

# L'atout d'un CGEIT pour votre organisation



# Les conférenciers

Amadou BA, MBA, PMP, CGEIT, COBIT 2019  
Conseiller Principal Performance TI  
Conseiller Recherche et Communications ISACA - Section de  
Québec



Arnaud FANKAM, PMP, CISM, CRISC, CGEIT  
Conseiller Senior en Sécurité COFOMO  
Directeur Recherche et Communications ISACA - Section de Québec



# Objectifs de la présentation

A la fin de cette présentation, le participant sera en mesure :

- d'identifier les cadres de gouvernance TI,
- de reconnaître les missions d'un CGEIT en entreprise,
- d'avoir un aperçu des connaissances requises pour mener à bien ses missions
- d'exploiter ce document comme base pour approfondir ses connaissances en gouvernance TI.

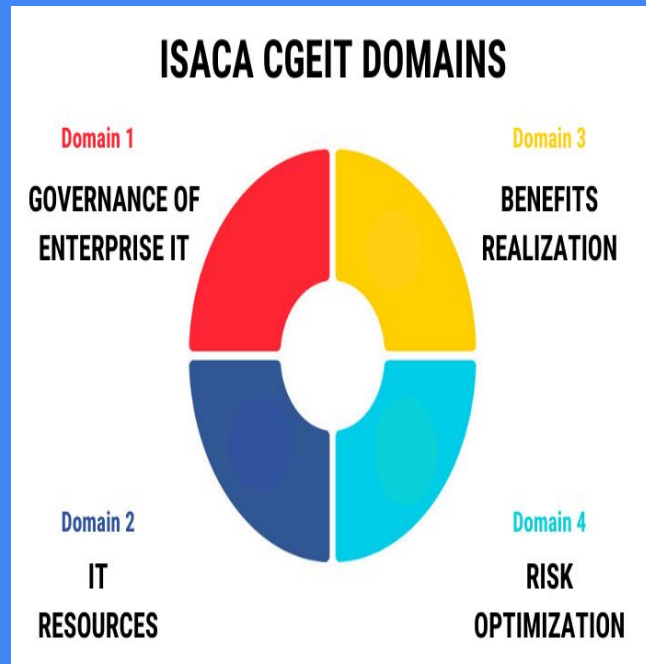


# Introduction

La structure de gouvernance précise la répartition des droits et des responsabilités entre les différents participants : le conseil, les dirigeants, les actionnaires et les autres parties prenantes. Elle fixe les paramètres de la gestion et de la direction de l'entreprise. Elle définit les buts, les objectifs, la culture et les valeurs organisationnelles, tout en énonçant les règles et les procédures pour la prise de décisions de gestion.

La gouvernance encadre l'établissement des objectifs et des moyens de les atteindre. Elle définit les indicateurs de performance clés et les objectifs principaux, et établit un processus pour accélérer l'obtention de résultats et apporter les changements nécessaires.

La gouvernance informatique quant à elle veille à ce que les ressources TI soient employées efficacement de façon à augmenter la valeur de l'entreprise et à favoriser la réalisation de sa mission et de sa vision.



