ISACA®
Trust in, and value from, information systems

COBIT® 5
RETOURS D'EXPÉRIENCES

Alain Bonneaud

CGEIT® - COBIT® - ITIL® - RESILIA® - ISO 27001 – ISO 20000 - ISO 22301 – Lean IT – PRINCE2®

AB Consulting
Conseil en Gouvernance IT

12 Avril 2016

CAS N°1
IMPLÉMENTATION

Contexte

- Munich (Bavière – Allemagne)
- Période : Janvier 2012 - …
- Secteur financier (Banque)
- Contexte économique
  - Economie forte
  - Taux de chômage faible (de l'ordre de 2%)
  - Contexte bancaire
- Lois et réglementations applicables
  - Europe / Allemagne / Bavière
  - Réglementation bancaire
- Etique, Culture et comportement
- Pratiques de l'industrie

Le contexte de la Banque

- Environ 1000 employés – DSI environ 120 personnes
- Joint-venture entre deux grandes institutions bancaires Européennes
- Ethique et culture
  - Multi-culturel (près de 20 nationalités)
  - Pas de communication entre DSI et métiers
- Mission, vision, valeurs
  - Différences profondes de vision entre les deux associés
- Stratégie des métiers de la banque
- Modèle d'opération
  - Deux Directeurs Généraux
  - Organisation en silos
- Style de Management (DSI, Métiers)
- Appétit du risque
- Aptitudes et ressources disponibles

L'origine de l'initiative de GRC

- Audit réalisé à la demande d'un des deux associés (à la demande du Groupe)
  - Audit externe réalisé par l'Inspection Générale
  - Périmètre : Gouvernance du SI
    - Une douzaine de processus TI au niveau 1
    - Organisation
    - Système de Gouvernance
    - Politiques, système de management
    - Reporting et monitoring
    - Ressources humaines
    - Informations / Sécurité
  - Equipe d'audit : 7 personnes – 4 mois (07/09/11 – 28/11/11)

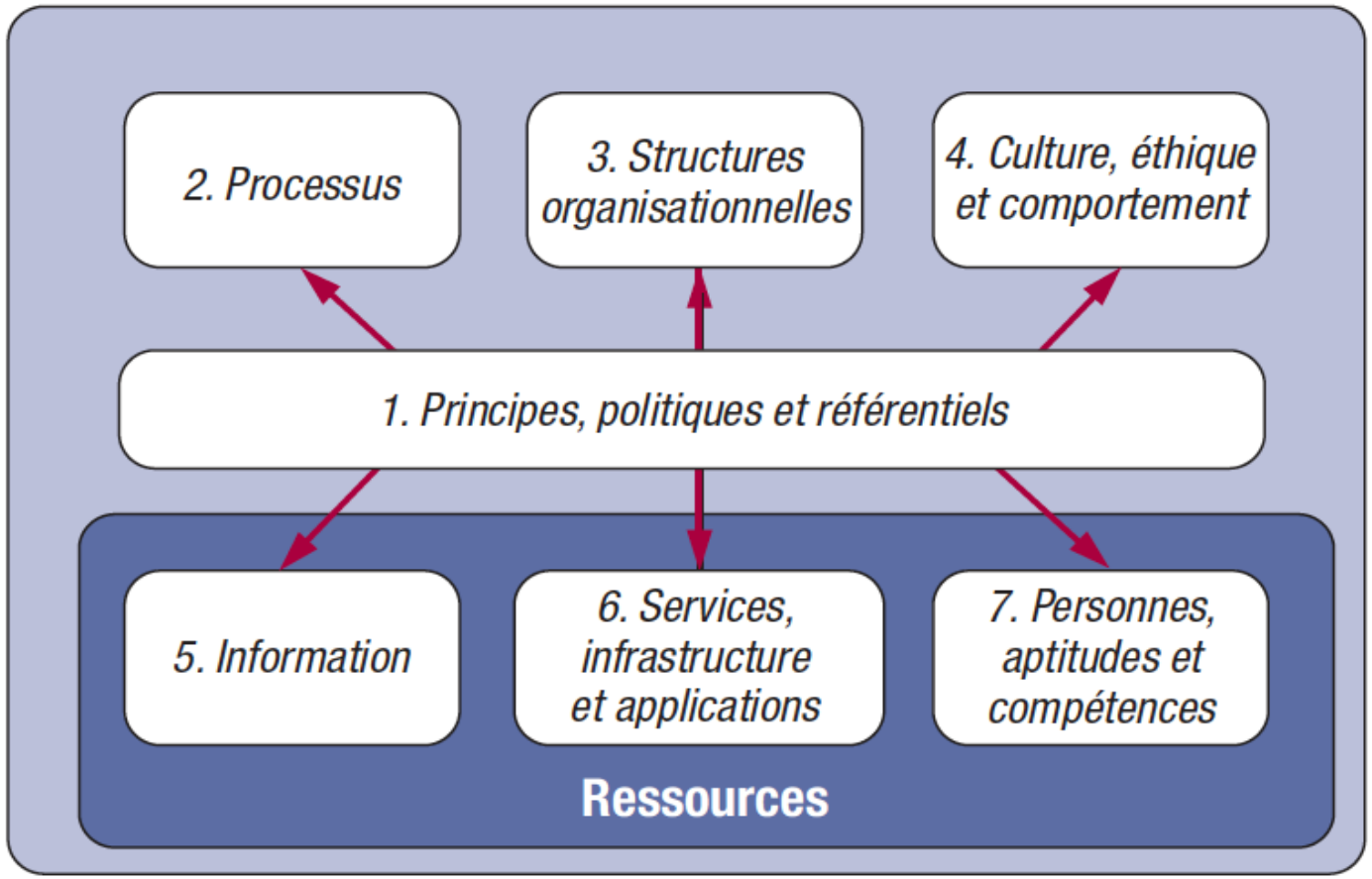
L'événement déclencheur

- Résultats de l'audit
  - 33 problèmes importants identifiés
    - 5 classés à risque critique
    - 23 classés à risque moyen
    - 5 relatifs à l'efficience
  - 38 recommandations à implémenter
    - 1 avant 29/02/2012
    - 5 avant 31/03/2012
    - 1 avant 31/05/2012
    - 17 avant 30/06/2012
    - 9 avant 30/09/2012
    - 5 avant 31/12/2012

