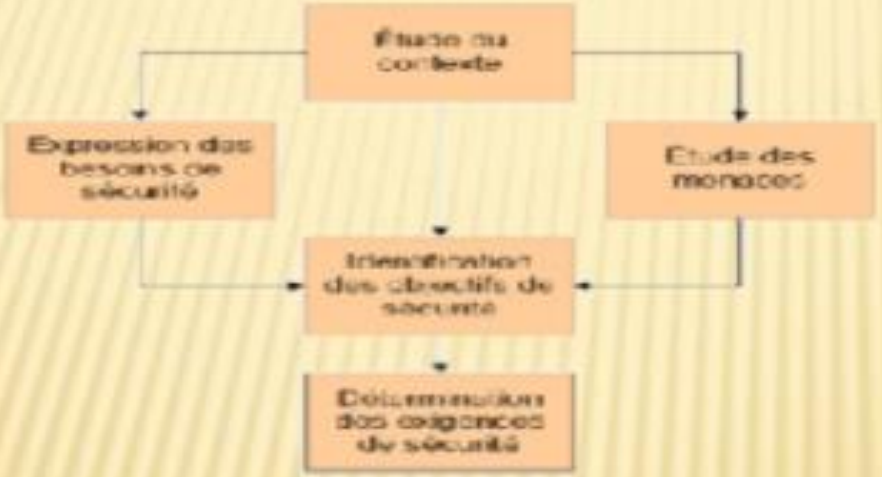
Synoptique de la démarche MEHARI
doc. Clusif

- Intérêts:
  - Appréciation des risques aux regards des objectifs de sécurité
  - Contrôle et gestion de la sécurité

Les outils de l'auditeur

Les méthodes

- EBIOS
  - Généralités : Créée en 1995 par la DCSSI
  - Structure:



  - Intérêts:
    - Construction d'une politique de sécurité basée sur une analyse des risques
    - L'analyse des risques repose sur l'environnement et les vulnérabilités du SI

Les outils de l'auditeur

Les critères de choix

- Origine géographique de la méthode
- Langue
- Existence de logiciels adaptés
- Ancienneté = capacité de recul, témoignages
- Qualité de la documentation
- Facilité d'utilisation
- Compatibilité avec les normes
- Le coût (matériel et humain)
- La popularité, la reconnaissance
- Généralement, combinaison de méthodes lors d'un audit

Guide de bonnes pratiques

Présentation SI – Prise de connaissance du SI

Etablissement		**Période (année)**	
Périmètre	Toutes applications	**Responsable du contrôle**	
Objectif d'audit	L'objectif de cette fiche est de synthétiser les principaux indicateurs permettant une meilleure compréhension du système d'information.		
Procédure	Compléter l'ensemble des informations demandées dans la présente fiche et référencer la documentation.		

Schéma Directeur SIH

Contrôle	Documentation attendue	Pièces justificatives
La stratégie du SIH est définie, partagée avec la direction générale de l'établissement et les métiers. Ce schéma directeur fait l'objet d'une planification pluriannuelle, réajustée en fonction du contexte de l'établissement ou des contraintes règlementaires. La gestion des changements (évolutions fonctionnelles du SI, infrastructure) est alignée sur le schéma directeur.	Schéma directeur Liste des Projets en cours ou à venir	Insérer la référence du document ici

Organigramme de la DSI

Contrôle	Documentation attendue	Pièces justificatives
L'organigramme permet d'identifier les liens fonctionnels, organisationnels et hiérarchiques de la fonction informatique au sein des établissements.	Organigramme de la DSI	Insérer la référence du document ici

Guide de bonnes pratiques

Présentation SI – Prise de connaissance du SI

Revue des applications

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principales applications financières ainsi que les applications métiers significatives.	Tableau de synthèse des applications dûment complété	Voir onglet Applications

Interfaces

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principales interfaces entre les principales applications du SI.	Tableau de synthèse des principales interfaces dûment complété	Voir onglet Interfaces

Cartographie applicative

Contrôle	Documentation attendue	Pièces justificatives
La cartographie applicative est disponible et représente sous forme graphique les principales applications du système d'information (fonctionnalités, système d'exploitation, base de données...) ainsi que les flux de données (type de données, format, fréquence du flux...). Un exemple de cartographie applicative est disponible dans l'onglet "cartographie applicative".	Cartographie applicative	Insérer la référence du document ici

Contrats/mutualisation

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principaux contrats conclus par la DSI ou ayant un impact direct sur la disponibilité des systèmes	Tableau de synthèse des principaux contrats dûment complété	Voir onglet contrats

