

L'AUDIT COBIT

Toute reproduction interdite



Cécile Pottiez

Auteur : C. Pottiez : cpottieztmim@gmail.com

Utilisation : Reproduction interdite sauf accord préalable.

Document confidentiel à l'intention exclusive des étudiants de Cécile Pottiez

PLANNING – JOUR 4

1. Qu'est-ce que COBIT ?

COBIT (Control Objectives for Information and Related Technologies) est un cadre de gouvernance et de management des systèmes d'information (SI) développé par ISACA.

⌚ Objectif principal :

Aligner l'informatique sur la stratégie de l'entreprise, tout en maîtrisant les risques, la performance et la conformité.

COBIT est utilisé par :

- la direction générale
- les DSI
- les auditeurs
- les responsables risques et conformité

2. Les principes de COBIT (rappel utile)

COBIT repose sur 5 principes fondamentaux :

1. Satisfaire les besoins des parties prenantes
2. Couvrir l'entreprise de bout en bout
3. Appliquer un référentiel intégré
4. Permettre une approche holistique
5. Séparer la gouvernance du management

👉 L'approche *holistique* est celle qui introduit les facilitateurs (enablers).

3. Les facilitateurs COBIT (Enablers)

Les facilitateurs sont les éléments qui permettent à la gouvernance et au management IT de fonctionner efficacement.

COBIT en identifie 7 :

1 Principes, politiques et cadres

- Règles et lignes directrices
- Exemples :
 - politique de sécurité informatique
 - charte IT
 - cadre de gestion des risques

📌 Rôle : donner une direction claire.

2 Processus

- Activités structurées pour atteindre des objectifs
- COBIT définit 40 processus (selon versions), avec leurs interférences (matrice RACI), ex :
 - Gestion des incidents
 - Gestion des changements

○ Gestion des risques IT

📌 Rôle : assurer la cohérence et la répétabilité.

3 Structures organisationnelles

- Rôles et responsabilités
- Exemples :
 - comité IT
 - comité de sécurité
 - DSI, RSSI

📌 Rôle : savoir qui décide quoi.

4 Culture, éthique et comportements

- Valeurs et attitudes des personnes
- Exemples :
 - respect des procédures
 - sensibilisation à la cybersécurité

📌 Rôle : sans bonne culture, les règles ne servent à rien.

5 Information

- Données nécessaires à la gouvernance IT
- Exemples :
 - indicateurs de performance
 - rapports d'audit
 - tableaux de bord

📌 Rôle : permettre la prise de décision.

6 Services, infrastructures et applications

- Outils et technologies
- Exemples :
 - ERP
 - serveurs
 - outils ITSM (ServiceNow, GLPI...)

📌 Rôle : supporter les processus métier.

7 Personnes, compétences et aptitudes

- Ressources humaines
- Exemples :
 - compétences techniques
 - formations
 - certifications

📌 Rôle : avoir les bonnes compétences au bon moment.

4. Facteurs clés de succès (FCS) dans COBIT

Les facteurs clés de succès sont les conditions indispensables pour que COBIT fonctionne efficacement.

Principaux FCS :

1. Soutien de la direction générale
2. Alignement IT / stratégie métier
3. Définition claire des rôles et responsabilités
4. Indicateurs de performance (KPI) pertinents
5. Bonne communication entre IT et métiers

6. Culture de gouvernance et de contrôle

7. Amélioration continue

⚠ Sans ces facteurs, COBIT devient juste un document théorique.

5. Cas pratique : mise en œuvre de COBIT

Contexte

Une banque subit :

- des pannes fréquentes de son système informatique
- des incidents de sécurité
- un manque de visibilité pour la direction

🎯 Objectif : améliorer la gouvernance IT et réduire les risques

Étape 1 : Identification des besoins

- Disponibilité élevée des systèmes
- Sécurité des données clients
- Conformité réglementaire

➡ Principe COBIT : *satisfaire les besoins des parties prenantes*

Étape 2 : Mise en place des facilitateurs

✓ Processus

- Mise en place des processus COBIT :
 - Gestion des incidents
 - Gestion des risques IT
 - Gestion de la continuité

