HOBUX consulting

AUDIT
D'UN SYSTÈME D'INFORMATION

HC-DFR-ASI

VERSION 2.0 - SEPTEMBRE 2023

CONTENU DE LA FORMATION

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE A -

VOCABULAIRE - TERMINOLOGIE

1 Organiser un système d'information

- Fonction IT
- Stratégie IT
- Budgets IT
- Projets IT
- **Externalisation**
- Etc.

L'organisation doit porter sur

2 Mettre en place et Maintenir un système d'information
(Acquérir, Mettre en place, Maintenir, etc.)

- Systèmes et Serveurs
- Réseaux et Télécoms
- BD et Applications
- Parc microinformatique
- Locaux techniques
- Energie secondaire
- Etc.

Les mesures de sécurité porte sur

3 Sécuriser un système d'information

- Risques IT
- Protection des actifs
- Dispositifs nomades
- Plan de reprise (PR)
- Plan de continuité (PC)
- Etc.

Donnée

Une donnée est un élément **brut** (**primaire, non traité, non transformée, etc.**). C'est un **symbole**. C'est le résultat direct d'une mesure. **Sans contexte, elle n'a pas de sens**. Elle n'appelle pas à l'action. Elle n'apporte rien si elle n'est pas transformée en information et ensuite assimilée,

La donnée est le plus bas niveau dans le processus de transformation vers la connaissance.
Elle peut-être collectée par un outil, par une personne ou juste récupérée via une source externe.

Information

Une information est une donnée à laquelle un sens (ou une interprétation) a été ajoutée.
Mise en contexte d'une donnée. C'est un ensemble de données intelligible ou augmenté d'un sens.
Grâce à une analyse ou transformation ou mise en contexte, une donnée peut devenir une information utile, pertinente, exploitable, fiable.

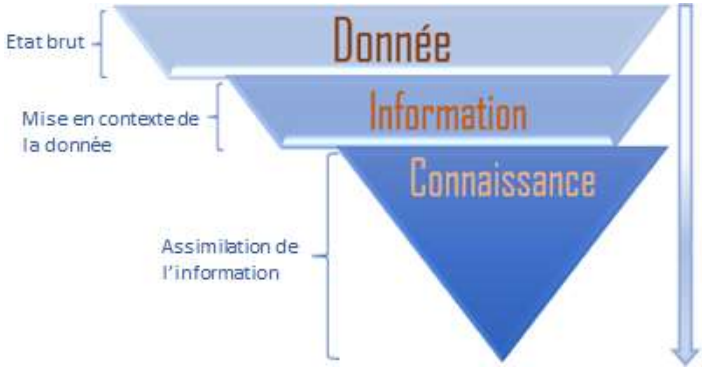
Connaissance

Lorsqu'elle est comprise et assimilée, l'information produit de la connaissance (qui permet de prendre de décision ou poser des actes).

Une connaissance est donc l'appropriation ou l'assimilation d'une information.

On distingue **deux (02) grandes classes** de connaissance :
- Connaissance **tacite** (détenue par les individus) ;
- Connaissance **explicite** (formalisée, normalisée).

Pour Albert EINSTEIN, « **la connaissance s'acquiert par l'expérience, tout le reste n'est qu'une information** ».



CAS D'ÉTUDE - QUESTIONS

1. Echanges sur les données et informations :
   - **Mot « Protocole »**
   - **Lettre « A » et Code « A »**
   - **Mots « Boulanger », « boulanger » et « BOULANGER »**
   - **Nombre « 25 » (degré ? km ? km/h ? FCFA ?)**

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** ? Quotidiennement, nous interagissons avec divers SI. Faites une **liste desdits SI** avec une description minimale.

Sécurité → Accidentel, Involontaire

Concerne, prévient les risques et conséquences d'un évènement accidentel ou involontaire.

Ensemble des mesures déployées pour prévenir pour protéger les biens des **accidents et catastrophes** causées naturellement tels les incendies, les inondations, la mauvaise protection des données et des infrastructures (qui peuvent causer des failles de sécurité), etc..

Sûreté → Intention malveillante, Volontaire, Intention de nuire

Permet d'anticiper, de détecter et de protéger contre les menaces ou **actes volontaires** par l'association de moyens humaines, de solutions techniques.

Ensemble des mesures déployées pour prévenir les **actes de malveillances humaines**, pour protéger les biens et les personnes de leurs conséquences telles les vols ou encore les attentats..