Guide de bonnes pratiques

Présentation SI – Prise de connaissance du SI

d'informations (contrats de maintenance, contrats de service…)		

Effectifs

Contrôle	Documentation attendue	Pièces justificatives
Document, à jour, synthétisant les effectifs internes et externes agissant pour le compte de la DSI	Tableau de synthèse des effectifs internes et externes	Insérer la référence du document ici

Guide de bonnes pratiques

Présentation SI – Liste des applications

Application	Interlocuteur MOA	Interlocuteur MOE	Fonctionnalités	Hébergemt (lieu si héb.en propre et/ou nom du tiers si applicable)	Hébergement (Local, externalisé)	Type 1- Développements internes 2- Développements par un tiers 3- Progiciel 4- Fichier bureautique	Date de mise en place	Support éditeur (N/A si développement spécifique)	Prestataire pour la maintenance	Date de fin d'utilisation prévue (si applicable)	OS du serveur hébergeant l'application	Base de données	Projet d'évolution	Virtualisé (O/N)	Criticité (1 à 5)
Exemple															
FINANCE +	Contrôle de Gestion	XX	Comptabilité générale Comptabilité analytique	Salle Serveur	Local	Progiciel	11/04/2001	OUI Jusqu'au 31/12/2018	XX Informatique	31/10/2016	Windows Server 2003	SQL Server	Montée de version en v8.2 en Janvier 2013	OUI	1
Applications financières critiques															
Autres applications significatives															

Guide de bonnes pratiques

Présentation SI – Liste des interfaces

ID	Source	Destination	Type de flux	Protocole	Périodicité	Déclenchement	Données échangées	Contrôles