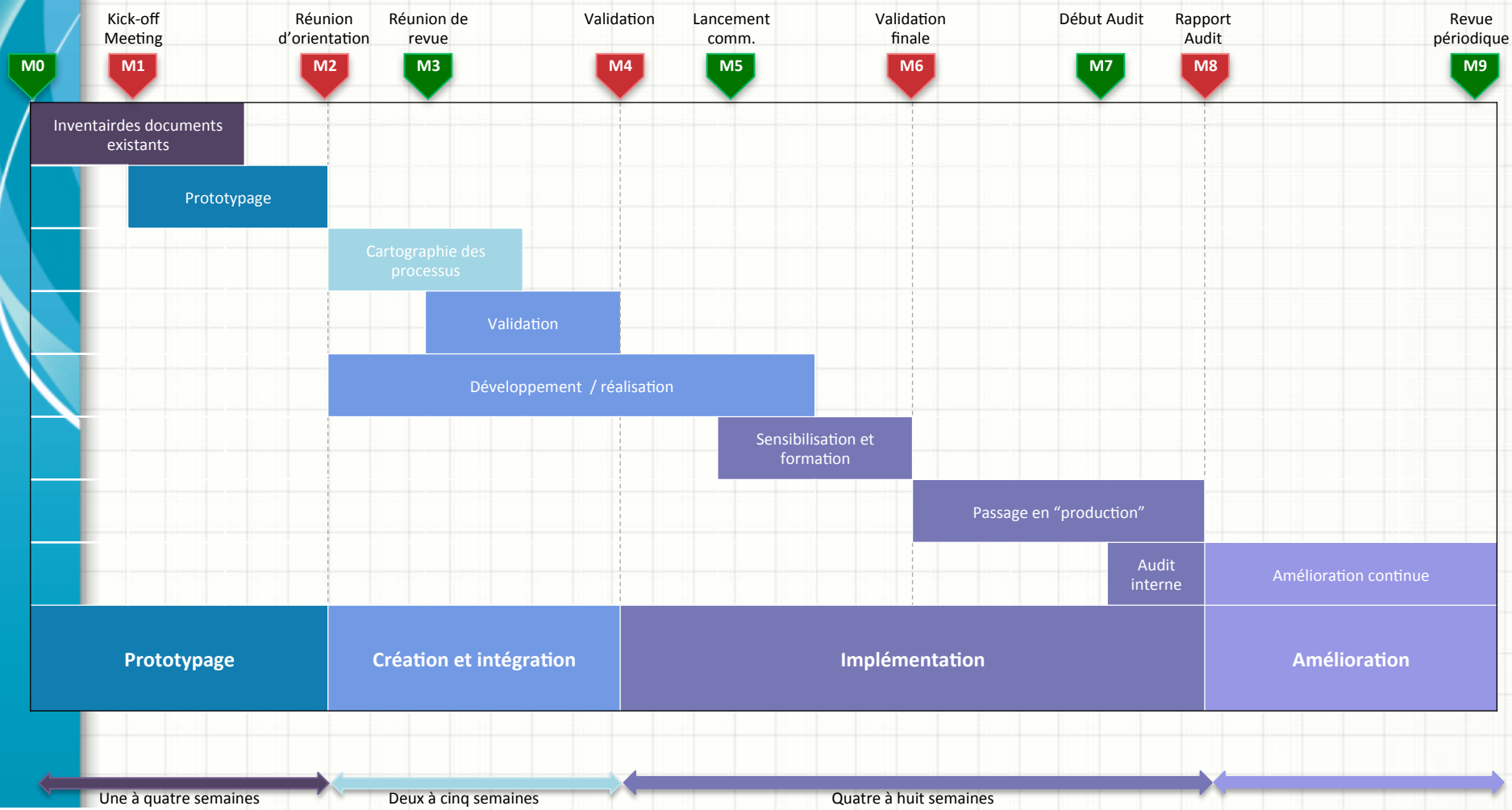
Résultats et recommandations

- Implémentation / Amélioration exigée de 10 processus
  - Gestion des incidents
  - Gestion des problèmes
  - Gestion des changements (2 recommandations)
  - Gestion de la capacité et de la performance
  - Gestion des niveaux de service
  - Gestion des projets et des programes (2 recommandations)
  - Gestion de la sécurité
  - Gestion des configurations(2 recommandations))
  - Gestion de la sécurité (8 recommandations)
  - Gestion des déploiements (non explicite)
- L'implémentation et l'amélioration des processus est un prérequis pour les autres recommandations (Contrôle, reporting, monitoring, Gouvernance …)

Les 7 axes de l'initiative (facilitateurs)



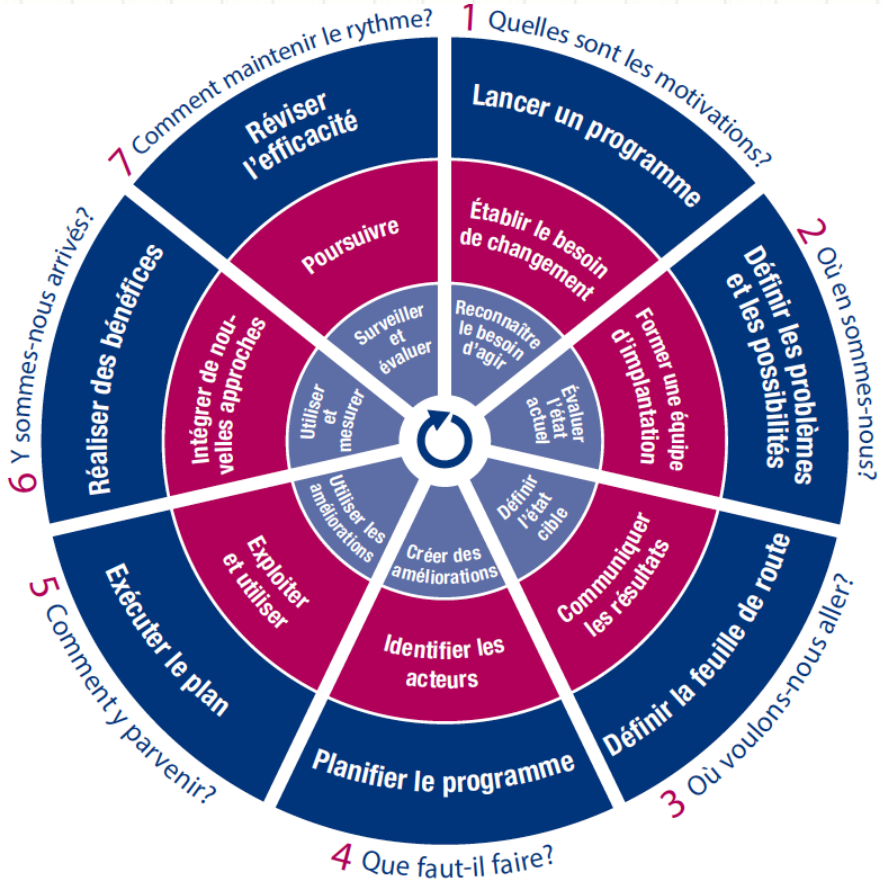
Approche proposée



Facteurs clés de succès

- Direction, mandat et engagement fort donnés par les deux Directeurs Généraux
- Compréhension par les métiers et les TI des enjeux, objectifs et contraintes liés à la Gouvernance du SI
- Communication efficace et facilitation du changement
- Ne jamais mentionner COBIT® mais **s'appuyer sur COBIT®** pour amener les parties-prenantes à concevoir leur propres facilitateurs
- Priorisez sur la base de « quick-wins » en commençant par ce qui est facile et visible

L'approche d'implémentation



- **Gestion du programme** *(anneau externe)*
- **Moteur de changement** *(anneau du milieu)*
- **Approche d'amélioration continue** *(anneau interne)*

Conclusion

- Ce n'est pas une initiative « court-terme » !!!
  - Plusieurs années sont nécessaires pour une mise en œuvre significative
  - Chaque cycle doit être limité en ambition et en délai
    - 6 mois maximum
- Ne jamais perdre de vue que l'objectif central de l'Organisation est de créer de la valeur grâce à ses métiers de base
  - Les priorités métiers doivent être évaluées en permanence
- Mettre l'accent sur la communication et la facilitation du changement
  - Vital pour le succès
- Rester « lite » et « agile »
  - Rester cohérent avec la taille de l'Organisation
  - Ne pas construire une « cathédrale » mais s'assurer que l'innovation par les métiers reste au centre des préoccupations
- Ne pas « ré-inventer la roue »
- Ne pas imposer des bonnes pratiques venues d'ailleurs mais s'appuyer sur ces bonnes pratiques et les adapter pour construire sur les forces de l'organisation
- Capitaliser en permanence sur la réussite d'objectifs à court terme et obtenir le « buy-in » du personnel de l'Organisation
  - Attention à ne pas créer de frustrations
- L'engagement fort de la Direction est clé pour la réussite à moyen et long terme !!!!

Questions / Réponses

CAS N°2
AUDIT DE RISQUES

Contexte

- Ile des Caraïbes
- Période : Mai – Juillet 2015
- Opérateur télécom
- Contexte économique
  - Economie forte
  - Taux de chômage faible
  - Opérateur historique
- Lois et réglementations applicables
  - Nationale, internationale
  - Réglementation Telcos
- Ethique, Culture et comportement
  - Syndicats puissants
- Pratiques de l'industrie
  - Concurrence forte
  - Opérateurs bien structurés et organisés