EN RÉSUMÉ

Généralement, il y a une confusion entre les termes « Sûreté » et « Sécurité ».
Aussi, la notion de « Sécurité » embarque généralement celle de « Sûreté ».

Piliers de la sécurité de l'information (piliers « ACID » + autres)

- Confidentialité : rendre les données inintelligibles à d'autres personnes (→ Protection, Masquage) ;
- Intégrité : garantir que les données n'ont pas été falsifiées (→ Chiffrement, Signature, etc.) ;
- Disponibilité : maintenir le bon fonctionnement du système d'information (→ PRA/PCA) ;
- Authentification : assurer que seules les personnes autorisées aient accès aux ressources ;
- Non-répudiation : garantir qu'une transaction ne peut être niée (→ Notion de preuve) ;
- Traçabilité : garantir que les accès et tentatives d'accès sont tracés et que ces traces sont conservées et exploitables (→ Notion de preuve).

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE B -

AUDIT D'UN SYSTÈME D'INFORMATION

N°	Audit spécifique	N°	Audit spécifique
01	**Audit de la gouvernance des SI**	**03**	**Audit des réseaux et télécommunications**
	Audit de la fonction IT		Audit des réseaux locaux
	Audit des ressources humaines et des compétences IT		Audit des interconnexions du WAN
	Audit des locaux techniques		Audit des VLAN (Virtual Local Area Network))
	Audit des projets IT		Audit des interconnexions avec les partenaires
	Audit des contrats (prestataires, fournisseurs) IT		Audit des liaisons de secours
	Audit des changements		...
	Audit de l'alignement du SI sur la stratégie	**04**	**Audit des applications et Bases de données**
	Audit de la satisfactions des utilisateurs		Audit des bases de données
	...		Audit des applications critiques et des interfaces
02	**Audit des systèmes et serveurs**		Audit des codes applicatifs
	Audit des systèmes d'exploitation		...
	Audit des serveurs (physiques et virtuels)	**05**	**Autres possibilités d'audit**
	Audit de l'exploitation des systèmes et serveurs		Audit des plans de reprise et de continuité d'activité
	Audit des VPN (Virtual Private Network)		Audit des risques et des contrôles internes
	Audit de la sécurité logique		Audit des dispositifs nomades
	...		...

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.

⇨ **MEILLEURES PRATIQUES** ⇦

Dossier « A. 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.

Dossier « B. 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.

Dossier « C. Fiches indicatives additionnelles »

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

Dossier « D. Circulaires de la Commission Bancaire »

- Guide du banquier ;
- Circulaires de 2017 à 2020 :
  - Circulaire n°01-2017/CB/C (voir page 23) ;
  - Circulaire n°04-2017/CB/C (voir page 23).

Dossier « E. Audit des SI »

- Audit A01 : initiation à l'audit informatique ;
- Audit A02 : audit informatique (tous concernés, 2019) ;
- Audit A03 : audit, un outil complémentaire.

Dossier « F. Guides d'audit des SI »

- Guide G01 : guide d'audit des systèmes d'information, version HOBUX (2013) ;
- Guide G02 : guide d'audit des systèmes d'information, version HOBUX (2015) ;
- Guide d'audit des systèmes d'information (du Comité d'harmonisation de l'audit interne).

Dossier « G. Questionnaires d'audit des SI »

- Questionnaire Q01 : questionnaire de contrôle interne et système d'information ;
- Questionnaire Q02 : extrait d'un questionnaire d'audit informatique.

Contrôle interne

- « **Processus qui repose sur la mise en œuvre de tâches et d'activités continues** », IFACI ;
- Repose sur un ensemble de règles et de manuels de procédures, de documents et de systèmes.

Contrôle interne vs Audit interne

- **Contrôle interne**
  - affaire de tous ;
  - opération continue ;
  - processus transversal continu ;
  - Intégré aux missions opérationnelles quotidiennes ;
  - basé sur règles et procédures de gestion internes ;
  - **outil transversal de maîtrise des risques**.
- **Audit interne**
  - service dédié ;
  - opération ponctuelle
  - réalisée à posteriori (planifiée ou à la demande du Top management) ;
  - activité normalisée basée sur des normes internationales ;
  - mesure l'efficience du dispositif de contrôle interne.

