



« Like a conscientious and methodical craftsman, every day, refine your practice. Only in this way will you be and remain an expert in your field. »

# TABLE DES MATIERES

LISTE DES TABLEAUX.....	8
LISTE DES IMAGES.....	8
INTRODUCTION GENERALE.....	10
a. Introduction .....	10
b. Nécessité d'un cours sur la pratique de l'Audit des Systèmes d'Information .....	11
c. Prérequis au cours.....	12
i. Connaissance d'un tableur : cas particulier de Microsoft Excel ou tout autre tableur .....	12
ii. Connaissance d'un traitement de texte : cas particulier de Microsoft Word ou tout autre traitement de texte.....	12
iii. Connaissance des notions d'Ingénierie des Processus .....	13
iv. Aptitude à lire et à assimiler rapidement .....	13
1) DEFINITIONS, CONCEPTS ET BASES POUR LE COURS.....	15
1.1. Définitions, Concepts et Bases de l'Audit et du Contrôle .....	15
1.1.1. Les différences entre l'Audit et le Contrôle .....	15
1.1.2. Assurance raisonnable.....	15
1.1.3. Risques.....	15
1.1.4. Contrôle Interne.....	20
1.1.5. Règle des Quatre Yeux .....	21
1.1.6. Allégorie des deux (2) mains .....	21
1.1.7. Trois piliers de l'Audit Interne.....	22
1.1.8. Point de contrôle.....	22
1.1.9. Objectif de contrôle .....	22
1.1.10. Critère d'évaluation .....	23
1.1.11. Question d'évaluation.....	23
1.1.12. Constatation d'Audit.....	24
1.1.13. Contradictoire .....	25
1.1.14. Observations.....	25
1.1.15. Sur place et sur pièces .....	25
1.1.16. Aveu de carence .....	26
1.2. Définitions, Concepts et Bases des Systèmes d'Information .....	26
1.2.1. Notion de système.....	26
1.2.2. Les Systèmes d'Information.....	26
1.2.2.1. Système informatique .....	26
1.2.2.2. Système d'information .....	26
1.2.2.3. Fonction informatique .....	27

1.2.2.4.	<i>Fonction d'information</i> .....	27
1.2.2.5.	<i>Problèmes inhérents aux SI</i> .....	27
1.2.2.6.	<i>Informatisation des SI</i> .....	27
1.2.2.7.	<i>Types de migration/changement de SI</i> .....	27
1.2.3.	<i>Système d'exploitation</i> .....	28
1.2.4.	<i>Système de fichier</i> .....	29
1.2.5.	<i>Fichiers</i> .....	29
1.2.6.	<i>Base de données</i> .....	29
1.2.7.	<i>Réseau informatique</i> .....	29
1.2.8.	<i>Sécurité informatique</i> .....	30
<b>1.3.</b>	<b>Les Contrôles en Audit des Systèmes d'Information</b> .....	30
1.3.1.	<i>Rôle</i> .....	30
1.3.2.	<i>Point de contrôle</i> .....	30
1.3.3.	<i>Contrôles dans les SI</i> .....	30
<b>1.4.</b>	<b>Evaluation des Connaissances</b> .....	36
1.4.1.	<i>QCM</i> .....	36
1.4.2.	<i>Questions à Trous</i> .....	38
1.4.3.	<i>Questions Ouvertes</i> .....	39
1.4.4.	<i>Cas pratique</i> .....	42
<b>2)</b>	<b>DEMARCHE GENERALE D'AUDIT DES SYSTEMES D'INFORMATION</b> .....	45
<b>2.1.</b>	<b>Champs d'application</b> .....	45
2.1.1.	<i>Audit d'une organisation</i> .....	45
2.1.2.	<i>Audit de processus</i> .....	45
2.1.3.	<i>Audit de régularité</i> .....	46
2.1.4.	<i>Audit des fonctions externalisées</i> .....	46
<b>2.2.</b>	<b>Travaux préparatoires</b> .....	46
2.2.1.	<i>Documents à solliciter</i> .....	46
2.2.2.	<i>Analyse préalable des risques</i> .....	49
2.2.3.	<i>Identification des ressources nécessaires pour la mission</i> .....	49
2.2.4.	<i>Documents à produire</i> .....	50
<b>2.3.</b>	<b>Planification</b> .....	50
2.3.1.	<i>Suivi et analyse des documents sollicités</i> .....	50
2.3.2.	<i>Choix de l'approche et du type d'audit</i> .....	51
2.3.3.	<i>Référentiels à utiliser</i> .....	51
2.3.4.	<i>Evaluation à priori du système de contrôle interne</i> .....	51
2.3.5.	<i>Outils d'aide à l'audit</i> .....	52
2.3.6.	<i>Préparation des entretiens et entrevues</i> .....	52

2.3.7.	<i>Rapport d'orientation/planification .....</i>	53
<b>2.4.</b>	<b>Exécution de la mission.....</b>	<b>53</b>
2.4.1.	<i>Réunion d'ouverture de la mission.....</i>	53
2.4.2.	<i>Collecte d'information.....</i>	54
2.4.3.	<i>Validation des résultats de l'analyse préalable des risques .....</i>	55
2.4.4.	<i>Suivi des documents sollicités.....</i>	55
2.4.5.	<i>Déploiement des outils conçus .....</i>	57
2.4.6.	<i>Évaluation des contrôles généraux et d'application.....</i>	58
2.4.8.	<i>Extraction de données.....</i>	58
2.4.9.	<i>Consignation des faits observés .....</i>	59
2.4.10.	<i>Rédaction des projets d'observation .....</i>	59
<b>2.5.</b>	<b>Communication des résultats .....</b>	<b>59</b>
2.5.1.	<i>Contradictoire.....</i>	60
2.5.2.	<i>Formulation des opinions d'audit .....</i>	60
2.5.3.	<i>Finalisation du rapport de mission.....</i>	60
2.5.4.	<i>Réunion de clôture de mission.....</i>	61
2.5.5.	<i>Transmission du rapport.....</i>	62
<b>2.6.</b>	<b>Evaluation des Connaissances.....</b>	<b>62</b>
2.6.1.	<i>QCM .....</i>	62
2.6.2.	<i>Questions à Trous .....</i>	65
2.6.3.	<i>Questions Ouvertes.....</i>	66
2.6.4.	<i>Cas pratique.....</i>	68
<b>3)</b>	<b>NORMES ET REFERENTIELS USUELS EN AUDIT DES SYSTEMES D'INFORMATION .....</b>	<b>71</b>
<b>3.1.</b>	<b>COSO .....</b>	<b>71</b>
3.1.1.	<i>Objectif principaux .....</i>	71
3.1.2.	<i>Structure du COSO.....</i>	72
3.1.3.	<i>Importance du COSO dans les audits des systèmes d'information .....</i>	73
<b>3.2.</b>	<b>COBIT .....</b>	<b>74</b>
3.2.1.	<i>Objectifs et apports du COBIT .....</i>	74
3.2.2.	<i>Evolution de la structure du COBIT.....</i>	74
3.2.3.	<i>Importance du COBIT pour les audits des systèmes d'information.....</i>	76
<b>3.3.</b>	<b>ISO 2700x et 270xx.....</b>	<b>77</b>
3.3.1.	<i>Aperçu de la gamme de normes.....</i>	77
3.3.2.	<i>Principales normes de la suite 27000.....</i>	78
3.3.3.	<i>Importance des normes ISO 2700X et 270XX en audit .....</i>	79
<b>3.4.</b>	<b>Evaluation des Connaissances.....</b>	<b>80</b>
3.4.1.	<i>QCM .....</i>	80



1.1.1.	Questions à Trous .....	83
1.1.2.	Questions Ouvertes.....	84
1.1.3.	Cas pratique.....	86
4)	<b>PRINCIPAUX TYPES D'AUDIT DANS LES SYSTEMES D'INFORMATION</b> .....	89
4.1.	<b>Audit des Applications en Service</b> .....	89
4.1.1.	But .....	89
4.1.2.	Différentes portées des audits d'application en service .....	89
4.1.3.	L'audit de fiabilité et de sécurité .....	89
4.1.4.	L'audit d'efficacité et de performance.....	89
4.1.5.	Fréquence recommandée pour les audits .....	89
4.1.6.	Points de contrôle .....	90
4.1.7.	Objectifs de contrôle classés par point de contrôle .....	90
4.1.8.	Critères classés par objectifs de contrôle ( Organisation) .....	94
4.1.9.	Eléments requis classés critère .....	96
4.1.10.	Questions d'évaluation classées par critère .....	97
4.1.11.	Risques classés questions d'évaluation .....	97
4.1.13.	Conduire une Mission d'Audit d'une Application en Service .....	98
4.2.	<b>Audit de la Fonction Informatique</b> .....	102
4.2.1.	But .....	102
4.2.2.	Fréquence recommandée pour les audits .....	102
4.2.3.	Points de contrôle.....	102
4.2.4.	Objectifs de contrôle classés par point de contrôle .....	102
4.2.5.	Critères classés par objectifs de contrôle .....	104
4.2.6.	Eléments requis classés critère .....	104
4.2.7.	Questions d'évaluation classées par critère .....	104
4.2.8.	Risques classés questions d'évaluation .....	104
4.2.9.	Conséquences classé par risque .....	104
4.2.10.	Conduire une Mission d'Audit de la Fonction Informatique .....	105
4.3.	<b>Audit et Contrôle des Projets Informatiques</b> .....	109
4.3.1.	But .....	109
4.3.2.	Fréquence recommandée pour les audits .....	109
4.3.3.	Points de contrôle.....	109
4.3.4.	Quelques objectifs de contrôle classés par point de contrôle .....	110
4.3.5.	Conduire une Mission d'Audit des Projets Informatiques .....	120
4.4.	<b>Audit du Support Utilisateur et de la Gestion du Parc</b> .....	124
4.4.1.	But .....	124
4.4.2.	Fréquence recommandée pour les audits .....	124

4.4.3.	<i>Points de contrôle</i> .....	124
4.4.4.	<i>Quelques objectifs de contrôle classés par point de contrôle</i> .....	124
4.4.5.	<i>Conduire une Mission d’Audit du Support aux utilisateurs et de la gestion du Parc</i> ....	127
<b>4.5.</b>	<b>Audit de Sécurité Informatique</b> .....	<b>131</b>
4.5.1.	<i>But</i> .....	131
4.5.2.	<i>Fréquence recommandée pour les audits</i> .....	131
4.5.3.	<i>Points de contrôle</i> .....	131
4.5.4.	<i>Quelques objectifs de contrôle classés par point de contrôle</i> .....	131
4.5.5.	<i>Conduire une Mission d’Audit de Sécurité</i> .....	135
<b>4.6.</b>	<b>Audit et Contrôle de la Fonction Etude</b> .....	<b>139</b>
4.6.1.	<i>But</i> .....	139
4.6.2.	<i>Fréquence recommandée pour les audits</i> .....	139
4.6.3.	<i>Points de contrôle</i> .....	139
4.6.4.	<i>Quelques objectifs de contrôle classés par point de contrôle</i> .....	139
4.6.5.	<i>Conduire une Mission d’Audit de la Fonction Etude</i> .....	141
4.7.	<i>Evaluation des Connaissances</i> .....	144
4.7.1.	<i>QCM</i> .....	144
4.7.2.	<i>Questions à Trous</i> .....	148
4.7.3.	<i>Questions Ouvertes</i> .....	149
4.7.4.	<i>Cas pratique</i> .....	151
<b>5)</b>	<b>DISCUSSIONS SUR DES SUJETS CONNEXES A L’AUDIT DES SI</b> .....	<b>154</b>
<b>5.1.</b>	<b>Discussion sur le rôle et l’impact de l’intelligence artificielle dans les systèmes d’information : cas de la société Lizbiz’s</b> .....	<b>154</b>
5.1.1.	<i>Introduction</i> .....	154
5.1.2.	<i>Les avantages de l’IA pour les systèmes d’information</i> .....	154
5.1.3.	<i>Les inconvénients et risques potentiels de l’IA dans un système d’information</i> .....	155
5.1.4.	<i>Enjeux clés pour un auditeur des systèmes d’information dans un contexte d’IA</i> .....	155
5.1.5.	<i>Les défis à relever dans l’intégration de l’IA pour un SI en évolution</i> .....	156
5.1.6.	<i>Conclusion : Une opportunité à saisir, mais avec précaution</i> .....	157
<b>5.2.</b>	<b>Discussion sur la fraude dans et par les systèmes d’information</b> .....	<b>158</b>
5.2.1.	<i>Introduction</i> .....	158
5.2.2.	<i>La nature de la fraude dans les systèmes d’information</i> .....	158
5.2.3.	<i>L’impact de la fraude sur la performance de Lizbiz’s</i> .....	158
5.2.4.	<i>Les parades contre la fraude dans les systèmes d’information</i> .....	159
5.2.5.	<i>Les défis à relever pour lutter contre la fraude</i> .....	160
5.2.6.	<i>Conclusion : Une vigilance continue pour protéger les actifs de Lizbiz’s</i> .....	161
<b>6)</b>	<b>CAS PRATIQUE</b> .....	<b>163</b>

<b>6.1. Consignes .....</b>	<b>163</b>
6.1.1. Objectifs .....	163
6.1.2. Énoncé du Cas .....	163
6.1.3. Mandat pour l'Équipe de Mission .....	163
<b>6.2. Modèles de rapport d'audit d'une Application en Service : APPLICATION .....</b>	<b>164</b>
6.2.1. Introduction .....	164
6.2.2. Evaluation du système de contrôle interne .....	165
6.2.3. Périmètre et Détails de l'Application .....	167
6.2.4. Résultats de l'Audit .....	172
6.2.4.3.2. Plan de Continuité d'Activité (PCA) .....	173
6.2.5. Observations .....	174
6.2.6. Synthèse des Recommandations .....	174
6.2.7. Conclusion .....	175
<b>6.3. Création et chargement de la base de données de l'application APPLICATION .....</b>	<b>175</b>
6.3.1. Notes : .....	175
6.3.2. Création de la base de données avec contraintes : .....	175
6.3.3. Chargement d'un jeu de données dans la base de données : .....	178
<b>6.4. Conception de l'outil pour l'évaluation du système de contrôle interne de l'application APPLICATION .....</b>	<b>182</b>
6.4.1. Domaine : Environnement de Contrôle .....	182
6.4.2. Domaine : Évaluation des Risques .....	184
6.4.3. Domaine : Activités de Contrôle .....	186
6.4.4. Domaine : Information et Communication .....	188
6.4.5. Activités de Surveillance .....	190
<b>6.5. Conception de l'outil pour l'audit des aspects métiers de l'application APPLICATION. ....</b>	<b>191</b>
6.5.1. Domaine : Gestion des Comptes .....	191
6.5.2. Domaine : Saisie des Écritures Comptables .....	192
6.5.3. Domaine : Gestion des Clients et Fournisseurs .....	193
6.5.4. Domaine : Facturation et Gestion des Recettes .....	194
6.5.5. Domaine : Suivi de la Trésorerie .....	194
6.5.6. Domaine : Gestion des Immobilisations .....	195
6.5.7. Domaine : États Financiers et Rapports Comptables .....	196
6.5.8. Conformité et Clôture de Fin d'Année .....	197
<b>6.6. Conception de l'outil pour l'audit des aspects informatiques de l'application APPLICATION.</b>	<b>199</b>
<b>6.7. Liste des outils et logiciels recommandés. ....</b>	<b>199</b>
6.7.1. Analyse de la Performance de l'Application .....	199
6.7.2. Analyse de la Sécurité de l'Application .....	199

6.7.3.	Analyse Statique et Dynamique de Code (SAST et DAST) : .....	200
6.7.4.	Monitoring et Détection d'Intrusions : .....	200
6.7.5.	Autres Outils Recommandés pour la Sécurité et la Performance .....	200
7)	LABORATOIRES D'AUDIT DES SYSTEMES D'INFROMATION .....	202
7.1.	Audit d'une application en service.....	202
7.1.1.	Objectif.....	202
7.1.2.	Énoncé du Cas : .....	202
7.1.3.	Étapes du Lab : .....	202
7.1.4.	Livrables : .....	203
7.1.5.	Calendrier : .....	204
7.2.	Audit de sécurité d'une infrastructure .....	205
7.2.1.	Objectifs .....	205
7.2.2.	Énoncé du Cas : .....	205
7.2.3.	Description de l'infrastructure : .....	205
7.2.4.	Phases du Lab : .....	206
7.2.5.	Calendrier : .....	208
	SUJETS TYPES EXAMENS.....	210
I.	QCM .....	210
II.	Connaissance du Cours.....	212
III.	Questions V/F .....	213
IV.	Cas Pratiques.....	214
V.	Questions ouvertes .....	217
	ANNEXES .....	219
	Modèle d'observation.....	219
	GLOSSAIRE.....	222
	SYLLABUS .....	225
	Ce support de cours a été préparé par Thierry MINKA.....	227



## LISTE DES TABLEAUX

Tableau 1: Quelques risques informatiques et leurs facteurs .....	17
Tableau 2: Différents types de migration de système.....	28
Tableau 3: Liste des documents à solliciter.....	47
Tableau 4: Suivi des documents sollicités .....	55
Tableau 5: structure idéale d'un rapport de mission d'audit.....	61
Tableau 6: Principes et composantes du COSO .....	72
Tableau 7: Les cinq (5) domaines du COBIT 2019.....	75
Tableau 8: ISO applicables à la sécurité des technologies de l'information et d'usage courant en audit des SI.....	79
Tableau 9: calendrier d'exécution de la mission.....	204
Tableau 10: calendrier d'exécution de la mission .....	208
Tableau 11: Questions Vrai/Faux.....	213
Tableau 12: Détail du cours par livre .....	225

## LISTE DES IMAGES

Figure 1: Liens entre les contrôles et les objectifs d'entreprise.....	77
Figure 2: Répartition de la note finale .....	226

**Cher apprenant,**

Ce cours d'audit des systèmes d'information est bien plus qu'une simple matière académique. C'est une opportunité unique de plonger dans un domaine crucial où rigueur, méthode et réflexion sont les clés de la réussite. Mon objectif est de t'aider à comprendre les principes fondamentaux de l'audit et à les appliquer dans des situations proches de la réalité professionnelle.

Tu découvriras comment analyser et évaluer des systèmes d'information, identifier les risques et proposer des solutions concrètes. À travers ce cours, je veux te transmettre des outils pratiques et une méthodologie structurée qui te seront utiles bien au-delà de cette classe.

L'audit est un domaine exigeant. Il demande une attention aux détails, une capacité d'analyse et une compréhension globale des systèmes. Mais je suis convaincu que tu as en toi tout ce qu'il faut pour réussir. Je te demande simplement de t'investir pleinement. La théorie que je vais t'enseigner ne prendra tout son sens que si tu t'engages à pratiquer, à réfléchir et à te poser des questions.

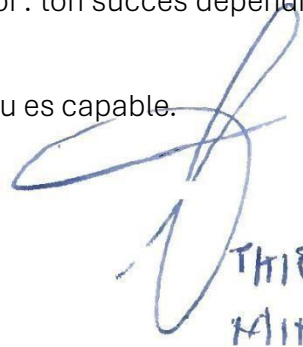
Nous travaillerons ensemble sur plusieurs aspects essentiels :

1. Les bases de l'audit : comprendre la méthodologie globale d'un audit des systèmes d'information, les différentes phases d'une mission et la documentation à requérir et à produire par phase. Puis comprendre les standards, comme ISO 27001 et COBIT, et leur rôle dans l'évaluation des systèmes.
2. La gestion des risques : apprendre à identifier, classer et documenter les risques, tout en proposant des recommandations adaptées.
3. Les cas pratiques : résoudre des problématiques concrètes qui te prépareront à ce que tu pourrais rencontrer dans ta carrière.

Ce que je te propose ici, ce n'est pas seulement un cours, mais une occasion de bâtir des compétences solides et d'affirmer ton potentiel. J'ai confiance en toi, et j'espère que tu prendras ce défi à cœur. Tu n'as rien à prouver à personne d'autre qu'à toi-même.

Je suis là pour te guider si nécessaire. Mais souviens-toi : ton succès dépendra avant tout de ton engagement et de ta volonté de progresser.

Bonne chance, et surtout, ne doute jamais de ce dont tu es capable.



THIERRY  
MINK.

# INTRODUCTION GENERALE

## a. Introduction

Ce cours vise à initier les apprenants aux principes fondamentaux de l'audit dans des environnements informatisés tout en leur offrant des outils concrets pour analyser, évaluer et sécuriser les systèmes d'information modernes. Il s'inscrit dans un contexte où les systèmes d'information sont devenus indispensables à la gestion des entreprises et des institutions publiques, mais aussi au cœur des enjeux de sécurité, de fiabilité et de conformité.

J'ai conçu ce cours a pour répondre à deux objectifs principaux :

1. **Fournir une base solide** : Les apprenants apprendront les cadres méthodologiques reconnus (ISO 27001, COBIT, etc.) et les techniques nécessaires pour identifier, évaluer et gérer les risques liés aux systèmes d'information.
2. **Préparer à la pratique professionnelle** : En travaillant sur des cas concrets, ils développeront une capacité d'analyse critique et une compréhension approfondie des défis techniques et organisationnels rencontrés par les auditeurs dans des environnements complexes.

Dans un monde où l'informatisation est omniprésente, maîtriser l'audit des systèmes d'information constitue une compétence clé pour tout ingénieur en cybersécurité. Les apprenants seront en mesure d'évaluer non seulement les performances techniques et opérationnelles des systèmes, mais aussi leur conformité avec les normes et les réglementations. Ils apprendront également à anticiper les risques et à proposer des recommandations pour améliorer la sécurité et la continuité des services.

Ce cours est une opportunité pour les apprenants de se familiariser avec une discipline stratégique, au croisement de la technologie et de la gestion des risques. L'objectif final est de les préparer à devenir des professionnels compétents, capables d'accompagner les organisations dans l'optimisation et la sécurisation de leurs systèmes d'information.

Le cas de la société fictive Lizbiz's sera déroulé tout au long du cours pour illustrer les notions présentées.

Rendu à sa troisième itération, le cours s'appuie sur une structure enrichie et cohérente, offrant un équilibre entre théorie et pratique. Il est organisé en huit livres complémentaires, qui permettent aux apprenants de progresser de manière structurée et de couvrir l'ensemble des dimensions de l'audit des systèmes d'information :

- ☑ Livre I : Définitions, concepts et bases pour le cours ;
- ☑ Livre II : Démarche générale d'audit des systèmes d'information ;
- ☑ Livre III : Normes et référentiels courants en audit des SI ;
- ☑ LIVRE IV : Principaux types d'audit dans les systèmes d'information ;
- ☑ Livre V : Discussions d'actualités ;
- ☑ Livre VI : Cas pratiques ;
- ☑ Livre VII : Sujets types;
- ☑ Livre VIII: Annexes.

Ce cadre structuré permet d'explorer les fondamentaux, les approches méthodologiques, les outils pratiques, et les cas concrets pour doter les apprenants des compétences nécessaires à une pratique professionnelle rigoureuse et alignée sur les standards internationaux.

## **b. Nécessité d'un cours sur la pratique de l'Audit des Systèmes d'Information**

Dans un contexte où la digitalisation transforme profondément les processus de gestion des finances publiques, la pratique de l'audit des systèmes d'information devient une composante essentielle dans la formation des auditeurs. Les systèmes d'information jouent un rôle central dans la collecte, le traitement, le stockage et la diffusion des données financières. Leur performance, leur sécurité et leur conformité aux réglementations impactent directement la transparence, l'efficacité et la fiabilité des opérations financières publiques.

Au Cameroun, la digitalisation des services publics, amorcée il y a une dizaine d'années, connaît aujourd'hui une accélération notable, notamment avec l'intégration croissante des technologies numériques dans la gestion des ressources publiques et des services administratifs. Cette transition rapide expose les systèmes à des risques accrus, tels que les cyberattaques, les erreurs de configuration ou le non-respect des cadres réglementaires.

Le cours d'audit des systèmes d'information joue un rôle central dans la formation d'ingénieurs spécialisés en cybersécurité et investigation numérique. Il leur permet d'acquérir une compréhension approfondie des systèmes d'information en tant que piliers des entreprises modernes, où la gestion des données, des processus et des opérations est cruciale. Ce cours enseigne comment analyser les failles organisationnelles et techniques, optimiser les performances des SI, et garantir leur fiabilité. Les concepts clés, tels que la gestion des accès, l'intégrité des données et l'identification des indicateurs de performance (KPI), permettent aux apprenants de prévenir les dysfonctionnements et de résoudre des problèmes critiques comme les retards ou les incohérences.

En cybersécurité, l'audit des SI complète les compétences techniques par une approche stratégique. Il forme les futurs ingénieurs à sécuriser les systèmes tout en alignant les technologies sur les objectifs métiers. Grâce à ce cours, les apprenants apprennent à identifier les vulnérabilités, à évaluer les risques et à recommander des solutions alignées sur des normes telles que COBIT ou ISO 27001. En combinant analyse des performances et gestion proactive des risques, l'audit des SI devient une compétence essentielle pour garantir la résilience et la conformité des infrastructures numériques.

En intégrant ce cours dans le cursus, les auditeurs sont mieux préparés à relever les défis liés à la transformation numérique des administrations publiques.

camerounaises et à jouer un rôle clé dans la mise en œuvre de pratiques de gouvernance informatique robustes et alignées sur les objectifs de transparence et de responsabilité.

### c. Prérequis au cours

#### i. *Connaissance d'un tableur : cas particulier de Microsoft Excel ou tout autre tableur*

Les tableurs sont des outils d'une importance majeure dans le traitement et l'analyse des données. Dans le cadre d'une mission d'audit, un auditeur peut être amené à manipuler une grande quantité de données, les pointages et traitements manuels sont générateurs de risques d'erreur sur les résultats, d'oubli ou non prise en compte de certaines valeurs, ou d'altération des données.

Sur un autre point, l'usage d'un tableur peut dans la phase de planification aider à la conception d'outils d'aide à l'audit, qui simplifieront par la suite l'exécution de la mission.

La connaissance et le bon usage d'un tableur comme Microsoft Excel ou tout autre est donc un avantage indéniable pour un auditeur. Dans le cadre de ce cours, un minimum d'aptitude à l'utilisation de Microsoft Excel est indispensable.

Les apprenants concevront progressivement un outil d'aide à l'audit au fil du cours.

#### ii. *Connaissance d'un traitement de texte : cas particulier de Microsoft Word ou tout autre traitement de texte*

L'auditeur ne réalise pas la mission d'audit pour lui-même, il doit en transmettre ultimement les résultats au commanditaire qui en fera l'usage souhaité. Pour cette transmission, il a besoin de consigner les travaux d'audit sous la forme convenue dans son entité. Ceci se fait par la rédaction qui fait appel à l'usage d'un traitement de texte.

Le style et l'observance des règles d'orthographe et de grammaire sont de rigueur pour la communication des résultats d'audit. Par ailleurs, du fait de la nature sensible de ces derniers, il n'est pas souvent souhaité que des personnes en dehors de l'équipe de mission y accèdent avant le commanditaire. L'auditeur doit donc être capable de bien se servir d'un traitement de texte comme Microsoft Word.

Dans le cadre de ce cours, un minimum d'aptitude à l'utilisation de Microsoft Word est indispensable.

Les apprenants seront amenés à rédiger un rapport de mission d'audit au fil du cours.



iii. *Connaissance des notions d'Ingénierie des Processus*

Dit simplement, l'ingénierie des processus est l'ensemble des règles et méthodes observées pour codifier une fonction ou partie d'une fonction métier de manière univoque et linéaire, en la transcrivant étape par étape, de son point de démarrage à celui de fin.

Elle permet à l'auditeur de cocher sur papier la transcription d'un processus en étapes distinctes permettant l'identification des points de contrôle.

Dans le cadre de ce cours, un minimum d'aptitude à conceptualiser un processus et à le transcrire est indispensable. Dans le cadre de ce cours, Les apprenants seront emmenés à linéariser des processus d'entreprise.

iv. *Aptitude à lire et à assimiler rapidement*

L'audit est un métier particulier qui exige du praticien d'avoir au minimum, le même niveau de compréhension du sujet d'audit que la personne auditée. Pour ce faire, l'auditeur doit cultiver et entretenir sa capacité à lire beaucoup et rapidement, ainsi que celle à vite et bien assimiler ce qu'il lit.

Sans ces deux éléments, les contraintes de temps, lot quotidien de l'auditeur deviendront intenable. En effet, en un laps de temps très court, il est demandé à l'auditeur de découvrir un domaine, le comprendre et d'être capable d'y effectuer son travail, alors même que les professionnels de ce domaine y travaillent au quotidien et souvent depuis des années.

Dans le cadre de ce cours, un minimum d'aptitude à lire et à assimiler rapidement est requis des apprenants pour ingurgiter le flot d'information nouvelle qui va déferler sur eux.



# Livre I : BASES, CONCEPTS ET FONDAMENTAUX

## **Objectif :**

Fixer le contexte global du cours. Donner les éléments de compréhension et notions manipulées tout au long du cours aux apprenants.

## **Objectif d'apprentissage :**

A la fin de ce livre, chaque apprenant doit être à mesure de bien manipuler les concepts et terminologies propres à l'audit des SI.

## 1) DEFINITIONS, CONCEPTS ET BASES POUR LE COURS

Ce chapitre constitue pose les fondations théoriques nécessaires à la compréhension approfondie des systèmes d'information, de leur audit, et des enjeux qui y sont associés. Il explore les notions de base, les concepts clés et les principes fondamentaux qui encadrent l'audit des systèmes d'information. En effet, une maîtrise rigoureuse de ces concepts est indispensable pour appréhender les méthodologies, normes et pratiques qui guident l'évaluation, le contrôle et la sécurisation des systèmes d'information. Ce chapitre vise donc à fournir aux apprenants un socle de connaissances solide, permettant de situer l'audit dans son contexte organisationnel et technologique, tout en éclairant les enjeux de gouvernance, de performance, et de sécurité qui lui sont inhérents.

### 1.1. Définitions, Concepts et Bases de l'Audit et du Contrôle

#### 1.1.1. Les différences entre l'Audit et le Contrôle

L'audit a pour sujet un processus, tandis que le contrôle lui s'applique à une opération.

Le but de l'audit est l'optimisation du processus sous revue pour en améliorer la participation dans la création de la valeur pour l'entité. Celui du contrôle peut être de s'assurer de l'exactitude, la complétude, l'existence, la cohérence, ... de l'opération visée.

#### 1.1.2. Assurance raisonnable

La notion d'assurance raisonnable est liée à la collecte des éléments probants nécessaires pour que l'auditeur puisse conclure que les éléments analysés pris dans leur ensemble ne comportent pas d'inexactitudes importantes, pouvant entacher les choix du commanditaire.

#### 1.1.3. Risques

##### 1.1.3.1. Définition académique du risque

Le risque est la probabilité qu'une menace exploite une vulnérabilité pour générer un impact sur une ressource identifiée.

L'élément capital pour l'existence du risque est donc la ressource.

Le risque est essentiellement probable, sa valeur est donc comprise dans l'intervalle ]0, 1[.

Dès matérialisation de la chose projetée, c'est-à-dire lorsque la valeur vaut 1 on parle d'incident. En revanche lorsqu'elle vaut 0 on parle d'opportunité.

##### 1.1.3.2. Généralités sur les Risques

Les éléments minimaux constitutifs du risque sont :

- ☒ La ressource ;
- ☒ La ou les vulnérabilités ;
- ☒ La ou les menaces ;

- ☑ Le ou les impacts.

A ceux-ci peuvent s'ajouter :

- ☑ Le ou les agents de menace ;
- ☑ La compétence de l'agent de menace ;
- ☑ La motivation de l'agent de menace ;
- ☑ ...



Chaque apprenant proposera un autre exemple.

L'évaluation des risques est un processus cyclique qui consiste à identifier les risques, à préciser leur impact potentiel sur l'entreprise, à recenser les contrôles en place pour les réduire, à évaluer la pertinence de ces contrôles et à déterminer si les risques résiduels sont acceptables par l'entreprise.

Par définition, sans ressource pas de risque. Le gestionnaire de risque doit donc savoir sur quelles éléments il la main, afin de bien dimensionner ses efforts.

En effet, parmi les éléments constitutifs du risque il y en a qui sont interne à l'entreprise et d'autres non. Une bonne compréhension de cette classification peut conduire à une meilleure utilisation des ressources.

Chaque apprenant proposera un tableau avec deux colonnes, dans la première les éléments constitutifs internes du risque, dans la seconde ceux externe à l'entité.



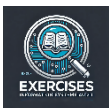
### 1.1.3.3. *Traitement du Risque*

Il existe seulement quatre méthodes pour traiter le risque :

- ☑ l'acceptation ;qui consiste à ne rien faire bien qu'étant pleinement conscient du risque encouru ;
- ☑ l'évitement ou arrêt de l'activité, qui préconise l'extinction de la raison du risque ;
- ☑ le transfert ou partage. Ici l'entité, par le mécanisme contractuel, s'assure de l'intervention d'un tiers pour l'aider le moment échéant à faire face à l'impact ;
- ☑ la réduction ou mitigation. Elle se matérialise par le déploiement de contre-mesure ou l'amélioration de mécanisme de contrôle déjà en place pour agir soit sur la vulnérabilité, soit sur la menace, ou encore sur l'impact ou une combinaison des trois.

A l'issue de l'exécution d'une méthode de traitement du risque, le risque résiduel doit avoir été minimisé.

Par abus de langage, quand on parle de gestion des risques, on entend généralement que la méthode de traitement est déjà choisie et qu'il s'agit de la réduction ou mitigation.



Chaque apprenant proposera un tableau avec deux colonnes, dans la première les méthodes de traitement des risques, dans la seconde trois exemple par méthodes de traitement.

#### 1.1.3.4. Principaux Groupes de Risques Informatiques

Il y a trois (3) principaux groupes de risques en informatique:

- ☑ les risques opérationnels;
- ☑ les risques financiers;
- ☑ les risques légaux ou de non-conformité.

Tableau 1: Quelques risques informatiques et leurs facteurs

Risques informatiques	Facteurs de risques
L'inadéquation du SI avec la stratégie de l'entité et les besoins des utilisateurs	<ul style="list-style-type: none"> <li>☑ manque d'implication de la direction dans la gestion de l'informatique ;</li> <li>☑ absence de schéma directeur ;</li> <li>☑ absence de gouvernance informatique ;</li> <li>☑ manque d'implication des utilisateurs (« bureaux métiers ») dans les projets informatiques ;</li> <li>☑ absence d'analyse de la valeur des SI mis en place.</li> </ul>
L'incapacité de l'organisation à redémarrer les systèmes informatiques en cas arrêt ou destruction	<ul style="list-style-type: none"> <li>☑ absence de sauvegarde régulière du SI (sauvegardes externes) ;</li> <li>☑ absence de plan de secours ;</li> <li>☑ absence de site de secours.</li> </ul>
La sécurité du SI inadaptée au niveau de risque identifié et accepté par la haute direction de l'entité	<ul style="list-style-type: none"> <li>☑ sécurité physique ;</li> <li>☑ sécurité logique ;</li> <li>☑ sécurité du réseau ;</li> <li>☑ sécurité de l'exploitation ;</li> <li>☑ sécurité des PC ;</li> <li>☑ sécurité des données.</li> </ul>
L'accès aux données et aux applications par des personnes non autorisées	<ul style="list-style-type: none"> <li>☑ absence de politique de sécurité ;</li> <li>☑ absence de gestion rigoureuse d'attribution des droits d'accès ;</li> <li>☑ absence de gestion rigoureuse des points d'accès ;</li> <li>☑ systèmes informatiques ne permettant pas une gestion fine des droits d'accès ;</li> <li>☑ gestion des mots de passe insuffisante.</li> </ul>
Les applications informatiques non fiables	<ul style="list-style-type: none"> <li>☑ erreurs dans la programmation des applications par rapport aux spécifications fonctionnelles ;</li> <li>☑ applications insuffisamment testées.</li> <li>☑ utilisateurs insuffisamment impliqués dans les phases de développements de l'application</li> </ul>
L'indisponibilité du système informatique	<ul style="list-style-type: none"> <li>☑ la mauvaise gestion de l'environnement matériel du SI (énergie, climatisation, protection physique, etc.) ;</li> <li>☑ l'absence de convention de service ;</li> <li>☑ l'absence d'outil de surveillance de la disponibilité du SI ;</li> <li>☑ l'absence de cellule réactive en cas d'indisponibilité ;</li> </ul>



Risques informatiques	Facteurs de risques
	<input checked="" type="checkbox"/> l'absence de contrat de maintenance des matériels informatiques.
La mauvaise utilisation du système informatique par les différents utilisateurs	<input checked="" type="checkbox"/> les applications informatiques non conviviales ; <input checked="" type="checkbox"/> les utilisateurs insuffisamment formés ; <input checked="" type="checkbox"/> la documentation utilisateur insuffisante et pas mise à jour ; <input checked="" type="checkbox"/> le manque de contrôles bloquants dans les applications informatiques.
La non-conformité du système informatique avec la législation	<input checked="" type="checkbox"/> les politiques et procédures informatiques non-conformes à la réglementation nationale et/ou internationale en vigueur en matière de : <ul style="list-style-type: none"> <li>○ cyber sécurité ;</li> <li>○ Données personnelles ;</li> <li>○ lutte contre le cyber criminalité ;</li> <li>○ commerce et communications électroniques.</li> </ul>
La non-pérennité du système informatique.	<input checked="" type="checkbox"/> l'utilisation de la sous-traitance informatique sans transfert de compétence en interne ;
L'absence ou la mauvaise de documentation du système	<input checked="" type="checkbox"/> la documentation informatique inexistante ou non mise à jour par suite des évolutions du SI ; <input checked="" type="checkbox"/> l'obsolescence de l'application et/ou de la technologie utilisée ; <input checked="" type="checkbox"/> la forte dépendance vis-à-vis de personnes clés qui peuvent quitter l'entité.

Chaque apprenant proposera un tableau avec trois colonnes, il reprendra les deux premières du tableau ci-haut en rajoutant une troisième pour le groupe de risque (opérationnel, financier ou légaux).

#### 1.1.3.5. *Risques en Audit*

L'informatique ne suffit pas à éliminer les risques, mais constitue un outil important pour mieux les gérer et assurer la synergie de tous les secteurs de l'entreprise, et leur convergence vers un but commun.

Dans le cadre des travaux d'audit, il faut obtenir une assurance raisonnable que les états financiers sont exempts d'inexactitudes importantes.

Un audit ne nécessite pas la validation de la totalité des transactions, l'exhaustivité est difficilement atteignable, d'où l'importance de la gestion des risques en audit.

##### 1.1.3.5.1. *Risque Inhérent*

Le risque inhérent est le risque lié soit à l'activité, soit à l'entité, soit au secteur dans lequel l'entité opère.

##### 1.1.3.5.2. *Risque de Non-contrôle*

Le risque de non-contrôle est fonction de l'efficacité avec laquelle la conception et le fonctionnement du contrôle interne permettent

d'atteindre les objectifs de l'entité. Il subsiste toujours un risque de non-contrôle en raison des limites liées au contrôle interne.

#### 1.1.3.5.3. *Risque de Non-détection*

Le risque de non-détection est le risque que l'auditeur ne détecte pas une inexactitude qui pourrait être importante, soit isolément soit cumulée avec d'autres inexactitudes. Le risque de non-détection est fonction de l'efficacité des procédés d'audit et de leur mise en œuvre par l'auditeur. Il est donc lié à l'auditeur, à son expertise, son expérience, sa compréhension du sujet d'audit et le choix de ses outils.

#### 1.1.3.5.4. *Risque Technologique*

Le risque technologique est lié à l'utilisation des technologies dans le but d'atteindre les objectifs de l'entreprise. Il peut être pris en compte dans le risque de non-détection.

#### 1.1.3.5.5. *Risque de Mission*

C'est le risque que l'auditeur exprime une opinion inappropriée sur les faits examinés contenant des inexactitudes significatives.

Le risque de mission d'audit est représenté par la formule suivante :  
$$RMA = RI \times RNC \times RND$$

- ☒ RMA : Risque de mission d'audit
- ☒ RI : Risque inhérent
- ☒ RNC : Risque de non-contrôle
- ☒ RND : Risque de non-détection



Chaque apprenant proposera deux exemples précis pour chaque type de risques énoncés plus haut.

#### 1.1.3.6. *Matrice des Risques*

##### 1.1.3.6.1. *Rôle et définition*

La matrice des risques est un outil opérationnel de gestion des risques. Elle permet d'avoir sur le même support, des informations utiles à la prise de décision en rapport avec les risques.

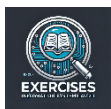
A ce titre, son usage est fortement remandé par les bonnes pratiques et les professionnels en la matière.

##### 1.1.3.6.2. *Contenu d'une Matrice des Risques*

La matrice des risques est un tableau récapitulatif qui met sur le même plan les points suivants :

- ☒ Un numéro d'ordre ;

- ☑ Le domaine ou cycle concerné ;
- ☑ La structure compétente ;
- ☑ Le poste de travail concerné ;
- ☑ Le ou les titulaires du poste de travail sur la période ;
- ☑ Le logiciel utilisé ;
- ☑ La phase ou l'étape du processus visé ;
- ☑ Le point de contrôle évalué ;
- ☑ Le ou les critères d'évaluation ;
- ☑ La ou les questions d'évaluation ;
- ☑ La réponse associée ;
- ☑ Le ou les éléments requis (futurs éléments probants) ;
- ☑ Le risque associé ;
- ☑ La conséquence majeure en cas de réalisation du risque relevé ;
- ☑ La criticité subséquente ; et
- ☑ Un commentaire le cas échéant.



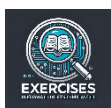
Chaque apprenant proposera une matrice des risques dans un fichier Excel contenant les éléments énumérés supra.

#### 1.1.4. Contrôle Interne

##### 1.1.4.1. Définition du contrôle Interne

Le référentiel COSO définit le contrôle interne comme un processus mis en œuvre par les dirigeants qui couvre tous les niveaux de l'entreprise et est destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants :

- ☑ L'efficacité et l'efficience des opérations ;
- ☑ La fiabilité des informations financières ;
- ☑ La conformité aux lois et règlements.



Chaque apprenant proposera une définition pour les termes suivants : efficacité ; efficience ; fiabilité ; conformité.

##### 1.1.4.2. Généralités sur le contrôle Interne

Le contrôle interne est une notion indispensable pour toutes les entreprises, notamment au niveau managérial. Il s'agit d'un véritable système de sécurité/veille, composé d'un ensemble de méthodes, de règles et de procédures définies par l'entreprise, mais aussi un ensemble de poste de travail et de fonctions présentes dans l'organigramme. Il s'adapte selon la taille et les caractéristiques de chaque entité. Plus la taille de l'entreprise est importante, plus les procédés du contrôle interne devraient être conséquents.

Le contrôle interne vise à avoir la pleine maîtrise de son entreprise et à éviter les erreurs. Il garantit la qualité de la gestion, ainsi que du système mis en place et la bonne utilisation de ses ressources.

Pour le mettre en place, il est nécessaire de posséder une vision claire de l'entité, ce qui passe par la bonne codification des processus de production.

#### 1.1.4.3. *Evaluation du Système de Contrôle Interne*

L'évaluation du système de contrôle interne a pour but de renseigner sur l'état du contrôle interne mis en place par l'entité en lien avec le sujet d'audit, afin d'en accroître la plus-value.

Dans le cadre de l'audit d'un pan de l'entité et non de l'entité au complet, l'auditeur devra réaliser l'abstraction du système de contrôle interne couvert par le mandat.

Le référentiel faisant autorité en matière d'évaluation de système de contrôle interne est le COSO, avec ses cinq (5) composantes et dix-sept (17) principes, qui assure une couverture de bout en bout de l'entreprise.



Chaque apprenant proposera dans la première colonne, les 5 composantes du COSO, et dans la seconde, les 17 principes rangés par composante. Une fois l'exercice fait, dans quelle cellule du tableau ainsi constitué devrait être rangé les bordereaux de transmission utilisés dans l'entité ?

#### 1.1.5. *Règle des Quatre Yeux*

##### 1.1.5.1. *Enoncé*

La première paire d'yeux observe, la seconde peut infirmer, confirmer ou réformer.

##### 1.1.5.2. *Explication*

Un auditeur n'achève jamais un travail seul, quel que soit son niveau d'expertise ou d'expérience. Il a toujours besoin que son travail soit révisé, pour confirmer qu'il ne s'est pas trompé, ou pour indiquer qu'il s'est trompé ou encore pour mettre son travail en perspective.



Chaque apprenant proposera deux exemples d'application de la règle des 4 yeux.

#### 1.1.6. *Allégorie des deux (2) mains*

On peut se servir de ses deux mains pour illustrer ce qu'est l'audit.

Dans la première main, l'auditeur charge le corpus réglementaire dont il se servira .

Dans la seconde il place les faits observés, la pratique sur le terrain.

Puis il place ses deux mains en regard pour en dégager les écarts, différences, éventuels.

### 1.1.7. Trois piliers de l'Audit Interne

L'audit interne repose sur trois piliers qui sont :

- ☑ *La spécification des tâches*, qui veut que ce qu'il y a à faire soit bien défini, précisé et communiqué. Elle se matérialise au niveau de l'agent par la fiche de poste.
- ☑ *La séparation des tâches et fonctions incompatibles*, qui a pour but d'éviter qu'un maillon de la chaîne ne concentre suffisamment de prérogatives pour seul, pouvoir exécuter de bout en bout une procédure. Ce pilier est implémenté en finances publiques au Cameroun par le principe qui stipule qu'un seul individu ne peut pas cumuler à la fois les fonctions d'ordonnateur et comptable public pour la même opération.
- ☑ *Le contrôle réciproque des tâches*, qui précise que le palier supérieur prolonge le travail du palier inférieur en le validant. Ce pilier se matérialise dans l'administration publique notamment par le système de visa hiérarchique sur les documents. C'est aussi le cas dans les divers workflows ou sans la validation explicite du n+1 la procédure n'avance pas.

### 1.1.8. Point de contrôle

#### 1.1.8.1. Définition

Un point de contrôle représente un élément dans la procédure auditée pour lequel l'auditeur souhaiterait obtenir des éclaircissements, en questionnant la conformité au référentiel établi, et en récoltant les éléments d'analyse.

Dans la pratique, si l'on linéarise la procédure à auditer, chaque acteur ou changement de phase peut être matérialisé par un point de contrôle.

Soit la procédure suivante : l'apprenant part du portail de l'école pour la salle de classe. Ici les points de contrôle peuvent être :

- ☑ Le portail ;
- ☑ L'entrée dans le bâtiment ;
- ☑ L'entrée dans la salle de classe.

Chaque apprenant proposera un exemple de procédure et en identifiera les points de contrôle. La procédure doit donner lieu à au moins 4 points de contrôle.



### 1.1.9. Objectif de contrôle

#### 1.1.9.1. Définition

On peut définir un objectif de contrôle comme étant la raison pour laquelle l'auditeur évalue un point de contrôle.

Pour chaque point de contrôle, il y a au moins un objectif de contrôle.

#### 1.1.9.2. Formulation

Il est usuel de formuler les objectifs de contrôle de l'une des façons suivantes :



- ☑ S'assurer que xxxxxxxxxxxx ;
- ☑ Vérifier que xxxxxxxxxxxx .

Pour les points de contrôle identifiés précédemment (point 2.1.7), voici quelques objectif de contrôle:

- ☑ Le portail :  
S'assurer que l'apprenant soit identifié au niveau du portail ;
- ☑ L'entrée dans le bâtiment :  
S'assurer que seuls les apprenants en règle avec la scolarité accèdent au bâtiment ;
- ☑ L'entrée dans la salle de classe :  
Vérifier qu'aucun apprenant n'entre en salle de classe après l'enseignant.



Chaque apprenant proposera un exemple d'objectif de contrôle pour chaque point de contrôle identifié précédemment dans sa propre procédure.

#### 1.1.10. Critère d'évaluation

##### 1.1.10.1. Définition

Les critères d'évaluation sont la matérialisation des jalons dont l'assemblage permet de réaliser l'objectif de contrôle. Il faut donc satisfaire l'ensemble des critères d'évaluation d'un point de contrôle pour que son évaluation soit concluante.

Dans la pratique il faut généralement plusieurs critères d'évaluation par objectif de contrôle.

Pour les objectifs de contrôle identifiés précédemment (point 2.1.8), voici quelques critères d'évaluation :

- ☑ S'assurer que l'apprenant soit identifié au niveau du portail :
  - L'apprenant a une pièce d'identité ;
  - Un vigile est présent à la guérite du portail ;
  - Le vigile dispose de la liste d'apprenants s'étant acquittés de leurs droits académiques ;
  - La liste dont dispose le vigile est à jour;
  - La comparaison entre la pièce d'identité de l'apprenant à la liste à jour dont dispose le vigile est probante.



Chaque apprenant proposera au moins deux exemples de critère d'évaluation pour chaque objectif de contrôle identifié dans son travail précédent.

#### 1.1.11. Question d'évaluation

##### 1.1.11.1. Définition

Les questions d'évaluation permettent de mesurer l'atteinte des objectifs de contrôle en transformant quasi-systématiquement chaque critère d'évaluation

en question libellée de façon univoque et de manière que les réponses soient booléennes.

Pour les objectifs de contrôle identifiés précédemment (point I.1.8.3), voici quelques questions d'évaluation:

- ☑ S'assurer que l'apprenant soit identifié au niveau du portail :
  - L'apprenant a-t-il une pièce d'identité ?
  - Y a-t-il un vigile à la guérite du portail ?
  - Le vigile dispose-t-il d'une liste d'apprenants s'étant acquittés de leurs droits académiques ?
  - Cette liste est-elle à jour ?
  - Le vigile compare-t-il la pièce d'identité de l'apprenant à la liste à jour dont il dispose ?



Chaque apprenant proposera au moins une question d'évaluation par critère d'évaluation identifié dans son travail précédent.

### 1.1.12. Constatation d'Audit

#### 1.1.12.1. Définitions

Plusieurs définitions coexistent dans la littérature, au finish elles renvoient toutes à la même réalité : une constatation d'audit est la consignation du fait observé par l'auditeur, c'est-à-dire un écart en rapport au référentiel utilisé comme *baseline*.

Quoi que peu courant, une constatation d'audit n'est pas toujours un écart négatif. Dans la pratique, sur des points précis, certaines entités performant au-delà de la *baseline* de référence, il s'agit donc là d'écart positif, et par conséquent d'une constatation d'audit positive.

C'est pourquoi la définition consistant à définir la constatation d'audit comme une *violation* d'une norme établie et diffusée n'a pas été retenue ici.

#### 1.1.12.2. Exemples

##### 1.1.12.2.1. Positive

L'équipe de mission a constaté qu'en sus de la règle établie et des bonnes pratiques en la matière qui fixent le nombre de mission d'audit annuelle pour les applications en service à une (1), l'entreprise Lizbiz's en a réalisé trois (3) en 2022.

##### 1.1.12.2.2. Négative

L'équipe de mission a constaté qu'en violation du second pilier de l'audit interne qui grave la séparation des tâches et fonctions incompatibles dans le marbre, repris et surligné par le point 10.3.2 d'ISO 27002 qui interdit le cumul des fonctions d'administrateur de base de données et celui d'administrateur réseau, dans l'entreprise

Lizbiz's, Monsieur BOMBA a régulièrement exercé ces deux fonctions pendant toute la période sous revue.



Chaque apprenant proposera au moins deux exemples pour chaque type de constatation d'audit (négative et positive) en rapport avec la procédure qu'il a formulé supra et sur laquelle il travaille au fil du cours.

#### 1.1.13. *Contradictoire*

Elément « sine qua non » du droit de la défense, il est repris en audit pour donner la possibilité à l'audité de présenter sa version du fait querellé, appuyée d'éléments probants suffisants au regard de constatation dressée par l'auditeur.

Il matérialise l'obligation d'impartialité, et la preuve d'humilité de l'auditeur, qui soumet à l'audité le premier jet de ce qu'il pense avoir établi comme constat, avant sa consignation définitive dans le rapport.

#### 1.1.14. *Observations*

Dans certains types de rapport de mission, notamment ceux d'ISC comme le Contrôle Supérieur de l'Etat, c'est la forme arrêtée pour consigner les travaux d'audit.

Une observation se compose de :

- ☑ Un numéro d'ordre ;
- ☑ L'énoncé de la norme visée ;
- ☑ La constatation d'audit ;
- ☑ Les risques ou conséquences du fait observé ;
- ☑ Le contradictoire ;
- ☑ L'analyse de l'auditeur ;
- ☑ La conclusion sur le fait observé ;
- ☑ La ou les recommandations pour contenir, réparer ou éviter à l'avenir la situation observée.

Cependant il faudra le cas échéant vous conformer à la structure arrêtée par votre entité.

Chaque apprenant proposera au moins deux exemples d'observation complète dont une prenant en compte une des constatations positives précédemment formulées, et l'autre prenant en compte une des constatations négatives précédemment formulées.



#### 1.1.15. *Sur place et sur pièces*

Ce concept revoie au fait que pour réaliser un audit, l'auditeur doit se déplacer physiquement de manière à être présent sur les lieux, y recueillir les pièces justificatives nécessaires puis les traiter en personne et se prononcer sur leur caractère suffisant ou non.

L'audit ne se base donc pas sur des oui-dire ou des allégations non factuelles, même si ces éléments peuvent être utilisés pour ouvrir ou pas des pistes d'audit.

#### 1.1.16. *Aveu de carence*

Lorsque l'audité est sollicité sur un fait pour en apporter une explication complémentaire à celle de l'équipe de mission et ne se manifeste pas, cette dernière peut conclure à l'aveu de carence après avoir fait la preuve que l'audité a été relancé sur le querellé fait plusieurs fois, par tout moyen laissant trace, et n'a pas réagi.

L'aveu de carence signifie donc l'acceptation tacite par l'audité du fait qui est porté à son attention. C'est donc une exception au principe du contradictoire.

## 1.2. Définitions, Concepts et Bases des Systèmes d'Information

### 1.2.1. *Notion de système*

Plusieurs définitions coexistent dans la littérature, certaines à la limite l'antinomisme.

Simplement dit, dans le cadre de ce cours, un système sera considéré comme étant un groupe d'éléments interagissant ensemble pour rendre un résultat prédictible.



Chaque apprenant proposera au moins une définition du mot prédictible. Par la suite il donnera un exemple de résultat prédictible de la procédure qu'il a défini au début du cours et sur laquelle il travaille.

### 1.2.2. *Les Systèmes d'Information*

#### 1.2.2.1. *Système informatique*

Représente l'ensemble des logiciels et matériels informatiques participant à l'acquisition, au stockage, au traitement, au transport et à la diffusion de l'information sous forme électronique au sein de l'organisation.

#### 1.2.2.2. *Système d'information*

Ensemble des ressources humaines, matérielles, logicielles et procédurales participant à l'acquisition, au stockage, au traitement, au transport et à la diffusion de l'information sous toutes ses formes au sein de l'organisation.

Il s'agit d'un système sociotechnique composé de deux sous-systèmes, l'un social et l'autre technique. Le sous-système social est composé de la structure organisationnelle et des personnes liées au SI. Le sous-système technique est composé des technologies (hardware, software et équipements de télécommunication) et des processus d'affaires concernés par le SI.

#### 1.2.2.3. *Fonction informatique*

La fonction informatique comprend, outre le système informatique, les personnes, processus, ressources financières et informationnelles. Elle a pour but de fournir à l'entreprise les éléments nécessaires à la réalisation optimale de ses missions.

#### 1.2.2.4. *Fonction d'information*

Ensemble organisé de personnes, de procédures et d'équipement qui a pour objet de réunir, de trier, d'analyser, d'évaluer et de distribuer, en temps utile, de l'information pertinente et valide, provenant de sources internes et externes à l'organisation, afin que tous ceux qui ont à prendre des décisions disposent des éléments leur permettant de choisir l'action la plus appropriée au moment adéquat.

#### 1.2.2.5. *Problèmes inhérents aux SI*

Comme tous les systèmes, les SI peuvent être sujets à des problèmes liés soit à l'agencement des éléments qui le constituent soit aux fonctions qu'il fournit, ou une combinaison des deux. Tous les problèmes inhérents au SI peuvent donc en absolu se classer dans l'une ces catégories.

#### 1.2.2.6. *Informatisation des SI*

Tous les systèmes d'information ne sont ni informatisés ni informatisable. L'informatisation d'un système d'information est une phase critique de sa vie.