# Partie 1 : Présentation du CGEIT



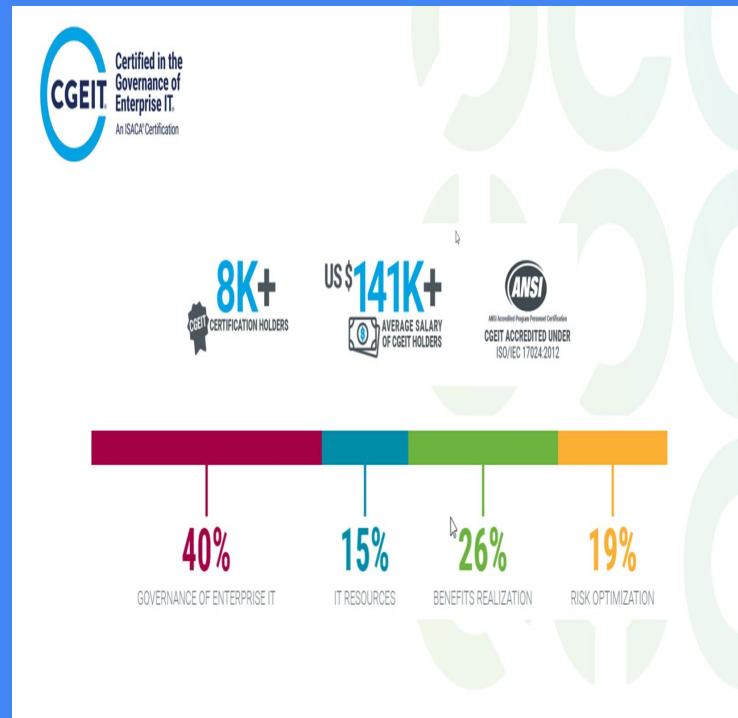
# Qu'est ce qu'un CGEIT ?

Certification en Gouvernance des technologies et de l'information d'entreprise (CGEIT)

C'est la certification de gouvernance de l'information et des technologies décernée par l'ISACA, qui peut vous donner l'état d'esprit nécessaire pour évaluer, concevoir, mettre en œuvre et gérer des systèmes de gouvernance de l'information et des technologies d'entreprise qui soient alignés sur les objectifs d'affaires globaux.

La certification CGEIT valide les compétences individuelles dans 4 domaines clés:

- Gouvernance d'entreprise des technologies et de l'information,
- Gestion des ressources des technologies et de l'Information,
- Réalisation des bénéfices,
- Optimisation des risques.



# Quels sont les prérequis pour être CGEIT ?

- Réussir l'examen CGEIT
- Faire la preuve de 5 ans d'expérience en Gouvernance des technologies et de l'information
- Adhérer au code d'éthique de l'ISACA

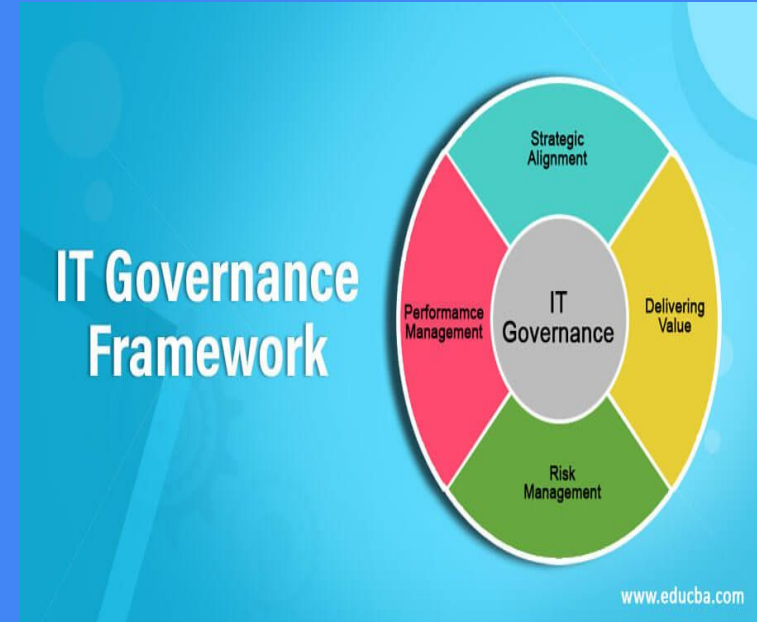


# Cadres de gouvernance TI

Parmi les cadres de gouvernance de l'informatique d'entreprise, on peut citer :

- **AS/NZS 8016:2013** - Governance of IT enabled Projects (Publié en 2013 et basé sur ISO/IEC 38500:2008),
- **ISO/IEC 38502:2014** - Governance of IT -- Cadre et modèle,
- **ISO/IEC TS 38501:2015** - Governance of IT -- Guide d'implémentation,
- **COBIT 5** aujourd'hui remplacé par **COBIT 2019**, cadre de gouvernance de l'ISACA le plus répandu et le mieux exploité dans la gouvernance de l'informatique d'entreprise. C'est le cadre de référence pour le CGEIT.

