



# AUDIT D'UN SYSTÈME D'INFORMATION

HC-DFR-ASI

VERSION 1.1 - JUILLET 2023



## PLAN DU SUPPORT DE FORMATION

PARTIE	PAGE	PARTIE	PAGE
<b>A. VOCABULAIRE - TERMINOLOGIE</b> <ul style="list-style-type: none"> <li>- Définitions, Sigles et Acronymes</li> <li>- Audit, Diagnostic, Evaluation et Inspection</li> </ul>	6	<b>F. MANAGEMENT « BD-APPLICATIONS »</b> <ul style="list-style-type: none"> <li>- Schéma synoptique des applications</li> <li>- Licences, Correctifs, Maintenances et Supports</li> <li>- Gestion « BD-Applications »</li> </ul>	57
<b>B. AUDIT D'UN SYSTÈME D'INFORMATION</b> <ul style="list-style-type: none"> <li>- Périmètre d'une mission d'audit</li> <li>- Démarche méthodologique</li> <li>- Normes, Référentiels et Circulaires</li> <li>- Fiches indicatives (de travail, de collecte)</li> <li>- Guides d'audit d'un système d'information</li> </ul>	16	<b>G. MANAGEMENT « UTILISATEURS-PARC IT »</b> <ul style="list-style-type: none"> <li>- Assistance et Support technique aux utilisateurs</li> <li>- Parc informatique et péri-informatique</li> <li>- Outils : Support-Gestion du parc</li> </ul>	65
<b>C. GOUVERNANCE D'UN SYSTÈME IT</b> <ul style="list-style-type: none"> <li>- Fonction informatique (IT)</li> <li>- Stratégie et Qualité d'un système IT</li> <li>- Marchés spécifiques au domaine IT</li> <li>- Budgets, Contrats et Redevances IT</li> <li>- Prestataires et Fournisseurs IT</li> <li>- Projets informatiques : Instances, Plannings, PAQ</li> </ul>	24	<b>H. MANAGEMENT « SÉCURITÉ IT »</b> <ul style="list-style-type: none"> <li>- Cadre organisationnel</li> <li>- Sécurité « Systèmes-Serveurs »</li> <li>- Sécurité « Réseaux-Télécoms »</li> <li>- Sécurité « BD-Applications »</li> <li>- Fonctions externalisées</li> </ul>	71
<b>D. MANAGEMENT « SYSTÈMES-SERVEURS »</b> <ul style="list-style-type: none"> <li>- Diagrammes de déploiement</li> <li>- Licences, Correctifs, Maintenances et Supports</li> <li>- Locaux techniques et Energie secondaire</li> <li>- Gestion « Systèmes-Serveurs »</li> </ul>	36	<b>I. RISQUES - MATRICE SWOT - MATURITÉ</b> <ul style="list-style-type: none"> <li>- Risques encourus</li> <li>- Matrice SWOT</li> <li>- Maturité d'un système d'information</li> </ul>	82
<b>E. MANAGEMENT « RÉSEAUX-TÉLÉCOMS »</b> <ul style="list-style-type: none"> <li>- Schéma synoptique et Structure d'un réseau</li> <li>- Licences, Correctifs, Maintenances et Supports</li> <li>- Gestion « Réseaux-Télécoms »</li> </ul>	47	<b>J. RECOMMANDATIONS - PLAN D' ACTIONS</b> <ul style="list-style-type: none"> <li>- Recommandations</li> <li>- Plan d'actions</li> </ul>	93
		<b>FORMATIONS RECOMMANDÉES</b>	101
		<b>ANNEXES</b>	103



## A. Vocabulaire - Terminologie

B. Audit d'un système d'information

C. Gouvernance d'un système IT

D. Management « Systèmes-Serveurs »

E. Management « Réseaux-Télécoms »

F. Management « BD-Applications »

G. Management « Utilisateurs-Parc IT »

H. Management « Sécurité IT »

I. Risques - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

# - MODULE A - VOCABULAIRE - TERMINOLOGIE

## A. VOCABULAIRE-TERMINOLOGIE 1. Définitions, Sigles et Acronymes

**Matériel** : Ensemble des éléments physiques d'un système informatique

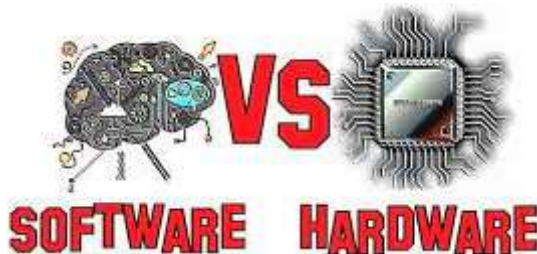
Aussi, appelé « pièce ou composant d'un appareil informatique » ou « partie physique de l'informatique » ou « hardware » (en anglais).

Exemples : ordinateurs, serveurs, dispositifs de stockage de données, etc.

**Logiciel** : Ensemble d'instructions et commandes nécessaires au fonctionnement du matériel informatique et à l'exécution des services attendus

Deux (02) principales catégories de logiciels peuvent être distinguées :

- Logiciels « systèmes » : destinés à effectuer des opérations en rapport le matériel informatique ;
- Logiciels « applicatifs » : destiné à aider les usagers à effectuer une certaine tâche.



**Equipement** : Ensemble du matériel et des logiciels nécessaires pour mener à bien une activité informatique

Exemples

- Ordinateur portable avec un logiciel bureautique, un navigateur internet, un lecteur de musique, etc. ;
- Tablette avec un calculateur, une caméra, un éditeur d'images, un outil de transfert de fichiers, etc.

## A. VOCABULAIRE-TERMINOLOGIE 1. Définitions, Sigles et Acronymes



N°	OS	Domaine d'utilisation
01	<b>DOS</b> <ul style="list-style-type: none"><li>- MS DOS</li><li>- FreeDOS</li></ul>	PC
02	<b>MS Windows</b> <ul style="list-style-type: none"><li>- MS Windows 95, 98, Me, XP, Vista, 7, 8, <b>10</b>, <b>11</b></li><li>- MS Windows Server NT4, 2000, 2003, 2008, 2012, <b>2016</b>, <b>2019</b>, <b>2022</b></li></ul>	PC et Serveurs
03	<b>MacOS</b>	Ordinateurs d'Apple
04	<b>Linux</b> <ul style="list-style-type: none"><li>- RedHat</li><li>- Ubuntu</li><li>- Fedora</li><li>- CentOS</li><li>- Debian</li></ul>	PC et Serveurs
05	<b>Unix</b> <ul style="list-style-type: none"><li>- AIX (IBM)</li><li>- Solaris (Sun)</li><li>- HP-UX (Hewlett-Packard)</li></ul>	Serveurs
06	<b>Android</b> (développé par Google) <ul style="list-style-type: none"><li>- Android x86 (pour PC)</li><li>- Android TV</li></ul>	PC, TV, Tablettes et Smartphones
07	<b>iOS</b> (développé par Apple)	PC, Tablettes et Smartphones

## A. VOCABULAIRE-TERMINOLOGIE 1. Définitions, Sigles et Acronymes

### Composante « Logiciels »

- Logiciels « systèmes » (MS Windows, Unix, iOS, etc.)
- Logiciels « applicatifs » (MS Office, Amplitude, etc.)