Des préalables doivent être respectés, comme :

- ☒ la définition claire et précise du but et des objectifs de l'informatisation ;
- ☒ les termes de références de son informatisation qui reprennent la définition du besoin, le périmètre des travaux, une certaine vision du futur système, les délais de réalisation, et les autres contraintes connexes, pour ne citer que ça ;
- ☒ l'allocation des ressources pour le projet d'informatisation, notamment matérielles, humaines et financières.
- ☒ Etc...

Chaque apprenant proposera un autre exemple.

L'informatisation d'un système d'information est donc un projet à traiter comme tel, dans le strict respect des usages et bonnes pratiques en la matière.

#### 1.2.2.7. *Types de migration/changement de SI*

Il existe trois (3) grands types de changement de système, le changement direct, le changement par étape et le changement en parallèle.



Ces différents type de changement sont présentés dans le tableau ci-contre.

Tableau 2: Différents types de migration de système

N°	Type de changement	Avantages majeurs	Inconvénients majeurs
1	Direct	Rapidité d'exécution	Aucun retour arrière possible
2	Par étape	<input checked="" type="checkbox"/> Possibilité de retour arrière si une étape se passe mal ; <input checked="" type="checkbox"/> Assimilation progressive du nouveau système brique par brique.	<input checked="" type="checkbox"/> Temps relativement long de mise en œuvre ; <input checked="" type="checkbox"/> Ressource en infrastructure requise pour supporter les deux systèmes.
3	En parallèle	<input checked="" type="checkbox"/> Temps d'apprentissage suffisant du nouveau système ; <input checked="" type="checkbox"/> Comparaison poussée des deux systèmes ; <input checked="" type="checkbox"/> Possibilité de basculer en tant que de besoin vers le système le plus avantageux.	Ressources requises pour faire tourner les deux systèmes simultanément.

Pour chacun de ces types de migration, l'auditeur devra recueillir la documentation et observer comment et si les règles inhérentes à la migration de système ont été respectées, notamment :

- ☒ L'exhaustivité du transfert des données de l'ancien vers le nouveau système ;
- ☒ La convertibilité des données le cas échéant ;
- ☒ L'intégrité des données au moment de leur transfert ;
- ☒ La préservation de la confidentialité des données ;
- ☒ L'exactitude ou la convergence des résultats du nouveau système ;
- ☒ La préservation des principes de séparation de tâches et fonctions incompatibles ;
- ☒ ...



Chaque apprenant proposera un autre exemple.

### 1.2.3. Système d'exploitation

Un système d'exploitation est un logiciel constitué de plusieurs fonctions dont le rôle est la gestion du matériel informatique qui constitue son hôte et les logiciels qui y sont installés.

Il est encore appelé logiciel de base, car les autres logiciels sont installés par-dessus lui.

Microsoft est le constructeur du célèbre système d'exploitation Windows, dont quelques déclinaisons sont : Windows XP ; Windows 10 ; Windows 11.

#### 1.2.4. Système de fichier

Un système de fichier décrit la façon dont le système d'exploitation organise la gestion des éléments sur un support physique (disque dur, disque amovible, clé USB).

FAT ; FAT 32 ; NTFS ; sont des systèmes de fichiers Windows.

#### 1.2.5. Fichiers

Un fichier est la matérialisation du stockage sur support physique des données suivant un format défini dans le système de fichier.

A chaque fichier est associé un logiciel particulier pour sa lecture et modification, le lien entre les deux se fait par une extension. On peut classer les fichiers par leur taille, leur extension ou leur nom, ou leur date de modification.

A titre d'exemple, Word ; le traitement de texte vu précédemment, ouvre en standard les fichiers d'extension « .doc » et « .docx », pour Excel ce sont les fichiers d'extensions « .xls ».



Chaque apprenant proposera au moins quatre applications et leurs extensions associées.

#### 1.2.6. Base de données

Une base de données est une collection organisée de données structurées, généralement stockées électroniquement dans un système informatique. Ainsi, une base de données peut se concevoir comme un classeur électronique qui contient des tiroirs et leurs contenus.

Les bases de données sont de plusieurs types, les plus répandus étant objet et relationnel.

C'est le Système de Gestion de Base de Données (SGBD) qui gère et contrôle la base de données.



Chaque apprenant proposera au moins un nom de SGBD et son type.

#### 1.2.7. Réseau informatique

Un réseau informatique est un système constitué de matériel et logiciel informatique interagissant entre eux pour acheminer des données.



Chaque apprenant proposera au moins deux topologies de réseaux différentes, avec ses avantages et ses inconvénients.

### 1.2.8. Sécurité informatique

La sécurité informatique peut se définir comme un ensemble constitué de moyens humains, matériels, procéduraux et financiers mis en œuvre dans le but de garantir l'intégrité, la disponibilité et la confidentialité des informations traitées, stockées, et acheminées aux moyens d'outils et de procédés informatiques.



Chaque apprenant proposera au moins une différence entre sécurité informatique et cybersécurité, si elle existe.

## 1.3. Les Contrôles en Audit des Systèmes d'Information

### 1.3.1. Rôle

Simplement dit, le rôle d'un contrôle est de s'assurer du respect d'une règle connue, établie et précise, avant la réalisation ou non d'une action subséquente.

### 1.3.2. Point de contrôle

Cet élément a été traité plus en détail à la section 1.1.8

### 1.3.3. Contrôles dans les SI

Lors de l'audit des SI, deux catégories majeures de contrôles sont évaluées : les contrôles généraux des systèmes d'information et les contrôles d'application. Ces deux types de contrôles agissent de manière complémentaire mais divergent dans leur portée et leur approche. Ce chapitre aborde en détail les caractéristiques, les complémentarités et les divergences de ces deux types de contrôles, en illustrant chaque section avec des exemples concrets adaptés à une entreprise publique (mais pas que), et en présentant une section spécifique sur l'évaluation des contrôles.

#### 1.3.3.1. Contrôles généraux

##### 1.3.3.1.1. Définition et objectif

Les contrôles généraux des systèmes d'information (General IT Controls ou GITC) concernent l'environnement informatique global d'une organisation. Ils sont mis en place pour garantir que l'infrastructure informatique est gérée de manière sécurisée et fiable. Ces contrôles sont transversaux et s'appliquent à l'ensemble des systèmes et applications informatiques, assurant ainsi une base stable pour leur bon fonctionnement.

- ☑ La validation d'une liasse comme étant propre à la saisie dans le système, après s'être assuré de l'exhaustivité des pièces la constituant, ainsi que de leur authenticité.
- ☑ La société Lizbiz's utilise plusieurs serveurs pour héberger ses systèmes de gestion agricole et commerciale. Les contrôles généraux vont s'assurer que ces serveurs sont protégés contre les accès non autorisés, que les mises à jour de sécurité sont régulièrement



effectuées, et que des procédures de sauvegarde sont en place en cas de défaillance matérielle ou d'incident informatique.



Chaque apprenant proposera un autre exemple de contrôle général.

#### 1.3.3.1.2. *Quelques champs d'application*

Les contrôles généraux incluent plusieurs domaines critiques pour la sécurité et la gestion des systèmes d'information notamment:

##### 1.3.3.1.2.1. *Sécurité des systèmes et gestion des accès*

Ce contrôle vise à s'assurer que seuls les utilisateurs autorisés ont accès aux systèmes d'information. Il implique des mesures de protection comme les mots de passe robustes, l'authentification multi-facteurs (MFA), et une gestion stricte des autorisations d'accès.

La société Lizbiz's met en place une politique de mots de passe obligeant les employés à changer leur mot de passe tous les 90 jours, avec des exigences de complexité (majuscules, minuscules, chiffres, caractères spéciaux). De plus, l'accès aux systèmes critiques de gestion des stocks ou des ressources humaines nécessite une authentification par application mobile en plus du mot de passe.



Page 31 sur 227



##### 1.3.3.1.2.2. *La gestion des changements*

Les processus de gestion des changements sont mis en place pour garantir que toutes les modifications apportées aux systèmes informatiques (comme les mises à jour logicielles ou les changements d'infrastructure) sont correctement planifiées, testées et approuvées. Cela permet de minimiser les risques de perturbation des systèmes.

Avant de déployer une nouvelle version du logiciel de gestion de la production cotonnière, l'équipe informatique de la société Lizbiz's suit une procédure formelle qui inclut des tests en environnement de pré-production, l'approbation du responsable IT, et une communication aux utilisateurs concernés sur les nouvelles fonctionnalités et les éventuels impacts.



##### 1.3.3.1.2.3. *La gestion des opérations informatiques*

Les opérations quotidiennes des systèmes informatiques doivent être surveillées pour assurer leur continuité. Cela inclut des contrôles sur les sauvegardes régulières, la gestion des incidents, et la planification de la maintenance.

La société Lizbiz's effectue des sauvegardes automatiques de ses bases de données commerciales chaque nuit. De plus, un système de surveillance en temps réel alerte l'équipe IT en cas de panne de serveur ou de ralentissement des performances.



#### 1.3.3.1.2.4. Plans de continuité des activités et reprise après sinistre

Le premier prévoit un ensemble de mécanismes pour s'assurer que les services identifiés et catégorisés comme critiques pour l'entreprise continuent d'être fonctionnels quel que soit l'incident, tandis que le second prévoit la restauration, à l'état normal, des systèmes d'information en cas d'incident majeur. L'objectif restant le même : minimiser les interruptions des activités critiques.

La société Lizbiz's héberge une copie de ses serveurs critiques dans un centre de données secondaire situé dans une autre région du Cameroun. En cas de catastrophe naturelle ou d'incident affectant le site principal, les opérations peuvent être basculées vers ce site de secours avec un temps d'interruption minimal.



#### 1.3.3.2. Contrôles d'application

##### 1.3.3.2.1. Définition et objectif

Les contrôles d'application sont quant à eux une transcription informatique des précédents. Encore appelés contrôles programmés, ils sont encodés au moyen de programmes informatiques dans les logiciels pour matérialiser l'existence d'une règle. Ils sont fréquents dans les opérations d'entrée, de traitement et de sortie de l'application. Leur objectif est de garantir l'intégralité, la fiabilité et l'exactitude du traitement des données. Contrairement aux contrôles généraux, les contrôles d'application se concentrent sur les processus métiers et les transactions spécifiques traités dans les applications informatiques.

- ☑ Le contrôle de conformité de la casse et du nombre de caractères d'un mot de passe par le système, avant de l'accepter comme bon.
- ☑ Dans le logiciel de gestion des approvisionnements de la société Lizbiz's, un contrôle d'application s'assure que les commandes de fournitures sont correctement validées en fonction des besoins exprimés et des budgets alloués, avant que les bons de commande ne soient générés et transmis aux fournisseurs.

Chaque apprenant proposera un autre exemple de contrôle d'application.

##### 1.3.3.2.2. Quelques champs d'application

Les contrôles d'application se focalisent sur différents aspects du traitement des données et des transactions au sein des systèmes :

##### 1.3.3.2.2.1. Contrôles d'entrée de données

Ces contrôles s'assurent que les données saisies dans les systèmes d'information sont exactes, complètes, et conformes aux règles et aux formats établis. Ils visent à réduire les erreurs dès la saisie.





Dans le système de gestion des récoltes de la Lizbiz's, un contrôle empêche l'enregistrement d'une nouvelle livraison de coton si les informations sur le poids et la qualité ne sont pas correctement renseignées, évitant ainsi des enregistrements incomplets ou erronés qui pourraient affecter la gestion des stocks.

#### 1.3.3.2.2.2. *Contrôle de traitement de données*

Ils vérifient que les transactions sont correctement exécutées selon les règles métier prédéfinies. Par exemple, ces contrôles peuvent s'assurer qu'une facture ne sera émise que si la commande correspondante a été validée.



Dans le système de facturation de la société Lizbiz's, un contrôle d'application empêche la génération d'une facture tant que la livraison n'a pas été confirmée dans le système et que toutes les étapes de validation n'ont pas été suivies.

#### 1.3.3.2.2.3. *Contrôle de sortie de données*

Ils garantissent que les informations générées par les systèmes (comme les rapports financiers ou les états de gestion) sont exactes, complètes, et conformes aux attentes.



Avant la génération des rapports financiers trimestriels à la Lizbiz's, des contrôles automatisés vérifient la cohérence entre les différents comptes de dépenses, de production et de vente, détectant ainsi toute anomalie ou divergence qui nécessiterait une investigation.

#### 1.3.3.2.2.4. *Contrôle d'accès spécifiques aux applications*

Ils s'assurent que seules les personnes habilitées peuvent effectuer certaines actions sensibles dans les applications, comme la validation de paiements ou la modification de données critiques.



Dans le système de gestion des ressources humaines de la société Lizbiz's, seuls les gestionnaires des paies peuvent approuver les versements salariaux, et chaque approbation est enregistrée avec un horodatage et l'identifiant de l'utilisateur pour des raisons de traçabilité.

### 1.3.3.3. *Complémentarité entre contrôles généraux et contrôles d'application*

#### 1.3.3.3.1. *Interdépendance fonctionnelle*

Les contrôles généraux créent un environnement sécurisé et stable, qui permet aux contrôles d'application de fonctionner efficacement. Par exemple, un contrôle général de gestion des accès garantit que seuls les utilisateurs autorisés peuvent interagir avec une application spécifique. De même, un contrôle général de gestion des changements

prévient les erreurs ou les pannes systémiques qui pourraient affecter les applications.



Si les serveurs de La société Lizbiz's sont correctement sécurisés (contrôle général), cela protège les applications hébergées contre les accès non autorisés. Ensuite, au sein de l'application de gestion des approvisionnements, les contrôles d'application s'assurent que seuls les employés autorisés peuvent valider les commandes ou effectuer des modifications dans les données critiques.

#### 1.3.3.3.2. *Sécurisation renforcée*

Les contrôles généraux protègent l'infrastructure informatique et l'environnement global, tandis que les contrôles d'application s'assurent que les processus métier spécifiques sont correctement exécutés. Par exemple, une application de gestion financière pourrait bénéficier de contrôles d'application qui valident les transactions, tandis que les contrôles généraux garantissent que l'accès à cette application est sécurisé et que les modifications du système sont correctement gérées.

Lors d'un audit de la société Lizbiz's, il a été constaté que bien que le système de gestion des ressources humaines ait des contrôles d'application solides pour valider les congés des employés, une faiblesse dans les contrôles généraux de gestion des accès a permis à un utilisateur non autorisé d'accéder au système et de modifier des données sensibles. Cela démontre l'importance de la complémentarité des deux types de contrôles.

#### 1.3.3.3.3. *Prévention des erreurs à différents niveaux*

Les contrôles généraux sont préventifs à un niveau global, évitant les erreurs systémiques et les failles de sécurité à grande échelle. Les contrôles d'application se concentrent sur la prévention des erreurs spécifiques aux transactions ou aux processus métier. Par exemple, des contrôles d'entrée de données empêchent les erreurs de saisie dans une application spécifique, tandis que des contrôles généraux assurent que le système qui héberge cette application reste sécurisé et opérationnel.

Un contrôle général au niveau de La société Lizbiz's assure que les mises à jour de sécurité des systèmes sont appliquées régulièrement, protégeant ainsi contre les vulnérabilités connues. Parallèlement, un contrôle d'application veille à ce que les calculs de taxes dans le logiciel de facturation soient mis à jour conformément aux changements de législation.



### 1.3.4. *Divergences entre contrôles généraux et contrôles d'application*

#### 1.3.4.1. *Portée*

Les contrôles généraux s'appliquent à l'ensemble des systèmes et des infrastructures informatiques de la société Lizbiz's. Ils touchent des aspects





comme la sécurité globale, la gestion des accès, et la gestion des changements dans tous les systèmes.



La politique de sécurité réseau de la société Lizbiz's interdit l'utilisation de clés USB sur les ordinateurs de l'entreprise pour prévenir la fuite de données ou l'introduction de logiciels malveillants.

Les contrôles d'application, en revanche, sont spécifiques à des logiciels ou à des systèmes particuliers. Ils se concentrent sur des processus métier bien définis et sur le traitement des transactions dans ces systèmes.



Dans le système de gestion des achats de la société Lizbiz's, un contrôle empêche la création d'une commande fournisseur si le montant dépasse le budget alloué sans approbation supplémentaire.

#### 1.3.4.2. Focalisation

Les contrôles généraux se focalisent sur la gestion et la sécurité de l'infrastructure informatique. Ils concernent la performance globale des systèmes et l'intégrité de l'environnement informatique.



La mise en place d'un pare-feu à l'échelle de La société Lizbiz's pour contrôler le trafic réseau entrant et sortant, protégeant ainsi tous les systèmes connectés.

Les contrôles d'application sont centrés sur les processus métier et les transactions spécifiques. Ils vérifient que les données sont correctement traitées dans des applications précises.



Dans le système de gestion des ressources humaines de la Lizbiz's, un contrôle empêche l'enregistrement d'un salaire en dehors de la fourchette salariale prédéfinie pour un poste donné.

#### 1.3.4.3. Approche proactive vs réactive

Les contrôles généraux sont principalement proactifs. Ils visent à prévenir les incidents et à garantir que l'infrastructure informatique est sécurisée et stable avant que des problèmes ne surviennent.



L'installation de logiciels antivirus sur tous les postes de travail et serveurs de La société Lizbiz's pour prévenir les infections par des logiciels malveillants.

Les contrôles d'application peuvent être à la fois proactifs et réactifs. Ils préviennent les erreurs dans les transactions, mais ils détectent également les anomalies ou les erreurs après qu'elles se sont produites.



Un contrôle dans le système financier de La société Lizbiz's alerte l'administrateur si une transaction financière inhabituelle est détectée, permettant une enquête et une action corrective si nécessaire.

## 1.4. Evaluation des Connaissances

### 1.4.1. QCM

- 1) **Lequel des éléments suivants constitue un système d'information ?**
  - a) Un ordinateur
  - b) Un ensemble de processus, personnes et outils
  - c) Un logiciel de gestion uniquement
  - d) Un disque dur uniquement
- 2) **Qu'est-ce qu'un système informatique ?**
  - a) Une partie du système d'information consacrée à l'analyse
  - b) Un ensemble de matériels et de logiciels
  - c) Une entité socio-technique complexe
  - d) Un réseau isolé
- 3) **Quelle est la principale différence entre système d'information et système informatique ?**
  - a) Le système informatique intègre les données humaines
  - b) Le système d'information inclut des aspects organisationnels
  - c) Le système informatique n'a pas d'aspect technique
  - d) Les deux sont strictement identiques
- 4) **Quel est un exemple de contrôle général des systèmes d'information ?**
  - a) Validation des saisies dans une application
  - b) Gestion des accès
  - c) Calcul automatisé des taxes
  - d) Reporting trimestriel automatisé
- 5) **Quel est le rôle principal d'un point de contrôle ?**
  - a) Valider les opérations commerciales
  - b) Assurer l'intégrité des processus
  - c) Détecter des écarts dans les rapports financiers
  - d) Superviser la stratégie de l'entreprise
- 6) **Parmi les méthodes suivantes, laquelle est considérée comme un type de migration de système ?**
  - a) Migration inversée
  - b) Migration en parallèle
  - c) Migration en tandem
  - d) Migration en alternance
- 7) **Une migration en parallèle a pour principal avantage :**
  - a) Une rapidité d'exécution
  - b) La possibilité de retour en cas de problème
  - c) Une réduction des coûts d'infrastructure
  - d) Un apprentissage rapide des utilisateurs
- 8) **Dans un système d'information, le sous-système technique comprend :**
  - a) Les processus d'affaires
  - b) Les équipements matériels et logiciels
  - c) Les utilisateurs
  - d) La structure organisationnelle
- 9) **Lequel des éléments suivants est un exemple de ressource humaine dans un système d'information ?**
  - a) Un ordinateur
  - b) Un administrateur réseau

- c) Un logiciel de gestion
- d) Un plan de sauvegarde

10) **La notion de gouvernance des systèmes d'information se réfère principalement :**

- a) À la gestion des matériels informatiques
- b) À la stratégie et à l'organisation des SI pour atteindre les objectifs de l'entreprise
- c) À la mise en place de logiciels
- d) À la réparation des pannes techniques

11) **Un système d'information performant doit :**

- a) Réduire le nombre d'utilisateurs
- b) Optimiser la prise de décision
- c) Supprimer tous les systèmes informatiques
- d) Être isolé des autres systèmes

12) **Quel est le rôle d'un référentiel comme COBIT dans un audit de SI ?**

- a) Fournir une documentation légale
- b) Définir des bonnes pratiques pour la gouvernance et la gestion des SI
- c) Remplacer les outils de gestion
- d) Détecter automatiquement les anomalies techniques

13) **Dans un audit de SI, une matrice des risques est utilisée pour :**

- a) Hiérarchiser les risques identifiés
- b) Élaborer des états financiers
- c) Configurer les logiciels de sauvegarde
- d) Automatiser les processus métier

14) **La migration en big bang présente l'inconvénient majeur de :**

- a) Nécessiter peu de planification
- b) Risquer une interruption complète des opérations en cas d'échec
- c) Être plus coûteuse que les autres méthodes
- d) Ne pas inclure de tests avant la migration

15) **L'intégrité des données dans un système d'information signifie que :**

- a) Les données sont disponibles en permanence
- b) Les données sont cohérentes, précises et fiables
- c) Les données sont sauvegardées quotidiennement
- d) Les utilisateurs ont un accès illimité

16) **Quelle est la première étape d'une démarche d'audit ?**

- a) La collecte des preuves
- b) La définition des objectifs et du périmètre
- c) L'élaboration du rapport final
- d) La mise en œuvre des contrôles correctifs

17) **Dans un audit, un risque inhérent se définit comme :**

- a) Un risque qui subsiste après la mise en place des contrôles
- b) Un risque existant avant tout contrôle
- c) Un risque lié à la non-conformité réglementaire
- d) Un risque de fraude uniquement

18) **Une documentation complète dans un système d'information est cruciale pour :**

- a) Faciliter la prise de décision stratégique
- b) Garantir la continuité des activités en cas de panne
- c) Réduire le nombre de serveurs nécessaires
- d) Accélérer le développement des nouvelles fonctionnalités

19) **Le modèle d'audit basé sur les risques vise à :**

- a) Inspecter chaque transaction individuelle
- b) Identifier et prioriser les zones de risques majeurs

- c) Remplacer les procédures standards par des outils automatisés
- d) Réduire les coûts en supprimant des étapes

**20) Le principal objectif d'un contrôle d'application est de :**

- a) Vérifier l'intégrité des processus techniques
- b) Valider les transactions automatisées
- c) Superviser les utilisateurs
- d) Sauvegarder les données sensibles

**21) Un audit interne de SI est principalement destiné à :**

- a) Identifier les faiblesses internes avant un audit externe
- b) Remplacer les procédures opérationnelles
- c) Répondre directement aux régulateurs
- d) Supprimer les risques techniques

**22) Un exemple de contrôle préventif dans un SI est :**

- a) La mise en place d'un pare-feu
- b) La vérification d'une facture après traitement
- c) La correction d'une erreur dans une base de données
- d) L'exécution d'un test de reprise après sinistre

**23) Un contrôle correctif a pour but de :**

- a) Identifier les causes d'une panne
- b) Réparer ou minimiser les impacts d'un problème détecté
- c) Empêcher les erreurs avant leur survenue
- d) Surveiller les transactions en temps réel

**24) La confidentialité dans un système d'information garantit que :**

- a) Les données sont accessibles à tous les employés
- b) L'accès aux données est limité aux personnes autorisées
- c) Les données sont sauvegardées quotidiennement
- d) Les données sensibles sont supprimées après utilisation

**25) Une stratégie efficace pour garantir la disponibilité d'un SI est :**

- a) Limiter l'accès des utilisateurs
- b) Mettre en œuvre un plan de continuité d'activité
- c) Sauvegarder uniquement les données critiques
- d) Automatiser tous les processus manuels

### *1.4.2. Questions à Trous*

Complétez chaque phrase avec le terme ou la notion appropriée.

- 1) Un système \_\_\_\_\_ se compose de matériels, logiciels et procédures collaborant pour traiter l'information.
- 2) La migration \_\_\_\_\_ permet de revenir à un ancien système si des problèmes surviennent lors du déploiement.
- 3) Le \_\_\_\_\_ est une ressource fondamentale d'un système d'information, incluant ses structures organisationnelles.
- 4) Les points de contrôle sont essentiels pour assurer \_\_\_\_\_ au sein des processus définis.

- 5) Un audit informatique est principalement réalisé pour évaluer \_\_\_\_\_ et conformité des systèmes.
- 6) Le rôle d'un \_\_\_\_\_ est de garantir que seuls les utilisateurs autorisés accèdent aux systèmes critiques.
- 7) Le \_\_\_\_\_ est un référentiel clé utilisé pour la gouvernance et le management des systèmes d'information.
- 8) Un contrôle \_\_\_\_\_ vise à empêcher les erreurs ou incidents avant qu'ils ne surviennent.
- 9) La \_\_\_\_\_ des données garantit qu'elles sont accessibles uniquement aux personnes autorisées.
- 10) Le \_\_\_\_\_ est un outil essentiel pour identifier les zones de risques majeurs dans un SI.
- 11) Un \_\_\_\_\_ dans un SI garantit la reprise rapide des activités en cas de sinistre.
- 12) La migration \_\_\_\_\_ implique un basculement complet vers un nouveau système sans période de chevauchement.
- 13) Un système d'information est performant lorsqu'il améliore \_\_\_\_\_ au sein de l'organisation.
- 14) Le \_\_\_\_\_ des données signifie qu'elles sont fiables et exactes à tout moment.
- 15) La \_\_\_\_\_ est la première étape d'une démarche d'audit, permettant de fixer le cadre et les objectifs.
- 16) Les \_\_\_\_\_ sont des outils utilisés pour documenter et formaliser les procédures dans un SI.
- 17) Une documentation complète dans un SI permet de garantir \_\_\_\_\_ en cas de défaillance.
- 18) L'accès aux données est limité par des \_\_\_\_\_ qui contrôlent les droits des utilisateurs.
- 19) Un audit basé sur les \_\_\_\_\_ se concentre sur les zones ayant le plus fort impact potentiel.
- 20) Les \_\_\_\_\_ permettent de valider les transactions et processus automatisés dans un SI.

#### 1.4.3. Questions Ouvertes

- 1) Expliquez la différence entre un système informatique et un système d'information. Donnez un exemple concret pour illustrer votre réponse.
- 2) Quels sont les principaux éléments constitutifs d'un système d'information ? Expliquez leur rôle respectif.

- 3) En quoi la migration en parallèle est-elle différente de la migration en big bang ? Citez un avantage et un inconvénient de chaque méthode.
- 4) Pourquoi la gouvernance des systèmes d'information est-elle essentielle pour une organisation moderne ? Donnez un exemple d'impact positif.
- 5) Décrivez le rôle d'un administrateur réseau dans un système d'information. Quels sont les risques liés à une mauvaise gestion des accès ?
- 6) Quels sont les avantages d'une documentation complète et à jour dans un système d'information ? Expliquez en quoi cela facilite l'audit.
- 7) Donnez un exemple d'application de la confidentialité dans un système d'information. Quels contrôles peuvent être mis en place pour la garantir ?
- 8) Expliquez ce qu'est une matrice des risques et comment elle est utilisée dans l'audit des systèmes d'information.
- 9) Quels sont les principaux contrôles préventifs dans un système d'information ? Donnez un exemple pratique.
- 10) Pourquoi l'intégrité des données est-elle essentielle ? Citez un cas concret d'impact lié à une perte d'intégrité des données.
- 11) Quel est l'objectif principal de la définition du périmètre dans une mission d'audit ? Expliquez comment cette étape contribue à la réussite de l'audit.
- 12) Quelles sont les conséquences possibles d'une migration informatique mal planifiée ? Donnez des recommandations pour les éviter.
- 13) Comment la mise en place de droits d'accès bien définis contribue-t-elle à la sécurité d'un système d'information ?
- 14) Décrivez un scénario où un audit basé sur les risques permet d'identifier des faiblesses critiques dans un système d'information.
- 15) Quels sont les éléments à prendre en compte lors de la rédaction d'un plan de continuité d'activité ? Pourquoi est-il important ?
- 16) Quelles bonnes pratiques recommanderiez-vous pour garantir la disponibilité d'un système d'information en cas de panne majeure ?
- 17) Expliquez comment un contrôle d'application fonctionne pour garantir la validité des transactions. Donnez un exemple concret.
- 18) En quoi le cadre COBIT est-il utile pour la gouvernance des systèmes d'information ? Donnez un exemple d'application pratique.
- 19) Comment une organisation peut-elle évaluer l'efficacité de ses contrôles préventifs ?
- 20) Pourquoi est-il important de hiérarchiser les risques identifiés lors d'un audit ? Citez un outil utilisé pour cela.
- 21) Expliquez le concept de migration progressive et comment il peut réduire les risques liés à une transformation systémique.

- 22) Quels sont les avantages et inconvénients de l'externalisation de la gestion des systèmes d'information ?
- 23) Comment un SI peut-il aider une organisation à se conformer aux réglementations telles que le RGPD ?
- 24) Quels sont les éléments clés à vérifier dans un audit de la gestion des sauvegardes d'un système d'information ?
- 25) Expliquez en quoi la standardisation des processus peut améliorer la qualité d'un système d'information.
- 26) Quels sont les principaux éléments d'une stratégie de reprise après sinistre pour un SI ?
- 27) Comment la transformation numérique impacte-t-elle les systèmes d'information des organisations ?
- 28) Quelles sont les conséquences d'un audit insuffisant sur la sécurité d'un SI ?
- 29) Pourquoi est-il crucial de tester régulièrement les plans de continuité d'activité ?
- 30) Quels outils ou technologies recommanderiez-vous pour renforcer la surveillance des systèmes d'information ?
- 31) Comment un tableau de bord SI peut-il aider les décideurs à suivre les performances des systèmes d'information ?
- 32) Quels sont les avantages d'utiliser une plateforme cloud pour un système d'information ? Quels risques doivent être pris en compte ?
- 33) Comment un audit interne diffère-t-il d'un audit externe pour les systèmes d'information ?
- 34) Expliquez pourquoi la formation des utilisateurs est essentielle pour réduire les risques dans un SI.
- 35) Quels sont les indicateurs clés de performance (KPI) couramment utilisés pour évaluer un SI ?
- 36) En quoi l'automatisation des contrôles peut-elle améliorer l'efficacité d'un SI ?
- 37) Pourquoi la segmentation du réseau est-elle une bonne pratique de sécurité dans les SI ?
- 38) Comment la gestion des identités et des accès (IAM) contribue-t-elle à la sécurité d'un SI ?
- 39) Quels sont les principaux rôles et responsabilités d'une équipe d'audit informatique ?
- 40) Pourquoi est-il important de réaliser un audit des contrats liés aux prestataires de SI ?
- 41) En quoi la virtualisation peut-elle simplifier la gestion des ressources d'un SI ?
- 42) Quels risques sont associés à l'utilisation de logiciels non licenciés dans un SI ?
- 43) Comment l'intelligence artificielle peut-elle améliorer la gestion des systèmes d'information ?
- 44) Quels sont les impacts d'un manque de maintenance préventive sur un SI ?



45) Expliquez comment la mise en place d'une charte informatique peut améliorer l'utilisation des systèmes d'information dans une organisation.

#### 1.4.4. Cas pratique

##### Énoncé :

Une PME spécialisée dans la distribution de fournitures de bureau, nommée **Lizbiz's**, souhaite optimiser et sécuriser son système d'information. Le système en place gère les commandes clients, les stocks, les factures et les rapports financiers. Toutefois, plusieurs problèmes récurrents ont été identifiés:

- 1) Les différents processus (commandes, gestion des stocks, facturation) ne sont pas coordonnés, ce qui cause des retards dans le traitement des commandes.
- 2) Les utilisateurs signalent des difficultés à accéder aux informations critiques en raison d'un manque d'organisation dans la gestion des données.
- 3) Les documents financiers contiennent des incohérences dues à des erreurs de saisie non détectées.
- 4) La direction n'a pas de vision claire sur les performances du système faute d'indicateurs clés.

L'objectif est de réaliser un audit pour analyser la situation et proposer des améliorations concrètes basées sur les concepts fondamentaux du Livre 1.

##### Questions :

- 1) Quels éléments doivent être analysés en priorité pour comprendre les retards dans le traitement des commandes ?
- 2) Comment peut-on optimiser la coordination entre les processus de commande, gestion des stocks et facturation ?
- 3) Quels types de systèmes d'information recommanderiez-vous pour structurer la gestion des données dans cette PME ?
- 4) Quelles méthodes peut-on utiliser pour identifier et corriger les incohérences dans les documents financiers ?
- 5) Quels outils recommanderiez-vous pour garantir une saisie des données fiable et cohérente ?
- 6) Proposez des indicateurs de performance (KPI) clés pour aider la direction à suivre les performances du système d'information.
- 7) Comment un système d'information bien organisé peut-il améliorer l'efficacité globale de l'entreprise ?
- 8) Quels sont les risques associés à une mauvaise gestion des données dans un système d'information ?

- 9) Quels avantages une documentation bien structurée pourrait-elle apporter à la gestion des processus critiques de cette PME ?
- 10) Comment une meilleure utilisation des concepts fondamentaux du chapitre 1 pourrait-elle aider Lizbiz's à atteindre ses objectifs stratégiques ?



## Livre II:

# DEMARCHE GENERALE D'AUDIT DES SYSTEMES D'INFORMATION

### **Objectif : Objectif du Livre :**

Présenter la démarche globale d'audit qui est commune à tous les types d'audits, mais aussi, présenter quelques éléments spécifiques aux audits des SI.

### **Objectif d'apprentissage :**

A la fin de ce livre, chaque apprenant doit être à mesure de comprendre l'agence et le rôle de chaque étape d'une mission d'audit des SI, ainsi que les documents qui y sont produits.

## 2) DEMARCHE GENERALE D'AUDIT DES SYSTEMES D'INFORMATION

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

Sur la base de mon expérience personnelle et de l'observation de la pratique générale, je recommande de répartir le temps global d'une mission ainsi qu'il suit :

- ☑ Travaux préparatoires : 15% ;
- ☑ Planification : 35% ;
- ☑ Exécution : 30% ;
- ☑ Communication des résultats : 15% ;
- ☑ Imprévus : 5%.

### 2.1. Champs d'application

#### 2.1.1. *Audit d'une organisation*

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

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

#### 2.1.2. *Audit de processus*

Dans une organisation pratiquant le pilotage par les processus (niveau de maturité encore peu répandu dans l'administration publique camerounaise), les projets informatiques devraient être pensés nativement dans une logique de processus.

L'audit d'un processus doit inclure un audit des outils informatiques sur lesquels il s'appuie. Cet audit doit inclure l'examen des données et informations manipulées au cours du déroulement du processus, y compris celles provenant d'autres processus, des applications qui servent ou automatisent tout ou partie des tâches ou procédures qui le composent, et des infrastructures informatiques de traitement et communication qu'il utilise.



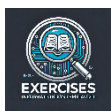
### 2.1.3. *Audit de régularité*

L'audit de la régularité d'une situation, qu'il s'agisse de vérifier le fonctionnement d'une entité, le déroulement d'un processus ou, plus généralement le respect d'une norme ou d'un corpus normatif, implique le plus souvent l'audit des ressources informatiques qui y contribuent. L'auditeur cherchera à vérifier que les activités portées par les ressources informatiques sont en elles-mêmes régulières et à mesurer leur contribution au contrôle interne de l'entité ou du processus, par leur architecture ou les règles qu'elles portent.

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

### 2.1.4. *Audit des fonctions externalisées*

Rares sont les fonctions externalisées qui n'ont pas besoin d'échanger régulièrement des données avec l'organisation, ce qui suppose une interconnexion entre systèmes informatiques. Souvent, le bon déroulement de ces échanges de données, en temps réel ou non, constitue une partie des obligations des deux cocontractants. Ils sont aussi le motif d'une ouverture du système informatique de l'organisation vers l'extérieur, parfois pour des actions aussi sensibles que de l'administration de serveurs, de données ou d'applications. Plus rares encore sont les fonctions externalisées qui n'ont pas à manipuler des données ou informations appartenant au patrimoine de l'organisation. Le cocontractant a alors la responsabilité de l'intégrité, de l'accessibilité et de la protection des données. Dans tous les cas, la dimension informatique de l'externalisation est au cœur de sa réversibilité. Elle peut être la cause de son irréversibilité. L'audit d'une fonction externalisée devra donc en aborder la dimension informatique, tant pour l'organisation que pour son cocontractant.



Chaque apprenant proposera au moins un exemple pour chaque domaine d'application de l'audit des systèmes d'information vu supra.

## 2.2. Travaux préparatoires

Les travaux préparatoires couvrent l'ensemble des travaux qui conduisent à l'élaboration des termes de référence (fiche technique) d'une mission.

### 2.2.1. *Documents à solliciter*

Pour mener à bien la phase des travaux préparatoires, certains documents sont requis à des fins d'analyse. Le tableau suivant en donne une liste non exhaustive, à personnaliser en fonction du sujet d'audit et de l'entité à auditer.

Tableau 3: Liste des documents à solliciter

N°	Documents requis	Utilité
01	Organigramme de l'entité	
02	Organigramme fonctionnel de la DSI	
03	Fiches de postes de la DSI	
04	Dernier rapport d'audit de l'ANTIC	
05	Dernier rapport de suivi de recommandations issues du rapport de l'ANTIC	
07	Dernier rapport d'audit du domaine d'audit	
08	États financiers de la période	
09	Liste des applications informatiques	
10	Liste des applications informatiques, avec leur descriptif	
11	Schéma/ diagramme d'interaction des applications informatiques métiers	
12	Diagramme de flux de données, des applications du domaine d'audit	
13	Manuel des procédures de la DSI	
14	Manuel des procédures des divisions en charge du domaine d'audit	
15	Liste des responsables présents dans le processus du domaine d'audit	
16	Liste des responsables de la DSI avec leur profil	
17	Manuels d'utilisation des applications du domaine d'audit	
18	Manuels d'administration des applications du domaine d'audit	
19	Date, objet, et descriptif des 5 dernières mises à jour des applications du domaine d'audit	
20	Infrastructure logicielle et matérielle hébergeant les applications du domaine d'audit	
21	Contrat de maintenance ou d'assistance pour les applications du domaine d'audit	
22	Liste des responsables de la DSI en charge de l'administration/support/maintenance des applications du domaine d'audit, application par application	
23	Liste des profils avec descriptifs, présents dans chaque application du domaine d'audit	
24	Matrice des autorisations/droits d'accès pour chaque application du domaine d'audit	
25	Procédures encadrant la gestion des incidents survenus en lien avec les applications du domaine d'audit	

N°	Documents requis	Utilité
26	Procédure de créations d'un nouvel utilisateur dans les applications du domaine d'audit	
27	Procédure de modification/changement de profil d'un utilisateur dans les applications du domaine d'audit	
29	Procédure de suppression/ désactivation d'un utilisateur dans les applications du domaine d'audit	
30	Liste des 100 derniers incidents survenus dans du domaine d'audit, ainsi que le sort qui leur a été réservé	
31	Matrice des taches et fonctions incompatibles	
32	Politiques SI et de sécurité SI de l'organisation	
33	Plan d'occupation des sols (POS) du SI et la liste des responsables de zones fonctionnelles	
34	Charte de l'utilisation des SI à laquelle sont soumis les membres de l'organisation	
35	Comptes rendus des comités ou groupes de travail (GT) consacrés pour tout ou partie aux SI	
36	Liste et le poids financier des principaux marchés SI en cours	
37	Stratégie de migration des données et la méthodologie de reprise des données retenue par l'organisation, le cas échéant	
38	Plan de reprise des activités	
39	Plan de continuité des activités	
40	Tableau de bord	
41	Organigramme des projets et la définition des rôles et responsabilités ; Cahiers de charges, le cas échéant	
42	Rapports de traitements des incidents	
43	Inventaires des licences	
44	Bilan de qualité logiciel	
45	Bilan de la satisfaction des utilisateurs	
46	Plan de formation	
47	Planning de formation avec liste des personnes formées	
48	Politique RH et de formation	



Chaque apprenant proposera le tableau précédent en remplissant la colonne Utilité, pour chaque Document requis.



### 2.2.2. Analyse préalable des risques

A cette phase, le but de l'analyse préalable des risques est de circonscrire le domaine d'audit, en fonction de certains paramètres dont les deux majeurs sont :

- ☑ La signification pour le commanditaire ;
- ☑ La criticité liée au domaine d'audit.

Idéalement pour la criticité liée au domaine d'audit, c'est la matrice des risques de l'entité qui est le document de base.

En l'absence de ce document important, c'est-à-dire si aucune matrice de risque n'existe ou si le domaine prévu pour être audité n'en fait pas partie, alors la décision peut être prise de façon empirique ou en raison d'un incident majeur survenu.

A cette occasion, les risques liés au domaine doivent faire l'objet d'une évaluation ou d'une réévaluation. Cette étape produit donc soit une matrice des risques révisée, soit une matrice de risques nouvelle.

### 2.2.3. Identification des ressources nécessaires pour la mission

L'identification des ressources a pour but de répondre aux questions suivantes :  
Quand ? Comment ? Par qui ? Avec quoi ?

#### 2.2.3.1. Quand ?

Il s'agit de la période sur laquelle va porter l'audit, mais aussi du temps alloué aux travaux d'audit à venir.

#### 2.2.3.2. Comment ?

Ici le type d'audit est défini, avec ses différentes séquences et les points particuliers pour lesquels le commanditaire voudrait des éclairages spécifiques.

#### 2.2.3.3. Par qui ?

Ce point renvoie aux profils requis pour effectuer la mission. Il peut aussi s'agir de dire si ce sera un audit réalisé par du personnel interne ou recours sera fait aux auditeurs externes.

Les précisions sur les contraintes particulières qui vont peser sur les auditeurs peuvent aussi être formulées ici.

#### 2.2.3.4. Avec quoi ?

Cette question renvoie aux moyens matériels et financiers nécessaires pour la réalisation de la mission d'audit. Elle fixe le coût de la mission.

#### 2.2.4. Documents à produire

A la fin de la phase des travaux préparatoires, les documents suivants sont produits :

- ☑ Les termes de références de la future mission d'audit ;
- ☑ Le contrat avec l'auditeur externe, le cas échéant ;
- ☑ L'accord de non-divulgence, le cas échéant ;
- ☑ L'engagement de non-conflit d'intérêt, le cas échéant ;
- ☑ La lettre de mission ;
- ☑ Les différents ordres de mission ;
- ☑ Les badges d'accès aux sites règlementés, le cas échéant ;
- ☑ ...



Chaque apprenant proposera le rôle et l'importance de chacun des documents mentionnés supra.

### 2.3. Planification

Dans la littérature, il est courant de voir qu'une mission d'audit commence à cette phase, omettant ainsi la précédente liée aux travaux préalables. Ceci est dû au fait que pour beaucoup, la mission commence avec les documents issus de la phase précédente, notamment la lettre de mission et la constitution de l'équipe de mission.

La phase de planification a pour but de préparer la descente immédiate de l'équipe de mission sur le terrain. Pour ce faire, les documents sollicités à la phase précédente sont analysés, des documents supplémentaires requis le cas échéant et l'équipe de mission se réunit pour commencer à travailler sur le sujet d'audit.

#### 2.3.1. Suivi et analyse des documents sollicités

Les documents sollicités à la phase précédente doivent être remis à l'équipe de mission pour qu'elle prenne connaissance de l'entité et du sujet d'audit. L'équipe analyse les documents reçus et le cas échéant, en requiert de nouveaux.

Elle peut donc concevoir une fiche de suivi des documents sollicités pour en avoir la situation exacte à date. Cette fiche peut prendre la forme de celle présentée au *Tableau 3: Suivi des documents sollicités*.

Il n'est pas rare de trouver dans la littérature qu'une mission d'audit commence par la prise de connaissance de l'entité, qui inclut de fait celle du sujet d'audit.

L'analyse des documents reçus permettra donc d'affiner la compréhension du sujet d'audit. Cette étape fait appel à la capacité de lecture et d'assimilation rapide de l'auditeur.

### 2.3.2. Choix de l'approche et du type d'audit

Le terme « choix » ici est un peu surfait. En réalité, l'équipe transcrit en approche et en type d'audit, les choix déjà effectués au niveau de la phase précédente.

C'est donc plus une formalisation qu'autre chose, car dans le libellé déjà présent sur la lettre de mission et/ou le contrat de service le cas échéant, les choix sont déjà arrêtés.

En effet, si la lettre de mission parle d'auditer une application du domaine d'audit fonctionnelle par exemple, alors le choix du type d'audit est subjacent, il s'agit d'un audit d'application informatique en service.

### 2.3.3. Référentiels à utiliser

Les référentiels à utiliser sont de deux grands ordres :

- ☒ Les référentiels internes à l'entité auditée ;
- ☒ Les référentiels externes.

#### 2.3.3.1. Référentiels internes

Généralement les référentiels internes sont :

- ☒ Les sections des manuels des procédures métiers qui couvrent le sujet d'audit ;
- ☒ Les sections des politiques et procédures IT qui couvrent le sujet d'audit ;
- ☒ Les sections des documents internes (organigramme, fiche de poste, convention collective, ...) qui couvrent le sujet d'audit.

#### 2.3.3.2. Référentiels externes

Les référentiels externes à utiliser en matière d'audit des SI sont :

- ☒ Les lois sur
  - La cybersécurité et la cybercriminalité ;
  - Les communications électroniques ;
  - L'archivage ;
  - Le code du travail ;
  - Le code de procédure pénale ;
  - ...
- ☒ Les normes internationales et bonnes pratiques
  - COSO ;
  - COBIT ;
  - ISO gamme 2700x et 270xx ;
  - ITIL.

Un point sur les normes et référentiels de bonnes pratiques mentionnés ici sera fait dans une section dédiée.

### 2.3.4. Evaluation à priori du système de contrôle interne

Le but de l'évaluation à priori du système de contrôle interne du domaine d'audit vise à en identifier les points forts et faibles. A cette étape, elle peut se confondre à une analyse SWOT pour établir le risque de non-contrôle.

Lorsque l'auditeur conclut que le système de contrôle interne est faible, alors il s'attend à réaliser un nombre important de diligences et à récolter beaucoup de pièces justificatives, et inversement.

Une fois cette évaluation réalisée, l'équipe peut mieux appréhender la charge de travail, et ainsi procéder au dimensionnement des efforts de chaque membre de l'équipe de mission. Au terme de ce dimensionnement, un chronogramme présentant les activités de la mission, les membres qui en sont responsables et les ressources nécessaires est conçu.



Chaque apprenant proposera un tableau représentant le chronogramme de la mission sur la base des informations mentionnées supra, y mettant en regard les membres de l'équipe de mission, les activités à réaliser et les ressources (financières, temporelles et matérielles) nécessaires.

#### 2.3.5. Outils d'aide à l'audit

L'auditeur travaille en permanence sous la contrainte des délais. Il se doit de rendre sa copie pour que ses résultats soient exploités en temps opportuns. Pour ce faire, il lui faut des outils d'aide à l'audit qui faciliteront son travail, lui permettant une réexécution rapide et diminuant à sa plus stricte expression, le risque de non-détection.

Le bon usage d'un tableur peut faire toute la différence en matière de conception d'outils d'aide à l'audit. Une partie importante du cas pratique du *livre V* y revient amplement.

Il existe dans le commerce des outils d'aide à l'audit comme IDEA et Audit360, seulement leur coût et leur mode de déploiement ne sied pas particulièrement aux auditeurs individuels ou aux entreprises à petit budget.



Chaque apprenant proposera le nom d'un autre outils d'aide à l'audit et ou au contrôle présent dans le commerce, avec un bref descriptif et le lien vers le site web de son vendeur/développeur.

#### 2.3.6. Préparation des entretiens et entrevues

La préparation des interviews est une étape importante de la phase de planification. Il est question de choisir les questions qui seront administrées à chaque audité en fonction des paramètres comme :

- ☒ Sa fonction ;
- ☒ Son grade ;
- ☒ Sa date de prise de fonction ;

- ☑ L'usage qu'il fait des technologies ;
- ☑ Son profil professionnel et académique ;
- ☑ ...

En faisant un bon usage d'un tableur et des référentiels retenus, des formulaires sur mesure par fonction dans le processus audité peuvent être conçus. Une partie importante du cas pratique du livre V y revient amplement.

### 2.3.7. Rapport d'orientation/planification

Le rapport d'orientation est le principal output de la phase de planification.

Il reprend le contexte de la mission, décrit le sujet d'audit, en relève les principaux risques, présente les méthodes et moyens à utiliser pour sa réalisation, annonce les outils et le chronogramme d'exécution.

C'est la boussole de la mission. A ce titre, il fait l'objet d'une validation formelle.



Un rapport d'orientation sera rédigé en salle. Les apprenants seront regroupés par 5.

## 2.4. Exécution de la mission

La phase d'exécution, encore appelée mission proprement dite, est celle qui, du fait des échanges pluriels avec l'entité audité est la plus visible, pourtant elle est fortement tributaire de phases précédentes plus silencieuses.

### 2.4.1. Réunion d'ouverture de la mission

La réunion de lancement est une séquence protocolaire où sont présentés aux principaux responsables de l'entité, l'équipe de mission le chronogramme des activités projetées, les principaux extraits du travail de mission, les méthodes et outils que vont utiliser les auditeurs le cas échéant, et les principaux interlocuteurs de la mission.

Son but principal est de faciliter et fluidifier le travail de l'équipe de mission, elle permet également une prise de contact.

Simplement dit, la réunion d'ouverture de mission indique au personnel de l'entité qu'une équipe de mission séjourne dans leurs murs, pour telle durée, qu'elle va déployer tels mécanismes et procédés d'audit, va rencontrer prioritairement tel et tel personnel, et travailler sur tel sujet d'audit.

A l'issue de cette réunion, les participants concernés peuvent se voir notifier la date de passage de l'équipe de mission pour des échanges poussés en rapport avec le sujet d'audit.

## 2.4.2. Collecte d'information

### 2.4.2.1. Entretiens et entrevues

Moyens indispensables pour recueillir les informations mais aussi le ressenti et les avis du personnel audité, les entretiens et entrevues doivent bien se préparer.

Il est usuel que cette phase suive immédiatement la réunion d'ouverture de la mission.

Pendant cet exercice, plus que pour le reste de la mission, l'auditeur doit s'armer de tact et de patience tel un charmeur de serpent, il doit conduire son vis-à-vis à lui communiquer le maximum d'information possible sans que ce dernier ne s'en rende compte le cas échéant.

### 2.4.2.2. Questionnaires

Les questionnaires conçus avec les outils d'aide à l'audit mentionnés plus haut (*point 3.3.5*) peuvent servir de conducteur pour les entretiens et entrevues. A défaut, ils peuvent être directement administrés via tout moyen laissant trace.

### 2.4.2.3. Extraction des données

L'auditeur peut être amené à extraire ou faire extraire, sous son contrôle, des données d'une base de données. Dans le cas où il réalise l'extraction lui-même, il devra en avoir la compétence, mais aussi, il devra le faire en présence de l'audité.

### 2.4.2.4. Biais des méthodes de collecte d'information

Il est important de noter que chaque méthode de collecte d'information a ses biais, un questionnaire peut être renseigné avec légèreté et donc renvoyer un contenu approximatif, un personnel peut soit ne pas être loquasse, soit ne pas dire la vérité pendant son entretien, d'autres encore peuvent harmoniser leurs réponses. L'extraction des données peut se faire sur une partie non exhaustive de la BD maquettée pour les besoins de la cause. De même, la structure des questions d'audit qui appellent une réponse de type booléenne, soit OUI, soit NON, est en elle-même génératrice de biais. J'ai d'ailleurs un article en cours de validation sur la question.

L'auditeur doit être conscient de ces biais et donc les mitiger en combinant plusieurs méthodes de collecte d'information. C'est pourquoi il est recommandé que les questionnaires soient utilisés en sus des entrevues et entretiens, et que les données extraites soient croisées avec d'autres sources, et répudiées pour validation et ou certification par l'audité.

### 2.4.3. Validation des résultats de l'analyse préalable des risques

L'auditeur procède à la validation des résultats de l'analyse préalable des risques effectuée au point II.2.3. Ceci est fait dans le cadre de l'évaluation du système de contrôle interne de sujet d'audit.

Pour ce faire, il déploie une combinaison de référentiels dont le COSO en est le majeur. Il est présenté dans une section dédiée.

Quel que soit le sujet d'audit, une évaluation du système de contrôle interne est requise. Elle va renseigner sur comment est-ce que l'entité s'est prémunie des risques liés au sujet d'audit, à la fois au niveau organisationnel et fonctionnel.

### 2.4.4. Suivi des documents sollicités

Le suivi de la documentation sollicitée permet d'en valider la réception, le remettant et la date de remise.

Ces informations permettent de se prononcer sur l'état de la collaboration du personnel de l'entité auditée, mais aussi de relancer les retardataires le cas échéant.

Le tableau suivant est un modèle de tableau de suivi de la documentation sollicitée, basé sur les documents requis à la phase de travaux préparatoires.

Tableau 4: Suivi des documents sollicités

N°	Documents requis	Documents reçus		
		Émetteur	Date	Remarques
01	Organigramme de l'entité			
02	Organigramme fonctionnel de la DSI			
03	Fiches de postes de la DSI			
04	Dernier rapport d'audit de l'ANTIC			
05	Dernier rapport de suivi de recommandations issues du rapport de l'ANTIC			
07	Dernier rapport d'audit du domaine d'audit			
08	États financiers de la période			
09	Liste des applications informatiques			
10	Liste des applications informatiques, avec leur descriptif			
11	Schéma/ diagramme d'interaction des applications informatiques métiers			
12	Diagramme de flux de données, des applications du domaine d'audit			





N°	Documents requis	Documents reçus		
		Émetteur	Date	Remarques
13	Manuel des procédures de la DSI			
14	Manuel des procédures des divisions en charge du domaine d'audit			
15	Liste des responsables présents dans le processus du domaine d'audit			
16	Liste des responsables de la DSI avec leur profil			
17	Manuels d'utilisation des applications du domaine d'audit			
18	Manuels d'administration des applications du domaine d'audit			
19	Date, objet, et descriptif des 5 dernières mises à jour des applications du domaine d'audit			
20	Infrastructure logicielle et matérielle hébergeant les applications du domaine d'audit			
21	Contrat de maintenance ou d'assistance pour les applications du domaine d'audit			
22	Liste des responsables de la DSI en charge de l'administration/support/maintenance des applications du domaine d'audit, application par application			
23	Liste des profils avec descriptifs, présents dans chaque application du domaine d'audit			
24	Matrice des autorisations/droits d'accès pour chaque application du domaine d'audit			
25	Procédures encadrant la gestion des incidents survenus en lien avec les applications du domaine d'audit			
26	Procédure de créations d'un nouvel utilisateur dans les applications du domaine d'audit			
27	Procédure de modification/changement de profil d'un utilisateur dans les applications du domaine d'audit			
29	Procédure de suppression/ désactivation d'un utilisateur dans les applications du domaine d'audit			
30	Liste des 100 derniers incidents survenus dans du domaine d'audit, ainsi que le sort qui leur a été réservé			
31	Matrice des taches et fonctions incompatibles			
32	Politiques SI et de sécurité SI de l'organisation			

N°	Documents requis	Documents reçus		
		Émetteur	Date	Remarques
33	Plan d'occupation des sols (POS) du SI et la liste des responsables de zones fonctionnelles			
34	Charte de l'utilisation des SI à laquelle sont soumis les membres de l'organisation			
35	Comptes rendus des comités ou groupes de travail (GT) consacrés pour tout ou partie aux SI			
36	Liste et le poids financier des principaux marchés SI en cours			
37	Stratégie de migration des données et la méthodologie de reprise des données retenue par l'organisation, le cas échéant			
38	Plan de reprise des activités			
39	Plan de continuité des activités			
40	Tableau de bord			
41	Organigramme des projets et la définition des rôles et responsabilités ; Cahiers de charges, le cas échéant			
42	Rapports de traitements des incidents			
43	Inventaires des licences			
44	Bilan de qualité logiciel			
45	Bilan de la satisfaction des utilisateurs			
46	Plan de formation			
47	Planning de formation avec liste des personnes formées			
48	Politique RH et de formation			

#### 2.4.5. Déploiement des outils conçus

Une fois l'exécution de la mission démarrée, l'équipe d'audit peut déployer l'ensemble des outils qu'elle a conçu pendant la phase de planification, pour se simplifier la tâche.

Si les outils nécessitent une modification ou un paramétrage de l'environnement logiciel de l'entité auditée, l'équipe doit en obtenir l'autorisation expresse, et laisser faire toutes ces modifications par le personnel IT de l'entité. Dans ce cas, à la fin de la mission, l'équipe doit s'assurer que les modifications effectuées sont supprimées de façon à laisser le système hôte dans son état initial.