PS: Il est de bon ton de préciser que contrairement à ce que beaucoup peuvent penser, **ITIL** n'est pas un cadre de gouvernance de l'informatique d'entreprise mais plutôt un cadre de gestion de l'informatique d'entreprise.





# Partie 2 : Missions d'un CGEIT en entreprise



# Gouvernance informationnelle d'entreprise

Pour mettre en place une gouvernance efficace, le CGEIT doit:

- Établir les objectifs du cadre de gouvernance des TI d'entreprise,
- Établir un cadre pour la gouvernance de l'informatique d'entreprise,
- Identifier les exigences internes et externes du cadre de gouvernance de l'informatique d'entreprise,
- S'assurer qu'un processus d'élaboration d'une analyse de rentabilité et de réalisation des bénéfices pour les investissements liés aux TI a été mis en place,
- Intégrer l'architecture de l'information dans le cadre de la gouvernance de l'informatique d'entreprise,
- Établir les rôles, les responsabilités et les obligations de rendre compte pour les actifs informationnels et les processus informatiques,
- Mettre en place un processus d'identification et de résolution des problèmes liés au cadre de gouvernance de l'entreprise,
- Évaluer, diriger et contrôler l'engagement des parties prenantes.



# Gestion des ressources informationnelles

Pour mettre en place une Gestion des RI efficace, le CGEIT doit:

- Veiller à ce qu'un processus d'élaboration d'analyses de rentabilité et de réalisation des avantages pour les investissements dans les TI soit mis en place,
  - Établir les rôles, les responsabilités et les obligations de rendre compte pour les actifs informationnels et les processus informatiques,
  - S'assurer que des processus sont en place pour gérer le cycle de vie des ressources et actifs informationnels et des capacités informatiques,
  - Intégrer des stratégies d'approvisionnement dans le cadre de la gouvernance de l'informatique d'entreprise afin de garantir l'optimisation et le contrôle,
- 
- Assurer l'alignement des processus de gestion des ressources informatiques avec la gestion des ressources de l'entreprise.
  - Veiller à ce que des processus soient en place pour l'évaluation et le développement du personnel afin de répondre aux besoins de l'entreprise,
  - Établir un programme de gestion du rendement pour les investissements axés sur la TI, les processus et les services de TI.



# Réalisation des bénéfices

Au sein d'une entreprise, afin de contribuer à la réalisation des bénéfices, le CGEIT doit être en mesure de :

- Veiller à ce que les investissements informatiques soient gérés comme un portefeuille d'investissements,
- Veiller à ce que les investissements informatiques soient gérés tout au long de leur cycle de vie économique pour obtenir des avantages commerciaux,
- S'assurer que la propriété et la responsabilité de l'entreprise pour les investissements informatiques sont établies et que les pratiques de gestion des investissements informatiques s'alignent sur les pratiques de gestion des investissements de l'entreprise,
- Veiller à ce que les portefeuilles d'investissement, les processus informatiques et les services informatiques soient évalués et comparés afin d'obtenir des avantages commerciaux,
- Veiller à ce que les résultats et les mesures de performance soient établis et évalués pour évaluer les progrès vers la réalisation des objectifs de l'entreprise et des TI,
- Veiller à ce que les mesures des résultats et du rendement soient surveillées et signalées en temps opportun,
- Veiller à ce que les initiatives d'amélioration soient définies, priorisées, lancées et gérées en fonction des résultats et des mesures de performance.