Organisation du contrôle interne

- Mise en place des règles, procédures de gestion, etc. ;
- Contrôle de 1er niveau par les collaborateurs/opérationnels « directs » ;
- Contrôle de 2nd niveau par les managers (Chefs de service, Directeurs, etc.) ;
- Contrôle de 3ème niveau par les auditeurs internes ;
- Etc.

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE C -

GOUVERNANCE D'UN SYSTÈME IT

Principaux documents à collecter

Pour plus d'infos
Voir la fiche T02

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** (souvent au niveau des 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 des équipements : 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 serveurs et systèmes ;
  - 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 maitrise des budgets, contrats, redevances et maintenances assure une bonne gestion d'un SI.

N°	Etape à envisager pour un audit « Locaux techniques »	
01	**Etape n°1** Collecte de données sur les locaux techniques	- Plans d'architecture des bâtiments et locaux techniques - Documentation sur les équipements installés ou à installer - Procédures de gestion + Rapports (maintenances, audits, tests, etc.)
02	**Etape n°2** Contrôle de l'environnement et des composants internes et externes des locaux	- Contrôle de la concordance des plans avec les bâtiments - Contrôle des moyens d'accès (rue, rdc, fenêtre, escalier externe, etc.) - Contrôle de la présence de matériaux combustibles/inflammables - Analyse de l'environnement des bâtiments et des locaux techniques - Analyse détaillée des composants des locaux techniques : • construite avec du matériau difficile à perforer • type de paroi (vitrée, opaque légère, opaque lourde, etc.) • température ambiante et régulateurs de température • infiltration d'eau (par les parois, par le plafond ou le toit, etc.) • qualité du plancher et du plafond
03	**Etape n°3** Contrôle des systèmes automatiques existants dans les locaux techniques	- Accessible par carte magnétique ou équivalent - Existence d'un dispositif anti-incendie et de détecteurs de fumée - Existence d'un système redondant de climatisation - Existence d'alarmes sonores et/ou d'alarmes visuelles - Existence d'un système de détection automatique d'humidité - Existence d'un éclairage de secours en cas de panne de l'éclairage - Existence d'une énergie secondaire bien calibrée
04	**Etape n°4** Revue des rapports ou des tests effectués sur les locaux techniques	- Etude sur les menaces physiques et/ou environnementales - Revue des rapports de test des systèmes automatiques + Maintenance - Revue des registres existants (gestion des actifs, E/S, incidents, etc.)

N°	Phase	Acteur - Action - Point de vigilance
01	**Phase « Expression des besoins »** - Etude de faisabilité - Analyse du marché - Elaboration des termes de référence - Elaboration d'un cahier de charges • Volet « **Fonctionnel** » • Volet « **Technique** » - Elaboration de spécifications techniques (si une acquisition de matériel et/ ou d'équipement est nécessaire) **Qualité de la demande**	- **Prise en charge par un expert métier** (spécialiste du système souhaité, collaborateur utilisant ou ayant utilisé un système similaire, collaborateur réalisant « manuellement » les activités relatives au système à acquérir, etc.) **si le catalogue de services et d'applications de la DSI n'en propose pas** - Volet « technique » du cahier de charges (technologies, sécurité, contraintes techniques à prendre en compte, etc.) pouvant être fourni et/ou complété par une équipe IT - Spécifications techniques (serveur, ordinateur, routeur, switch, système d'exploitation, etc.) à élaborer par une équipe IT
02	**Phase « Acquisition »** - Sélection des prestataires et fournisseurs - Négociation des offres techniques et financières - Contractualisation	- Procédure interne d'acquisition à utiliser
03	**Phase « Mise en place »** - Mise en place d'un environnement de test - Installation, configuration et paramétrage - Tests d'acceptation (ou recette) et Validation - Mise en préproduction - Formation des administrateurs - Formation des utilisateurs - Mise en production (exploitation)	- Nécessité d'un **responsable de haut niveau** (rang « Directeur », rang « DGA », etc.) pour la supervision des tests et validation - Nécessité d'un **cahier de recette** avant le démarrage effectif des tests d'acceptation - Nécessité d'un **cadre spécial pour les tests** : salle équipée et réservée, périodes et horaires de tests bien définis - Nécessité d'un **rapport périodique** ou d'une **remontée périodique** des résultats de tests
04	**Phase « Assistance post-production »** - Assistance à la gestion des 1ères anomalies - Assistance à la prise en charge du système	- A prévoir dans les contrats d'acquisition et de mise en place - Une assistance post-production (d'environ 3 à 12 mois) est recommandée selon la complexité du système acquis