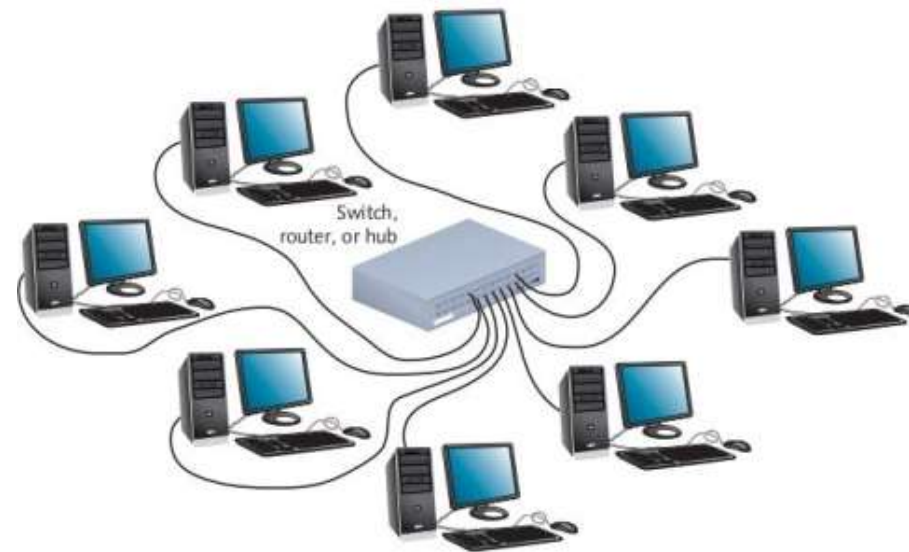
- Interaction avec le matériel
- Sans interaction avec le matériel

### Composante « Matériel »

- Ordinateurs (de bureau, portable) ;
- Serveurs, espaces de stockage, etc. ;
- Câbles, switchs, routeurs, pare-feux, etc. ;
- Energie secondaire (onduleurs, groupes) ;
- Locaux techniques ;
- Etc.

### Composante « Organisation »

- Procédures de travail ;
- Processus d'entreprise ;
- Personnel.



Matériel

Logiciels

**Systeme Informatique**

Matériel

Logiciels

Données

Organisation

**Systeme d'Information**

### **IT : Information Technology (Technologies de l'Information)**

Utilisation d'ordinateurs et d'autres équipements, infrastructures et processus de stockage physique ou de réseau pour créer, traiter, stocker, protéger et échanger toutes les formes de données électroniques.

### **SI : Système Informatique**

Ensemble organisé de ressources (matériel, logiciels, **personnel informatique**) permettant d'acquérir, de stocker, de traiter, de communiquer des **données** pour répondre aux besoins des utilisateurs.

### **SI : Système d'Information**

Ensemble organisé de ressources (matériel, logiciels, **personnel, données, procédures, processus**) permettant d'acquérir, de stocker, de traiter, de communiquer des **informations** sous différentes formes (textes, images, sons, etc.) dans et vers des organisations.

#### Fonctions d'un SI

- (1) Collecte/Acquisition de données
- (2) Mémorisation/Stockage de données
- (3) Traitement/Analyse de données
- (4) Diffusion/Transmission/Communication d'informations

### **Infra. IT : Infrastructure IT**

Composants combinés nécessaires au fonctionnement et à la gestion des services et des environnements informatiques d'une entreprise.

Est aussi appelé « système informatique » ou « architecture informatique ».



### CAS D'ÉTUDE - QUESTIONS

- 1.Exemples et généralités sur les données, informations et connaissances.
- 2.Un excellent auditeur d'un cabinet d'audit IT mène ses missions « en solo » et ne fournit aucun document relatif à son approche méthodologique et ses outils de travail. **Ses connaissances sont-elles facilement transmissibles ?**
- 3.Les connaissances extraites d'un manuel de procédures validé par le Conseil d'administration d'une entreprise **sont-elles tacites ou explicites ? Justifier.**
- 4.Pour Albert EINSTEIN, « **la connaissance s'acquiert par l'expérience, tout le reste n'est qu'une information** ». Vrai ? Faux ? Justifier.
- 5.De quelle composante d'un SI fait partie l'élément ci-dessous :
  - **MS Windows Server 2019 Standard Edition**
  - **HPE ProLiant DL380 Gen11**
  - **Expert en Sécurité des SI**
- 6.Parmi les principales composantes d'un SI, **laquelle est la plus importante** pour le succès d'une organisation commerciale ?
- 7.Quotidiennement, nous interagissons avec divers SI. Faites une **liste desdits SI** tout en donnant une description minimale.
- 8.Proposer des **processus (de pilotage, de support)** utilisés dans votre entreprise.





A.Vocabulaire - Terminologie

**B.Audit d'un système d'information**

C.Gouvernance d'un système IT

D.Management « Systèmes-Serveurs »

E.Management « Réseaux-Télécoms »

F.Management « BD-Applications »

G.Management « Utilisateurs-Parc IT »

H.Management « Sécurité IT »

I.Risques - Matrice SWOT - Maturité

J.Recommandations - Plan d'actions

## **- MODULE B -**

# AUDIT D'UN SYSTÈME D'INFORMATION

### Normes → exigences (internationales)

- **ISO 27001**, exigences en matière de management de la sécurité des systèmes d'information ;
- **ISO 27005**, lignes directrices relatives à la gestion des risques en sécurité de l'information ;
- **PCI DSS** (Payment Card Industry Data Security Standard), normes de sécurité des données applicables à l'industrie des cartes de paiement.



### Référentiels → recommandations, guides, boîtes à outils

- **ITIL** (Information Technology Infrastructure Library), guide de bonnes pratiques dans le domaine de la gestion et la fourniture des services informatiques ;
- **COBIT** (Control Objectives for Information and related Technology), outil de référence pour l'audit des SI, l'évaluation des contrôles associés et la gouvernance des SI.

### Circulaires → exigences dans le milieu bancaire ou financier de l'UMOA

Circulaires pouvant être utilisés dans le cadre d'un audit des SI dans un milieu bancaire ou financier :

- **Circulaire n°01-2017/CB/C** relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA : article 5 (principes généraux de gouvernance) et 7 ;
- **Circulaire n°04-2017/CB/C** relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA : articles n°4, 8, 9 et 12 (systèmes d'information), 22, 31, 33, 37, 39 (gestion de la continuité de l'activité), 40, 41.



### Bonnes pratiques

- **CMMi** (Capability Maturity Model + Integration), cadre méthodologique pour assurer une efficacité organisationnelle globale. Objectif visé : mesurer la capacité d'une structure à mener à bien des projets ou des activités, en termes de délais, de fonctionnalités et de budget.

### **Fiches indicatives de collecte de données**

- Fiche C01 : collecte de données sur un parc informatique ;
- Fiche C02 : collecte de données relatives aux budgets informatiques ;
- Fiche C03 : collecte de données relatives aux formations suivies ou planifiées ;
- Fiche C04 : collecte de données relatives aux systèmes applicatifs ;
- Fiche C05 : collecte de données relatives aux serveurs et systèmes ;
- Fiche C06 : collecte de données relatives aux antivirus et outils de sécurité ;
- Fiche C07 : collecte de données relatives aux liaisons télécoms ;
- Fiche C08 : collecte de données relatives aux équipements réseaux-télécoms ;
- Fiche C09 : collecte de données relatives aux prestataires et fournisseurs.