# Optimisation des risques

Pour ce qui est de l'optimisation des risques, les missions qui incombent au CGEIT sont les suivantes :

- Veiller à ce que des processus complets de gestion des risques informatiques soient établis pour identifier, analyser, atténuer, gérer, surveiller et communiquer les risques informatiques,
- Veiller à ce que les exigences de conformité légales et réglementaires soient traitées par le biais de la gestion des risques informatiques,
- Veiller à ce que la gestion des risques informatiques soit alignée sur le cadre de gestion des risques de l'entreprise,
- Assurer le parrainage approprié de la haute direction pour la gestion des risques informatiques,
- Veiller à ce que les politiques, procédures et normes de gestion des risques informatiques soient élaborées et communiquées,
- Assurer l'identification des principaux indicateurs de risque,
- Assurer un signalement en temps opportun et une escalade appropriée des événements à risque et des réponses aux niveaux de gestion appropriés.



# Partie 3 : Connaissances requises au CGEIT pour l'atteinte des objectifs



# Connaissances requises pour la gouvernance informatique

Pour mener à bien la gouvernance informatique, le CGEIT doit connaître :

- les composants d'un cadre pour la gouvernance de l'informatique d'entreprise,
- les pratiques, normes et cadre de l'industrie de la gouvernance informatique,
- les méthodes pour gérer le changement organisationnel, de processus et culturel,
- les moteurs d'activité liés à la gouvernance informatique,
- les catalyseurs de gouvernance informatique,
- les techniques utilisées pour identifier la stratégie informatique,
- composants, principes, cadres et concepts liés à l'architecture d'entreprise,
- les modèles et méthodes pour établir la responsabilité des besoins en informations, de la propriété des données et des systèmes et des processus informatiques,
- les processus/mécanismes de surveillance de la gouvernance informatique,
- les processus/mécanismes de reporting de gouvernance informatique,
- les structures organisationnelles et leurs rôles et responsabilités,



# Connaissances requises pour la gouvernance informatique (Suite)

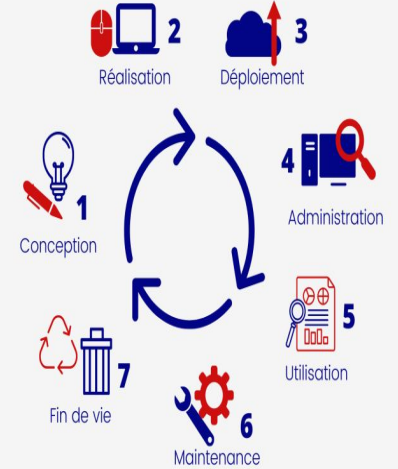
- les techniques de communication et de promotion,
- les méthodologies et techniques d'assurance,
- le plan stratégique d'une entreprise et son lien avec l'informatique,
- les processus et techniques de planification stratégique.
- l'impact du changement de stratégie commerciale sur la stratégie informatique,
- les obstacles à la réalisation de l'alignement stratégique,
- les politiques et procédures nécessaires pour soutenir l'alignement de la stratégie informatique et commerciale,
- les méthodes pour documenter et communiquer les processus de planification stratégique informatique (par exemple, tableau de bord informatique / tableau de bord prospectif, indicateurs clés),
- les technologies actuelles et futures,
- les processus de priorisation liés aux initiatives informatiques,
- la portée, objectifs et avantages des programmes d'investissement en TI,
- les rôles et responsabilités informatiques et méthodes pour transmettre les objectifs ,commerciaux et informatiques au personnel informatique.





# Connaissances requises pour la gestion des ressources informationnelles

- Stratégies d'approvisionnement TI,
- Planification de la capacité des ressources TI,
- Acquisition des ressources TI,
- Cycle de vie des ressources IT et Gestion des actifs TI,
- Gestion des ressources humaines et du personnel TI,
- Gestion des relations avec les fournisseurs.