Un procès-verbal doit matérialiser toutes les modifications subies par le système hôte du fait de l'équipe d'audit.

#### 2.4.6. Évaluation des contrôles généraux et d'application

L'évaluation des contrôles en audit des systèmes d'information consiste à analyser leur efficacité et leur capacité à atteindre les objectifs de sécurité et de fiabilité des systèmes. Cela inclut les étapes suivantes :

##### 2.4.6.1. Vérification de la conception des contrôles

Il s'agit de s'assurer que les contrôles sont bien conçus pour répondre aux risques identifiés. Pour les contrôles généraux, cela pourrait inclure une évaluation de la politique de gestion des accès, la documentation des procédures de gestion des changements, ou encore le plan de continuité des activités.



À la société Lizbiz's, un auditeur pourrait examiner les politiques de sécurité des mots de passe pour vérifier si elles sont conformes aux meilleures pratiques de l'industrie et si elles sont suffisamment robustes pour prévenir des attaques par force brute.

##### 2.4.6.2. Test d'efficacité opérationnelle

Après avoir vérifié que les contrôles sont bien conçus, il est nécessaire de s'assurer qu'ils fonctionnent effectivement comme prévu. Cela implique des tests des contrôles en situation réelle.



Un audit de la société Lizbiz's pourrait inclure des tests pour vérifier que seuls les utilisateurs autorisés peuvent accéder au système de gestion des ressources humaines ou que les changements dans les applications critiques sont bien approuvés et documentés.

##### 2.4.7. Analyse des faiblesses et recommandations

L'évaluation se termine par une analyse des faiblesses des contrôles et des recommandations pour les améliorer. Cela permet à l'organisation d'identifier des risques potentiels non couverts et d'apporter des ajustements aux contrôles existants.



Lors d'un audit à la LIZBIZ'S, l'auditeur pourrait recommander d'améliorer la surveillance des activités des utilisateurs privilégiés afin de réduire le risque de fraude interne ou d'intrusion non détectée dans le système

##### 2.4.8. Extraction de données

Pour certain type de mission, une extraction de données du système hôte est nécessaire. Cela peut aller des données contenues dans une base de données ou celles d'un équipement actif comme un routeur, un pare-feu ou un switch manageable.

L'équipe, si elle utilise des outils qui lui sont propres doit les communiquer à l'entité audité, en obtenir l'autorisation écrite, et se faire assister par les responsables en charge de la gestion desdits équipements pendant toute l'opération d'extraction. Sinon elle peut aussi solliciter que les extractions soient réalisées par le personnel de l'entité audité sous son contrôle et lui soient remises sans aucun autre traitement.

Lorsqu'il s'agit d'extraction de données, il est important d'avoir au sein de l'équipe de mission un spécialiste des systèmes dont l'extraction est requise, au risque de se faire balader par le personnel de l'entité audité.



Chaque apprenant proposera le nom d'un équipement actif, les informations dont l'auditeur pourrait avoir besoin sur cet équipement et les outils, mécanismes ou méthodes d'extraction possible de ces informations sur ces équipements.

#### 2.4.9. Consignation des faits observés

L'équipe consigne systématiquement tout fait dont elle estime la portée importante pour la mission.

La consignation des faits est réalisée suivant le modèle de la constatation présentée à la section 2.1.11 précédente.

Page 59 sur 227



#### 2.4.10. Rédaction des projets d'observation

Une certaine école recommande d'attendre l'approche de la fin de mission pour effectuer une rédaction coordonnée et groupée des projets d'observation. Une autre quant à elle conseille la rédaction au fil de l'eau desdits projets.

En tout état de cause, les projets d'observation doivent être rédigés et discutés, puis validés par l'ensemble de l'équipe et revêtir, sauf disposition contraire, la forme présentée à la section 2.1.13.



Deux modèles projet d'observations seront rédigés en salle, Les apprenants conserveront les groupes précédents.

### 2.5. Communication des résultats

L'auditeur ne réalise pas l'ensemble des travaux décrit ici par son propre chef. Il a été mandaté, il se doit donc de rendre compte.

Mais avant, il doit sacrifier au principe du contradictoire qui, comme vu précédemment est un héritage du droit de la défense, puis il formule son opinion et finalise le rapport.

Dans la littérature courante, cette phase est réservée à la finalisation du rapport et son acheminement. C'est une approche limitative. Etant donné que lors de l'exercice du

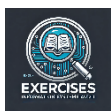
contradictoire l'auditeur communique des éléments qui feront partie ou pas du rapport final, on est en droit de considérer que le contradictoire est bel et bien compris dans la phase de communication des résultats, et non dans celle d'exécution.

### 2.5.1. *Contradictoire*

L'équipe d'audit a l'obligation, faute d'irrecevabilité, de faire toutes les diligences pour réaliser le contradictoire suivant l'explication donnée à la section 2.1.12.

Dans le cas où l'audité serait en vie et injoignable, l'équipe peut recourir aux communiqués radio, télé et à la publication dans les journaux. En tout état de cause, charge revient à l'équipe de démontrer qu'elle a épuisé tout ce qui était humainement possible pour joindre l'intéressé.

Si, cependant, l'équipe fait la preuve qu'elle a joint l'intéressé et que ce dernier n'a pas répondu après un certain nombre de relances à lui adressées, alors l'équipe peut conclure à l'aveu de carence tel que présenté à la section 2.1.16.



Chaque apprenant proposera un argumentaire sur la nuance entre l'aveu de carence et l'impossibilité de joindre un audité, en démontrant l'impact de l'un et l'autre sur les résultats du rapport d'audit.

### 2.5.2. *Formulation des opinions d'audit*

Suivant les écoles, l'opinion d'audit se formule soit pour chaque fait, soit pour l'ensemble du sujet d'audit.

Il est plus logique, puisqu'il s'agit d'une sorte d'avis motivé, que l'opinion d'audit soit formulée pour chaque objectif assigné à la mission. C'est un bon compromis entre les deux voies précédentes. En effet, on peut considérer qu'à l'issue du rapport, au travers de ses observations, l'équipe devrait avoir répondu point par point aux objectifs de la mission clairement formulés dans les TDR, et repris dans la lettre de mission. C'est donc logique que je recommande qu'au moment de conclure son rapport de mission, l'auditeur formule une opinion pour chaque objectif consigné dans les termes de référence de la mission.

### 2.5.3. *Finalisation du rapport de mission*

Après avoir réalisé le contradictoire, l'équipe dispose dorénavant d'observations. Le rapport de mission n'est pas une thèse, ce n'est pas un compte rendu des travaux, c'est la présentation structurée et cohérentes des observations issues des travaux d'audit.

La structure idéale d'un rapport de mission d'audit est décrite dans le tableau suivant.

Tableau 5: structure idéale d'un rapport de mission d'audit

N°	Partie	Contenu	Remarque
1.1	Introduction générale	Cadre d'exécution et sujet d'audit	Obligatoire
1.2		Normes, référentiels, textes réglementaires et documents internes	
1.3		Méthodologie	
1.4		Difficultés rencontrées	
1.5		Equipe de mission	
1.6		Structure du Rapport	
2	Présentation du suivi des recommandation des missions antérieures sur des questions similaires ou connexes		Optionnel
3	Une présentation du sujet d'audit		Obligatoire
4.1	Evaluation du système de contrôle interne du sujet d'audit	Introduction	En fonction de la pratique
4.2		L'environnement de contrôle	
4.3		L'évaluation des risques	
4.4		Les activités de contrôle	
4.5		L'information et la communication	
4.6		Le pilotage (le contrôle du contrôle)	
4.7		Conclusion	
5.1	Analyse des données récoltées	Introduction	
5.2		Flux des données	
5.3		Grandes masses	
5.4		Critères et échantillons	
5.5		Résultats	
5.6		Conclusion	
6.1	Observations retenues par point de contrôle	Volet métier	Obligatoire
6.2		Volet IT	
7	Tableau récapitulatif des constatations et recommandations formulées par l'équipe de mission, classées par point de contrôle		En fonction de la pratique
8.1	Conclusion générale	Rappel du sujet d'audit et des objectifs	Obligatoire
8.2		Principaux résultats	
8.3		Opinion des auditeurs	
8.4		Perspectives	
9	Des annexes		Obligatoire

#### 2.5.4. Réunion de clôture de mission

Tout comme la réunion d'ouverture de mission, c'est un exercice protocolaire.

Il est question ici de présenter quelques résultats significatifs de la mission, de remercier les parties prenantes pour leur disponibilité et d'annoncer la fin officielle de la mission.

Simplement dit, la réunion de clôture de mission indique au personnel de l'entité qu'une équipe de mission a séjourné dans leurs murs, pendant telle durée, qu'elle a déployé tels mécanismes et procédés d'audit, a rencontré prioritairement tel et tel personnel, travaillé sur tel sujet d'audit et est arrivée à tel résultat.

### 2.5.5. Transmission du rapport

Une fois le rapport rédigé, validé, paraphé page par page (en fonction de la pratique dans l'entité) et signé, il est acheminé au commanditaire de la mission dans le plus bref délai suivant les mécanismes propres à chaque entité.

## 2.6. Evaluation des Connaissances

### 2.6.1. QCM

**1. Quelle est la première phase dans une démarche générale d'audit des systèmes d'information ?**

- a) Communication des résultats
- b) Exécution de la mission
- c) Planification
- d) Travaux préparatoires

**2. Quel document est essentiel pour définir le périmètre d'un audit ?**

- a) Feuille de route du projet
- b) Termes de référence
- c) Rapport d'analyse des risques
- d) Rapport budgétaire annuel

**3. Quelle phase consomme généralement la plus grande partie du temps d'un audit ?**

- a) Exécution
- b) Planification
- c) Communication des résultats
- d) Travaux préparatoires

**4. Quel est l'objectif principal de l'évaluation des risques dans un audit ?**

- a) Déterminer l'allocation budgétaire
- b) Identifier et évaluer les risques potentiels
- c) Documenter les spécifications du système
- d) Former le personnel

**5. Quel est le principal livrable de la phase de planification ?**

- a) Rapport final
- b) Matrice des risques
- c) Rapport d'orientation
- d) Outils de collecte des preuves

**6. Lors de la phase d'exécution, quelle est la première réunion officielle ?**

- a) Réunion de finalisation
- b) Réunion stratégique
- c) Réunion d'ouverture
- d) Réunion d'analyse des risques

**7. Quelle évaluation garantit l'efficacité des contrôles internes ?**

- a) Analyse SWOT
- b) Test d'efficacité opérationnelle

- c) Analyse préliminaire des données
- d) Revue par la direction

**8. Quel type de document est essentiel pour examiner les vulnérabilités du système ?**

- a) Manuels d'utilisation
- b) Journaux d'incidents
- c) Contrats avec les fournisseurs
- d) Organigrammes

**9. Quel est le rôle principal d'une matrice des risques dans un audit ?**

- a) Attribuer les responsabilités d'audit
- b) Résumer les rapports financiers
- c) Cartographier et prioriser les risques
- d) Analyser la performance de l'équipe

**10. Que signifie SLA dans le contexte des audits IT ?**

- a) Accord de niveau sécurisé
- b) Accord de niveau de service
- c) Accord sur la licence système
- d) Arrangement de licence standard

**11. Quelle méthode est souvent utilisée pour réduire les biais dans la collecte des informations ?**

- a) Combiner plusieurs techniques de collecte
- b) Limiter le nombre de participants
- c) Utiliser uniquement des enquêtes quantitatives
- d) Éviter les données secondaires

**12. Quel est l'objectif principal de la phase contradictoire dans un audit ?**

- a) Valider l'évaluation des risques préliminaires
- b) Permettre à l'audité de présenter ses arguments
- c) Mener des entretiens avec la direction
- d) Réviser la documentation pour conformité

**13. Quel est un résultat commun de la phase d'exécution ?**

- a) Plan de formation
- b) Observations provisoires
- c) Nouveau design système
- d) Budget finalisé

**14. Que signifie la "vérification sur place" dans un audit ?**

- a) Examiner les enregistrements de présence des employés
- b) Collecter des preuves physiques et observer les opérations
- c) Réaliser une analyse système à distance
- d) Examiner les états financiers

**15. Quelle considération clé est importante pour planifier les entretiens d'audit ?**

- a) Le rôle et les responsabilités de l'interviewé
- b) L'allocation budgétaire pour l'entretien



- c) Le calendrier des événements externes
- d) Le type de système audité

**16. Sur quoi se concentrent les contrôles applicatifs ?**

- a) L'architecture système
- b) La gouvernance interne
- c) La saisie, le traitement et la sortie des données
- d) La fiabilité de l'infrastructure

**17. Pourquoi les contrôles généraux IT sont-ils cruciaux dans les audits ?**

- a) Ils éliminent le besoin de revue manuelle
- b) Ils assurent la sécurité et la fiabilité globales des systèmes
- c) Ils réduisent les coûts opérationnels
- d) Ils automatisent les procédures d'audit

**18. Quel document définit les responsabilités de l'équipe d'audit ?**

- a) Manuel organisationnel
- b) Lettre de mission
- c) SLA
- d) Diagramme des flux de données

**19. Que signifie le "contradictoire" en audit ?**

- a) Imposer des décisions finales à l'audité
- b) Permettre à l'audité de présenter des contre-arguments
- c) Exclure des preuves incomplètes
- d) Mener une seconde phase d'audit

**20. Quel outil est couramment utilisé pour suivre l'avancement d'un audit ?**

- a) Matrice des risques
- b) Diagramme de Gantt
- c) Analyse SWOT
- d) Organigramme

**21. Que garantit l'alignement du rapport d'audit avec les objectifs de la mission ?**

- a) Mises à jour régulières de la lettre de mission
- b) Référencement croisé aux termes de référence
- c) Réalisation d'entretiens supplémentaires
- d) Réduction du périmètre de l'audit

**22. Quel est un risque majeur d'un contrôle inadéquat lors d'un audit ?**

- a) Augmentation des coûts opérationnels
- b) Perte de crédibilité de l'équipe d'audit
- c) Exposition à des vulnérabilités critiques du système
- d) Réduction de la conformité aux objectifs financiers

**23. Quel problème est courant dans l'évaluation des risques liés aux applications ?**

- a) Documentation système incomplète
- b) Trop grande dépendance aux contrôles généraux

- c) Manque d'outils d'audit standardisés
- d) Mises à jour irrégulières des termes de service

**24. Quel document formalise le début d'un audit ?**

- a) Rapport d'orientation
- b) Énoncé de mission
- c) Termes de référence
- d) Accord de confidentialité

**25. Quel est l'objectif principal du rapport final d'audit ?**

- a) Fournir une description détaillée des tâches
- b) Résumer les constatations et proposer des recommandations
- c) Former l'audité à de nouvelles techniques
- d) Mettre en place un nouveau cadre de gouvernance

*2.6.2. Questions à Trous*

Complétez chaque phrase avec le terme ou la notion appropriée.

1. La première étape d'une mission d'audit est la phase des \_\_\_\_\_, qui permet de préparer la mission en définissant ses objectifs et son périmètre.
2. Les \_\_\_\_\_ sont des documents essentiels à solliciter pour la phase préparatoire afin de mieux comprendre l'entité auditée.
3. Le \_\_\_\_\_ d'une mission d'audit est souvent défini dans les termes de référence et clarifié lors de la phase de planification.
4. Une matrice des \_\_\_\_\_ est utilisée pour identifier, hiérarchiser et évaluer les risques associés au domaine audité.
5. Le \_\_\_\_\_ est une réunion initiale organisée pour présenter l'équipe de mission, le périmètre de l'audit, et les objectifs de la mission aux parties prenantes.
6. Lors d'un audit, la phase \_\_\_\_\_ inclut la collecte des informations, les entretiens, et les tests pour évaluer les systèmes et processus.
7. Les \_\_\_\_\_ d'audit permettent d'évaluer la qualité des informations et l'efficacité des contrôles au sein des systèmes audités.
8. Les documents tels que le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA) sont cruciaux pour évaluer la gestion des \_\_\_\_\_.
9. Le processus de validation des résultats d'analyse préalable des risques repose souvent sur des référentiels comme \_\_\_\_\_ ou COBIT.
10. Une \_\_\_\_\_ des observations est réalisée à la fin de l'audit pour discuter les constats avec les audités avant de rédiger le rapport final.
11. L'un des principaux livrables de la phase d'exécution est la rédaction des \_\_\_\_\_ d'observation, qui synthétisent les écarts constatés par rapport aux normes.

12. Dans un audit, les \_\_\_\_\_ généraux IT couvrent l'ensemble de l'environnement informatique, tandis que les contrôles d'application se concentrent sur des processus spécifiques.
13. La phase de \_\_\_\_\_ des résultats inclut la rédaction du rapport final et son partage avec le commanditaire de l'audit.
14. Le \_\_\_\_\_ d'audit est un document qui structure les constats, recommandations et conclusions de la mission.
15. La \_\_\_\_\_ est un élément essentiel pour garantir l'impartialité dans la collecte et l'analyse des informations au cours d'un audit.
16. Les questionnaires et entretiens sont des outils de collecte d'informations, mais ils peuvent être biaisés par une réponse non \_\_\_\_\_ ou des informations incomplètes.
17. Une \_\_\_\_\_ des tâches au sein de l'équipe auditée est souvent un point clé vérifié pour garantir la séparation des responsabilités.
18. Les \_\_\_\_\_ d'accès doivent être strictement gérés pour garantir que seuls les utilisateurs autorisés peuvent accéder aux systèmes critiques.
19. L'audit basé sur les \_\_\_\_\_ consiste à se concentrer sur les domaines les plus susceptibles d'avoir un impact significatif.
20. Le \_\_\_\_\_ de mission, signé par le commanditaire, est le document qui formalise le lancement officiel de la mission d'audit.

### 2.6.3. Questions Ouvertes

- 1) En quoi consistent les travaux préparatoires dans une mission d'audit des systèmes d'information ?
- 2) Quels documents sont essentiels à solliciter lors des travaux préparatoires et pourquoi ?
- 3) Comment la matrice des risques est-elle utilisée pour évaluer la criticité d'un domaine audité ?
- 4) Pourquoi est-il important de définir un périmètre clair pour une mission d'audit ?
- 5) Quels rôles jouent les termes de référence dans la phase préparatoire d'une mission d'audit ?
- 6) Quels sont les principaux objectifs de la phase de planification dans une mission d'audit ?
- 7) Expliquez les différences entre les référentiels internes et externes utilisés en audit. Donnez des exemples pour chacun.
- 8) En quoi consiste l'évaluation a priori du système de contrôle interne ?
- 9) Quels outils peuvent être utilisés pour faciliter la planification d'une mission d'audit ?

- 10) Pourquoi est-il crucial de préparer des entretiens et questionnaires adaptés pour chaque profil audité ?
- 11) Quelles sont les principales étapes de la phase d'exécution dans une mission d'audit ?
- 12) Comment la réunion d'ouverture de mission contribue-t-elle au bon déroulement de l'audit ?
- 13) Pourquoi est-il nécessaire de croiser plusieurs méthodes de collecte d'information pendant l'exécution ?
- 14) Quels biais peuvent affecter les résultats de la collecte d'informations et comment les mitiger ?
- 15) En quoi consiste la validation des résultats de l'analyse préalable des risques ?
- 16) Quelles informations clés peuvent être obtenues lors d'entretiens avec les responsables de la DSI ?
- 17) Pourquoi est-il important de documenter chaque étape de l'extraction des données pendant un audit ?
- 18) Quels types de contrôles (généraux et applicatifs) sont évalués dans un audit des SI, et quelles sont leurs différences ?
- 19) En quoi les logs systèmes et les journaux d'incidents sont-ils utiles dans une mission d'audit ?
- 20) Comment les résultats des tests techniques contribuent-ils à l'évaluation des risques identifiés dans un audit ?
- 21) Quelles sont les étapes clés de la phase contradictoire dans une mission d'audit ?
- 22) Comment rédiger des observations d'audit claires et exploitables ?
- 23) Pourquoi est-il important de présenter les projets d'observation avant de finaliser le rapport d'audit ?
- 24) Quels sont les impacts possibles d'une absence de réponse de l'audité lors du contradictoire ?
- 25) Donnez un exemple d'observation négative dans un audit et proposez une recommandation correspondante.
- 26) En quoi consiste la phase de communication des résultats dans une mission d'audit ?
- 27) Pourquoi est-il nécessaire d'organiser une réunion de clôture après la finalisation d'un audit ?
- 28) Quels éléments doivent figurer dans un rapport de mission d'audit bien structuré ?
- 29) Comment les recommandations formulées dans le rapport d'audit peuvent-elles être hiérarchisées selon leur criticité ?
- 30) En quoi une synthèse exécutive est-elle importante pour les décideurs ?

- 31) Quels sont les avantages d'utiliser des outils spécialisés dans la collecte et l'analyse des données pendant un audit ?
- 32) Expliquez comment le référentiel COSO peut être utilisé pour évaluer un système de contrôle interne.
- 33) Quelles sont les différences entre le COBIT et l'ISO 27001 en termes d'applications en audit des SI ?
- 34) En quoi la matrice des autorisations d'accès est-elle cruciale pour évaluer la gestion des accès dans un système d'information ?
- 35) Comment un auditeur peut-il utiliser les normes ISO pour assurer la conformité réglementaire d'un système d'information ?
- 36) Expliquez les étapes de traitement des risques identifiés lors d'un audit des SI.
- 37) Comment un auditeur peut-il identifier les faiblesses d'un contrôle interne pendant une mission d'audit ?
- 38) Pourquoi est-il important d'évaluer les risques résiduels à la fin d'un audit ?
- 39) Donnez un exemple concret d'un risque technologique dans un SI et expliquez comment le traiter.
- 40) En quoi le dimensionnement des efforts d'audit dépend-il des faiblesses identifiées dans le système de contrôle interne ?
- 41) Quels critères un auditeur doit-il considérer pour rédiger des recommandations pertinentes et applicables ?
- 42) Comment le suivi des recommandations issues d'un audit peut-il être organisé efficacement ?
- 43) Pourquoi est-il nécessaire d'évaluer l'impact des recommandations sur la performance globale d'un SI ?
- 44) Comment les retours d'expérience d'un audit précédent peuvent-ils améliorer les pratiques futures ?
- 45) Quels indicateurs clés de performance (KPI) peuvent être utilisés pour suivre la mise en œuvre des recommandations d'un audit ?

#### *2.6.4. Cas pratique*

##### **Énoncé :**

La société **Lizbiz's**, spécialisée dans la distribution de fournitures de bureau, souhaite réaliser un audit de sa fonction informatique. L'objectif est d'évaluer la maturité de son service IT, d'identifier les faiblesses potentielles et de s'assurer que les systèmes soutiennent les objectifs stratégiques de l'entreprise.

Les principaux constats sont les suivants :

1. Il existe un organigramme IT, mais les rôles et responsabilités des employés ne sont pas clairement définis.
2. Les processus de gestion des incidents et des changements ne sont pas documentés.
3. Les indicateurs clés de performance (KPI) ne sont pas suivis pour mesurer la performance du service IT.
4. Le plan de continuité d'activité (PCA) n'a pas été mis à jour depuis trois ans.
5. Les utilisateurs signalent des retards dans le traitement des demandes IT, affectant les opérations commerciales.

L'auditeur a pour mission :

- ☒ De vérifier l'organisation et la structure de la fonction informatique.
- ☒ D'évaluer les processus de gestion des incidents, changements et performances.
- ☒ De formuler des recommandations pour améliorer la maturité et l'efficacité de la fonction IT.

### Questions :

- 1) Quels documents vérifieriez-vous pour confirmer que les rôles et responsabilités au sein de la fonction IT sont correctement définis ?
- 2) Quels éléments doivent figurer dans une procédure de gestion des incidents pour garantir leur efficacité ?
- 3) Comment évalueriez-vous l'alignement de la fonction IT avec les objectifs stratégiques de Lizbiz's ?
- 4) Quels KPI recommanderiez-vous pour suivre la performance du service IT et pourquoi ?
- 5) Quels points vérifieriez-vous pour évaluer si le PCA actuel est encore adapté aux besoins de Lizbiz's ?
- 6) Quelles sont les étapes clés d'un processus de gestion des changements informatiques efficace ?
- 7) Comment mesureriez-vous la satisfaction des utilisateurs vis-à-vis des services IT de Lizbiz's ?
- 8) Quels contrôles internes recommanderiez-vous pour garantir la sécurité des systèmes informatiques de Lizbiz's ?
- 9) Quels critères utiliseriez-vous pour évaluer si les qualifications des employés IT sont adaptées à leurs rôles ?
- 10) Quels éléments clés intégreriez-vous dans votre rapport pour aider Lizbiz's à améliorer la maturité de sa fonction informatique ?

## Livre III:

# NORMES ET REFERENTIELS USUELS EN AUDIT DES SYSTEMES D'INFORMATION

### Objectif :

Présenter les normes et référentiels usuels en audit des Systèmes d'Information.

### Objectif d'apprentissage :

A la fin de ce livre, chaque apprenant doit être à mesure de comprendre l'usage de chaque référentiel et les diverses combinaisons possibles pour adresser des pans spécifiques d'une mission.

### 3) NORMES ET REFERENTIELS USUELS EN AUDIT DES SYSTEMES D'INFORMATION

L'audit des systèmes d'information repose sur des cadres normatifs et des référentiels bien établis qui assurent une évaluation rigoureuse, cohérente et alignée sur les meilleures pratiques internationales. Ces outils permettent d'uniformiser les processus d'audit, de garantir la conformité réglementaire, et d'optimiser la gestion des risques informatiques. Parmi ces cadres, les normes et référentiels tels que le COSO, les ISO, le COBIT et l'ITIL occupent une place centrale.

Le COSO (Committee of Sponsoring Organizations of the Treadway Commission) est largement utilisé pour la gestion des risques et le contrôle interne. Il fournit une approche structurée pour évaluer l'efficacité des contrôles au sein des systèmes d'information. Son cadre, axé sur les objectifs stratégiques, opérationnels et de conformité, est un pilier incontournable dans les audits qui touchent à la gouvernance des SI.

Les normes ISO, notamment l'ISO 27001 pour la gestion de la sécurité de l'information et l'ISO 20000 pour la gestion des services informatiques, offrent des référentiels mondialement reconnus. Elles définissent des exigences claires pour mettre en place et maintenir des systèmes d'information fiables, sécurisés et performants, tout en favorisant l'amélioration continue.

Page 71 sur 227



Enfin, le COBIT (Control Objectives for Information and Related Technologies) et l'ITIL (Information Technology Infrastructure Library) se concentrent sur la gouvernance informatique et la gestion des services IT, respectivement. Le COBIT offre une vue d'ensemble des processus informatiques à aligner avec les objectifs stratégiques, tandis que l'ITIL fournit des bonnes pratiques pour garantir la qualité des services IT. Ensemble, ces deux cadres complètent les normes ISO et COSO, en offrant des approches concrètes pour intégrer les audits dans un contexte opérationnel.

#### 3.1. COSO

Référentiel par excellence d'évaluation du système de contrôle interne, le COSO offre une approche structurée et reconnue pour garantir la fiabilité des opérations, la transparence des rapports financiers et la conformité aux lois et règlements applicables.

##### 3.1.1. Objectif principaux

Ils peuvent être regroupés en cinq grandes articulations :

- ☑ **Prévenir les fraudes** : Le COSO établit des mécanismes pour identifier les risques de fraude, renforcer les dispositifs de contrôle et promouvoir une culture de vigilance. Il intègre des pratiques pour dissuader les comportements frauduleux à tous les niveaux de l'organisation.
- ☑ **Adapter le contrôle interne aux transformations de l'organisation** : En réponse aux changements constants dans les environnements économiques, technologiques et réglementaires, le COSO aide les organisations à maintenir



un contrôle interne efficace, quelles que soient les évolutions structurelles ou stratégiques.

- ☑ **Mobiliser le management et instaurer le "Tone in the middle"** : En plus du "Tone at the top" (impulsion de la gouvernance), le COSO met en avant l'importance du rôle des managers intermédiaires dans l'instauration d'un environnement propice au contrôle interne, en servant de relais des valeurs et des politiques organisationnelles.
- ☑ **Assurer la cohérence entre les dispositifs contribuant à la maîtrise des activités** : Le référentiel vise à aligner les différents dispositifs de contrôle (gestion des risques, éthique et conformité, audit interne) pour créer une gouvernance unifiée et réduire les redondances.
- ☑ **Maîtriser les opérations externalisées** : Avec l'externalisation croissante des processus critiques, le COSO fournit des directives pour évaluer, surveiller et intégrer les prestataires externes dans le système de contrôle global.

### 3.1.2. Structure du COSO

Le COSO, dans sa version actualisée de 2013, repose sur dix-sept (17) principes regroupés en cinq (5) composantes interconnectées. Ces composantes, essentielles pour un contrôle interne robuste, se déclinent comme suit :

- ☑ **Environnement de contrôle** : Constitue le socle du contrôle interne. Il comprend les valeurs éthiques, la gouvernance, les compétences des employés et la structure organisationnelle. Un environnement solide inspire confiance et engagement.
- ☑ **Évaluation des risques** : Permet de comprendre les événements susceptibles de compromettre les objectifs organisationnels. Elle repose sur l'identification, l'analyse et la hiérarchisation des risques, y compris ceux liés aux systèmes d'information.
- ☑ **Activités de contrôle** : Inclut les politiques, procédures et mécanismes conçus pour réduire les risques identifiés. Par exemple, cela peut impliquer des validations automatiques, des séparations de tâches ou des approbations manuelles.
- ☑ **Information et communication** : Garantit que les informations pertinentes sont accessibles et communiquées de manière efficace, tant en interne qu'en externe. Cela inclut la mise en place de systèmes qui collectent et diffusent les données nécessaires aux parties prenantes.
- ☑ **Activité de pilotage** : Permet d'assurer un suivi continu ou périodique de l'efficacité du contrôle interne. Les activités de surveillance, comme les audits internes, identifient les failles et favorisent leur correction en temps opportun.

Tableau 6: Principes et composantes du COSO

N°	Principes	Composantes
1	L'organisation manifeste son engagement en faveur de l'intégrité et des valeurs éthiques.	Environnement de Contrôle Interne
2	Le Conseil fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du dispositif de contrôle interne.	

N°	Principes	Composantes
3	Le management, agissant sous la surveillance du Conseil, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités.	
4	L'organisation manifeste son engagement à attirer, former et fidéliser des collaborateurs compétents.	
5	L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne.	
6	L'organisation définit des objectifs de façon suffisamment claire pour rendre possible l'identification et l'évaluation des risques susceptibles d'affecter leur réalisation.	Evaluation des risques
7	L'organisation identifie les risques associés à la réalisation de ses objectifs dans l'ensemble de son périmètre et procède à leur analyse de façon à déterminer comment ils doivent être gérés.	
8	L'organisation intègre le risque de fraude sans son évaluation des risques.	
9	L'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle interne.	
10	L'organisation sélectionne et développe les activités de contrôle qui contribuent à ramener les risques à des niveaux acceptables.	Activités de contrôle
11	L'organisation sélectionne et développe des contrôles généraux informatiques	
12	L'organisation met en place les activités de contrôle par le biais des règles et des procédures qui mettent en œuvre ces règles.	
13	L'organisation génère des informations pertinentes et fiables nécessaires au bon fonctionnement des autres composantes du contrôle interne.	Information et communication
14	L'organisation communique en interne les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne	
15	L'organisation communique avec les tiers sur les points qui affectent le fonctionnement des autres composantes du contrôle interne	
16	L'organisation sélectionne, développe et réalise des évaluations continues et ou ponctuelles afin de vérifier si les composantes du contrôle interne sont mises en place et fonctionnelles	Activité de pilotage
17	L'organisation évalue et communique en temps voulu les faiblesses de contrôle interne aux parties chargées de prendre des mesures correctives.	



pour chacun des 17 principes du COSO ci-haut, proposer au moins 10 objectifs de contrôle.

### 3.1.3. Importance du COSO dans les audits des systèmes d'information

Dans un environnement numérique en pleine expansion, le COSO joue un rôle crucial en aidant les auditeurs à évaluer les processus liés aux systèmes d'information. Il offre un cadre pour analyser les vulnérabilités, garantir l'intégrité des données, et s'assurer que les technologies soutiennent les objectifs stratégiques de l'organisation.

De plus, le COSO est souvent utilisé en complément d'autres normes, comme l'ISO 27001 pour la sécurité de l'information ou le COBIT pour la gouvernance informatique, afin de fournir une vision globale des contrôles. Par exemple, les auditeurs peuvent utiliser le COSO pour vérifier si les systèmes d'information

intègrent bien des contrôles relatifs à la prévention des fraudes, à la continuité des opérations ou à la conformité réglementaire.

## 3.2. COBIT

Les entreprises doivent satisfaire à des exigences fiduciaires, ainsi qu'à des exigences de qualité et de sécurité, non seulement pour leur information, mais également pour tous leurs autres actifs stratégiques. Dans ce contexte, les dirigeants sont confrontés à un double impératif : d'une part, garantir la protection et la gestion efficace des ressources informatiques, et d'autre part, optimiser l'utilisation des ressources disponibles telles que les applications, les données, les infrastructures et le personnel. Pour s'acquitter de ces responsabilités, ils doivent avoir une vue claire de leur architecture système et prendre des décisions éclairées concernant la gouvernance et les contrôles à mettre en place.

Le COBIT (*Control Objectives for Information and Related Technology*) constitue un cadre de référence reconnu mondialement, qui propose des bonnes pratiques organisées par domaines et processus. Ces bonnes pratiques sont présentées dans une structure logique et facilement compréhensible, ce qui permet aux décideurs de s'appuyer sur un référentiel clair et méthodique pour gérer leurs ressources informatiques. Le COBIT se distingue par son approche basée sur le contrôle, orientée vers les objectifs stratégiques et la gouvernance informatique.

### 3.2.1. Objectifs et apports du COBIT

Les bonnes pratiques définies par le COBIT sont le fruit d'un consensus d'experts issus de divers domaines, ce qui garantit leur robustesse et leur applicabilité. Elles sont principalement axées sur :

- ☑ **L'optimisation des investissements informatiques** : Le COBIT aide à maximiser la valeur tirée des ressources IT en alignant les technologies sur les objectifs stratégiques de l'organisation.
- ☑ **La garantie de la fourniture des services** : Il permet de s'assurer que les services IT sont fournis de manière fiable, conforme et efficace.
- ☑ **La mise à disposition d'outils de mesure** : Le COBIT propose des indicateurs de performance (métriques) pour évaluer les processus et identifier les dysfonctionnements.

Cette approche permet aux organisations d'assurer un contrôle rigoureux de leurs systèmes d'information tout en favorisant l'amélioration continue et la conformité avec les normes et réglementations.

### 3.2.2. Evolution de la structure du COBIT

Le COBIT, désormais dans sa version 2019, reflète une évolution constante pour s'adapter aux besoins changeants des organisations et aux avancées technologiques. Cette version met particulièrement en avant la distinction entre

gouvernance et management, deux dimensions complémentaires mais distinctes :

- ☑ **Gouvernance** : S'assure que les objectifs stratégiques de l'organisation sont atteints grâce à une utilisation efficace des technologies de l'information. Elle repose sur des pratiques telles que l'évaluation des besoins, la prise de décision et le suivi des performances.
- ☑ **Management** : Se concentre sur l'exécution des processus IT pour répondre aux besoins opérationnels quotidiens. Cela inclut la planification, l'organisation, la construction et la livraison des services IT.

Le COBIT 2019 introduit également des éléments clés tels que des facteurs de conception (Design Factors) pour personnaliser la gouvernance en fonction des besoins spécifiques de chaque organisation et des objectifs de gouvernance et de management qui couvrent l'ensemble des activités informatiques.

Elle est structurée en 5 domaines et 7 composantes.

Tableau 7: Les cinq (5) domaines du COBIT 2019

N°	Domaines	Abréviation	Ressorts
1	Evaluer, Diriger et Surveiller	EDM	Gouvernance
2	Aligner, Planifier et Organiser	APO	Management
3	Bâtir, Acquérir et Implémenter	BAI	
4	Délivrer, Servir et Supporter	DSS	
5	Surveiller, Evaluer et Contrôler	MEA	

Les 7 composantes du COBIT 2019 sont :

- ☑ Les processus ;
- ☑ La structure organisationnelle ;
- ☑ Les flux d'information et éléments ;
- ☑ Les personnes, leurs aptitudes et compétences ;
- ☑ Les politiques et procédures ;
- ☑ La culture, l'éthique et le comportement ;
- ☑ Les services, infrastructures et applications.

Les Design Factors dans COBIT 2019 (facteurs de conception) sont des éléments clés permettant d'adapter et de personnaliser la gouvernance des systèmes d'information en fonction des spécificités et des besoins de chaque organisation.

Voici les principaux Design Factors identifiés dans COBIT 2019 :

- ☑ **Stratégie d'entreprise** : Le type de stratégie adopté par l'organisation (par exemple, innovante, orientée vers la croissance, ou centrée sur l'efficacité opérationnelle) influence la gouvernance informatique.
- ☑ **Profil des objectifs d'entreprise** : L'importance relative des différents objectifs stratégiques de l'entreprise, comme la création de valeur, la gestion des risques ou l'optimisation des ressources.

- ☑ **Risque d'entreprise** : Le niveau de risque que l'organisation est prête à accepter dans ses opérations, ce qui détermine l'approche de la gouvernance informatique.
- ☑ **Modèle de menace** : Les menaces spécifiques auxquelles l'organisation est exposée (par exemple, les cyberattaques, les interruptions de service, ou les défaillances internes).
- ☑ **Exigences de conformité** : Les réglementations et normes spécifiques auxquelles l'organisation doit se conformer (par exemple, RGPD, ISO 27001).
- ☑ **Fonctionnement du rôle informatique** : Le rôle de la fonction IT dans l'organisation (fournisseur de services, partenaire stratégique, moteur d'innovation).
- ☑ **Méthode d'approvisionnement informatique** : Les modes d'acquisition des services IT, comme l'internalisation, l'externalisation, ou l'utilisation du cloud computing.
- ☑ **Type d'implémentation informatique** : La manière dont les systèmes d'information sont mis en œuvre et maintenus (par exemple, systèmes centralisés ou décentralisés).
- ☑ **Taille de l'entreprise** : La taille de l'organisation (grande entreprise, PME, ou organisation publique) influence la structure et l'ampleur de la gouvernance informatique.
- ☑ **Rôle de la technologie** : Le rôle que joue la technologie dans l'organisation (support, transformation ou innovation).
- ☑ **Adoption de nouvelles technologies** : La rapidité et l'ampleur de l'adoption des technologies émergentes (comme l'intelligence artificielle, la blockchain, ou l'IoT).
- ☑ **Culture organisationnelle** : La culture et les valeurs d'entreprise influencent l'adhésion aux principes de gouvernance et aux processus IT.
- ☑ **Capacités et ressources IT actuelles** : L'état actuel des capacités informatiques de l'organisation, y compris les compétences des équipes, les infrastructures et les budgets.

Les Design Factors permettent d'ajuster la gouvernance et la gestion des systèmes d'information pour :

- ☑ Prioriser les objectifs spécifiques de l'organisation ;
- ☑ Aligner les pratiques de gouvernance sur les besoins stratégiques ;
- ☑ Maximiser la pertinence et l'efficacité du cadre COBIT dans un contexte unique.

En les analysant, les organisations peuvent personnaliser les processus et les pratiques recommandées dans COBIT pour atteindre des résultats optimaux.

### 3.2.3. Importance du COBIT pour les audits des systèmes d'information

En tant que norme et référentiel, le COBIT joue un rôle crucial dans les audits des systèmes d'information. Il fournit aux auditeurs un cadre structuré pour évaluer la gouvernance informatique, identifier les lacunes dans les processus et recommander des améliorations alignées sur les objectifs stratégiques. Par exemple, les métriques proposées par le COBIT permettent de mesurer la

performance des processus IT et d'établir des rapports transparents sur leur conformité.

Le COBIT est particulièrement utile pour :

- ☑ Identifier les écarts entre la gouvernance actuelle et les bonnes pratiques reconnues ;
- ☑ Garantir l'alignement stratégique entre les services IT et les besoins de l'organisation ;
- ☑ Renforcer la sécurité, la qualité et l'efficacité des services informatiques.



faites le lien entre les 7 composantes du COBIT et les 5 composantes du COSO.

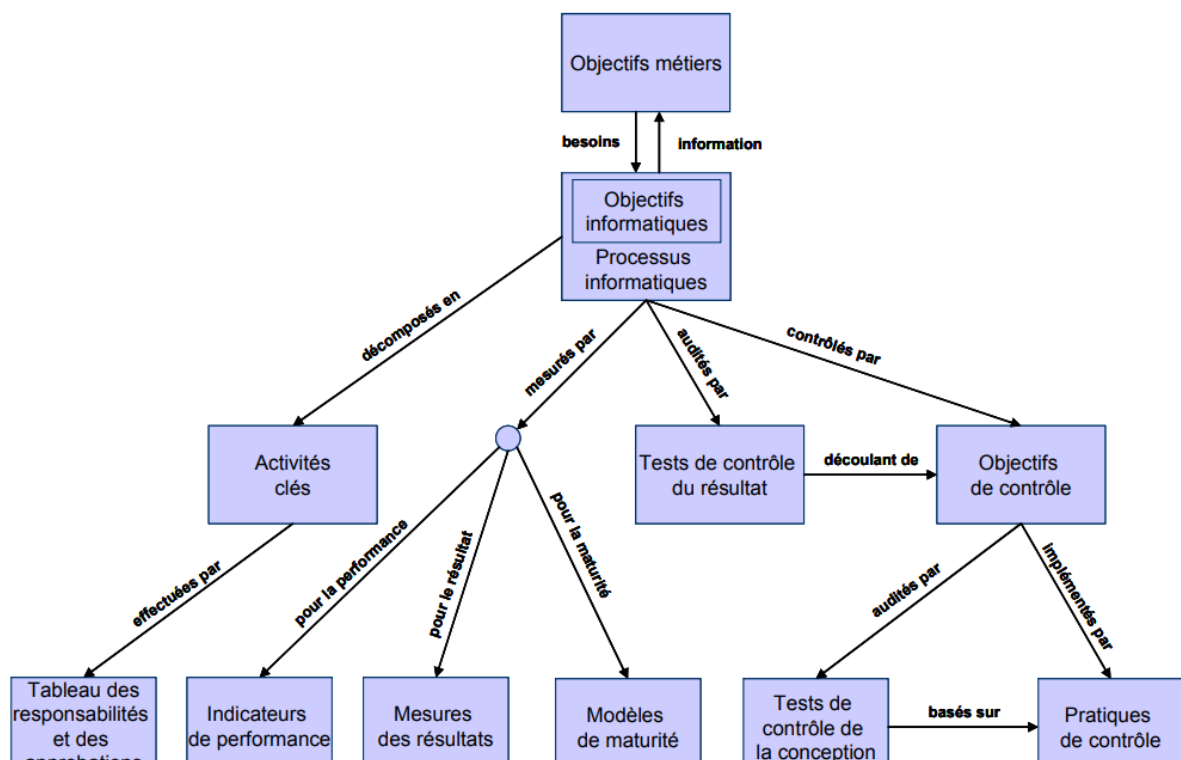


Figure 1: Liens entre les contrôles et les objectifs d'entreprise

### 3.3. ISO 2700x et 270xx

#### 3.3.1. Aperçu de la gamme de normes

Les gammes **ISO 2700X** et **270XX** constituent un ensemble de normes internationales dédiées à la gestion de la sécurité des systèmes d'information. Publiées pour la plupart en 2005 et révisées en 2013, ces normes font partie de la suite **ISO/CEI 27000**, qui offre un cadre complet pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (*Information Security Management System*, ISMS). Elles permettent également de certifier aussi bien les organisations que les individus.

Ces normes définissent un ensemble de points de contrôle qui doivent être évalués pour déterminer la maturité et l'efficacité du système audité. Elles servent de guide aux organisations pour protéger leurs actifs informationnels tout en garantissant la confidentialité, l'intégrité et la disponibilité des données.

### 3.3.2. Principales normes de la suite 27000

#### ☑ ISO/CEI 27001 : 2013

Cœur de la suite ISO 27000, cette norme spécifie les exigences pour établir un ISMS efficace. Elle décrit un processus basé sur le cycle PDCA (Plan-Do-Check-Act) et inclut des contrôles pour :

- L'identification et l'évaluation des risques ;
- La gestion des politiques de sécurité ;
- La mise en œuvre de mesures organisationnelles et techniques ;
- L'amélioration continue.

#### ☑ ISO/CEI 27002 : 2022

Complémentaire à l'ISO 27001, cette norme fournit des **lignes directrices** sur la sélection et l'implémentation des contrôles de sécurité. Elle couvre :

- Les politiques organisationnelles ;
- La sécurité des ressources humaines ;
- La gestion des actifs ;
- La protection des réseaux, applications et données.

#### ☑ ISO/CEI 27005 : 2018

Cette norme se concentre spécifiquement sur la gestion des risques de sécurité de l'information. Elle offre un cadre méthodologique pour :

- Identifier les actifs et leurs vulnérabilités ;
- Évaluer les menaces potentielles ;
- Définir des mesures d'atténuation adaptées.

#### ☑ ISO/CEI 27017 : 2015

Norme dédiée à la sécurité dans le **cloud computing**, elle propose des contrôles spécifiques pour :

- La gestion des environnements multi-tenants ;
- La protection des données hébergées ;
- La clarification des responsabilités entre le fournisseur et l'utilisateur du cloud.

#### ☑ ISO/CEI 27018 : 2019

Cette norme porte sur la protection des données personnelles dans le cloud. Elle s'aligne sur les exigences du RGPD et couvre :

- La transparence des traitements ;
- La confidentialité des données stockées et traitées ;
- Les mécanismes de gestion des violations de données.

#### ☑ ISO/CEI 27701 : 2019

Extension de l'ISO 27001, cette norme intègre des exigences pour un **système de management des informations personnelles (PIMS)**. Elle est particulièrement utile pour les organisations cherchant à démontrer leur conformité aux réglementations sur la protection des données, comme le RGPD.



Le tableau suivant présente les normes de la gamme avec leur champs d'application

Tableau 8: ISO applicables à la sécurité des technologie de l'information et d'usage courant en audit des SI

N°	Gammes	Normes	Champs d'application
1	2700X	ISO 27001	Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
2		ISO 27002	Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information
4		ISO 27004	Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation
5		ISO 27005	Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information
6		ISO 27006	Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et la certification des systèmes de management de la sécurité de l'information
7		ISO 27007	Sécurité de l'information, cybersécurité et protection des données privées — lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
8	270XX	ISO 27018	Technologies de l'information — Techniques de sécurité — Sécurité de réseau — Partie 6: Sécurisation de l'accès réseau IP sans fil
9		ISO 27033.1	Technologies de l'information — Techniques de sécurité — Sécurité de réseau — Partie 1: Vue d'ensemble et concepts
10		ISO 27033.2	Technologies de l'information — Techniques de sécurité — Sécurité de réseau — Partie 2: Lignes directrices pour la conception et l'implémentation de la sécurité de réseau
11		ISO 27033.4	Technologies de l'information — Techniques de sécurité - Sécurité de réseau — Partie 4: Sécurisation des communications entre réseaux en utilisant des portails de sécurité
12		ISO 27035.5	Technologies de l'information — Techniques de sécurité - Sécurité de réseau — Partie 5: Sécurité des communications au travers des réseaux utilisant des réseaux privés virtuels (VPNs)
13		ISO 27034.5	Technologies de l'information — Techniques de sécurité — Sécurité des applications — Partie 5: Protocoles et structure de données de contrôles de sécurité d'application



Sur le modèle fourni en classe concevez un outil d'aide à l'audit basé sur les normes ISO ci-haut.

### 3.3.3. Importance des normes ISO 2700X et 270XX en audit

Pour les auditeurs, ces normes offrent un cadre structuré et universel permettant d'évaluer la maturité et l'efficacité des pratiques de sécurité de l'information d'une organisation.

Voici leurs principaux apports :

- ☑ **Alignement sur les meilleures pratiques internationales** : Les normes ISO garantissent une uniformité des processus et une reconnaissance mondiale.
- ☑ **Évaluation des risques et contrôle** : Elles fournissent des référentiels pour identifier les lacunes et mettre en place des mesures correctives adaptées.



- ☒ **Certification et conformité** : Elles permettent de vérifier si une organisation respecte les exigences réglementaires et industrielles.

### 3.4. Evaluation des Connaissances

#### 3.4.1. QCM

- 1) Quel est le rôle principal d'un référentiel en audit des systèmes d'information ?
  - a) Augmenter la complexité des audits
  - b) Fournir des lignes directrices et des standards
  - c) Réduire la durée de la mission d'audit
  - d) Automatiser l'ensemble des processus
- 2) Quelle norme est spécifiquement conçue pour la sécurité de l'information ?
  - a) COBIT
  - b) ISO 27001
  - c) ITIL
  - d) COSO
- 3) Le référentiel COBIT est principalement utilisé pour :
  - a) La gestion des services IT
  - b) La gouvernance et la gestion des systèmes d'information
  - c) L'analyse des risques financiers
  - d) La documentation des processus
- 4) Quelle norme traite de la gestion des services IT ?
  - a) ISO 20000
  - b) ISO 27034
  - c) COSO
  - d) ISO 31000
- 5) Qu'est-ce qu'un SLA dans le contexte des systèmes d'information ?
  - a) Un accord de sécurité
  - b) Un contrat de niveau de service
  - c) Une analyse de risque
  - d) Une méthodologie de migration
- 6) Pourquoi est-il important d'utiliser un cadre normatif en audit des SI ?
  - a) Pour éviter les biais dans les conclusions
  - b) Pour garantir la conformité aux meilleures pratiques
  - c) Pour faciliter la communication avec les audités
  - d) Toutes les réponses ci-dessus
- 7) Le COSO se concentre principalement sur :
  - a) La gestion des risques et le contrôle interne
  - b) La sécurité de l'information
  - c) Les services informatiques
  - d) La migration des systèmes

8) Quel outil est le plus adapté pour mesurer l'efficacité des contrôles internes ?

- a) Une matrice des risques
- b) Un diagramme de Gantt
- c) Un plan de sauvegarde
- d) Une analyse SWOT

9) ITIL est un référentiel dédié à :

- a) La gestion de projets
- b) La gestion des services IT
- c) L'audit financier
- d) La gestion des ressources humaines

10) Une matrice des risques inclut généralement :

- a) Les ressources, les menaces et les impacts
- b) Les utilisateurs, les administrateurs et les fournisseurs
- c) Les budgets, les calendriers et les projets
- d) Les SLA, les PCA et les PRA

11) Quelle norme aide spécifiquement à gérer les incidents de sécurité dans les applications ?

- a) ISO 31000
- b) ISO 27034
- c) COBIT
- d) ITIL

12) En audit, un plan de continuité d'activité (PCA) est utilisé pour :

- a) Gérer les migrations de systèmes
- b) Planifier les sauvegardes quotidiennes
- c) Maintenir les opérations en cas de crise
- d) Optimiser les temps de réponse

13) Quelle est la différence principale entre un PRA et un PCA ?

- a) Le PRA est axé sur la prévention des incidents, le PCA sur la continuité des activités
- b) Le PRA concerne les sauvegardes, le PCA concerne la sécurité des données
- c) Le PRA est dédié à la reprise après un incident, le PCA assure la continuité pendant la crise
- d) Aucune différence notable

14) Qu'est-ce qu'un point de contrôle en audit ?

- a) Une étape intermédiaire d'un projet
- b) Une action corrective pour un processus
- c) Un élément à évaluer pour assurer la conformité
- d) Une méthode pour organiser les audits

15) Quels critères sont essentiels pour évaluer un contrôle interne ?

- a) Sa documentation et son efficacité
- b) Sa complexité et son coût
- c) Son applicabilité et sa simplicité
- d) Son impact et son taux d'adoption

16) Un SIEM est un outil utilisé pour :

- a) Gérer les sauvegardes
- b) Surveiller les événements de sécurité en temps réel
- c) Réaliser une analyse financière
- d) Documenter les processus métier

17) Quel est l'objectif principal d'un SLA ?

- a) Garantir la qualité des services fournis
- b) Identifier les menaces potentielles
- c) Assurer la continuité des opérations
- d) Gérer les ressources humaines

18) Quelle méthodologie est couramment utilisée pour analyser les risques en audit ?

- a) Analyse SWOT
- b) Matrice des risques
- c) Diagramme de flux
- d) Méthode empirique

19) La norme ISO 31000 est dédiée :

- a) À la gouvernance informatique
- b) À la gestion des risques
- c) À la gestion des services IT
- d) À la sécurité des données

20) Pourquoi documenter les observations lors d'un audit ?

- a) Pour éviter les contradictions
- b) Pour faciliter la validation des constats avec l'audité
- c) Pour respecter les exigences légales
- d) Toutes les réponses ci-dessus

21) Quelle est la finalité principale du référentiel ISO 27001 ?

- a) Créer des indicateurs financiers
- b) Standardiser les pratiques de sécurité de l'information
- c) Gérer les migrations de systèmes
- d) Mesurer la satisfaction des utilisateurs

22) Les PCA et PRA sont regroupés sous la catégorie :

- a) Gestion des services IT
- b) Gestion de la continuité des activités
- c) Gouvernance informatique
- d) Gestion des sauvegardes

23) Quels sont les avantages de l'utilisation d'un référentiel reconnu comme COBIT ?

- a) Optimisation des processus IT
- b) Réduction des coûts de l'audit
- c) Simplification des exigences légales
- d) Standardisation des bases de données

24) Dans un audit, que mesure-t-on avec des KPI ?

- a) La conformité réglementaire
- b) La performance des processus et des systèmes
- c) La qualité des migrations système
- d) Les coûts associés aux SLA

25) Pourquoi est-il essentiel de tester les PCA et PRA régulièrement ?

- a) Pour évaluer leur pertinence en situation réelle
- b) Pour identifier les menaces potentielles
- c) Pour réduire les coûts de maintenance
- d) Pour garantir l'alignement avec le COSO

### 1.1.1. Questions à Trous

Complétez chaque phrase avec le terme ou la notion appropriée.

1. Le référentiel \_\_\_\_\_ est largement utilisé pour la gestion des risques et le contrôle interne.
2. La norme \_\_\_\_\_ est dédiée à la gestion de la sécurité de l'information et repose sur le cycle PDCA (Plan-Do-Check-Act).
3. Le référentiel \_\_\_\_\_ fournit des bonnes pratiques pour la gouvernance et la gestion des systèmes d'information.
4. La norme \_\_\_\_\_ est spécifiquement conçue pour la gestion des services IT.
5. Un \_\_\_\_\_ assure la continuité des activités critiques en cas de crise.
6. Le \_\_\_\_\_ est activé pour rétablir les systèmes après un incident majeur.
7. La norme \_\_\_\_\_ est utilisée pour la sécurité dans les applications et la gestion des incidents.
8. Le cadre \_\_\_\_\_ inclut cinq composantes principales : environnement de contrôle, évaluation des risques, activités de contrôle, information et communication, et surveillance.
9. Les indicateurs de performance, ou \_\_\_\_\_, sont utilisés pour mesurer l'efficacité des processus et des systèmes.
10. Un \_\_\_\_\_ est un contrat qui définit les niveaux de service à fournir par un prestataire IT.
11. Les \_\_\_\_\_ généraux des SI s'assurent de la sécurité et de la fiabilité de l'ensemble de l'environnement informatique.
12. Les contrôles d'application se concentrent sur la \_\_\_\_\_ des données dans des processus métiers spécifiques.
13. Une \_\_\_\_\_ des risques est un outil utilisé pour identifier, évaluer et prioriser les menaces potentielles.

14. La norme \_\_\_\_\_ offre des lignes directrices pour la protection des données personnelles dans le cloud.
15. Le référentiel \_\_\_\_\_ est utilisé pour structurer et améliorer la gestion des services IT.
16. Les tests réguliers des \_\_\_\_\_ permettent de vérifier leur pertinence en situation réelle.
17. Une \_\_\_\_\_ d'observation en audit est un constat rédigé en lien avec une norme ou un référentiel donné.
18. La norme \_\_\_\_\_ aide à gérer les risques liés à la sécurité de l'information et offre une méthodologie claire pour leur évaluation.
19. Le cadre \_\_\_\_\_ permet d'évaluer la performance des processus IT et d'établir des rapports transparents sur leur conformité.
20. Une \_\_\_\_\_ est essentielle pour garantir la traçabilité des actions correctives recommandées dans un audit.