### **Fiches indicatives de travail**

- Fiche T01 : guide d'entretien ;
- Fiche T02 : liste de la documentation souhaitée pour une mission d'audit d'un SI ;
- Fiche T03 : liste des principaux interlocuteurs (nom, prénoms, email, téléphone, etc.) ;
- Fiche T04 : outil d'analyse des données collectées sur un parc IT ;
- Fiche T05 : document/outil d'évaluation de la maturité d'un système d'information.

### **Fiches indicatives additionnelles**

- Fiche A01 : engagement de confidentialité et de non divulgation.



A.Vocabulaire - Terminologie

B.Audit d'un système d'information

**C.Gouvernance d'un système IT**

D.Management « Systèmes-Serveurs »

E.Management « Réseaux-Télécoms »

F.Management « BD-Applications »

G.Management « Utilisateurs-Parc IT »

H.Management « Sécurité IT »

I.Risques - Matrice SWOT - Maturité

J.Recommandations - Plan d'actions

## - MODULE C - GOUVERNANCE D'UN SYSTÈME IT

#### Principaux documents à collecter

1. Schéma directeur des systèmes d'information (SDSI) ;
2. Politique de la sécurité des systèmes d'information (PSSI) ;
3. Manuel de procédures relatif au système informatique ;
4. Fiches de poste des collaborateurs de l'entité en charge de l'informatique ;
5. Lettres de mission de l'entité en charge de l'informatique ;
6. Dispositifs de mesures ou Tableaux de bord de la fonction informatique ;
7. Rôle et responsabilités du Comité informatique (pour le pilotage du SI) ;
8. Rapports d'audit (interne, externe) portant sur l'informatique ;
9. Mémos, PV de réunion ou rapports internes à l'IT ou au Comité IT ;
10. Historiques, fichiers logs et/ou bases portant sur les incidents ;
11. Liste des prestataires et fournisseurs dans le domaine IT ;
12. Liste du matériel (Serveurs, Réseaux, Télécoms, Energie, etc.) ;
13. Liste des formations et séminaires suivis par les collaborateurs de l'entité IT ;
14. Liste des systèmes applicatifs (applications métier, outils bureautiques, etc.) ;
15. Liste des licences des systèmes logiciels : OS, applications, sécurité, etc. ;
16. Liste des contrats : acquisition, mise en œuvre, assistance, maintenance, etc. ;
17. Documentation sur le PCA-PRA ou le Plan de secours ;
18. Toute autre documentation jugée utile.

La planification budgétaire, l'allocation des ressources budgétaires et la restructuration des budgets sont des **activités pilotées par le Top Management** (voir les Conseils d'Administration ou de Surveillance) des entreprises/organisations.

Les choix stratégiques d'une entreprise/organisation, **notamment les orientations stratégiques et les allocations budgétaires**, sont pilotés par le Top Management.

La gestion des budgets, contrats, redevances et maintenances IT nécessite une revue détaillées et périodiques des aspects suivants :

**- Principales rubriques budgétaires pour un système d'information**

- Acquisition, mise en place et gestion des systèmes applicatifs ;
- Acquisition, mise en place et gestion du matériel : serveurs, réseau, télécoms, etc. ;
- Maintenances, redevances, licences, etc.

**- Principaux contrats pour un système d'information**

- Contrats d'acquisition, mise en place et gestion des systèmes applicatifs ;
- Contrats d'acquisition, mise en place et gestion des équipements ;
- Contrats d'acquisition, mise en place et gestion des équipements réseaux et télécoms ;
- Autres contrats : prestations intellectuelles, formations, séminaires, etc.

**- Principales redevances dans la gestion d'un système d'information**

- Redevances pour les aspects « interconnexions » : FO, VSAT, BLR, Internet, etc.
- Redevances pour les licences logicielles (systèmes d'exploitation, applications métier, etc.) ;
- Redevances pour les maintenances (serveurs, parc informatique, équipements réseaux, etc.).

**La maîtrise des budgets, contrats, redevances  
et maintenances assure une bonne gestion d'un SI.**



### CAS D'ÉTUDE - QUESTIONS

1. Points de vigilance relatifs aux **marchés spécifiques au domaine IT**.
2. Importance de la mise en place d'un **Comité Informatique** dans une entreprise/organisation utilisant les TI.
3. Dispositifs de mesure - **Tableaux de bord de la fonction IT** (pour le Top Management, pour l'entité en charge des TI) : Serveurs, Réseaux, BD-Applications, Licences, Maintenance, etc.
4. **Evaluation périodique des prestataires et fournisseurs IT** : canevas, acteurs impliqués, cadre permanent/périodique d'évaluation, communication avec les prestataires/fournisseurs.
5. **Formation des collaborateurs** d'une entité informatique : management des ressources (RH, Finance), sécurité des SI, compétences en reporting, etc.
6. Mémos, PV de réunion ou rapports internes à l'IT ou au Comité IT.
7. Politique de **gestion des projets informatiques** (au sein de votre entreprise ou organisation).
8. Alignement de la stratégie informatique à la stratégie d'entreprise.



A.Vocabulaire - Terminologie

B.Audit d'un système d'information

C.Gouvernance d'un système IT

**D.Management « Systèmes-Serveurs »**

E.Management « Réseaux-Télécoms »

F.Management « BD-Applications »

G.Management « Utilisateurs-Parc IT »

H.Management « Sécurité IT »

I.Risques - Matrice SWOT - Maturité

J.Recommandations - Plan d'actions

## - MODULE D - MANAGEMENT « SYSTÈMES-SERVEURS »



Un **diagramme de déploiement** est un schéma synoptique permettant de mettre en évidence une partie de l'infrastructure IT. Il permet d'avoir une vue simplifiée et les interrelations entre « matériel », « systèmes » et autres « composants hébergés ».

### **Serveurs**

- Identification des serveurs (physiques, virtuels) et leurs localisations ;
- Echanges sur les serveurs « doublés » pour les besoins de redondance/sécurité ;
- Catégorisation des serveurs identifiés par niveau de criticité ;
- Description des fonctions principales par serveur (physique, virtuel) ;
- Echange sur l'état d'obsolescence des serveurs et des éventuels risques encourus.

### **Systèmes d'exploitation**

- Mise en évidence des systèmes d'exploitation installés par serveur ;
- Echanges sur les versions et correctifs des systèmes d'exploitation.

### **Composants hébergés**

- Identification des applications clés hébergées par serveur ;
- Identification des systèmes de sécurité hébergés par serveur.

### **Diagrammes de déploiement**

- Mise en évidence des interdépendances entre serveurs et composants hébergés ;
- Mise en évidence des matrices de flux entre serveurs ;
- Description des VPN utilisés (par des acteurs internes ou externes).

**Présentation des serveurs, des systèmes et des composants hébergés sous un format facilitant la mise en évidence des insuffisances ou points de vigilance.**

Dans une infrastructure IT, les « licences », les « correctifs », les « contrats de maintenance » et les « contrats de support » sont **à bien surveiller**. Un ou des **tableaux de bord IT spécifiques seront utiles**.

### Licences

- Analyser les besoins en licences sur la base de l'infrastructure « Serveurs-Systèmes » ;
- Faire des acquisitions optimisées **en évitant les prévisions non réalistes** ;
- Être en conformité avec les exigences des contrats de licences ;

**NB** : les **cas de dépassement des quantités acquises** ou de **non-respect du périmètre de la licence** sont constitutifs d'actes de contrefaçon, et exposent leur auteur à des poursuites civiles comme pénales, si un accord n'est pas trouvé avec l'éditeur du logiciel pour régulariser le litige.

