« Le Système de Contrôle Interne »
Plan général du cours

Chapitre 1 : Système de contrôle interne :
Section 1 : Définition d'un SCI
Section 2 : Référentiels de gestion des risques : CoSO 1 et CoSO 2
Section 3 : Risques & Assertions de CI versus audit financier

Chapitre 2 : Cadre conceptuel du système de contrôle interne :
Section 1 : Composantes du SCI (CoSO1)
Section 2 : Principes du SCI (1992-2013)
Section 3 : Outils de description du SCI

Chapitre 3 : Démarche d'Evaluation du système de contrôle interne
Section 1 : Démarche traditionnelle
Section 2 : Démarche CosO d'évaluation du SCI
Section 3 : Remédiation et pilotage des améliorations.

Chapitre 4 : Exemples de procédures de contrôle interne (Exposés)
Section 1 : ventes-clients
Section 2 : achats-fournisseurs
Section 3 : paie
Section 13 : gestion des stocks
Section 14 : investissements
Section 15 : trésorerie

« Le Système de Contrôle Interne »
Référentiel CoSO de CI & de gestion de risques

<u>Objectifs du chap 2 SCI</u>:
L'étudiant(e) devrait, en se basant sur les concepts et définition de base, être capable :

- Distinguer entre composantes du CoSO, le rôle de chacune, et les principes du CoSO
- D'utiliser les principes du CoSO pour conduire une 1ere phase élémentaire d'évaluation d'un SCI en situation nouvelle.
- D'utiliser la matrice Soft-CoSO pour conduire une 2ème phase d'évaluation avancée d'un SCI en situation nouvelle.

Chap 2 : « Composantes & principes du CoSO »
Plan

Section 1 : Composantes du CoSO (et du SCI)

1.1 Environnement de contrôle
1.2 Evaluation des risques de CI
1.3 Activités de contrôle (procédures SCI & leurs contrôles)
1.4 Information & communication
1.5 Pilotage du SCI

Section 2 : Principes du CoSO et du SCI

2.1 Principes version 1992 du CoSO 1
2.2 Principes version 2013 du CoSO 1
2.3 Evaluation du SCI par ses principes (matrice soft coso)

Section 3 : Outils de description du SCI

3.1 Manuel de procédures
3.2 Flowcharting

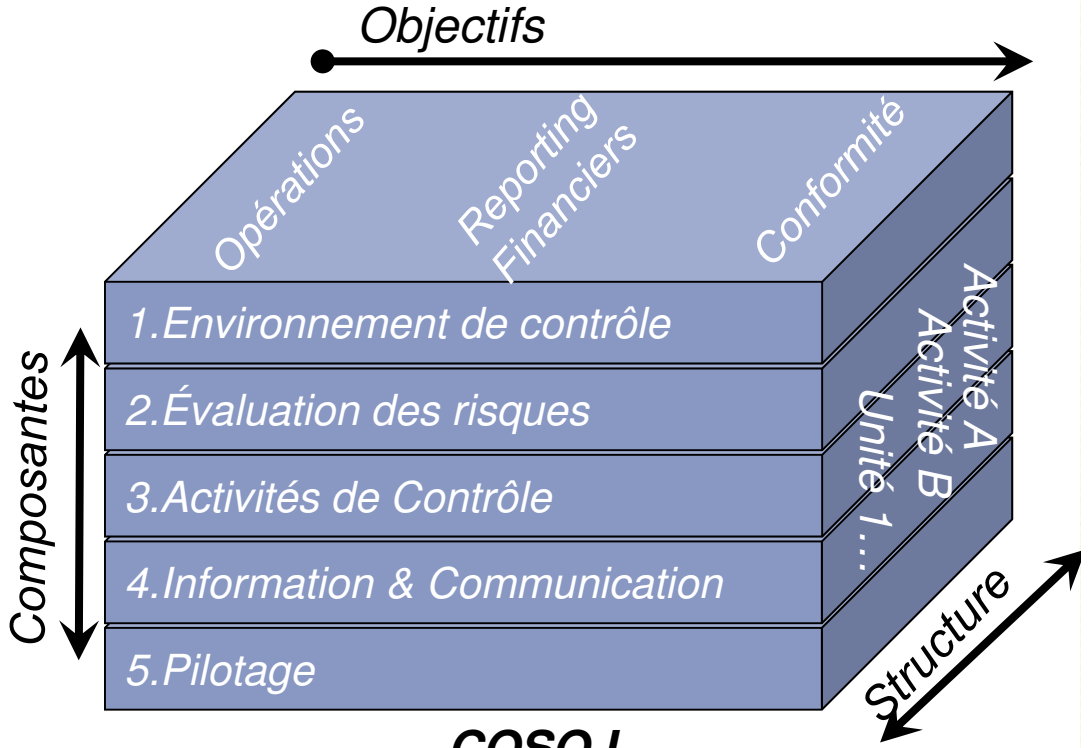
Référentiel CoSO

Le Référentiel

Section I : Composantes du CoSO

- **Référentiel CoSO 1** :
  - 3 dimensions (Composantes/Objectifs/Structure)
  - 3 objectifs (Operations/reporting/conformité)
  - 5 composantes
  - Référentiel intégré (inter-relié)

- Les composantes du CoSO1 sont aussi les étapes ordonnées de mise en place, en une firme, d'un SCI conforme au CoSO.



COSO I
(1992, 2013)

Référentiel CoSO

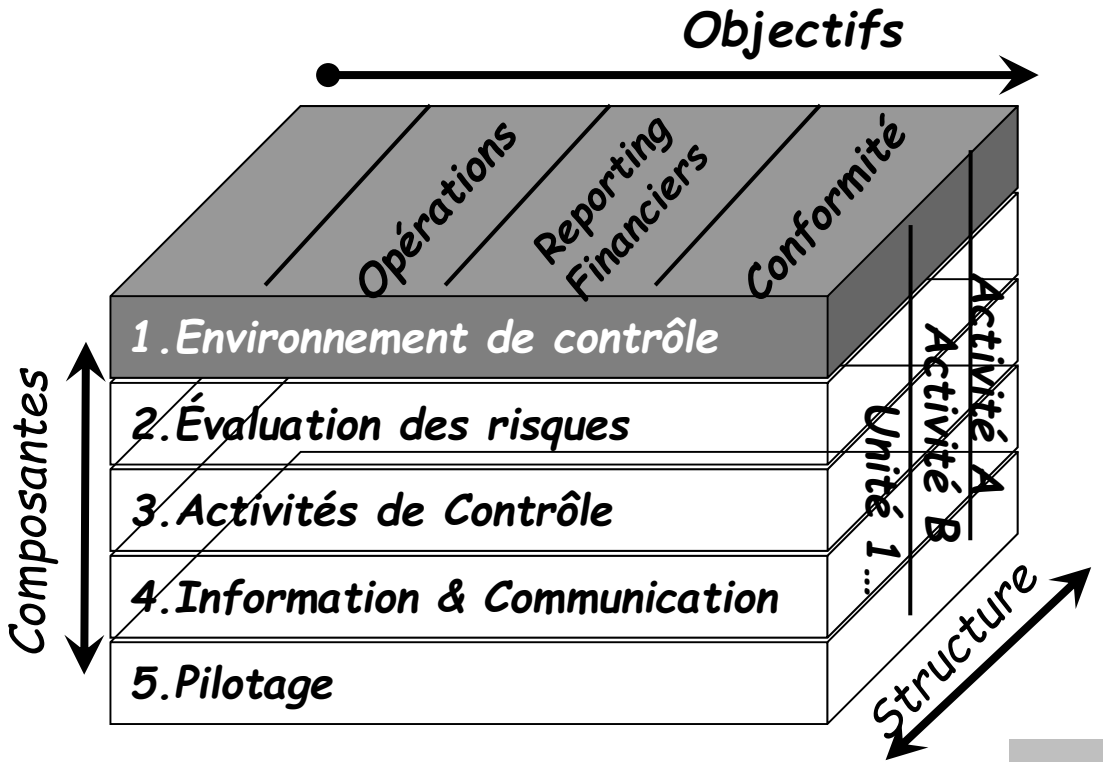
1.1. Environnement de Contrôle

Section I : Composantes du CoSO I

Environnement de Contrôle
1. Démontrer son engagement envers l'intégrité et les valeurs éthiques
2. Exercer une responsabilité de surveillance
3. Etablir : Structure, Autorité et Responsabilité
4. Démontrer son engagement envers la compétence (formations…)
5. Imposer l'auto-responsabilité de rendre compte

Principes à appliquer / vérifier pour cette composante 1 :

Il regroupe les fonctions de gouvernement d'entreprise et de direction ainsi que le comportement, le degré de sensibilisation et les actions de la Direction et du personnel, au regard du SCI et de son importance dans l'entité.