# Connaissances requises pour la réalisation de bénéfices

Afin de mener à bien cette mission, le CGEIT doit posséder des acquis sur les :

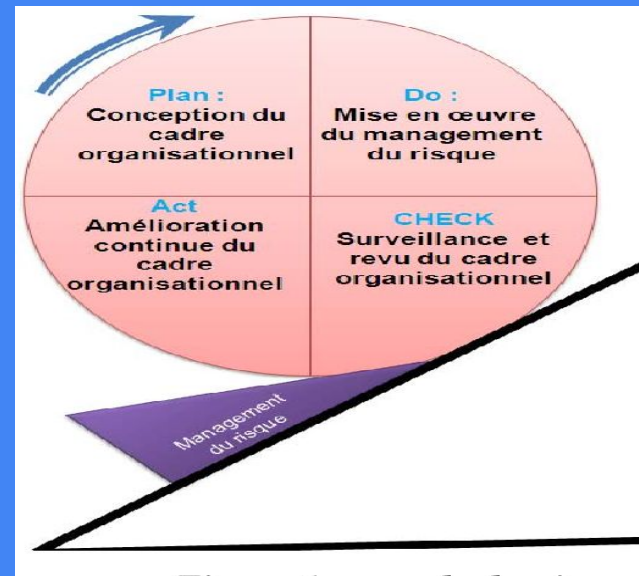
- Processus et pratiques de planification, de développement, de transition, de livraison et de support des solutions et services informatiques,
- Techniques de mesure des processus et des services (par exemple, modèles de maturité, benchmarking, indicateurs de performance clés),
- Processus de gestion des investissements informatiques, y compris le cycle de vie économique des investissements,
- Techniques de calcul des avantages (valeur acquise, coût total de possession, retour sur investissement),
- Stratégies d'optimisation des coûts (par exemple, externalisation, adoption de nouvelles technologies),
- Techniques de mesure des résultats et des performances (par exemple, métriques de service, KPI),
- Modèles et méthodes pour établir la responsabilité des investissements informatiques,
- Procédures pour gérer et rendre compte de l'état des investissements informatiques,
- Techniques d'élaboration et d'évaluation d'analyse de rentabilisation,
- Cadres de livraison de valeur (par exemple, Val IT),
- Principes de base de la gestion de portefeuille,
- Concepts et principes d'amélioration continue.



# Connaissances pour l'optimisation des risques

Pour remplir cette mission, les connaissances du CGEIT doivent s'étaler sur :

- les types de risques commerciaux, d'expositions et de menaces (par exemple, environnement externe, environnement interne, sécurité de l'information) qui peuvent être traités à l'aide de ressources informatiques,
- l'application de la gestion des risques aux niveaux stratégique, portefeuille, programme, projet et opérations,
- la relation entre l'approche de gestion des risques et la résilience de l'entreprise (par exemple BCP, DRP),
- la relation entre l'approche de gestion des risques et la conformité légale et réglementaire,



# Connaissances pour l'optimisation des risques (suite)

- les risques, menaces, vulnérabilités et opportunités inhérents à l'utilisation de l'informatique,
- les méthodes de surveillance de l'efficacité des stratégies d'atténuation et/ou des contrôles,
- les cadres et normes de gestion des risques (par exemple, Risk IT, COSO ERM, ISO 31000),
- les stratégies d'atténuation des risques liés à l'informatique dans l'entreprise,
- les méthodes d'alignement de l'informatique à la gestion des risques d'entreprise,
- les méthodes quantitatives et qualitatives d'évaluation des risques,
- l'analyse des parties prenantes et les techniques de communication,
- les méthodes de gestion et de notification de l'état du risque identifié,
- les méthodes de conception des indicateurs clés de risque (KRI),
- l'appétit et la tolérance aux risques d'entreprise.

# Conclusion

Les professionnels certifiés CGEIT (Certified in the Governance of Enterprise IT) de l'ISACA peuvent améliorer la valeur stratégique qu'ils apportent aux organisations.

Ils apportent les connaissances et l'expérience nécessaires pour aligner l'informatique sur les stratégies et les objectifs de l'entreprise, gérer les investissements informatiques pour maximiser le retour sur investissement et rechercher l'excellence dans les opérations et la gouvernance informatiques tout en minimisant les risques.

# Références

<https://www.isaca.org/credentialing/cgeit> Review manual 7th and 8th Edition

[https://fr.wikipedia.org/wiki/Information\\_Technology\\_Infrastructure\\_Library](https://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library)

MERCI

Q&A