### Correctifs

Un correctif est destiné **(1)** à mettre à niveau un logiciel, **(2)** à corriger un problème ou encore à résoudre une vulnérabilité dans celui-ci. Les problèmes logiciels peuvent provenir d'anomalies dans le code ou de failles entraînant des vulnérabilités.

Des dispositions spéciales (**veille technologique, adéquation du support technique, cycle de gestion des correctifs, responsabilisation**, etc.) doivent être prises afin de **systematiser** la mise à jour des correctifs.

### Maintenances et Supports techniques

Les maintenances et les supports techniques portant sur les « Serveurs-Systèmes » doivent faire l'objet d'un suivi adéquat à l'aide d'un tableau de bord.

**Les licences, les correctifs, les maintenances et les supports techniques constituent des postes budgétaires à analyser et à optimiser.**

9. Les serveurs sont-ils sous **garantie, monitorés, ondulés** et bénéficient-ils de sauvegardes systèmes et de mises à jour de sécurité ?
10. Un **plan de secours informatique (PSI)** est-il défini et adapté à l'infrastructure de votre entreprise/organisation ?
11. Des tests du PSI sont-ils **régulièrement effectués**, au moins une (01) fois par an ?
12. Les bandes/disques de sauvegarde de données sont-elles **uniquement** dans les locaux techniques ?
13. Les locaux techniques sont-ils **construits/protégés suivant des normes**, des référentiels ou des bonnes pratiques connus ? Lesquels : pour les normes de construction, pour les normes de protection ?
14. Les **données de monitoring/supervision** des serveurs et des systèmes sont-elles stockées et analysées ?
15. L'environnement des serveurs (local, énergie principale, énergie secondaire, sécurité incendie, contrôle d'accès, surveillance, température, hygrométrie, etc.) est-il bien mis en place et maîtrisé ?
16. Les équipements (serveurs, systèmes, applicatifs) mis en place pour le **PRI (plan de reprise informatique)** disposent-ils d'un plan de maintenance adéquat ? Les correctifs sont-ils régulièrement/périodiquement mis à jour ?



### CAS D'ÉTUDE - QUESTIONS

1. Cas d'étude sur les **licences, correctifs maintenances et supports** d'une infrastructure « Systèmes-Serveurs » :

- Réalisation d'un diagramme de déploiement ;
- Echange sur les licences nécessaires ;
- Echange sur les correctifs ;
- Echange sur les maintenances et supports techniques.

2. Cas d'étude sur les **locaux techniques**

- Identification des locaux techniques ;
- Présentation des composants du local technique principal ;
- Echange sur les composants « serveurs », « onduleurs », « groupes électrogènes », etc.

3. Cas d'étude sur le **VPN**

- Echange sur la mise en place d'un VPN ;
- Echange sur les besoins d'accès extérieurs pour une assistance technique.

4. Utilité d'un diagramme de déploiement pour un auditeur (interne, externe).

5. Le déclenchement d'un PSI ou d'un PRI est-il garanti par l'existence d'un ensemble de serveurs entreposés dans un local distant, **sans interconnexion avec le système principal**, et contenant tous les systèmes, applicatifs et données de l'entreprise/l'organisation ?



- A. Vocabulaire - Terminologie
- B. Audit d'un système d'information
- C. Gouvernance d'un système IT
- D. Management « Systèmes-Serveurs »
- E. Management « Réseaux-Télécoms »**
- F. Management « BD-Applications »
- G. Management « Utilisateurs-Parc IT »
- H. Management « Sécurité IT »
- I. Risques - Matrice SWOT - Maturité
- J. Recommandations - Plan d'actions

## - MODULE E - MANAGEMENT « RÉSEAUX-TÉLÉCOMS »

## E. MANAGEMENT « RÉSEAUX-TÉLÉCOMS » 1. Schéma synoptique et Structure du réseau

Elaborer le schéma d'un réseau d'entreprise nécessite une bonne connaissance des composants et sous-composants dudit réseau : LAN, système d'interconnexion, etc.

### LAN du site principal et WAN

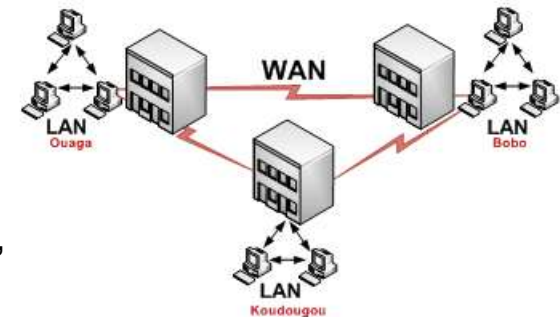
- Identification des principaux équipements du **LAN (Local Area Network : réseau local)** principal ;
- Echanges sur les règles de segmentation du **WAN (Wide Area Network : réseau global/étendu)** ;
- Echange sur les mécanismes de protection des équipements du LAN du site principal.

### LAN des autres sites

- Identification des principaux équipements des LAN des autres sites ;
- Echange sur les mécanismes de protection des équipements des LAN des autres sites.

### Systèmes d'interconnexion

- Identification des systèmes d'interconnexion : FO, BLR, VSAT, abonnement internet, etc. ;
- Mise en évidence des liaisons principales et des liaisons de secours ;
- Mise en évidence des débits pour chaque lien d'interconnexion ;
- Mise en évidence des liaisons avec les partenaires.



### Schéma synoptique et Structure du réseau

Avec les données collectées (matériel réseau, systèmes d'interconnexion, partenaires externes, etc.), un schéma synoptique peut-être établi.

Avec ledit schéma, la structure du réseau peut-être **analysée sous plusieurs angles** :

- Organisation du réseau : architecture physique, segmentation des réseaux, etc. ;
- Extension du réseau et prise en compte des « micro réseaux hors site » (points de service, etc.) ;
- Protection du réseau global.

**Présentation des réseaux et télécoms sous un format facilitant la mise en évidence des insuffisances ou points de vigilance.**

7. Un **invité** (partenaire technique, auditeur externe, etc.) arrive dans votre entreprise/organisation et **souhaite avoir accès à Internet**. Quelle est la démarche à suivre ? Cette démarche est-elle documentée et encadrée ?
8. Une procédure formelle de **création/mise à jour des VPN** existe-t-elle ? Un VPN créé et mis à disposition d'un partenaire externe fait-il l'objet d'un suivi particulier ?
9. Le **plan de câblage** est-il bien documenté ? Cette documentation est-elle uniquement accessible à des personnes autorisées ?
10. Des **indicateurs de capacité** sont-ils périodiquement/régulièrement collectés afin de mesurer la performance du réseau ? Quelle est la périodicité de collecte ? Quels sont les outils utilisés ?
11. Les **accès réseau sont-ils doublés** ? Les accès de secours font-ils l'objet de tests périodiques de bascule ?
12. Un **outil de supervision réseau** est-il mis en place ?
13. Quelle est la **politique d'accès à Internet** ? Des outils de contrôle des périodes de connexion et des personnes autorisées sont-ils utilisés ?
14. Afin d'optimiser la gestion des ressources, des VLAN (Virtual LAN) ont-ils été mis en place ? Le schéma de l'architecture réseau met-il en évidence ces VLAN ? Ledit schéma est-il mis à jour ?