N°	Risque identifié/potentiel	Mesures d'atténuation et/ou Réponse
08	Restauration de données impossible après la mise en place d'un correctif	- Meilleure gestion des sauvegardes de données - Meilleure application des procédures de sauvegarde
09	Dérives budgétaires (budget projet, budget activité, etc.)	- Adaptation des chefs de projet en fonction des projets et des activités à piloter - Amélioration de la veille technologique afin de disposer de solutions, systèmes ou partenaires adéquats, fiables, etc.
10	Expression de besoins (TDRs, cahier de charges, spécifications techniques) non adaptée	- Forte implication des experts métiers - Revue qualité de documents par une équipe métier/IT
11	Omission dans les fichiers transférés	- Automatisation des opérations manuelles - Mise en place de scripts de transfert de fichiers
12	Utilisateurs avec des habilitations (systèmes, applications) inappropriées	- Revue des procédures de gestion des habilitations - Analyse périodique des droits des utilisateurs
13	Politique de formation inadaptée	- Prise en compte de l'évolution de l'infrastructure IT - Revue des compétences du personnel IT
14	Absence de contrat de service permettant une garantie, maintenance et assistance de qualité	- Suivi et analyse périodique des contrats IT - Mise en place d'un tableau de bord pour les contrats

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE D -

MANAGEMENT « SYSTÈMES-SERVEURS »

N°	Fabricant (serveurs, PCs)	N°	Editeur (systèmes)
01	**HP** www.hp.com	01	**Microsoft** www.microsoft.com
02	**Dell** www.dell.com	02	**Red Hat** www.redhat.com
03	**IBM** www.ibm.com	03	**Linux** www.linux.org
04	**Apple** www.apple.com	04	**Apple** www.apple.com

N°	Terminologie	Compléments d'informations
01	**EOL** Support technique devient très limité	**End-Of-Life** : Fin de vie Tous les produits atteignent la **fin de leur cycle de vie** pour plusieurs raisons, notamment les demandes du marché, l'innovation technologique et les changements liés au développement, ou la maturité des produits et leur remplacement par une technologie plus complète sur le plan fonctionnel.
02	**EOS**	**End-Of-Sale** : Arrêt de commercialisation Date à partir de laquelle il n'est plus possible de commander et d'acheter un matériel auprès du fabricant.
02	**EOS**	**End-Of-Support** : Fin du support Date à partir de laquelle il n'est plus possible d'obtenir des mises à jour, des correctifs ou une assistance technique de la part du fabricant.

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 **systématiser** 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.

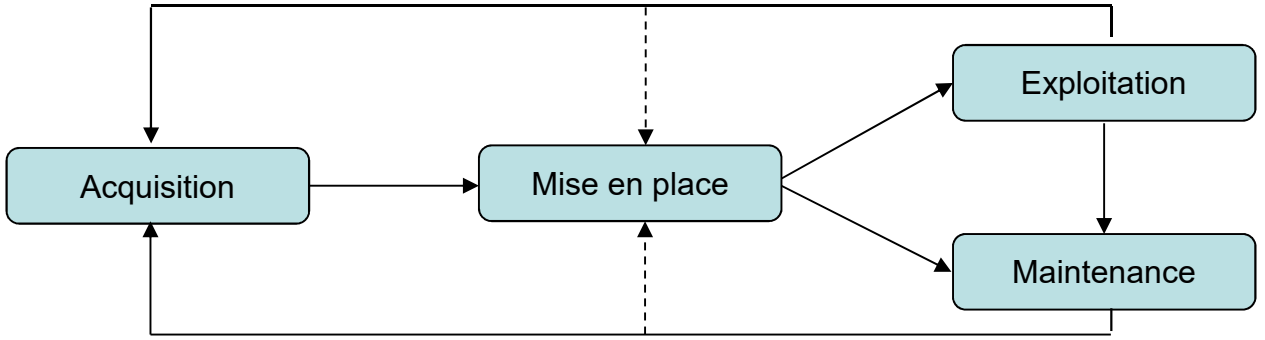
CYCLE DE VIE « SYSTÈMES-SERVEURS »

Acquisition

- Acquisition de serveurs physiques
- Acquisition de baies de disques, de racks, etc.
- Acquisition de systèmes d'exploitation (MS Windows, Linux/Unix, etc.) et licences associées