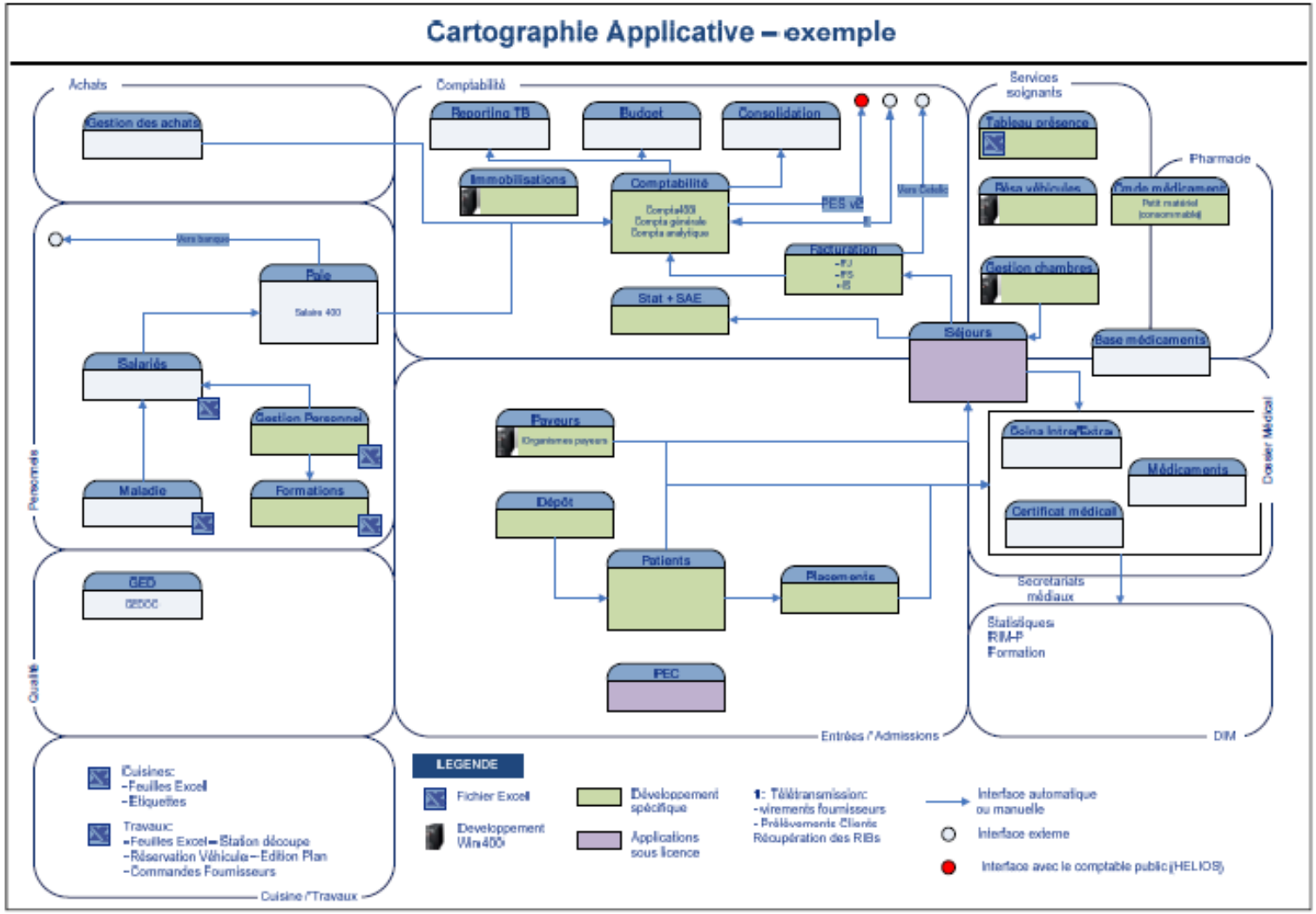
Guide de bonnes pratiques

Présentation SI – Liste des contrats

Partenaire	Objet du contrat	Date d'engagement	Date de fin d'engagement	Indicateurs de niveau de service	....	....	....

Guide de bonnes pratiques

Présentation SI – Exemple de cartographie applicative



Guide de bonnes pratiques

Mécanismes d'identification

Catégorie	Contrôles généraux informatiques	**Domaine**	Identification et authentification
Thème	Mécanismes d'identification		

Objectif

Les applications clés du SIH mettent en œuvre un mécanisme d'identification permettant d'associer un identifiant et un mot de passe à un utilisateur.

Exemples de bonnes pratiques

La politique de sécurité précise que l'ensemble des applications clés du SIH doit mettre en œuvre des mécanismes d'identification permettant d'associer un identifiant et un mot de passe à un utilisateur.

Les revues annuelles des comptes utilisateurs sont validées par les responsables hiérarchiques des utilisateurs.

Documentation à préparer

Liste des utilisateurs des applications, bases de données et systèmes d'exploitation clés.
Documentation justifiant de la nécessité d'utilisation d'un mot de passe pour se connecter aux applications, bases de données et systèmes d'exploitation clés (copies d'écran, extraction de tables de paramétrage...)

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux mécanismes d'identification.
Mise en œuvre	Vérifier le paramétrage des accès aux applications et s'assurer qu'un mot de passe et un identifiant sont requis pour toute connexion.

Guide de bonnes pratiques

Comptes génériques

Catégorie	Contrôles généraux informatiques	**Domaine**	Identification et authentification
Thème	Comptes génériques		

Objectif

Les comptes génériques sont limités et justifiés par les besoins des services.

Exemples de bonnes pratiques

Les comptes génériques doivent être limités au maximum afin de garantir la traçabilité des opérations.

Documentation à préparer

Liste des utilisateurs des applications, bases de données et systèmes d'exploitation clés.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux comptes génériques.
Mise en œuvre	Lister les comptes utilisateurs et contrôler qu'il n'existe pas de comptes génériques ou qu'ils sont limités et justifiés.

Guide de bonnes pratiques

Configuration des mots de passe

Catégorie	Contrôles généraux informatiques	Domaine	Identification et authentification
Thème	Configuration des mots de passe - Applications		

Objectif

Les paramètres de gestion des mots de passe applicatifs sont configurés en accord avec la politique de sécurité de l'établissement et les meilleures pratiques.

Exemples de bonnes pratiques

Les mots de passe utilisés pour l'authentification aux applications clés suivent des règles de gestion et de syntaxe établies par l'établissement, conformes aux meilleures pratiques :
- Obligation de changer le mot de passe lors de la première connexion,
- Modification régulière du mot de passe (durée de vie maximale recommandée <= 90 jours),
- Non trivialité des mots de passe
- Règles de syntaxe :
    - Longueur minimale >= 8 caractères recommandés,
    - Obligation de recourir à des caractères alphanumériques et/ou caractères spéciaux recommandés,
- Historisation des derniers mots de passe (12 recommandé).
- Nombre maximal de tentatives infructueuses de connexion avant blocage du compte (3 recommandé).

Documentation à préparer

Extractions système du paramétrage des contraintes de mot de passe pour les applications du périmètre.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux contraintes de mot de passe.

Guide de bonnes pratiques

Configuration des mots de passe

Mise en œuvre	Recenser le paramétrage des contraintes de mot de passe pour les applications concernées. S'assurer, dans la limite des contraintes techniques, que le paramétrage est conforme à celui décrit dans la politique de sécurité.