### CAS D'ÉTUDE - QUESTIONS

#### 1. Cas d'étude sur la **conception et mise en place d'un LAN** :

- Listing des principaux composants d'un LAN principal ;
- Analyse des besoins de communication « interne » et « externe » ;
- Analyse des exigences et contraintes : réglementation, limites des opérateurs télécom, etc. ;
- Choix et évaluation du matériel nécessaire pour la mise en place du futur LAN ;
- Choix et évaluation des principaux besoins additionnels (énergie secondaire, sécurité, etc.) ;
- Analyse des besoins en redondance (matériel réseau, énergie, sécurité, etc.) et évaluation ;
- Elaboration du schéma synoptique du futur LAN.

#### 2. Cas d'étude sur la **conception et mise en place d'un WAN** :

- Analyse des besoins en composants pour les LANs secondaires ;
- Analyse des offres et possibilités d'interconnexion avec le site principal ;
- Elaboration du schéma synoptique « modèle » pour les LANs secondaires ;
- Interconnexion des LANs secondaires au LAN principal → WAN.

#### 3. Cas d'étude sur la **sécurisation d'un LAN ou d'un WAN** :

- Mise en place d'une DMZ (DeMilitarized Zone = Zone DéMilitarisée) ;
- Mise en place d'un pare-feu ou firewall ;
- Mise en place d'un serveur proxy.

**NB** : une zone démilitarisée est un **sous-réseau séparé du réseau local et isolé de celui-ci** ainsi que d'Internet par un **pare-feu**. Ce sous-réseau contient les serveurs/ordinateurs étant susceptibles d'être accédés depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

On peut considérer que le **réseau local est une zone de confiance**, tandis qu'**Internet est une zone non maîtrisée/à risque**. Grâce à la DMZ (« **zone tampon** »), le réseau local sera protégé d'Internet, tout en permettant la communication entre les deux (02) zones, mais de **façon contrôlée et filtrée**.





- A. Vocabulaire - Terminologie
- B. Audit d'un système d'information
- C. Gouvernance d'un système IT
- D. Management « Systèmes-Serveurs »
- E. Management « Réseaux-Télécoms »
- F. Management « BD-Applications »**
- G. Management « Utilisateurs-Parc IT »
- H. Management « Sécurité IT »
- I. Risques - Matrice SWOT - Maturité
- J. Recommandations - Plan d'actions

## - MODULE F - MANAGEMENT « BD-APPLICATIONS »

Une **cartographie des applications** est un schéma synoptique permettant de mettre en évidence une partie de l'infrastructure IT et les interrelations entre « bases de données », « applications », « systèmes » et autres « composants IT ».

### Applications clés

- Identification des applications clés et les bases de données associées ;
- Description des applications identifiées et bases de données associées ;
- Prise en compte de l'infrastructure supportant les applications identifiées ;
- Prise en compte des éléments de sécurité : certificat, **système d'habilitations**, etc.
- Mise en évidence des principaux états/listings générés.



### Flux d'informations

- Identification des interfaces d'échanges de données, des référentiels de données, etc. ;
- Qualification des flux d'information : automatique, manuel, semi-automatique, uni ou bi-directionnel ;
- Mise en évidence des principaux fichiers produits ou utilisés par les différentes applications ;

### SI externalisé

- Prise en compte des applications totalement ou partiellement hébergées/gérées par des tiers ;
- Prise en compte des éléments de sécurité : certificat, système d'habilitation, cadres contractuels, etc.

### Schéma synoptique → **Cartographie des applications**

- Mise en évidence des interdépendances entre applications, bases de données et autres composants ;
- Prise en compte de l'infrastructure (serveurs et systèmes notamment).

**Présentation des applications sous un format facilitant la mise en évidence des insuffisances ou points de vigilance.**

9. Un **référentiel unique de données** est-il disponible pour toutes les applications clés de l'entreprise/l'organisation ? Sinon, quel mécanisme permet de maîtriser les échanges de paramètres communs entre les différentes applications ?
10. Des **manuels** (d'utilisation, d'administration, de paramétrage, etc.) existent-ils pour chaque application ? Les utilisateurs et/ou les administrateurs des applications ont-ils suivis des formations sur les applications utilisés/administrés ?
11. La **sauvegarde de données** est-elle effectuée suivant une procédure bien documentée ?
12. Des **tests de restauration** de données sont-ils souvent effectués ? Quelle est la fréquence desdits ou quels sont les événements déclencheurs ?
13. L'administration des bases de données, le développement/la maintenance des applications et l'exploitation informatique sont-ils gérés par la **même sous-entité de l'entité informatique** ? Si oui, quelles sont les dispositions prises afin d'éviter un risque de fraude ou de manipulation non autorisée des données ? Des contrôles périodiques/réguliers sont-ils effectués par le responsable de l'entité informatique ?
14. Un **tableau de bord de gestion** des applications et des bases de données (BD) est-il disponible ? Le temps d'indisponibilité des BD est-il renseigné ? Le nombre d'anomalies (déclarées, en cours de résolution, etc.) de chaque application est-il connu ?



### CAS D'ÉTUDE - QUESTIONS

#### 1. Cas d'étude sur les **fonctions externalisées** :

- Listing des applications, partiellement ou totalement, hébergées à l'extérieur ;
- Listing des certificats et/ou systèmes de sécurité mis en place ;
- Mise en évidence des interactions entre « fonctions externalisées » et « applications in-house ».

#### 2. Cas d'étude sur les **échanges de données inter-applications** :

- Listing des applications les plus utilisées ;
- Présentation des principales fonctionnalités desdites applications ;
- Présentation des principaux fichiers générés ou « consommés » par lesdites applications ;
- Mise en évidence des interactions entre les applications : automatique, manuel, etc.

#### 3. Cas d'étude sur les **licences et correctifs** :

- Listing des applications les plus utilisées ;
- Echange sur les cadres contractuels ;
- Echange sur les mises à jour suite à des « anomalies », « failles de sécurité », « évolutions réglementaires », etc.

#### 4. Cas d'étude sur les maintenances des applicatifs :

- Description du cadre général de maintenance des applications ;
- Description des environnements « tests », « homologation » et « production » ;
- Présentation de la procédure de mise en place de correctifs pour chaque application critique ;
- Echange sur la production documentaire relative aux tests de correctifs avant toute mise en production ;
- Présentation des organes/instances de validation avant toute mise en production.