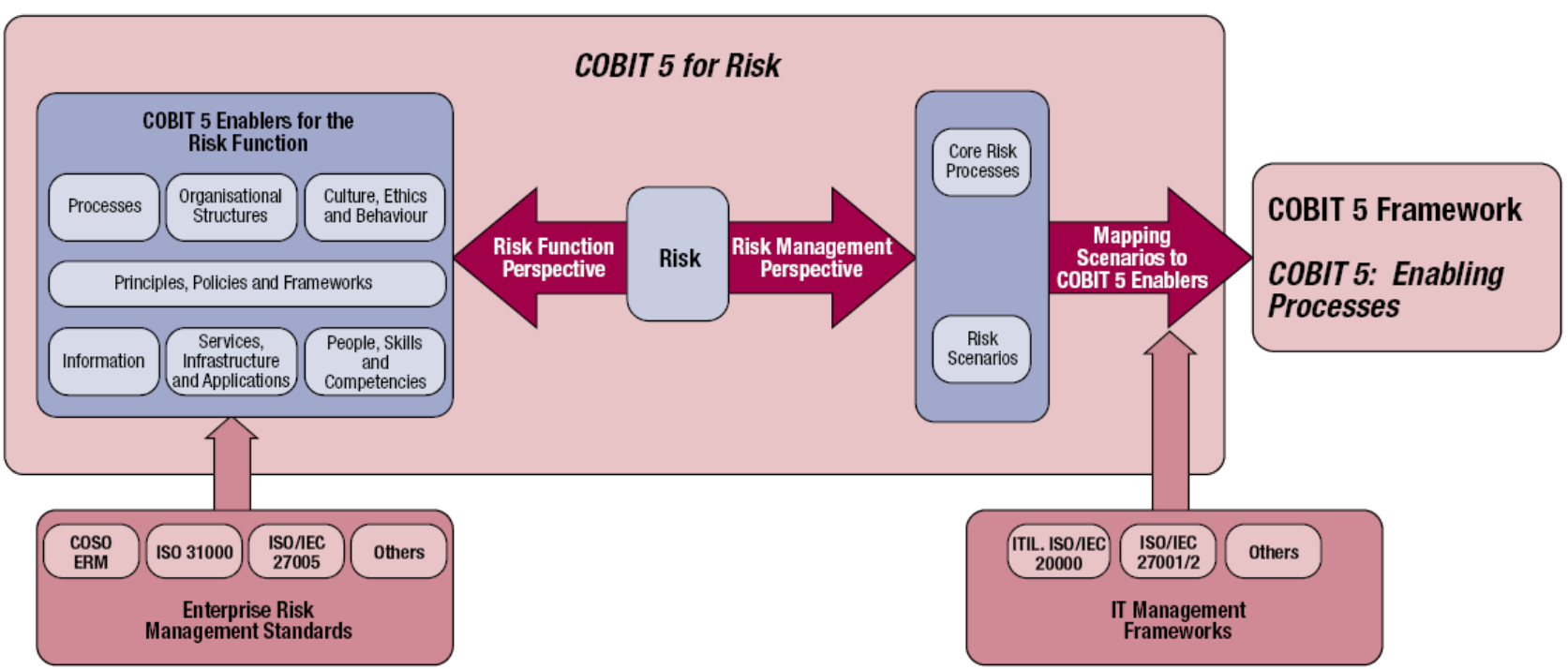
Le contexte de l'Entreprise

- Environ 1000 employés – Une centaine de personnes à la DSI
- Deux actionnaires : Etat + Une société de téléphonie privée obligée de se retirer du capital
- Ethique et culture
  - Culture très « sociale »
  - Peu de communication entre DSI et métiers
- Mission, vision, valeurs
  - Différences profondes de vision entre les deux actionnaires
- Stratégie de survie dans un monde concurrentiel
  - Fin du monopole
  - Portabilité du numéro
  - Réduction des coûts (plan social)
- Modèle d'opération
  - Comité exécutif « faible »
  - Organisation en silos
- Style de Management (DSI, Métiers)
- Appétit du risque
- Aptitudes et ressources disponibles

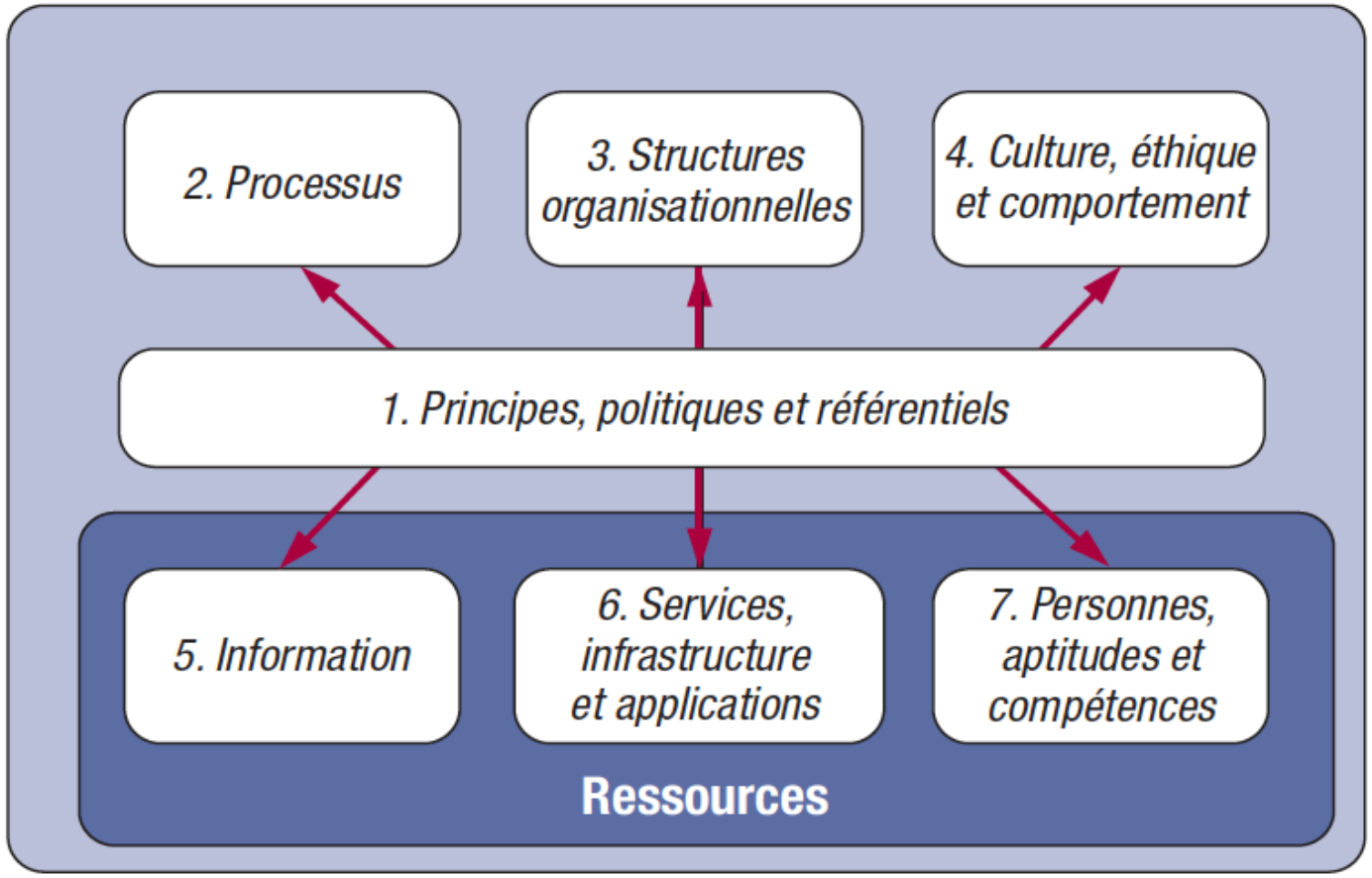
L'origine de l'initiative

- Audit réglementaire réalisé annuellement par le cabinet Ernst & Young
  - Exigence d'avoir un audit des risques du SI
  - Choix de COBIT® 5 par le comité d'audit de l'Entreprise
  - Périmètre : Gouvernance & Gestion des risques du SI
    - Deux processus centraux au niveau 1 minimum (EDM03 et APO12)
    - Autres processus induits (notamment gestion de la sécurité APO13)
    - Organisation
    - Système de Gouvernance
    - Politiques, système de management
    - Reporting et monitoring
    - Ressources humaines
    - Informations / Sécurité
  - Equipe d'audit : 2 personnes – 2mois (Mai-Juin 2015)

La perspective Risques selon COBIT® 5



La perspective des risques vue par COBIT®



COBIT 5 for Risk fournit des lignes directrices sur la façon dont chaque facilitateur contribue à la gouvernance et à la gestion du risque global d'Entreprise.