### *1.1.2. Questions Ouvertes*

1. Pourquoi les référentiels sont-ils essentiels dans un audit des systèmes d'information ?
2. Quels sont les principaux objectifs de l'utilisation d'un référentiel tel que COBIT dans la gestion des SI ?
3. En quoi la norme ISO 27001 se distingue-t-elle des autres référentiels en matière de sécurité ?
4. Quels critères faut-il prendre en compte pour choisir un référentiel adapté à un audit des SI ?
5. Quelle est la différence entre un référentiel de gouvernance (ex. COBIT) et un référentiel de sécurité (ex. ISO 27001) ?
6. Quels sont les avantages d'utiliser la norme ISO 20000 pour la gestion des services IT ?
7. Expliquez le rôle du COSO dans la gestion des risques et des contrôles internes.
8. Pourquoi la norme ISO 27034 est-elle importante pour la sécurité des applications ?
9. En quoi ITIL est-il pertinent pour structurer la gestion des services IT dans une organisation ?
10. Comment les normes ISO contribuent-elles à l'harmonisation des pratiques de sécurité dans différentes organisations ?

11. Comment une matrice des risques est-elle construite et utilisée dans un audit des SI ?
12. Quels sont les principaux facteurs de risque à considérer dans un environnement informatique complexe ?
13. Comment évaluer l'impact d'un risque sur les opérations d'une organisation ?
14. Expliquez le processus d'évaluation des risques selon la norme ISO 31000.
15. Pourquoi est-il important de prioriser les risques identifiés dans un audit ?
16. Quelles sont les étapes clés pour élaborer un plan de continuité d'activité (PCA) ?
17. En quoi le plan de reprise d'activité (PRA) complète-t-il le PCA dans une organisation ?
18. Comment tester l'efficacité d'un PCA ou d'un PRA ?
19. Quels sont les risques associés à un PCA qui n'a pas été mis à jour depuis plusieurs années ?
20. Quels indicateurs pourraient être utilisés pour évaluer la maturité des PCA et PRA dans une entreprise ?
21. Comment évaluer l'efficacité des contrôles généraux des systèmes d'information ?
22. Quels sont les éléments à vérifier dans les contrôles d'application liés à la gestion des données ?
23. Pourquoi est-il essentiel de documenter les contrôles internes dans une organisation ?
24. En quoi les logs systèmes peuvent-ils être utiles pour évaluer l'efficacité des contrôles IT ?
25. Quels outils peuvent aider à automatiser les contrôles internes dans une entreprise ?
26. Quelle est la finalité principale d'un SLA dans un contexte IT ?
27. Comment vérifier qu'un SLA respecte les attentes opérationnelles de l'organisation ?
28. Quels éléments doivent être inclus dans un SLA pour garantir la qualité des services ?
29. En quoi le suivi des SLA contribue-t-il à la performance globale des services IT ?
30. Comment gérer les non-conformités détectées dans un SLA existant ?
31. Quels sont les principaux défis rencontrés lors de l'implémentation d'un référentiel comme COBIT ?
32. Comment les référentiels peuvent-ils aider à améliorer la gouvernance IT dans une organisation ?
33. Expliquez comment un référentiel peut être adapté aux spécificités d'une entreprise.

34. Quels sont les bénéfices d'intégrer plusieurs référentiels (ex. ISO 27001 et ITIL) dans une stratégie IT globale ?
35. Quels mécanismes de contrôle permettent de vérifier l'application effective des référentiels dans une organisation ?
36. Quels KPI recommanderiez-vous pour mesurer la performance des processus IT ?
37. Comment les KPI peuvent-ils aider à identifier des opportunités d'amélioration dans une organisation ?
38. En quoi la mesure régulière des KPI contribue-t-elle à une gestion proactive des systèmes d'information ?
39. Quels outils peuvent être utilisés pour automatiser le suivi des KPI liés aux services IT ?
40. Quels indicateurs spécifiques peuvent être associés aux SLA pour suivre leur performance ?
41. Comment un auditeur peut-il s'assurer que les recommandations proposées sont applicables et pertinentes ?
42. Quels sont les impacts potentiels d'une non-conformité à un référentiel tel que ISO 27001 ?
43. Pourquoi est-il essentiel de valider les observations d'audit avec les parties prenantes avant de finaliser le rapport ?
44. Comment les référentiels peuvent-ils guider la rédaction d'un rapport d'audit ?
45. Quelles mesures prendre pour garantir un suivi efficace des recommandations formulées dans un audit ?

### *1.1.3. Cas pratique*

#### **Énoncé :**

La société **Lizbiz's**, spécialisée dans la gestion de solutions de logistique, a récemment constaté des problèmes récurrents dans la gestion de ses services IT, notamment :

1. Une absence de suivi des indicateurs clés de performance (KPI) pour évaluer la qualité des services IT.
2. Une absence de documentation des processus critiques tels que la gestion des incidents et des changements.
3. Une faible maîtrise des risques liés à la sécurité de l'information.
4. Des plans de continuité d'activité (PCA) et de reprise d'activité (PRA) qui n'ont pas été testés depuis plus de deux ans.

#### **Mission de l'auditeur :**

L'équipe d'audit doit évaluer la maturité actuelle des pratiques de Lizbiz's en matière de gouvernance IT et de sécurité de l'information, en s'appuyant sur des référentiels tels que COBIT, ISO 27001, et ITIL. L'objectif est de proposer des recommandations concrètes pour améliorer la gestion des services IT et renforcer la résilience de l'entreprise.

**Questions :**

1. Quels documents devez-vous examiner pour évaluer la conformité des processus IT de Lizbiz's par rapport au référentiel ITIL ?
2. Quels contrôles internes recommanderiez-vous pour mieux sécuriser les données critiques de Lizbiz's ?
3. Comment établiriez-vous une matrice des risques pour identifier et prioriser les menaces pesant sur les systèmes d'information de Lizbiz's ?
4. Quels éléments essentiels incluriez-vous dans un plan d'atténuation des risques lié à la sécurité de l'information ?
5. Quels tests recommanderiez-vous pour évaluer l'efficacité des PCA et PRA actuels de Lizbiz's ?
6. Quels sont les principaux indicateurs à suivre pour garantir que le PRA répond aux besoins stratégiques de l'entreprise en cas de crise ?
7. Quels KPI spécifiques recommanderiez-vous à Lizbiz's pour mesurer la performance de ses services IT ?
8. Comment analyseriez-vous les écarts entre les KPI actuels et les objectifs définis dans un SLA (Service Level Agreement) ?
9. Quels défis Lizbiz's pourrait-elle rencontrer lors de l'implémentation simultanée de COBIT et ISO 27001 ? Proposez des solutions.
10. Comment le référentiel ISO 27001 peut-il guider Lizbiz's dans la mise en place d'un système de gestion de la sécurité de l'information (SMSI) efficace ?





## Livre IV:

# PRINCIPAUX TYPES D'AUDIT DANS LES SYSTEMES D'INFORMATION

### **Objectif :**

Présenter les différents types d'audits des Systèmes d'Information dans leurs spécificités, points communs, divergences, et exigences. Présenter les normes et référentiels usuels en audit des SI

### **Objectif d'apprentissage :**

A la fin de ce livre, chaque apprenant doit être à mesure de connaître les principaux types d'audit des systèmes d'information dans leurs différences, et leur convergences, mais aussi de dérouler le processus qui va de l'identification d'un point de contrôle aux conséquences qui découleraient de son dysfonctionnement.

## 4) PRINCIPAUX TYPES D'AUDIT DANS LES SYSTEMES D'INFORMATION

### 4.1. Audit des Applications en Service

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

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

#### 4.1.1. But

Le but de l'audit d'une application en service (opérationnelle) est de donner au destinataire du rapport d'audit, une assurance raisonnable sur son fonctionnement.

#### 4.1.2. Différentes portées des audits d'application en service

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

#### 4.1.3. L'audit de fiabilité et de sécurité

Il a pour objectif d'émettre une appréciation motivée sur la fiabilité de l'outil informatique, c'est-à-dire sur la qualité du contrôle interne de l'application et la validité des données traitées et restituées.

Ce type d'audit permettra de mettre en évidence d'éventuelles failles dans la chaîne de contrôle composée de contrôles programmés (Contrôles d'Application) effectués par la machine, et de contrôles manuels restant à la charge des utilisateurs (Contrôles Généraux).

#### 4.1.4. L'audit d'efficacité et de performance

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

#### 4.1.5. Fréquence recommandée pour les audits

Il est recommandé d'auditer une application de gestion tous les deux (2) ou trois (3) ans en moyenne et lorsqu'il y a des changements qui y surviennent, de façon à s'assurer qu'elle fonctionne correctement et, le cas échéant, pouvoir apporter les améliorations requises.



Chaque apprenant proposera deux raisons d'auditer une application en service avant les 2 ou 3 ans réglementaires.

#### 4.1.6. Points de contrôle

Conformément au guide d'audit des systèmes d'information, section consacrée à l'audit des applications en service (production) page 56-66, les points de contrôle de ce type d'audit sont au nombre de 6, et définis comme suit :

- 4.1.6.1. *Organisation ;*
- 4.1.6.2. *Application ;*
- 4.1.6.3. *Fonction informatique ;*
- 4.1.6.4. *Adéquation de l'application aux besoins ;*
- 4.1.6.5. *Performance et de la rentabilité ;*
- 4.1.6.6. *Evolutivité/pérennité de l'application.*



Chaque apprenant procèdera à la création d'une feuille de calcul qu'il nommera MonNom\_Outil\_Audit dans laquelle il créera une colonne « Point de Contrôle » et y insérera les 6 points de contrôle énumérés supra

#### 4.1.7. Objectifs de contrôle classés par point de contrôle

##### 4.1.7.1. Organisation

- 4.1.7.1.1. S'assurer de l'existence d'un comité informatique ;
- 4.1.7.1.2. S'assurer de l'existence d'une politique relative aux applications ;
- 4.1.7.1.3. S'assurer que les rôle et responsabilités des utilisateurs sont bien définis ;
- 4.1.7.1.4. S'assurer qu'une analyse des risques a été réalisée ;
- 4.1.7.1.5. S'assurer que le prolongement de l'analyse de risque et de son expansion ont été réalisés ;
- 4.1.7.1.6. S'assurer que l'analyse et évaluation du niveau de sensibilité a été réalisée ;
- 4.1.7.1.7. Vérifier l'existence d'un manuel d'administration de l'application ;
- 4.1.7.1.8. Vérifier l'existence de procédures formalisées ;
- 4.1.7.1.9. S'assurer de l'existence et de la mise à disposition du compte rendu mensuel au propriétaire ;
- 4.1.7.1.10. S'assurer de l'existence d'un guide d'utilisateur, manuel de procédures.

##### 4.1.7.2. Application

- 4.1.7.2.1. S'assurer que l'accès aux ressources de l'application (données et transactions) est restreint par un système de gestion d'accès ;
- 4.1.7.2.2. S'assurer qu'une procédure de gestion des profils utilisateurs existe ;
- 4.1.7.2.3. Vérifier que l'identification des utilisateurs est réalisée ;

- 4.1.7.2.4. Vérifier qu'un mot de passe est associé à l'identifiant ;
- 4.1.7.2.5. S'assurer que les tentatives de connexions infructueuses à l'application sont suivies ;
- 4.1.7.2.6. S'assurer que l'accès aux données et aux transactions de l'application est géré ;
- 4.1.7.2.7. Vérifier l'existence de pistes d'audit sur le système d'administration de l'application ;
- 4.1.7.2.8. Vérifier que tous les documents servant de base à la saisie sont pris en compte ;
- 4.1.7.2.9. S'assurer que les facilités de saisie, l'ergonomie de la saisie, les messages écrans et les contrôles sont mis en œuvre ;
- 4.1.7.2.10. S'assurer que les contrôles de validation des « brouillards » de saisie pour validation par réconciliation existent ;
- 4.1.7.2.11. Vérifier que les saisies des données « sensibles » et notamment les données permanentes, sont gérés ;
- 4.1.7.2.12. Vérifier que les opérations effectuées sur des données sensibles sont suivies ;
- 4.1.7.2.13. Vérifier l'existence des procédures de transmission de fichiers en entrée ;
- 4.1.7.2.14. S'assurer de l'effectivités des contrôles mis en œuvre lors de l'intégration des données par fichiers à l'application ;
- 4.1.7.2.15. S'assurer de la conservation de toutes les données rejetées ;
- 4.1.7.2.16. S'assurer qu'une analyse et correction des données rejetées est effectuée ;
- 4.1.7.2.17. S'assurer qu'un contrôle des corrections des données rejetées est effectif ;
- 4.1.7.2.18. Vérifier que la mise à jour des données sensibles est suivie ;
- 4.1.7.2.19. S'assurer que la journalisation des mises à jour est effective ;
- 4.1.7.2.20. Vérifier l'existence des contrôles automatiques périodiques ;
- 4.1.7.2.21. Vérifier que la couverture, le contenu et la distribution des états de sortie est effective ;
- 4.1.7.2.22. S'assurer que la revue détaillée des états disponibles et de leur destinataire est effective ;
- 4.1.7.2.23. Vérifier que le niveau d'information et de moyen de contrôle adapté ;
- 4.1.7.2.24. S'assurer que la distribution des états de sortie est effective ;
- 4.1.7.2.25. Vérifier que les contrôles utilisateurs des états de sortie sont effectifs ;
- 4.1.7.2.26. S'assurer que les procédures de validation des résultats existent ;
- 4.1.7.2.27. Vérifier que l'homogénéisation des codifications et des règles de gestion est effective ;
- 4.1.7.2.28. S'assurer que l'intégrité et l'exhaustivité des données transmises entre les différents modules est garantie.

- 4.1.7.3.1. S'assurer que les tâches relatives au développement et à l'exploitation de l'application sont bien suivies et documentées ;
- 4.1.7.3.2. S'assurer que l'accès aux bibliothèques de production est réglementé ;
- 4.1.7.3.3. Vérifier que la maintenance de la séparation des tâches est effective ;
- 4.1.7.3.4. S'assurer que l'équipe actuelle en charge de la maintenance est autonome et compétente ;
- 4.1.7.3.5. S'assurer de l'existence de procédure formalisée et standard de maintenance de l'application ;
- 4.1.7.3.6. Vérifier que les nouvelles versions (développement interne, progiciel) sont suivies ;
- 4.1.7.3.7. Vérifier l'existence de procédure formalisée de transfert des programmes entre les environnements ;
- 4.1.7.3.8. S'assurer que la documentation de l'application est effective ;
- 4.1.7.3.9. Vérifier que les corrections effectuées en urgence sur les programmes sont suivies ;
- 4.1.7.3.10. S'assurer de l'existence d'un logiciel de contrôle de programmes sources et de programmes exécutables ;
- 4.1.7.3.11. S'assurer que les travaux batch de l'application, qu'ils soient périodiques ou à la demande, sont bien suivis ;
- 4.1.7.3.12. S'assurer que l'existence d'une procédure de contrôle des traitements batch et d'archivage des comptes-rendus d'exécution est garantie ;
- 4.1.7.3.13. Vérifier que la gestion des incidents en général et les procédures d'urgence en particulier est bien documentée ;
- 4.1.7.3.14. S'assurer de l'existence de la documentation d'exploitation ;
- 4.1.7.3.15. S'assurer de l'existence et l'application d'un Contrat de Service (SLA) ;
- 4.1.7.3.16. S'assurer que les engagements de service et la mesure rigoureuse du niveau de service sont respectés ;
- 4.1.7.3.17. S'assurer que le niveau de service est effectué par l'analyse des tableaux de bord ;
- 4.1.7.3.18. Vérifier que les procédures de sauvegarde et de reprise de l'application sont effectives ;
- 4.1.7.3.19. Vérifier que les sauvegardes sont effectives ;
- 4.1.7.3.20. S'assurer de l'existence d'un plan de secours en adéquation avec les besoins et les enjeux ;
- 4.1.7.3.21. S'assurer que des tests et mises à jour du plan sont effectifs ;
- 4.1.7.3.22. Vérifier la présence de responsable sécurité et d'une politique formalisée en matière de sécurité informatique ;
- 4.1.7.3.23. Vérifier que les accès aux commandes système, aux bibliothèques et bases de données de production sont réglementés ;
- 4.1.7.3.24. S'assurer que les accès aux logiciels de base et utilitaires sensibles sont réglementés ;

4.1.7.3.25. Vérifier l'existence des procédures de contrôle périodique des accès aux ressources de l'application.

#### *4.1.7.4. Adéquation de l'application aux besoins*

- 4.1.7.4.1. Vérifier qu'un Schéma-directeur du système d'information existe et est à jour ;
- 4.1.7.4.2. S'assurer qu'une évaluation de l'alignement stratégique de l'application avec les orientations de l'entreprise a été réalisée ;
- 4.1.7.4.3. S'assurer que la définition des spécifications ou les critères de choix de la solution a été clairement établie ;
- 4.1.7.4.4. Vérifier que les tâches des utilisateurs dans l'application sont clairement définies ;
- 4.1.7.4.5. Vérifier que des systèmes parallèles sont maintenus en activité ;
- 4.1.7.4.6. S'assurer qu'une évaluation de l'adéquation aux besoins des utilisateurs a été réalisée.

#### *4.1.7.5. Performance et de la rentabilité*

- 4.1.7.5.1. Vérifier qu'une évaluation de la rentabilité existe ;
- 4.1.7.5.2. S'assurer qu'une intégration des coûts de déploiement a été réalisée ;
- 4.1.7.5.3. S'assurer qu'une étude sérieuse des offres du marché a été réalisée ;
- 4.1.7.5.4. Vérifier que les délais de mise en œuvre de l'application ont été pris en compte ;
- 4.1.7.5.5. S'assurer qu'un bilan post-projet a été réalisé ;
- 4.1.7.5.6. Vérifier qu'une analyse de la réduction des charges a été effectuée ;
- 4.1.7.5.7. Vérifier que des améliorations non quantifiables ont été prises en compte ;
- 4.1.7.5.8. S'assurer qu'une réingénierie des processus est disponible ;
- 4.1.7.5.9. Vérifier que les processus métiers ont été pris en compte ;
- 4.1.7.5.10. S'assurer que les traitements ont été pris en compte ;
- 4.1.7.5.11. Vérifier que l'architecture technique est prise en compte ;
- 4.1.7.5.12. S'assurer que les indicateurs de performance et un contrat de service sont disponibles ;
- 4.1.7.5.13. S'assurer que les outils de mesure de la performance et les tableaux de bord sont disponibles.

#### *4.1.7.6. Evolutivité/pérennité de l'application*

- 4.1.7.6.1. Vérifier que les technologies utilisées sont conformes aux aspirations de l'entité ;
- 4.1.7.6.2. S'assurer que la technologie du logiciel est conforme aux aspirations de l'entité ;
- 4.1.7.6.3. Vérifier que les technologies utilisées sont matures ;

- 4.1.7.6.4. S'assurer que les technologies utilisées peuvent s'adapter à la croissance ;
- 4.1.7.6.5. S'assurer que l'application peut s'intégrer dans le système de l'entité ;
- 4.1.7.6.6. S'assurer que l'application est modulaire et adaptable ;
- 4.1.7.6.7. S'assurer que l'application significativement version par version ;
- 4.1.7.6.8. Vérifier que le volume des demandes de maintenance évolutive est acceptable et cohérent avec l'utilisation de l'application ;
- 4.1.7.6.9. Vérifier que structure en charge de la maintenance est autonome et compétente ;
- 4.1.7.6.10. S'assurer que le niveau de dépendance vis-à-vis de la structure de développement de l'application est acceptable ;
- 4.1.7.6.11. S'assurer que l'éditeur de l'application a des références indiscutables ;
- 4.1.7.6.12. S'assurer que la version du progiciel installée dans l'organisation est la plus récente ;
- 4.1.7.6.13. S'assurer que les développements spécifiques sont bien suivis ;
- 4.1.7.6.14. Vérifier que l'entité est membre d'un club utilisateurs ;
- 4.1.7.6.15. S'assurer que l'entité a un contrat de maintenance avec l'éditeur ;
- 4.1.7.6.16. S'assurer que les redevances de maintenance sont payées dans les délais ;
- 4.1.7.6.17. S'assurer qu'une clause dite d' « Escrow Agreement » est présente dans le contrat ;
- 4.1.7.6.18. Vérifier que les montées de versions sont suivies ;
- 4.1.7.6.19. S'assurer qu'il existe des engagements et ou une visibilité suffisante pour la pérennité du progiciel.



Chaque apprenant rajoutera une colonne « Objectif de Contrôle » à la précédente feuille de calcul et y insérera les différents objectifs de contrôle listés supra classés par points de contrôle.

#### 4.1.8. Critères classés par objectifs de contrôle ( Organisation )

##### 4.1.8.1. S'assurer de l'existence d'un comité informatique

- 4.1.8.1.1. Existence d'un comité informatique ;
- 4.1.8.1.2. Le Comité est présidé par le Directeur Général ;
- 4.1.8.1.3. Les directions utilisatrices sont représentées au sein de ce Comité ;
- 4.1.8.1.4. Les directions utilisatrices sont influentes au sein de ce Comité.

##### 4.1.8.2. S'assurer de l'existence d'une politique relative aux applications

- 4.1.8.2.1. Il existe une politique relative aux applications au sein de l'institution ;
- 4.1.8.2.2. La politique est connue des utilisateurs d'applications ;
- 4.1.8.2.3. La politique est largement diffusée ;

- 4.1.8.2.4. La politique est mise en œuvre ;
- 4.1.8.2.5. La politique couvre l'ensemble du cycle de vie de l'application ;
- 4.1.8.2.6. La politique favorise la responsabilisation des utilisateurs dans l'usage de leur système d'information (application) ;
- 4.1.8.2.7. La politique préconise l'attribution formelle de responsabilités aux utilisateurs du système (application).

*4.1.8.3. S'assurer que les rôle et responsabilité des utilisateurs sont bien définis*

- 4.1.8.3.1. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application sont clairement identifiés ;
- 4.1.8.3.2. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application couvrent l'analyse des risques ;
- 4.1.8.3.3. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application couvrent la définition des besoins de sécurité ;
- 4.1.8.3.4. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application couvrent la gestion des changements et des évolutions ;
- 4.1.8.3.5. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application couvrent l'administration de l'application.

*4.1.8.4. S'assurer qu'une analyse des risques a été réalisée*

- 4.1.8.4.1. Une analyse des risques spécifique à l'application a été réalisée ;
- 4.1.8.4.2. L'analyse des risques a débouché sur la définition des besoins de sécurité.

*4.1.8.5. S'assurer que le prolongement de l'analyse de risque et de son expansion ont été réalisés*

- 4.1.8.5.1. Il y a eu un prolongement de l'analyse des risques et de l'expression des besoins de sécurité ;
- 4.1.8.5.2. Un contrat de service (SLA) entre l'informatique et la direction utilisatrice a été mis en œuvre.

*4.1.8.6. S'assurer que l'analyse et évaluation du niveau de sensibilité a été réalisée*

- 4.1.8.6.1. Il y a une séparation des tâches au sein de la direction utilisatrice indépendamment de l'application ;
- 4.1.8.6.2. Il y a une « maturité » de l'organisation vis-à-vis de ses systèmes d'information.

*4.1.8.7. Vérifier l'existence d'un manuel d'administration de l'application*

- 4.1.8.7.1. Un ou des manuels pour l'application existe ;
- 4.1.8.7.2. Le manuel est à jour ;
- 4.1.8.7.3. Le manuel est maîtrisé ;
- 4.1.8.7.4. Le manuel comprend un mode d'emploi ;



- 4.1.8.7.5. Le manuel comprend une présentation du module d'administration de l'application ;
- 4.1.8.7.6. Le manuel comprend des droits d'accès.

#### 4.1.8.8. *Vérifier l'existence de procédures formalisées*

- 4.1.8.8.1. Des procédures formalisées imposant l'accord du « propriétaire » de l'application pour tout changement sur les programmes de l'application existent ;
- 4.1.8.8.2. Des procédures formalisées imposant l'accord du « propriétaire » de l'application pour tout changement sur la planification des traitements informatiques existent ;
- 4.1.8.8.3. Des procédures formalisées imposant l'accord du « propriétaire » de l'application pour tout changement sur l'environnement technologique de l'application existent ;
- 4.1.8.8.4. L'administration est bien assurée par les utilisateurs.

#### 4.1.8.9. *S'assurer de l'existence et de la mise à disposition du compte rendu mensuel au propriétaire*

- 4.1.8.9.1. Le propriétaire dispose d'un compte rendu mensuel de la performance de l'application ;
- 4.1.8.9.2. Le compte rendu respecte le contrat du service.

#### 4.1.8.10. *S'assurer de l'existence d'un guide d'utilisateur, manuel de procédures*

- 4.1.8.10.1. Il existe un guide utilisateurs / manuel de procédures ;
- 4.1.8.10.2. Le manuel est diffusé ;
- 4.1.8.10.3. Le manuel est à jour ;
- 4.1.8.10.4. Le manuel est maîtrisé ;
- 4.1.8.10.5. Le manuel comprend le mode d'emploi de l'application ;
- 4.1.8.10.6. Le manuel comprend une description des contrôles programmés et des contrôles manuels compensatoires à chaque phase du traitement.



Chaque apprenant rajoutera une colonne « Critère d'évaluation » à la précédente feuille de calcul et y insérera les différents critères listés supra, les complètera et les classera par objectif de contrôle.

#### 4.1.9. *Éléments requis classés critère*

##### 4.1.9.1. *Existence d'un comité informatique*

- 4.1.9.1.1. Décision de création du comité informatique signée par le DG.

##### 4.1.9.2. *Le Comité est présidé par le Directeur Général*

- 4.1.9.2.1. PV de session du comité.

4.1.9.3. *Les directions utilisatrices sont représentées au sein de ce Comité*

4.1.9.3.1. Décision d'affectation des directions au comité ;

4.1.9.3.2. PV de session du comité.

4.1.9.4. *Les directions utilisatrices sont influentes au sein de ce Comité*

4.1.9.4.1. PV de session du comité.



Chaque apprenant rajoutera une colonne « Eléments Requis » à la précédente feuille de calcul et y insérera les différents documents requis listés supra, les complétera et les classera par critère d'évaluation.

4.1.10. *Questions d'évaluation classées par critère*

4.1.10.1. *Existence d'un comité informatique*

4.1.10.1.1. Existe-t-il un comité informatique ?

4.1.10.2. *Le Comité est présidé par le Directeur Général*

4.1.10.2.1. Le Comité est-il présidé par le Directeur Général ?

4.1.10.3. *Les directions utilisatrices sont représentées au sein de ce Comité*

4.1.10.3.1. Les directions utilisatrices sont-elles représentées au sein de ce Comité ?

4.1.10.4. *Les directions utilisatrices sont influentes au sein de ce Comité*

4.1.10.4.1. Les directions utilisatrices sont-elles influentes au sein de ce Comité ?



Chaque apprenant rajoutera une colonne « Question d'évaluation » à la précédente feuille de calcul et y insérera les différentes questions d'évaluation listées supra, les complétera et les classera par critère d'évaluation.

4.1.11. *Risques classés questions d'évaluation*

4.1.11.1. *Existe-t-il un comité informatique ?*

4.1.11.1.1. Inexistence d'un comité informatique.

4.1.11.2. *Le Comité est-il présidé par le Directeur Général ?*

4.1.11.2.1. Le Comité n'est pas présidé par le Directeur Général.

4.1.11.3. *Les directions utilisatrices sont-elles représentées au sein de ce Comité ?*

4.1.11.3.1. Les directions utilisatrices ne sont pas représentées au sein de ce Comité.

#### 4.1.11.4. *Les directions utilisatrices sont-elles influentes au sein de ce Comité ?*

4.1.11.4.1. Les directions utilisatrices ne sont pas influentes au sein de ce Comité.



Chaque apprenant rajoutera une colonne « Risques » à la précédente feuille de calcul et y insérera les différents risques listés supra, les complètera et les classera par question d'évaluation.

#### 4.1.12. *Conséquences classé par risque*

##### 4.1.12.1. *Inexistence d'un comité informatique*

4.1.12.1.1. Incohérence des choix stratégiques.

##### 4.1.12.2. *Le Comité n'est pas présidé par le Directeur Général*

4.1.12.2.1. Présence au comité des personnels n'ayant pas le bon niveau décisionnels.

##### 4.1.12.3. *Les directions utilisatrices ne sont pas représentées au sein de ce Comité*

4.1.12.3.1. Application non adaptée aux besoins du métier.

##### 4.1.12.4. *Les directions utilisatrices ne sont pas influentes au sein de ce Comité*

4.1.12.4.1. Application non adaptée aux besoins du métier.



Chaque apprenant rajoutera une colonne « Conséquence » à la précédente feuille de calcul et y insérera les différents conséquences listées supra, les complètera et les classera par risque.



La feuille de calcul servant d'outil d'aide à l'audit sera affinée en salle pour y insérer l'ensemble des formules nécessaires à la rendre automatique.

#### 4.1.13. *Conduire une Mission d'Audit d'une Application en Service*

##### 4.1.13.1. *Phase 1 : Planification*

La phase de planification constitue une étape clé pour définir les fondations d'un audit réussi. Elle permet de clarifier les objectifs, de délimiter le périmètre, d'identifier les risques associés et de structurer les actions à venir en tenant compte des ressources disponibles et des parties prenantes. À travers cette phase, les tâches suivantes seront réalisées pour garantir une approche méthodique et efficace de l'audit.

4.1.13.1.1. Identifier les objectifs de l'audit :

- ☑ Déterminer si l'audit est centré sur la conformité réglementaire (ex. RGPD, ISO 27001), la sécurité des données, la performance, ou la continuité des activités.
- ☑ Prioriser les objectifs en fonction des risques organisationnels identifiés.



**Référence savante : Willcocks et Lester (1997)** soulignent dans *Beyond the IT Productivity Paradox* l'importance de bien aligner les audits SI avec les objectifs stratégiques de l'organisation

#### 4.1.13.1.2. Définir le périmètre :

- ☑ Identifier les modules ou fonctionnalités de l'application à auditer, les interfaces critiques, et les bases de données associées.
- ☑ Préciser si l'audit inclut les environnements de préproduction ou uniquement la production.
- ☑ *Délimiter les dépendances avec d'autres systèmes (interopérabilité, API).*

#### 4.1.13.1.3. Analyser les risques liés à l'application :

- ☑ Réaliser une cartographie des risques en tenant compte des impacts sur les processus métiers et sur la sécurité des informations.
- ☑ Utiliser des outils comme le cadre ISO 31000 pour structurer l'analyse des risques.



**Référence savante : Basel Committee on Banking Supervision (2001)** mentionne que l'identification des risques technologiques est cruciale pour éviter des impacts significatifs sur les processus métiers.

#### 4.1.13.1.4. Établir le plan d'audit :

- ☑ Rédiger un programme d'audit détaillant les étapes, les objectifs spécifiques, les outils à utiliser, et le calendrier.
- ☑ Assigner les membres de l'équipe selon leurs compétences techniques et organisationnelles.

#### 4.1.13.1.5. Préparer un questionnaire d'audit :

- ☑ Inclure des questions sur la documentation, la gestion des accès, les sauvegardes, et les mises à jour.

#### 4.1.13.1.6. Documents à solliciter :

- ☑ Documentation technique et fonctionnelle de l'application.
- ☑ Diagrammes d'architecture (flux de données et schémas de bases de données).
- ☑ Politique de gestion des accès.
- ☑ Rapport d'incidents des 12 derniers mois.
- ☑ Contrats de maintenance avec les fournisseurs.

#### 4.1.13.1.7. Actions complémentaires :

- ☑ Organisation d'une réunion de cadrage avec les parties prenantes pour valider le périmètre et les attentes.
- ☑ Validation des outils nécessaires pour la collecte et l'analyse des données (ex : Wireshark pour analyser les flux de données).

### 4.1.13.2. Phase 2 : Exécution

La phase d'exécution est le cœur de la mission d'audit, où les plans définis prennent vie à travers des actions concrètes. Elle consiste à collecter les preuves, analyser les données, observer les pratiques, et évaluer les systèmes et processus en fonction des critères établis. Les tâches suivantes seront réalisées pour garantir une évaluation rigoureuse et objective de la situation auditée.

*4.1.13.2.1. Analyse documentaire :*

- ☑ Comparer les spécifications fonctionnelles actuelles avec celles documentées.
- ☑ Examiner les politiques de sécurité applicative pour vérifier leur alignement avec les standards (ISO 27034).
- ☑ Évaluer les SLA pour s'assurer que les niveaux de service sont respectés.

*4.1.13.2.2. Tests techniques :*

- ☑ Effectuer des tests de fonctionnalité : s'assurer que les modules clés répondent aux besoins utilisateurs.
- ☑ Réaliser des tests de charge et de performance à l'aide d'outils comme JMeter ou LoadRunner.
- ☑ Exécuter des scans de vulnérabilité avec Nessus ou Burp Suite.
- ☑ Vérifier l'efficacité des mécanismes d'authentification et de gestion des sessions.



Référence savante : Ross J. Anderson (2001), dans *Security Engineering*, recommande une approche systématique pour tester les systèmes critiques.

*4.1.13.2.3. Évaluation des contrôles internes :*

- ☑ Évaluer la gestion des accès (listes des utilisateurs et rôles, analyse des privilèges excessifs).
- ☑ Vérifier les mécanismes de sauvegarde et la fréquence des restaurations testées.
- ☑ Contrôler les mesures de journalisation (logs d'accès et d'erreurs).

*4.1.13.2.4. Observation et entretiens :*

- ☑ Observer les utilisateurs dans leur utilisation quotidienne pour identifier les pratiques non conformes ou inefficaces.
- ☑ Interviewer les administrateurs pour comprendre les contraintes et éventuelles zones d'ombre dans la gestion de l'application.

*4.1.13.2.5. Documents à solliciter :*

- ☑ Journaux système (logs d'accès, d'erreurs, etc.).
- ☑ Résultats des tests de restauration de sauvegardes.
- ☑ Rapports de scans ou de tests de sécurité antérieurs.
- ☑ Liste des droits et rôles des utilisateurs.

*4.1.13.2.6. Actions complémentaires :*

- ☑ Organiser des tests en environnement isolé pour éviter de perturber la production.
- ☑ Utiliser des scénarios métier pour tester les fonctionnalités clés en collaboration avec les utilisateurs finaux.

*4.1.13.3. Phase 3 : Communication des résultats*

La phase de communication des résultats constitue l'aboutissement de l'audit, où les constats, analyses et recommandations sont présentés de manière claire et structurée aux parties prenantes. Cette étape vise à fournir des informations exploitables et à favoriser l'engagement pour la mise en œuvre des actions correctives. Les tâches suivantes seront réalisées pour assurer une restitution efficace et impactante des conclusions de l'audit:

4.1.13.3.1. *Rédiger le rapport d'audit :*

- ☑ Structurer le rapport en trois parties :
  - Constatations majeures (points forts/faibles).
  - Recommandations hiérarchisées (sécurité, performance, conformité).
  - Plan d'action détaillé avec responsables assignés et échéances.
- ☑ Inclure des graphiques ou tableaux pour illustrer les résultats.

4.1.13.3.2. *Préparer une synthèse :*

- ☑ Rédiger une synthèse exécutive pour les décideurs.
- ☑ Mettre l'accent sur les risques critiques et les gains potentiels d'une mise en conformité ou d'améliorations.

4.1.13.3.3. *Restituer les résultats :*

- ☑ Organiser une réunion de restitution avec toutes les parties prenantes (propriétaire de l'application, DSI, utilisateurs clés).
- ☑ Discuter des priorités pour les actions correctives et obtenir un consensus sur leur mise en œuvre.

4.1.13.3.4. *Documents à solliciter :*

- ☑ Synthèse des recommandations approuvées.
- ☑ Feuille de route pour le suivi des actions correctives.
- ☑ Procès-verbal de la réunion de restitution.

4.1.13.3.5. *Actions complémentaires :*

- ☑ Proposer des indicateurs pour suivre la mise en œuvre des recommandations.
- ☑ Prévoir une revue de suivi six mois après la restitution pour vérifier les progrès.

- ☑ **IT Governance Institute (2005) dans COBIT Framework for IT Governance and Control** : insiste sur l'importance de la formalisation des processus d'audit pour améliorer la maturité organisationnelle.
- ☑ **Debra Geihlsler et Michael Westerman (2004)**, dans *Managing IT as a Business*, expliquent que l'audit des applications en service est central pour garantir un ROI durable et minimiser les risques métiers.

## 4.2. Audit de la Fonction Informatique

### 4.2.1. But

L'objectif de l'audit est d'évaluer la « maturité » informatique de l'organisation et l'adéquation du rôle, du positionnement et des objectifs de l'unité en charge des systèmes d'information avec les enjeux de l'Organisation, ses relations avec les utilisateurs, ses méthodes de travail.

### 4.2.2. Fréquence recommandée pour les audits

Il est recommandé d'auditer la fonction informatique chaque trois (3) ans en moyenne et lorsqu'il y a des changements qui y surviennent comme une modification d'organigramme, ou la désignation de nouveaux responsables.

### 4.2.3. Points de contrôle

Conformément au guide d'audit des systèmes d'information, section consacrée à l'audit de la fonction informatique page 37-42, les points de contrôle de ce type d'audit sont au nombre de 6, et définis comme suit :

- 4.2.3.1. *Rôle et positionnement de l'informatique dans l'organisation ;*
- 4.2.3.2. *Planification stratégique ;*
- 4.2.3.3. *Budgets et coûts informatiques ;*
- 4.2.3.4. *Mesure et suivi de la performance informatique ;*
- 4.2.3.5. *Organisation et structure de la DSI ;*
- 4.2.3.6. *Cadre législatif et réglementaire Camerounais.*

### 4.2.4. Objectifs de contrôle classés par point de contrôle

#### 4.2.4.1. *Rôle et positionnement de l'informatique dans l'organisation*

- 4.2.4.1.1. Vérifier qu'ont été créés des Comités « informatique » (stratégique, pilotage,...) regroupant les différentes directions de l'Organisation en charge de recenser les besoins et les opportunités, gérer les priorités et suivre les projets ;
- 4.2.4.1.2. Vérifier l'existence d'une charte informatique ou de tout autre document définissant le rôle et le périmètre de responsabilité de la DSI ;
- 4.2.4.1.3. Évaluer le degré d'implication et de maîtrise des organes de gestion dans les systèmes d'information de l'Organisation ;
- 4.2.4.1.4. Vérifier en pratique que le leadership des grands projets est assuré par les organes de gestion ;
- 4.2.4.1.5. Vérifier que les métiers assurent leur rôle de MOA.

#### 4.2.4.2. *Planification stratégique*

- 4.2.4.2.1. Vérifier la couverture du périmètre fonctionnel ;
- 4.2.4.2.2. Vérifier l'existence d'une analyse à jour des procédures de pilotage et de mise à jour du plan informatique ;

- 4.2.4.2.3. Vérifier l'existence des documents à jour d'urbanisme de l'Organisation ;
- 4.2.4.2.4. Vérifier l'existence d'une analyse à jour des procédures de pilotage et de mise à jour du plan d'occupation des sols (POS) ;
- 4.2.4.2.5. Vérifier la cohérence et l'homogénéité des technologies ;
- 4.2.4.2.6. Vérifier l'existence et l'unicité des référentiels (clients, fournisseurs, articles...) et des saisies.

#### 4.2.4.3. *Budgets et coûts informatiques*

- 4.2.4.3.1. Évaluer l'organisation et les processus existants ;
- 4.2.4.3.2. Vérifier l'existence des ratios et des éléments de benchmark (interne et/ou externe, ratio coûts/CA, ...).

#### 4.2.4.4. *Mesure et suivi de la performance informatique*

- 4.2.4.4.1. Vérifier que des objectifs de court, moyen et long termes existent et sont assignés à la DSI (approche BSC ?) et que ces objectifs sont déclinés au sein de l'entité ;
- 4.2.4.4.2. Vérifier l'existence d'un comité informatique regroupant les différentes directions de l'organisation ;
- 4.2.4.4.3. Évaluer la pertinence des indicateurs de qualité et de performance ainsi que les moyens et outils de mesure ;
- 4.2.4.4.4. Vérifier que la DSI tient un tableau de bord (idéalement de type BSC) permettant un suivi consolidé de la performance (opérationnelle et financière) et de la qualité des prestations informatiques ;
- 4.2.4.4.5. Vérifier qu'il est systématiquement effectué un bilan après chaque projet et notamment un bilan économique (bilan rapproché des prévisions de l'étude préalable).

#### 4.2.4.5. *Organisation et structure de la DSI*

- 4.2.4.5.1. Vérifier l'existence d'un organigramme à jour de la DSI ;
- 4.2.4.5.2. Vérifier l'existence d'une définition de fonction et d'un partage clair des rôles et des responsabilités pour chaque poste figurant sur l'organigramme ;
- 4.2.4.5.3. Vérifier que l'ensemble des composantes d'une fonction informatique est convenablement pris en compte, notamment la veille technologique, la sécurité informatique, la fonction qualité & méthodes, la gestion des ressources humaines, le contrôle de gestion, le support utilisateurs (de proximité et à distance), l'administration des serveurs ;
- 4.2.4.5.4. Évaluer l'adéquation des effectifs aux besoins et aux enjeux ;
- 4.2.4.5.5. Évaluer l'adéquation des qualifications du personnel avec les fonctions qu'ils occupent ;
- 4.2.4.5.6. Vérifier que l'expression des besoins, les spécifications fonctionnelles et la recette des applications sont effectuées par les utilisateurs ;



- 4.2.4.5.7. Vérifier que les tâches, les locaux et les environnements relatifs aux fonctions études et exploitation, qu'ils soient assurés ou fournis en interne, ou externalisés, sont séparés ;
- 4.2.4.5.8. Vérifier l'existence d'une procédure de mise en production ;
- 4.2.4.5.9. Lorsque les organisations le permettent, vérifier que les différentes tâches d'administration des bases de données -DBA- sont séparées entre les études et l'exploitation ;
- 4.2.4.5.10. Vérifier que la séparation des tâches est maintenue et assurée lors de la rotation des équipes, des vacances et du départ d'un personnel ;
- 4.2.4.5.11. Évaluer le caractère « raisonnable » du turn-over de la DSI (5 à 15% / an) ;
- 4.2.4.5.12. Évaluer la capacité de l'Organisation à gérer les carrières des informaticiens ;
- 4.2.4.5.13. Vérifier l'adéquation du niveau de rémunération du personnel informatique et évaluer le « moral » des équipes ;
- 4.2.4.5.14. Évaluer la dépendance de l'Organisation vis-à-vis d'une ou plusieurs personnes ;
- 4.2.4.5.15. Vérifier que les contrats des informaticiens contiennent des clauses spécifiques de confidentialité et de non-concurrence ;
- 4.2.4.5.16. Vérifier si les informaticiens sont- dispensés de préavis en cas de rupture brutale du contrat de travail ;
- 4.2.4.5.17. Vérifier l'existence d'un plan de formation nominatif pour l'ensemble des informaticiens ;
- 4.2.4.5.18. Vérifier que l'effort de formation est adapté, suffisant et qu'il s'inscrit dans la durée.

#### 4.2.4.6. *Cadre législatif et réglementaire Camerounais*

- 4.2.4.6.1. Vérifier que les prescriptions légales découlant des loi de 2010 sur le cybersécurité et la cyber criminalité ; ainsi que les transactions électroniques sont connues et respectées ;
- 4.2.4.6.2. Vérifier que les articles sur la fraude informatique sont connus et que des mesures préventives ont été prises ;
- 4.2.4.6.3. Vérifier que les articles sur l'usage de moyens de chiffrement et de la signature électronique sont connues respectées.
- 4.2.4.6.4. Vérifier que la loi sur l'archivage électronique est connue et respectée ;
- 4.2.4.6.5. Vérifier que les articles sur la propriété intellectuelle / logiciel « pirate » sont connus respectés.

Sur le modèle présenté ci-haut (5.1), compléter et achever les points suivants :

- 4.2.5. *Critères classés par objectifs de contrôle*
- 4.2.6. *Éléments requis classés critère*
- 4.2.7. *Questions d'évaluation classées par critère*
- 4.2.8. *Risques classés questions d'évaluation*
- 4.2.9. *Conséquences classé par risque*



Votre feuille de calcul devrait être sur le même modèle que celle obtenue à l'issue de la Section 4.1

#### 4.2.10. Conduire une Mission d'Audit de la Fonction Informatique

##### 4.2.10.1. Phase 1 : Planification

La phase de planification constitue une étape clé pour définir les fondations d'un audit réussi. Elle permet de clarifier les objectifs, de délimiter le périmètre, d'identifier les risques associés et de structurer les actions à venir en tenant compte des ressources disponibles et des parties prenantes. À travers cette phase, les tâches suivantes seront réalisées pour garantir une approche méthodique et efficace de l'audit.

###### 4.2.10.1.1. Définir les objectifs de l'audit :

- ☒ Évaluer l'efficacité de la fonction informatique dans la réalisation des objectifs stratégiques de l'organisation.
- ☒ Vérifier la conformité avec les cadres de gouvernance (COBIT, ITIL, ISO 20000).
- ☒ Identifier les risques liés à la gestion des ressources, des projets et des opérations IT.

###### 4.2.10.1.2. Délimiter le périmètre :

- ☒ Définir les domaines à auditer : organisation de la fonction, gestion des ressources humaines et financières, gestion des projets, services IT, gouvernance, etc.
- ☒ Préciser les interactions avec les autres fonctions de l'organisation (finance, RH, production).

###### 4.2.10.1.3. Analyser les risques associés à la fonction IT :

- ☒ Cartographier les principaux risques : obsolescence technologique, mauvaise gestion des fournisseurs, insuffisance des compétences, dépassements budgétaires.
- ☒ Prioriser les risques en fonction de leur impact et de leur probabilité.

Référence savante : ITGI (2007) dans *Enterprise Value: Governance of IT Investments* souligne que l'alignement stratégique et la gestion efficace des ressources sont des objectifs primordiaux d'un audit IT.

###### 4.2.10.1.4. Établir le plan d'audit :

- ☒ Détailler les tâches à accomplir, les outils nécessaires et les étapes à suivre.
- ☒ Identifier les parties prenantes clés à consulter (DSI, chefs de service, utilisateurs finaux).

###### 4.2.10.1.5. Préparer le questionnaire d'audit :

- ☑ Inclure des questions sur la gouvernance, la gestion des projets, la planification stratégique, et les processus opérationnels.

#### 4.2.10.1.6. Documents à solliciter :

- ☑ Organigramme de la fonction IT.
- ☑ Plan stratégique informatique.
- ☑ Budgets IT des trois dernières années.
- ☑ Politiques et procédures IT (gestion des changements, des incidents, des problèmes).
- ☑ Rapports d'activité IT.

#### 4.2.10.1.7. Actions complémentaires :

- ☑ Réunir les informations nécessaires sur les principales parties prenantes et leur rôle dans la fonction IT.
- ☑ Évaluer les certifications des employés (CISA, ITIL, PMP, etc.).

### 4.2.10.2. Phase 2 : Exécution

La phase d'exécution est le cœur de la mission d'audit, où les plans définis prennent vie à travers des actions concrètes. Elle consiste à collecter les preuves, analyser les données, observer les pratiques, et évaluer les systèmes et processus en fonction des critères établis. Les tâches suivantes seront réalisées pour garantir une évaluation rigoureuse et objective de la situation auditée.

#### 4.2.10.2.1. Analyse documentaire :

- ☑ Examiner les politiques, procédures et plans pour vérifier leur pertinence et conformité avec les standards internationaux.
- ☑ Vérifier la mise en œuvre du cadre de gouvernance adopté (ex. COBIT).
- ☑ Analyser les budgets pour identifier les écarts entre planification et exécution.

#### 4.2.10.2.2. Entrevues et observations :

- ☑ Interviewer le DSI pour comprendre la stratégie, les défis et les priorités de la fonction IT.
- ☑ Rencontrer les chefs de projet pour analyser les processus de gestion des projets.
- ☑ Observer les opérations IT (gestion des incidents, changements) pour évaluer leur efficacité.

#### 4.2.10.2.3. Évaluation des processus clés :

- ☑ Évaluer la gestion des services IT :
  - Niveau de maturité des processus (modèle CMMI ou équivalent).
  - Respect des SLA avec les utilisateurs internes et externes.
- ☑ Examiner la gestion des ressources humaines IT :
  - Disponibilité des compétences nécessaires.
  - Formation et développement professionnel.
- ☑ Vérifier les outils et technologies utilisés pour la gestion des services et des projets.

#### 4.2.10.2.4. Tests et analyses :

- ☑ Analyser la performance des projets IT récents : respect des délais, budgets, et objectifs.
- ☑ Évaluer la gestion des fournisseurs (contrats, SLA, respect des engagements).
- ☑ Tester la continuité des activités en cas de sinistre (vérification du PRA et PCA).

#### 4.2.10.2.5. Documents à solliciter :

- ☑ Rapports d'analyse budgétaire (prévisions vs dépenses).
- ☑ Registre des risques IT.
- ☑ SLA (accords de niveau de service) et contrats de fournisseurs.
- ☑ Rapports de projets récents.
- ☑ Rapports de gestion des incidents et des problèmes.

#### 4.2.10.2.6. Actions complémentaires :

- ☑ Utiliser des outils comme ServiceNow pour analyser les processus opérationnels.
- ☑ Réaliser un benchmark des pratiques IT avec des organisations similaires.

### 4.2.10.3. Phase 3 : Communication des résultats

La phase de communication des résultats constitue l'aboutissement de l'audit, où les constats, analyses et recommandations sont présentés de manière claire et structurée aux parties prenantes. Cette étape vise à fournir des informations exploitables et à favoriser l'engagement pour la mise en œuvre des actions correctives. Les tâches suivantes seront réalisées pour assurer une restitution efficace et impactante des conclusions de l'audit.

#### 4.2.10.3.1. Rédiger le rapport d'audit :

- ☑ Structurer le rapport en incluant :
  - Résumé des points forts et faibles.
  - Analyse des écarts entre les pratiques actuelles et les standards.
  - Recommandations détaillées et priorisées selon l'impact et la faisabilité.
- ☑ Fournir des indicateurs quantitatifs pour appuyer les constats (ex. budgets dépassés, délais non respectés).

#### 4.2.10.3.2. Préparer une synthèse exécutive :

- ☑ Présenter les constats et recommandations clés dans un format accessible pour la direction générale.
- ☑ Insister sur l'impact stratégique des recommandations.

#### 4.2.10.3.3. Restituer les résultats :

- ☑ Organiser une réunion de restitution avec la DSI et les parties prenantes clés.
- ☑ Mettre en avant les bénéfices de la mise en œuvre des recommandations (amélioration de la performance, réduction des coûts, etc.).
- ☑ Discuter et valider le plan d'action correctif.

#### 4.2.10.3.4. Documents à solliciter :

- ☑ Rapport final approuvé par l'équipe d'audit.
- ☑ Feuille de route pour les actions correctives.
- ☑ PV de la réunion de restitution.

#### 4.2.10.3.5. Actions complémentaires :

- ☑ Proposer un calendrier pour suivre les progrès de la mise en œuvre des recommandations.
- ☑ Établir des KPI pour mesurer l'évolution de la maturité de la fonction IT.
- ☑ **Willcocks et Smith (1995) dans Managing IT as a Strategic Resource** : insistent sur l'importance d'un alignement étroit entre la gouvernance IT et les objectifs métiers.
- ☑ **Ross et Weill (2004) dans IT Governance: How Top Performers Manage IT Decision Rights for Superior Results** : offrent des cadres solides pour évaluer la gouvernance IT et sa valeur pour l'organisation.
- ☑ **COBIT Framework (ISACA)** : reste une référence incontournable pour l'évaluation de la fonction informatique, en particulier dans les audits de gouvernance et de processus IT.



## 4.3. Audit et Contrôle des Projets Informatiques

Un projet est un ensemble de tâches interdépendantes concourant à la réalisation d'un objectif prédéfini et mesurable avec des spécifications, des contraintes, des moyens humains, financiers et matériels, des délais (un début, une fin) et des risques.

Un projet informatique produit généralement de nouvelles applications et/ou maintien des applications existantes. Il peut aussi s'agir d'un renouvellement matériel majeur.

La conduite de projet est un ensemble de processus permettant de maîtriser la réalisation d'un projet et de la mener à terme.

Cette maîtrise passe par un découpage du projet en processus, étapes, phases, activités et tâches. Il est indispensable d'avoir une définition claire des entrées des processus, des phases et étapes, des productions attendues et des conditions de passage d'une phase à l'autre. Par ailleurs, le rôle et les responsabilités des acteurs doivent être clairement définis.

### 4.3.1. But

L'audit des projets informatiques vise à s'assurer que les projets informatiques au sein de l'entité se déroulent normalement et que l'enchaînement des opérations se fait de manière logique et efficace, de façon que l'on ait de fortes chances d'arriver à la fin de la phase de développement à une application qui sera performante et opérationnelle.

### 4.3.2. Fréquence recommandée pour les audits

Il est recommandé d'auditer tous les projets informatiques dès leur terme, qu'ils soient achevés ou tout simplement abandonnés ou même suspendus pour une période prolongée.

### 4.3.3. Points de contrôle

Conformément au guide d'audit des systèmes d'information, section consacrée à l'audit de la fonction informatique page 73-90, les points de contrôle de ce type d'audit sont au nombre de 15, et définis comme suit :

- 4.3.3.1. Objectifs et enjeux du projet ;
- 4.3.3.2. Étude d'opportunité et expression des besoins ;
- 4.3.3.3. Planification ;
- 4.3.3.4. Instances de pilotage;
- 4.3.3.5. Méthodes et outils;
- 4.3.3.6. Qualité;
- 4.3.3.7. Conception générale et analyse ;
- 4.3.3.8. Conception détaillée ;
- 4.3.3.9. Développement, réalisation ou paramétrage ;
- 4.3.3.10. Tests et recettes ;
- 4.3.3.11. Conduite du changement et mise en œuvre ;

- 4.3.3.12. *Documentation ;*
- 4.3.3.13. *Structures mises en place à l'occasion du projet ;*
- 4.3.3.14. *Gestion des évolutions ;*
- 4.3.3.15. *Mise en production.*

#### 4.3.4. *Quelques objectifs de contrôle classés par point de contrôle*

##### 4.3.4.1. *Objectifs et enjeux du projet*

- 4.3.4.1.1. S'assurer qu'une étude de la valeur et des études d'opportunité et d'impacts ont été réalisées ;
- 4.3.4.1.2. S'assurer qu'un bilan critique des processus existants a été effectué ;
- 4.3.4.1.3. S'assurer que le choix de recourir à un nouveau système est obtenu après optimisation des processus concernés et vérification que cette optimisation ne suffit pas à apporter par elle-même les gains de performance attendus ;
- 4.3.4.1.4. S'assure que les objectifs et périmètres du projet sont définis, partagés et stabilisés ;
- 4.3.4.1.5. S'assurer que les principales orientations du système cible ont été explicitées ;
- 4.3.4.1.6. S'assurer que les principaux acteurs sont identifiés ;
- 4.3.4.1.7. S'assurer que les coûts sont évalués ;
- 4.3.4.1.8. S'assurer que les liens et impacts avec des projets connexes et les infrastructures (Datacenter, réseaux, etc.) sont pris en compte.

##### 4.3.4.2. *Étude d'opportunité et expression des besoins*

- 4.3.4.2.1. S'assurer que l'expression détaillée des besoins est formalisée dans un cahier des charges fait par la MOA ;
- 4.3.4.2.2. S'assurer que le cahier des charges préconise une solution fonctionnellement et techniquement pertinente au regard des besoins exprimés ;
- 4.3.4.2.3. S'assurer que les exigences utilisateurs, les populations ciblées, les options et principes de gestion retenus sont précisés et priorisés ;
- 4.3.4.2.4. S'assurer que le projet est cohérent avec le plan directeur informatique ;
- 4.3.4.2.5. S'assurer que le projet est cohérent avec le SI actuel ou futur ;
- 4.3.4.2.6. S'assurer que la direction est bien impliquée dans le projet ;
- 4.3.4.2.7. S'assurer que les acteurs de l'équipe projet et leurs responsabilités sont bien identifiés ;
- 4.3.4.2.8. S'assurer que les compétences du personnel sont en adéquation avec les tâches ;
- 4.3.4.2.9. S'assurer qu'une étude d'opportunité est validée ;
- 4.3.4.2.10. S'assurer que ce document comprend les objectifs du projet ;
- 4.3.4.2.11. S'assurer que ce document comprend l'analyse des déficiences des systèmes existants ;

- 4.3.4.2.12. S'assurer que ce document comprend les enjeux et la faisabilité du projet ;
- 4.3.4.2.13. S'assurer que ce document comprend les bénéfices attendus et la rentabilité économique du projet ;
- 4.3.4.2.14. S'assurer que ce document comprend les contraintes relatives au projet ;
- 4.3.4.2.15. S'assurer que ce document comprend la liste des acteurs concernés ;
- 4.3.4.2.16. S'assurer que l'étude d'opportunité a été revue par les directions utilisatrices et par la direction informatique ;
- 4.3.4.2.17. S'assurer que l'approbation de l'étude d'opportunité a été formalisée par écrit par une personne ayant autorité pour le faire.