Référentiel CoSO

I.1. Environnement de Contrôle

Section I : Composantes du CoSO I

→ Sensibiliser les employés à l'existence des contrôles

1. Communication et maintien des valeurs éthiques
   (code d'éthique, notes de service, tone at the top…)
2. Engagement à l'égard de la compétence
   (Direction engagée envers ses employés)
3. Participation des responsables de la gouvernance
   (réunions effectives, rémunérations à l'effort…)
4. Philosophie et style de gestion appliqués par la Direction
   (Leadership…)
5. Structure organisationnelle
   (Organigramme, fiches de fonctions détaillées…)
6. Attribution des pouvoirs et des responsabilités
   (critères de recrutement clairs et traçables…)
7. Politiques et pratiques de gestion des RH…
   →fournit « Discipline & Structure »
   →impact diffus

Référentiel CoSO

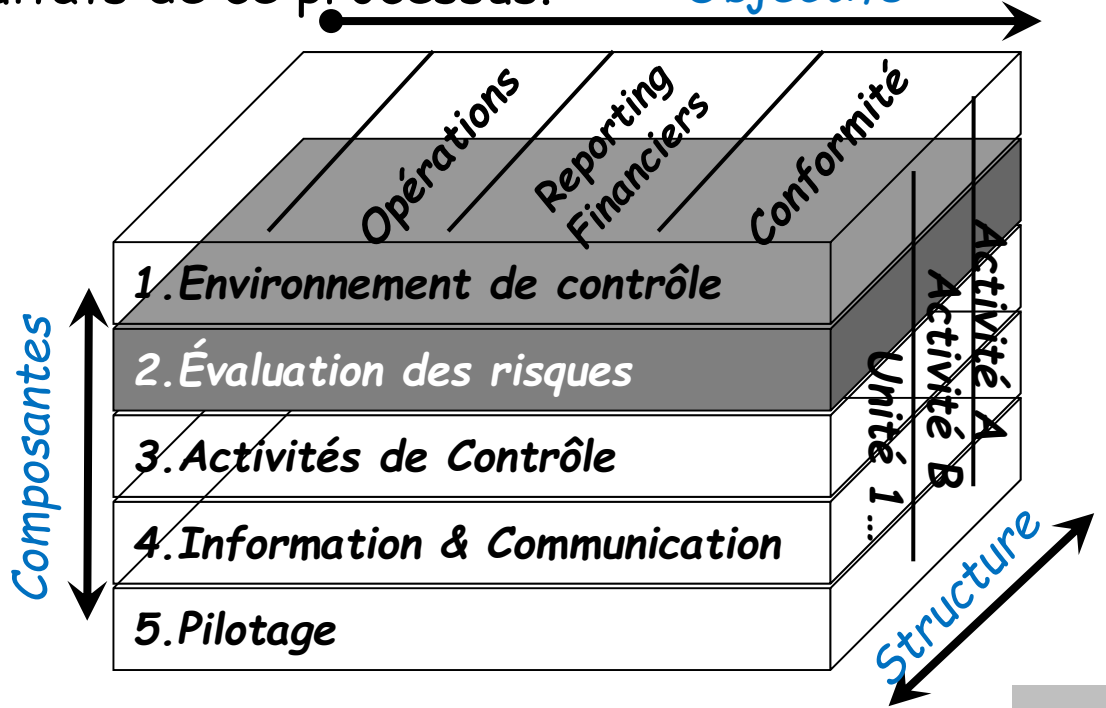
1.2. Identification et évaluation des risques

Section I : Composantes du CoSO I

Identification et evaluation des risques
6. Spécifier des objectifs adéquats
7. Identifier et analyser les risques du SCI
8. Evaluer le risque de fraude
9. Identifier et analyser les changements significatifs

Principes à appliquer / vérifier pour cette composante 2 :

L'auditeur doit acquérir la connaissance du processus suivi par l'entité pour identifier les risques liés à l'activité en rapport avec les objectifs de l'information financière et de décider des mesures adéquates à mettre en œuvre pour gérer ces risques et des résultats de ce processus.



Exemple élémentaire d'Analyse de risques de CI

Petite Firme de service : photocopie :

- R1 : Tremblement de terre
  - Sa proba d'occurrence en l'année : 30 ans (= 1/30 par an)
  - Si réalisé : quelle perte financière subira-t-on ? (ex : de 50 000 dt)
    - Score R1 = Freq x proba = (1/30) x 50 000 = 1667
- R2 : Vol périodique des rames papier
  - 220 x 4 fréquence de réalisation = 880 fois par an
  - 12dt
  - Score R 2 = 10560
- R3 : Coupure d'électricité (machine et lumière)
  - 3 fois par an
  - prix de la photocopieuse : 10 000
  - Score 30 000
- Risque accident camion
  - 12 fois par an
  - 40 000

Référentiel CoSO

1.2. Identification et évaluation des risques

- Risques détectés par SCI ≠ Risque d'audit financier
  Les risques de contrôle interne sont de tout type, les risques d'audit financier liés au contrôle interne ne concernent que les aspects comptables.

- SCI traite des opérations répétitives (d'où le fait qu'une procédure défaillante crée autant d'erreurs que de transaction liée à cette procédure) (rarement des opérations exceptionnelles) (et ce quelle que soit la répétitivité du risque)

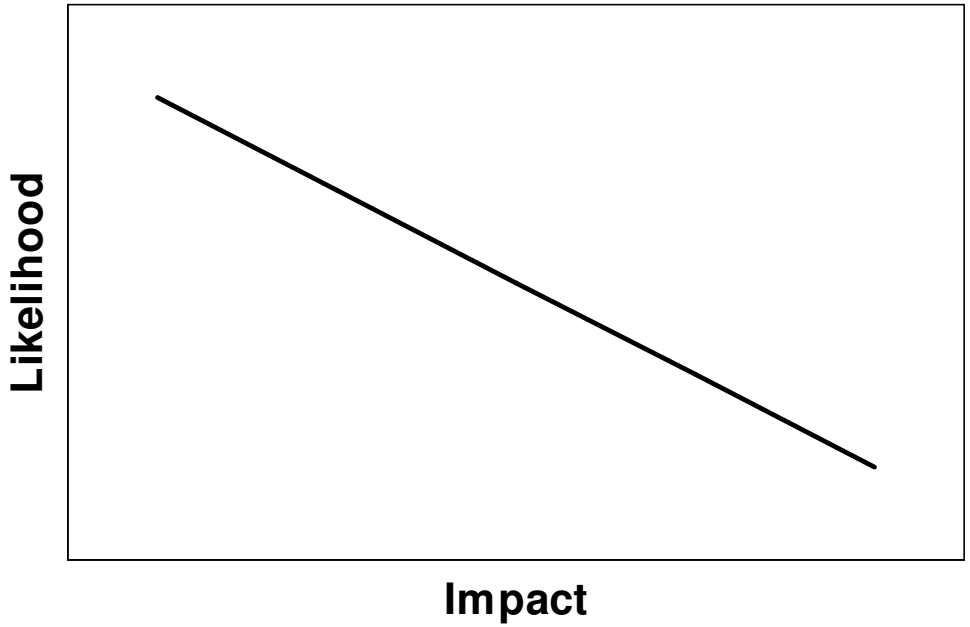
- Les Risques de Contrôle interne (différents des risques d'audit fin – les incluant plutôt) sont relatifs aux opérations répétitives touchant :
  - aux actifs physiques,
  - aux actifs financiers,
  - aux clients,
  - aux fournisseurs,
  - & aux employés.

(Pour une grande entreprise il faut appliquer le référentiel *COSO 2*, additionnant les actifs relatifs à la firme comme sa réputation, sa capacité d'innovation, sa capacité d'adaptation…).

Référentiel CoSO

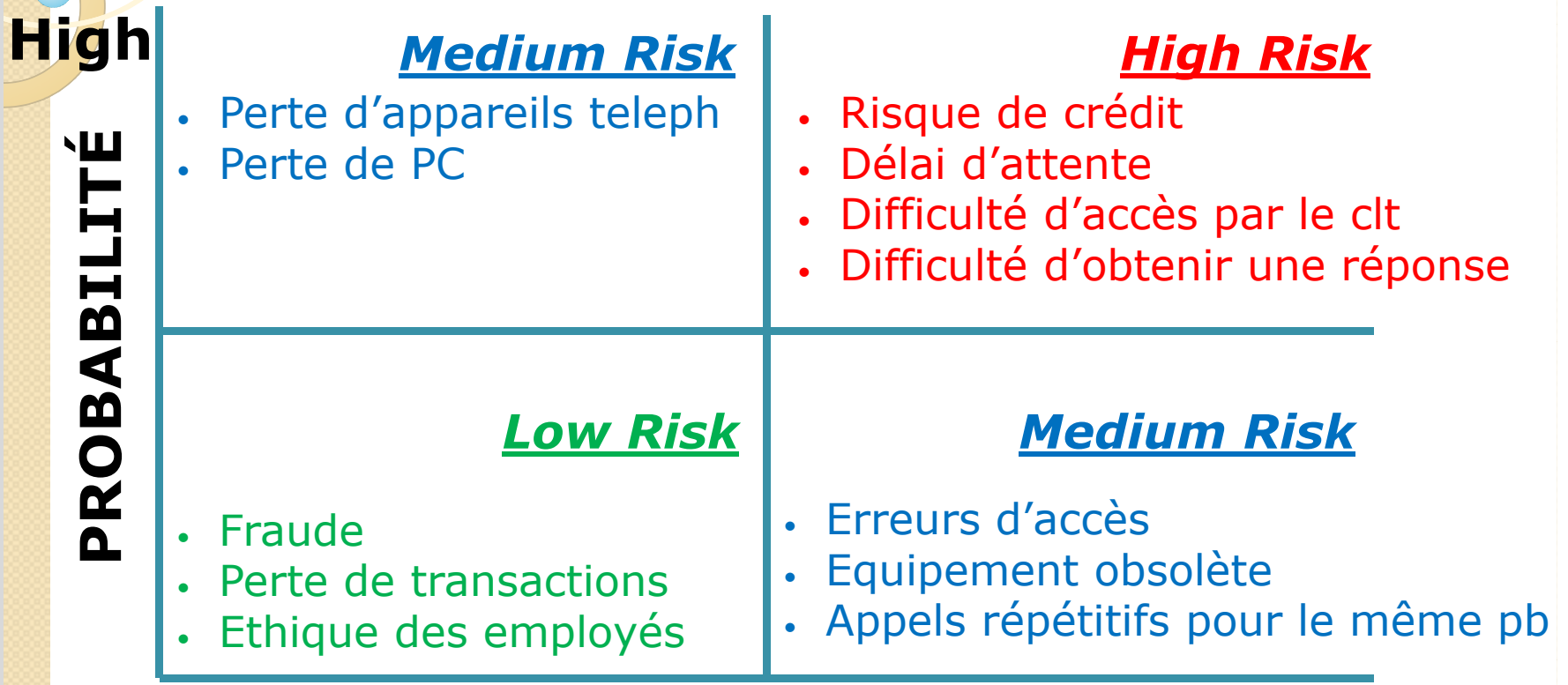
1.2. Identification et évaluation des risques