Perspective de gestion des risques

- Quels **Processus** il est nécessaire de définir et d'optimiser pour soutenir la fonction risque, gouverner et gérer les risques au sein de l'Entreprise,
- Quels **Flux d'information** doivent exister pour gouverner et gérer le risque (univers de risque, profils de risque)
- Quelles **Structures organisationmelles** sont nécessaires pour gouverner et gérer le risque efficacement (Enterprise Risk Committee, Fonction Risque)
- Quels **Personnels et avec quelles compétences** doivent être désignés pour établir et opérer une fonction risque efficace

Perspective de gestion des risques

COBIT 5 Process Identification	Reasoning
EDM03 Ensure Risk Optimisation	This process covers the understanding, articulation and communication of the enterprise risk appetite and tolerance and ensures identification and management of risk to the enterprise value that is related to IT use and its impact. The goals of this process are to: • Define and communicate risk thresholds and make sure that key IT-related risk is known. • Effectively and efficiently manage critical IT-related enterprise risk. • Ensure IT-related enterprise risk does not exceed risk appetite.
APO12 Manage Risk	This process covers the continuous identification, assessment and reduction of IT-related risk within levels of tolerance set by enterprise executive management. Management of IT-related enterprise risk should be integrated with overall ERM. The costs and benefits of managing IT-related enterprise risk should be balanced by: • Collecting appropriate data and analysing risk • Maintaining the risk profile of the enterprise and articulating risk • Defining the risk management action portfolio and responding to risk

COBIT 5 for Risk fournit des conseils spécifiques pour chacun des facilitateur afin de gérer efficacement le risque:

- Les processus clés **de Gestion des risques** nécessaire à l'implémentation efficace et efficiente d'une gestion des risques d'Entreprise permettant de créer de la valeur pour les parties-prenantes de l'entreprise
- **Des scénarios de risque concrets, tangibles et mesurables de représenation du risque** , (c-a-d les éléments d'information clés nécessaires à l'identification, l'analyse et la réponse au risque) et comment les facilitateurs de COBIT® 5 permettent de répondre efficacement aux risques correspondants

Drivers pour la gestion des risques

Les principaux drivers pour la gestion des risques incluent la fourniture:

- Aux parties-prenantes, d'avis argumentés et cohérents sur le niveau courant du risque auquel est exposée l'Entreprise
- De conseils sur comment maintenir les risques dans le cadre acceptable de l'appétit du risque de l'Entreprise
- De conseils sur comment créer une culture de gestion des risques dans l'Entreprise
- Si possible, des évaluations quantitatives des risques permettant aux parties-prenantes de prendre une décision sur la nécessité de mettre en place un plan de réponse

Pour atteindre ces objectifs, la publication **COBIT 5 for *Risk*** fournit:

- Des conseils sur l'utilisation de COBIT® 5 pour soutenir l'établissement de la Gouvernance et de la Gestion du risque dans l'Entreprise
- Des conseils et une approche structurée sur l'utilisation des principes et des facilitateurs de COBIT® 5 pour Gouverner et Gérer les risques liés au SI
- Une compréhension claire de l'alignement de **COBIT 5 for Risk** avec les autres cadres existants

Qui peut bénéficier de COBIT® 5 pour la gestion des risques?

- Les professionnels du risques dans l'Entreprise
  - Aide pour intégrer le risque lié au SI au système global de gestion des risques dans l'Entreprise
- Conseils d'Administration et Comités de Direction:
  - Compréhension claire de leurs rôles et respondabilités en matière de risque dans l'Entreprise, notamment en matière de conformité
  - L'implication des risques liés au SI sur les objectifs stratégiques de l'Organisation
  - Comment optimiser l'utilisation du SI pour mieux réussir l'exécution de la stratégie d'Entreprise
- Gestionnaires IT et métiers:
  - Comprendre comment identifier et gérer le risque TI et communiquer sur ce sujet avec les décisionnaires