Mise en place

- Mise en place des environnements de production
- Mise en place des environnements de réplication/de secours
- Mise en place d'un environnement de tests, d'homologation, etc.
- Mise en place de tableaux de bord pour la gestion des « systèmes-serveurs »
- Mise en place des contrats de maintenance des « systèmes-serveurs »



Exploitation

- Exploitation des systèmes en production
- Assistance et support technique aux utilisateurs
- Gestion des incidents, anomalies, ..., des demandes d'évolution
- Collecte des données pour l'amélioration des « systèmes-serveurs »

Maintenance

- Suivi et revue des contrats de maintenance
- Planification et suivi des opérations de maintenance

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 mois 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 maitrisé ?
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 ?

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 »

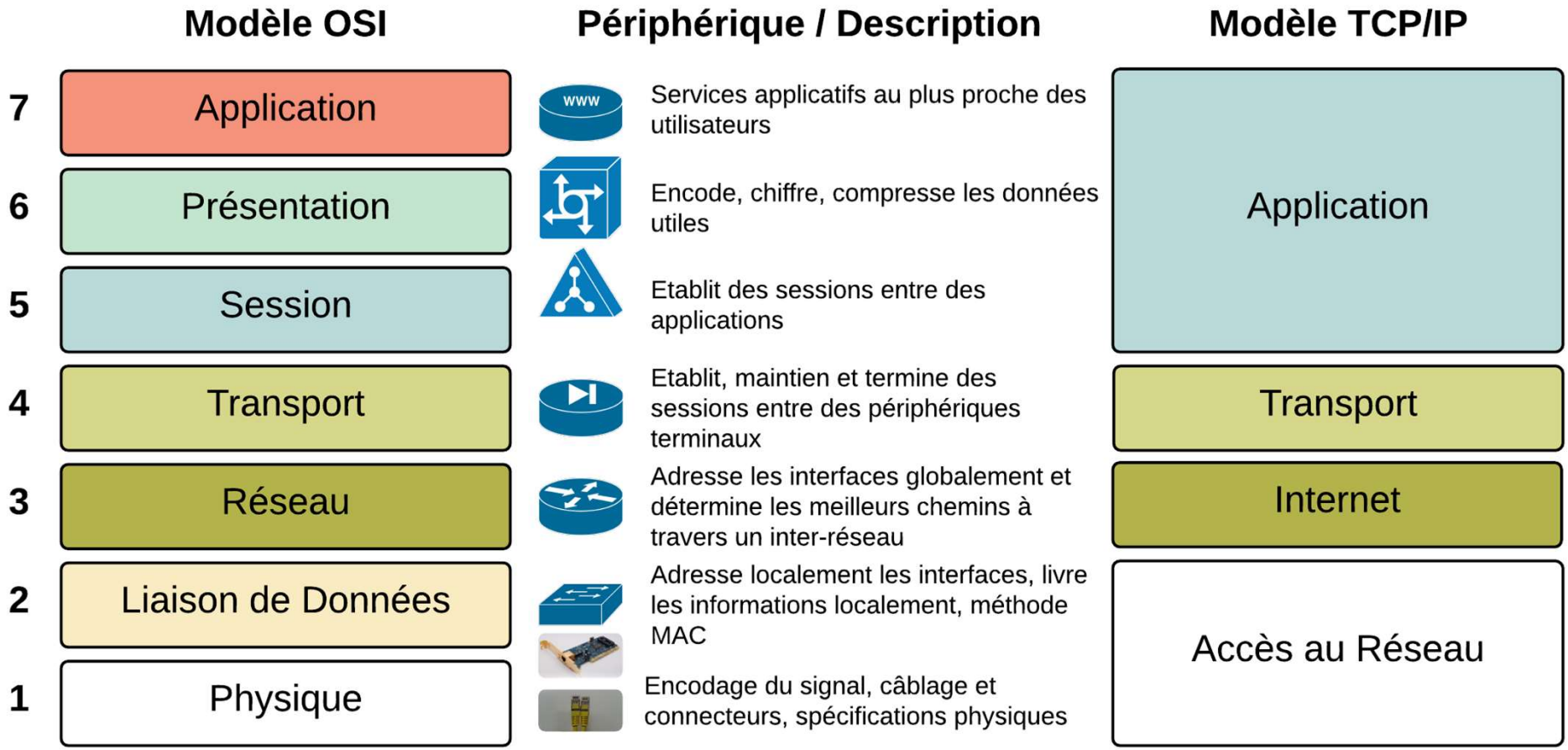
H.Management « Sécurité IT »