- Assess risks : Evaluation des risques
  - What is likelihood of occurrence ?
    (probabilité d'occurrence)
  - What is potential impact ?
    (Impact financier)



En tout domaine, il a toujours été vérifié que statistiquement cette courbe baisse tant que la fréquence baisse et l'impact financier augmente

Ex : Eval des risques d'un Call Center



Pour une TPE, il y a peu de risques à gérer, on utilise une telle matrice pour les classer et en identifier les plus graves. Pour une Grande Firme, le nombre de risques à gérer devient infini, ils sont alors classés en nuage de points en une cartographie de risques.

Référentiel CoSO

1.2.1. Matrice de classement des risques

- Mettre en application la composante 2 du CoSO signifie : L'auditeur interne doit investiguer comment la Direction :
  - Identifie ces risques (d'opérations répétitives),
  - Leur Estime une probabilité de survenance et un impact financier possible
  - Les Classe en priorité (matrice/cartographie des risques)
  - Évalue le caractère significatif de ces risques (selon l'emplacement en la matrice ou cartographie),
  - Décide des activités à mettre en place pour en couvrir les plus graves

Matrice de classement des risques de CI

Probabilité d'occurrence	Impact financier : de 0 à 150 000 dt	Impact financier : de 150 001 dt à 800 000 dt	Impact financier : de 800 001 dt à 2 000 000 dt &
Très fréquent	2 E,F	3 A	3
Moyennement fréquent	1 H	2 B, C	3 D,G,I
Peu fréquent	1 J	1 K	2

Source : global Association for Risk Professionals

Référentiel CoSO

I.2.2. Logique d'identification de la réponse au risque

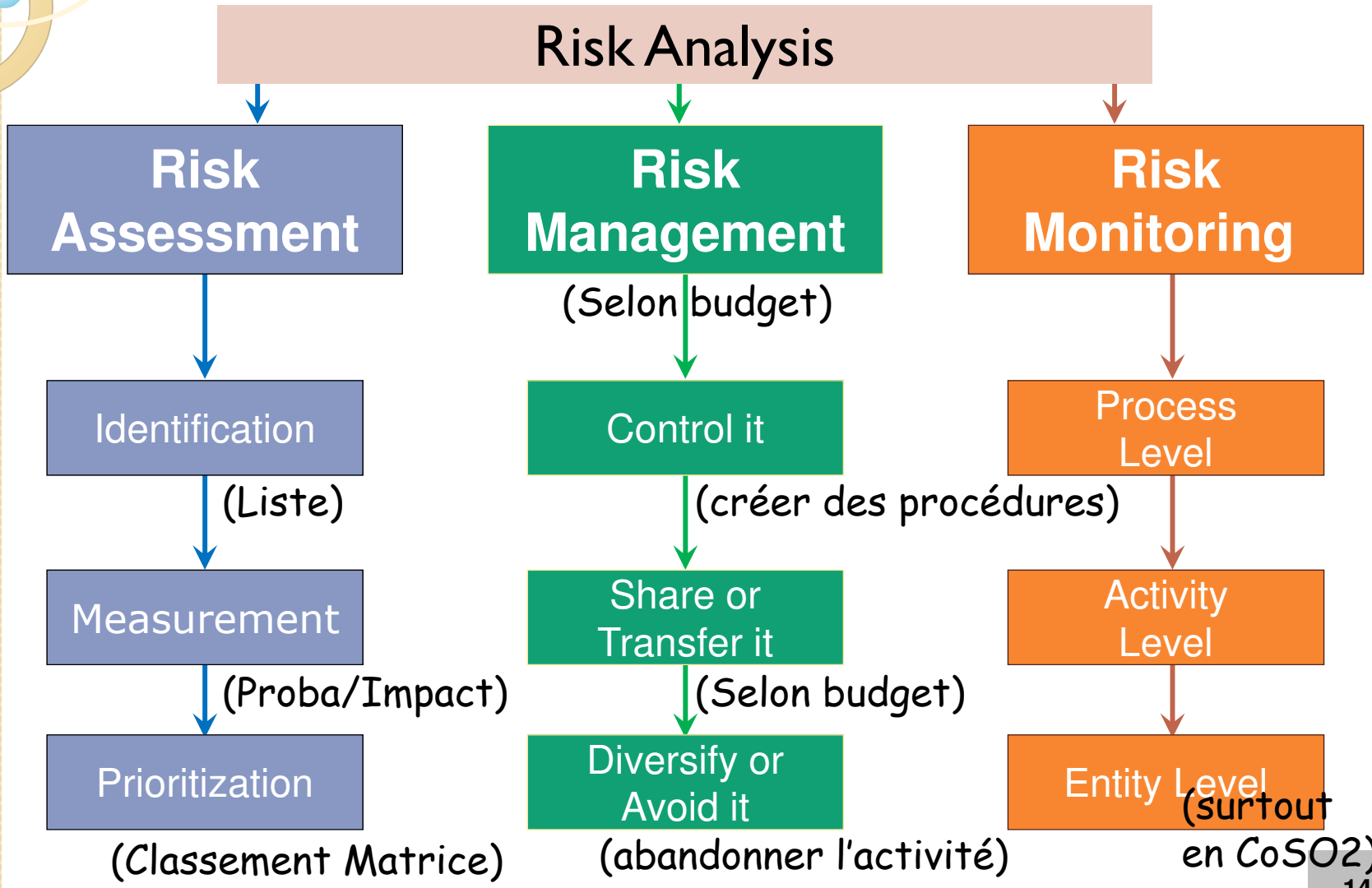
Une fois les risques de CI les plus graves (les plus urgents à couvrir) sont identifiés (via l'analyse et le classement par la matrice :

- Quantification de l'exposition au risque (via le classement par la matrice / cartographie)

- Options disponibles :
  - Accepter = laisser faire (si le risque est classé faible)
  - Réduire = instituer des contrôles (si le budget à rattacher à la procédure de CI serait réduit abordable)
  - Partager (transférer) = avec un partenaire (si le coût de la procédure de CI est inabordable *(ex : assurance))*
  - Eviter ou diversifier = éliminer *(ex : abandonner l'activité risquée)*
- Risque résiduel : le risque non couvert par la procédure de CI mise en place *(RR doit être faible, non significatif)*

Référentiel CoSO

1.2.3. Phases du risk management



Référentiel CoSO

1.3. Activités de Contrôle

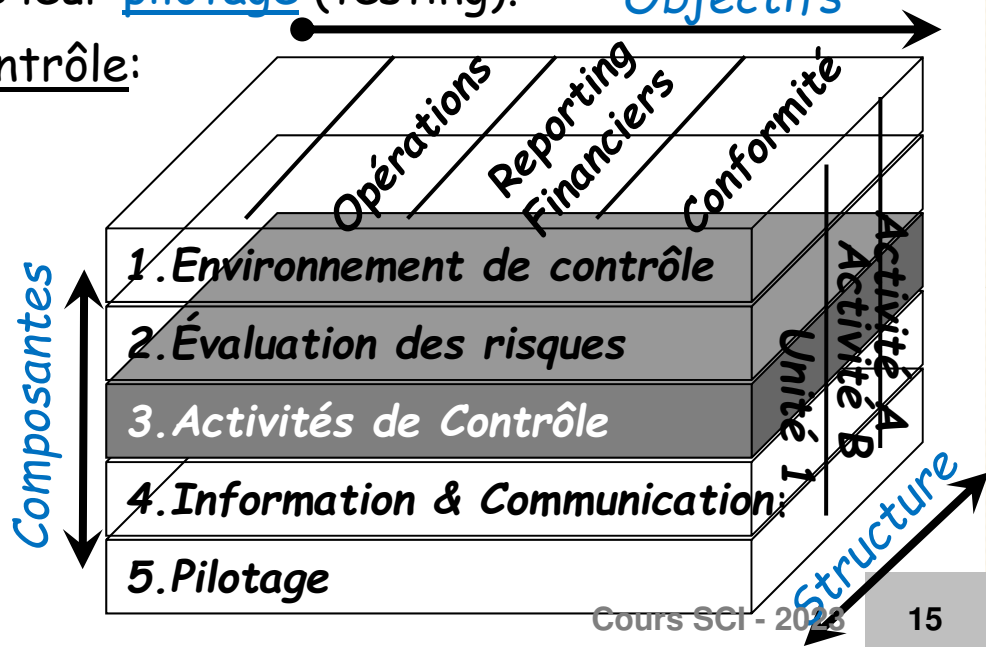
Section I : Composantes du CoSO I

Activités de contrôle
10. Sélectionner et développer les activités de contrôle (procédures SCI)
11. Sélectionner et développer les contrôles généraux des technologies
12. Déployer les activités de contrôle via les politiques et procédures

Composante 3 : Activités de contrôle (procédures de SCI)
Face aux risques identifiés les plus urgents à couvrir, l'auditeur interne doit concevoir ou identifier des activités de contrôle, les classer par ordre d'efficience, les proposer à la Direction qui en sélectionne les plus adéquates (selon budget dispo), puis l'auditeur interne et les Directeurs se chargent de l'implémentation des procédures sélectionnées (en former et informer le personnel aussi). Enfin l'auditeur interne se charge de leur pilotage (testing).