Evaluation d'aptitude de processus

Basée surCOBIT® 5

1 – Démarrage

2 – Planification de l'évaluation

3 – Instructions

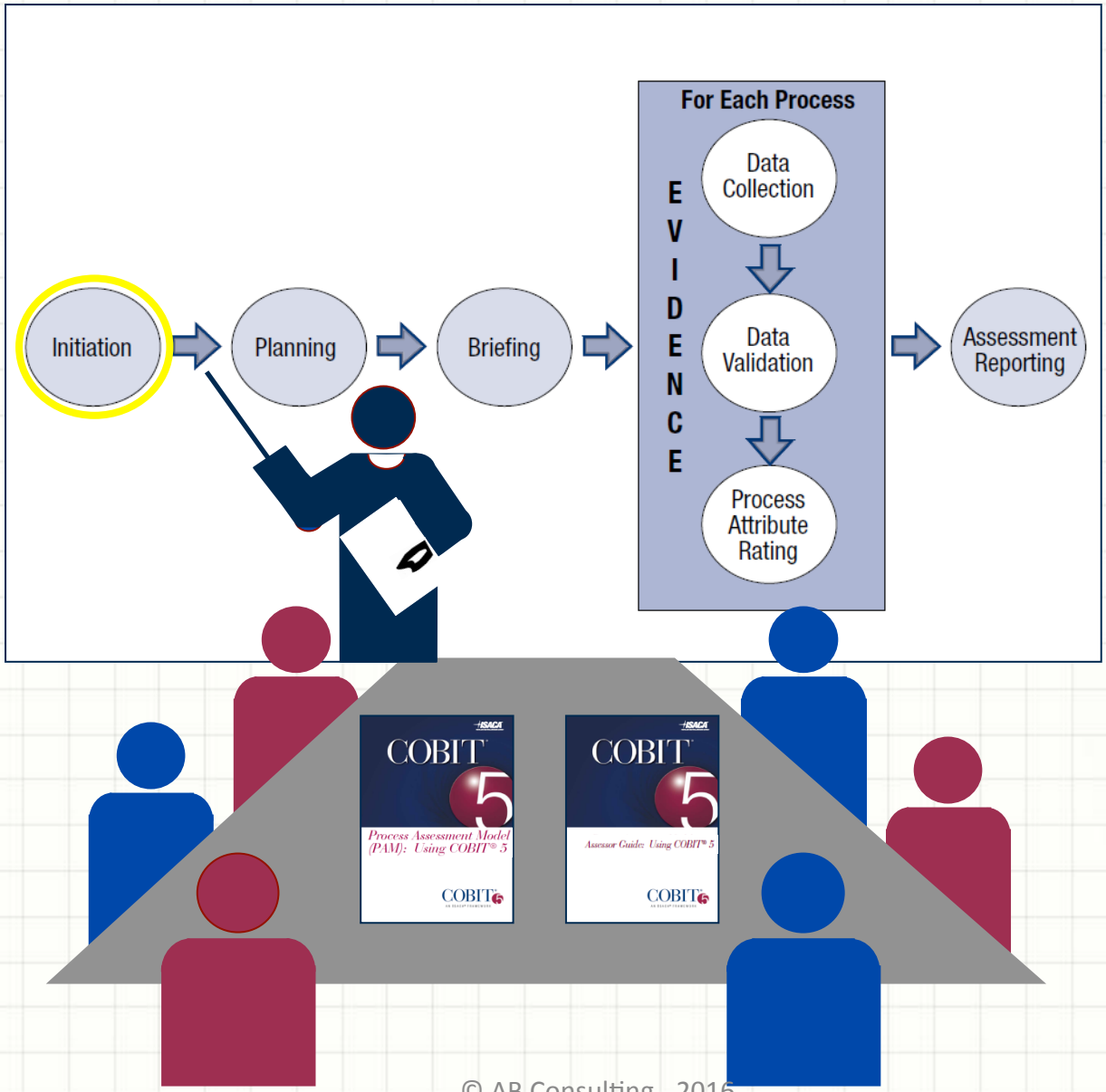
4 – Collecte des données

5 – Validation des données

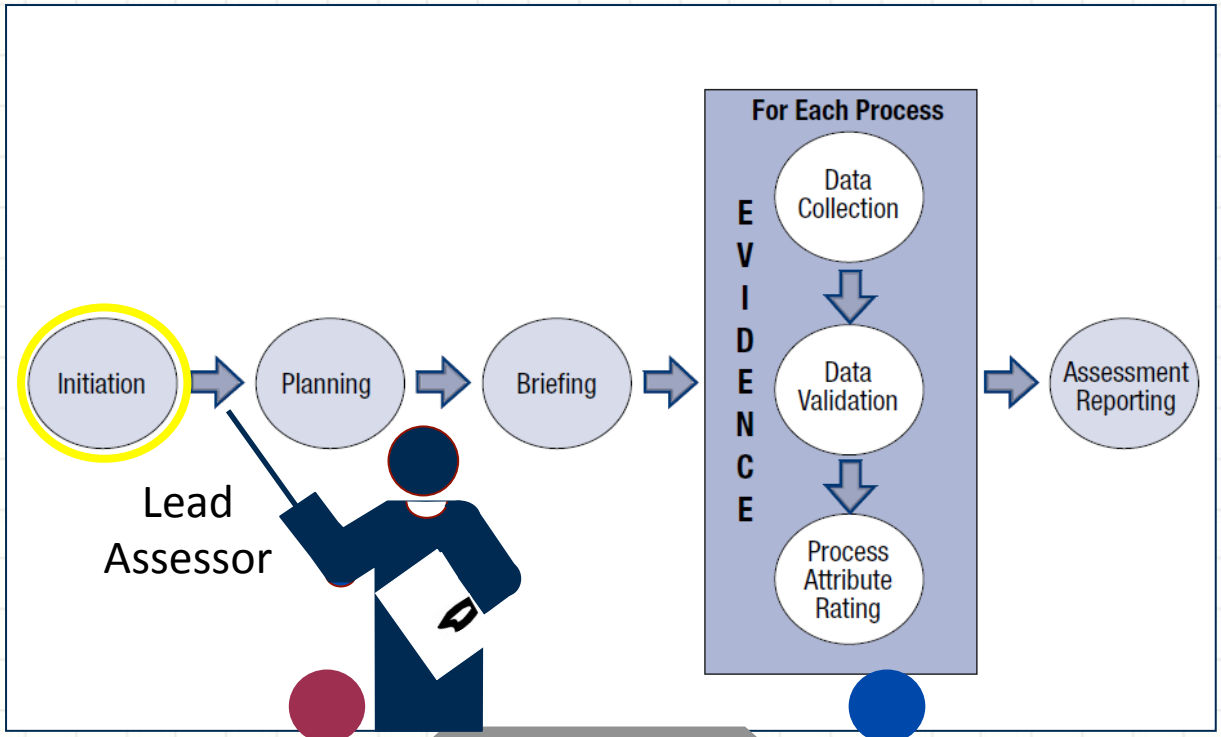
6 – Notation des attributs des processus

7 – Rapport d'audit

1 – Démarrage



Rôles & responsibilités



Sponsor

Propriétaires de processus

Coordinateur

Autres Participants

Parties prenantes des processus

Rôles & Responsabilités

Key Roles and Responsibilities in a COBIT Assessment Programme Assignment	
Roles	**Responsibilities**
Sponsor	❑ Verify that the lead assessor is a competent assessor. An indication is whether the person is a certified assessor, if such a certification is available. ❑ Ensure that resources are made available to conduct the assessment. ❑ Ensure that the assessment team has access to the relevant resources. ❑ Agree to the assessment scope. ❑ Accept assessment results on behalf of the organization
Lead Assessor	❑ Confirm the sponsor's commitment to proceed with the assessment. ❑ Ensure that the assessment is conducted in accordance with the requirements of the COBIT assessment programme. ❑ Ensure that participants in the assessment are briefed on the purpose, scope and approach of the assessment. ❑ Ensure that all members of the assessment team have knowledge and skills appropriate to their roles. ❑ Ensure that all members of the assessment team have access to appropriate documented guidance on how to perform the defined assessment activities. ❑ Ensure that the assessment team has the competencies to use the tools chosen to support the assessment. ❑ Confirm receipt of the assessment result deliverables by the sponsor. ❑ On completion of the assessment, verify and document the extent of conformance of the assessment to the COBIT assessment programme and ISO/IEC 15504

ISACA
Trust in, and value from, information systems

1 – Phase de démarrage

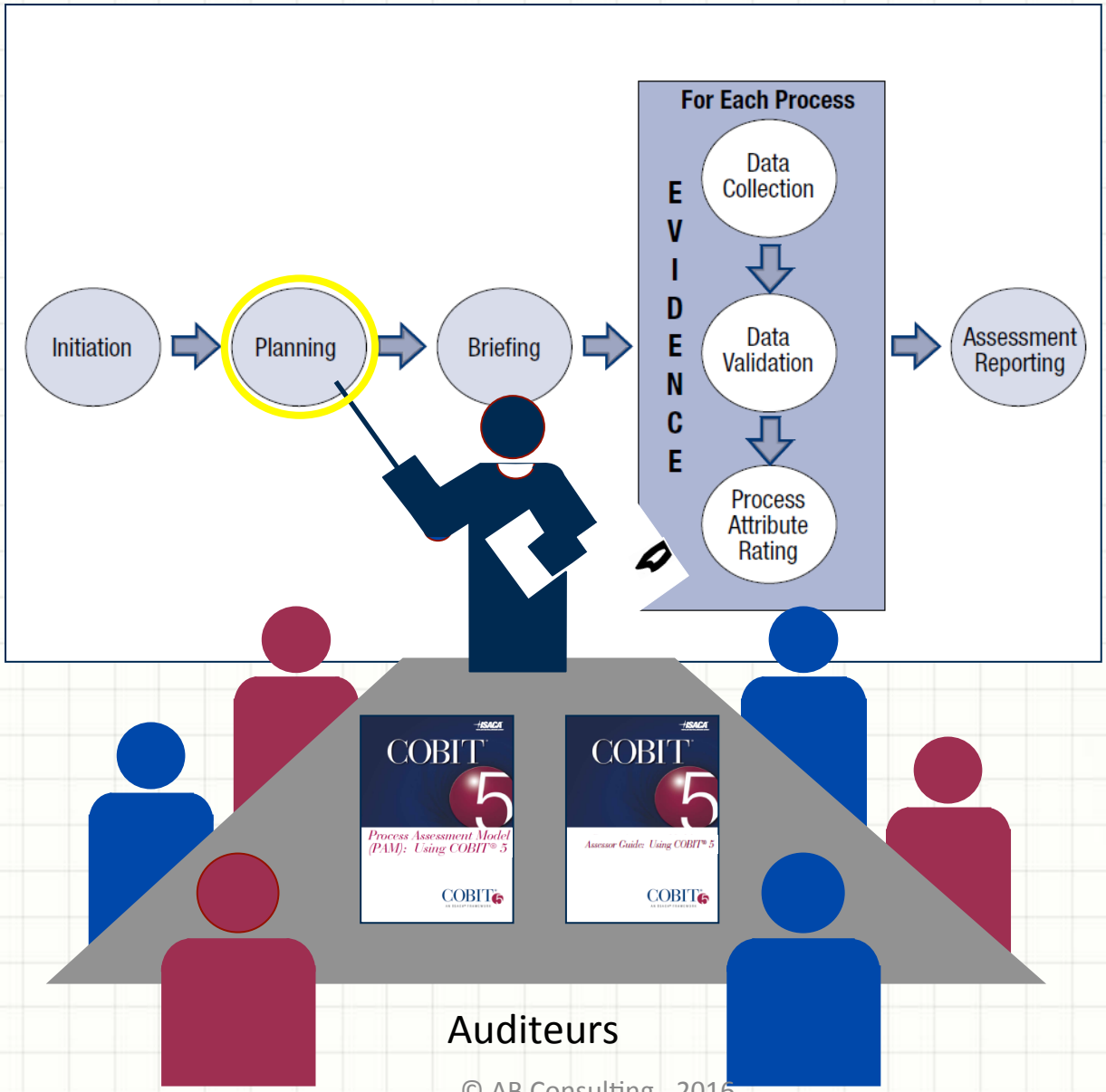
Key Roles and Responsibilities in a COBIT Assessment Programme Assignment	
Roles	**Responsibilities**
Assessor	❑ Ensure that the assessment is conducted in accordance with the requirements of the COBIT assessment programme. ❑ Rate the process attributes necessary to complete the process profile. ❑ Carry out the assigned activities associated with the assessment (detailed planning, data collection, data validation and reporting) ❑ and ensure that they are supported by proper evidence
Co-ordinator	❑ Ensure that the assessment team has adequate interaction with the necessary organisational roles needed to complete the assessment. ❑ Ensure that resources are made available in a timely manner to meet the assessment schedule. ❑ Serve as interface for logistical concerns to ensure that both the needs of the business and the needs of the assessment are adequately served

1 - Phase de démarrage

L'étape de démarrage commence par la **confirmation du sponsor,** la vérification qu'il y a bien un **accord sur l'objet et le périmètre de l'évaluation**.

Au cours de cette étape, il sera également nécessaire **d'identifier toutes les contraintes**, de produire **un planning initial de l'évaluation** (y compris des informations complémentaires susceptibles d'être nécessaires), **de choisir les participants à l'évaluation** ainsi que **la totalité de l'équipe d'auditeurs**, et de **définir les rôles de chacun des membres de l'équipe.**

2 – Planification de l'évaluation



2- Planification de l'évaluation

La planification d'une évaluation COBIT® 5 nécessite l'élaboration d'un plan d'audit décrivant l'ensemble des activités de la mission d'audit incluant la collecte des évidences et la conduite de l'évaluation.