I.Continuité - Matrice SWOT - Maturité

J.Recommandations - Plan d'actions

- MODULE E -

MANAGEMENT « RÉSEAUX-TÉLÉCOMS »



Modèle OSI : modèle à 7 couches

Conçu dans les années 1970 par Huber Zimmermann et Charles Bachman, le modèle a été officiellement présenté en mars 1978. Considéré comme un **modèle conceptuel, théorique**, académique, etc., il est principalement utilisé pour **décrire, concevoir et comprendre l'architecture d'un système de communication**, notamment les fonctions individuelles des réseaux.

Modèle TCP/IP : modèle à 4 couches

Fonctionnel depuis 1976, il est considéré comme un modèle « C/S » pour la transmission de données sur Internet. Objectif initial : **maintenir les communications coûte que coûte, même en cas d'attaque nucléaire** (créé et vulgarisé par le Ministère américain de la Défense).

Depuis près d'un demi-siècle, Internet est utilisé comme moyen de communication entre les systèmes informatiques.

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 ?

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE F -

MANAGEMENT « BD-APPLICATIONS »

N°	SGBD	Compléments d'informations
01	**SGBD « C/S »** - Oracle Database - MS SQL Server - PostgreSQL - MySQL - MariaDB - DB2	**SGBD** (Système gestion de bases de données) **ou DBMS** (Database management system). Deux (02) avantages fondamentaux : **(1)** minimiser le trafic des données sur un réseau, **(2)** assurer une plus grande intégrité lors du traitement des données
02	**SGBD « fichier »** - MS Access - Paradox - FoxPro - FileMaker Pro	Système à base de fichiers : chaque poste de travail **traite localement les données**. Dans un **SGBD C/S**, tous les traitements sont effectués sur le serveur par le biais de requêtes.
03	**SGBD « embarqué »** - SQLite - Derby (JavaDB) - dBase - MaxDB	SGBD **embarqué (embedded)** est un SGBD incorporé directement dans une application.

Axes d'approfondissement		
- SGBD libres - SGBD open source	- SGBD gratuits - SGBD commerciaux	- SGBD multi-plateformes

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-directionel ;
- 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 toute les applications clé de l'entreprise/l'organisation ? Sinon, quel mécanisme permet de maitriser 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 évènements 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/régulière 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 » ;
   - Analyse des cas spécifiques de « **Shadow IT** » ou « **Informatique fantôme** » **(Classeurs MS Excel avec des macros, Solutions hébergées dans un cloud, Matériel informatique, Solutions VOIP, Informaticien travaillant hors de la DSI, fichiers professionnels stockés sur des espaces cloud, etc.)**.
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 « consommées » 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 règlementaires », 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.

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE G -

MANAGEMENT « UTILISATEURS-PARC IT »

CAS D'ÉTUDE - QUESTIONS

1. Cas d'étude sur la **collecte de données sur un parc IT**
   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. Continuité - 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 ?

4. Existe-t-il des procédures/politiques de gestion des **incidents de sécurité** ou de réaction face à de tels incidents ?

5. Les **actifs du SI** (matériel, applicatifs, etc.) sont-ils inventoriés et catégorisés par valeur, degré d'importance ou nécessité de protection ?

6. Les utilisateurs sont-ils **formés, sensibilisés, rappelés sur les questions relatives à la sécurité des SI** et aux bonnes pratiques ? Des procédures disciplinaires existent-ils en cas d'infraction aux règles liées à la sécurité des SI ?

7. Les collaborateurs de l'entreprise (ou uniquement les membres du Top Management) sont-ils astreints à la non-divulgation des données ou informations après un départ ?

8. Les mécanismes de gestion des accès ou systèmes d'habilitation sont-ils régulièrement/périodiquement revus et documentés ?

9. Les utilisateurs non autorisés ou temporairement indisponibles sont-ils désactivés ?

10. Le système d'authentification est-il centralisé ? Les utilisateurs, obligés d'avoir plusieurs identifiants/mots de passe, ont-ils un gestionnaire de mots de passe robuste ?