Ex. d'activités de contrôle:

- l'évaluation des performances
- l'autorisation
- le traitement d'info
- les contrôles physiques
- la séparation des tâches…



Référentiel CoSO

1.3. Activités de Contrôle

- Une fois les risques les plus graves identifiés, des procédures de CI doivent être à leur tour identifiées et sélectionnées parmi les plus efficaces et efficientes dans la limite du budget (relatif au département d'audit interne) y consacré chaque année.
  - Ex : Contre le risque d'achat de M1eres inadéquates (en qualité/prix/dispo…), on peut sélectionner une procédure d'approvisionnement par : étude de marché, ou appel d'offre, ou convention avec un fournisseurs stratégique, etc… La procédure la + efficace et la moins coûteuse sera choisie…
- Une procédure peut couvrir plusieurs risques de CI et plusieurs procédures peuvent couvrir un unique risque
- La procédure la plus efficiente choisie doit toujours induire un risque résiduel non significatif.

- Les procédures opérationnelles de CI (relatives aux différents départements de la firme) sont précédées par des procédures de budgétisation et sont complétées par des procédures de contrôle informatique (ITgeneral controls)

- Selon sa complexité et son importance dans le SCI, une fois la procédure la + efficiente sélectionnée pour couvrir un risque donné, son implémentation nécessite les phases d'achat/création, mise en place, formation des employés à son exécution, test de démarrage et rectifs possibles & enfin tests de démarrage final.

Fonctions incompatibles

La séparation des fonctions incompatibles est un des principes de contrôle interne qui consiste à une répartition des responsabilités et des tâches de manière à éviter qu'une personne les cumulant au point d'augmenter le risque d'erreurs ou de fraude. Cette séparation vise essentiellement à rendre :

- La fraude difficile à réaliser parce qu'elle nécessite la complicité d'au moins deux personnes
- L'empêchement et la détection des erreurs plus faciles et en temps opportun.

Ainsi, les différentes personnes qui interviennent dans le processus de traitement doivent se contrôler mutuellement et éviter qu'une personne puisse **commettre et dissimuler ses propres erreurs** ou malversations.

Quelles sont les fonctions incompatibles ?

Aucun employé ne doit avoir sous sa responsabilité toutes les étapes clefs d'une opération donnée. Ces étapes concernent :

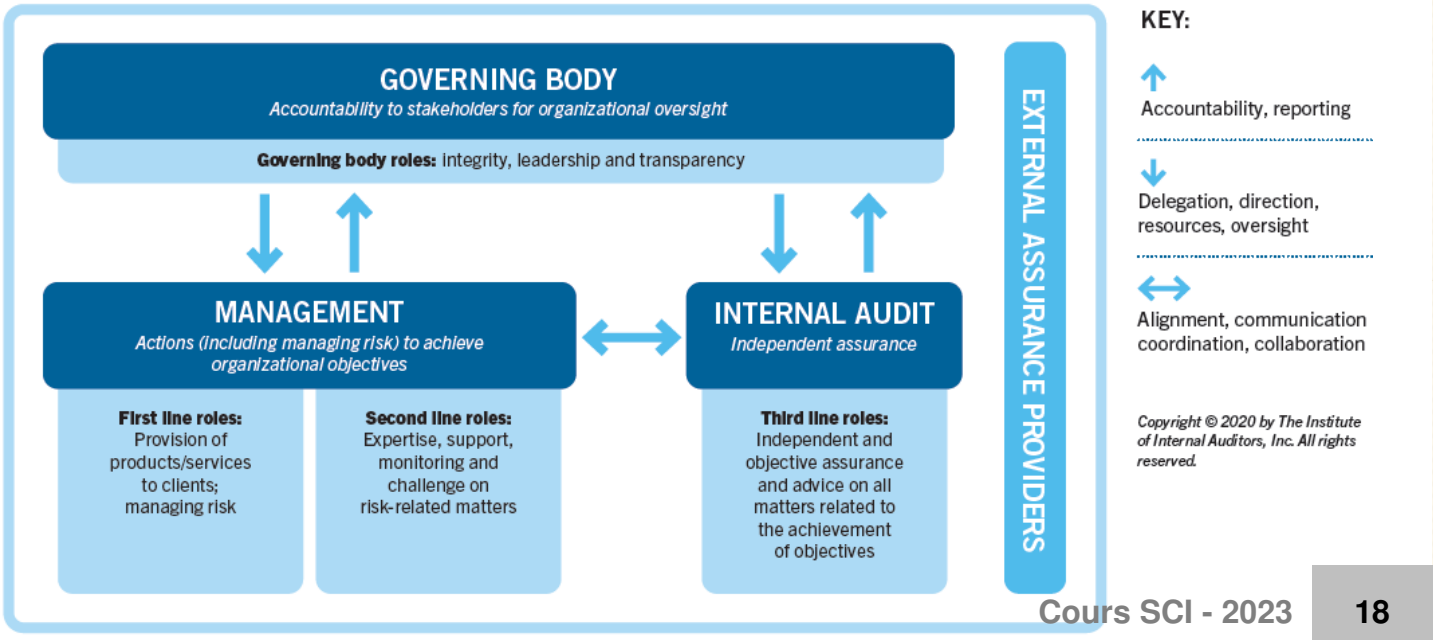
1. **Autorisation** (authorization)-**Décision** : avoir le pouvoir d'engager l'entreprise
2. **Conservation** (custody) de biens (ex magasinier), de valeurs (ex : coffrefort)
3. **Enregistrement** (recording): tenue de la comptabilité, tenue des fiches stock
4. **Contrôle** : sous ses diverses formes (rapprochement des comptes, audit, Inspection…)

Référentiel CoSO

1.3.1. Les lignes de défenses contre les risques

3 lignes de défense contre les erreurs de procédures de CI :

- Exécution par les employés : Procédure de contrôle interne à chaque transaction
- Exécution par les Directeurs responsables d'activité de contrôle : Contrôler la bonne exécution de la procédure à chaque transaction (Contrôle de toutes les transactions/an (ex: 1000/an)
- Exécution par l'Auditeur interne de tests des contrôles : Tester les contrôles : Auditer de façon périodique (→ échantillon de 20 parmi les 1000).



Référentiel CoSO

1.3.2. Typologie des Contrôles selon le CoSO I

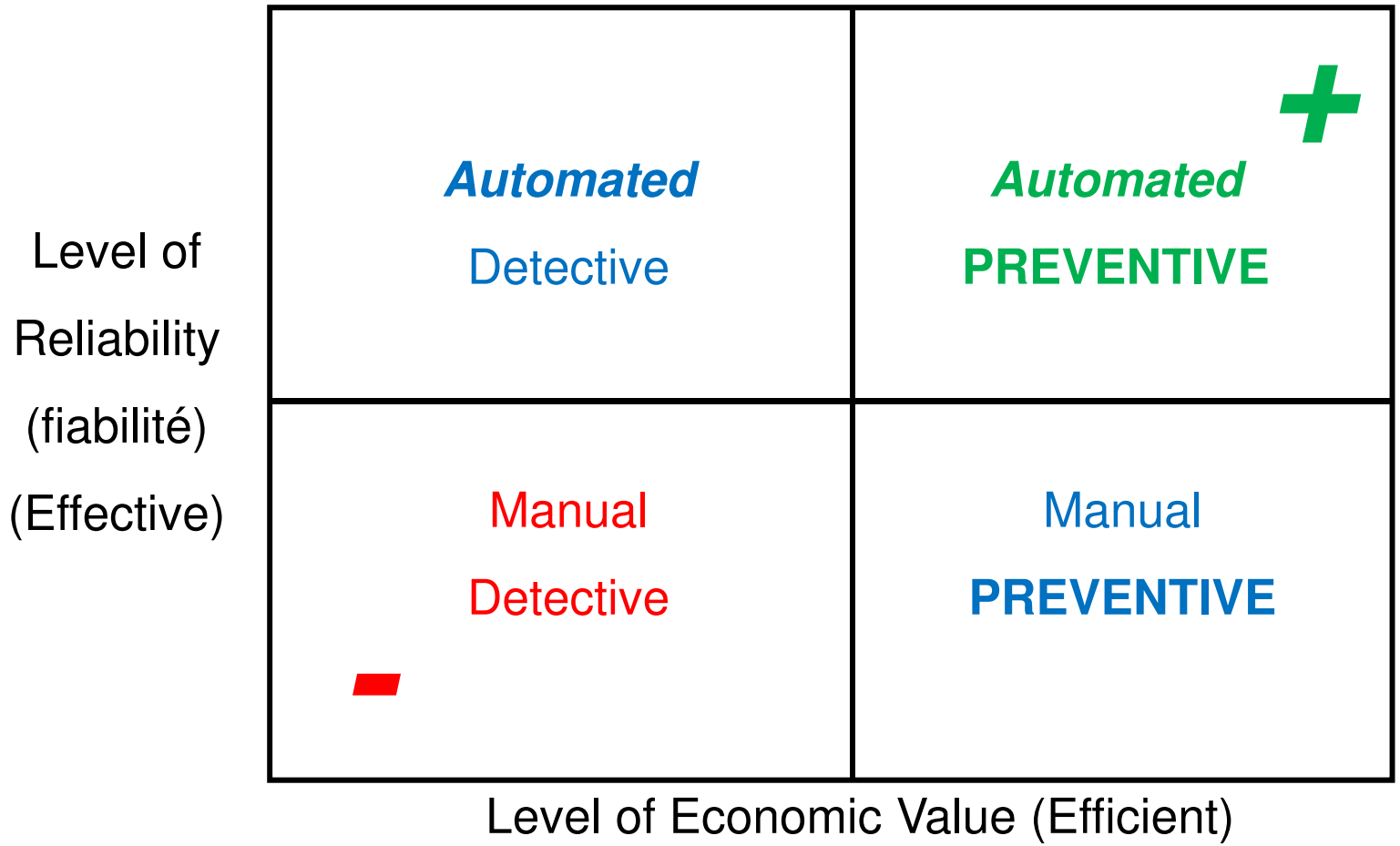
- **Contrôles automatisés** - Incorporés au système / algorithmes d'application – indépendant des personnes
  - Ex : le système recherche automatiquement un bon de commande correspondant avant de payer une facture
- **Contrôles manuels** - exécutés par des personnes en dehors du système ou de l'application
  - Ex : signature du superviseur sur le relevé d'une carte de crédit