Problématiques clés:

- Gestion de projet (un audit est un projet en soi)
- Niveau d'effort requis (Périmètre, Classe de l'évaluation et niveau d'aptitude)
- Outils utilisés
- Stratégie de collecte des données

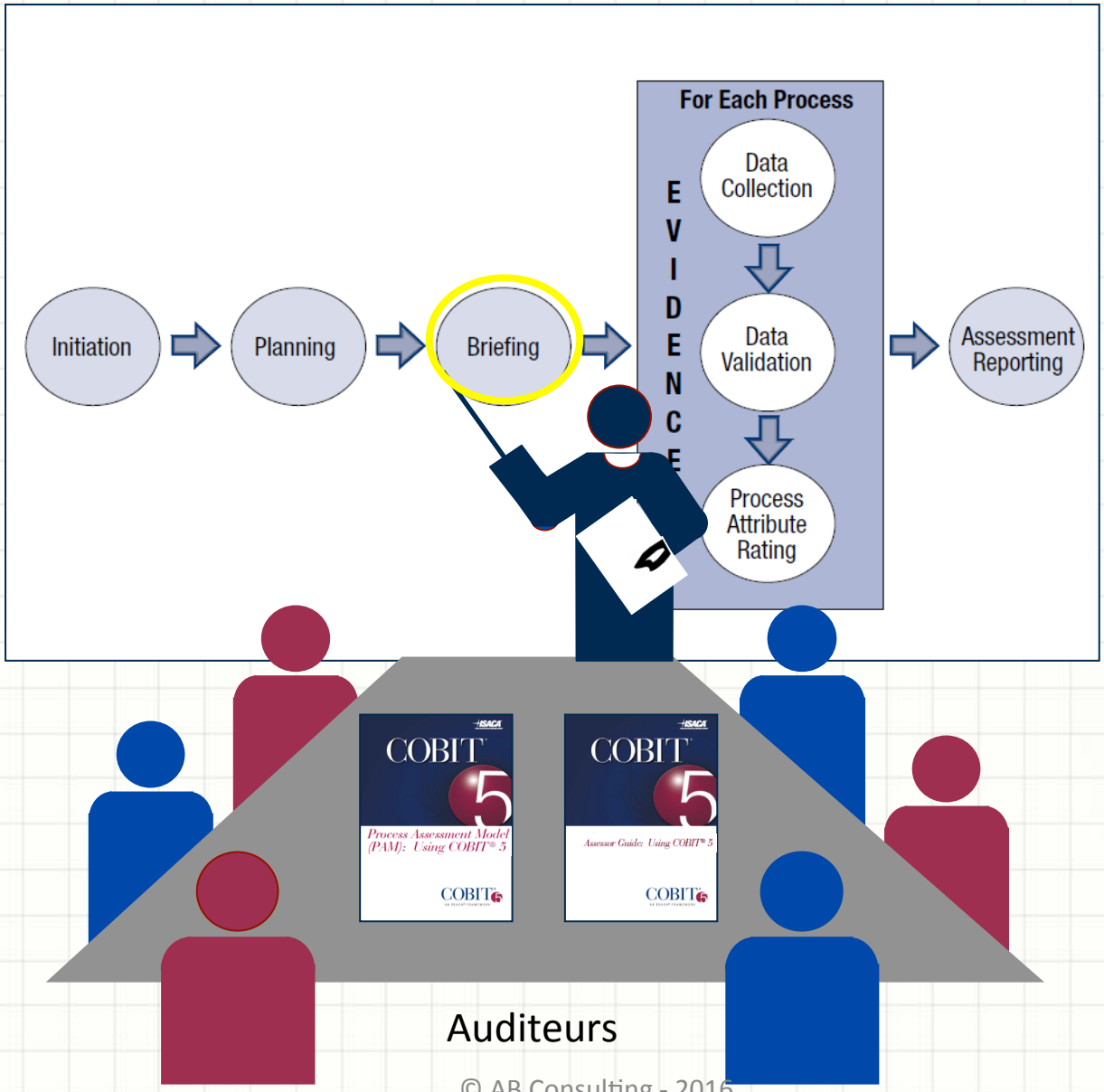
Classe de l'évaluation

Figure 17-Class Purpose, Overall Skills and Evidentail Requirements			
Topic	**Class One Assessment**	**Class Two Assessment**	**Class Three Assessment**
Purpose	• To provide a level of confidence in the results of the assessment such that the results are well suited for comparisons across different organisations • To enable assessment conclusions to be drawn as to the relative strengths and weaknesses of the organisations compared • Examples include providing a sound and solid basis for process improvement and capability determination	• To provide a level of confidence in the assessment results that may indicate the overall capability of the selected key processes in the organisation unit, which are suitable for comparisons of capability across an organisation or product line scope • To enable assessment conclusions to be drawn about the opportunities for improvement • To provide a basis for an initial assessment at the commencement of an improvement programme	• To generate capability assessment results that may indicate critical opportunities for improvement • To be suitable for monitoring the ongoing progress of an improvement programme or to identify key issues that would support a later class one or two assessment for the process in question
Assessor requirements	• At least two members, including the lead assessor. The certified assessor shall be independent of the organisation unit being assessed.	• At least two members, ideally including a certified assessor. Can be performed internally or by an independent assessor.	• At least one member. Can be performed internally or by an independent assessor.

Classe de l'évaluation

Figure 17-Class Purpose, Overall Skills and Evidentail Requirements			
Topic	**Class One Assessment**	**Class Two Assessment**	**Class Three Assessment**
Evidential requirements	• A minimum of four process instances shall be identified for each process within the scope of the assessment. For each process attribute of each process in the scope of the assessment, across the set of process instances, objective evidence drawn both from evaluation of work products and from testimony of performers of the process shall be collected. • For each process instance, objective evidence drawn both from evaluation of work products and from testimony of performers of the process shall be collected for each process within the scope of the assessment.	• A minimum of two process instances shall be identified for each process within the scope of the assessment. If there are fewer than the required number of process instances available in the organisation, all process instances shall be selected. • For each process instance, objective evidence drawn both from evaluation of work products and from testimony of performers of the process shall be collected for each process within the scope of the assessment.	• There is no minimum of process instances stated. • For each process instance, objective evidence drawn both from evaluation of work products and from testimony of performers of the process shall be collected for each process within the scope of the assessment.