Guide de bonnes pratiques

Accès Administrateur

Catégorie	Contrôles généraux informatiques	**Domaine**	Administrateurs
Thème	Accès administrateur		

Objectif

L'attribution des droits d'administration est limitée.

Exemples de bonnes pratiques

L'accès aux comptes d'administrateurs des applications clés, ou ayant des droits étendus, est limité à un nombre restreint d'administrateurs justifiés par les besoins des services.

Documentation à préparer

Liste des administrateurs par application, système et domaine
Liste des employés (RH) avec précision de la fonction de la personne.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux comptes d'administration.
Mise en œuvre	Les utilisateurs ayant des droits d'administrateur ou ayant accès au compte administrateur pour les applications, bases de données et systèmes d'exploitation clés sont justifiés.

Guide de bonnes pratiques

Gestion des droits d’accés

Catégorie	Contrôles généraux informatiques	**Domaine**	Configuration des droits d'accès
Thème	Gestion des règles d'accès		

Objectif

L'attribution des droits d'accès des applications, bases de données et systèmes d'exploitation clés est réalisée conformément aux besoins métiers de l'utilisateur.

Exemples de bonnes pratiques

Des profils ont été définis dans les applications et les systèmes afin d’attribuer des droits d’accès en relation avec les rôles et les responsabilités des utilisateurs.

Documentation à préparer

Extraction des profils utilisateurs et des droits associés
Extraction de la liste des utilisateurs avec indication des profils attribués pour les applications, bases de données et systèmes d'exploitation clés
Liste des employés (RH) avec précision de la fonction de la personne

Eléments à préparer

Formalisation	La politique de sécurité identifie les règles de gestion des droits d'accès.
Mise en œuvre	Les profils d'autorisation dans les applications sont définis en fonction des besoins opérationnels des utilisateurs.

Guide de bonnes pratiques

Matrice de séparation des tâches

Catégorie	Contrôles généraux informatiques	**Domaine**	Configuration des droits d'accès
Thème	Matrice de séparation des tâches		

Objectif
Les principes de séparation des tâches sont respectés pour les applications du périmètre (voir guide partie 2.3.1).

Exemples de bonnes pratiques
Une matrice de séparation des fonctions est définie et validée par la direction générale et est appliquée au niveau informatique.

Documentation à préparer
Matrice de séparation des tâches validée par la DSI Extraction des profils utilisateurs et des droits associés

Eléments à préparer	
Formalisation	La politique de sécurité traite des points relatifs à la séparation des tâches.
Mise en œuvre	Une matrice de séparation des tâches existe et est validée. La matrice a été appliquée dans les systèmes (construction des profils, etc.). Les profils d'autorisation dans les applications correspondent à la matrice de séparation des tâches.

Guide de bonnes pratiques

Revue périodique des accés aux applications

Catégorie	Contrôles généraux informatiques	**Domaine**	Gestion des accès
Thème	Revue périodique des accès aux applications		

Objectif

Les accès aux applications, bases de données et systèmes d'exploitation clés sont régulièrement revus.

Exemples de bonnes pratiques

Une procédure de revue périodique des comptes, des droits d'accès associés et du respect de la séparation des fonctions par les Responsables "Métiers" est en place pour les applications clés. Ces revues impliquent la DSI et les Responsables de services.
La DSI initie la revue en éditant les listes d'utilisateurs avec leurs droits d'accès.
Les Responsables de service revoient ces listes en identifiant les utilisateurs et les droits d'accès injustifiés.
Les responsables applicatifs effectuent dans le système les corrections nécessaires sur les droits d'accès conformément aux commentaires des Responsables de service.

Documentation à préparer

Documents formalisant la revue des droits d'accès
Preuves de la correction des anomalies identifiées
Logs de connexion des applications du périmètre

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux revues périodiques des accès aux applications

Guide de bonnes pratiques

Revue périodique des accés aux applications

Eléments à préparer	
Formalisation	La politique de sécurité traite des points relatifs aux revues périodiques des accès aux applications
Mise en œuvre	La dernière revue des comptes utilisateurs a été formalisée et date de moins d'un an. Elle a été réalisée avec les Responsables des services concernés. Les anomalies détectées ont été corrigées. Si applicable, sélectionner aléatoirement X comptes à supprimer et recenser des preuves que les corrections nécessaires ont été effectuées dans le système, dans des délais raisonnables (par exemple, moins d'une semaine après la revue). Si applicable, vérifier que les logs de connexions infructueuses sont contrôlés et que des actions sont prises afin d'en détecter les origines.