- **Contrôles préventifs** - Intégrés au processus ou au système pour éviter ou minimiser les risques. Aide à rendre les processus plus efficaces et peut réduire le coût des actions correctives.
  - Ex : Contrôles d'accès - Seules les personnes ayant un accès approuvé peuvent effectuer des transactions
- **Contrôles de détection** - Fournit une évaluation du processus pour identifier les problèmes potentiels pour un examen plus approfondi
  - Ex : L'unité rapproche le registre des salaires bruts pour s'assurer que toutes les transactions sont correctes
  - Ex : Paie : examine tous les frais non valides

Référentiel CoSO

I.3.3. Classement des Activités de Contrôle

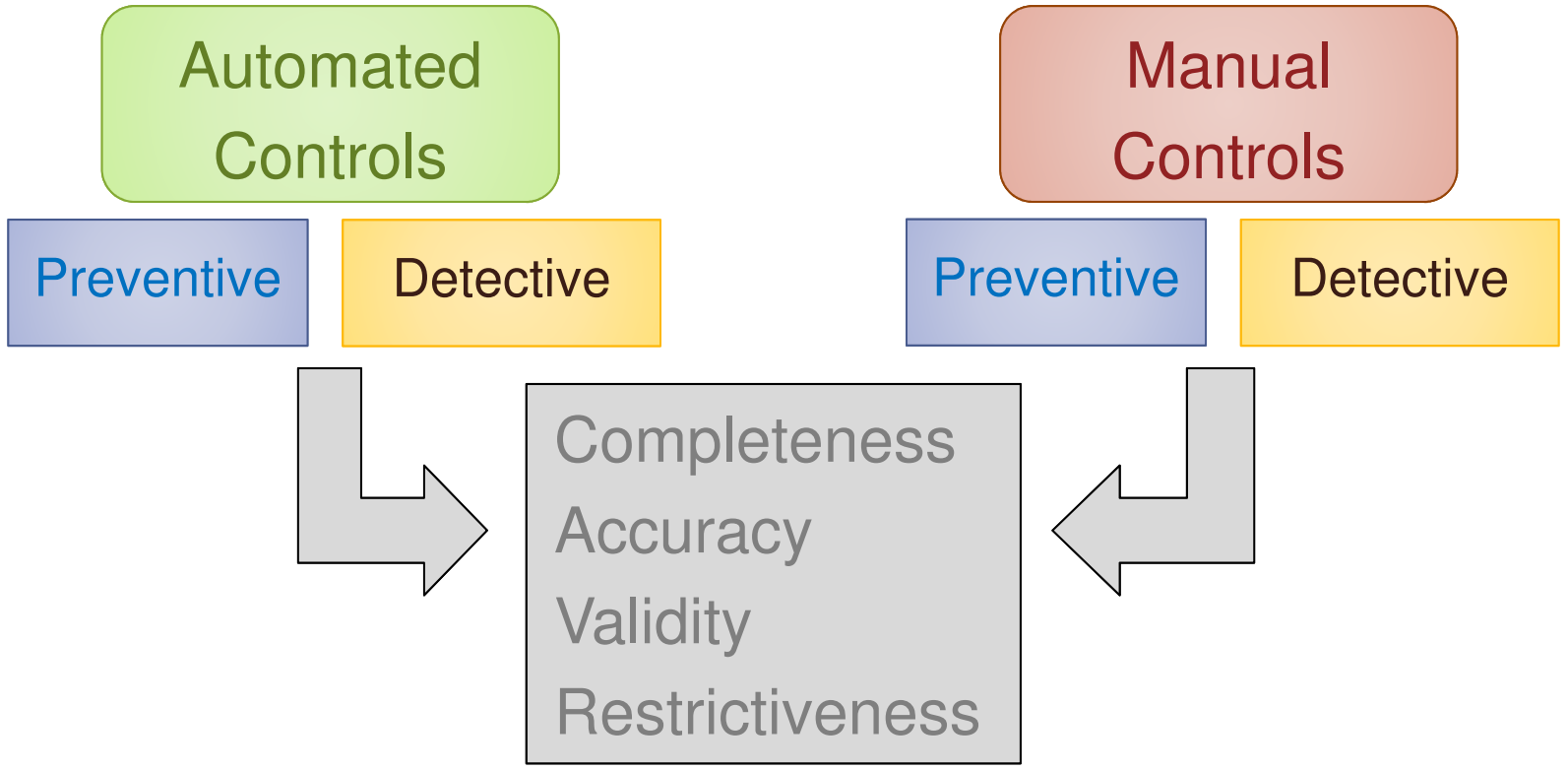
Alors que les contrôles automatisés sont généralement plus efficaces,
Les contrôles préventifs sont généralement plus efficients



Référentiel CoSO

I.3.4. Les Assertions de Contrôle Interne

Vue des interrelations entre contrôles et assertions

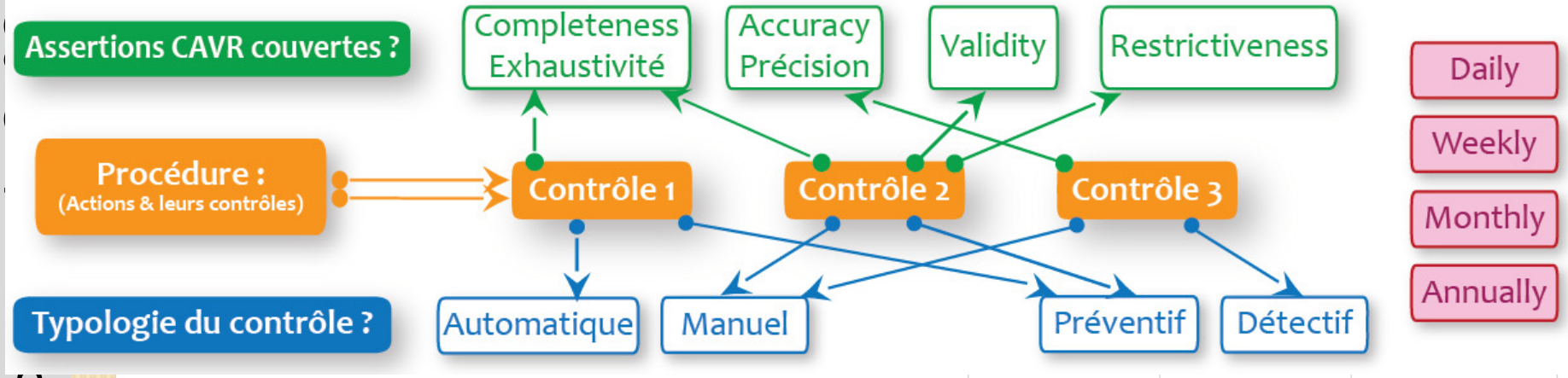


- Tout Contrôle automatisé est généralement efficace mais coûteux
- et tout Contrôle Préventif est efficient mais coûteux

Référentiel CoSO

1.3.5. Logique de la Matrice des Tests de Contrôles

Logique à adopter en préparant la Matrice des Tests de Contrôles :



Ainsi que la **<u>périodicité</u>** du contrôle, qui va servir à identifier la taille de l'échantillon pour le test -fait par l'auditeur interne- du contrôle

Si population homogène :		
	Population	Taille échant.
Daily	220	20
Weekly	56	7
Monthly	12	3
Annually	1	1

Logique adoptée par l'auditeur interne lors de ses tests :

Plus la matrice indique des contrôles automatisés et préventifs
& Plus la matrice indique des assertions couvertes par les contrôles
→ Mieux est évalué le SCI.