3 – Instructions aux participants

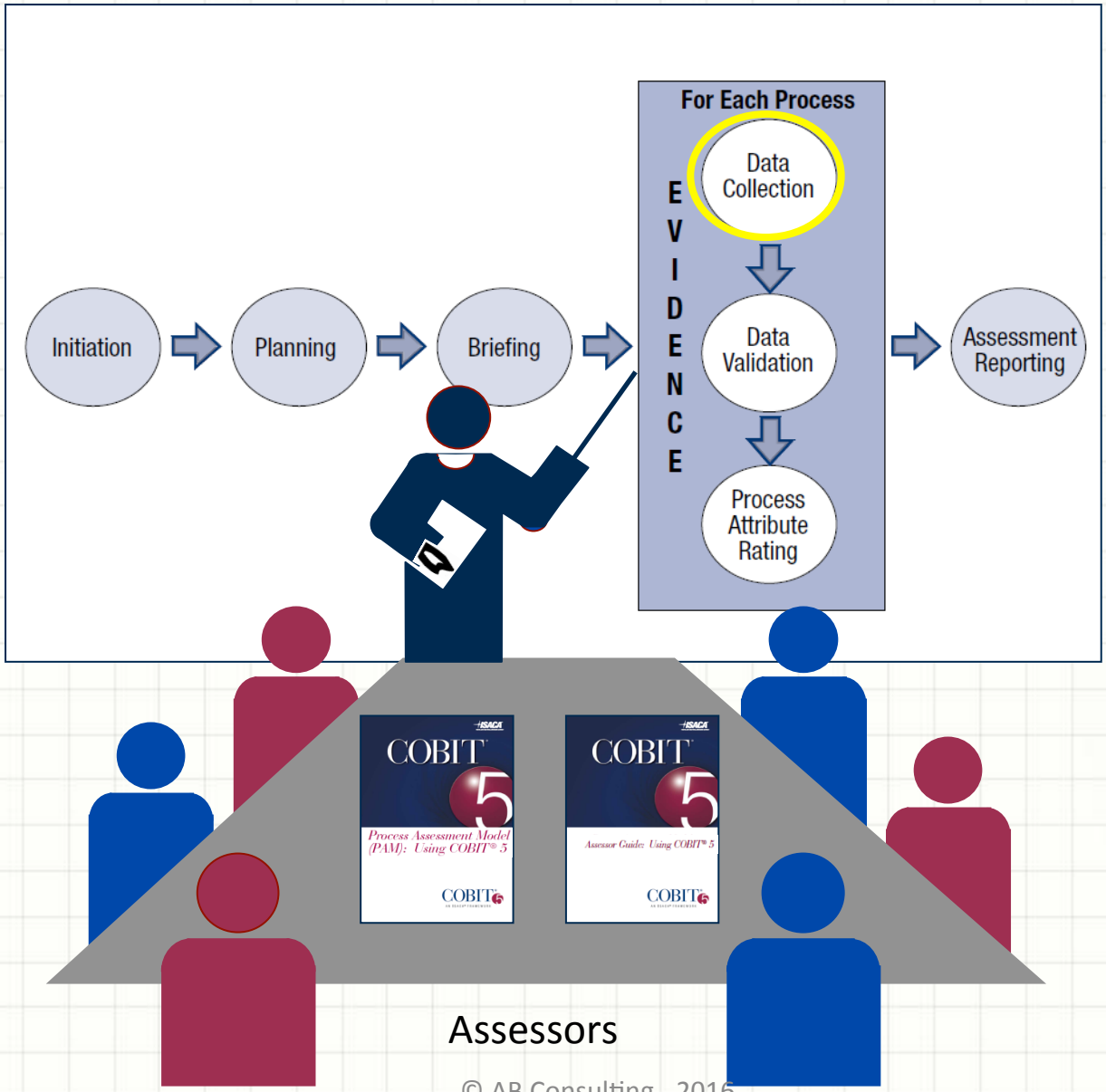


3 - Instructions aux participants

Avant de commencer la collecte des données, le **Lead Assessor doit d'abord s'assurer que l'équipe d'auditeurs comprend le processus d'audit, les entrées et les sorties.**

Les **personnes de l'Entreprise qui doivent être consultées dans le cadre de l'évaluation doivent également être informées de la façon dont l'évaluation se déroulera, des objectifs visés ainsi que des entrées et des sorties attendues. C'est une évaluation d'aptitude des processus et non au audit sur la façon de travailler du personnel.**

4 – Collecte des évidences



4 - Collecte des évidences

La collecte des données vise à obtenir des évidences soutenant l'évaluation d'aptitude des processus sélectionnés dans le périmètre de l'évaluation.

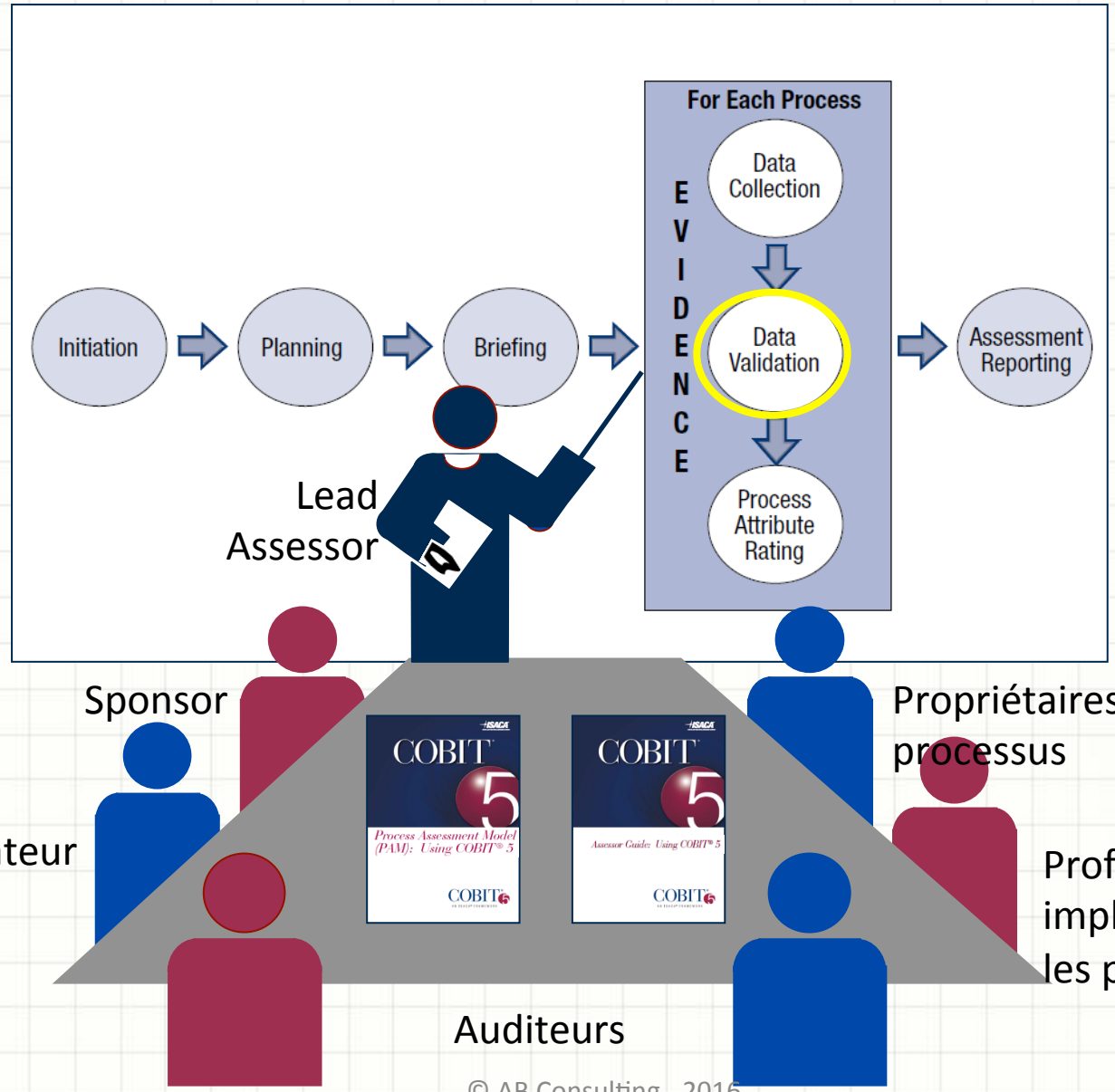
Une stratégie de collecte doit être élaborée, rédigée et approuvée durant cette phase.

Il est important de noter que la période de collecte des données doit être soigneusement choisie car elle peut avoir un impact sur les résultats de l'évaluation.

Problématiques clés:

- Stratégie de collecte des données rédigée et validée
- Choix des instances du processus
- Exigences relatives aux évidences
- Enregistrement systématique
- Préparation