N°	SGBD	Compléments d'informations
01	<b>SGBD « C/S »</b> <ul style="list-style-type: none"> <li>- Oracle Database</li> <li>- MS SQL Server</li> <li>- PostgreSQL</li> <li>- MySQL</li> <li>- MariaDB</li> <li>- DB2</li> </ul>	<b>SGBD</b> (Système gestion de bases de données) <b>ou DBMS</b> (Database management system).  Deux (02) avantages fondamentaux : <b>(1)</b> minimiser le trafic des données sur un réseau, <b>(2)</b> assurer une plus grande intégrité lors du traitement des données
02	<b>SGBD « fichier »</b> <ul style="list-style-type: none"> <li>- MS Access</li> <li>- Paradox</li> <li>- FoxPro</li> <li>- FileMaker Pro</li> </ul>	Système à base de fichiers : chaque poste de travail <b>traite localement les données</b> .  Dans un <b>SGBD C/S</b> , tous les traitements sont effectués sur le serveur par le biais de requêtes.
03	<b>SGBD « embarqué »</b> <ul style="list-style-type: none"> <li>- SQLite</li> <li>- Derby (JavaDB)</li> <li>- dBase</li> <li>- MaxDB</li> </ul>	<b>SGBD embarqué (embedded)</b> est un SGBD incorporé directement dans une application.
<b>Axes d'approfondissement</b>		
<ul style="list-style-type: none"> <li>- SGBD libres</li> <li>- SGBD open source</li> </ul>	<ul style="list-style-type: none"> <li>- SGBD gratuits</li> <li>- SGBD commerciaux</li> </ul>	<ul style="list-style-type: none"> <li>- SGBD multi-plateformes</li> </ul>



- A. Vocabulaire - Terminologie
- B. Audit d'un système d'information
- C. Gouvernance d'un système IT
- D. Management « Systèmes-Serveurs »
- E. Management « Réseaux-Télécoms »
- F. Management « BD-Applications »
- G. Management « Utilisateurs-Parc IT »**
- H. Management « Sécurité IT »
- I. Risques - Matrice SWOT - Maturité
- J. Recommandations - Plan d'actions

## - MODULE G - MANAGEMENT « UTILISATEURS-PARC IT »

La **bonne gestion d'un parc informatique** nécessite les actions suivantes :

- Recenser tous les éléments du parc IT ;
- Schématiser les interactions entre les différents actifs du parc IT ;
- Gérer les prestataires externes (opérateur Internet, supports techniques, etc.) ;
- Assurer l'administration des serveurs ;
- Prévoir des maintenances régulières du parc IT ;
- Analyser les besoins en renouvellement de matériel selon des cycles de vie prédéfinis ;
- S'assurer de la formation des utilisateurs internes à l'utilisation des équipements ;
- S'assurer de la bonne compréhension des règles minimales de bonne utilisation des équipements informatique ;
- Etc.

**Quelques outils de gestion de parc IT, d'assistance et de support**

- **GLPI** (inventaires des actifs, gestion des besoins d'assistance, etc.) ;
- **OCS Inventory NG** (inventaire des actifs, gestion des déploiements, etc.).
- **JIRA** (gestion des tickets d'assistance, gestion des incidents, etc.) ;
- **SolarWinds**.



### CAS D'ÉTUDE - QUESTIONS

#### 1. Cas d'étude sur la **collecte de données sur un parc**

Collecte de données sur un parc informatique à l'aide des fiches indicatives.

Le matériel didactique ou le matériel des participants peut faire office de parc informatique.

#### 2. Cas d'étude « **Analyse des données collectées** »

Analyse des données collectées sur le parc informatique ;

Etablissement d'une liste des principales constatations sur le parc informatique.

#### 3. Cas d'étude « **Tableaux de bord** »

Echange sur des canevas de tableaux de bord pour une meilleure gestion d'un parc informatique.

#### 4. Cas d'étude « **Assistance et Support technique** »

Analyse de la gestion des outils et applications métier : existence d'un outil d'assistance et de support technique, extraction de données, etc. ;

Echange sur les mémos et rapports relatifs à l'assistance et au support technique.

#### 5. Cas d'étude « **Bonnes pratiques pour la gestion d'un parc IT** »

Aspects « Contractuels », « Evaluation des acteurs », « Collecte des besoins des utilisateurs », « Procédures de renouvellement d'un parc IT ».





- A. Vocabulaire - Terminologie
- B. Audit d'un système d'information
- C. Gouvernance d'un système IT
- D. Management « Systèmes-Serveurs »
- E. Management « Réseaux-Télécoms »
- F. Management « BD-Applications »
- G. Management « Utilisateurs-Parc IT »
- H. Management « Sécurité IT »**
- I. Risques - Matrice SWOT - Maturité
- J. Recommandations - Plan d'actions

## - MODULE H - MANAGEMENT « SÉCURITÉ IT »

Le cadre organisationnel de la sécurité porte sur les **politiques/procédures**, les **équipes dédiées**, les **mesures prises**, la **formation et sensibilisation** des utilisateurs, le mécanisme de **gestion des habilitations** et des **incidents de sécurité**, etc.

### QUESTIONNAIRE

1. Existe-t-il une **politique de sécurité des systèmes d'information (PSSI)** formalisée, validée par l'instance de gouvernance, avec une implication de la Direction Générale ? Une revue régulière de la PSSI est-elle effectuée afin de vérifier son adéquation avec les évolutions des activités de l'entreprise/l'organisation, les changements technologiques et/ou l'historique des incidents ?
2. Une **structure** ou un **personne dédiée à la sécurité des systèmes d'information (Comité sécurité, RSSI)** est-il en place ? Quel est son niveau de hiérarchie ? Son activité fait-il l'objet d'une revue périodique ?
3. Des **mesures de protection des données** (clause de confidentialité, charte d'utilisation du SI, masquage de données, données de test, etc.) sont-elles établies et suivies ? Lesdites mesures sont-elles systématiquement acceptées ou imposées aux tiers (fournisseurs, prestataires, auditeurs externes, etc.) ? Les exigences de sécurité sont-elles prises en compte dans les conditions contractuelles ?

12. Les exigences normatives, réglementaires ou de conformité sont-elles prises en compte dans les procédures et politiques de sécurité ?
13. La sécurité du SI a-t-elle déjà fait l'objet d'un audit par une entité externe spécialisée ? Cette démarche est-elle régulièrement renouvelée ?
14. Un **PCA-PRA** (Plan de Continuité d'Activités - Plan de Reprise d'Activités) est-il bien défini, mis en place, régulièrement/périodiquement testé ?
15. Le RSSI est-il responsable de la gestion de la PSSI ?

En raison du **besoin conservation et de protection des données**, la sécurité des « Systèmes-Serveurs » est une priorité dans les entreprises/organisations.

### QUESTIONNAIRE

1. Les serveurs, et autres matériels critiques, sont-ils bien logés dans des **locaux normés et sécurisés** ?
2. Existe-t-il des procédures/politiques pour autoriser l'**intégration de nouveaux serveurs ou systèmes logiciels** dans l'infrastructure existante ?
3. Les **accès internes au SI** sont-ils contrôlés et régulièrement ajustés ?
4. Les  **mises à jour « Systèmes-Serveurs »** sont-ils régulièrement/périodiquement effectuées et documentées ? Une stratégie appropriée est-elle définie ?
5. Une **solution antivirale**, avec une gestion et une supervision centralisée, est-elle mise en place ? Un déploiement généralisé par le biais d'une console de gestion est-il possible ?
6. Les ordinateurs disposent-ils d'un **antivirus régulièrement mis à jour** ? Les systèmes d'exploitation sont-ils régulièrement mis à jour ?
7. Le RSSI supervise-t-il la sécurité orienté « Systèmes-Serveurs » ?
8. Le RSSI et/ou l'administrateur est-il **abonné aux lettres d'informations** sur la sécurité « Systèmes-Serveurs » ?