#### 4.3.4.3. *Planification*

- 4.3.4.3.1. S'assurer qu'il existe un planning directeur commun à tout le projet ;
- 4.3.4.3.2. S'assurer qu'il existe un plan de projet initial ;
- 4.3.4.3.3. S'assurer que ce plan de projet a été révisé ;
- 4.3.4.3.4. S'assurer qu'il existe des plans détaillés ;
- 4.3.4.3.5. S'assurer que ces plans ont été révisés ;
- 4.3.4.3.6. S'assurer que les plans intègrent une gestion optimale des ressources ;
- 4.3.4.3.7. S'assurer qu'il existe une évaluation des risques liés à la nature du projet ;
- 4.3.4.3.8. S'assurer qu'il existe une évaluation des risques liés à la technologie utilisée ;
- 4.3.4.3.9. S'assurer qu'il existe une évaluation des risques liés aux projets en cours ;
- 4.3.4.3.10. S'assurer qu'il existe une évaluation des risques liés aux délais ;
- 4.3.4.3.11. S'assurer qu'il existe une évaluation des risques liés à la synchronisation des activités ;
- 4.3.4.3.12. S'assurer que les acteurs se sont engagés à respecter le planning général du projet ;
- 4.3.4.3.13. S'assurer que les lots sont bien identifiés et suivis dans le planning ;
- 4.3.4.3.14. S'assurer que les lots sont bien identifiés et suivis dans le planning ;
- 4.3.4.3.15. S'assurer qu'une estimation périodique du reste à faire est effectuée ;
- 4.3.4.3.16. S'assurer qu'il existe des "capteurs" d'alerte ;
- 4.3.4.3.17. S'assurer qu'il existe des procédures pour traiter les alertes urgentes ;
- 4.3.4.3.18. S'assurer qu'une méthode d'estimation des charges est appliquée ;
- 4.3.4.3.19. S'assurer que cette méthode est cohérente ;



- 4.3.4.3.20. S'assurer que la mise en adéquation des moyens techniques est cohérente.

#### 4.3.4.4. *Instances de pilotage*

- 4.3.4.4.1. S'assurer que la structure de pilotage est formalisée et connue de tous les acteurs ;
- 4.3.4.4.2. S'assurer que les différentes instances de pilotage connaissent leurs niveaux de délégation ;
- 4.3.4.4.3. S'assurer que les objectifs des délégations sont atteints ;
- 4.3.4.4.4. S'assurer qu'il existe un comité de pilotage ;
- 4.3.4.4.5. S'assurer qu'il existe un comité de projet ;
- 4.3.4.4.6. S'assurer qu'il existe un comité des utilisateurs ou, a minima, une participation des utilisateurs ;
- 4.3.4.4.7. S'assurer que les participants aux différents comités sont représentatifs et ont le bon niveau de décision ;
- 4.3.4.4.8. S'assurer que les participants ne sont pas trop nombreux, au Cameroun un texte du Premier Ministre encadre le nombre de participants aux comités, commissions et groupe de travail ;
- 4.3.4.4.9. S'assurer que les gestionnaires de la production sont intégrés dans les structures de pilotage ;
- 4.3.4.4.10. S'assurer que la fréquence des comités est appropriée ;
- 4.3.4.4.11. S'assurer qu'il existe une réunion périodique de revue du projet pour suivre son avancement ;
- 4.3.4.4.12. S'assurer que la traçabilité des évolutions de périmètre, coût et délai est assurée ;
- 4.3.4.4.13. S'assurer qu'il existe des indicateurs de suivi du projet ;
- 4.3.4.4.14. S'assurer que les indicateurs sont adaptés à l'étape en cours ;
- 4.3.4.4.15. S'assurer que les indicateurs sont mis à jour ;
- 4.3.4.4.16. S'assurer que les indicateurs sont pertinents par rapport aux objectifs du projet (contraintes de délais, de qualité, de coût, ...) ;
- 4.3.4.4.17. S'assurer qu'il existe un formalisme de reporting (tableau de bord par exemple) ;
- 4.3.4.4.18. S'assurer que la fréquence du reporting est correcte.

#### 4.3.4.5. *Méthodes et outils*

- 4.3.4.5.1. S'assurer qu'il existe une méthode de conduite de projet et celle-ci est appliquée ;
- 4.3.4.5.2. S'assurer que la méthode repose sur un découpage des projets en tâches ;
- 4.3.4.5.3. S'assurer que la méthode repose sur une attribution formelle des responsabilités par tâche ;
- 4.3.4.5.4. S'assurer que la méthode repose sur une identification précise des points de contrôle et des livrables ;
- 4.3.4.5.5. S'assurer que la méthode repose sur un reporting des temps à travers une feuille de temps ;
- 4.3.4.5.6. S'assurer que la méthode repose sur un outil de planification ;

- 4.3.4.5.7. S'assurer que la méthode repose sur des outils ;
- 4.3.4.5.8. S'assurer que les outils de suivi des délais et des coûts sont adaptés ;
- 4.3.4.5.9. S'assurer que le plan général du projet est suffisamment précis ;
- 4.3.4.5.10. S'assurer que les tâches identifiées constituent des unités gérables ;
- 4.3.4.5.11. S'assurer que les tâches identifiées constituent des unités gérables.

#### 4.3.4.6. *Qualité*

- 4.3.4.6.1. S'assurer qu'il existe un dispositif d'assurance qualité documenté ;
- 4.3.4.6.2. S'assurer qu'il existe un manuel d'assurance qualité de l'entité ;
- 4.3.4.6.3. S'assurer qu'il existe un plan d'assurance qualité du projet ;
- 4.3.4.6.4. S'assurer que les objectifs de qualité du produit sont formalisés ;
- 4.3.4.6.5. S'assurer que les objectifs de qualité de service attendu sont formalisés ;
- 4.3.4.6.6. S'assurer que le groupe assurance qualité est indépendant des équipes de développement du projet ;
- 4.3.4.6.7. S'assurer qu'une procédure de suivi des revues d'assurance qualité est formalisée ;
- 4.3.4.6.8. S'assurer que les conclusions des revues d'assurance qualité sont prises en compte par l'équipe projet ;
- 4.3.4.6.9. S'assurer qu'il existe un circuit d'approbation des livrables ;
- 4.3.4.6.10. S'assurer que ce circuit d'approbation est pertinent ;
- 4.3.4.6.11. S'assurer qu'il existe un audit de la qualité du projet par une personne extérieure.

#### 4.3.4.7. *Conception générale et analyse*

- 4.3.4.7.1. S'assurer qu'il existe une analyse des différents scénarios possibles en termes de solution retenue ;
- 4.3.4.7.2. S'assurer que tous les scénarios ont été envisagés, même celui de ne rien faire ;
- 4.3.4.7.3. S'assurer que les contraintes liées aux technologies (besoins en matériels, en formation, en RH, contraintes juridiques, faisabilité opérationnelle, ...) ont été prises en compte ;
- 4.3.4.7.4. S'assurer qu'une analyse économique (bénéfices attendus, coûts de développement, de formation, de maintenance, ...) a été intégrée au choix de la solution ;
- 4.3.4.7.5. S'assurer qu'une analyse des risques a été mise en place pour chaque alternative ;
- 4.3.4.7.6. S'assurer que le choix de la solution a été fait en toute objectivité en se basant sur des critères d'évaluation pertinents ;
- 4.3.4.7.7. S'assurer que les aspects de contrôle interne et de sécurité ont été pris en compte dans le cahier des charges ;

- 4.3.4.7.8. S'assurer que les contrôles d'exploitation ont été identifiés ;
- 4.3.4.7.9. S'assurer que la conception générale du futur système s'inscrit dans les objectifs généraux de contrôle en vigueur, dans l'environnement ;
- 4.3.4.7.10. S'assurer que les besoins spécifiques en matière de contrôles ont été pris en considération ;
- 4.3.4.7.11. S'assurer que les besoins en matière de contrôles programmés ont été identifiés et décrits ;
- 4.3.4.7.12. S'assurer que les études de faisabilité ont été revues par les membres du comité adéquat ;
- 4.3.4.7.13. S'assurer que les différentes solutions possibles ont été présentées au comité adéquat ;
- 4.3.4.7.14. S'assurer que la poursuite du projet a été approuvée par écrit par une personne compétente.

#### 4.3.4.8. *Conception détaillée*

- 4.3.4.8.1. S'assurer qu'il existe une méthode d'analyse et de conception ;
- 4.3.4.8.2. S'assurer que cette méthode est correctement utilisée ;
- 4.3.4.8.3. S'assurer que cette méthode est maîtrisée par l'équipe projet ;
- 4.3.4.8.4. S'assurer que les spécifications détaillées sont exhaustives par rapport au cahier des charges ;
- 4.3.4.8.5. S'assurer qu'il existe des contrôles adaptés à chaque point critique du système (préventifs et correctifs) ;
- 4.3.4.8.6. S'assurer que le responsable de la sécurité est impliqué dans le projet ;
- 4.3.4.8.7. S'assurer qu'il existe des pistes d'audit permettant de suivre la totalité des transactions ;
- 4.3.4.8.8. S'assurer que les acteurs concernés sont impliqués dans le projet (utilisateurs, administrateurs de données, responsable sécurité, ...) ;
- 4.3.4.8.9. S'assurer que la conception détaillée a été revue ;
- 4.3.4.8.10. S'assurer que la poursuite du projet a été approuvée par écrit par une personne compétente.

#### 4.3.4.9. *Développement, réalisation ou paramétrage*

- 4.3.4.9.1. S'assurer qu'il existe une méthode de développement ;
- 4.3.4.9.2. S'assurer que cette méthode est correctement utilisée ;
- 4.3.4.9.3. S'assurer que cette méthode est parfaitement maîtrisée par les développeurs ;
- 4.3.4.9.4. S'assurer qu'il existe des normes de documentation ;
- 4.3.4.9.5. S'assurer que ces normes sont appliquées par les développeurs ;
- 4.3.4.9.6. S'assurer que les développements sont bien documentés ;
- 4.3.4.9.7. S'assurer que la documentation est revue par le responsable du service des études ;
- 4.3.4.9.8. S'assurer qu'il existe un programme général de tests formalisé ;

- 4.3.4.9.9. S'assurer qu'il existe un plan de mise en place ;
- 4.3.4.9.10. S'assurer que le plan de mise en place définit la nature des travaux à réaliser et leur ordonnancement ;
- 4.3.4.9.11. S'assurer que le plan de mise en place définit les charges de travail correspondantes et la durée de travaux ;
- 4.3.4.9.12. S'assurer que le plan de mise en place définit les acteurs concernés ;
- 4.3.4.9.13. S'assurer que le plan de mise en place définit les rôles et les responsabilités des acteurs ;
- 4.3.4.9.14. S'assurer que le plan de mise en place est approuvé et diffusé ;
- 4.3.4.9.15. S'assurer qu'il existe un plan de migration ;
- 4.3.4.9.16. S'assurer que les normes de développement et de vérification du programme de conversion sont respectées ;
- 4.3.4.9.17. S'assurer que les procédures de contrôle en matière de passage en production sont respectées ;
- 4.3.4.9.18. S'assurer qu'il existe une image des systèmes et des données avant et après conversion ;
- 4.3.4.9.19. S'assurer qu'il existe une image des systèmes et des données avant et après conversion ;
- 4.3.4.9.20. S'assurer qu'il existe un dossier de spécification de paramétrage ;
- 4.3.4.9.21. S'assurer que ce dossier consigne les options retenues sur le produit.

#### 4.3.4.10. Tests et recettes

- 4.3.4.10.1. S'assurer que la MOE réalise des tests ;
- 4.3.4.10.2. S'assurer que la MOE s'assure que chacun des composants de l'application fonctionne tel qu'il a été décrit dans le dossier de spécifications ;
- 4.3.4.10.3. S'assurer que la MOE réalise des tests sur l'ensemble des composants de l'application sur le plan fonctionnel et technique ;
- 4.3.4.10.4. S'assurer que la MOE réalise des tests sur les interfaces de l'application dans le SI ;
- 4.3.4.10.5. S'assurer que des tests utilisateurs sont réalisés ;
- 4.3.4.10.6. S'assurer que les tests portent sur l'adéquation de l'application livrée par la MOE avec les besoins exprimés par la MOA ;
- 4.3.4.10.7. S'assurer que les tests portent sur l'acceptation technique du système (ergonomie, performance, qualité des entrées/sorties...) ;
- 4.3.4.10.8. S'assurer qu'il existe des tests de pré-exploitation ;
- 4.3.4.10.9. S'assurer que ces tests s'assurent de la bonne intégration de l'application dans l'environnement de production ;
- 4.3.4.10.10. S'assurer que l'application est recettée ;
- 4.3.4.10.11. S'assurer que l'application s'intègre bien dans l'ensemble du SI ;
- 4.3.4.10.12. S'assurer qu'il existe une procédure formalisée de recette finale destinée à accepter formellement l'application ;

- 4.3.4.10.13. S'assurer que tous les acteurs concernés participent activement à la phase de recette ;
- 4.3.4.10.14. S'assurer que les jeux d'essais sont pertinents et assurent l'étendue des tests ;
- 4.3.4.10.15. S'assurer que les résultats des jeux d'essais et de la recette finale sont formalisés par la direction du département utilisateur ;
- 4.3.4.10.16. S'assurer qu'il existe un dossier d'organisation de la reprise des données ;
- 4.3.4.10.17. S'assurer que le niveau de qualité des données d'origine est bien maîtrisé ;
- 4.3.4.10.18. S'assurer qu'il existe des contrôles automatiques de la qualité des données obtenues après reprise (exhaustivité et exactitude) ;
- 4.3.4.10.19. S'assurer que les utilisateurs devant participer à la reprise des données ont été mobilisés le plus tôt possible ;
- 4.3.4.10.20. S'assurer que les utilisateurs devant participer à la reprise des données ont été mobilisés le plus tôt possible ;
- 4.3.4.10.21. S'assurer que le bilan de qualité prend comme référence les exigences qualité fixées par la MOA et traduites par la MOE en objectifs et critères à respecter ;
- 4.3.4.10.22. S'assurer que le logiciel est conforme aux besoins fonctionnels exprimés par le cahier des charges ;
- 4.3.4.10.23. S'assurer que le logiciel est conforme au niveau de performance attendu ;
- 4.3.4.10.24. S'assurer que le logiciel est conforme au niveau de sécurité attendu ;
- 4.3.4.10.25. S'assurer que le logiciel est conforme au niveau de sécurité attendu.

#### *4.3.4.11. Conduite du changement et mise en œuvre*

- 4.3.4.11.1. S'assurer qu'il existe une synthèse de l'évaluation des changements ;
- 4.3.4.11.2. S'assurer que l'évaluation des changements a été validée ;
- 4.3.4.11.3. S'assurer que les entretiens réalisés sont représentatifs ;
- 4.3.4.11.4. S'assurer que les utilisateurs participent à l'évaluation des changements ;
- 4.3.4.11.5. S'assurer qu'il existe un plan de communication complet ;
- 4.3.4.11.6. S'assurer que les messages sont clairs et simples ;
- 4.3.4.11.7. S'assurer que la communication évolue et progresse par rapport au développement du projet ;
- 4.3.4.11.8. S'assurer que la communication est fortement soutenue par la MOA ;
- 4.3.4.11.9. S'assurer qu'il existe un plan de formation ;
- 4.3.4.11.10. S'assurer que la hiérarchie des personnes à former est impliquée ;
- 4.3.4.11.11. S'assurer que les profils types des personnes à former sont identifiés ;

- 4.3.4.11.12. S'assurer que la population à former est pertinente ;
- 4.3.4.11.13. S'assurer que les sessions de formations sont évaluées et repensées selon l'évaluation ;
- 4.3.4.11.14. S'assurer que le planning de formation est cohérent avec le planning du projet ;
- 4.3.4.11.15. S'assurer que la durée du programme de formation est pertinente ;
- 4.3.4.11.16. S'assurer que les formateurs et le contenu de la formation sont de qualité ;
- 4.3.4.11.17. S'assurer qu'il existe une procédure d'évaluation des formés et des formateurs ;
- 4.3.4.11.18. s'assurer que l'organisation générale de la formation est bien anticipée.
- 4.3.4.11.19. S'assurer que les différents niveaux de soutien sont coordonnés et cohérents ;
- 4.3.4.11.20. S'assurer que le niveau de qualité des données d'origine est bien maîtrisé ;
- 4.3.4.11.21. S'assurer qu'il existe des contrôles automatiques de la qualité des données obtenues après reprise (exhaustivité et exactitude) ;
- 4.3.4.11.22. S'assurer que les utilisateurs devant participer à la reprise des données ont été mobilisés le plus tôt possible.

#### 4.3.4.12. *Documentation*

- 4.3.4.12.1. S'assurer qu'il existe un manuel d'utilisation ;
- 4.3.4.12.2. S'assurer que le manuel utilisateur est conforme aux normes en vigueur ;
- 4.3.4.12.3. S'assurer que le manuel d'utilisateur est disponible et compréhensible par l'ensemble des utilisateurs ;
- 4.3.4.12.4. S'assurer que le manuel utilisateur comprend les objets du système et la description des dessins d'écran et des commandes disponibles ;
- 4.3.4.12.5. S'assurer que le manuel utilisateur comprend les responsables concernant le redressement des erreurs ou anomalies ;
- 4.3.4.12.6. S'assurer que le manuel utilisateur comprend la description des sorties et leur mode de diffusion ;
- 4.3.4.12.7. S'assurer que le manuel utilisateur comprend les responsabilités en matière de sauvegarde/archivage ;
- 4.3.4.12.8. S'assurer que le manuel d'utilisateur fait l'objet d'une procédure de mise à jour ;
- 4.3.4.12.9. S'assurer qu'il existe un manuel d'exploitation ;
- 4.3.4.12.10. S'assurer que le manuel d'exploitation est accessible et compréhensible pour les opérateurs ;
- 4.3.4.12.11. S'assurer que le manuel d'exploitation a été testé lors des tests finaux ;
- 4.3.4.12.12. S'assurer que le manuel d'exploitation comprend la fonction des programmes ;

- 4.3.4.12.13. S'assurer que le manuel d'exploitation comprend le libellé exact des fichiers concernés ;
- 4.3.4.12.14. S'assurer que le manuel d'exploitation comprend la liste des messages opérateurs et les réponses attendues ;
- 4.3.4.12.15. S'assurer que le manuel d'exploitation comprend les actions à suivre en cas d'anomalies ;
- 4.3.4.12.16. S'assurer que le manuel d'exploitation comprend la liste des états générés et leurs destinations ;
- 4.3.4.12.17. S'assurer que le manuel d'exploitation comprend les procédures de reprise ;
- 4.3.4.12.18. S'assurer que le manuel d'exploitation comprend les procédures de reprise ;
- 4.3.4.12.19. S'assurer que le manuel d'exploitation fait l'objet d'une procédure de mise à jour.

#### 4.3.4.13. Structures mises en place à l'occasion du projet

- 4.3.4.13.1. S'assurer que les rôles et les responsabilités respectifs de la MOA et de la MOE sont clairement définis ;
- 4.3.4.13.2. S'assurer que les prérogatives du chef de projet sont clairement définies ;
- 4.3.4.13.3. S'assurer que le chef de projet dispose de l'autorité suffisante pour résoudre les éventuels conflits ;
- 4.3.4.13.4. S'assurer que la MOA et la MOE disposent des compétences et des ressources managériales, techniques et fonctionnelles suffisantes ;
- 4.3.4.13.5. S'assurer que les principales décisions et orientations du projet sont prises par le niveau de management adéquat ;
- 4.3.4.13.6. S'assurer que les principaux intervenants sur le projet sont 100% dédiés au projet avec suppression, pendant la durée du projet, des anciens liens hiérarchiques ;
- 4.3.4.13.7. S'assurer que la MOA ou la MOE ont bénéficié d'une assistance extérieure au cours du projet ;
- 4.3.4.13.8. S'assurer que la consultation et l'implication des utilisateurs a été suffisante au cours des différentes phases du projet ;
- 4.3.4.13.9. S'assurer qu'il existe un contrat de prestation entre la MOA et la MOE ;
- 4.3.4.13.10. S'assurer qu'il existe un engagement de résultat.

#### 4.3.4.14. Gestion des évolutions

- 4.3.4.14.1. S'assurer que les demandes d'évolution du périmètre sont fréquentes ;
- 4.3.4.14.2. S'assurer que les demandes d'évolutions sont formalisées ;
- 4.3.4.14.3. S'assurer qu'il existe une procédure de gestion des évolutions du périmètre ;
- 4.3.4.14.4. S'assurer qu'une mesure d'impact est effectuée ;
- 4.3.4.14.5. S'assurer qu'il existe une gestion des versions ;



- 4.3.4.14.6. S'assurer que les décisions sont prises dans un délai satisfaisant ;
- 4.3.4.14.7. S'assurer que les décisions sont prises sur la base d'un niveau d'information pertinent ;
- 4.3.4.14.8. S'assurer que le manuel d'exploitation fait l'objet d'une procédure de mise à jour ;
- 4.3.4.14.9. S'assurer que l'organisation de soutien aux utilisateurs est informée des évolutions et les a anticipées ;
- 4.3.4.14.10. S'assurer qu'il existe un bilan de qualité de l'évolution ;
- 4.3.4.14.11. S'assurer que le bilan de qualité prend comme référence les exigences qualité fixées par la MOA et traduites par la MOE en objectifs et critères à respecter ;
- 4.3.4.14.12. S'assurer que l'évolution est conforme aux besoins fonctionnels exprimés par le cahier des charges ;
- 4.3.4.14.13. S'assurer que l'évolution est conforme au niveau de performance attendu ;
- 4.3.4.14.14. S'assurer que l'évolution est conforme au niveau de sécurité attendu ;
- 4.3.4.14.15. S'assurer que l'évolution est conforme au niveau de convivialité attendu.

#### 4.3.4.15. *Mise en production*

- 4.3.4.15.1. S'assurer que les responsabilités respectives des directions des projets et de la production sont clairement établies et les périmètres décrits respectent les principes de séparation des tâches ;
- 4.3.4.15.2. S'assurer qu'il existe un document décrivant les responsabilités respectives des projets et de la production lors d'une mise en production ;
- 4.3.4.15.3. S'assurer que les équipes projet et de production connaissent et respectent ce document ;
- 4.3.4.15.4. S'assurer que les équipes projet et de production connaissent et respectent ce document ;
- 4.3.4.15.5. S'assurer que les équipes projet et de production connaissent et respectent ce document ;
- 4.3.4.15.6. S'assurer que les membres de l'organisation et les fournisseurs respectent leurs obligations lors de la mise en production ;
- 4.3.4.15.7. S'assurer que la bascule de la garantie vers la maintenance est organisée à travers des documents contractuels clairs.

Sur le modèle présenté ci-haut (5.1.), compléter et achever les points :

- 5.3.5. Critères classés par objectifs de contrôle
- 5.3.6. Eléments requis classés par critère
- 5.3.7. Questions d'évaluation classées par critère
- 5.3.8. Risques classés par questions d'évaluation
- 5.3.9. Conséquences classées par risque





Votre feuille de calcul devrait être sur le même modèle que celle obtenue à l'issue de la Section 4.1.

#### 4.3.5. Conduire une Mission d'Audit des Projets Informatiques

##### 4.3.5.1. Phase 1 : Planification

La phase de planification constitue une étape clé pour définir les fondations d'un audit réussi. Elle permet de clarifier les objectifs, de délimiter le périmètre, d'identifier les risques associés et de structurer les actions à venir en tenant compte des ressources disponibles et des parties prenantes. À travers cette phase, les tâches suivantes seront réalisées pour garantir une approche méthodique et efficace de l'audit.

###### 4.3.5.1.1. Définir les objectifs de l'audit :

- ☒ Évaluer la conformité des projets avec les méthodologies adoptées (PRINCE2, Agile, PMBOK, etc.).
- ☒ Identifier les risques liés à la gestion de projet : dépassements de délais, surcoûts, non-atteinte des objectifs.
- ☒ Analyser l'alignement des projets avec les objectifs stratégiques de l'organisation.



Référence savante : Kerzner (2009) dans *Project Management: A Systems Approach* souligne l'importance de l'alignement des projets avec les objectifs stratégiques pour maximiser leur impact.

###### 4.3.5.1.2. Délimiter le périmètre :

- ☒ Identifier les projets actifs et récents à auditer.
- ☒ Définir les phases du cycle de vie du projet à examiner (initiation, planification, exécution, clôture).

###### 4.3.5.1.3. Analyser les risques :

- ☒ Cartographier les risques associés aux projets : mauvaise gestion des parties prenantes, absence de suivi, modifications fréquentes des exigences.
- ☒ Évaluer les impacts potentiels sur l'organisation (ex. retards impactant la livraison d'autres projets critiques).

###### 4.3.5.1.4. Établir le plan d'audit :

- ☒ Décrire les tâches, les outils, et les techniques d'audit (ex. analyse des jalons, vérification des livrables, évaluation des budgets).
- ☒ Identifier les parties prenantes (chefs de projet, sponsors, utilisateurs clés).

###### 4.3.5.1.5. Préparer un questionnaire d'audit :

- ☒ Questions types :
  - Les projets disposent-ils d'une charte claire et validée ?
  - Les jalons clés et les indicateurs de performance (KPI) sont-ils définis et suivis ?

- Les risques sont-ils identifiés, documentés, et gérés ?

#### 4.3.5.1.6. Documents à solliciter :

- ☒ Charte et plan de projet.
- ☒ Calendrier des jalons et livrables.
- ☒ Rapport de suivi des projets (progress reports).
- ☒ Registre des risques et plans d'atténuation.
- ☒ Budget du projet et rapports financiers.

#### 4.3.5.1.7. Actions complémentaires :

- ☒ Organiser une réunion initiale avec les parties prenantes pour clarifier les objectifs de l'audit.
- ☒ Collecter les données sur les outils de gestion de projet utilisés (ex : MS Project, JIRA).

### 4.3.5.2. Phase 2 : Exécution

La phase d'exécution est le cœur de la mission d'audit, où les plans définis prennent vie à travers des actions concrètes. Elle consiste à collecter les preuves, analyser les données, observer les pratiques, et évaluer les systèmes et processus en fonction des critères établis. Les tâches suivantes seront réalisées pour garantir une évaluation rigoureuse et objective de la situation auditée.

#### 4.3.5.2.1. Analyse documentaire :

- ☒ Examiner les chartes et plans de projet pour s'assurer qu'ils sont complets et alignés avec les objectifs organisationnels.
- ☒ Vérifier la cohérence entre les livrables, les jalons, et les indicateurs de performance.
- ☒ Évaluer les plans de communication et leur efficacité dans la gestion des parties prenantes.

#### 4.3.5.2.2. Entrevues et observations :

- ☒ Interviewer les chefs de projet pour comprendre les défis rencontrés et leur gestion.
- ☒ Rencontrer les membres clés de l'équipe pour évaluer leur compréhension des objectifs et des processus.
- ☒ Observer les réunions de suivi pour évaluer leur efficacité (réunions d'avancement, de risque, etc.).

#### 4.3.5.2.3. Évaluation des processus de gestion :

- ☒ Évaluer la gestion des changements : sont-ils documentés, validés et gérés correctement ?
- ☒ Vérifier la gestion des ressources humaines : disponibilité et compétence des équipes.
- ☒ Analyser la gestion des fournisseurs et des contrats liés aux projets.

#### 4.3.5.2.4. Vérification technique et financière :

- ☒ Comparer le budget initial avec les dépenses actuelles pour identifier les écarts.
- ☒ Vérifier les livrables par rapport aux critères de qualité définis.
- ☒ Auditer les outils de gestion de projet utilisés pour s'assurer qu'ils facilitent le suivi et la communication.

#### 4.3.5.2.5. Documents à solliciter :

- ☑ Registre des changements (Change Log).
- ☑ Rapports d'avancement et tableaux de bord (Dashboards).
- ☑ Liste des parties prenantes et leur niveau d'implication.
- ☑ Contrats avec les fournisseurs liés au projet.

#### 4.3.5.2.6. Actions complémentaires :

- ☑ Réaliser une analyse comparative avec des projets similaires (benchmarking).
- ☑ Vérifier l'intégration des enseignements tirés des projets antérieurs dans la gestion actuelle.

#### 4.3.5.3. Phase 3 : Communication des résultats

La phase de communication des résultats constitue l'aboutissement de l'audit, où les constats, analyses et recommandations sont présentés de manière claire et structurée aux parties prenantes. Cette étape vise à fournir des informations exploitables et à favoriser l'engagement pour la mise en œuvre des actions correctives. Les tâches suivantes seront réalisées pour assurer une restitution efficace et impactante des conclusions de l'audit.

##### 4.3.5.3.1. Rédiger le rapport d'audit :

- ☑ Inclure les sections suivantes :
  - Résumé des points forts et des lacunes.
  - Analyse des écarts entre le plan initial et la situation actuelle.
  - Recommandations hiérarchisées selon leur urgence et leur impact.
- ☑ Soutenir les constatations avec des données quantitatives (ex. dépassements budgétaires en pourcentage, retards moyens).

##### 4.3.5.3.2. Préparer une synthèse exécutive :

- ☑ Simplifier les constats et recommandations pour les rendre accessibles aux décideurs (ex. comité de direction).
- ☑ Proposer des actions correctives pour améliorer les pratiques de gestion de projet.

##### 4.3.5.3.3. Restituer les résultats :

- ☑ Organiser une présentation interactive avec les parties prenantes.
- ☑ Discuter des axes prioritaires pour la mise en œuvre des recommandations.
- ☑ Suggérer un plan de suivi pour garantir l'amélioration continue.

##### 4.3.5.3.4. Documents à solliciter :

- ☑ Rapport final validé.
- ☑ Feuille de route pour les actions correctives.
- ☑ Procès-verbal de la réunion de restitution.

##### 4.3.5.3.5. Actions complémentaires :

- ☑ Proposer des ateliers de formation ou de sensibilisation pour améliorer les pratiques de gestion de projet.
- ☑ Suivre les recommandations avec des indicateurs (KPI) tels que le respect des délais, la gestion des risques, ou la satisfaction des parties prenantes.



- ☑ **PMI (Project Management Institute) dans PMBOK Guide (7e édition) :** fournit un cadre pour évaluer la gestion des projets à chaque étape du cycle de vie.
- ☑ **Kerzner (2009) dans Advanced Project Management :** met l'accent sur l'importance de l'audit comme un outil pour améliorer la gestion des projets et réduire les échecs.
- ☑ **Wideman (1992) dans Project and Program Risk Management :** propose des approches pour auditer et améliorer la gestion des risques dans les projets.

## 4.4. Audit du Support Utilisateur et de la Gestion du Parc

La mission de la fonction support est orientée autour de deux axes :

- ☑ fournir l'assistance et le support aux utilisateurs des systèmes d'information et améliorer en permanence leur niveau de satisfaction ;
- ☑ améliorer la performance globale des systèmes.

La performance d'un centre d'assistance (help-desk) ainsi que ses répercussions sur la productivité des utilisateurs doivent être évalués.

Il est nécessaire que la fonction de support d'une part anticipe ses besoins et dimensionne convenablement ses équipes et, d'autre part, contribue à la mise en place de règles de gestion du matériel et des applications informatiques de l'organisation en analysant le retour d'expérience.

### 4.4.1. But

Elle doit permettre d'identifier les domaines sur lesquels il semble possible d'accroître la productivité des utilisateurs, notamment les besoins en formation.

### 4.4.2. Fréquence recommandée pour les audits

Il est recommandé d'auditer la fonction support chaque trois (2) ans en moyenne et lorsqu'il y a des changements qui y surviennent comme la mise en place ou l'extinction d'un service ou d'une application, ou encore la désignation de nouveaux responsables.

### 4.4.3. Points de contrôle

Conformément au guide d'audit des systèmes d'information, section consacrée à l'audit du support utilisateurs et de la gestion du parc page 67 et 68, les points de contrôle de ce type d'audit sont au nombre de 4, et définis comme suit :

- 4.4.3.1. *Fonction support : audit fiabilité et sécurité ;*
- 4.4.3.2. *Fonction support : audit d'efficacité et de performance ;*
- 4.4.3.3. *Gestion du parc matériel et logiciel : audit fiabilité et sécurité ;*
- 4.4.3.4. *Gestion du parc matériel et logiciel : audit d'efficacité et de performance.*

### 4.4.4. Quelques objectifs de contrôle classés par point de contrôle

#### 4.4.4.1. *Fonction support : audit fiabilité et sécurité*

- 4.4.4.1.1. S'assurer qu'une structure de centre d'assistance (help-desk) (HD) est mise en place ;
- 4.4.4.1.2. S'assurer qu'une procédure de gestion des demandes d'assistance est diffusée et connue des utilisateurs ;
- 4.4.4.1.3. S'assurer qu'une procédure d'escalade mise en place ;
- 4.4.4.1.4. S'assurer de la couverture géographique du HD ;
- 4.4.4.1.5. S'assurer de la couverture fonctionnelle du HD ;

- 4.4.4.1.6. S'assurer qu'un outil est implémenté pour la prise d'appel et le suivi des tickets ;
- 4.4.4.1.7. S'assurer que des critères à renseigner pour la qualification des tickets existent ;
- 4.4.4.1.8. S'assure qu'il existe une liste de questions à dérouler lors d'un appel afin préciser au mieux la demande de l'utilisateur ;
- 4.4.4.1.9. S'assurer que les problèmes sont gérés ;
- 4.4.4.1.10. S'assurer qu'un processus de gestion des problèmes existe ;
- 4.4.4.1.11. S'assurer que les incidents de production de nuit et jour ferrier sont aussi saisis dans l'outil ;
- 4.4.4.1.12. S'assurer que des comités mis en place pour suivre les incidents et leur résolution existent et définissent, Qui participe, et comment sont suivies les actions ;
- 4.4.4.1.13. S'assurer que si le HD est externalisé, il existe un contrat de service ;
- 4.4.4.1.14. S'assurer que les indicateurs pour suivre le contrat de service existent ;
- 4.4.4.1.15. S'assurer qu'il y a un planning systématique concernant les mises en production ;
- 4.4.4.1.16. S'assurer que le DSI, le responsable HD, des utilisateurs, et l'équipe HD participent à la vie du HD ;
- 4.4.4.1.17. Vérifier les extractions de la base de ticket ;
- 4.4.4.1.18. Vérifier les reporting de suivi.

#### 4.4.4.2. *Fonction support : audit d'efficacité et de performance*

- 4.4.4.2.1. S'assurer qu'il existe une aide à la saisie pour la saisie des tickets ;
- 4.4.4.2.2. S'assurer qu'il existe des revues qualité pour la saisie des tickets ;
- 4.4.4.2.3. Vérifier l'existence d'une base de connaissance ;
- 4.4.4.2.4. S'assurer qu'une procédure de mise à jour de la base de connaissance existe ;
- 4.4.4.2.5. S'assurer que les appels sont enregistrés ;
- 4.4.4.2.6. S'assurer que des études de satisfaction sont réalisées auprès des utilisateurs ;
- 4.4.4.2.7. S'assurer qu'il existe une évaluation de l'équipe HD, notamment pour les prestataires afin d'en évaluer le niveau de connaissance ;
- 4.4.4.2.8. S'assurer que l'obtention des certifications (ITIL, ISO, COBIT, SIGMA) est encouragée au sein de la DSI, et du HD en particulier ;
- 4.4.4.2.9. Vérifier la stratégie de formation des utilisateurs et de l'équipe Helpdesk ;
- 4.4.4.2.10. Vérifier que les procédures de reporting et de suivi sont fonctionnelles ;
- 4.4.4.2.11. Vérifier que les résultats des études de satisfaction sont pris en compte.

#### 4.4.4.3. *Gestion du parc matériel et logiciel : audit fiabilité et sécurité*

- 4.4.4.3.1. Vérifier la procédure de déploiement des mises à jour, d'un nouveau logiciel ;
- 4.4.4.3.2. Vérifier les outils mis en place pour gérer les versions des logiciels ;
- 4.4.4.3.3. Vérifier les outils mis en place pour gérer le matériel informatique ;
- 4.4.4.3.4. S'assurer que l'installation des PC / portables est faite à partir d'un master (configuration minimum et standardisée) ;
- 4.4.4.3.5. S'assurer qu'il existe un processus spécifique pour le suivi des mises à jour sur les portables ;
- 4.4.4.3.6. S'assurer que le déploiement de nouveaux logiciels ou mises à jour est possible à distance (utile pour les utilisateurs nomades) ;
- 4.4.4.3.7. Vérifier qu'il est possible pour le HD de prendre la main à distance, si oui, en vérifier la procédure ;
- 4.4.4.3.8. Vérifier comment est géré le parc informatique, quel type de machine, et quels outils y sont déployés ;
- 4.4.4.3.9. S'assurer que l'inventaire du parc informatique comprend la localisation des machines ;
- 4.4.4.3.10. Vérifier que les utilisateurs sont sensibilisés à la sécurité informatique, notamment à l'installation de logiciel "non officiel".

#### 4.4.4.4. *Gestion du parc matériel et logiciel : audit d'efficacité et de performance*

- 4.4.4.4.1. Vérifier comment est effectué l'inventaire des licences (logiciel, version, date de mise en production, nombre d'utilisateurs) ;
- 4.4.4.4.2. S'assurer que les outils de type SAM (Software Asset Management) sont déployés ;
- 4.4.4.4.3. S'assurer qu'il existe des revues régulières des licences ;
- 4.4.4.4.4. S'assurer qu'il existe une base de données de gestion de configuration de type CMDB (Configuration Management Data Base) ;
- 4.4.4.4.5. S'assurer que la DSI est sensibilisée aux enjeux de la maîtrise des licences ? (notamment en cas de contrôle) ;
- 4.4.4.4.6. Vérifier que des audits sont réalisés ;
- 4.4.4.4.7. Vérifier qu'une politique logicielle existe.

Sur le modèle présenté ci-haut (5.1), compléter et achever les points :

- 5.4.5. Critères classés par objectifs de contrôle
- 5.4.6. Éléments requis classés par critère
- 5.4.7. Questions d'évaluation classées par critère
- 5.4.8. Risques classés par questions d'évaluation
- 5.4.9. Conséquences classées par risque.



Votre feuille de calcul devrait être sur le même modèle que celle obtenue à l'issue de la Section 4.1.

#### 4.4.5. Conduire une Mission d'Audit du Support aux utilisateurs et de la gestion du Parc

##### 4.4.5.1. Phase 1 : Planification

La phase de planification constitue une étape clé pour définir les fondations d'un audit réussi. Elle permet de clarifier les objectifs, de délimiter le périmètre, d'identifier les risques associés et de structurer les actions à venir en tenant compte des ressources disponibles et des parties prenantes. À travers cette phase, les tâches suivantes seront réalisées pour garantir une approche méthodique et efficace de l'audit.

##### 4.4.5.1.1. Définir les objectifs de l'audit :

- ☒ Évaluer la qualité du support utilisateur (temps de résolution, satisfaction).
- ☒ Vérifier la gestion du cycle de vie des équipements informatiques (acquisition, maintenance, renouvellement, mise au rebut).
- ☒ Identifier les risques liés à une gestion inefficace (pannes fréquentes, obsolescence technologique, faible satisfaction des utilisateurs).

Référence savante : Heeks (2006) dans *Implementing and Managing e-Government* insiste sur la nécessité d'une infrastructure informatique robuste et d'un support utilisateur efficace pour le succès des systèmes organisationnels.

##### 4.4.5.1.2. Délimiter le périmètre :

- ☒ Déterminer les départements, niveaux de support (1er, 2e, 3e), et catégories d'équipements à auditer.
- ☒ Identifier les logiciels de gestion utilisés (ex. ITSM, CMDB).

##### 4.4.5.1.3. Analyser les risques :

- ☒ Identifier les risques spécifiques : indisponibilité des services critiques, inventaire incomplet, absence de gestion proactive des incidents.
- ☒ Prioriser les risques par leur impact sur les utilisateurs et les opérations métier.

##### 4.4.5.1.4. Établir le plan d'audit :

- ☒ Planifier l'examen des processus de support et de gestion des actifs IT.
- ☒ Identifier les parties prenantes (DSI, équipes de support, utilisateurs finaux).

##### 4.4.5.1.5. Préparer un questionnaire d'audit :

- ☒ Questions types :
  - Les demandes d'assistance sont-elles documentées et suivies jusqu'à résolution ?
  - Les actifs informatiques sont-ils répertoriés dans une base à jour (CMDB) ?



- Les équipements obsolètes sont-ils identifiés et remplacés selon un plan ?

#### 4.4.5.1.6. Documents à solliciter :

- ☑ Politiques de gestion des incidents et des problèmes.
- ☑ Rapports d'activité des équipes de support (tickets ouverts/résolus).
- ☑ Inventaire des équipements (base CMDB, fichiers Excel, etc.).
- ☑ Contrats de maintenance et garanties des équipements.
- ☑ Rapports de satisfaction utilisateur (enquêtes, feedback).

#### 4.4.5.1.7. Actions complémentaires :

- ☑ Identifier les outils de gestion de tickets et d'inventaire utilisés (ServiceNow, GLPI, etc.).
- ☑ Planifier des entretiens avec les responsables du support et des utilisateurs finaux.

### 4.4.5.2. Phase 2 : Exécution

La phase d'exécution est le cœur de la mission d'audit, où les plans définis prennent vie à travers des actions concrètes. Elle consiste à collecter les preuves, analyser les données, observer les pratiques, et évaluer les systèmes et processus en fonction des critères établis. Les tâches suivantes seront réalisées pour garantir une évaluation rigoureuse et objective de la situation auditée.

#### 4.4.5.2.1. Analyse documentaire :

- ☑ Examiner les politiques de support utilisateur pour vérifier leur alignement avec les bonnes pratiques ITIL.
- ☑ Analyser les rapports de tickets pour évaluer le respect des SLA (temps de réponse et de résolution).
- ☑ Vérifier la mise à jour et la complétude de la base d'inventaire des équipements.

#### 4.4.5.2.2. Observation et entretiens :

- ☑ Observer les processus de support en temps réel (prise de ticket, diagnostic, résolution).
- ☑ Interviewer les techniciens pour comprendre les défis rencontrés et les processus de gestion des incidents.
- ☑ Rencontrer des utilisateurs pour évaluer leur satisfaction et leurs attentes.

#### 4.4.5.2.3. Évaluation des processus :

- ☑ Évaluer la gestion proactive des incidents : les problèmes récurrents sont-ils identifiés et traités ?
- ☑ Vérifier la conformité des équipements avec les normes de sécurité (ex. gestion des correctifs).
- ☑ Analyser le cycle de vie des équipements :
  - *Plans de renouvellement des équipements obsolètes.*
  - *Processus de mise au rebut respectant les réglementations (ex. RGPD pour la suppression des données).*

#### 4.4.5.2.4. Tests et analyses :

- ☒ Réaliser des simulations d'incidents pour évaluer la rapidité et l'efficacité des réponses (ex. panne simulée).
- ☒ Vérifier l'inventaire physique des équipements pour détecter des écarts avec les bases de données.
- ☒ Contrôler les licences logicielles pour éviter les usages non conformes ou les sous-licences.

#### 4.4.5.2.5. Documents à solliciter :

- ☒ Rapports des incidents et problèmes récurrents.
- ☒ Rapports sur les cycles de vie des équipements.
- ☒ Liste des licences logicielles et leurs statuts.
- ☒ Procédures de remplacement et de mise au rebut des équipements.

#### 4.4.5.2.6. Actions complémentaires :

- ☒ Réaliser un benchmarking avec des organisations similaires pour comparer la gestion du support et des équipements.
- ☒ Évaluer la maturité de la gestion des actifs et des services selon des modèles comme ITIL ou ISO 20000.

### 4.4.5.3. Phase 3 : Communication des résultats

La phase de communication des résultats constitue l'aboutissement de l'audit, où les constats, analyses et recommandations sont présentés de manière claire et structurée aux parties prenantes. Cette étape vise à fournir des informations exploitables et à favoriser l'engagement pour la mise en œuvre des actions correctives. Les tâches suivantes seront réalisées pour assurer une restitution efficace et impactante des conclusions de l'audit.

#### 4.4.5.3.1. Rédiger le rapport d'audit :

- ☒ Inclure les sections suivantes :
  - *Résumé des points forts et des lacunes (ex. faible satisfaction utilisateur, équipements obsolètes non remplacés).*
  - *Analyse des écarts entre les pratiques actuelles et les standards (ITIL, ISO 19770).*
  - *Recommandations hiérarchisées avec estimation des coûts et bénéfices.*

#### 4.4.5.3.2. Préparer une synthèse exécutive :

- ☒ Mettre en avant les constats critiques impactant directement les opérations métier.
- ☒ Proposer un plan d'amélioration avec des actions immédiates (ex. mise à jour de l'inventaire, formation des techniciens).

#### 4.4.5.3.3. Restituer les résultats :

- ☒ Organiser une présentation interactive avec la DSI et les responsables des équipes de support.
- ☒ Obtenir un engagement pour la mise en œuvre des recommandations.

#### 4.4.5.3.4. Documents à solliciter :

- ☒ Rapport final approuvé.
- ☒ Plan d'action pour le remplacement des équipements obsolètes.

- ☑ PV de la réunion de restitution.

#### 4.4.5.3.5. Actions complémentaires :

- ☑ Proposer un suivi trimestriel pour évaluer la mise en œuvre des recommandations.
- ☑ Définir des indicateurs de performance pour le support utilisateur (temps moyen de résolution, taux de satisfaction).

- ☑ **Van Bon et Verheijen (2006) dans Foundations of IT Service Management Based on ITIL** : guide essentiel pour auditer les processus de gestion des incidents et des actifs.
- ☑ **IT Governance Institute (2005) dans COBIT 4.1 Framework** : propose une méthodologie complète pour évaluer la gestion des actifs informatiques et du support utilisateur.
- ☑ **ISO 19770** : norme spécifique à la gestion des actifs IT, utile pour structurer l'audit du parc informatique.



## 4.5. Audit de Sécurité Informatique

L'information est un actif précieux de l'organisation. À ce titre, il faut la protéger contre la perte, l'altération et la divulgation. Les systèmes qui la supportent doivent quant à eux être protégés contre l'indisponibilité et l'intrusion.

La sécurité est une démarche globale de l'organisation, organisée autour d'une politique de sécurité. Il faut donc considérer les systèmes dans leur globalité et prendre en compte l'ensemble des acteurs.

L'informatisation et l'utilisation accrue d'internet ont induit un accroissement des risques liés à l'utilisation des technologies dans toutes les entités.

### 4.5.1. But

L'audit de la sécurité informatique a pour but de donner une assurance raisonnable quant au niveau d'exposition, en matière de sécurité, du système concerné.

### 4.5.2. Fréquence recommandée pour les audits

Il est recommandé de réaliser un audit de sécurité chaque année, et lorsqu'il y a des changements qui surviennent dans l'entité.

L'ANTIC est l'organe étatique en charge des audits de sécurité pour le compte de l'Etat du Cameroun.

### 4.5.3. Points de contrôle

Conformément au guide d'audit des systèmes d'information, section consacrée à l'audit de sécurité page 43 à 49, les points de contrôle de ce type d'audit sont au nombre de 9, et définis comme suit :

- 4.5.3.1. Facteurs clés de succès ;
- 4.5.3.2. Politique de sécurité ;
- 4.5.3.3. Organisation de la sécurité ;
- 4.5.3.4. Classification et contrôle des actifs ;
- 4.5.3.5. Sécurité du personnel ;
- 4.5.3.6. Gestion des communications et des opérations ;
- 4.5.3.7. Conformité ;
- 4.5.3.8. Gestion des identifiants et des mots de passe ;
- 4.5.3.9. Contrôle des accès ;
- 4.5.3.10. Développement et maintenance des systèmes.

### 4.5.4. Quelques objectifs de contrôle classés par point de contrôle

#### 4.5.4.1. Facteurs clés de succès

- 4.5.4.1.1. Vérifier qu'une politique de sécurité est définie et correspond à l'activité de l'Organisation ;
- 4.5.4.1.2. Vérifier qu'une démarche de mise en œuvre de la gestion de la sécurité est adoptée et compatible avec la culture de l'Organisation ;

- 4.5.4.1.3. Vérifier que la direction assure un soutien total et un engagement visible pour la sécurité;
- 4.5.4.1.4. Vérifier que les exigences de sécurité et les risques sont compris et évalués ;
- 4.5.4.1.5. Vérifier que l'ensemble des responsables et des employés sont sensibilisés et informés ;
- 4.5.4.1.6. Vérifier que les lignes directrices de la politique de sécurité et des normes de sécurité de l'information sont distribuées à tous les employés et à tous les fournisseurs ;
- 4.5.4.1.7. Vérifier que les acteurs de la sécurité sont formés de manière appropriée ;
- 4.5.4.1.8. Vérifier qu'un système de mesure complet est mis en place afin d'évaluer l'efficacité de la gestion de la sécurité de l'information et pour collecter les suggestions d'amélioration.

#### 4.5.4.2. *Politique de sécurité*

- 4.5.4.2.1. S'assurer qu'il existe une politique de sécurité formalisée avec une implication de la direction générale et une définition claire des responsabilités ;
- 4.5.4.2.2. S'assurer que la communication se fait à tous les utilisateurs sous une forme pertinente, accessible et compréhensible au lecteur ;
- 4.5.4.2.3. S'assurer qu'une revue régulière de la politique est réalisée afin de vérifier son adéquation avec ;
- 4.5.4.2.4. S'assurer que la démarche de sécurité inclut la totalité de l'informatique et non les seuls réseaux, serveurs et applications. Les imprimantes et téléphones sous IP, l'informatique technique et industrielle, l'informatique de gestion technique des bâtiments, celle de gestion des accès et temps de travail, etc. bénéficient sans exception ni zone d'ombre du dispositif de sécurité.

#### 4.5.4.3. *Organisation de la sécurité*

- 4.5.4.3.1. S'assurer qu'il existe une structure dédiée à la gestion de la sécurité de l'information : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité dans les unités ;
- 4.5.4.3.2. Vérifier qu'il y a une attribution claire des responsabilités ;
- 4.5.4.3.3. S'assurer qu'un propriétaire est désigné, il est responsable de la mise en œuvre et du suivi des évolutions à apporter ;
- 4.5.4.3.4. S'assurer qu'il existe des procédures d'autorisation de nouveaux matériels ou logiciels ;
- 4.5.4.3.5. S'assurer qu'il existe des procédures applicables à l'accès aux informations de l'organisation par des tiers ;
- 4.5.4.3.6. S'assurer que des modalités de protection de l'information confiée à des sous-traitants existent ;
- 4.5.4.3.7. Vérifier qu'il existe des modalités de réaction aux incidents de sécurité et aux défauts de fonctionnement ;

4.5.4.3.8. S'assure qu'il existe une revue régulière de la sécurité par des audits aussi bien internes qu'externes.

#### 4.5.4.4. *Classification et contrôle des actifs*

- 4.5.4.4.1. Vérifier que les actifs sont inventoriés et hiérarchisés par valeur pour l'organisation ;
- 4.5.4.4.2. Vérifier que pour tout actif important, un propriétaire est désigné et informé de ses responsabilités ;
- 4.5.4.4.3. Vérifier qu'il existe un système de classification qui définit un ensemble approprié de niveaux de protection ;
- 4.5.4.4.4. Vérifier que chaque actif a fait l'objet d'une étude visant à déterminer son niveau de classification.

#### 4.5.4.5. *Sécurité du personnel*

- 4.5.4.5.1. Vérifier que les postes et les ressources sont définis ;
- 4.5.4.5.2. Vérifier qu'il existe un programme de formation pour tous les personnels ;
- 4.5.4.5.3. Vérifier que le programme de formation prenne en compte la spécificité des postes de travail et des profils ;
- 4.5.4.5.4. Vérifier que tous les personnels participent aux formations ;
- 4.5.4.5.5. Vérifier que des évaluations « anté » et « post » formation sont réalisées pour évaluer l'impact de ces dernières ;
- 4.5.4.5.6. S'assurer que des sondages existent pour évaluer l'impact des formations dans le travail quotidien des utilisateurs.

#### 4.5.4.6. *Sécurité : gestion des communications et des opérations*

- 4.5.4.6.1. Vérifier que la documentation des procédures et les responsabilités opérationnelles existe ;
- 4.5.4.6.2. Vérifier que le contrôle des modifications opérationnelles est réalisé ;
- 4.5.4.6.3. Vérifier que des procédures de gestion des incidents existent ;
- 4.5.4.6.4. Vérifier que la séparation des fonctions et des infrastructures existe ;
- 4.5.4.6.5. Vérifier qu'une étude de sécurité en cas de gestion externe des infrastructures a été réalisée ;
- 4.5.4.6.6. Vérifier que les mesures de protection contre les infections logiques existent ;
- 4.5.4.6.7. Vérifier que les sauvegardes des données sont réalisées ;
- 4.5.4.6.8. Vérifier que les modalités de gestion des supports de données sont clairement définies ;
- 4.5.4.6.9. Vérifier que les modalités de gestion des supports de données sont appliquées.

#### 4.5.4.7. *Conformité*

- 4.5.4.7.1. Vérifier que les politique et procédures de sécurité internalisent les exigences légales et réglementaires ;
- 4.5.4.7.2. Vérifier que la convergence vers le cadre règlementaire national est recherchée ;
- 4.5.4.7.3. S'assurer qu'un document retraçant le gap entre l'état actuel des politiques et procédures de sécurité interne et le cadre réglementaire existe et est tenu à jour ;
- 4.5.4.7.4. S'assurer que tous les audits réglementaires sont réalisés ;
- 4.5.4.7.5. S'assurer qu'un responsable conformité est désigné.

#### 4.5.4.8. *Gestion des identifiants et des mots de passe*

- 4.5.4.8.1. Vérifier qu'il y a un seul utilisateur par identifiant ;
- 4.5.4.8.2. Vérifier que les identifiants inutilisés pendant un certain délai sont révoqués ;
- 4.5.4.8.3. Vérifier que des règles de gestion de la casse des mots de passe existent ;
- 4.5.4.8.4. Vérifier que ces règles sont respectées ;
- 4.5.4.8.5. Vérifier qu'il existe une procédure de gestion des mots de passe ;
- 4.5.4.8.6. Vérifier que la procédure de gestion des mots de passe statue sur leur réutilisation ;
- 4.5.4.8.7. Vérifier que la procédure de gestion des mots de passe statue sur leur stockage ;
- 4.5.4.8.8. Vérifier que la procédure de gestion des mots de passe statue sur leur diffusion ;
- 4.5.4.8.9. Vérifier que la procédure de gestion des mots de passe statue sur leur réinitialisation.

#### 4.5.4.9. *Contrôle des accès*

- 4.5.4.9.1. Vérifier que la définition et la documentation de la politique de contrôle d'accès existent ;
- 4.5.4.9.2. S'assurer que la gestion des accès utilisateurs est effective ;
- 4.5.4.9.3. S'assurer que l'utilisation de mots de passe et de systèmes de déconnexion automatique est effective ;
- 4.5.4.9.4. Vérifier que le contrôle des accès aux réseaux est effectif ;
- 4.5.4.9.5. Vérifier que le contrôle d'accès aux systèmes d'exploitation est effectif ;
- 4.5.4.9.6. Vérifier que le contrôle d'accès aux applications est effectif ;
- 4.5.4.9.7. Vérifier que la surveillance des accès aux systèmes et leur utilisation sont effectives ;
- 4.5.4.9.8. Vérifier que la gestion de l'informatique mobile est prise en compte ;
- 4.5.4.9.9. Vérifier que des suites sont systématiquement données aux incidents.

#### 4.5.4.10. *Développement et maintenance des systèmes*

- 4.5.4.10.1. S'assurer que les exigences de sécurité des systèmes existent ;
- 4.5.4.10.2. S'assurer que la sécurité des systèmes d'application est effective.
- 4.5.4.10.3. S'assurer qu'un protocole de recette existe ;
- 4.5.4.10.4. S'assurer que le protocole de recette a été testé ;
- 4.5.4.10.5. S'assurer que la sécurité des fichiers est prise en compte.