5 – Validation des données



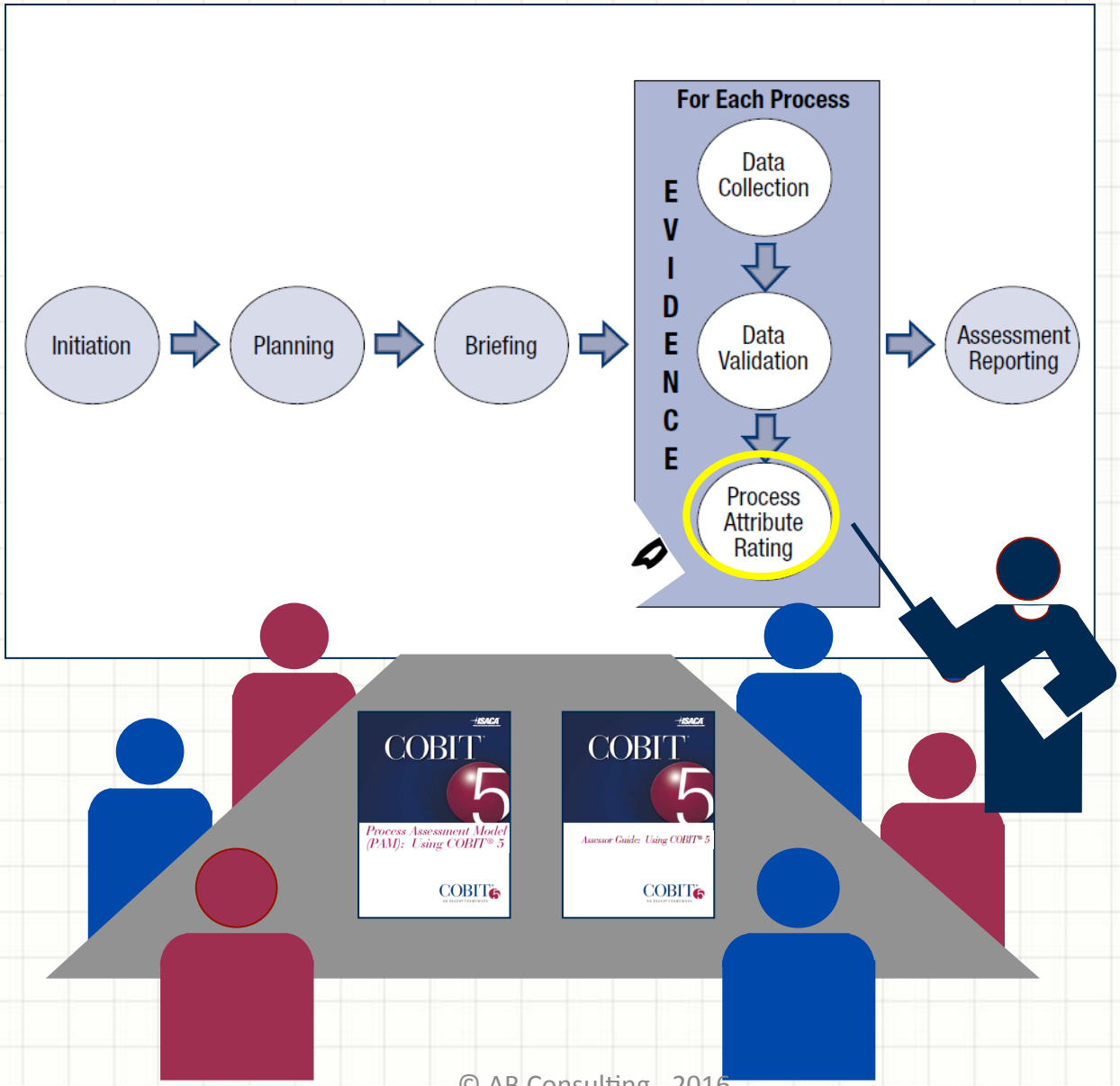
5 - Validation des données

La validation des données implique la confirmation que les évidences collectées sont bien objectives et suffisantes pour couvrir l'étendue du périmètre et pour satisfaire l'objet de l'évaluation ainsi que la cohérence globale des données collectées.

Problématiques clés:

- Revue des données collectées
- Gérer les éventuelles déficiences

6 – Notation des attributs



6 - Notation des attributs

Pour chaque processus évalué, une note est attribuées à chacun des attributs du processus, jusqu'au niveau d'évaluation qui a été décidé lors de la définition du périmètre. La note est calculée sur la base des données validées lors de l'étape 5.

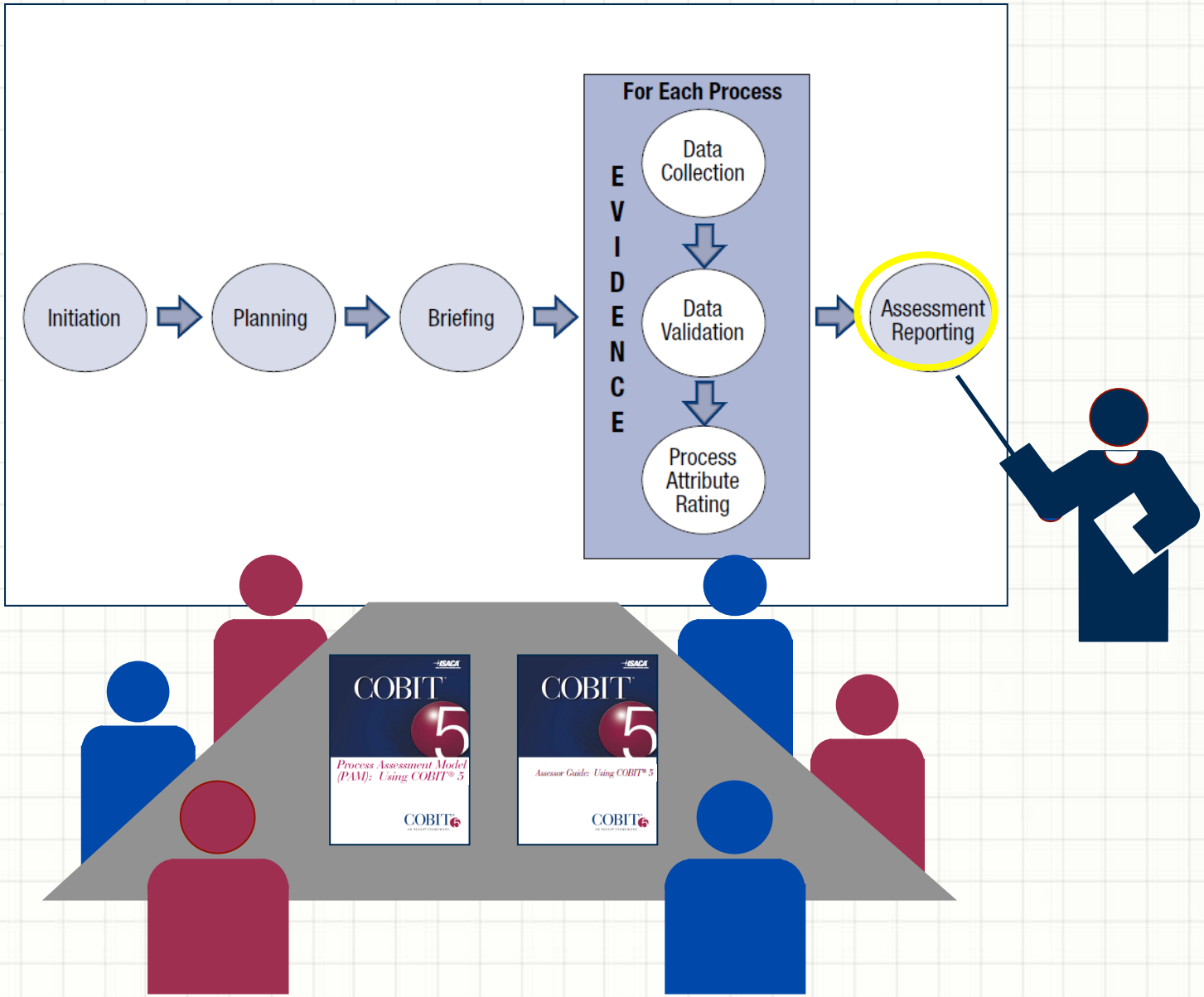
La traçabilité doit impérativement être **maintenue entre les évidences collectées** et la **note attribuée à chaque attribut du processus**.

Pour chaque attribut noté, la relation entre les indicateurs et l'évidence elle-même doit impérativement être enregistrée.

Problématiques clés:

- Le niveau 1 d'aptitude
- L'échelle de notation
- Le processus de décision

7 – Rapport d'évaluation



7 – Rapport d'évaluation

Au cours de cette phase, **les résultats de l'évaluation sont analysés et présentés au sponsor et aux autres parties-prenantes selon les cas.**

Comme souligné dans la phase 1 (démarrage de la mission d'évaluation), il est important de souligner que le rapport est:

- **Un rapport d'évaluation d'aptitude de processus, basé sur COBIT® 5, réalisé sous la conduite d'un auditeur compétent (COBIT® 5 Certified Assessor by ISACA)** et en aucun cas une attestation de certification ou un rapport donnant l'assurance de l'efficacité des contrôles internes, de la gestion des risques ou de tout autre aspect relatif à la performance de l'Entreprise
- Destiné à **une utilisation strictement interne par le management de l'Entreprise pour comprendre le niveau d'aptitude des processus IT basé sur le PAM de COBIT® 5** et (si cela fait partie du périmètre) à permettre une initiative d'amélioration des processus correspondants sur la base des résultats de l'évaluation réalisée

Problématiques clés:

- Nature de l'engagement
- Rapport
- Contenu
- Implications des résultats de l'évaluation
- Présentation aux participants

Questions / Réponses