**QUESTIONNAIRE**

1. Les **accès distants ou externes** ou les échanges avec les partenaires sont-ils contrôlés (avec une authentification forte), chiffrés et régulièrement ajustés ?
2. Les mises à jour des équipements « Réseaux-Télécoms » sont-ils régulièrement / périodiquement effectuées et documentées ? Une stratégie appropriée est-elle définie ?
3. En terme de connexion internet, un **dispositif capable de filtrer les URL visités** (proxy, firewall, etc.) existe-t-il dans le SI ?
4. Le SI dispose-t-il d'un **équipement** ou des équipements **capable(s) de faire de la détection** « contre les intrusions », « anti-malware », « applicative » ?
5. Une **zone cloisonnée appelée « DMZ »** est-elle en place afin d'isoler les serveurs publiés sur internet du réseau global ?
7. Un filtre IPS strict est-il en place sur le trafic entrant ? Un WAF (Web Application Firewall) est-il en place ?
8. Les **ports ouverts sur internet** sont-ils identifiés et limités au strict nécessaire ?
9. Existe-t-il un **système de cloisonnement ou des règles de filtrage fines** entre différents groupes d'utilisateurs, entre les utilisateurs et les serveurs métiers, entre les groupes de serveurs métiers ou encore entre les différents sites ?

L'**externalisation (ou outsourcing)** est une stratégie d'entreprise qui consiste à confier la réalisation de certaines activités à un prestataire externe (reconnu expert dans son domaine).

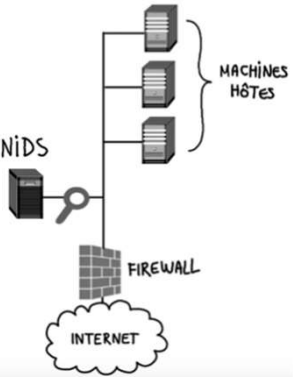
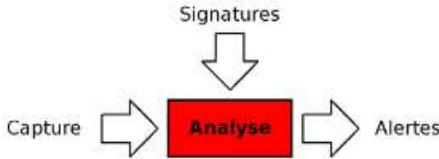
Pour le domaine IT, l'externalisation peut porter sur :

- les données (en utilisation, sauvegardées) ;
- les systèmes et outils de développement ;
- le matériel « Serveurs » et « Réseaux » ;
- les systèmes applicatifs.

### **QUESTIONNAIRE**

1. Une **partie du SI** est-elle logée **chez des partenaires** ou gérée par des entités externes à l'entreprise ?
2. Des procédures/politiques sont-elles mises en place pour **maîtriser la gestion des fonctions externalisées** ?
3. Le RSSI et/ou le Comité IT (s'il en existe) supervise-t-il les fonctions externalisées de l'entreprise/l'organisation ?
4. Des **tableaux de bord** sont-ils mis en place afin de maîtriser les fonctions externalisées ? Des **mémos ou rapports** sont-ils régulièrement/périodiquement produits pour le Top Management ?



N°	Outil	Informations complémentaires
01	<p><b>SIEM</b></p> <ul style="list-style-type: none"> <li>- Splunk</li> <li>- Fusion SIEM</li> <li>- Elastic Security</li> <li>- IBM Qradar</li> <li>- Varonis</li> </ul>	<p><b>SIEM = Security Event management</b></p> <p><b>SIEM = SIM</b> (gestion des informations de sécurité) + <b>SEM</b> (gestion des évènements de sécurité). Terme dans le domaine de la cybersécurité où les services et produits logiciels combinent deux (02) systèmes (SIM, SEM).</p> <p>Un <b>système SEM</b> centralise le <b>stockage</b> et l'<b>interprétation des logs</b>, permet une <b>analyse en quasi-temps réel</b> et <b>détecter les menaces</b> avant qu'elles ne perturbent leurs activités.</p>
02	<p><b>IDS / IPS</b></p> <ul style="list-style-type: none"> <li>- Check Point (IDS)</li> <li>- Tipping Point (IPS)</li> <li>- Tripwire (IDS)</li> <li>- FireEye (IPS)</li> <li>- Juniper (IPS)</li> </ul> 	<p><b>IDS = Intrusion detection system / IPS : Intrusion prevention system</b></p> <p>Les systèmes de <b>détection d'intrusion (IDS)</b> et de <b>prévention d'intrusion (IPS)</b> surveillent un réseau en permanence afin d'<b>identifier les incidents potentiels</b>.</p> <p>Ils consignent les informations afférentes dans des journaux, résolvent les incidents et les signalent aux administrateurs chargés de la sécurité.</p>  <p>Un NIDS (IDS réseau) se découpe en trois (03) grandes parties : la <b>capture</b>, les <b>signatures</b> et les <b>alertes</b>.</p>



- A. Vocabulaire - Terminologie
- B. Audit d'un système d'information
- C. Gouvernance d'un système IT
- D. Management « Systèmes-Serveurs »
- E. Management « Réseaux-Télécoms »
- F. Management « BD-Applications »
- G. Management « Utilisateurs-Parc IT »
- H. Management « Sécurité IT »
- I. Risques - Matrice SWOT - Maturité**
- J. Recommandations - Plan d'actions

## - MODULE I - RISQUES - MATRICE SWOT - MATURITÉ



Le référentiel **COBIT** et les normes **ISO 27005** (Gestion des risques en sécurité de l'information), **ISO 31000** (Management du risque - Lignes directrices) et **ISO 22301** (Management de la continuité d'activité) sont de **bons outils de travail dans le domaine de la gestion des risques**.

Ci-dessous, quelques **exemples de risques** :

#### - Risques « **Gouvernance des SI** »

- Stratégie informatique non alignée sur la stratégie de l'entreprise/l'organisation ;
- Evolution du système d'information en déphasage avec la stratégie métier ;
- Forte dépendance vis-à-vis des prestataires et fournisseurs externes ;
- Procédures de gestion formalisées mais non appliquées.

#### - Risques « **BD-Applications** »

- Anomalies majeurs non détectées en temps opportun ;
- Incertitude sur la qualité et l'exhaustivité des sauvegardes effectuées ;
- Perte de données sensibles en cas de sinistre ou incident majeur ;
- Accès non autorisé aux données par usurpation d'un compte utilisateur.

#### - Risques « **Systèmes-Serveurs** »

- Indisponibilité prolongée des serveurs de production ;
- Changements de configuration système non autorisés ;
- Incapacité à rétablir des services et systèmes critiques en temps opportun.

#### - Risques « **Réseaux-Télécoms** »

- Incapacité à garantir une bonne qualité du réseau ;
- Interruption d'activité par suite d'une défaillance du cœur du réseau.

# I. RISQUES - MATRICE SWOT - MATURITÉ

## 1. Risques encourus

N°	Risque identifié/potentiel	Mesures d'atténuation et/ou Réponse
01	Stratégie informatique non alignée sur la stratégie de l'entreprise/l'organisation	<ul style="list-style-type: none"> <li>- Mise en place d'un schéma directeur des SI (SDSI)</li> <li>- Planification, exécution et suivi des projets identifiés dans le SDSI</li> </ul>
02	Incertitude sur la qualité et l'exhaustivité des sauvegardes effectuées	<ul style="list-style-type: none"> <li>- Mise en place de procédures adéquates de sauvegarde et de restauration de données</li> <li>- Respect des procédures de restauration de données</li> </ul>
03	Indisponibilité prolongée des serveurs de production	<ul style="list-style-type: none"> <li>- Suivi régulier et traitement des incidents et problèmes remontés</li> <li>- Suivi régulier et traitement adéquat des plans de maintenance des serveurs de production</li> </ul>
04	Forte dépendance vis-à-vis des prestataires et fournisseurs externes	<ul style="list-style-type: none"> <li>- Faible implication des collaborateurs en charge de l'IT</li> <li>- Respect des plans de formation des collaborateurs en charge du SI</li> </ul>
05	Evolution du système d'information en déphasage avec la stratégie métier ;	<ul style="list-style-type: none"> <li>- Amélioration de la coordination entre les équipes en charge de l'IT et celles métier</li> <li>- Mise en place de processus adéquats de gestion de projets impliquant des acteurs (IT, métier)</li> </ul>
...	...	...