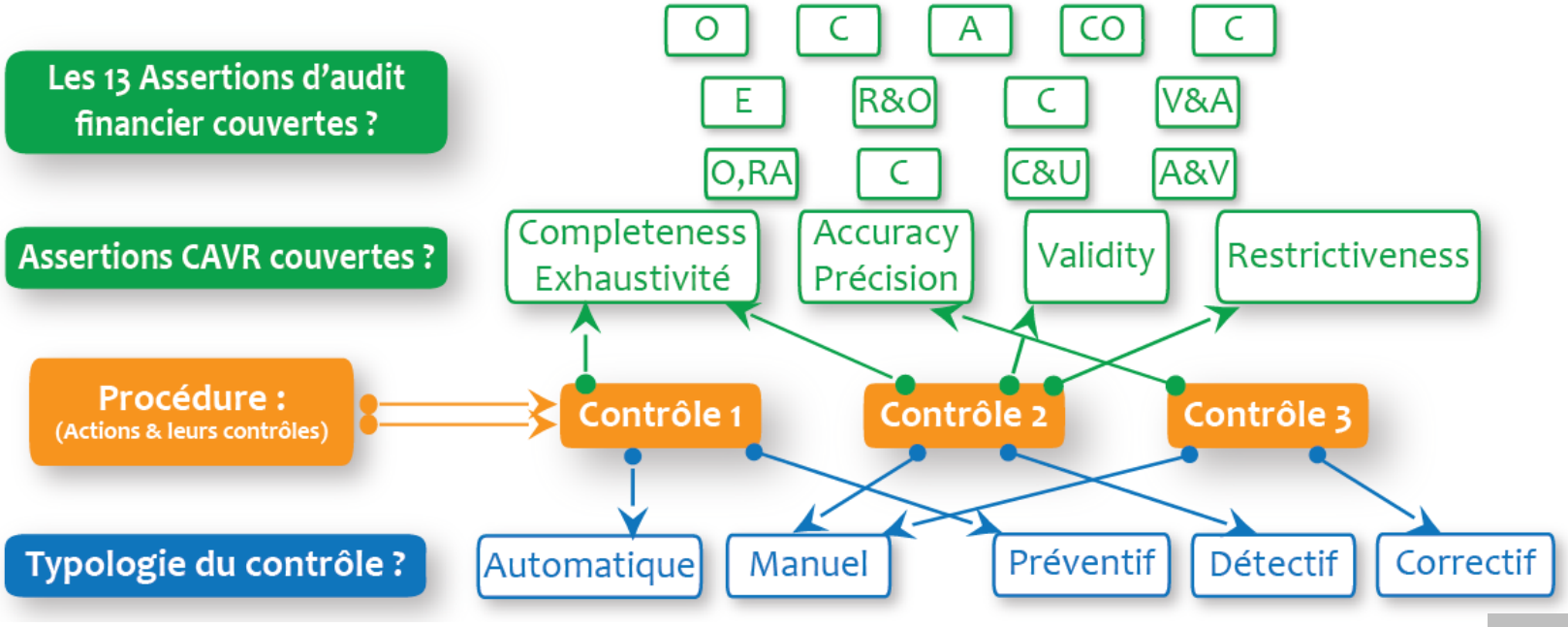
Référentiel CoSO

1.3.5. Logique de la Matrice des Tests de Contrôles

La typologie du CoSO ne comprend pas la modalité « correctif », qui appartient plutôt aux normes ISA d'audit financier.

En mission d'audit financier, l'auditeur financier externe ne teste que les contrôles ayant un impact significatif sur les comptes comptables; Il les teste suivant les 4 assertions de CI et les 13 assertions d'audit financier.

→ Il n'évalue donc qu'une partie du SCI et non la totalité.



Référentiel CoSO

1.3.6. Matrice des Tests de Contrôles

- Exemple simple d'une MTC établie sur excel :

Matrice des tests des contrôles :

												Auditeur interne		
												Test du Contrôle		
Procédure	N° du Ctrl	Description	Automatisé	Manuel	Préventif	Détectif	C	A	V	R	Périodicité	description du test	Taille échantillon	Observ - Conclusion
Procédure A d'achat MP	1	Le Directeur des Approv. vérifie la signature et le cachet de l'ingénieur sur le doc d'expression des besoins.		X		X			X		Daily	L'AI sélectionne un échantillon des Doc d'expr des besoins et en vérifie les cachet s et les signatures	20	xxxxxxx
	2	Le D. App quand il reçoit la permission de la part du DAF pour passer la commande suite à la disponibilité de la somme, vérifie son cachet et sa signature dessus.		X		X			X		Daily	L'AI sélectionne un échantillon des Doc de permission à passer la Cde par le DAF et en vérifie les cachet s et les signatures	20	xxx
Procédure B de	3	xxxxxxxxxx	X		X		X				WEEKLY	xxxxxxxxxx	7	xxxxx
	4	xxxxxxxxxxxxxxxxxxxxxxx	X			X		X			MONTHLY	xxxx	3	xx
	5	xxxxxxxx		X	X		X			X	WEEKLY	xxxxxx	7	xxxxxxxx
Procédure C de	6	xxxxxxxxxxxxxxxxxxxxxxxxxxxx		X		X				X	ANNUALLY	xx	1	xxx
	7	xxxxxxx		X		X			X		MONTHLY	xxxx	3	xxxx

Référentiel CoSO

1.3.6. Matrice des Tests des Contrôles

Composition idéale de la MTC : (23 colonnes)

- Process (Procédure – opération réalisée par les employés)
- Contrôle n° (réalisé souvent par un responsable de département)
- Objectif du contrôle
- Risque couvert par ce contrôle
- Description du Contrôle (issue du manuel des procédures)
- Périodicité (fréquence qui indique la taille de toute la population de docs qui feront l'objet du testing, généralement homogène)
- Responsable du Contrôle (Control owner) le vis-à-vis de l'Auditeur
- Contrôle informatisé l'accompagnant
- Typologie du Contrôle (automatisé - manuel / préventif - Détectif)
- Assertion de CI couverte par ce contrôle (C/A/V/R)

→ jusqu'ici la matrice obtenue s'appelle « Matrice des contrôles » et aide à obtenir une description fine des différentes contrôles (activités de contrôles) sélectionnés pour être testés par l'Auditeur interne. Elle contient 16 colonnes et autant de lignes que de contrôles.

- Description du testing
- Type (automatisé / par échantillon)
- Taille décidée de l'échantillon (selon la périodicité du contrôle)
- Timing de conduite du test
- Responsable (de qui demander les docs à tester ou autre)
- Conclusion du Test (contrôle effectif ou non)
- Remediation plan (description d'un nouveau contrôle de remédiation à proposer à la Direction)

Référentiel CoSO

I.3.7. Testing Design

Modalités de testing considérées par le CoSO 1: Enquêtes,Observations Examen de Documentation, Re-exécution, et Analyse de données

- **Enquête** : Demander des explications à propos d'un contrôle à un control owner. Modalité à faible crédibilité, nécessite d'être accompagnée par d'autres tests, car insuffisante pour conclure que le contrôle a été effectif durant la période objet du testing.
- **Observation** - Pendant l'observation, l'équipe d'audit interne regarde les performances réelles du contrôle. L'observation fonctionne bien quand l'équipe veut observer en temps réel un contrôle d'application tel que par ex. un système générant un « refus d'accès car non autorisé », type de message d'erreur lorsqu'un employé tente d'accéder à une partie d'une application dans laquelle le contrôle est conçu. L'équipe d'audit demanderait à un employé de faire une tentative d'obtenir un accès non autorisé et d'observer l'application en train de refuser l'accès non autorisé. L'équipe peut également obtenir des captures d'écran tout au long des étapes d'observation pour avoir la preuve du test et le documenter en leur papiers de travail. L'observation est aussi utile pour valider la conception d'un contrôle manuel pour comprendre si le processus décrit au Manuel des procédures est ce qui est réellement effectué.

Référentiel CoSO

I.3.7. Testing Design

Modalités de testing considérées par le CoSO 1: Enquêtes,Observations Examen de Documentation, Re-exécution, et Analyse de données

- **Examen de documentation** : sert à comprendre l'opération ayant nécessité ce contrôle. Sert aussi à évaluer la conception et le fonctionnement du contrôle. Par exemple, un contrôle peut déclarer que les enregistrements en un registre sont examinés et approuvés par le personnel approprié avant d'entrer dans le système. Les tests incluraient généralement l'examen des imprimés (ou fichiers à l'appui) générés par l'exécution du contrôle, comme preuve de la revue de l'enregistrement et de ses bons attributs, montants… (données complètes et précises).
- **Re-Exécution** (RePerformance) : modalité de testing utilisée face à des contrôles manuels ou exécutés de façon peu fréquente. L'équipe d'audit interne re-effectuerait le contrôle étape par étape, pour essayer d'obtenir les mêmes « bons » résultats ou effets que prévus.
- **Analyse de données** (Data analytics) : grâce à des outils souvent indépendants de l'ERP même, l'analyse de données sert à tester les infos sauvegardées en large population et à en extraire des incohérences difficilement réalisable par test manuel.

Référentiel CoSO

I.3.7. Testing Design

Caractéristiques des testing considérées par le CoSO 1:

- **Timing d'un testing** : Le moment des tests de contrôle est souvent déterminé selon la gravité et de la forte probabilité (risque plus élevé d'échec du contrôle par ex. en raison de la complexité du processus ou rotation du personnel clé…). Plus tôt le test effectué, moins la probabilité d'échec du contrôle serait subie. Une période de remédiation plus longue serait possible en conséquence (Ex. probabilité accrue de vol ou fraude résultant de l'insuffisance du contrôle).

- **Etendue d'un testing** : dépend de nombreux facteurs :
  - L'importance de la procédure de CI pour l'entité
  - Volume des transactions affectées par période
  - Complexité du contrôle
  - Importance de l'impact financier lorsque le contrôle s'avère défaillant ou autre type d'impact

- Les tests peuvent être statistiques (au hasard selon loi statistique) ou ciblés (non statistiques) et peuvent se baser sur les conclusions d'experts externes…

- Les tests conduits devraient être classés selon leur urgence.