Sur le modèle présenté ci-haut (5.1), compléter et achever les points :



- 5.5.5. Critères classés par objectifs de contrôle
- 5.5.6. Eléments requis classés par critère
- 5.5.7. Questions d'évaluation classées par critère
- 5.5.8. Risques classés par questions d'évaluation
- 5.5.9. Conséquences classées par risque



Votre feuille de calcul devrait être sur le même modèle que celle obtenue à l'issue de la Section 4.1.

#### 4.5.5. Conduire une Mission d'Audit de Sécurité

##### 4.5.5.1. Phase 1 : Planification

La phase de planification constitue une étape clé pour définir les fondations d'un audit réussi. Elle permet de clarifier les objectifs, de délimiter le périmètre, d'identifier les risques associés et de structurer les actions à venir en tenant compte des ressources disponibles et des parties prenantes. À travers cette phase, les tâches suivantes seront réalisées pour garantir une approche méthodique et efficace de l'audit.

##### 4.5.5.1.1. Définir les objectifs de l'audit :

- ☒ Identifier les failles potentielles de sécurité (techniques, organisationnelles, humaines).
- ☒ Vérifier la conformité aux réglementations et standards (ISO 27001, RGPD, PCI-DSS, etc.).
- ☒ Évaluer l'efficacité des contrôles de sécurité mis en place (préventifs, détectifs et correctifs).



Référence savante : Bruce Schneier (2000), dans *Secrets and Lies: Digital Security in a Networked World*, insiste sur l'importance d'évaluer la sécurité non seulement techniquement, mais aussi organisationnellement.

##### 4.5.5.1.2. Délimiter le périmètre :

- ☒ Déterminer les domaines à auditer : réseaux, applications, postes de travail, politiques de sécurité, processus de gestion des incidents.
- ☒ Identifier les zones critiques : bases de données sensibles, accès privilégiés, systèmes connectés à l'extérieur (DMZ).

##### 4.5.5.1.3. Analyser les risques :



- ☑ Cartographier les principales menaces : cyberattaques, erreurs humaines, défaillances techniques.
- ☑ Prioriser les zones à fort impact potentiel : confidentialité, intégrité et disponibilité des données.

#### 4.5.5.1.4. Établir le plan d'audit :

- ☑ Décrire les tâches à effectuer, les ressources nécessaires, et les outils d'audit (scanners de vulnérabilités, outils de pentesting).
- ☑ Identifier les parties prenantes (RSSI, administrateurs réseau, utilisateurs clés).

#### 4.5.5.1.5. Préparer un questionnaire d'audit :

- ☑ Questions types :
  - Une politique de sécurité formalisée est-elle en place et mise à jour ?
  - Les droits d'accès sont-ils limités selon le principe du moindre privilège ?
  - Les journaux d'accès et d'activité sont-ils analysés régulièrement ?

#### 4.5.5.1.6. Documents à solliciter :

- ☑ Politique de sécurité et procédures associées.
- ☑ Registres de gestion des incidents et des risques.
- ☑ Rapports d'audits ou tests de sécurité antérieurs.
- ☑ Liste des utilisateurs et leurs niveaux d'accès.
- ☑ Journaux (logs) des systèmes critiques.

#### 4.5.5.1.7. Actions complémentaires :

- ☑ Organiser une réunion initiale pour discuter des préoccupations principales avec le RSSI et les responsables techniques.
- ☑ Identifier les outils de sécurité en place (antivirus, SIEM, firewall, etc.).

### 4.5.5.2. Phase 2 : Exécution

La phase d'exécution est le cœur de la mission d'audit, où les plans définis prennent vie à travers des actions concrètes. Elle consiste à collecter les preuves, analyser les données, observer les pratiques, et évaluer les systèmes et processus en fonction des critères établis. Les tâches suivantes seront réalisées pour garantir une évaluation rigoureuse et objective de la situation auditée.

#### 4.5.5.2.1. Analyse documentaire :

- ☑ Examiner les politiques et procédures de sécurité pour vérifier leur alignement avec les standards internationaux.
- ☑ Analyser les rapports d'incidents pour identifier les tendances ou failles récurrentes.
- ☑ Évaluer la gestion des droits d'accès, notamment pour les utilisateurs ayant des privilèges élevés.

#### 4.5.5.2.2. Observation et entretiens :

- ☑ Interviewer les administrateurs réseau et système pour comprendre les pratiques en place.
- ☑ Observer les processus de réponse aux incidents (rapidité, efficacité).
- ☑ Consulter les utilisateurs pour identifier les pratiques non conformes (shadow IT, mots de passe faibles).

#### 4.5.5.2.3. Tests techniques :

- ☑ Réaliser un scan de vulnérabilités avec des outils comme Nessus, OpenVAS, ou Qualys.
- ☑ Effectuer des tests d'intrusion sur les systèmes critiques (applications, réseaux, bases de données).
- ☑ Tester les mécanismes de défense :
  - Efficacité des firewalls et IDS/IPS.
  - Résistance aux attaques par force brute sur les authentifications.
- ☑ Analyser les logs des systèmes critiques pour détecter des anomalies.

#### 4.5.5.2.4. Vérification des contrôles :

- ☑ Valider la mise en œuvre des sauvegardes et leur capacité à être restaurées.
- ☑ Évaluer la conformité des configurations réseau (segmentation, DMZ, VPN).
- ☑ Tester la mise en œuvre des mises à jour de sécurité (correctifs).

#### 4.5.5.2.5. Documents à solliciter :

- ☑ Logs des firewalls, IDS/IPS, et SIEM.
- ☑ Plans de sauvegarde et restauration.
- ☑ Rapports de tests de vulnérabilités passés.
- ☑ Inventaire des équipements et leurs configurations.

#### 4.5.5.2.6. Actions complémentaires :

- ☑ Réaliser des simulations d'incidents de sécurité (phishing, ransomware) pour évaluer la réponse des équipes.
- ☑ Vérifier les certificats SSL et autres mécanismes de chiffrement (TLS).

### 4.5.5.3. Phase 3 : Communication des résultats

La phase de communication des résultats constitue l'aboutissement de l'audit, où les constats, analyses et recommandations sont présentés de manière claire et structurée aux parties prenantes. Cette étape vise à fournir des informations exploitables et à favoriser l'engagement pour la mise en œuvre des actions correctives. Les tâches suivantes seront réalisées pour assurer une restitution efficace et impactante des conclusions de l'audit

#### 4.5.5.3.1. Rédiger le rapport d'audit :

- ☑ Inclure les sections suivantes :
  - Constatations clés : forces et faiblesses identifiées.
  - Analyse des écarts par rapport aux standards (ISO 27001, NIST).
  - Recommandations hiérarchisées : court, moyen, et long terme.
  - Estimation des impacts des failles identifiées (confidentialité, intégrité, disponibilité).
- ☑ Illustrer les constats avec des graphiques, tableaux, ou exemples concrets (captures de logs, résultats de scans).

#### 4.5.5.3.2. Préparer une synthèse exécutive :

- ☑ Fournir une version concise pour les décideurs, mettant l'accent sur les risques critiques.
- ☑ Proposer des actions correctives et des solutions pratiques (politiques, outils).

#### 4.5.5.3.3. Restituer les résultats :

- ☑ Organiser une réunion avec le RSSI, la DSI, et les responsables métier.
- ☑ Présenter les résultats en hiérarchisant les actions en fonction des risques.
- ☑ Obtenir un consensus sur un plan d'action immédiat et de suivi.

#### 4.5.5.3.4. Documents à solliciter :

- ☑ Rapport final validé avec les constats et recommandations.
- ☑ Feuille de route pour la mise en œuvre des correctifs.
- ☑ PV de la réunion de restitution.

#### 4.5.5.3.5. Actions complémentaires :

- ☑ Proposer un suivi semestriel pour vérifier la mise en œuvre des recommandations.
- ☑ Définir des indicateurs de performance (KPI) pour mesurer l'amélioration de la sécurité :
  - Temps moyen de résolution des incidents.
  - Nombre de vulnérabilités critiques corrigées.

- ☑ **Anderson (2001) dans Security Engineering: A Guide to Building Dependable Distributed Systems** : met l'accent sur l'importance des tests techniques et des mécanismes organisationnels dans la sécurité.
- ☑ **ISO/IEC 27001** : Norme internationale pour la gestion de la sécurité de l'information, essentielle pour structurer les audits.
- ☑ **NIST Cybersecurity Framework (2014)** : propose un cadre flexible pour évaluer la posture de sécurité.
- ☑ **Shon Harris (2019) dans CISSP All-in-One Exam Guide** : fournit des détails pratiques sur l'évaluation des contrôles de sécurité et la gestion des risques.

## 4.6. Audit et Contrôle de la Fonction Etude

Les études sont une fonction sensible de la DSI en charge du développement et de la maintenance des applications informatiques. La fonction étude a la charge de la conception et de la réalisation des applications, de leur test, de leur mise en œuvre (avec la production) et de leur maintenance (corrective, réglementaire et évolutive).

### 4.6.1. But

Le but de l'audit de cette fonction consiste à analyser sa capacité à assurer la maintenance du patrimoine applicatif existant, conduire ou accompagner les évolutions à venir du système d'information conformément au plan ou au schéma directeur informatique. Il faut veiller à ne pas confondre audit des études avec audit de projet.

L'audit d'un projet s'adresse à une organisation temporaire et sur mesure, tandis que l'audit des études s'adresse à une structure permanente de l'organisation.

### 4.6.2. Fréquence recommandée pour les audits

Il est recommandé d'auditer cette fonction en moyenne chaque deux ans, et en cas de changements majeurs.

### 4.6.3. Points de contrôle

Conformément au guide d'audit des systèmes d'information, section consacrée à l'audit de la fonction informatique page 69-72, les points de contrôle de ce type d'audit sont au nombre de 3, et définis comme suit :

- 4.6.3.1. Activité de pilotage ;
- 4.6.3.2. Activités opérationnelles ;
- 4.6.3.3. Développement des applications spécifiques ;

### 4.6.4. Quelques objectifs de contrôle classés par point de contrôle

#### 4.6.4.1. Activité de pilotage

- 4.6.4.1.1. S'assurer que la ligne de partage entre études et production est clairement définie et documentée ;
- 4.6.4.1.2. S'assurer qu'il existe une cellule dédiée en charge du suivi et du contrôle des projets et des ressources (gestion des plannings et des budgets, suivi des temps et des coûts) ;
- 4.6.4.1.3. Vérifier l'existence d'une procédure de planification détaillée par projet et/ou par ressource (en fonction des besoins et des enjeux : taille des équipes, nombre et nature des projets) ;
- 4.6.4.1.4. Vérifier que la procédure de planification est nominative et suffisamment détaillée pour permettre une bonne visibilité du taux prévisionnel d'occupation des ressources ;
- 4.6.4.1.5. Vérifier l'existence d'une procédure périodique (hebdomadaire à mensuelle en fonction des enjeux), de suivi de l'activité et de mise à jour du planning ;

- 4.6.4.1.6. Vérifier que pour les travaux de maintenance, la charge de réalisation (en jours/homme) est systématiquement rapprochée de l'estimation initiale afin d'une part, d'affiner les méthodes d'évaluation des demandes et, d'autre part, de mesurer la productivité relative des développeurs ;
- 4.6.4.1.7. Vérifier l'existence d'un tableau de bord mensuel de l'activité des études offrant une bonne visibilité de l'activité actuelle et à venir des études ;
- 4.6.4.1.8. S'assurer que ce tableau de bord est communiqué et analysé par le Comité informatique.

#### 4.6.4.2. *Activités opérationnelles*

- 4.6.4.2.1. Vérifier l'existence d'une MOA forte et d'une fonction études « limitée » à la MOE ;
- 4.6.4.2.2. Évaluer le rôle du Comité Informatique dans le contrôle de l'activité des études ;
- 4.6.4.2.3. Évaluer la qualité du « contre poids » de la production et de l'équilibre entre ces deux fonctions de la DSI ;
- 4.6.4.2.4. S'assurer qu'il existe une procédure standard et formalisée de maintenance ;
- 4.6.4.2.5. Vérifier que pour la maintenance évolutive, le « versionning » (2 à 3 par an) est préféré à la maintenance « au fil de l'eau » ;
- 4.6.4.2.6. S'assurer que les nouveaux programmes/versions sont systématiquement testés puis recettés dans un environnement dédié avant d'être livrés à l'exploitation ;
- 4.6.4.2.7. S'assurer que les nouveaux programmes/versions sont systématiquement testés puis recettés dans un environnement dédié avant d'être livrés à l'exploitation ;
- 4.6.4.2.8. Vérifier que la documentation de l'application est systématiquement mise à jour après chaque intervention de maintenance ;
- 4.6.4.2.9. Vérifier dans les programmes l'existence d'historique des modifications sous forme en commentaires ;
- 4.6.4.2.10. S'assurer que les corrections urgentes (bug bloquant de gravité 1) sont tracées (logs) et effectuées dans un cadre bien défini et font l'objet d'un rapport systématique revu par la DSI (responsable des études, production, assurance qualité, ...) ;
- 4.6.4.2.11. Pour les environnements obsolètes, s'assurer que les langages et compilateurs sont toujours opérationnels et maintenus (assembleurs, cobol, ...).

#### 4.6.4.3. *Le développement des Applications spécifiques*

- 4.6.4.3.1. Vérifier l'utilisation des méthodes et outils de conception et de modélisation d'application (UML, Rational Case, ...) ;
- 4.6.4.3.2. S'assurer que ces outils et méthodes sont adaptés, maîtrisés et partagés par l'ensemble des équipes concernées ;

- 4.6.4.3.3. S'assurer que la formation reçue pour ces outils est adaptée ;
- 4.6.4.3.4. S'assurer qu'il existe des normes de programmation et de codification dont les règles sont formalisées dans un manuel à l'attention des programmeurs ;
- 4.6.4.3.5. Vérifier l'application de ces normes (revue de code) ;
- 4.6.4.3.6. S'assurer qu'il existe une documentation utilisateurs par application (incluse dans la recette) comportant notamment le manuel d'utilisation, la description des données saisies et mises à jour, les états de contrôle disponibles, les contrôles automatiques effectués.

Sur le modèle présenté ci-haut (5.1), compléter et achever les points :



- 5.6.5. Critères classés par objectifs de contrôle
- 5.6.6. Eléments requis classés par critère
- 5.6.7. Questions d'évaluation classées par critère
- 5.6.8. Risques classés par questions d'évaluation
- 5.6.9. Conséquences classées par risque



Votre feuille de calcul devrait être sur le même modèle que celle obtenue à l'issue de la Section 4.1.



Chacun rassemblera en un seul classeur, l'ensemble de feuille de calcul de chaque section correspondante à chaque type d'audit (4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6). Ce classeur sera nommé : Outil\_Final\_NomApprenant.

#### 4.6.5. Conduire une Mission d'Audit de la Fonction Etude

##### 4.6.5.1. Phase 1 : Planification

La phase de planification constitue une étape clé pour définir les fondations d'un audit réussi. Elle permet de clarifier les objectifs, de délimiter le périmètre, d'identifier les risques associés et de structurer les actions à venir en tenant compte des ressources disponibles et des parties prenantes. À travers cette phase, les tâches suivantes seront réalisées pour garantir une approche méthodique et efficace de l'audit.

##### 4.6.5.1.1. Définir les objectifs de l'audit :

- ☒ Évaluer la capacité de la fonction étude à traduire les besoins métiers en solutions informatiques efficaces.
- ☒ Vérifier la conformité aux méthodologies de développement (cycle en V, Agile, DevOps, etc.).
- ☒ Identifier les risques liés à une mauvaise gestion des études (retards, dépassements budgétaires, inadéquation des livrables avec les attentes).



Pressman (2005) dans *Software Engineering: A Practitioner's Approach* souligne l'importance d'une gestion structurée des études pour minimiser les écarts entre besoins et livrables.

#### 4.6.5.1.2. Délimiter le périmètre :

- ☑ Déterminer les projets ou études clés à examiner.
- ☑ Identifier les phases du processus d'étude à auditer : analyse des besoins, conception, documentation, validation.

#### 4.6.5.1.3. Analyser les risques :

- ☑ Identifier les risques critiques : exigences mal définies, faible implication des parties prenantes, documentation insuffisante.
- ☑ Prioriser les études à fort impact sur les processus métiers.

#### 4.6.5.1.4. Établir le plan d'audit :

- ☑ Planifier l'évaluation des méthodologies, outils, et processus de la fonction étude.
- ☑ Identifier les parties prenantes (chefs de projet, analystes fonctionnels, métiers).

#### 4.6.5.1.5. Préparer un questionnaire d'audit :

- ☑ Questions types :
  - Les besoins métiers sont-ils correctement formalisés et validés ?
  - Existe-t-il des méthodologies standardisées pour les études ?
  - Les parties prenantes sont-elles impliquées tout au long du processus d'étude ?

#### 4.6.5.1.6. Documents à solliciter :

- ☑ Cahiers des charges et documents d'analyse des besoins.
- ☑ Diagrammes de flux, modèles de données, et documents de conception.
- ☑ Plan de gestion des exigences.
- ☑ Documentation des études réalisées et des projets en cours.
- ☑ Rétro-plannings et rapports d'avancement des études.

#### 4.6.5.1.7. Actions complémentaires :

- ☑ Réunir les outils utilisés pour la gestion des études (ex. JIRA, Confluence, UML).
- ☑ Prévoir des réunions avec les analystes métiers et chefs de projet pour clarifier les processus.

### 4.6.5.2. Phase 2 : Exécution

La phase d'exécution est le cœur de la mission d'audit, où les plans définis prennent vie à travers des actions concrètes. Elle consiste à collecter les preuves, analyser les données, observer les pratiques, et évaluer les systèmes et processus en fonction des critères établis. Les tâches suivantes seront réalisées pour garantir une évaluation rigoureuse et objective de la situation auditée.

#### 4.6.5.2.1. Analyse documentaire :

- ☑ Vérifier la clarté et la complétude des cahiers des charges.
- ☑ Évaluer la pertinence des documents de conception technique et fonctionnelle.

- ☒ Analyser les rapports de validation des études pour vérifier leur alignement avec les besoins métiers.

#### 4.6.5.2.2. Observation et entretiens :

- ☒ Interviewer les analystes et chefs de projet pour comprendre leurs méthodes de travail.
- ☒ Rencontrer les utilisateurs finaux pour évaluer leur satisfaction vis-à-vis des solutions livrées.
- ☒ Observer les ateliers d'analyse des besoins ou de validation des livrables.

#### 4.6.5.2.3. Évaluation des processus :

- ☒ Analyser la gestion des exigences (évolution, priorisation, traçabilité).
- ☒ Vérifier l'application des méthodologies de conception (UML, BPMN, Agile, etc.).
- ☒ Évaluer la collaboration entre les équipes techniques et fonctionnelles.

#### 4.6.5.2.4. Vérification des livrables :

- ☒ Comparer les besoins initialement définis avec les résultats obtenus.
- ☒ Analyser les écarts entre les estimations (temps, coût) et la réalité.
- ☒ Contrôler la qualité des études via des indicateurs : taux de révision des spécifications, délais moyens de validation, etc.

#### 4.6.5.2.5. Documents à solliciter :

- ☒ Registres de gestion des exigences.
- ☒ Résultats des ateliers de validation.
- ☒ Rapports de gestion des changements.
- ☒ Livrables intermédiaires et finaux des études.

#### 4.6.5.2.6. Actions complémentaires :

- ☒ Réaliser un benchmarking avec des études similaires dans des organisations comparables.
- ☒ Vérifier l'utilisation d'outils spécifiques (modélisation, gestion des exigences).

### 4.6.5.3. Phase 3 : Communication des résultats

La phase de communication des résultats constitue l'aboutissement de l'audit, où les constats, analyses et recommandations sont présentés de manière claire et structurée aux parties prenantes. Cette étape vise à fournir des informations exploitables et à favoriser l'engagement pour la mise en œuvre des actions correctives. Les tâches suivantes seront réalisées pour assurer une restitution efficace et impactante des conclusions de l'audit.

#### 4.6.5.3.1. Rédiger le rapport d'audit :

- ☒ Inclure les sections suivantes :
  - Synthèse des points forts et axes d'amélioration.
  - Analyse des écarts : méthodologies utilisées vs bonnes pratiques (ex. IEEE 830 pour la spécification des besoins).
  - Recommandations concrètes pour améliorer les pratiques d'étude : standardisation, outils, implication des parties prenantes.
- ☒ Appuyer les constats avec des exemples tirés des études analysées.

#### 4.6.5.3.2. Préparer une synthèse exécutive :

- ☒ Simplifier les constats pour une présentation aux décideurs.



- ☑ Insister sur l'impact des recommandations sur la qualité des projets livrés et leur alignement avec les besoins métiers.

#### 4.6.5.3.3. Restituer les résultats :

- ☑ Organiser une réunion avec les parties prenantes : responsables métiers, chefs de projet, analystes fonctionnels.
- ☑ Hiérarchiser les recommandations en fonction de leur impact et de leur faisabilité.
- ☑ Proposer un calendrier de mise en œuvre des recommandations prioritaires.

#### 4.6.5.3.4. Documents à solliciter :

- ☑ Rapport final d'audit validé.
- ☑ Plan d'amélioration pour la fonction étude.
- ☑ PV de la réunion de restitution.

#### 4.6.5.3.5. Actions complémentaires :

- ☑ Proposer des sessions de formation ou d'accompagnement pour améliorer les compétences en gestion des exigences et en modélisation.
- ☑ Suivre la mise en œuvre des recommandations via des KPI :
  - Taux de satisfaction des utilisateurs finaux.
  - Pourcentage de spécifications validées dès la première présentation.
  - Taux de conformité des livrables avec les besoins initiaux.

- ☑ **Karl Wiegers (2003) dans Software Requirements** : met en avant les bonnes pratiques pour la gestion des exigences et leur validation.
- ☑ **Pressman (2005) dans Software Engineering: A Practitioner's Approach** : décrit les méthodologies d'étude et leurs impacts sur la qualité des projets.
- ☑ **ISO/IEC 29148** : Norme internationale sur les exigences des systèmes et du logiciel, utile pour évaluer la gestion des études.
- ☑ **IEEE 830** : Fournit des lignes directrices pour documenter les spécifications des besoins.

## 4.7. *Evaluation des Connaissances*

### 4.7.1. QCM

1) Quel est l'objectif principal d'un audit des applications en service ?

- a) Vérifier l'efficacité des applications dans leur environnement opérationnel
- b) Identifier de nouveaux besoins fonctionnels
- c) Planifier une migration des données
- d) Former les utilisateurs sur les fonctionnalités des applications

2) Quel type d'audit s'assure de la conformité aux lois et réglementations en vigueur ?

- a) Audit des projets
- b) Audit de conformité
- c) Audit de sécurité
- d) Audit des processus

3) Dans un audit de sécurité, quelle est la priorité principale ?

- a) La disponibilité des ressources humaines
- b) L'identification des vulnérabilités dans le système
- c) L'efficacité des processus de gestion financière
- d) La gestion des données obsolètes

4) Quel est l'objectif principal d'un audit des processus ?

- a) Optimiser les systèmes d'information
- b) Vérifier l'efficacité et l'efficience des processus métiers
- c) Détecter les failles de sécurité
- d) Créer une matrice des risques

5) Quel audit vise à évaluer la gestion et l'exécution d'un projet informatique ?

- a) Audit de conformité
- b) Audit des projets
- c) Audit des processus
- d) Audit des applications en service

6) Une matrice des risques est particulièrement utilisée dans :

- a) L'audit de sécurité
- b) L'audit des applications en service
- c) L'audit des projets
- d) L'audit de conformité

7) L'objectif principal d'un audit des données est :

- a) Vérifier l'exactitude, la complétude et la cohérence des données
- b) S'assurer de la performance des utilisateurs
- c) Identifier les besoins en formation
- d) Tester les fonctionnalités des applications

8) Un audit de conformité se concentre principalement sur :

- a) L'évaluation des processus internes
- b) L'alignement avec les réglementations et standards externes
- c) La gestion des incidents de sécurité
- d) L'analyse des projets en cours

9) Quelle étape est cruciale dans un audit des projets ?

- a) La vérification des logs d'accès
- b) La validation des objectifs par rapport aux attentes initiales
- c) La gestion des comptes utilisateurs
- d) La planification des sauvegardes

10) Dans un audit des systèmes, quel élément est prioritaire ?

- a) Les aspects financiers
- b) La gouvernance des systèmes d'information
- c) Les compétences des utilisateurs
- d) L'analyse des SLA

11) Quel type d'audit est particulièrement concerné par la mise en place d'un PCA (Plan de Continuité d'Activité) ?

- a) Audit des processus
- b) Audit de sécurité
- c) Audit des projets
- d) Audit de conformité

12) L'audit des applications, quelle est une étape clé ?

- a) L'analyse des logs systèmes
- b) L'évaluation des besoins de migration
- c) La vérification des fonctionnalités par rapport aux attentes des utilisateurs
- d) La mise à jour des contrats fournisseurs

13) L'audit de sécurité inclut souvent :

- a) L'analyse des bases de données utilisateur
- b) La revue des politiques d'accès et de chiffrement
- c) La création de nouveaux référentiels
- d) La formation des administrateurs réseau

14) Quel est un résultat attendu d'un audit des processus ?

- a) Un plan détaillé pour implémenter un système ERP
- b) Une liste de recommandations pour améliorer l'efficacité des processus
- c) Une matrice des risques mise à jour
- d) Une évaluation de la conformité juridique

15) Un audit des projets identifie principalement :

- a) Les anomalies dans les données utilisateurs
- b) Les écarts entre le plan initial et l'exécution réelle
- c) Les vulnérabilités du système de chiffrement
- d) Les SLA non respectés

16) Quel outil est clé dans un audit des données ?

- a) Une matrice des accès
- b) Un logiciel d'analyse de données
- c) Un organigramme des processus
- d) Un tableau de bord

17) Dans un audit de conformité, les standards les plus courants incluent :

- a) COSO et ITIL
- b) ISO 27001 et GDPR
- c) COBIT et SWOT
- d) ITIL et SLA

18) Quel est le rôle principal des logs dans un audit de sécurité ?

- a) Fournir des statistiques d'utilisation
- b) Identifier les anomalies et activités suspectes
- c) Planifier les migrations de systèmes
- d) Former les équipes techniques

19) Lors d'un audit des projets, quelle étape est essentielle ?

- a) La revue des politiques de sauvegarde
- b) La documentation des livrables du projet
- c) La gestion des comptes utilisateurs
- d) L'évaluation des incidents passés

20) L'audit des processus est particulièrement utile pour :

- a) Tester de nouvelles applications
- b) Identifier des goulots d'étranglement dans les flux de travail
- c) Gérer les incidents en temps réel
- d) Analyser les SLA

21) Quelle norme est souvent utilisée dans l'audit de sécurité des données ?

- a) ISO 20000
- b) ISO 27001
- c) GDPR
- d) COSO

22) Quel audit se concentre sur la continuité des opérations en cas d'incident majeur ?

- a) Audit des applications en service
- b) Audit des processus
- c) Audit de sécurité
- d) Audit des projets

23) Quels sont les principaux livrables d'un audit des projets ?

- a) Une matrice des accès utilisateurs
- b) Un plan d'action pour la gestion des risques du projet
- c) Une liste des logiciels installés
- d) Un tableau de bord des SLA

24) Dans l'audit des données, une attention particulière est portée à :

- a) La structure des bases de données
- b) Les contrats fournisseurs
- c) Les migrations prévues
- d) Les incidents de sécurité

25) Quel est l'objectif principal d'un audit de sécurité ?

- a) Planifier de nouveaux investissements IT
- b) Prévenir les menaces et sécuriser les systèmes critiques
- c) Développer des outils analytiques
- d) Former les équipes au GDPR

#### 4.7.2. Questions à Trous

Complétez chaque phrase avec le terme ou la notion appropriée.

1. Un audit des \_\_\_\_\_ a pour objectif d'évaluer l'efficacité des fonctionnalités et leur adéquation avec les besoins des utilisateurs.
2. L'audit de \_\_\_\_\_ vise à s'assurer que les activités sont alignées avec les lois, règlements et standards applicables.
3. Lors d'un audit de sécurité, une attention particulière est portée à l'identification des \_\_\_\_\_ dans le système.
4. L'audit des \_\_\_\_\_ consiste à examiner l'efficacité et l'efficience des activités liées aux processus métiers.
5. Un audit des \_\_\_\_\_ permet d'évaluer les écarts entre le plan initial et l'exécution réelle d'un projet.
6. Une matrice des \_\_\_\_\_ est un outil clé pour prioriser les menaces dans un audit de sécurité.
7. L'audit des données se concentre sur l'exactitude, la complétude et la \_\_\_\_\_ des données.
8. L'évaluation de la conformité réglementaire est souvent guidée par des normes telles que \_\_\_\_\_ et GDPR.
9. Lors d'un audit des projets, il est essentiel de vérifier si les \_\_\_\_\_ livrés respectent les attentes définies.
10. L'audit de sécurité inclut souvent une revue des politiques de \_\_\_\_\_ pour garantir un accès contrôlé aux systèmes.
11. Un plan de continuité d'activité (PCA) est principalement évalué dans le cadre d'un audit de \_\_\_\_\_.
12. Une étape clé dans l'audit des applications est de vérifier leur \_\_\_\_\_ par rapport aux attentes des utilisateurs.
13. L'analyse des \_\_\_\_\_ est souvent utilisée dans les audits de sécurité pour identifier les anomalies et activités suspectes.
14. L'audit des processus permet d'identifier des \_\_\_\_\_ dans les flux de travail pour améliorer l'efficacité.
15. La documentation des \_\_\_\_\_ est une étape cruciale dans l'audit des projets pour garantir la transparence.
16. Lors d'un audit des données, il est important d'évaluer la structure et la qualité des \_\_\_\_\_.

17. Une politique efficace de \_\_\_\_\_ est essentielle pour protéger les systèmes critiques dans un audit de sécurité.
18. Les audits de sécurité visent à prévenir les \_\_\_\_\_ et à renforcer les systèmes de protection.
19. Dans un audit de conformité, les \_\_\_\_\_ externes sont comparés aux standards et réglementations applicables.
20. Les recommandations issues d'un audit des processus doivent se concentrer sur l'amélioration de leur \_\_\_\_\_ et leur efficacité.

#### 4.7.3. Questions Ouvertes

- 1) Quels sont les objectifs principaux d'un audit des applications en service ?
- 2) Comment évaluer l'efficacité des fonctionnalités d'une application par rapport aux besoins des utilisateurs ?
- 3) Quels critères utiliseriez-vous pour juger de la performance des applications auditées ?
- 4) Quelles sont les étapes nécessaires pour auditer une application en service ?
- 5) En quoi un audit des applications peut-il contribuer à l'amélioration des processus métiers ?
- 6) Pourquoi l'audit de conformité est-il essentiel pour une organisation ?
- 7) Comment vérifier si une organisation est conforme aux normes telles que ISO 27001 ou GDPR ?
- 8) Quels sont les risques pour une entreprise en cas de non-conformité réglementaire ?
- 9) Quelles méthodes sont utilisées pour évaluer la conformité d'une organisation ?
- 10) Comment l'audit de conformité peut-il contribuer à une meilleure gouvernance d'entreprise ?
- 11) Quels sont les principaux objectifs d'un audit de sécurité des systèmes d'information ?
- 12) Comment identifier les vulnérabilités dans un système d'information lors d'un audit de sécurité ?
- 13) Quels outils recommanderiez-vous pour analyser les politiques d'accès et de chiffrement dans un audit de sécurité ?
- 14) En quoi la revue des logs peut-elle aider à détecter des anomalies de sécurité ?
- 15) Comment tester l'efficacité des plans de continuité d'activité (PCA) et de reprise d'activité (PRA) lors d'un audit de sécurité ?
- 16) Quels sont les indicateurs clés pour évaluer l'efficacité d'un processus métier ?
- 17) Comment identifier des goulots d'étranglement dans les processus métiers lors d'un audit ?

- 18) Pourquoi est-il important d'auditer les processus d'une organisation ?
- 19) Quels sont les livrables attendus d'un audit des processus ?
- 20) En quoi un audit des processus peut-il améliorer la performance organisationnelle ?
- 21) Quelles sont les étapes clés d'un audit des projets informatiques ?
- 22) Comment évaluer les écarts entre les objectifs initiaux et les résultats réels d'un projet ?
- 23) Quels critères sont utilisés pour juger de la réussite d'un projet audité ?
- 24) Pourquoi est-il important de documenter les livrables d'un projet dans le cadre d'un audit ?
- 25) Quels sont les principaux défis rencontrés lors d'un audit des projets ?
- 26) Pourquoi est-il essentiel de vérifier la qualité des données dans une organisation ?
- 27) Quels outils utiliseriez-vous pour auditer la structure des bases de données ?
- 28) Comment l'audit des données peut-il contribuer à la prise de décisions stratégiques ?
- 29) Quels sont les principaux éléments à vérifier lors de l'audit de la cohérence des données ?
- 30) En quoi un audit des données peut-il révéler des faiblesses dans les processus de collecte d'informations ?
- 31) Comment choisir le type d'audit adapté aux besoins d'une organisation ?
- 32) En quoi la matrice des risques est-elle utile pour prioriser les éléments à auditer ?
- 33) Quels référentiels ou normes recommanderiez-vous pour réaliser un audit des SI ?
- 34) Pourquoi est-il important de suivre un cadre méthodologique structuré pour chaque type d'audit ?
- 35) Quels critères permettent d'évaluer la pertinence des recommandations formulées après un audit ?
- 36) Comment l'audit contribue-t-il à renforcer la gouvernance des systèmes d'information ?
- 37) Quels sont les liens entre audit de sécurité et gouvernance informatique ?
- 38) Comment les audits des projets et des processus influencent-ils les décisions stratégiques d'une organisation ?
- 39) Quels rôles jouent les parties prenantes dans la réussite d'un audit ?
- 40) Pourquoi les audits réguliers des systèmes d'information sont-ils indispensables dans un environnement réglementaire complexe ?
- 41) Comment garantir que les recommandations issues d'un audit sont mises en œuvre efficacement ?
- 42) Quels indicateurs peuvent être utilisés pour mesurer l'impact des recommandations sur la performance organisationnelle ?

- 43) En quoi le suivi des recommandations permet-il d'améliorer les pratiques de l'organisation ?
- 44) Pourquoi est-il crucial d'impliquer les responsables métiers dans le suivi des actions post-audit ?
- 45) Quelles sont les bonnes pratiques pour assurer la traçabilité des recommandations dans le temps ?

#### 4.7.4. Cas pratique

##### Énoncé :

La société **Lizbiz's**, spécialisée dans la gestion des stocks pour des entreprises de taille moyenne, rencontre des incidents de sécurité récurrents. Ces incidents incluent :

1. Des tentatives d'accès non autorisé aux systèmes critiques, détectées par les logs d'activité.
2. Une absence de politique de gestion des mots de passe pour les utilisateurs.
3. Des sauvegardes de données qui ne sont ni régulières ni testées.
4. Un plan de continuité d'activité (PCA) obsolète et non aligné avec les besoins actuels de l'entreprise.
5. Une absence de chiffrement pour les échanges d'informations sensibles entre les systèmes internes et les partenaires externes.

La mission d'audit confiée par Lizbiz's vise à :

- ☒ Identifier les failles dans les mesures de sécurité existantes.
- ☒ Évaluer les politiques actuelles de gestion des accès et de protection des données.
- ☒ Proposer des recommandations concrètes pour renforcer la sécurité et la résilience des systèmes.

##### Questions :

- 1) Quels éléments vérifieriez-vous dans les logs pour détecter des tentatives d'accès non autorisées et des anomalies dans le système ?
- 2) Quels contrôles recommanderiez-vous pour renforcer la politique de gestion des mots de passe des utilisateurs ?
- 3) Comment évalueriez-vous l'efficacité des sauvegardes actuelles et leur adéquation aux exigences du PCA ?
- 4) Quels protocoles de chiffrement recommanderiez-vous pour sécuriser les échanges d'informations sensibles avec les partenaires externes ?
- 5) Quelles actions immédiates doivent être entreprises pour corriger les faiblesses des politiques de sécurité de Lizbiz's ?



- 6) Quels sont les éléments clés que vous vérifieriez pour actualiser le PCA de Lizbiz's en fonction des besoins actuels de l'entreprise ?
- 7) Comment sensibiliseriez-vous les utilisateurs de Lizbiz's à la sécurité des systèmes d'information et aux bonnes pratiques ?
- 8) Comment classeriez-vous les failles identifiées selon leur criticité pour définir un plan d'action prioritaire ?
- 9) Quels référentiels ou normes recommanderiez-vous à Lizbiz's pour s'assurer de la conformité de ses pratiques de sécurité ?
- 10) Quels indicateurs utiliseriez-vous pour mesurer l'efficacité des recommandations mises en œuvre par Lizbiz's ?



## Livre V:

# DISCUSSIONS SCIENTIFIQUES SUR DES SUR DES SUJETS CONNEXES A L'AUDIT DES SI

### **Objectif :**

Donner des éléments de base méthodologique aux apprenants pour conduire des discussions scientifiques dans des domaines connexes à l'audit

### **Objectif d'apprentissage :**

A la fin de ce livre, chaque apprenant doit être à mesure de construire un outil d'aide à l'audit partant d'un référentiel quelconque.

## 5) DISCUSSIONS SUR DES SUJETS CONNEXES A L'AUDIT DES SI

### 5.1. Discussion sur le rôle et l'impact de l'intelligence artificielle dans les systèmes d'information : cas de la société Lizbiz's

#### 5.1.1. Introduction

L'intelligence artificielle (IA) a le potentiel de transformer profondément les systèmes d'information des entreprises, y compris celles opérant dans des secteurs tels que l'agro-industrie, à l'exemple de la société Lizbiz's. Cette société, spécialisée dans la production et la transformation du coton, gère une chaîne d'approvisionnement complexe, depuis la production agricole jusqu'à la vente du produit fini. L'intégration de l'IA dans son système d'information peut offrir des avantages considérables mais aussi soulever des défis que l'auditeur des systèmes d'information doit examiner attentivement.

#### 5.1.2. Les avantages de l'IA pour les systèmes d'information

L'IA peut apporter une multitude d'avantages aux systèmes d'information de La société Lizbiz's :

##### 5.1.2.1. Automatisation des processus :

L'IA permet d'automatiser les tâches répétitives, réduisant ainsi les erreurs humaines et augmentant l'efficacité. Par exemple, des algorithmes peuvent gérer la collecte des données, les prévisions de la production, et même le suivi en temps réel de la chaîne d'approvisionnement.

##### 5.1.2.2. Analyse des données améliorée :

Les capacités de l'IA à traiter de grandes quantités de données (Big Data) permettent à La société Lizbiz's de mieux comprendre les tendances du marché, les conditions climatiques, et les comportements des clients. Cela peut améliorer la prise de décision stratégique et opérationnelle.

##### 5.1.2.3. Prévision et optimisation :

Grâce à des modèles prédictifs, l'IA peut aider à prévoir la demande, optimiser les niveaux de stock, et améliorer la planification logistique. Cela réduit les gaspillages et améliore la rentabilité.

##### 5.1.2.4. Gestion des risques :

En matière de cybersécurité, l'IA peut détecter des anomalies dans les systèmes d'information en temps réel, prévenant ainsi des attaques ou des fuites de

données. De plus, elle peut surveiller les comportements des utilisateurs pour repérer des activités suspectes.

### *5.1.3. Les inconvénients et risques potentiels de l'IA dans un système d'information*

Cependant, il est crucial de reconnaître que l'introduction de l'IA présente aussi des risques, que l'auditeur des systèmes d'information doit évaluer :

#### *5.1.3.1. Dépendance à la technologie :*

En s'appuyant fortement sur des systèmes automatisés, La société Lizbiz's pourrait devenir trop dépendante de la technologie, ce qui pose un risque en cas de panne du système ou d'erreurs algorithmiques. Une défaillance du système d'IA pourrait perturber toute l'opération.

#### *5.1.3.2. Manque de transparence et biais des algorithmes :*

Les systèmes d'IA sont souvent perçus comme des « boîtes noires », ce qui rend difficile la compréhension du fonctionnement interne des algorithmes. Cela pose un problème pour un auditeur qui doit s'assurer de la transparence et de l'équité des décisions automatisées. De plus, l'IA peut introduire des biais qui peuvent affecter les décisions opérationnelles et stratégiques.

#### *5.1.3.3. Coûts d'implémentation :*

La mise en place d'une infrastructure IA demande des investissements conséquents, tant en termes de matériel que de formation du personnel. Pour une société comme la LIZBIZ'S, ces coûts peuvent être perçus comme des obstacles, surtout si les résultats ne sont pas immédiats.

#### *5.1.3.4. Impacts sur l'emploi :*

L'automatisation de certaines fonctions peut entraîner une réduction des postes de travail, ce qui peut avoir des implications sociales importantes. Cela nécessite une gestion du changement pour accompagner les équipes concernées.

### *5.1.4. Enjeux clés pour un auditeur des systèmes d'information dans un contexte d'IA*

Du point de vue d'un auditeur des systèmes d'information, plusieurs enjeux doivent être pris en compte lors de l'intégration de l'IA dans une entreprise comme La société Lizbiz's :

#### *5.1.4.1. Conformité réglementaire :*

L'auditeur doit veiller à ce que l'utilisation de l'IA soit conforme aux lois et réglementations en vigueur, notamment en matière de protection des données

(comme le RGPD si applicable). La collecte et l'analyse de données doivent respecter les droits des individus et les exigences légales.

#### *5.1.4.2. Contrôles internes et gouvernance de l'IA :*

Il est essentiel de mettre en place des contrôles robustes pour assurer que les systèmes d'IA fonctionnent comme prévu. Cela inclut la vérification des algorithmes, la gestion des risques associés à l'automatisation, et la mise en place d'une gouvernance pour surveiller les performances des systèmes.

#### *5.1.4.3. Cybersécurité et résilience :*

L'IA peut à la fois renforcer et exposer à des risques de cybersécurité. Un auditeur devra s'assurer que les systèmes d'IA ne deviennent pas une cible pour des cyberattaques, notamment en renforçant les pare-feu, la détection des intrusions, et en menant des audits réguliers de sécurité.

#### *5.1.4.4. Éthique de l'IA :*

L'auditeur doit veiller à ce que l'utilisation de l'IA soit éthique, sans causer de discrimination ou de traitement inéquitable. Cela implique une analyse des données utilisées pour entraîner les algorithmes, ainsi qu'une vérification des décisions prises par ces systèmes.

### *5.1.5. Les défis à relever dans l'intégration de l'IA pour un SI en évolution*

L'intégration de l'IA dans les systèmes d'information d'une entreprise comme La société Lizbiz's présente des défis importants :

#### *5.1.5.1. Changement organisationnel :*

L'IA nécessite souvent une refonte des processus internes, une évolution des compétences du personnel, et un changement de culture d'entreprise. La résistance au changement est un facteur que l'auditeur devra identifier et évaluer.

#### *5.1.5.2. Sécurité des données :*

L'IA nécessite d'importantes quantités de données pour être efficace. Cependant, cela soulève des préoccupations quant à la sécurité et à la confidentialité des données sensibles. L'auditeur doit donc évaluer la manière dont les données sont stockées, partagées et protégées.

#### *5.1.5.3. Formation et compétences :*

La réussite d'une telle transformation dépend en grande partie de la capacité du personnel à utiliser ces technologies. La formation continue devient ainsi un enjeu majeur, et l'auditeur devra vérifier l'adéquation des compétences disponibles pour soutenir l'IA.

#### 5.1.5.4. *Interopérabilité des systèmes :*

La société Lizbiz's utilise probablement des systèmes d'information hérités qui doivent être intégrés aux nouvelles technologies basées sur l'IA. Cela peut entraîner des difficultés d'intégration et de compatibilité que l'auditeur devra prendre en compte.

#### 5.1.6. *Conclusion : Une opportunité à saisir, mais avec précaution*

L'intégration de l'IA dans les systèmes d'information de La société Lizbiz's offre des perspectives de gains d'efficacité et de compétitivité. Toutefois, ces bénéfices doivent être équilibrés avec les risques et les défis associés, notamment du point de vue de l'auditeur des systèmes d'information. L'IA doit être implémentée de manière stratégique, avec une gouvernance rigoureuse, pour garantir que l'organisation tire pleinement parti de cette technologie tout en protégeant ses actifs critiques et en respectant les obligations légales et éthiques.

## 5.2. Discussion sur la fraude dans et par les systèmes d'information

### 5.2.1. Introduction

Dans un environnement où les systèmes d'information jouent un rôle central, comme c'est le cas à Lizbiz's, la fraude constitue une menace sérieuse. Que ce soit par l'exploitation des failles de sécurité ou par la manipulation des systèmes internes, la fraude peut affecter gravement la performance de l'entreprise. La prévention et la détection de la fraude sont donc des enjeux critiques pour garantir la pérennité et la rentabilité de l'entreprise.

### 5.2.2. La nature de la fraude dans les systèmes d'information

La fraude dans les systèmes d'information peut prendre plusieurs formes et touche à différents aspects des opérations d'une entreprise comme Lizbiz's :

#### 5.2.2.1. Fraude interne

Il s'agit des fraudes perpétrées par des employés ou des partenaires ayant accès aux systèmes internes. Ces fraudes peuvent inclure la manipulation des données comptables, l'altération des résultats financiers, ou l'accès non autorisé aux systèmes pour commettre des malversations. Par exemple, des modifications des bases de données financières peuvent passer inaperçues sans contrôles rigoureux.

#### 5.2.2.2. Fraude externe

Les cybercriminels externes peuvent exploiter les vulnérabilités des systèmes d'information pour s'introduire dans le réseau de l'entreprise et voler des informations sensibles, détourner des fonds, ou perturber les opérations via des attaques comme le phishing ou le ransomware.

#### 5.2.2.3. Fraude technologique

Celle-ci implique l'utilisation malveillante de technologies de plus en plus sophistiquées. Elle peut inclure la création de faux comptes, la falsification de transactions, ou l'usurpation d'identité à travers des mécanismes automatisés (robots, logiciels malveillants, etc.).

### 5.2.3. L'impact de la fraude sur la performance de Lizbiz's

La fraude dans les systèmes d'information peut avoir des répercussions sévères sur la performance globale d'une société informatisée comme Lizbiz's :

#### 5.2.3.1. Perte financière

Les fraudes, qu'elles soient internes ou externes, peuvent entraîner des pertes financières directes. Cela inclut le détournement de fonds, le vol de ressources, ou encore les coûts liés à la récupération des systèmes après une attaque.

#### 5.2.3.2. *Atteinte à la réputation*

La découverte d'une fraude peut gravement ternir l'image de Lizbiz's auprès de ses partenaires commerciaux et financiers. La confiance des parties prenantes peut être ébranlée, ce qui affecte la compétitivité de l'entreprise sur le marché.

#### 5.2.3.3. *Perturbation des opérations*

Une fraude bien orchestrée peut provoquer des dysfonctionnements au niveau des systèmes critiques, ralentissant ou arrêtant la production, la gestion de la chaîne d'approvisionnement ou les ventes. Cela affecte directement les performances opérationnelles.

#### 5.2.3.4. *Impact juridique et réglementaire*

La fraude expose également l'entreprise à des risques juridiques, notamment en cas de non-conformité avec des réglementations locales ou internationales. Des amendes ou des sanctions peuvent être infligées, aggravant les pertes financières et nuisant à la réputation.

#### 5.2.3.5. *Pertes de données*

Le vol de données sensibles, telles que les informations sur les clients ou les partenaires, peut aussi avoir des effets dévastateurs, d'autant plus que ces informations sont cruciales pour les prises de décisions stratégiques.

### 5.2.4. *Les parades contre la fraude dans les systèmes d'information*

Pour faire face à ces risques, il est essentiel de mettre en place des parades efficaces. Plusieurs stratégies et technologies peuvent être envisagées pour prévenir, détecter et gérer la fraude :

#### 5.2.4.1. *Contrôles d'accès rigoureux :*

Un des moyens les plus efficaces de prévenir la fraude interne est de limiter l'accès aux systèmes d'information critiques à un nombre restreint d'utilisateurs. Cela inclut l'implémentation de l'authentification multi-facteurs, la gestion des droits d'accès et une surveillance stricte des connexions.

#### 5.2.4.2. *Segmentation des systèmes :*

Segmenter les réseaux et les systèmes permet de limiter la portée d'une attaque ou d'une fraude. Si une partie du système est compromise, la segmentation empêche les fraudeurs d'accéder à l'ensemble du réseau de l'entreprise.

#### 5.2.4.3. *Surveillance proactive :*

La mise en place d'outils de surveillance en temps réel, qui analysent les comportements suspects et les anomalies dans le réseau, peut permettre de détecter les tentatives de fraude avant qu'elles ne causent des dommages



significatifs. Des systèmes basés sur l'IA peuvent aussi aider à analyser de grands volumes de données pour identifier des tendances suspectes.

#### *5.2.4.4. Politiques de sécurité renforcées :*

Il est important que LIZBIZ'S dispose de politiques claires et actualisées en matière de cybersécurité et de prévention de la fraude. Ces politiques doivent inclure des directives strictes sur l'utilisation des systèmes d'information, la gestion des mots de passe, et les protocoles en cas de suspicion de fraude.

#### *5.2.4.5. Audits réguliers des systèmes d'information :*

Un audit régulier permet de détecter d'éventuelles failles de sécurité ou des activités suspectes. L'auditeur des systèmes d'information a un rôle clé pour garantir que les contrôles sont efficaces et que les processus en place réduisent les risques de fraude.

#### *5.2.4.6. Formation du personnel :*

La sensibilisation des employés aux risques de fraude et aux meilleures pratiques de cybersécurité est essentielle. Des formations régulières peuvent aider à réduire les erreurs humaines, qui sont souvent à l'origine de nombreuses failles de sécurité.

#### *5.2.4.7. Outils de gestion des fraudes :*

La société Lizbiz's peut également s'appuyer sur des solutions logicielles spécialisées dans la détection des fraudes. Ces outils analysent les transactions en temps réel et déclenchent des alertes en cas de comportements anormaux ou de violation des règles.

#### *5.2.4.8. Collaboration inter-organisationnelle :*

La lutte contre la fraude nécessite souvent la collaboration entre plusieurs départements : informatique, finances, ressources humaines, et audit. En favorisant une collaboration efficace, Lizbiz's peut renforcer sa capacité à détecter et à réagir rapidement aux tentatives de fraude.

### *5.2.5. Les défis à relever pour lutter contre la fraude*

Malgré les nombreuses parades possibles, certaines difficultés persistent dans la lutte contre la fraude, et elles doivent être anticipées pour garantir une stratégie de protection efficace :

#### *5.2.5.1. Évolution rapide des techniques de fraude*

Les fraudeurs utilisent des technologies de plus en plus sophistiquées pour contourner les systèmes de sécurité. L'auditeur doit donc s'assurer que les dispositifs de sécurité sont régulièrement mis à jour pour faire face à ces nouvelles menaces.

#### 5.2.5.2. *Coût des technologies de prévention*

Les technologies les plus avancées pour prévenir la fraude peuvent être coûteuses à mettre en place, surtout pour une entreprise de la taille de Lizbiz's. L'enjeu sera de trouver un équilibre entre les investissements en cybersécurité et les bénéfices de ces systèmes.

#### 5.2.5.3. *Gestion des faux positifs*

Les systèmes de détection automatique de fraude peuvent parfois générer des faux positifs, ce qui peut ralentir les opérations légitimes et créer de la frustration. Il est donc nécessaire de calibrer les systèmes pour assurer une détection précise.

#### 5.2.5.4. *Évolution des réglementations*

Avec l'évolution des réglementations sur la protection des données et la cybersécurité, il peut être difficile pour une entreprise comme Lizbiz's de se maintenir en conformité. L'auditeur doit veiller à ce que les politiques de prévention de la fraude soient alignées avec les exigences réglementaires.

#### 5.2.6. *Conclusion : Une vigilance continue pour protéger les actifs de Lizbiz's*

La fraude dans les systèmes d'information représente un risque significatif pour une entreprise comme Lizbiz's. Ses impacts sur les finances, la réputation et les opérations peuvent être dévastateurs. Il est donc crucial que l'entreprise mette en place des parades solides pour minimiser ces risques. Cependant, la lutte contre la fraude est un processus continu, qui nécessite une attention permanente, des audits réguliers et une capacité d'adaptation face aux nouvelles menaces. En s'appuyant sur une combinaison de technologies avancées, de politiques internes robustes et de formation du personnel, Lizbiz's peut renforcer la sécurité de ses systèmes d'information et préserver sa performance.



## Livre VI: CAS PRATIQUE

### **Objectif de la séance :**

Immerger les apprenant dans une mission d’audit, par le parcours de toutes les phases depuis les travaux préparatoires jusqu’à la production du rapport

### **Objectif d’apprentissage :**

A la fin de la séance, chaque apprenant doit être à mesure dérouler seul l’ensemble des phases d’une mission d’audit des systèmes d’information.

## 6) CAS PRATIQUE

### 6.1. Consignes

#### 6.1.1. Objectifs

Ce cas pratique a pour objectifs de :

- ☒ Développer des compétences pratiques en audit des systèmes d'information, avec un focus sur les applications en service.
- ☒ Appliquer les méthodologies et normes d'audit des SI à une application spécifique en fonction dans une organisation.
- ☒ Apprendre à structurer un rapport d'audit en identifiant les contrôles clés et en proposant des recommandations adaptées aux risques identifiés.
- ☒ Mettre en place un cadre de suivi et de validation des contrôles dans le contexte de l'application APPLICATION.

#### 6.1.2. Énoncé du Cas

Le cas consiste en l'audit de l'application APPLICATION, une application en service utilisée pour la gestion comptable d'une organisation. L'équipe de mission doit évaluer la conformité de APPLICATION aux standards de sécurité, de performance, et de conformité, en tenant compte des meilleures pratiques en audit des SI.

#### 6.1.3. Mandat pour l'Équipe de Mission

Le mandat de l'équipe de mission comprend :

- ☒ Périmètre de l'audit :  
Effectuer un audit exhaustif de l'application APPLICATION, en incluant ses fonctionnalités de gestion comptable et les processus de contrôle interne associés.
- ☒ Objectifs :  
Identifier les forces et les faiblesses de l'application, proposer des recommandations pour remédier aux vulnérabilités détectées et améliorer les contrôles.
- ☒ Méthodologie :  
Appliquer les standards d'audit pertinents (par exemple, le cadre COSO pour les contrôles internes), utiliser des outils d'évaluation et de collecte de preuves, et documenter les résultats de manière rigoureuse.
- ☒ Rapports :  
Préparer un rapport final d'audit comprenant les observations, les points de contrôle évalués, les recommandations, et les annexes détaillant les preuves et documents de contrôle.

## 6.2. Modèles de rapport d'audit d'une Application en Service : APPLICATION

### 6.2.1. Introduction

#### 6.2.1.1. Contexte de l'audit

Ce rapport présente les résultats de l'audit de l'application APPLICATION, actuellement en service. L'objectif de cet audit est de s'assurer que l'application répond aux exigences en termes de sécurité, performance, conformité, et continuité de service, et de fournir des recommandations pour l'amélioration de son exploitation.

#### 6.2.1.2. Objectifs de l'audit

Les principaux objectifs de cet audit sont :

- ☒ Vérifier la conformité de APPLICATION avec les politiques de sécurité internes et les normes réglementaires.
- ☒ Évaluer l'efficacité des contrôles de sécurité mis en place.
- ☒ Analyser les performances de l'application sous différentes charges.
- ☒ S'assurer que des mécanismes adéquats de continuité de service (PRA/PCA) sont en place.
- ☒ Proposer des recommandations pour remédier aux vulnérabilités identifiées.

#### 6.2.1.3. Méthodologie

L'audit a été réalisé selon la méthodologie suivante :

- ☒ Revue des documents et politiques liées à APPLICATION.
- ☒ Analyse des flux d'information et des composants critiques.
- ☒ Tests de sécurité et de performance.
- ☒ Interviews avec les utilisateurs clés et l'équipe technique.
- ☒ Vérification de la conformité réglementaire.
- ☒ Revue des logs et incidents de l'application.
- ☒ Évaluation du Système de Contrôle Interne de l'Application APPLICATION

#### 6.2.1.4. Equipe de Mission

L'audit de l'application en service APPLICATION a été réalisé de xxx à xxx par l'équipe ainsi constituée :

- ☒ xxxxxxxxxxxx, spécialité, grade, Chef de Mission.
- ☒ xxxxxxxxxxxx, spécialité, grade, Chef de Mission.
- ☒ xxxxxxxxxxxx, spécialité, grade, Chef de Mission.
- ☒ xxxxxxxxxxxx, spécialité, grade, Chef de Mission.
- ☒ xxxxxxxxxxxx, spécialité, grade, Chef de Mission.