11. Les mots de passe, utilisés dans le SI, sont-ils une combinaison de majuscules, minuscules, chiffres, caractères spéciaux ?

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 (1) la gestion des fonctions externalisées et (2) les cas de « Shadow IT »** (aussi appelé **« Informatique fantôme »**) ?
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 maitriser les fonctions externalisées ? Des **mémos ou rapports** sont-ils régulièrement/périodiquement produits pour le Top Management ?

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE I -

CONTINUITÉ - MATRICE SWOT - MATURITÉ

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 » k
- 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.

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. Continuité - Matrice SWOT - Maturité

J. Recommandations - Plan d'actions

- MODULE J -

RECOMMANDATIONS - PLAN D'ACTIONS

PLAN D'ACTIONS À LONG TERME (période < 2 ans)

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

ANNEXE 01

ORGANISATION - EXEMPLES - CANEVAS

ORGANISATION

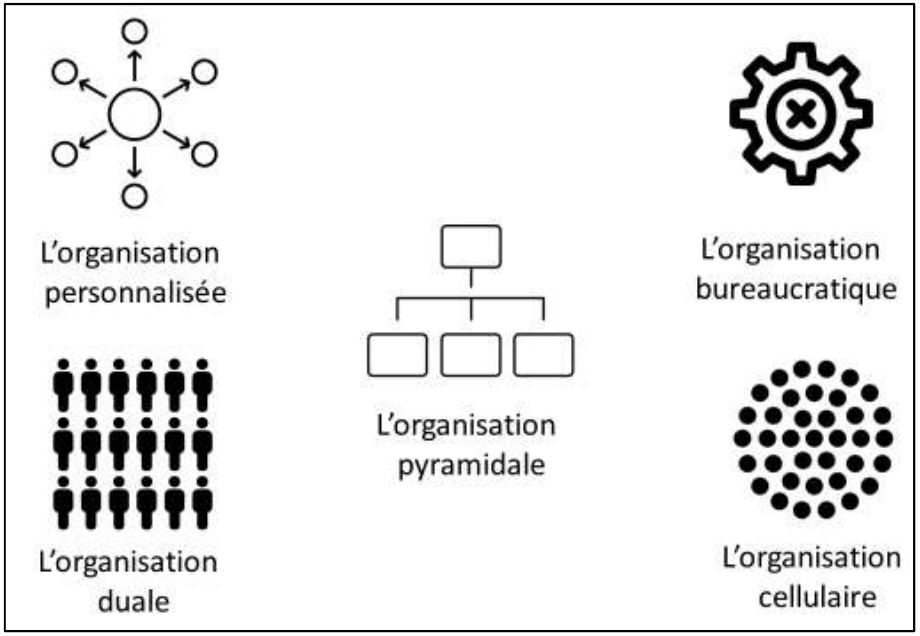
- Structure qui coordonne l'activité des individus pour les rendre capables de coopération en vue de réaliser un objectif commun
- Exemples : entreprises, administrations, associations, etc.

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



Canevas « **Rapport synthétique de formation - 1 page** »

1. Identification et financement de la formation	
Thème	
Lieu	
Période et durée	
Centre ou organisme de formation	
Financement par ...	
2. Résumé de la formation	
3. Appréciation de la formation et des outils	
Contenu adapté à mon profil	
Contenu conforme au prévisionnel	
Contenu correspondant à mes attentes	
Maitrise du contenu par le formateur	
Moyens pédagogiques utilisés (salle, matériel, support, etc.)	
4. Recommandations	

Canevas « **Evaluation des prestataires/fournisseurs - 1 page** »

1. Identification du prestataire/fournisseur	
Raison sociale (ou Nom/Prénom)	
Adresse géographique	
Téléphone - Email	
2. Principaux contrats/activités avec le prestataire/fournisseur	
Contrat n°1 (Activité, Période, Montant)	
Contrat n°2 (Activité, Période, Montant)	
Contrat n°3 (Activité, Période, Montant)	
Contrat n°4 (Activité, Période, Montant)	
Contrat n°5 (Activité, Période, Montant)	
3. Appréciation des prestations du prestataire/fournisseur	
Respect des délais	
Qualité des équipes techniques	
Capacité d'anticipation	
Qualité des recommandations	
Assistance technique	
4. Avis du comité d'évaluation - Evaluation	
Recommandations	**Evaluation** /20

ANNEXE 03

QUALITÉ - PROCESSUS - PROCÉDURES