Référentiel CoSO

1.4. Information et communication

Section I : Composantes du CoSO I

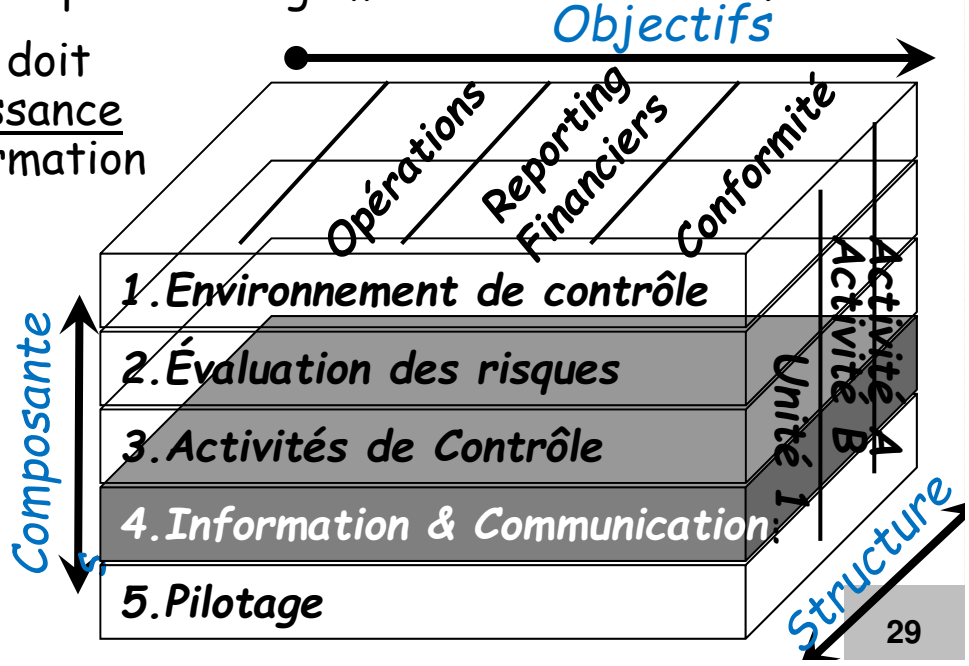
Information and communication
13. Utiliser des informations pertinentes
14. Communiquer en interne
15. Communiquer en externe

Composante 4 : Le SCI doit garantir que :

- l'information collectée en interne ou externe, traitée, produite ou divulguée soit pertinente à la prise décision,
- que la communication nécessaire en interne se fasse,
- & que la communication en externe, nécessaire, se fasse.

La direction identifie, saisit et communique les informations pertinentes sous une forme et dans un délai qui permettent aux gens de s'acquitter de leurs responsabilités.
La communication se produit largement à tous les sens.

L'auditeur interne doit acquérir la connaissance du système d'information et des processus opérationnels d'élaboration de l'information financière ou autre, des rôles et responsabilités de chacun et les évaluer.



Référentiel CoSO

I.4.1. Implémentation de la composante 4

La Composante 4 : Information & communication vise que :

- Toutes les procédures de CI en vigueur au sein de la firme sont à communiquer au personnel et éventuellement aux autres parties prenantes de la firme lorsque nécessaire
- Des formations sont à dispenser au personnel pour la compréhension et la correcte application des procédures de CI
- Le personnel nouveau est à orienter systématiquement par rapport aux procédures de CI existantes
- Les responsabilités du personnel en matière de CI sont à intégrer à leurs objectifs annuels et à être prises en compte lors de l'évaluation de chacun d'eux
- Le personnel est à former correctement à l'utilisation des outils et systèmes informatiques de la firme
- Un mécanisme de gestion des connaissances devrait exister au sein de la firme, qui permet de partager les leçons apprises des événements (positifs ou négatifs) avec l'ensemble du personnel et d'en tenir compte pour le futur. (Ex : cas de fraude confirmés : font-ils l'objet d'une communication adéquate au sein de la firme et au besoin vis-à-vis des autorités judiciaires ?)…

Référentiel CoSO

1.4.2. Testing de la composante 4

Le testing de cette composante (par interviews ou autre) réussit lorsqu'il permet à l'Auditeur interne de :

1. comprendre le dispositif mis en place pour le suivi des objectifs et des contrôles
2. identifier les indicateurs retenus pour la mesure des objectifs.
3. Vérifier que les indicateurs retenus sont communiqués au management via les rapports d'activités périodiques (annuelle, trimestrielle, mensuelle…)
4. S'assurer que les activités sont régulièrement rapportées au management
5. Vérifier que ces indicateurs/Rapports sont systématiquement analysés par le management et que des décisions appropriées sont prises pour corriger les insuffisances observées. Examiner pour cela les comptes rendus de réunions.
6. Vérifier qu'un suivi des recommandations des différents fournisseurs d'assurance (auditeurs internes, auditeurs externes, régulateurs…) est effectué et que des décisions appropriées sont prises par le management et mise en œuvre pour la correction des défaillances éventuelles identifiées.
7. Vérifier que pour chaque décision prise pour l'amélioration du contrôle interne, le management a identifié un ou plusieurs control owners et a effectué un suivi formel de la mise en œuvre des décisions.

Référentiel CoSO

1.5. Pilotage du SCI (Monitoring)

Activité de pilotage
16. Conduire des évaluations permanentes et/ou séparées
17. Evaluer et communiquer les défaillances

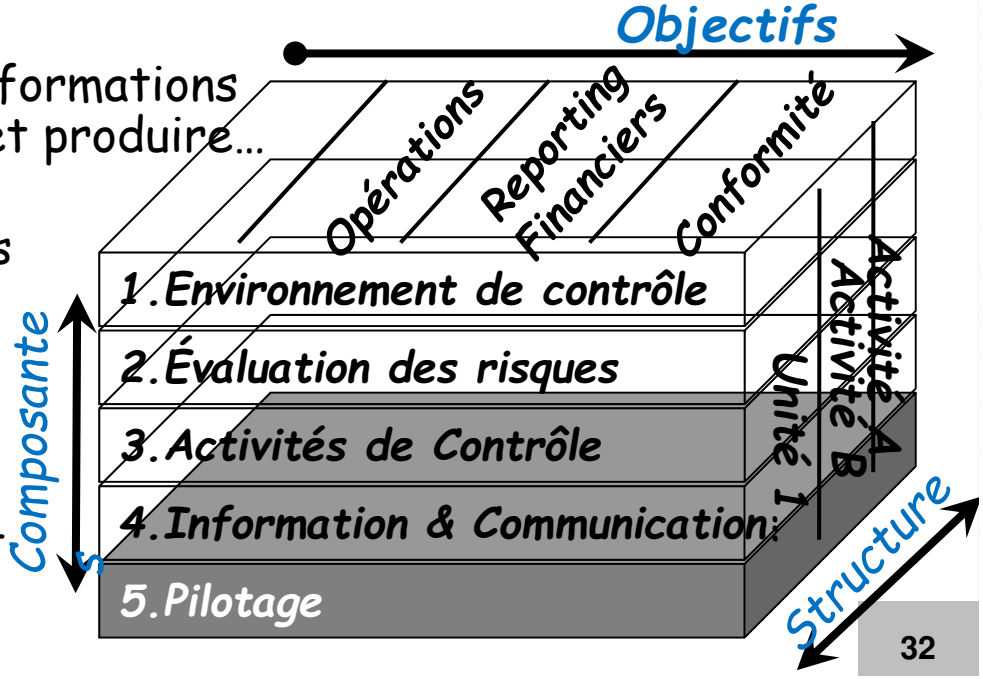
Composante 5 : Pilotage du SCI : (contrôle du contrôle) Le suivi des contrôles est un processus continu destiné à évaluer l'efficacité et la performance du SCI au fil du temps.

Il implique à la Direction de mettre en place un système de pilotage du SCI face à tout changement possible :

- en termes de risques nouveaux à couvrir,
- en termes de procédures nouvelles à identifier, étudier et mettre en place,
- en termes de nouvelles informations à identifier ou à traiter et produire…

Piloter =

- Collecter et synthétiser des informations
- Tester et analyser pour conclure si :
  - Les risques de CI sont correctement traités
  - Les contrôles s'efforcent effectivement à atténuer ces risques



Référentiel CoSO

I.5. Pilotage du SCI (Monitoring)

Continuous Monitoring :

Le pilotage continue implique que la firme s'investit en modalités de testing automatisées, généralement informatisées, mais coûteuses

Separate evaluations

Les évaluations séparées se font via des modalités de testing statistiques ou non statistiques, par échantillonnage, moins efficientes mais moins coûteuses

→ Une combinaison des deux :

Le pilotage le plus efficient combine selon l'importance des procédures les testings automatisés et les testings par échantillonnage.

→ Plus la procédure de CI et les contrôles y rattachés sont importants à la firme, plus leur pilotage devrait s'automatiser.

Le Pilotage se fait à trois niveaux :

- Niveau de la procédure de CI (par le testings des contrôles)
- Niveau de l'activité de la firme (par le pilotage des performances)
- Niveau global de la firme (par le pilotage stratégique).