✓ Structures organisationnelles

- Crédation d'un comité de gouvernance IT
- Nomination d'un RSSI

✓ Principes et politiques

- Politique de sécurité
- Politique de gestion des accès

✓ Information

- Tableaux de bord :
 - taux de disponibilité
 - nombre d'incidents
 - incidents critiques

✓ Personnes et compétences

- Formation du personnel IT
 - Sensibilisation des employés aux risques cyber
-

Étape 3 : Facteurs clés de succès appliqués

- Engagement fort de la direction
 - Indicateurs suivis mensuellement
 - Communication régulière entre IT et métiers
-

Résultats obtenus

- ✓ Réduction des incidents
 - ✓ Meilleure disponibilité des systèmes
 - ✓ Meilleure conformité réglementaire
 - ✓ Décisions IT basées sur des indicateurs fiables
-

6. Conclusion synthétique

- COBIT est un cadre de gouvernance IT
- Les facilitateurs sont les leviers d'action
- Les facteurs clés de succès garantissent l'efficacité
- Le cas pratique montre comment COBIT transforme la gestion IT

Introduction - COBIT - Quelques vidéos

Vidéo Le pentagone de COBIT <https://www.youtube.com/watch?v=N8Zwuz13N20>

Vidéo Présentation du document COBIT 4.1 <https://www.youtube.com/watch?v=5QDhcImNASo>

Vidéo CoBIT c'est quoi ?

https://www.google.com/search?sa=X&sca_esv=760e5d65b7c9552a&udm=7&fb=AlljpHx4nJifGojPVHhEACUHPiMQ_p_bq5bWizQs3A_klenitcpTTqBUdyVgzq0c3_k8z34EAuM72an33IMW6RWde9ePJpwNFtZw3UQvFloZy04_0a7Y_s9Q2prhO8GUp_RabNoWBXexBhzeXMQIUILLh2ARDDTV-nnosywhVrODAUve9aakXHuWS74Aezq_NwMv3Fi27KqMhoaWfXUAe78fv--Srzwq&q=cobit+2019&ved=2ahUKEwi6rt3S4PmRAxVQoScCHeE4lucQtKqLegQIDxAB&biw=1578&bih=735&dpr=1#fpst=ate=ive&ip=1&vld=cid:daec4fd1,vid:FL3qixG5vUc,st:0

Question : Résumer ces vidéos pour comprendre COBIT en général. Faites une explication.

https://www.youtube.com/watch?v=uomItoaDdiQ&list=PL73WzVfh2gWmTod3RIdDCWSm_Xw9Ps_4W

<https://www.youtube.com/watch?v=W1BP4qJhdoE>

Question : Pour comprendre le détail de COBIT maintenant ; Qu'entend-on par goals cascade, Qu'est-ce que les enablers (facilitateurs/facteur clé de succès), quels sont-ils ? Quelles sont les pratiques de gestion clé ? Lister les (tableau). Lister les exigences. Lister les key metrics (tableau). Qu'est-ce qu'une scorecard ?

<https://ab-audit.com/utiliser-itil-et-cobit-2019-pour-un-cadre-it-integre/>

<https://www.isaca.org/resources/news-and-trends/industry-news/2017/applying-the-goals-cascade-to-the-cobit-5-principle-meeting-stakeholder-needs>

CAS DIGITEX

L'entreprise DIGITEX, spécialisée dans le commerce en ligne, connaît depuis plusieurs mois des difficultés liées à son système d'information :

- Pannes fréquentes de la plateforme e-commerce
- Retards dans le traitement des commandes
- Incidents de sécurité (accès non autorisés)

- Absence d'indicateurs fiables pour la direction
- Manque de coordination entre les équipes IT et métiers

La direction souhaite mettre en place un cadre de gouvernance IT afin d'améliorer la performance, la sécurité et l'alignement du SI avec la stratégie de l'entreprise.

QUESTIONS

1. Identifier le cadre de gouvernance IT le plus adapté et justifier le choix.
2. Expliquer trois principes COBIT applicables à ce contexte.
3. Identifier et expliquer quatre facilitateurs (enablers) COBIT à mettre en œuvre chez DIGITEX.
4. Identifier trois facteurs clés de succès pour la réussite de COBIT dans cette entreprise.
5. Proposer un plan d'actions simplifié basé sur COBIT pour améliorer la situation.