Sous la supervision de xxxxxxxxxxxxxxxxxxxx, spécialité, grade, Directeur de l'Audit Interne.

Avec l'accompagnement de xxxxxx, spécialité, consultant.

## 6.2.2. Evaluation du système de contrôle interne

### 6.2.2.1. Environnement de Contrôle

#### 6.2.2.2. Engagement envers l'intégrité et les valeurs éthiques

- ☒ Observation : [Évaluation de l'engagement éthique dans le cadre de l'application].
- ☒ Recommandation : [Proposition pour renforcer les valeurs éthiques].

#### 6.2.2.2.1. Conseil d'administration indépendant et surveillant

- ☒ Observation : [Niveau de supervision par le conseil d'administration ou un comité équivalent].
- ☒ Recommandation : [Proposition d'améliorations de la gouvernance].

#### 6.2.2.2.2. Structures, autorités et responsabilités

- ☒ Observation : [Clarté dans la répartition des responsabilités au sein de l'application].
- ☒ Recommandation : [Suggestions pour clarifier les rôles].

#### 6.2.2.2.3. Compétences des individus

- ☒ Observation : [Niveau de compétence et formation des utilisateurs et administrateurs].
- ☒ Recommandation : [Proposition de formation pour combler les lacunes].

#### 6.2.2.2.4. Responsabilité et délégation

- ☒ Observation : [Existence et respect des mécanismes de délégation et de responsabilisation].
- ☒ Recommandation : [Actions pour renforcer la responsabilisation].

### 6.2.2.3. Évaluation des Risques

#### 6.2.2.3.1. Spécification des objectifs appropriés

- ☒ Observation : [Évaluation des objectifs assignés à APPLICATION et leur pertinence].
- ☒ Recommandation : [Ajustements nécessaires pour clarifier les objectifs].

#### 6.2.2.3.2. Identification et analyse des risques

- ☒ Observation : [Qualité des processus d'identification des risques liés à l'application].
- ☒ Recommandation : [Propositions pour améliorer la détection des risques].

#### 6.2.2.3.3. Prise en compte de la fraude

- ☒ Observation : [Contrôles pour prévenir et détecter la fraude dans l'utilisation de l'application].
- ☒ Recommandation : [Actions pour renforcer la protection contre la fraude].

#### 6.2.2.3.4. Identification et analyse des changements significatifs

- ☑ Observation : [Réactivité face aux évolutions dans l'environnement technologique et réglementaire].
- ☑ Recommandation : [Propositions pour améliorer l'adaptabilité].

#### 6.2.2.4. *Activités de Contrôle*

##### 6.2.2.4.1. *Sélection et développement des activités de contrôle*

- ☑ Observation : [Évaluation de la pertinence des contrôles techniques mis en place].
- ☑ Recommandation : [Suggestions pour renforcer les activités de contrôle].

##### 6.2.2.4.2. *Développement des activités de contrôle sur les technologies*

- ☑ Observation : [Approche adoptée pour les contrôles technologiques].
- ☑ Recommandation : [Améliorations possibles pour les contrôles technologiques].

##### 6.2.2.4.3. *Mise en œuvre des politiques et procédures*

- ☑ Observation : [Conformité aux politiques et procédures établies].
- ☑ Recommandation : [Renforcement des procédures ou leur formalisation].

#### 6.2.2.5. *Information et Communication*

##### 6.2.2.5.1. *Utilisation d'informations de qualité*

- ☑ Observation : [Fiabilité et qualité des données utilisées par APPLICATION].
- ☑ Recommandation : [Mesures pour améliorer la qualité des informations].

##### 6.2.2.5.2. *Communication interne*

- ☑ Observation : [Clarté et efficacité de la communication entre les utilisateurs de l'application et les équipes support].
- ☑ Recommandation : [Actions pour renforcer la communication interne].

##### 6.2.2.5.3. *Communication externe*

- ☑ Observation : [Communication avec les parties prenantes externes et les utilisateurs finaux].
- ☑ Recommandation : [Suggestions pour améliorer la transparence et la communication externe].

#### 6.2.2.6. *Activités de Surveillance*

##### 6.2.2.6.1. *Évaluations continues et indépendantes*

- ☑ Observation : [Fréquence et rigueur des évaluations de contrôle interne pour l'application].
- ☑ Recommandation : [Propositions pour améliorer la surveillance continue].

##### 6.2.2.6.2. *Évaluation des déficiences*

- ☑ Observation : [Capacité à détecter et corriger les défaillances dans les contrôles].
- ☑ Recommandation : Actions pour améliorer la détection et la correction des déficiences].

### 6.2.3. Périmètre et Détails de l'Application

#### 6.2.3.1. Description de l'application

APPLICATION est une solution logicielle de gestion comptable conçue pour répondre aux besoins des entreprises de toutes tailles. Elle vise à faciliter le suivi financier, l'automatisation des processus comptables, et à offrir une visibilité en temps réel sur la santé financière de l'entreprise. APPLICATION permet de centraliser les données financières, d'assurer la conformité aux normes comptables, et de produire des rapports précis pour la prise de décision.

#### 6.2.3.2. Environnement technique

- ☑ Base de données : [Type et version de la base de données utilisée].
- ☑ Serveur d'application : [Type et version du serveur].
- ☑ Middleware : [Description des intergiciels utilisés].
- ☑ Langage de programmation : [Langage utilisé pour le développement de l'application].
- ☑ Nombre d'utilisateurs actifs : [Détails sur le nombre et le type d'utilisateurs].
- ☑ Dépendances : Liste des systèmes tiers et des interfaces critiques utilisées par APPLICATION.

#### 6.2.3.3. Environnement métier (fonctionnement)

##### 6.2.3.3.1. Fonctionnalités Principales

- ☑ Gestion des Comptes
  - Création et gestion des comptes comptables (actifs, passifs, capitaux, etc.).
  - Suivi des soldes de chaque compte avec une mise à jour en temps réel des transactions.
  - Possibilité de configurer un plan comptable personnalisé en fonction des besoins spécifiques de l'entreprise.
- ☑ Saisie des Écritures Comptables
  - Enregistrement des écritures comptables : entrées et sorties de fonds, opérations inter-comptes, etc.
  - Saisie automatisée ou manuelle avec possibilité d'ajouter des commentaires pour chaque opération.
  - Gestion des pièces justificatives en pièces jointes pour chaque transaction.
- ☑ Gestion des Clients et Fournisseurs
  - Suivi des comptes clients et fournisseurs, incluant les soldes et l'historique des transactions.
  - Relances automatiques pour les factures impayées et notifications de paiement.
  - Génération de rapports d'encours clients et de dettes fournisseurs.
- ☑ Facturation et Gestion des Recettes





- Création et envoi de factures personnalisées aux clients avec options de paiement en ligne.
- Suivi des paiements et rapprochement automatique avec les comptes.
- Gestion des reçus et des acomptes pour les transactions en plusieurs versements.
- ☑ Suivi de la Trésorerie
  - Visualisation des flux de trésorerie (entrées et sorties) en temps réel.
  - Prévisions de trésorerie basées sur les historiques de transactions et les prévisions de paiements.
  - Rapprochement bancaire automatique pour assurer la concordance des données entre les comptes bancaires et les comptes internes.
- ☑ Gestion des Immobilisations
  - Suivi des immobilisations (biens et équipements) avec calculs automatiques des amortissements.
  - Génération de fiches d'immobilisations avec valeurs d'achat, durées de vie, et taux d'amortissement.
  - Gestion des cessions et des réévaluations pour un suivi complet des actifs de l'entreprise.
- ☑ État Financier et Rapports Comptables
  - Génération de bilans comptables, comptes de résultats, et rapports de trésorerie.
  - Production de rapports détaillés pour le suivi des dépenses, revenus, et marges bénéficiaires.
  - Outils d'analyse et de visualisation pour une compréhension claire des indicateurs financiers clés.
- ☑ Conformité et Clôture de Fin d'Année
  - Préparation des écritures de clôture comptable pour la fin de l'exercice.
  - Génération d'états financiers pour les déclarations fiscales et la conformité réglementaire.
  - Archivage des données financières et des documents justificatifs conformément aux obligations légales.

#### 6.2.3.3.2. *Avantages de l'Application*

- ☑ Automatisation des tâches : Réduction des erreurs grâce à des fonctionnalités de saisie et de rapprochement automatiques.
- ☑ Gain de temps : Simplification des processus quotidiens et des tâches de clôture, permettant aux équipes comptables de se concentrer sur des analyses financières stratégiques.
- ☑ Visibilité financière : Accès en temps réel aux données financières pour une meilleure prise de décision.
- ☑ Conformité : Assure le respect des normes et des régulations comptables, limitant les risques de non-conformité.

#### 6.2.3.4. Procédures de l'application

##### 6.2.3.4.1. Gestion des Comptes

☒ Objectif :

Créer et gérer les comptes comptables pour le suivi financier.

☒ Etapes:

- 1) Accéder au module de gestion des comptes.
- 2) Sélectionner « Créer un nouveau compte ».
- 3) Remplir les champs requis : nom du compte, catégorie (actif, passif, etc.), et numéro de compte.
- 4) Enregistrer le compte pour l'ajouter au plan comptable.
- 5) Pour modifier un compte existant, sélectionner le compte, apporter les modifications nécessaires, puis enregistrer.
- 6) Consulter les soldes en accédant au tableau récapitulatif des comptes.

##### 6.2.3.4.2. Saisie des Écritures Comptables

☒ Objectif :

Enregistrer les transactions financières dans les comptes concernés.

☒ Etapes :

- 1) Ouvrir le module de saisie des écritures.
- 2) Cliquer sur « Ajouter une écriture ».
- 3) Renseigner les informations de l'écriture :
  - Date de la transaction.
  - Type d'opération (dépense, revenu, etc.).
  - Montant.
  - Compte débité et compte crédité.
- 4) Attacher toute pièce justificative au besoin (reçu, facture).
- 5) Enregistrer l'écriture pour la finaliser.
- 6) Vérifier l'écriture dans le journal comptable.

##### 6.2.3.4.3. Gestion des Clients et Fournisseurs

☒ Objectif :

Suivre les transactions avec les clients et les fournisseurs.

☒ Etapes :

- 1) Accéder au module de gestion des clients/fournisseurs.
- 2) Cliquer sur « Ajouter un client » ou « Ajouter un fournisseur ».
- 3) Remplir les informations requises (nom, adresse, coordonnées).
- 4) Enregistrer le profil du client/fournisseur.
- 5) Pour consulter les soldes :Sélectionner un client/fournisseur pour voir l'historique de ses transactions et le solde actuel.
- 6) Configurer des relances automatiques pour les factures impayées dans les paramètres de notifications.

#### 6.2.3.4.4. Facturation et Gestion des Recettes

- ☑ Objectif : Générer des factures pour les clients et enregistrer les paiements.
- ☑ Etapes :
  - 1) Ouvrir le module de facturation.
  - 2) Cliquer sur « Créer une nouvelle facture ».
  - 3) Renseigner les informations de la facture :
    - Client.
    - Détails des services/prestations.
    - Montant et conditions de paiement.
  - 4) Enregistrer et envoyer la facture par email ou lien de paiement sécurisé.
  - 5) Lors de la réception d'un paiement : Sélectionner la facture correspondante et cliquer sur « Enregistrer un paiement ».
  - 6) Si le paiement est partiel, enregistrer le montant reçu et le solde restant.
  - 7) Vérifier l'enregistrement de la transaction dans le journal des recettes.

#### 6.2.3.4.5. Suivi de la Trésorerie

- ☑ Objectif :

Visualiser les entrées et sorties de fonds pour gérer la trésorerie.
- ☑ Procédure :
  - 1) Accéder au module de trésorerie.
  - 2) Consulter le tableau de bord des flux de trésorerie pour voir les entrées et sorties actuelles.
  - 3) Pour visualiser les prévisions de trésorerie :
    - Sélectionner la période à analyser (hebdomadaire, mensuelle).
    - Examiner les prévisions générées à partir des transactions passées et des paiements à venir.
  - 4) Effectuer le rapprochement bancaire :
    - Importer les relevés bancaires.
    - Associer les transactions bancaires aux écritures dans APPLICATION.
    - Enregistrer le rapprochement pour la période concernée.

#### 6.2.3.4.6. Gestion des Immobilisations

- ☑ Objectif :

Suivre les actifs de l'entreprise et calculer les amortissements.
- ☑ Etapes :
  - 1) Accéder au module de gestion des immobilisations.
  - 2) Cliquer sur « Ajouter une immobilisation ».
  - 3) Renseigner les détails de l'immobilisation :
    - Nom, description.
    - Date d'acquisition.
    - Valeur d'acquisition et durée de vie estimée.

- 4) Sélectionner le mode de calcul d'amortissement (linéaire, dégressif).
- 5) Enregistrer l'immobilisation pour la suivre dans l'actif de l'entreprise.
- 6) Pour calculer l'amortissement périodique :
  - Accéder aux fiches d'immobilisation et générer les amortissements.
  - Consulter le tableau des amortissements pour voir les valeurs résiduelles.

#### 6.2.3.4.7. *États Financiers et Rapports Comptables*

- ☑ Objectif :  
Générer des rapports financiers pour le suivi de la performance financière.
- ☑ Etapes :
  - 1) Accéder au module des rapports financiers.
  - 2) Sélectionner le type de rapport à générer (bilan, compte de résultat, trésorerie).
  - 3) Choisir la période souhaitée (exercice comptable, mois, trimestre).
  - 4) Cliquer sur « Générer » pour obtenir le rapport.
  - 5) Examiner le rapport pour vérifier les informations.
  - 6) Exporter le rapport dans le format souhaité (PDF, Excel) ou l'imprimer pour archivage.

Page 171 sur 227



#### 6.2.3.4.8. *Conformité et Clôture de Fin d'Année*

- ☑ Objectif :  
Préparer les états financiers pour la fin d'exercice et assurer la conformité.
- ☑ Etapes :
  - 1) Ouvrir le module de clôture de fin d'année.
  - 2) Examiner les écritures et vérifier les soldes des comptes.
  - 3) Effectuer les écritures de clôture :
    - Calculer les écritures de régularisation (provisions, charges à payer, etc.).
    - Enregistrer les écritures de clôture pour l'exercice.
  - 4) Générer les états financiers finaux pour la déclaration fiscale (bilan, compte de résultat).
  - 5) Sauvegarder et archiver les rapports pour la conformité réglementaire.
  - 6) Clôturer officiellement l'exercice pour empêcher toute modification future.

#### 6.2.3.5. *Parties prenantes*

- ☑ Propriétaire de l'application : [Nom du responsable métier], [date de prise de fonction].
- ☑ Administrateurs système : [Nom des responsables techniques] , [date de prise de fonction].

- ☑ Utilisateurs clés : [Exemples d'utilisateurs stratégiques ou métiers] , [date de prise de fonction].

#### 6.2.4. Résultats de l'Audit

##### 6.2.4.1. Sécurité

###### 6.2.4.1.1. Contrôles d'accès

- ☑ Évaluation :

Les contrôles d'accès sont correctement implémentés pour la plupart des utilisateurs. Cependant, des droits excessifs ont été accordés à certains profils d'utilisateurs, notamment dans les modules [nom du module].

- ☑ Recommandation :

Mettre en place une revue régulière des droits d'accès avec la suppression des privilèges non justifiés.

###### 6.2.4.1.2. Chiffrement des données

- ☑ Évaluation :

Les données sensibles sont partiellement chiffrées. Les informations de connexion ne sont pas toujours transmises via un canal chiffré (ex : utilisation de http au lieu de HTTPS).

- ☑ Recommandation :

Activer le chiffrement SSL/TLS pour toutes les communications sensibles et renforcer la politique de chiffrement au niveau de la base de données.

###### 6.2.4.1.3. Journalisation des événements

- ☑ Évaluation :

La journalisation des événements est bien implémentée, mais certaines activités critiques (modification des données, accès aux zones sensibles) ne sont pas suffisamment suivies.

- ☑ Recommandation :

Améliorer la granularité des logs pour capturer toutes les opérations critiques, et intégrer les journaux dans un SIEM pour une analyse proactive des menaces.

##### 6.2.4.2. Performance

###### 6.2.4.2.1. Temps de réponse

- ☑ Évaluation :

Le temps de réponse moyen de l'application sous charge normale est de [X] secondes, ce qui est acceptable. Toutefois, des ralentissements significatifs ont été observés lors des pics de charge (> [nombre] utilisateurs simultanés).

- ☑ Recommandation :

Optimiser la gestion des sessions utilisateurs et envisager une mise à niveau de l'infrastructure serveur pour mieux supporter les pics de charge.

###### 6.2.4.2.2. Utilisation des ressources

- ☑ Évaluation :

Les ressources CPU et mémoire du serveur sont utilisées à [X]% de manière stable. Toutefois, des pics d'utilisation mémoire dépassant [Y]% ont été constatés lors de certaines opérations massives (ex : génération de rapports).

☑ **Recommandation :**

Effectuer un audit détaillé des processus consommateurs de ressources et envisager des optimisations logicielles.

#### 6.2.4.3. *Continuité d'activité*

##### 6.2.4.3.1. *Plan de Reprise d'Activité (PRA)*

☑ **Évaluation :**

Un plan de reprise d'activité est en place, mais il n'a pas été testé récemment.

☑ **Recommandation :**

Effectuer des tests réguliers du PRA, en particulier pour s'assurer que les sauvegardes sont fiables et que les temps de restauration sont conformes aux exigences.

##### 6.2.4.3.2. *Plan de Continuité d'Activité (PCA)*

☑ **Évaluation :**

Aucun plan formel de continuité n'a été identifié. L'application ne dispose pas de redondance suffisante pour garantir un service continu en cas de panne critique.

☑ **Recommandation :**

Mettre en place un PCA adapté, incluant des serveurs de secours et un basculement automatique en cas de défaillance.

#### 6.2.4.4. *Conformité*

☑ **Évaluation :**

APPLICATION est partiellement conforme aux exigences réglementaires locales et internationales. Des écarts ont été constatés dans la gestion des données personnelles, en particulier en ce qui concerne le RGPD.

☑ **Recommandation :**

Mettre à jour la politique de gestion des données personnelles pour se conformer pleinement aux règlements en vigueur (ex : droit à l'effacement, information des utilisateurs).

#### 6.2.4.5. *Gestion des changements*

☑ **Évaluation :**

Les processus de gestion des changements sont en place, mais certaines modifications critiques n'ont pas été correctement documentées.

☑ **Recommandation :**

Renforcer les processus de documentation des changements, en particulier pour les mises à jour importantes de l'application.

## 6.2.5. Observations

### 6.2.5.1. Observations Techniques

- ☑ Infrastructure :  
Certaines composantes de l'infrastructure hébergeant APPLICATION présentent des faiblesses en termes de [précisez : redondance, obsolescence matérielle, etc.], augmentant les risques de panne.
- ☑ Architecture Logicielle :  
La structure du code n'est pas optimisée pour supporter une montée en charge, ce qui entraîne des ralentissements aux heures de pointe.
- ☑ Gestion des Ressources :  
Une allocation inefficace des ressources, particulièrement en mémoire, a été identifiée, causant des performances dégradées lors des traitements lourds.
- ☑ Systèmes de Sauvegarde :  
Les sauvegardes sont réalisées, mais sans tests réguliers de restauration, augmentant le risque de défaillance en cas de sinistre.

### 6.2.5.2. Observations Métiers

- ☑ Alignement sur les Besoins Utilisateurs :  
Certains utilisateurs ont exprimé que l'interface de APPLICATION ne répond pas complètement aux besoins métier, entraînant des étapes manuelles supplémentaires.
- ☑ Précision et Disponibilité des Données :  
Des écarts dans l'actualisation des données métier (ex. : rapports financiers) ont été identifiés, affectant la prise de décision.
- ☑ Support Utilisateur :  
Les utilisateurs rapportent un manque de support technique réactif, ce qui ralentit la résolution des problèmes rencontrés lors de l'utilisation de l'application.
- ☑ Conformité aux Exigences de l'Entreprise :  
Des modifications récentes dans les processus métier ne sont pas encore intégrées dans APPLICATION, limitant ainsi son efficacité.

## 6.2.6. Synthèse des Recommandations

- ☑ Revue régulière des droits d'accès.
- ☑ Mise en place du chiffrement SSL/TLS pour toutes les communications.
- ☑ Amélioration des logs d'audit.
- ☑ Optimisation des performances et renforcement des infrastructures serveurs.
- ☑ Test régulier du PRA et mise en place d'un PCA.
- ☑ Mise à jour de la gestion des données personnelles pour la conformité RGPD.

### 6.2.7. Conclusion

Cet audit de APPLICATION met en évidence des points forts en matière de gestion des accès et de journalisation des événements. Cependant, plusieurs améliorations sont nécessaires pour renforcer la sécurité des données, améliorer la performance de l'application sous forte charge, et garantir la continuité du service. Les recommandations fournies doivent être rapidement mises en œuvre pour réduire les risques identifiés.

## 6.3. Création et chargement de la base de données de l'application APPLICATION.

### 6.3.1. Notes :

Chaque apprenant devra exécuter le script suivant pour générer la base de données de l'application APPLICATION à fin de mener à bien le cas pratique. Le but est d'avoir sur son ordinateur portable la même application fonctionnelle pour tous.

### 6.3.2. Création de la base de données avec contraintes :

#### 6.3.2.1. Création de la table pour gérer les plans comptables

```
CREATE TABLE PlanComptable (  
    id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque plan comptable  
    nom VARCHAR(255) NOT NULL UNIQUE,-- Nom du plan comptable, doit être unique  
    description TEXT-- Description optionnelle du plan comptable  
);
```

#### 6.3.2.2. Création de la table pour gérer les comptes

```
CREATE TABLE Compte (  
    id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque compte  
    nom VARCHAR(255) NOT NULL,-- Nom du compte  
    type VARCHAR(50) NOT NULL CHECK (type IN ('Actif', 'Passif', 'Capitaux propres')),-- Type de compte  
    (avec validation)  
    numero VARCHAR(50) NOT NULL UNIQUE,-- Numéro unique du compte  
    solde DECIMAL(18, 2) NOT NULL DEFAULT 0 CHECK (solde >= 0),-- Solde du compte, ne peut pas être  
    négatif  
    plan_comptable_id INT NOT NULL,-- Référence au plan comptable associé  
    FOREIGN KEY (plan_comptable_id) REFERENCES PlanComptable(id) ON DELETE CASCADE-- Suppression  
    en cascade si le plan comptable est supprimé  
);
```



### 6.3.2.3. Création de la table pour gérer les écritures comptables

```
CREATE TABLE Ecriture (  
    id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque écriture  
    date DATE NOT NULL CHECK (date <= CURRENT_DATE),-- Date de l'écriture, ne peut pas être future  
    montant DECIMAL(18, 2) NOT NULL CHECK (montant > 0),-- Montant de l'écriture, doit être positif  
    commentaire TEXT,-- Commentaire optionnel sur l'écriture  
    justificatif VARCHAR(255),-- Chemin du justificatif de l'écriture (optionnel)  
    debit_id INT NOT NULL,-- Référence au compte débité  
    credit_id INT NOT NULL,-- Référence au compte crédité  
    FOREIGN KEY (debit_id) REFERENCES Compte(id) ON DELETE CASCADE,-- Suppression en cascade si le  
    compte débité est supprimé  
    FOREIGN KEY (credit_id) REFERENCES Compte(id) ON DELETE CASCADE-- Suppression en cascade si le  
    compte crédité est supprimé  
);
```

### 6.3.2.4. Création de la table pour gérer les clients

```
CREATE TABLE Client (  
    id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque client  
    nom VARCHAR(255) NOT NULL,-- Nom du client  
    adresse TEXT,-- Adresse du client (optionnelle)  
    email VARCHAR(255) UNIQUE CHECK (email ~* '^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}$'),--  
    Email unique et formaté  
    telephone VARCHAR(50)-- Téléphone du client (optionnel)  
);
```

### 6.3.2.5. Création de la table pour gérer les fournisseurs

```
CREATE TABLE Fournisseur (  
    id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque fournisseur  
    nom VARCHAR(255) NOT NULL,-- Nom du fournisseur  
    adresse TEXT,-- Adresse du fournisseur (optionnelle)  
    email VARCHAR(255) UNIQUE CHECK (email ~* '^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}$'),--  
    Email unique et formaté  
    telephone VARCHAR(50)-- Téléphone du fournisseur (optionnel)  
);
```

### 6.3.2.6. Création de la table pour gérer les factures

CREATE TABLE Facture (

id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque facture

numero VARCHAR(50) NOT NULL,-- Numéro de la facture

date\_emission DATE NOT NULL CHECK (date\_emission <= CURRENT\_DATE),-- Date d'émission, ne peut pas être future

date\_echeance DATE NOT NULL CHECK (date\_echeance >= date\_emission),-- Date d'échéance, doit être postérieure ou égale à la date d'émission

montant\_total DECIMAL(18, 2) NOT NULL CHECK (montant\_total >= 0),-- Montant total de la facture, doit être positif ou nul

etat VARCHAR(50) NOT NULL CHECK (etat IN ('Non payé', 'Partiellement payé', 'Payé')),-- État de la facture (avec validation)

client\_id INT,-- Référence au client associé (optionnel)

fournisseur\_id INT,-- Référence au fournisseur associé (optionnel)

FOREIGN KEY (client\_id) REFERENCES Client(id) ON DELETE SET NULL,-- Si le client est supprimé, mettre la référence à NULL

FOREIGN KEY (fournisseur\_id) REFERENCES Fournisseur(id) ON DELETE SET NULL-- Si le fournisseur est supprimé, mettre la référence à NULL

);

#### 6.3.2.7. Création de la table pour gérer la trésorerie

CREATE TABLE Tresorerie (

id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque entrée de trésorerie

date DATE NOT NULL CHECK (date <= CURRENT\_DATE),-- Date de l'entrée/sortie, ne peut pas être future

flux VARCHAR(50) NOT NULL CHECK (flux IN ('Entrée', 'Sortie')),-- Type de flux (Entrée ou Sortie)

montant DECIMAL(18, 2) NOT NULL CHECK (montant > 0),-- Montant de la trésorerie, doit être positif

description TEXT-- Description optionnelle de l'entrée/sortie

);

#### 6.3.2.8. Création de la table pour gérer les immobilisations

CREATE TABLE Immobilisation (

id SERIAL PRIMARY KEY,-- Identifiant unique pour chaque immobilisation

nom VARCHAR(255) NOT NULL,-- Nom de l'immobilisation

description TEXT,-- Description optionnelle de l'immobilisation

date\_acquisition DATE NOT NULL CHECK (date\_acquisition <= CURRENT\_DATE),-- Date d'acquisition, ne peut pas être future

valeur\_acquisition DECIMAL(18, 2) NOT NULL CHECK (valeur\_acquisition >= 0),-- Valeur d'acquisition, doit être positive ou nulle

duree\_de\_vie INT NOT NULL CHECK (duree\_de\_vie > 0),-- Durée de vie de l'immobilisation, doit être positive

taux\_amortissement DECIMAL(5, 4) NOT NULL CHECK (taux\_amortissement BETWEEN 0 AND 1),-- Taux d'amortissement (entre 0 et 1)

valeur\_residuelle DECIMAL(18, 2) CHECK (valeur\_residuelle >= 0)-- Valeur résiduelle, doit être positive ou nulle

);

### 6.3.3. Chargement d'un jeu de données dans la base de données :

#### 6.3.3.1. Données de la table PlanComptable

INSERT INTO PlanComptable (nom, description) VALUES

('Plan Comptable Général', 'Plan comptable standard pour entreprises.'),

('Plan Comptable Simplifié', 'Plan comptable pour les petites entreprises.'),

('Plan Comptable Avancé', 'Plan comptable pour les grandes entreprises.'),

('Plan Comptable Associatif', 'Plan comptable pour associations.'),

('Plan Comptable Bancaire', 'Plan comptable spécifique au secteur bancaire.');

#### 6.3.3.2. Données de la table Compte

INSERT INTO Compte (nom, type, numero, solde, plan\_comptable\_id) VALUES

('Caisse', 'Actif', '1000', 15000.00, 1),

('Banque', 'Actif', '1001', 50000.00, 1),

('Capital Social', 'Capitaux propres', '3000', 100000.00, 1),

('Dettes Fournisseurs', 'Passif', '2000', 25000.00, 1),

('Immobilisations Corporelles', 'Actif', '4000', 75000.00, 1);

-- Génération de 100 lignes supplémentaires pour la table Compte

DO \$\$

DECLARE

i INT;

BEGIN

FOR i IN 6..100 LOOP

INSERT INTO Compte (nom, type, numero, solde, plan\_comptable\_id)

VALUES (

'Compte ' || i,

CASE WHEN i % 3 = 0 THEN 'Actif' WHEN i % 3 = 1 THEN 'Passif' ELSE 'Capitaux propres' END,

'10' || i,

ROUND(RANDOM() \* 10000, 2),

```

1
);
END LOOP;
END $$;

```

#### 6.3.3.3. *Données de la table Ecriture*

```

DO $$
DECLARE
    i INT;
BEGIN
    FOR i IN 1..100 LOOP
        INSERT INTO Ecriture (date, montant, commentaire, debit_id, credit_id)
        VALUES (
            CURRENT_DATE- (i * INTERVAL '1 day'),
            ROUND(RANDOM() * 5000 + 100, 2),
            'Ecriture automatique ' || i,
            (i % 20) + 1,
            ((i + 10) % 20) + 1
        );
    END LOOP;
END $$;

```

#### 6.3.3.4. *Données de la table Client*

```

DO $$
DECLARE
    i INT;
BEGIN
    FOR i IN 1..100 LOOP
        INSERT INTO Client (nom, adresse, email, telephone)
        VALUES (
            'Client ' || i,
            'Adresse ' || i,
            'client' || i || '@example.com',

```

```

        '6' || i || '0000000'
    );
END LOOP;
END $$;

```

#### 6.3.3.5. Données de la table Fournisseur

```

DO $$
DECLARE
    i INT;
BEGIN
    FOR i IN 1..100 LOOP
        INSERT INTO Fournisseur (nom, adresse, email, telephone)
        VALUES (
            'Fournisseur ' || i,
            'Adresse ' || i,
            'fournisseur' || i || '@example.com',
            '7' || i || '0000000'
        );
    END LOOP;
END $$;

```

#### 6.3.3.6. Données de la table Facture

```

DO $$
DECLARE
    i INT;
BEGIN
    FOR i IN 1..100 LOOP
        INSERT INTO Facture (numero, date_emission, date_echeance, montant_total, etat, client_id,
fournisseur_id)
        VALUES (
            'F' || LPAD(i::TEXT, 3, '0'),
            CURRENT_DATE - (i * INTERVAL '1 day'),
            CURRENT_DATE + ((i % 10) * INTERVAL '1 day'),
            ROUND(RANDOM() * 1000 + 500, 2),

```

```

CASE WHEN i % 3 = 0 THEN 'Non payé' WHEN i % 3 = 1 THEN 'Partiellement payé' ELSE 'Payé' END,
(i % 20) + 1,
((i + 5) % 20) + 1
);
END LOOP;
END $$;

```

#### 6.3.3.7. Données de la table Tresorerie

```

DO $$
DECLARE
    i INT;
BEGIN
    FOR i IN 1..100 LOOP
        INSERT INTO Tresorerie (date, flux, montant, description)
        VALUES (
            CURRENT_DATE - (i * INTERVAL '1 day'),
            CASE WHEN i % 2 = 0 THEN 'Entrée' ELSE 'Sortie' END,
            ROUND(RANDOM() * 3000 + 500, 2),
            'Transaction ' || i
        );
    END LOOP;
END $$;

```

#### 6.3.3.8. Données de la table Immobilisation

```

DO $$
DECLARE
    i INT;
BEGIN
    FOR i IN 1..100 LOOP
        INSERT INTO Immobilisation (nom, description, date_acquisition, valeur_acquisition, duree_de_vie,
        taux_amortissement, valeur_residuelle)
        VALUES (
            'Immobilisation ' || i,
            'Description de l'immobilisation ' || i,

```

```

CURRENT_DATE- ((i * 30) * INTERVAL '1 day'),
ROUND(RANDOM() * 10000 + 1000, 2),
(i % 10) + 1,
ROUND(RANDOM(), 4),
ROUND(RANDOM() * 500, 2)
);
END LOOP;
END $$;

```

## 6.4. Conception de l'outil pour l'évaluation du système de contrôle interne de l'application APPLICATION.

### 6.4.1. *Domaine : Environnement de Contrôle*

#### 6.4.1.1. *Point de contrôle : Engagement envers l'intégrité et les valeurs éthiques*

##### 6.4.1.1.1. *Objectifs de contrôle :*

- ☒ *S'assurer que l'organisation dispose d'une charte éthique formelle qui couvre l'ensemble des pratiques professionnelles et des interactions au sein de l'organisation, y compris les activités liées aux systèmes d'information.*
- ☒ *Vérifier que des mécanismes existent pour garantir que tous les acteurs (employés, partenaires, prestataires) respectent cette charte éthique dans leurs activités professionnelles, y compris dans leur utilisation des systèmes d'information*
- ☒ *S'assurer que des actions de sensibilisation, telles que des formations régulières, sont mises en place pour garantir que tous les employés et intervenants comprennent et appliquent les principes éthiques dans leurs interactions avec les systèmes d'information*
- ☒ *S'assurer que l'organisation dispose d'un mécanisme de suivi et de gestion des violations éthiques, permettant de détecter, traiter et sanctionner tout comportement contraire à la charte éthique, y compris dans le cadre des activités liées aux systèmes d'information.*

#### 6.4.1.2. *Point de contrôle : Le Conseil fait preuve d'indépendance vis-à-vis du management.*

##### 6.4.1.2.1. *Objectifs de contrôle :*

- ☒ *S'assurer que le Conseil est composé de membres indépendants du management, avec une structure de gouvernance claire garantissant cette indépendance.*

- ☑ Vérifier que le Conseil dispose des ressources et des informations nécessaires pour surveiller efficacement la mise en place et le bon fonctionnement du dispositif de contrôle interne.
- ☑ S'assurer que le Conseil reçoit régulièrement des rapports détaillés sur l'efficacité du dispositif de contrôle interne et qu'il est impliqué dans l'évaluation des résultats des audits internes.
- ☑ Vérifier que le Conseil joue un rôle actif dans la définition des objectifs et des critères de performance du contrôle interne, et qu'il veille à leur alignement avec les objectifs stratégiques de l'organisation.
- ☑ S'assurer que le Conseil prend des mesures appropriées lorsque des dysfonctionnements ou des lacunes dans le contrôle interne sont identifiés, y compris la mise en place de plans d'action correctifs.
- ☑ Vérifier que le Conseil évalue régulièrement la performance des responsables du contrôle interne et veille à ce que leurs actions soient indépendantes et objectives.

#### 6.4.1.3. Point de contrôle : Structures, autorités et responsabilités

##### 6.4.1.3.1. Objectifs de contrôle :

- ☑ S'assurer que la structure organisationnelle est clairement définie, incluant les rattachements hiérarchiques, les rôles, les responsabilités et les pouvoirs de chaque collaborateur.
- ☑ Vérifier que les responsabilités et les pouvoirs sont attribués de manière appropriée, en fonction des compétences et des objectifs stratégiques de l'organisation.
- ☑ S'assurer que la structure organisationnelle est régulièrement revue et mise à jour pour tenir compte des changements dans l'environnement interne ou externe de l'organisation.
- ☑ Vérifier que le management reçoit l'approbation du Conseil pour les modifications de la structure organisationnelle, afin d'assurer une supervision adéquate des changements importants.
- ☑ S'assurer que des mécanismes sont en place pour communiquer la structure organisationnelle à tous les collaborateurs, afin qu'ils comprennent clairement leurs rôles et leurs responsabilités.
- ☑ Vérifier que les structures, les rattachements et les responsabilités sont clairement documentés et accessibles pour consultation, garantissant une traçabilité des décisions organisationnelles.

#### 6.4.1.4. Point de contrôle : Compétences des individus

##### 6.4.1.4.1. Objectifs de contrôle :

- ☑ S'assurer que l'organisation dispose de processus clairs et formalisés pour attirer des talents qualifiés dans les domaines nécessaires à son fonctionnement, y compris pour les systèmes d'information.
- ☑ Vérifier que l'organisation met en place des programmes de formation continue pour ses collaborateurs, en particulier dans les



domaines stratégiques comme la gestion des systèmes d'information et la cybersécurité.

- ☑ S'assurer que des mécanismes de fidélisation des talents sont en place, tels que des parcours de carrière, des avantages compétitifs et des opportunités de développement personnel, pour encourager les collaborateurs à rester au sein de l'organisation.
- ☑ Vérifier que des évaluations régulières de la performance des collaborateurs sont menées, avec des retours constructifs et des opportunités de développement, afin d'assurer leur progression professionnelle.
- ☑ S'assurer que les processus d'attraction, de formation et de fidélisation des talents sont alignés avec les objectifs stratégiques de l'organisation, en garantissant qu'ils contribuent à la performance globale.

#### 6.4.2. Domaine : Évaluation des Risques

##### 6.4.2.1. Point de contrôle : Spécification des objectifs appropriés

###### 6.4.2.1.1. Objectifs de contrôle :

- ☑ S'assurer que les responsabilités de chaque collaborateur en matière de contrôle interne sont clairement définies, documentées et communiquées à l'ensemble de l'organisation.
- ☑ Vérifier que des mécanismes de suivi sont mis en place pour s'assurer que les responsables respectent leurs responsabilités en matière de contrôle interne et rendent compte de leur gestion.
- ☑ S'assurer que des processus de reporting sont en place pour permettre à chaque responsable de rendre compte de l'accomplissement de ses tâches liées au contrôle interne, avec des indicateurs de performance définis.
- ☑ Vérifier que des procédures de contrôle sont en place pour évaluer la conformité des actions des responsables avec les normes de contrôle interne, et pour identifier les non-conformités ou les écarts.
- ☑ S'assurer que des actions correctives sont mises en place lorsque des responsables ne respectent pas leurs responsabilités en matière de contrôle interne, avec des mesures de soutien ou de discipline appropriées.
- ☑ Vérifier que des mécanismes de formation et de sensibilisation sont mis en place pour renforcer la compréhension et l'engagement de chaque collaborateur vis-à-vis de ses responsabilités en matière de contrôle interne.

##### 6.4.2.2. Point de contrôle : Identification et analyse des risques

###### 6.4.2.2.1. Objectifs de Contrôle :

- ☑ S'assurer que l'organisation dispose d'une structure organisationnelle clairement définie, incluant les rôles et responsabilités relatifs à la gestion des systèmes d'information.

- ☑ Vérifier que les responsabilités liées à la sécurité des systèmes d'information et à la gestion des données sont attribuées à des postes spécifiques, avec des descriptions de rôle formalisées.
- ☑ S'assurer que les responsables des systèmes d'information, ainsi que les autres parties prenantes, sont dotés des ressources et des autorisations nécessaires pour exercer efficacement leurs responsabilités.
- ☑ Vérifier que des mécanismes de communication efficaces existent pour assurer une coordination fluide entre les différents départements et les responsables des systèmes d'information.
- ☑ S'assurer qu'il existe une hiérarchie de responsabilité permettant de rendre compte de la performance des systèmes d'information, avec des rapports réguliers destinés à la direction.

#### 6.4.2.3. Point de contrôle : Prise en compte de la fraude

##### 6.4.2.3.1. Objectifs de Contrôle :

- ☑ S'assurer que le risque de fraude est explicitement intégré dans le processus d'évaluation des risques, en identifiant les risques spécifiques de fraude qui pourraient affecter les objectifs de l'organisation.
- ☑ Vérifier que des méthodologies spécifiques sont utilisées pour évaluer le risque de fraude, incluant l'identification des domaines vulnérables à la fraude et l'analyse des contrôles existants pour les atténuer.
- ☑ S'assurer que des responsables sont désignés pour l'évaluation et la gestion du risque de fraude, et qu'ils reçoivent une formation adéquate pour identifier et traiter ce type de risque de manière proactive.
- ☑ Vérifier que des mécanismes de surveillance et de contrôle spécifiques sont mis en place pour surveiller en continu les risques de fraude, avec des rapports réguliers sur l'état des contrôles et des incidents potentiels.
- ☑ S'assurer que le risque de fraude est pris en compte dans les évaluations de performance et que des mesures correctives sont mises en place si des failles dans le système de contrôle interne sont identifiées.
- ☑ Vérifier que des rapports détaillés sur les risques de fraude sont fournis régulièrement à la direction, avec des évaluations sur les risques identifiés et les mesures prises pour y faire face.

#### 6.4.2.4. Point de Contrôle : Identification et analyse des changements significatifs

##### 6.4.2.4.1. Objectifs de Contrôle :

- ☑ S'assurer que l'organisation met en place un processus structuré pour identifier les changements, qu'ils soient internes (réorganisations, nouvelles technologies, etc.) ou externes (évolutions réglementaires, marché, etc.), susceptibles d'affecter le système de contrôle interne.

- ☑ S'assurer que l'organisation met en place un processus structuré pour identifier les changements, qu'ils soient internes (réorganisations, nouvelles technologies, etc.) ou externes (évolutions réglementaires, marché, etc.), susceptibles d'affecter le système de contrôle interne.
- ☑ S'assurer que l'organisation met en place un processus structuré pour identifier les changements, qu'ils soient internes (réorganisations, nouvelles technologies, etc.) ou externes (évolutions réglementaires, marché, etc.), susceptibles d'affecter le système de contrôle interne.
- ☑ Vérifier que les changements identifiés sont évalués de manière formelle et structurée, avec une analyse de l'impact potentiel sur les contrôles internes et les risques associés.
- ☑ S'assurer que les responsables du contrôle interne sont impliqués dans l'identification et l'évaluation des changements, afin qu'ils puissent adapter les contrôles en conséquence.
- ☑ Vérifier que des plans d'action sont mis en place pour ajuster le système de contrôle interne en fonction des changements identifiés, y compris des processus de mise à jour et de révision des contrôles existants.
- ☑ S'assurer que les changements et leur impact sur le système de contrôle interne sont régulièrement suivis et que des rapports détaillés sont fournis à la direction pour assurer une prise de décision informée.
- ☑ Vérifier que le Conseil ou un comité de gouvernance est informé des changements significatifs affectant le contrôle interne et qu'il valide les mesures prises pour adapter le système en conséquence.

#### 6.4.3. Domaine : Activités de Contrôle

##### 6.4.3.1. Point de contrôle : Sélection et développement des activités de contrôle

##### 6.4.3.1.1. Objectifs de Contrôle :

- ☑ S'assurer que l'organisation identifie et évalue les risques potentiels qui pourraient affecter la réalisation de ses objectifs stratégiques, opérationnels et financiers.
- ☑ Vérifier que l'évaluation des risques est effectuée de manière continue, avec des processus de mise à jour réguliers pour prendre en compte les nouvelles menaces ou opportunités.
- ☑ Vérifier que l'évaluation des risques est effectuée de manière continue, avec des processus de mise à jour réguliers pour prendre en compte les nouvelles menaces ou opportunités.
- ☑ S'assurer que les risques identifiés sont évalués en fonction de leur probabilité d'occurrence et de leur impact potentiel sur l'organisation.
- ☑ Vérifier que l'organisation met en place des actions de gestion des risques pour atténuer ou minimiser les risques significatifs identifiés.

- ☑ S'assurer que les résultats de l'évaluation des risques sont documentés et communiqués aux parties prenantes pertinentes, y compris à la direction, pour garantir une gestion proactive des risques.

#### 6.4.3.2. Développement des activités de contrôle sur les technologies

##### 6.4.3.2.1. Objectifs de Contrôle :

- ☑ S'assurer que l'organisation sélectionne des activités de contrôle adaptées aux risques identifiés, en prenant en compte la nature, l'ampleur et la criticité des risques.
- ☑ Vérifier que des mécanismes de suivi sont mis en place pour évaluer l'efficacité des activités de contrôle dans la réduction des risques à des niveaux acceptables.
- ☑ S'assurer que les activités de contrôle sont intégrées dans les processus opérationnels de l'organisation, de manière à garantir que les risques sont gérés de manière continue et proactive.
- ☑ Vérifier que les activités de contrôle sont adaptées à l'évolution des risques, avec des ajustements réguliers pour garantir qu'elles restent efficaces face à des risques changeants.
- ☑ Vérifier que les activités de contrôle sont adaptées à l'évolution des risques, avec des ajustements réguliers pour garantir qu'elles restent efficaces face à des risques changeants.
- ☑ S'assurer que les responsabilités des différentes parties prenantes concernant les activités de contrôle sont clairement définies et que les ressources nécessaires sont allouées pour leur mise en œuvre.
- ☑ Vérifier que les résultats des activités de contrôle sont documentés et partagés avec la direction, permettant une évaluation régulière et un ajustement des stratégies de gestion des risques.

#### 6.4.3.3. Point de contrôle : Mise en œuvre des politiques et procédures

##### 6.4.3.3.1. Objectifs de Contrôle :

- ☑ S'assurer que l'organisation sélectionne des contrôles généraux informatiques appropriés pour protéger les systèmes d'information contre les menaces internes et externes.
- ☑ Vérifier que les contrôles généraux informatiques sont conçus pour être efficaces à tous les niveaux de l'infrastructure informatique, incluant les réseaux, les bases de données, les applications et les dispositifs matériels.
- ☑ S'assurer que les contrôles généraux informatiques sont régulièrement réévalués pour tenir compte des évolutions technologiques, des nouvelles menaces et des changements dans l'infrastructure de l'organisation.
- ☑ Vérifier que des mécanismes de suivi sont en place pour surveiller la mise en œuvre des contrôles généraux informatiques et évaluer leur efficacité en continu.
- ☑ S'assurer que les responsables de la mise en œuvre des contrôles généraux informatiques sont qualifiés et formés pour gérer les risques informatiques et maintenir les contrôles à jour.

- ☑ Vérifier que des procédures documentées sont en place pour la mise en œuvre, la gestion et la réévaluation des contrôles généraux informatiques, garantissant la cohérence et la traçabilité des actions entreprises.
- ☑ Vérifier que des procédures documentées sont en place pour la mise en œuvre, la gestion et la réévaluation des contrôles généraux informatiques, garantissant la cohérence et la traçabilité des actions entreprises.
- ☑ S'assurer que des tests d'audit sont régulièrement réalisés pour vérifier l'efficacité des contrôles généraux informatiques et leur conformité aux normes et réglementations applicables.
- ☑ S'assurer que des règles de contrôle claires et bien définies sont mises en place pour chaque domaine critique, et qu'elles couvrent toutes les activités pertinentes pour assurer la conformité et la gestion des risques.
- ☑ Vérifier que des procédures détaillées sont établies pour mettre en œuvre les règles de contrôle, avec des instructions précises sur la manière de suivre et de maintenir ces règles dans les opérations quotidiennes.
- ☑ S'assurer que les règles et procédures sont régulièrement révisées et mises à jour pour refléter les changements dans l'environnement interne et externe, les évolutions réglementaires ou les améliorations des meilleures pratiques.
- ☑ Vérifier que les responsables des contrôles sont impliqués dans la définition et la mise à jour des règles et des procédures, afin de garantir que celles-ci répondent aux besoins spécifiques des systèmes d'information et aux exigences de contrôle.

#### 6.4.4. Domaine : Information et Communication

##### 6.4.4.1. Point de contrôle : Utilisation d'informations de qualité

##### 6.4.4.1.1. Objectifs de Contrôle :

- ☑ S'assurer que des mécanismes de suivi sont en place pour garantir le respect des règles et procédures de contrôle, avec des rapports réguliers sur leur mise en œuvre et des audits pour vérifier leur efficacité.
- ☑ Vérifier que des actions correctives sont prises lorsque des écarts sont identifiés dans l'application des règles et procédures de contrôle, avec des processus de mise à jour ou de renforcement des contrôles si nécessaire.
- ☑ Vérifier que des actions correctives sont prises lorsque des écarts sont identifiés dans l'application des règles et procédures de contrôle, avec des processus de mise à jour ou de renforcement des contrôles si nécessaire.
- ☑ S'assurer que des formations régulières sont proposées aux collaborateurs pour garantir leur compréhension et leur capacité à mettre en œuvre correctement les règles et procédures de contrôle.

- ☑ S'assurer que des mécanismes sont en place pour collecter des informations fiables et pertinentes sur les activités de l'organisation, en particulier celles liées au contrôle interne.
- ☑ S'assurer que des mécanismes sont en place pour collecter des informations fiables et pertinentes sur les activités de l'organisation, en particulier celles liées au contrôle interne.
- ☑ Vérifier que les informations générées sont complètes, précises et à jour, de manière à refléter fidèlement la situation de l'organisation et ses performances en matière de contrôle interne.
- ☑ S'assurer que les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne sont accessibles en temps utile et sous un format compréhensible pour les responsables concernés.

#### 6.4.4.2. Point de contrôle : Communication interne

##### 6.4.4.2.1. Objectifs de Contrôle :

- ☑ Vérifier que des processus formels de validation des informations sont mis en place pour garantir leur exactitude, leur fiabilité et leur cohérence avant leur utilisation dans les autres composantes du contrôle interne.
- ☑ S'assurer que les informations relatives aux risques et aux contrôles internes sont régulièrement mises à jour et partagées avec les parties prenantes pertinentes, y compris la direction et le Conseil.
- ☑ Vérifier que des outils de gestion de l'information et des technologies appropriées sont utilisés pour faciliter la collecte, l'analyse et la distribution des informations pertinentes relatives au contrôle interne.
- ☑ S'assurer que l'organisation a mis en place des processus formels pour communiquer de manière régulière et transparente les informations nécessaires au fonctionnement du contrôle interne à tous les niveaux de l'organisation.
- ☑ Vérifier que les informations sont partagées de manière appropriée, en fonction des rôles et des responsabilités des différentes parties prenantes, et qu'elles sont adaptées à leur niveau de responsabilité.
- ☑ S'assurer que les informations partagées en interne sont pertinentes et à jour, en particulier celles relatives aux risques identifiés, aux actions de contrôle mises en place et aux résultats des évaluations de performance.

#### 6.4.4.3. Point de contrôle : Communication externe

##### 6.4.4.3.1. Objectifs de Contrôle :

- ☑ Vérifier que des mécanismes de feedback sont mis en place pour permettre aux parties prenantes internes de poser des questions et d'obtenir des éclaircissements sur les informations reçues.
- ☑ S'assurer que des outils de communication adéquats (réunions, rapports, systèmes d'information) sont utilisés pour faciliter l'échange d'informations entre les différentes parties prenantes impliquées dans le contrôle interne.



- ☑ *Vérifier que la communication interne des informations nécessaires au contrôle interne est régulièrement suivie, avec des rapports ou des audits pour évaluer l'efficacité des mécanismes de communication en place.*
- ☑ *S'assurer que l'organisation dispose de processus formels pour communiquer avec les tiers sur les points pertinents concernant le contrôle interne, notamment les risques et les mesures prises pour y faire face.*
- ☑ *Vérifier que les parties prenantes externes sont informées en temps utile des évolutions qui peuvent avoir un impact sur le fonctionnement du contrôle interne, en particulier lorsqu'il y a des changements significatifs dans l'organisation ou dans la réglementation applicable.*
- ☑ *S'assurer que les informations partagées avec les tiers sont pertinentes, complètes et compréhensibles, et qu'elles sont adaptées au rôle et aux besoins de chaque partie prenante externe.*

#### 6.4.5. Activités de Surveillance

##### 6.4.5.1. Évaluations continues et indépendantes

###### 6.4.5.1.1. Objectifs de Contrôle :

- ☑ *Vérifier que des mécanismes de suivi et de contrôle sont en place pour s'assurer que les tiers respectent les engagements relatifs au contrôle interne, et que les résultats de cette coopération sont régulièrement évalués.*
- ☑ *S'assurer que des mesures sont mises en place pour gérer les risques associés à la communication avec les tiers, notamment en termes de confidentialité, de conformité aux réglementations et de protection des données sensibles.*
- ☑ *Vérifier que les résultats des échanges avec les tiers sont documentés et intégrés dans le système de gestion des risques, afin d'assurer que le contrôle interne reste efficace face aux risques externes.*
- ☑ *S'assurer que l'organisation met en place des processus d'évaluation continue pour surveiller l'efficacité des composantes du contrôle interne de manière régulière et systématique.*
- ☑ *Vérifier que des évaluations ponctuelles sont réalisées lors de changements importants (réorganisation, introduction de nouvelles technologies, etc.) pour s'assurer que les composantes du contrôle interne restent adaptées et efficaces dans ces nouveaux contextes.*
- ☑ *S'assurer que les responsables des composantes du contrôle interne sont impliqués dans les évaluations et qu'ils sont informés des résultats afin de pouvoir apporter des améliorations lorsque cela est nécessaire.*

##### 6.4.5.2. Évaluation des déficiences

###### 6.4.5.2.1. Objectifs de Contrôle :

- ☑ *Vérifier que des critères d'évaluation clairs et mesurables sont utilisés pour évaluer l'efficacité des composantes du contrôle interne, y compris des indicateurs de performance et des seuils de tolérance définis.*
- ☑ *S'assurer que les résultats des évaluations sont documentés et partagés avec la direction et le Conseil, afin qu'ils puissent prendre des décisions éclairées sur les actions correctives et l'adaptation du contrôle interne.*
- ☑ *Vérifier que les évaluations sont suivies de plans d'action correctifs lorsque des failles ou des défaillances sont identifiées, et que ces plans sont mis en œuvre efficacement dans les délais impartis.*

## 6.5. Conception de l'outil pour l'audit des aspects métiers de l'application APPLICATION.

### 6.5.1. *Domaine : Gestion des Comptes*

#### 6.5.1.1. *Point de Contrôle : Création des comptes comptables*

- ☑ Objectif de Contrôle : Assurer que les comptes sont créés conformément au plan comptable.
- ☑ Critère d'Évaluation : Le compte suit le format et les catégories du plan comptable de l'entreprise.
- ☑ Question d'Évaluation : Le compte est-il conforme aux catégories prédéfinies dans le plan comptable ?
- ☑ Document Requis : Plan comptable de l'entreprise.
- ☑ Risque : Non-conformité avec le plan comptable.
- ☑ Conséquence : Difficulté de suivre les transactions.
- ☑ Criticité : Élevé

#### 6.5.1.2. *Point de Contrôle : Validation des comptes créés*

- ☑ Objectif de Contrôle : Assurer l'exactitude et la validation des nouveaux comptes créés.
- ☑ Critère d'Évaluation : Tous les comptes créés sont approuvés par un responsable.
- ☑ Question d'Évaluation : Les comptes créés ont-ils été validés par un responsable ?
- ☑ Document Requis : Fiche d'approbation des comptes.
- ☑ Risque : Création de comptes non validés.
- ☑ Conséquence : Comptes redondants ou erronés.
- ☑ Criticité : Moyen

#### 6.5.1.3. *Point de Contrôle : Mise à jour des soldes de comptes*



- ☑ Objectif de Contrôle : Vérifier que les soldes sont actualisés après chaque transaction.
- ☑ Critère d'Évaluation : Les soldes sont révisés en temps réel après chaque transaction.
- ☑ Question d'Évaluation : Les soldes des comptes sont-ils automatiquement mis à jour ?
- ☑ Document Requis : Journal de transactions.
- ☑ Risque : Retard dans la mise à jour des soldes.
- ☑ Conséquence : Déséquilibres financiers.
- ☑ Criticité : Élevé

## 6.5.2. *Domaine : Saisie des Écritures Comptables*

### 6.5.2.1. *Point de Contrôle : Exactitude des informations saisies*

- ☑ Objectif de Contrôle : Garantir que les transactions sont enregistrées correctement.
- ☑ Critère d'Évaluation : Les écritures saisies incluent tous les détails (montant, comptes concernés, date).
- ☑ Question d'Évaluation : Les transactions sont-elles enregistrées avec toutes les informations requises ?
- ☑ Document Requis : Pièce justificative.
- ☑ Risque : Saisie incomplète des informations.
- ☑ Conséquence : Informations comptables inexactes.
- ☑ Criticité : Élevé

### 6.5.2.2. *Point de Contrôle : Revue et approbation des transactions*

- ☑ Objectif de Contrôle : Assurer que les transactions sont validées avant enregistrement définitif.
- ☑ Critère d'Évaluation : Chaque transaction est approuvée par un responsable.
- ☑ Question d'Évaluation : La transaction a-t-elle été validée par un responsable ?
- ☑ Document Requis : Fiche de validation de transaction.
- ☑ Risque : Enregistrement de transactions non validées.
- ☑ Conséquence : Risque d'erreurs non détectées.
- ☑ Criticité : Moyen

### 6.5.2.3. *Point de Contrôle : Attachement de la pièce justificative*

- ☑ Objectif de Contrôle : Vérifier la traçabilité des transactions.
- ☑ Critère d'Évaluation : Chaque transaction est appuyée par une pièce justificative.
- ☑ Question d'Évaluation : Une pièce justificative est-elle attachée à chaque transaction ?
- ☑ Document Requis : Copie des pièces justificatives.
- ☑ Risque : Absence de justificatif pour les transactions.
- ☑ Conséquence : Faible traçabilité.