Chap 2 : « Composantes & principes du CoSO »
Plan

Section 1 : Composantes du CoSO (et du SCI)

1.1 Environnement de contrôle
1.2 Evaluation des risques de CI
1.3 Activités de contrôle (procédures SCI & leurs contrôles)
1.4 Information & communication
1.5 Pilotage du SCI

Section 2 : Principes du CoSO et du SCI

2.1 Principes version 1992 du CoSO 1
2.2 Principes version 2013 du CoSO 1
2.3 Evaluation du SCI par ses principes (matrice soft coso)

Section 3 : Outils de description du SCI

3.1 Manuel de procédures
3.2 Flowcharting

Référentiel CoSO

2.1. Principes du CoSO (version 1992)

- Lorsque les principes énumérés par le CoSO ne sont pas vérifiés/appliqués tout le SCI devient défaillant.
- L'Annexe du chap2 explique quelques principes de l'ancienne version.

COSO'S PRINCIPLES OF INTERNAL CONTROL

1. Integrity and Ethical Values
2. Importance of Board of Directors
3. Management's Philosophy and Operating Style
4. Organizational Structure
5. Commitment to Financial Reporting Competencies
6. Authority and Responsibility
7. Human Resources
8. Importance of Financial Reporting Objectives
9. Identification and Analysis of Financial Reporting Risks
10. Assessment of Fraud Risk
11. Elements of a Control Activity
12. Control Activities Linked to Risk Assessment
13. Selection and Development of Control Activities
14. Information Technology
15. Information Needs
16. Information Control
17. Management Communication
18. Upstream Communication
19. Board Communication
20. Communication with Outside Parties
21. Ongoing Monitoring
22. Separate Evaluations
23. Reporting Deficiencies
24. Management Roles
25. Board and Audit Committees
26. Other Personnel

Référentiel CoSO

2.2. Principes du CoSO I (version 2013)

Environnement de Contrôle	Identification et evaluation des risques	Activités de contrôle	Information and communication	Activité de pilotage
1. Démontrer son engagement envers l'intégrité et les valeurs éthiques	6. Spécifier des objectifs adéquats	10. Sélectionner et développer les activités de contrôle (procédures SCI)	13. Utiliser des informations pertinentes	16. Conduire des évaluations permanentes et/ou séparées
2. Exercer une responsabilité de surveillance	7. Identifier et analyser les risques du SCI	11. Sélectionner et développer les contrôles généraux des technologies	14. Communiquer en interne	17. Evaluer et communiquer les défaillances
3. Etablir : Structure, Autorité et Responsabilité	8. Evaluer le risque de fraude	12. Déployer les activités de contrôle via les politiques et procédures	15. Communiquer en externe	
4. Démontrer son engagement envers la compétence (formations…)	9. Identifier et analyser les changements significatifs			
5. Imposer l'auto-responsabilité de rendre compte				

« Principes du Coso I » (version 2013)
Source : www.coso.org

Ces 17 principes sont utilisés aussi pour l'évaluation du SCI.

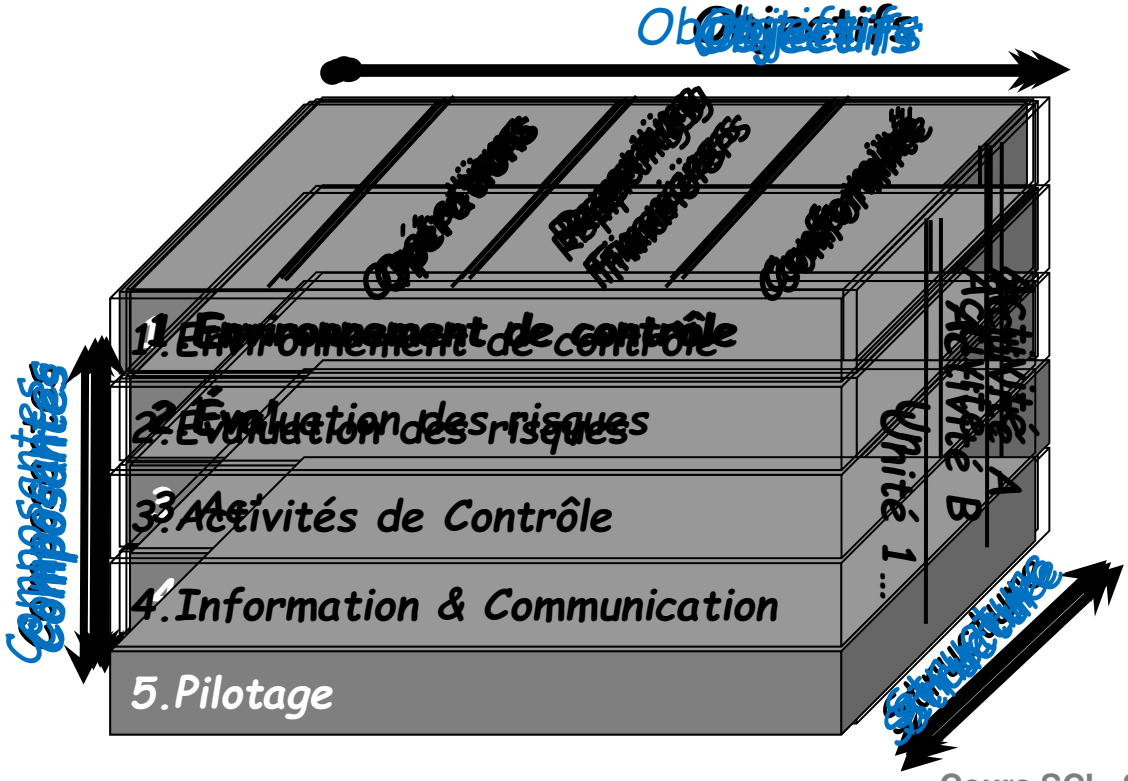
Référentiel CoSO

2.3. Eval du SCI par ses principes

Section 2 : Typologie des risques de CI / CoSO

Activité de pilotage
16. Conduire des évaluations permanentes et/ou séparées
17. Evaluer et communiquer les défaillances

Chaque lot parmi les 17 principes doit être vérifié pour une composante à part du CoSO 1, chaque principe devient une question à poser et à en vérifier l'application.



Référentiel CoSO

2.3. Eval du SCI par ses principes (Soft-CoSO)

Matrice Soft CoSO pour l'évaluation globale des 5 composantes CoSO au sein de SYNOPSIS

Composantes Coso	Les bonnes pratiques : ce qui devrait être :		Etat des lieux en l'entité auditée : ce qui est : réponses de la Direction :	Docs
1. Environnement de contrôle	1.1. Gouvernance (Rôle et implication des organes de gouvernance)	1. Les instances de gouvernance participent régulièrement aux travaux et réunions permettant :	à renseigner suivant les faits vécus par l'entreprise auditée	
		a) Le suivi des performances de la société.		
		b) La compréhension et l'analyse des opérations de l'entité (ponctuelles et régulières) ; leur correcte traduction dans les états financiers.	L'activité est budgétisée par la société mère et est contrôlée par la société mère via des :	
		c) L'évaluation du niveau de compétence et d'expérience des responsables opérationnels et administratifs.	- Rapports mensuels entre Directeur Synonpsis et directeur région Nord Afrique-Europe	Doc 1
		d) Le contrôle de la mise en œuvre des décisions de management.	- Statistiques des ventes des médicaments par région établies par la mère	Doc 2
		e) Le contrôle du respect des règles de gestion interne.	- ...etc...	...
		2. Les instances de gouvernance ont accès aux informations clés (données financières, informations sensibles, etc.) et aux données sensibles (litiges, contentieux, non respect de dispositions légales, ou réglementaires, fraudes, enquêtes en cours,etc.).		
	1.2. Style de Management	1. Le management n'engage pas l'entité dans des opérations risquées, ou seulement après en avoir mesuré dûment les risques. La nature des risques acceptés par le management n'appelle pas de commentaires particuliers.		
		2. Les décisions du management en matière comptable et financière n'appellent pas de commentaires particuliers ;		
	1.5. Engagement de la Direction envers la	1. Le management et les employés (en particulier dans les départements comptables et financiers) disposent des compétences généralement requises	Aucune action de formation n'a été gérée ou prise en charge par Synopsis, sauf le coaching	

IMPACT DE L'ANALYSE PRELIMINAIRE DE L'ENVIRONNEMENT DE CONTROLE SUR LA DEMARCHE D'AUDIT :

Environnement de contrôle satisfaisant, sauf le volet Formations : Risques induits : **Risque comptable** puisque La comptable de Synopsis n'a reçu aucune formation depuis la création de Synopsis et le recrutement de la comptable : les normes établies en Tunisie depuis la date de création Synopsis sont méconnues et donc non appliquées. **Risque "technique"** les médicaments issus du Labo Société mère et qui ont été retirés du marché sont ignorés par Synopsis puisque aucune action de veille n'a été faite en ce sens...

Chap 2 : « Composantes & principes du CoSO »
Plan

Section 1 : Composantes du CoSO (et du SCI)

1.1 Environnement de contrôle
1.2 Evaluation des risques de CI
1.3 Activités de contrôle (procédures SCI & leurs contrôles)
1.4 Information & communication
1.5 Pilotage du SCI

Section 2 : Principes du CoSO et du SCI

2.1 Principes version 1992 du CoSO 1
2.2 Principes version 2013 du CoSO 1
2.3 Evaluation du SCI par ses principes (matrice soft coso)

Section 3 : Outils de description du SCI

3.1 Manuel de procédures
3.2 Flowcharting

Référentiel CoSO

3.1. Manuel des procédures

Voir Exemple en annexe

Référentiel CoSO

3.2. Flowcharting

Voir Exemple en TD