# I. RISQUES - MATRICE SWOT - MATURITÉ 3. Maturité d'un SI

		Faible	Acceptable	Maîtrisé	Optimisé
<b>Gouvernance des systèmes d'information</b>	Organisation de la fonction informatique		■		
	Formation et gestion des compétences		■		
	Séparation des fonctions	■			
	Procédures informatiques		■		
	Sécurité informatique		■		
	Outils de surveillance et de pilotage	■			
<b>Applications et données</b>	Couverture fonctionnelle des applications		■		
	Confidentialité des données		■		
	Fiabilité des données	■			
	Traçabilité des données		■		
	Sécurité des applications		■		
	Sécurité des bases de données		■		
<b>Infrastructures techniques</b> (systèmes, serveurs, réseaux, télécoms)	Etat/gestion des locaux techniques	■			
	Etat/gestion du parc informatique	■			
	Gestion des systèmes serveur	■			
	Gestion des réseaux (LAN, WAN)	■			
	Exploitation et maintenance	■			
	Sécurité des infrastructures techniques	■			

Situation cible à envisager dans 3 ans

Evaluation de la maturité d'un « **SI exemple** »



- A. Vocabulaire - Terminologie
- B. Audit d'un système d'information
- C. Gouvernance d'un système IT
- D. Management « Systèmes-Serveurs »
- E. Management « Réseaux-Télécoms »
- F. Management « BD-Applications »
- G. Management « Utilisateurs-Parc IT »
- H. Management « Sécurité IT »
- I. Risques - Matrice SWOT - Maturité
- J. Recommandations - Plan d'actions**

## - MODULE J - RECOMMANDATIONS - PLAN D' ACTIONS

## J. RECOMMANDATIONS - PLAN D' ACTIONS 2. Plan d'actions

### PLAN D' ACTIONS À MOYEN TERME (période comprise entre 1 et 2 ans)

N°	Action	Acteur(s)	Date début	Date fin	Coût estimé
01					
02					
03					



### **INFORMATIQUE**

1. Initiation aux bases de données pour un non initié (2j)
2. Initiation aux réseaux et télécoms pour un non initié (2j)
3. Initiation aux systèmes et serveurs pour un non initié (2j)

### **MONÉTIQUE**

1. Initiation à la monétique (2j)
2. Risques et fraudes monétiques (1j)
3. Audit d'un système monétique (3j)

### **SYSTÈMES D'INFORMATION**

1. Elaboration d'un tableau de bord de gestion SI (3j)
2. Elaboration d'une cartographie de risques SI (2j)

### **GOVERNANCE D'ENTREPRISE**

1. Introduction à la démarche qualité (2j)
2. Introduction à la continuité et reprise d'activité (PCA-PRA) (1j)

## ORGANISATION - DOCUMENTATION IT

### ORGANISATION

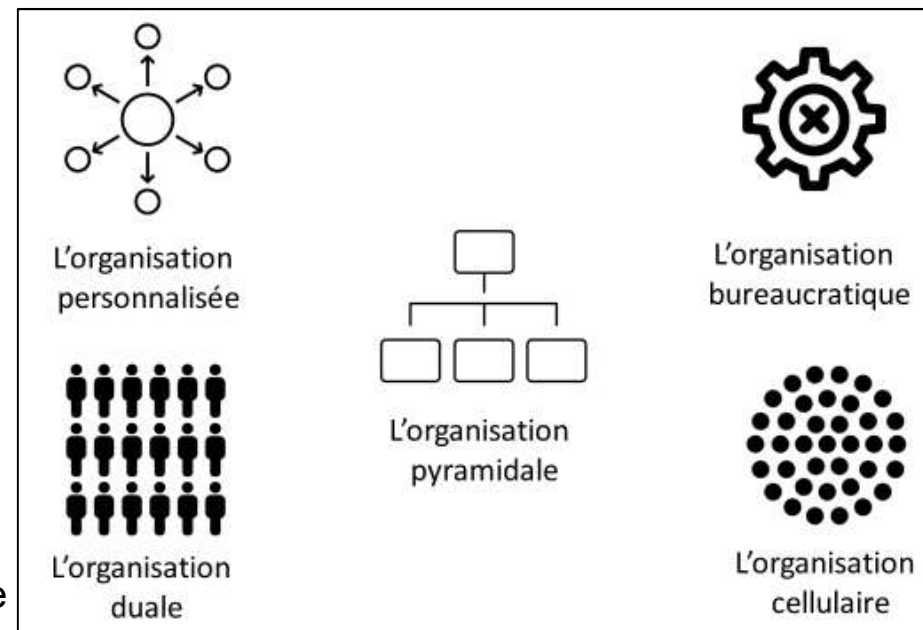
- Structure qui coordonne l'activité des individus pour les rendre capables de coopération en vue de réaliser un objectif commun
- Exemples : entreprises, administrations, associations, etc.

### ENTREPRISE

- Toute entreprise est une organisation
- **Unité économique et juridique** produisant des biens et services destinés à être vendus sur un marché afin de réaliser des bénéfices

### POLITIQUE INFORMATIQUE VS PROCÉDURE

- Stratégie visant à améliorer/optimiser les services informatiques d'une organisation
- Matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures
- Définit l'ensemble des **principes généraux** tandis qu'une procédure indique comment mettre en œuvre ces principes
- Rédigée sous la forme d'**énoncés** ou de **règles**
- Procédure : **instructions** à suivre selon un ordre logique et des étapes déterminées



## CONTINUITÉ D'ACTIVITÉ - SECOURS IT

### PCA : PLAN DE CONTINUITÉ D'ACTIVITÉ

- Vise le **maintien de l'activité** de l'entreprise pendant un sinistre
- Prise en compte des aspects « opérationnel » et « informatique »
- Comprend un **PGC** (Plan de gestion de crise), un **PCC** (Plan de communication de crise), un **PCI** (Plan de continuité informatique), un **PCO** (Plan de continuité opérationnelle), etc.

### PCI : PLAN DE CONTINUITÉ INFORMATIQUE

- Vise le **maintien de l'accès à l'infrastructure informatique** de l'entreprise pendant un sinistre
- Prise en compte des aspects « informatique » uniquement

### PRA : PLAN DE REPRISE D'ACTIVITÉ

- Se concentre sur la **restauration de l'activité** après un sinistre

### PRI : PLAN DE REPRISE INFORMATIQUE

- Se concentre sur la **restauration de l'accès à l'infrastructure informatique** après un sinistre

### PRINCIPALES ÉTAPES NÉCESSAIRES À LA MISE EN PLACE D'UN PCA/PRA

- Etape 1 : Prise en main par la Direction Générale
- Etape 2 : Identification risques majeurs de l'activité
- Etape 3 : Identification des processus et ressources critiques
- Etape 4 : Choix majeurs relatifs à la mise en place du PCA/PRA
- Etape 5 : Conduite de tests réguliers et documentation
- Etape 6 : Mise à jour constante du PCA/PRA