- ☑ Criticité : Élevé

### 6.5.3. *Domaine : Gestion des Clients et Fournisseurs*

#### 6.5.3.1. *Point de Contrôle : Création des profils clients*

- ☑ Objectif de Contrôle : Assurer que chaque profil client est complet.
- ☑ Critère d'Évaluation : Les informations de chaque client sont complètes et à jour.
- ☑ Question d'Évaluation : Les informations du profil client sont-elles complètes et à jour ?
- ☑ Document Requis : Formulaire de profil client.
- ☑ Risque : Données incomplètes sur les clients.
- ☑ Conséquence : Problèmes de suivi des transactions.
- ☑ Criticité : Moyen

#### 6.5.3.2. *Point de Contrôle : Création des profils fournisseurs*

- ☑ Objectif de Contrôle : Assurer que chaque profil fournisseur est complet.
- ☑ Critère d'Évaluation : Les informations de chaque fournisseur sont complètes et à jour.
- ☑ Question d'Évaluation : Les informations du profil fournisseur sont-elles complètes et à jour ?
- ☑ Document Requis : Formulaire de profil fournisseur.
- ☑ Risque : Données incomplètes sur les fournisseurs.
- ☑ Conséquence : Problèmes de suivi des transactions.
- ☑ Criticité : Moyen

#### 6.5.3.3. *Point de Contrôle : Suivi des soldes clients*

- ☑ Objectif de Contrôle : Assurer la mise à jour des soldes clients.
- ☑ Critère d'Évaluation : Les soldes clients sont mis à jour après chaque transaction.
- ☑ Question d'Évaluation : Les soldes clients sont-ils mis à jour après chaque transaction ?
- ☑ Document Requis : État des comptes clients.
- ☑ Risque : Informations obsolètes sur les soldes clients.
- ☑ Conséquence : Mauvais suivi des créances.
- ☑ Criticité : Élevé

#### 6.5.3.4. *Point de Contrôle : Suivi des soldes fournisseurs*

- ☑ Objectif de Contrôle : Assurer la mise à jour des soldes fournisseurs.
- ☑ Critère d'Évaluation : Les soldes fournisseurs sont mis à jour après chaque transaction.
- ☑ Question d'Évaluation : Les soldes fournisseurs sont-ils mis à jour après chaque transaction ?
- ☑ Document Requis : État des comptes fournisseurs.

- ☑ Risque : Informations obsolètes sur les soldes fournisseurs.
- ☑ Conséquence : Mauvais suivi des dettes.
- ☑ Criticité : Élevé

#### 6.5.4. *Domaine : Facturation et Gestion des Recettes*

##### 6.5.4.1. *Point de Contrôle : Création des factures*

- ☑ Objectif de Contrôle : Assurer que chaque facture est générée avec exactitude.
- ☑ Critère d'Évaluation : La facture est générée avec les bonnes informations (montant, client).
- ☑ Question d'Évaluation : La facture est-elle générée avec les bonnes informations ?
- ☑ Document Requis : Copie de la facture.
- ☑ Risque : Factures incorrectes.
- ☑ Conséquence : Difficulté de recouvrement.
- ☑ Criticité : Moyen

##### 6.5.4.2. *Point de Contrôle : Validation des factures*

- ☑ Objectif de Contrôle : Assurer que chaque facture est validée avant envoi.
- ☑ Critère d'Évaluation : La facture est validée par un responsable avant envoi.
- ☑ Question d'Évaluation : La facture a-t-elle été validée avant envoi ?
- ☑ Document Requis : Fiche de validation des factures.
- ☑ Risque : Envoi de factures non validées.
- ☑ Conséquence : Retards dans le recouvrement.
- ☑ Criticité : Moyen

##### 6.5.4.3. *Point de Contrôle : Enregistrement des paiements*

- ☑ Objectif de Contrôle : Assurer que chaque paiement est enregistré avec précision.
- ☑ Critère d'Évaluation : Chaque paiement est enregistré sans délai.
- ☑ Question d'Évaluation : Le paiement est-il enregistré sans délai ?
- ☑ Document Requis : Relevé de paiement.
- ☑ Risque : Retard dans l'enregistrement des paiements.
- ☑ Conséquence : Déséquilibres dans les comptes clients.
- ☑ Criticité : Élevé

#### 6.5.5. *Domaine : Suivi de la Trésorerie*

##### 6.5.5.1. *Point de Contrôle : Réalisation du rapprochement bancaire*

- ☑ Objectif de Contrôle : Vérifier que le rapprochement bancaire est effectué périodiquement.
- ☑ Critère d'Évaluation : Le rapprochement bancaire est réalisé chaque mois.
- ☑ Question d'Évaluation : Le rapprochement bancaire est-il effectué chaque mois ?

- ☑ Document Requis : Rapport de rapprochement bancaire mensuel.
- ☑ Risque : Écarts non détectés entre comptes bancaires et comptables.
- ☑ Conséquence : Informations financières inexactes.
- ☑ Criticité : Élevé

#### 6.5.5.2. *Point de Contrôle : Validation du rapprochement bancaire*

- ☑ Objectif de Contrôle : Assurer que le rapprochement bancaire est validé par un responsable.
- ☑ Critère d'Évaluation : Chaque rapprochement bancaire est validé par un responsable.
- ☑ Question d'Évaluation : Le rapprochement bancaire est-il validé par un responsable ?
- ☑ Document Requis : Signature d'approbation du rapprochement bancaire.
- ☑ Risque : Rapprochement bancaire non validé.
- ☑ Conséquence : Erreurs non corrigées.
- ☑ Criticité : Moyen

### 6.5.6. *Domaine : Gestion des Immobilisations*

#### 6.5.6.1. *Point de Contrôle : Enregistrement des immobilisations*

- ☑ Objectif de Contrôle : Assurer que chaque immobilisation est enregistrée dans le système avec un enregistrement complet.
- ☑ Critère d'Évaluation : Chaque immobilisation dispose d'une fiche complète indiquant son nom, sa date d'acquisition, sa valeur et sa durée de vie.
- ☑ Question d'Évaluation : L'immobilisation est-elle enregistrée avec toutes les informations requises ?
- ☑ Document Requis : Fiche d'immobilisation complète.
- ☑ Risque : Immobilisations mal enregistrées ou incomplètes.
- ☑ Conséquence : Mauvaise gestion des actifs et erreurs d'amortissement.
- ☑ Criticité : Moyen

#### 6.5.6.2. *Point de Contrôle : Calcul des amortissements*

- ☑ Objectif de Contrôle : Assurer l'exactitude des calculs d'amortissement pour chaque immobilisation.
- ☑ Critère d'Évaluation : Le calcul de l'amortissement est effectué selon la méthode approuvée (linéaire, dégressif).
- ☑ Question d'Évaluation : L'amortissement est-il calculé selon la méthode appropriée ?
- ☑ Document Requis : Rapport de calcul des amortissements.
- ☑ Risque : Mauvais calcul de l'amortissement.
- ☑ Conséquence : Valeurs d'actifs incorrectes et impacts financiers.
- ☑ Criticité : Élevé

#### 6.5.6.3. *Point de Contrôle : Validation des calculs d'amortissement*

- ☑ Objectif de Contrôle : Vérifier que les calculs d'amortissement sont validés par un responsable.
- ☑ Critère d'Évaluation : Les calculs d'amortissement sont vérifiés et approuvés par un responsable comptable.
- ☑ Question d'Évaluation : Les calculs d'amortissement sont-ils validés par un responsable ?
- ☑ Document Requis : Signature d'approbation des calculs d'amortissement.
- ☑ Risque : Calculs d'amortissement non validés.
- ☑ Conséquence : Erreurs dans les états financiers.
- ☑ Criticité : Élevé

#### 6.5.6.4. *Point de Contrôle : Mise à jour des fiches d'immobilisations*

- ☑ Objectif de Contrôle : Assurer que les fiches d'immobilisations sont mises à jour après chaque réévaluation ou cession.
- ☑ Critère d'Évaluation : Les fiches d'immobilisations sont actualisées suite à toute modification de valeur ou changement de statut.
- ☑ Question d'Évaluation : Les fiches d'immobilisations sont-elles mises à jour après chaque modification ?
- ☑ Document Requis : Fiche d'immobilisation mise à jour.
- ☑ Risque : Données obsolètes sur les immobilisations.
- ☑ Conséquence : Informations inexactes pour la gestion des actifs.
- ☑ Criticité : Moyen

### 6.5.7. *Domaine : États Financiers et Rapports Comptables*

#### 6.5.7.1. *Point de Contrôle : Production des états financiers*

- ☑ Objectif de Contrôle : Assurer la complétude et l'exactitude des états financiers.
- ☑ Critère d'Évaluation : Les états financiers incluent toutes les données nécessaires et sont produits sans omission.
- ☑ Question d'Évaluation : Les états financiers sont-ils complets et sans omission ?
- ☑ Document Requis : États financiers approuvés.
- ☑ Risque : Production d'états incomplets.
- ☑ Conséquence : Prises de décision sur des informations incomplètes.
- ☑ Criticité : Élevé

#### 6.5.7.2. *Point de Contrôle : Vérification de la conformité des états financiers*

- ☑ Objectif de Contrôle : Assurer la conformité des états financiers aux normes comptables en vigueur.
- ☑ Critère d'Évaluation : Les états financiers sont conformes aux normes comptables (ex. : IFRS, GAAP).

- ☑ Question d'Évaluation : Les états financiers sont-ils conformes aux normes comptables en vigueur ?
- ☑ Document Requis : Rapport de conformité aux normes comptables.
- ☑ Risque : États financiers non conformes aux normes.
- ☑ Conséquence : Risque de sanctions réglementaires.
- ☑ Criticité : Élevé

#### 6.5.8. Conformité et Clôture de Fin d'Année

##### 6.5.8.1. Point de Contrôle : Écritures de clôture

- ☑ Objectif de Contrôle : Assurer que les écritures de clôture sont passées correctement.
- ☑ Critère d'Évaluation : Toutes les écritures de clôture sont enregistrées avant la fin de l'exercice.
- ☑ Question d'Évaluation : Les écritures de clôture sont-elles passées avant la fin de l'exercice ?
- ☑ Document Requis : Journal des écritures de clôture.
- ☑ Risque : Écritures de clôture non enregistrées.
- ☑ Conséquence : Comptes incomplets en fin d'exercice.
- ☑ Criticité : Élevé

##### 6.5.8.2. Point de Contrôle : Vérification des régularisations

- ☑ Objectif de Contrôle : Assurer l'exactitude des écritures de régularisation.
- ☑ Critère d'Évaluation : Les écritures de régularisation sont calculées et saisies avec précision.
- ☑ Question d'Évaluation : Les écritures de régularisation sont-elles exactes et complètes ?
- ☑ Document Requis : Journal des écritures de régularisation.
- ☑ Risque : Écritures de régularisation incorrectes.
- ☑ Conséquence : Résultats financiers faussés.
- ☑ Criticité : Élevé

##### 6.5.8.3. Point de Contrôle : Archivage des documents de clôture

- ☑ Objectif de Contrôle : Assurer l'archivage des documents comptables pour la conformité.
- ☑ Critère d'Évaluation : Tous les documents de clôture sont archivés de manière sécurisée.
- ☑ Question d'Évaluation : Les documents de clôture sont-ils archivés conformément aux normes ?
- ☑ Document Requis : Archives des documents de clôture.
- ☑ Risque : Manque de traçabilité des documents financiers.
- ☑ Conséquence : Difficulté de contrôle et de vérification.
- ☑ Criticité : Moyen



## 6.6. Conception de l'outil pour l'audit des aspects informatiques de l'application APPLICATION.

Voir Section 4.1 Audit des Applications en Service

## 6.7. Liste des outils et logiciels recommandés.

### 6.7.1. Analyse de la Performance de l'Application

#### 6.7.1.1. APM (Application Performance Management) Outils :

- ☑ **Dynatrace** : Offre une analyse approfondie de la performance de bout en bout, avec des fonctionnalités pour le suivi des transactions, des applications, des infrastructures et des réseaux.
- ☑ **New Relic** : Un autre outil d'APM populaire qui fournit des informations en temps réel sur les performances des applications et l'expérience utilisateur.
- ☑ **AppDynamics** : Suivi des transactions et de la performance pour identifier les goulots d'étranglement au niveau des applications, de la base de données et du réseau.

#### 6.7.1.2. Profiling Outils :

- ☑ **JProfiler ou VisualVM** (pour les applications Java) : Permettent de visualiser l'utilisation des ressources (CPU, mémoire) et d'identifier les problèmes de performance.
- ☑ **dotTrace** (pour les applications .NET) : Un outil de profilage pour identifier les goulots d'étranglement dans le code .NET.

#### 6.7.1.3. Outils de Test de Charge :

- ☑ **JMeter** : Open-source, utilisé pour tester la charge et simuler plusieurs utilisateurs pour évaluer la capacité de réponse et la robustesse de l'application.
- ☑ **LoadRunner** : Solution commerciale pour des tests de charge à grande échelle.
- ☑ **Gatling** : Un autre outil open-source, connu pour ses performances dans les tests de charge et de stress.

### 6.7.2. Analyse de la Sécurité de l'Application

#### 6.7.2.1. Outils de Scanning de Vulnérabilités :

- ☑ **OWASP ZAP (Zed Attack Proxy)** : Un scanner open-source pour tester la sécurité des applications web. Très utile pour identifier les vulnérabilités courantes telles que l'injection SQL, les failles XSS, etc.
- ☑ **Burp Suite** : Un autre outil très utilisé pour l'audit des applications web, offrant une gamme d'outils de détection de vulnérabilités et de tests de pénétration.
- ☑ **Nessus** : Scanner de vulnérabilités réseau, utile pour identifier les failles de sécurité non seulement au niveau de l'application mais aussi de l'infrastructure.  
Tenable.com



#### 6.7.3. Analyse Statique et Dynamique de Code (SAST et DAST) :

- ☑ **SonarQube** : Utile pour l'analyse statique de code, détectant les vulnérabilités dans le code source avant le déploiement.
- ☑ **Checkmarx** : Permet une analyse de sécurité des applications avec une détection des vulnérabilités à partir du code source.
- ☑ **Veracode** : Fournit des analyses statiques et dynamiques pour détecter les failles de sécurité dans les applications en production.

#### 6.7.4. Monitoring et Détection d'Intrusions :

- ☑ **OSSEC** : Un système de détection d'intrusions open-source, qui peut être utile pour surveiller les logs d'application et détecter les comportements suspects.
- ☑ **Splunk ou ELK Stack (Elasticsearch, Logstash, Kibana)** : Permettent de centraliser les logs de l'application, identifier les tentatives d'intrusion, et suivre les incidents de sécurité.
- ☑ **Splunk** : Permet de centraliser les logs, détecter les incidents de sécurité, et effectuer une analyse en temps réel. Solution payante avec un essai gratuit.
- ☑ **ELK Stack (Elasticsearch, Logstash, Kibana)** : Un ensemble d'outils open-source pour centraliser, rechercher, et analyser les logs de l'application et des systèmes, très utile pour le monitoring et la sécurité.

#### 6.7.5. Autres Outils Recommandés pour la Sécurité et la Performance

- ☑ **Aqua Security** : Spécialisé dans la sécurité des conteneurs et des environnements cloud, Aqua Security fournit une suite d'outils pour protéger les applications basées sur Docker et Kubernetes.
- ☑ **Snyk** : Solution pour la sécurité des dépendances et des bibliothèques open-source, elle aide à gérer les vulnérabilités dans le code tiers.
- ☑ **Prometheus & Grafana** : Une combinaison open-source pour le monitoring et la visualisation des métriques, idéale pour surveiller les applications distribuées et les conteneurs.



## Livre VII: LABORATOIRES D'AUDIT DES SI

### **Objectif :**

Immerger les apprenants dans les différentes pratiques de l'audit des systèmes d'information.

### **Objectif d'apprentissage :**

A la fin de ce livre, chaque apprenant doit être à mesure d'affronter sereinement les différents examens (CC et SN).

## 7) LABORATOIRES D'AUDIT DES SYSTEMES D'INFORMATION

### 7.1. Audit d'une application en service

#### 7.1.1. Objectif

Ce laboratoire a pour objectif d'initier les apprenants à l'audit pratique d'une application en service fonctionnant sur un serveur installé dans une DMZ (zone démilitarisée) d'un réseau local. L'application, nommée **APPLICATION**, est accessible depuis l'extérieur de l'organisation ainsi que depuis les postes de travail internes. Les apprenants devront identifier les vulnérabilités potentielles, évaluer les mesures de sécurité existantes et formuler des recommandations pour renforcer la sécurité de l'application.

#### 7.1.2. Énoncé du Cas :

L'organisation Lizbiz's souhaite réaliser un audit de sécurité et de performance de **APPLICATION**, une application critique de gestion des commandes et des stocks. L'application est utilisée par les clients pour passer des commandes et par les employés pour gérer les stocks en interne.

Les préoccupations principales de l'organisation sont :

- ☒ La sécurité des données transmises et stockées.
- ☒ L'accès non autorisé potentiel depuis l'extérieur.
- ☒ La gestion des droits d'accès des utilisateurs internes.
- ☒ La robustesse de l'infrastructure hébergeant APPLICATION.
- ☒ L'intégrité et la confidentialité des données stockées dans la base de données.

#### 7.1.3. Étapes du Lab :

##### 7.1.3.1. Préparation du Lab

- ☒ Mettre en place un environnement de test simulant le serveur hébergeant APPLICATION dans une DMZ.
- ☒ Configurer un pare-feu pour permettre les connexions HTTP/HTTPS externes et les connexions SSH internes.
- ☒ Simuler des utilisateurs externes (clients) et internes (employés) avec des postes de travail configurés.

##### 7.1.3.2. Tâches Techniques

- ☒ **Création de l'outil d'aide à l'audit** : identifier la structure (point de contrôles, objectif de contrôle, critère d'évaluation, question d'évaluation, etc), et créer sur cette base un outil d'aide à l'audit sur mesure pour cette application en service.
- ☒ **Accès réseau** : Identifier les ports ouverts et les protocoles utilisés (Nmap, Netstat).

- ☑ **Tests de sécurité Web** : Utiliser un outil comme OWASP ZAP ou Burp Suite pour détecter les vulnérabilités de l'application (ex. injections SQL, failles XSS, etc.).
- ☑ **Audit des logs** : Examiner les fichiers de logs (Apache/Nginx, MySQL) pour identifier les tentatives d'accès suspectes.
- ☑ **Gestion des droits d'accès** : Vérifier les politiques de gestion des droits des utilisateurs dans l'application.
- ☑ **Chiffrement des données** : Valider que les communications HTTPS sont correctement configurées et sécurisées (certificat SSL/TLS valide).
- ☑ **Extraction et analyse des données de la base de données** :
  - Identifier les tables principales de la base de données.
  - Extraire un échantillon de données pour analyser leur intégrité, leur cohérence et leur confidentialité.
  - Vérifier les permissions des utilisateurs sur la base de données (ex. comptes admin inutilisés, mots de passe par défaut).
  - Détecter d'éventuelles failles de sécurité comme les données en clair ou les colonnes non protégées.
- ☑ **Analyse des sauvegardes** : Vérifier l'existence, la régularité et la qualité des sauvegardes de la base de données.
- ☑ **Simulation d'attaque SQL** : Tester les vulnérabilités potentielles aux injections SQL sur les champs d'entrée utilisateur.

#### 7.1.3.3. *Analyse des Résultats*

- ☑ Identifier les vulnérabilités critiques dans **APPLICATION** (ex. mots de passe faibles, ports inutiles exposés, failles SQL).
- ☑ Évaluer la conformité aux bonnes pratiques de sécurité (ISO 27001, OWASP Top 10).
- ☑ Proposer des solutions pour corriger les vulnérabilités identifiées, notamment pour la base de données.

#### 7.1.4. *Livrables* :

Chaque groupe devra produire :

- ☑ Rapport technique détaillé :
  - Description des vulnérabilités identifiées.
  - Analyse des logs et des configurations réseau.
  - Résultats de l'extraction et de l'analyse des données.
  - Recommandations pour chaque problème détecté.

- ☒ Présentation PowerPoint : Résumé des constats majeurs et des recommandations.

#### 7.1.5. Calendrier :

Tableau 9: calendrier d'exécution de la mission

N°	Activités	Livrables	Semaines
1	Préparation et collecte des informations : périmètre, configuration, logs, documentation.	Plan d'audit, liste des éléments collectés.	3 jours
2	Tests techniques (réseau, application, base de données) et analyse des résultats.	Rapport intermédiaire, liste des vulnérabilités.	10 jours
3	Validation contradictoire, rédaction du rapport final et recommandations.	Rapport final, plan d'action, présentation.	3 jours

## 7.2. Audit de sécurité d'une infrastructure

### 7.2.1. Objectifs

Ce laboratoire vise à initier les apprenants à l'audit de sécurité d'une infrastructure réseau comprenant une **DMZ**, un sous-réseau pour les postes clients, un sous-réseau de serveurs internes, un **firewall**, un **routeur frontal**, un **switch manageable** et un site web hébergé dans la DMZ. Les apprenants doivent identifier les vulnérabilités potentielles, évaluer les configurations réseau et systèmes, et proposer des recommandations pour renforcer la sécurité globale de l'infrastructure.

### 7.2.2. Énoncé du Cas :

Lizbiz's souhaite réaliser un audit de sécurité complet de son infrastructure réseau pour :

- ☒ Identifier les vulnérabilités dans la configuration des équipements (routeur, firewall, switch).
- ☒ Évaluer la sécurité des flux réseau entre la DMZ, les postes clients et les serveurs internes.
- ☒ Vérifier la protection et l'exposition des services hébergés, notamment le site web dans la DMZ.
- ☒ Analyser la segmentation réseau et les règles d'accès appliquées.
- ☒ Formuler des recommandations pour améliorer la sécurité globale de l'infrastructure.

### 7.2.3. Description de l'infrastructure :

- ☒ **Routeur frontal :**
  - Connecte l'infrastructure au WAN (Internet).
  - Configure la redirection des ports pour le trafic web vers la DMZ.
- ☒ **Firewall :**
  - Sépare la DMZ, le sous-réseau des postes clients, et le sous-réseau des serveurs.
  - Applique des règles d'accès strictes entre les différents segments du réseau.
- ☒ **Switch manageable :**
  - Gère la segmentation VLAN entre les différents sous-réseaux.
- ☒ **DMZ :**
  - Contient un serveur web (HTTP/HTTPS) exposé à Internet.
  - Séparée du réseau interne par le firewall.
- ☒ **Sous-réseau des postes clients :**

- Permet aux utilisateurs internes d'accéder aux ressources internes et externes.

☒ **Sous-réseau des serveurs internes :**

- Héberge les services sensibles non accessibles directement depuis l'extérieur (base de données, sauvegardes, etc.).

#### 7.2.4. Phases du Lab :

##### 7.2.4.1. Préparation du Lab

Mettre en place un environnement simulé avec :

- ☒ Un routeur virtuel configuré pour gérer le trafic entrant et sortant.
- ☒ Un firewall avec des règles préconfigurées pour contrôler l'accès entre les sous-réseaux.
- ☒ Un switch manageable configuré pour gérer les VLAN des sous-réseaux.
- ☒ Une machine virtuelle hébergeant un site web vulnérable dans la DMZ.
- ☒ Deux sous-réseaux distincts (clients et serveurs internes).

##### 7.2.4.2. Tâches Techniques

Les apprenants effectueront les tâches suivantes :

☒ **Cartographie de l'infrastructure :**

- Identifier tous les équipements, leurs adresses IP et les segments de réseau associés à l'aide de **Nmap**.
- Visualiser la topologie réseau.

☒ **Analyse des configurations du routeur :**

- Vérifier les paramètres NAT et de redirection de ports.
- Identifier les services ouverts (telnet, SSH) exposés à Internet.

☒ **Audit du firewall :**

- Analyser les règles d'accès entre la DMZ, les postes clients et les serveurs internes.
- Vérifier les politiques de logs et leur activation pour surveiller les tentatives d'accès non autorisées.

☒ **Analyse du switch manageable :**

- Identifier les VLAN configurés.
- Vérifier les règles de segmentation et les accès inter-VLAN.

☒ **Audit de la DMZ :**

- Tester les vulnérabilités du site web hébergé dans la DMZ à l'aide d'**OWASP ZAP** ou **Burp Suite**.

- Simuler des attaques potentielles sur le serveur web (injections SQL, XSS, etc.).

☑ **Analyse des flux réseau :**

- Capturer et analyser le trafic réseau entre la DMZ, les postes clients et les serveurs internes avec **Wireshark**.
- Identifier les éventuelles transmissions non chiffrées.

☑ **Examen des politiques d'accès utilisateurs :**

- Vérifier les règles de gestion des mots de passe et les politiques de permissions.
- Auditer les comptes administrateurs actifs sur le routeur, le firewall et les serveurs internes.

☑ **Validation des sauvegardes :**

- Vérifier la configuration des sauvegardes automatiques pour le serveur web et les équipements réseau.

☑ **Simulation d'attaque brute force :**

- Tester la résistance des équipements (routeur, firewall) à une attaque brute force.

☑ **Analyse des journaux (logs) :**

- Examiner les logs générés par le firewall, le serveur web et le routeur pour détecter les anomalies.

7.2.4.3. *Livrables :*

☑ **Rapport technique détaillé :**

- Cartographie complète de l'infrastructure.
- Liste des vulnérabilités identifiées (équipements, règles, services).
- Analyse des configurations réseau et des flux capturés.
- Recommandations pratiques pour corriger les failles.

☑ **Présentation PowerPoint :**

- Synthèse des résultats avec focus sur les vulnérabilités critiques et recommandations prioritaires.

7.2.4.4. *Outils Recommandés :*

- ☑ **Nmap** : Analyse des ports et services ouverts.
- ☑ **OWASP ZAP / Burp Suite** : Tests de sécurité applicative.
- ☑ **Wireshark** : Capture et analyse des paquets réseau.



- ☑ **RouterSploit** : Test des vulnérabilités des équipements réseau.
- ☑ **SQLMap** : Test des injections SQL sur le site web.
- ☑ **Firewall Analyzer** : Analyse et audit des règles de firewall.

### 7.2.5. Calendrier :

Tableau 10: calendrier d'exécution de la mission

N°	Activités	Livrables	Semaines
1	Préparation et collecte des informations : périmètre, configuration, logs, documentation.	Plan d'audit, liste des éléments collectés.	3 jours
2	Tests techniques (réseau, application, base de données) et analyse des résultats.	Rapport intermédiaire, liste des vulnérabilités.	10 jours
3	Validation contradictoire, rédaction du rapport final et recommandations.	Rapport final, plan d'action, présentation.	3 jours



## Livre VIII:

# SUJETS TYPES EXAMENS

### **Objectif :**

Immerger les apprenants dans le type de question qu'ils auront à l'examen

### **Objectif d'apprentissage :**

A la fin de ce livre, chaque apprenant doit être à mesure d'affronter sereinement les différents examens (CC et SN).

# SUJETS TYPES EXAMENS

## I. QCM

1- Laquelle des fonctions suivantes fait partie de celles de l'auditeur ?

- A. Police
- B. Conseil
- C. Sanction
- D. Communication

2- Laquelle, des séquences suivantes, décrit le mieux une mission d'audit ?

- A. Procédés préliminaires, planification, exécution, communication des résultats, suivi des recommandations
- B. Planification, exécution, communication des résultats
- C. Planification, suivi des recommandations, exécution, communication des résultats
- D. Exécution, communication des résultats, planification

3- Lequel des procédés de vérification suivants est indispensables dès qu'il est question de valeurs numériques ?

- A. Corroboration
- B. Réexécution
- C. Observation
- D. Interview
- E. Aucun

4- Si l'on considère que l'auditeur a une bonne connaissance de l'entité auditée, lequel des éléments suivants est critique pour la bonne exécution d'une mission ?

- A. La compétence
- B. La maîtrise et le respect des procédures
- C. La connaissance des logiciels spécialisés
- D. La connaissance de l'entité à auditer

5- Parmi les éléments suivants, lequel est indispensable pour parler de système d'information au service de la comptabilité ?

- A. Le serveur du service de la comptabilité

- B. Le Chef service de la comptabilité
- C. Les procédures comptables
- D. Les registres du service de la comptabilité

6- Parmi les éléments suivants, lequel ne fait pas partie du mandat d'une mission d'audit en milieu informatisé ?

- A. La désignation claire et nette de l'entité objet du contrôle
- B. La période de contrôle (exercice couverts)
- C. La liste des responsables informatiques
- D. Des consignes particulières

## II. Connaissance du Cours

1. Définir les termes et expressions suivantes :
  - ☒ Audit ;
  - ☒ Système d'Information ;
  - ☒ Risque ;
  - ☒ Contradictoire ;
  - ☒ Système de contrôle interne ;
2. Enoncer les principes et ou concepts suivants présentés durant le cours :
  - ☒ Règles des 4 yeux ;
  - ☒ Allégorie des 2 mains ;
  - ☒ Contrôle réciproque des tâches ;
  - ☒ Séparation des tâches et fonctions incompatibles ;
  - ☒ Spécification des tâches ;
3. Lister les principales phases d'une mission d'audit des systèmes d'information, en précisant à chaque fois les documents en entrée de phase (input) et les documents produits à l'issue de la phase (output).
4. Si elles existent, quelles sont les différences entre l'audit et le contrôle.
5. Lister les principaux types d'audit des systèmes d'information.
6. Quel est l'organe régalien de l'Etat en matière d'audit de sécurité ?
7. Lister trois (3) normes usuelles en audit des SI, en précisant leurs champs d'application respectifs.
8. Lister les principales phases d'une mission d'audit des systèmes d'information, en précisant à chaque fois les documents en entrée de phase (input) et les documents produits à l'issue de la phase (output).
9. Si elles existent, quelles sont les différences entre l'audit et le contrôle.
10. Lister en donnant leurs différences les principaux types d'audit des systèmes d'information.
11. Quel est l'organe régalien de l'Etat en matière d'audit de sécurité ?
12. Lister quatre (4) normes usuelles en audit des SI, en précisant leurs champs d'application respectifs.
13. Qu'est-ce que le contradictoire dans un audit, à quelle phase d'un audit intervient-il ? donnez un exemple de formulation de contradictoire.
14. Après en avoir rappelé les constituantes, formulez une observation complète d'audit dans le cadre d'une constatation positive.
15. Après avoir rappelé 5 types d'audits les plus courants dans les systèmes d'information, choisissez-en un pour lequel vous décrirez.

### III. Questions V/F

Répondez par V ou F

Tableau 11: Questions Vrai/Faux

N°	Libellé	V/F
A	La mise en place d'un système de contrôle interne n'est pas de la responsabilité du top management	
B	Il existe plus de 3 types de risques	
C	Seuls les informaticiens peuvent faire de l'audit des systèmes d'information	
D	L'extraction des données est de la responsabilité exclusive de l'informaticien de l'équipe de mission	
E	L'avènement de l'informatique impacte le métier d'auditeur	
F	L'audit et la détection de la fraude sont exactement les mêmes disciplines	
G	SQL signifie: Structured Query Language	
H	Le SGBD est le nom d'un système d'exploitation qui permet d'interroger les bases de données relationnelles	
I	Le rapport de l'ANTIC fait foi en matière d'audit de sécurité des Systèmes Informatiques au Cameroun	
J	Un auditeur expérimenté n'a pas besoin de lire les normes spécifiques à une entité avant de l'auditer	
K	Le risque de Mission et le Risque de contrôle sont similaires	
L	Tout système peut être représenté par : entrées/traitements/sorties	
M	Il existe seulement 4 méthodes de traitement du risque	
N	La conversion de système est un moyen d'installer un système d'exploitation	
O	Le rapport d'études préalables est produit à la fin de la mission de contrôle	

## IV. Cas Pratiques

### IV.1. *Sujet 1*

#### **Contexte :**

Après avoir brillamment achevé vos études au PSSFP, vous êtes portés à la tête d'une brigade de contrôle dont le niveau administratif correspond à une sous-direction. Vous devez constituer une équipe d'auditeurs pour faire la lumière sur un cas de dénonciation issue d'un service de votre administration qui est en contact permanent avec des usagers. Ce service possède une application dédiée au traitement de ses données financières.

#### **Questions :**

1. Après l'avoir clairement identifié, reformulez le problème principal de ce libellé
2. Quels sont les trois profils fondamentaux qu'il faudrait dans votre équipe de mission pour résoudre le problème identifié à la question A, justifiez chaque réponse.
3. Quels sont les procédés d'audit que vous comptez employer, justifiez chaque réponse.
4. Une équipe de missions, réalisant un audit en milieu informatisé auprès d'une entité, qui constate une violation en cours et flagrante de la loi sur la cybersécurité et la cybercriminalité de 2010 en vigueur au Cameroun, doit entreprendre quelle action immédiate, si cette violation n'entre pas dans son mandat ?

Page 214 sur 227



### IV.2. *Sujet 2*

#### **Contexte :**

Dans le cadre l'exécution des Très Hautes Instructions du Chef de l'Etat, une brigade de contrôle de vérificateurs des services Contrôle Supérieur de l'Etat, séjourne actuellement dans votre structure.

Le chef de mission a servi des demandes de renseignements relatives aux frais de mission pour la période allant de 2011 à 2022, sollicitant entre autres les éléments suivants :

- ☒ Lettre de mission ;
- ☒ Ordre de mission ;
- ☒ Rapport de mission ;

En votre qualité d'expert en finances publiques, option audit et contrôle, le chef de la structure vous confie la rédaction d'un draft de réponse devant servir de base pour tous vos collègues.

En vous appuyant sur l'ensemble de votre cursus au PSSFP, de votre expérience personnel, et de votre culture en matière de textes législatifs et réglementaires en matière de finances publiques, notamment les régimes financier de l'Etat, répondez aux questions suivantes :

### Questions :

5. le mandat de l'équipe de mission est-il légal, au sens strict, c'est-à-dire, respecte-t-il la réglementation en vigueur ? Justifiez votre réponse
6. quelle est la durée de conservation légale des archives numériques
7. classez les éléments requis par l'équipe de mission, suivant leur émetteur, et destinataire final
8. l'équipe a extrait et agrégé par montant total et par personne les frais de mission payés sur la période. Le chef de division informatique de votre structure qui a mis la base de données à sa disposition, pouvait-il faire autrement ? Justifiez votre réponse
9. quel procédé d'audit recommandez-vous à chacun de vos collègues concernant les données agrégées sur sa demande de renseignement ? Justifiez votre réponse
10. la demande formulée par votre hiérarchie, est-elle légale, en d'autres termes y a-t-il quelque chose de répréhensible à se faire aider pour répondre à une demande de renseignements reçue d'une brigade de contrôle de services du Contrôle Supérieur de l'Etat ? Justifiez votre réponse
11. répondez à la sollicitation de votre hiérarchie en proposant un draft de pas plus de 300 mots, qui servira de base de réponse à chacun de vos collègues

### IV.3. Sujet 3

#### Contexte :

Vous êtes Chef de Mission d'une équipe de mission d'audit des SI déployée dans une Entreprise d'Etat afin d'en connaître du fonctionnement de ses applications liées processus de facturation. Votre équipe est constituée de 4 membres. La période sous revue couvre deux (2) exercices budgétaires.

#### Questions

1. Quel est le document qui matérialise le mandat donné à votre équipe de mission pour se déployer ? Justifiez votre réponse.
2. Faire une proposition de profils pour les 4 membres de l'équipe en rapport avec le sujet d'audit, justifier chaque profil.
3. Dans quelle phase situez-vous la conception des outils d'aide à l'audit ?
4. Précisez le type d'audit que vous serez amenés à réaliser avec votre équipe.
5. Pour ce type d'audit en particulier, classez les compétences d'auditeur ci-contre par ordre de priorité :
  - a. Compréhension des codes sources des applications utilisées ;
  - b. Fluidité dans l'utilisation de Microsoft Excel ;
  - c. Ingénierie des processus ;
  - d. Bonne connaissance de l'entité ;
  - e. Bonnes aptitudes rédactionnelles ;



f. Qualité interpersonnelle.

6. Lorsque vous saisissez les parties prenantes pour solliciter des compléments d'information sur des faits que vous avez relevés, dans laquelle des phases de la mission vous situez-vous ?

#### IV.4. Sujet 4

##### **Contexte :**

Vous recevez mandat pour faire la lumière sur la véracité de certaines informations qui circulent dans une salle de classe diffusées au travers de groupes WhatsApp, du bouche à oreille et message direct d'un utilisateur à un autre.

##### **Questions**

1. Définir système d'information en prenant soin de souligner au stylo à bille, dans votre proposition de définition les éléments indispensables pour la validité de ladite définition.
2. Définir audit des systèmes d'information en prenant soin de souligner au stylo à bille, dans votre proposition de définition les éléments indispensables pour la validité de ladite définition.
3. Cette mission peut-elle être assimilée à un audit des systèmes d'information? Si oui elle rentrerait dans quel type d'audit des systèmes d'information ?
4. Dans la suite de votre réponse donnée à la question 3, allez-vous accepter la mission, justifiez votre réponse.
5. dans la perspective de la réalisation de ladite mission, c'est-à-dire, en supposant qu'il s'agisse d'une mission d'audit des systèmes d'information, citez 4 compétences requises pour mener à bien votre mandat, justifiez chacune des compétences.

#### IV.5. Sujet 5

##### **Contexte :**

Vous êtes placés en situation d'audit interne, dans l'exécution d'une mission pour laquelle vous n'avez pas participé aux phases antérieures. Votre chef de mission, vous assigne les rôles suivants :

- ☒ extraction des données ;
- ☒ analyse des données ;
- ☒ préparation des entretiens ;
- ☒ rédaction et acheminement du rapport au commanditaire ;
- ☒ validation du plan d'audit.

##### **Questions**

1. Après avoir brillamment suivi votre cours d'audit des systèmes d'information en HN3, quelle est l'impression majeure qui se dégage de l'examen de ces tâches ? justifiez votre réponse pour chacun des 5 éléments.
2. Que devez-vous faire face à cette situation ? Argumentez.

## V. Questions ouvertes

1. En 300 mots maximum, résumez le cours d'Audit et Contrôle des Systèmes d'Information.
2. En 500 mots maximum, relevez les éléments du cours que vous avez retenus mais qui ne sont pas posés comme question dans cette épreuve.
3. Dans Microsoft Excel, quelle est l'utilité de la fonction NB.SI pour la réalisation d'un outil d'aide à l'audit ?
4. Quelle est l'utilité ou la raison de la certification des auditeurs en général et ceux des SI en particulier ?
5. Quelles sont les deux (2) certifications majeures en audit ?



## Livre VIII: ANNEXES

## ANNEXES

### Modèle d'observation

Dans certains types de rapport de mission, notamment ceux d'ISC comme le Contrôle Supérieur de l'Etat, c'est la forme arrêtée pour consigner les travaux d'audit. Une observation se compose de :

- ☒ Un numéro d'ordre ;
- ☒ La désignation de l'irrégularité ;
- ☒ L'énoncé de la norme visée ;
- ☒ La constatation d'audit ;
- ☒ Les risques ou conséquences du fait observé ;
- ☒ Le contradictoire ;
- ☒ L'analyse de l'auditeur ;
- ☒ La conclusion sur le fait observé ;
- ☒ La ou les recommandations pour contenir, réparer ou éviter à l'avenir la situation observée.

**1. Un numéro d'ordre :**

N°01

**2. La désignation de l'irrégularité :**

Cumul des fonctions réputées incompatibles, d'administrateurs réseau et de base de données.

**3. L'énoncé de la norme visée :**

Le second pilier de l'audit interne qui grave la séparation des tâches et fonctions incompatibles dans le marbre, repris et surligné par le point 10.3.2 d'ISO 27002, interdisent le cumul des fonctions d'administrateur de base de données et celui d'administrateur réseau.

**4. La constatation d'audit :**

**Monsieur NKUS** a régulièrement exercé les deux fonctions d'administrateur réseau et de base de données pendant toute la période sous revue.

**5. Les risques ou conséquences du fait observé:**

Cette situation lui confère la possibilité d'un accès complet au système, sans aucun contrôle externe.

**6. Le contradictoire :**

Interrogé sur cet état des choses, le sieur NKUS a répondu que : « à ma nomination à ce poste, j'ai trouvé que mon profil avait déjà ces droits. Ce n'est donc pas de mon fait. »

## **7. Cas1 : Le sieur NKUS dit la vérité :**

### **7.1. L'analyse de l'auditeur :**

Bien que le sieur NKUS ait raison quant au fait que son profil possédait déjà ces droits à son arrivée au poste, il n'en demeure pas moins que cette pratique est repréhensible et contraire aux bons usages, et que les risques mentionnés supra restent constants. Par ailleurs, un contrôle des droits d'accès avec mise à jour de la matrice des droits d'accès aurait permis d'identifier rapidement cet état de chose et de proposer les corrections nécessaires pour le retour à l'orthodoxie.

### **7.2. La conclusion sur le fait observé :**

En définitive, le sieur NKUS aurait pu/du relever dès qu'il en a eu connaissance ce dysfonctionnement pour qu'il soit corrigé. En ne le faisant pas, il a participé à prolongé cet état des chose, s'en rendant donc complice de fait.

## **8. Cas2 : Le sieur NKUS ne dit pas la vérité :**

### **8.1. L'analyse de l'auditeur :**

L'exploitation des journaux d'événements systèmes à la fois des équipements réseaux, mais aussi de la base de données, laisse observer qu'aucun des prédécesseurs de Monsieur NKUS ne cumulait les droits d'administrateur réseau et de base donnée. PJ N°xxx, xxx et xxx (extraction des fichier journaux).

Il est donc évident que Monsieur NKUS a menti à l'équipe de mission car le cumul de ces droits est bien limité uniquement à son magistère. Par ailleurs, une analyse poussée des fichiers journaux, PJ N°xxx, démontre que c'est bien l'utilisateur NKUS de mot de passe xxxx, qui s'est lui-même attribué lesdits droits d'administration et date xxxx, achevant ainsi de démontrer la mauvaise fois dans la réponse du sieur NKUS.

### **8.2. La conclusion sur le fait observé :**

L'équipe retient donc, non seulement, la responsabilité de Monsieur NKUS dans l'usage du cumul des droits d'administration, mais aussi comme étant celui qui a intentionnellement créer cette situation.

## **9. La ou les recommandations pour contenir, réparer ou éviter à l'avenir la situation observée :**

L'équipe recommande donc :

- ☒ Que les droits d'administrateur réseau lui soient retirés, puisque sa fonction est celle d'administrateur de base de données ;
- ☒ Qu'une matrice des droits d'accès soit créer, si elle n'existe pas ; et mise à jour dans le cas contraire.
- ☒ Que des vérification pour identifier des cas similaires soient faites à l'échelle de tous les administrateurs ;

- ☒ Qu'une analyse approfondie des actions réalisées par le sieur NKUS, dans le système, soit menée pour vérifier qu'il n'a pas usé de cet avantage pour la commission d'actes répréhensibles.

## GLOSSAIRE

### A

- ☑ **Audit** : Processus d'examen systématique pour évaluer si les systèmes ou pratiques respectent les normes établies.
- ☑ **Authentification** : Méthode permettant de vérifier l'identité d'un utilisateur ou d'un système.
- ☑ **Anomalie** : Écart ou irrégularité détectée dans un système ou un processus.

### B

- ☑ **Backup (Sauvegarde)** : Copie des données pour les protéger contre une perte ou un incident.
- ☑ **Batch** : Séquence de traitement automatique, également appelée « traitement par lots », généralement réalisée en temps différé.
- ☑ **Big Data** : Ensemble volumineux de données complexes, souvent analysées pour en tirer des informations utiles.
- ☑ **Bonnes pratiques** : Recommandations et méthodologies reconnues pour améliorer la qualité et l'efficacité d'un processus.

### C

- ☑ **Cloud Computing** : Utilisation de services informatiques (stockage, logiciels, etc.) via Internet, au lieu de ressources locales.
- ☑ **Confidentialité** : Principe qui garantit que seules les personnes autorisées ont accès à certaines informations.
- ☑ **Cryptographie** : Science qui consiste à sécuriser les informations en les transformant pour les rendre illisibles sans clé.

### D

- ☑ **DLP (Data Loss Prevention)** : Outils ou politiques visant à empêcher la perte ou le vol de données sensibles.
- ☑ **DSI (Direction des Systèmes d'Information)** : Département chargé de la gestion et de l'optimisation des systèmes d'information d'une organisation.

### E

- ☑ **Examen de conformité** : Vérification de l'adhésion à des lois, règlements ou politiques internes.
- ☑ **ERP (Enterprise Resource Planning)** : Logiciel intégré qui gère les ressources et processus d'une organisation.

### G

- ☑ **Gouvernance informatique** : Ensemble de pratiques pour s'assurer que les systèmes informatiques soutiennent les objectifs de l'organisation.
- ☑ **Gouvernance du SI** : La « Gouvernance des Systèmes d'Information » ou « Gouvernance informatique » désigne le dispositif mis en place par une organisation pour contrôler et réguler son SI. À ce titre, la gouvernance du SI fait partie intégrante de la gouvernance de l'organisation et consiste d'abord à fixer au SI des objectifs découlant de la stratégie de l'organisation.

- ☑ **GDPR (General Data Protection Regulation)** : Règlement européen sur la protection des données personnelles.

## I

- ☑ **Informatique en Nuage ou Cloud Computing** : L'informatique en nuage est une technologie qui consiste à s'appuyer sur les capacités des réseaux pour mettre à la disposition des utilisateurs finaux un service, fourni par des logiciels et une infrastructure informatique souvent distants.

## L

- ☑ **Logs** : Enregistrements des événements ou activités sur un système pour une analyse ultérieure.

## M

- ☑ **Maîtrise d'œuvre (MOE)** : Entité ou personne chargée de la réalisation technique d'un projet, en respectant les besoins exprimés par la maîtrise d'ouvrage.
- ☑ **Maîtrise d'ouvrage (MOA)** : Entité ou personne responsable de définir les objectifs et les besoins d'un projet, souvent le client ou commanditaire.
- ☑ **Malware** : Logiciel malveillant conçu pour endommager ou exploiter un système informatique.

## P

- ☑ **Politique de sécurité** : Ensemble de règles définissant comment les systèmes et données doivent être protégés.
- ☑ **Plan de Reprise d'Activité (PRA)** : Stratégie pour rétablir les activités après un sinistre majeur.
- ☑ **Plan Stratégique du Système d'Information (PSSI)** : Document qui définit les grandes orientations d'un système d'information pour répondre aux besoins de l'organisation.
- ☑ **Plan d'Occupation des Sols (POS)** : C'est un plan d'occupation dans lequel le patrimoine applicatif est réparti en zones, quartiers, ilots et blocs fonctionnels. Les applications actuelles et futures y sont réparties entre chacune des subdivisions.
- ☑ **Progiciel de Gestion Intégrée – PGI (ERP)** : Un PGI (progiciel de gestion intégré) ou ERP (Enterprise Resources Planning) est un progiciel qui intègre les principales composantes fonctionnelles de l'entreprise : gestion de production, gestion commerciale, logistique, ressources humaines, comptabilité, contrôle de gestion. À l'aide de ce système unifié, les utilisateurs de différents métiers travaillent dans un environnement applicatif identique qui repose sur une base de données unique. Ce modèle permet d'assurer l'intégrité des données, la non-redondance de l'information, ainsi que la réduction des temps de traitement.

## R

- ☑ **Redondance** : Duplication de composants pour assurer la continuité du service en cas de panne.
- ☑ **Risque informatique** : Probabilité qu'un événement affecte la disponibilité, l'intégrité ou la confidentialité des systèmes d'information.



## S

- ☑ **Système d'Information (SI)** : Ensemble de ressources (humaines, matérielles, logicielles) qui permettent de collecter, traiter, stocker et diffuser des informations.
- ☑ **SDI (Schéma Directeur des Systèmes d'Information)** : Document stratégique qui planifie l'évolution des systèmes d'information d'une organisation sur plusieurs années.
- ☑ **SIEM (Security Information and Event Management)** : Outil qui centralise et analyse les événements de sécurité.

## T

- ☑ **Traçabilité** : Capacité à suivre l'historique des actions et des événements dans un système.

## U

- ☑ **Urbanisation des SI** : La multiplication des applications présentant des recoupements fonctionnels a conduit à la notion d'urbanisation du système d'information. Il s'agit, par analogie avec les outils du développement urbain, de fixer des règles régissant le développement applicatif pour améliorer la couverture fonctionnelle de certaines activités de l'organisation, éviter la duplication des outils informatiques, fournir une vision prospective de l'évolution du patrimoine applicatif, etc.

## V

- ☑ **VPN (Virtual Private Network)** : Technologie qui sécurise les communications en ligne en créant un tunnel crypté.
- ☑ **Vulnérabilité** : Point faible d'un système qui peut être exploité pour causer un dommage.

# SYLLABUS

Syllabus du cours d'audit et contrôle des Systèmes d'Information:

## 1. Dispensé par :

Thierry MINKA.

## 2. Durée : 50 heures.

2.1. Cours en salle : 40 heures

2.2. Travaux Dirigés en salle : 10 heures

Travaux Personnels de l'Apprenant : 30 heures

## 3. Objectif global du cours :

L'objectif global du cours est de capaciter les apprenants en leur fournissant les bases du métier d'auditeur en général, et de celles d'auditeur des Systèmes d'Information en particulier.

## 4. Contenu du cours

Tableau 12: Détail du cours par livre

N°	Sections du Cours	Objectifs
1	Introduction	Fixer le contexte global du cours
2	<b>LIVRE I : Définitions, concepts et bases pour le cours</b>	Donner les éléments de compréhension et notions manipulées dans le cours
2.1	Définitions, concepts et bases de l'audit et du contrôle	
2.2	Définitions, concepts et bases des systèmes d'information	
3	<b>LIVRE II: Démarche générale d'audit des systèmes d'information</b>	Présenter la démarche globale d'audit qui est commune à tous les types d'audits, mais aussi, présenter quelques éléments spécifiques aux audits des SI
3.1	Travaux préparatoires	
3.2	Planification	
3.3	Exécution de la mission	
3.4	Communication des résultats	
3.5	Normes et Référentiels usuels en audit des SI	
4	<b>LIVRE III: Normes et Référentiels courants en audit des SI</b>	Présenter les normes et référentiels usuels en audit des SI
5	<b>LIVRE IV : Principaux types d'audit dans les systèmes d'information</b>	Présenter les différents types d'audits des SI dans leurs spécificités, points communs, divergences, et exigences
5.1	Audit et contrôle des applications en service	
5.2	Audit et contrôle de la fonction informatique	
5.3	Audit et contrôle des projets informatiques	
5.4	Audit et contrôle de l'exploitation informatique	
5.5	Audit et contrôle de sécurité informatique	
5.6	Audit et contrôle des études informatiques	
6	<b>LIVRE V: Discussions d'actualités</b>	Donner des éléments de base méthodologique aux apprenants pour conduire des discussions scientifiques dans des domaines connexes à l'audit
7	<b>LIVRE VI: Cas pratiques</b>	Introduire les apprenants pas à pas dans une mission d'audit d'une application en service
8	<b>LIVRE VII: Sujets types</b>	Donner un aperçu du type de questions qui viendra aux différents examens

9	LIVRE VIII: Annexes	Mettre à la disposition des apprenants quelques documents non couverts par le secret et le copyright.
---	---------------------	---

## 5. Critères d'évaluation :

Les apprenants seront évalués suivants plusieurs axes :

- ✓ Assiduité :
  - La présence au cours ;
  - La participation aux échanges durant le cours ;
  - Le retour des devoirs dans les délais prescrits.
- ✓ L'appropriation :
  - La compréhension du cours ;
  - La rétention du cours ;
  - La capacité à restituer les concepts en ses propres termes ;
  - La facilité à mettre en œuvre lors du cas pratique.

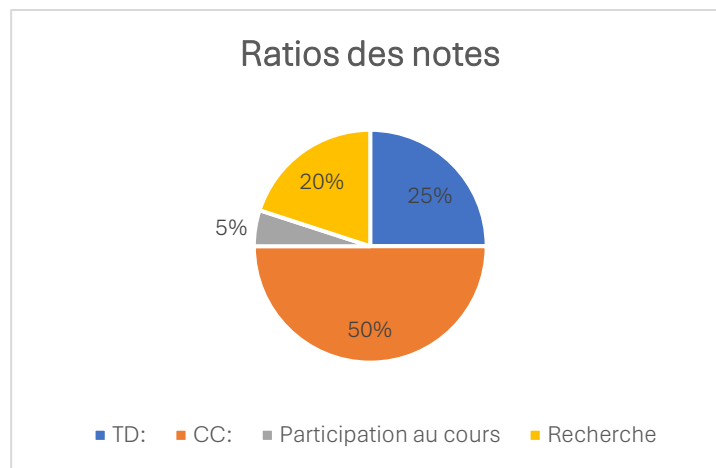


Figure 2: Répartition de la note finale

## Ce support de cours a été préparé par MINKA Thierry

Il est actuellement, *Ingénieur en Chef d'Informatique*, Doctorant et Enseignant Chercheur en Audit des Système d'Information à l'Ecole Nationale Supérieure Polytechnique de Yaoundé, sa formation de base relève de l'ingénierie, dans laquelle il a obtenu tour à tour les diplômes de Technicien Supérieur, d'Ingénieur des Travaux, de Master en Informatique Appliquée à la Gestion d'Entreprise, d'Ingénieur de Conception, de Master en Système Distribués Temps Réels.

Sous-Directeur dans les Services du Contrôle Supérieur de l'Etat, c'est un auditeur chevronné, qui pratique l'audit au quotidien. A titre privé, il réalise des audits à la demande pour plusieurs entreprises publiques et privées du continent.

Il est par ailleurs titulaire de plusieurs certifications (une quarantaine) en audit et les domaines connexes. C'est le premier francophone au monde, à avoir terminé le big 4 chez ISACA en 2020, ce qui lui a valu le titre de Guru. Il détient entre autres, en relation avec l'audit des Systèmes d'Information :

- |   |  |   |
|---|--|---|
| <input checked="" type="checkbox"/> CISA ;  | <input checked="" type="checkbox"/> COBIT ;                  | <input checked="" type="checkbox"/> ISO 9001 Lead Implementor ; |
| <input checked="" type="checkbox"/> CISM ;  | <input checked="" type="checkbox"/> CSX ;                    | <input checked="" type="checkbox"/> ISO 9001 Quality Manager ;  |
| <input checked="" type="checkbox"/> CGEIT ; | <input checked="" type="checkbox"/> ISO 27001 Lead Auditor ; | <input checked="" type="checkbox"/> ISO 22301Lead Implementor ; |
| <input checked="" type="checkbox"/> CRISC ; | <input checked="" type="checkbox"/> ISO 27001 Risk Manager ; | <input checked="" type="checkbox"/> ISO 22301 Lead Auditor ;    |
| <input checked="" type="checkbox"/> CDPSE ; | <input checked="" type="checkbox"/> ISO 9001 Lead Auditor ;  | <input checked="" type="checkbox"/> ISO 22301 Risk Manager.     |

Page 227 sur 227



Dans une autre vie, c'est l'un des cinq (5) Experts Judiciaires du pays en matière de cybersécurité-cybercriminalité.

C'est, aussi, un consultant chevronné qui a déjà notamment travaillé sur des projets pour le compte de la Banque Mondiale, la Commission de l'Union Européenne et la Banque Africaine de Développement. Dans ce cadre, il s'implique principalement dans les problématiques de sécurisation d'infrastructures critiques, de protection de données stratégiques, de développement durable impliquant les technologies, de réduction de la fracture numérique et d'inclusion.

Il enseigne au Programme Supérieur de Spécialisation en Finances Publiques depuis 2016 et à l'Ecole Nationale Supérieure Polytechnique de Yaoundé depuis 2017.

Ecce homo !

[linkedin.com/in/thierry-minka-872961112](https://www.linkedin.com/in/thierry-minka-872961112)