

# L'audit, un outil de pilotage pour vos projets

*par Marc Barbezat*



- ▶ Auditeur interne IT,  
Groupe Banque Cantonale Vaudoise
- ▶ Représentant romand du comité de  
l'association suisse des auditeurs  
informatiques ISACA
- ▶ Initiateur et coordinateur de la formation  
certifiante d'audit informatique CISA en Suisse  
romande
- ▶ Créateur et responsable de la cellule  
d'intelligence économique pour la banque et la  
finance B3B.ch



<http://www.bcv.ch/>



Switzerland Chapter

<http://www.isaca.ch/>



<http://www.iseig.ch/>

**B3B** VEILLE &  
CONNAISSANCE  
.ch

*Intelligence économique  
pour la Banque et la Finance*

- ▶ Quels sont les *objectifs* d'un audit de projet ?
- ➔ **L'audit: Définition, terminologie et principes**
- ▶ Comment *préparer et accompagner* le déroulement d'un audit de projet ?
- ▶ Quelles *informations* issues de l'audit peuvent être exploitées pour le pilotage du projet ?
- ➔ **Présentation de l'approche d'audit**

***Focalisé sur la gestion de projet***

# L'audit

- *Définition et contexte d'intervention*
- *Terminologie*
- *Construction du risque*
- *Gestion du risque versus contrôle du risque*

## → L'audit

- ▶ L'audit, exercé par un auditeur, est un processus **méthodique**, **indépendant** et **documenté** permettant de recueillir des informations objectives pour déterminer dans quelle mesure les exigences satisfont aux référentiels du domaine concerné.



### *Objectifs des audits:*

- ▶ Fournir au management l'assurance que les objectifs de contrôle relevant sont atteints
- ▶ Identifier les faiblesses significatives dans ces contrôles
- ▶ Documenter le risque connecté avec de telles faiblesses
- ▶ Conseiller le management sur les mesures à implémenter

## *Pour l'auditeur:*

- ▶ L'audit est le processus permettant la vérification de l'information et déterminer la précision et la fiabilité des assertions du rapport
  - La vérification est le processus de collecte d'évidence suffisante permettant à l'auditeur de confirmer l'exactitude de ses constatations, in extenso de sa prise de position
    - Les évidences d'audit sont toutes les informations qu'un auditeur utilise pour démontrer ses constats

## Code of Professional Ethics

The Information Systems Audit and Control Association®, Inc. (ISACA) sets forth this *Code of Professional Ethics* to guide the professional and personal conduct of members of the Association and/or its certification holders.

Members and ISACA Certification holder's shall:

1. **Conformité avec les standards et les meilleures pratiques**
2. **Diligence et professionnalisme**
3. **Servir l'intérêt des actionnaires de manière honnête et respectueuse des lois**  
profession.
4. **Respect de la confidentialité et des affaires privées**  
used for personal benefit or released to inappropriate parties.
5. **Maintien des compétences**  
competence.
6. **Informier et communiquer de manière appropriée**
7. **Eduquer et sensibiliser les actionnaires**



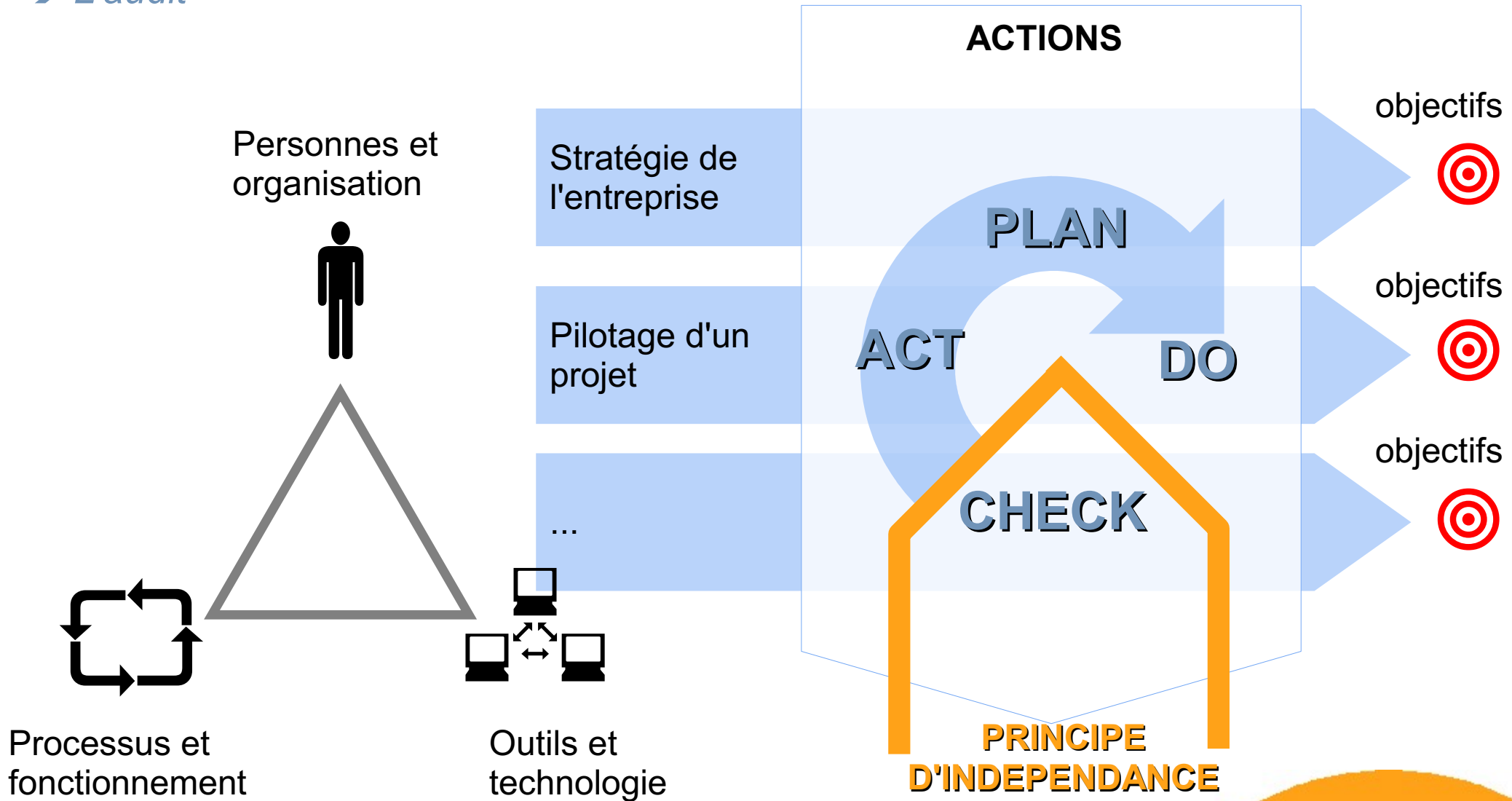
→ *L'audit* → *Définition*

*Quelques exemples:*

- ▶ Audit financier
- ▶ Audit opérationnel
- ▶ Audit de conformité (lois, règlements)
- ▶ Autres audits spécifiques:
  - Audit intégré (combinant les aspects financiers et opérationnels)
  - Audit administratifs (évaluation de l'efficacité opérationnelle / productivité)
  - Audit du système d'information
  - Audit spécialisé (domaine spécifique, démarche standardisée,...)
  - Audit de forensic (cas de fraude)
  - ...

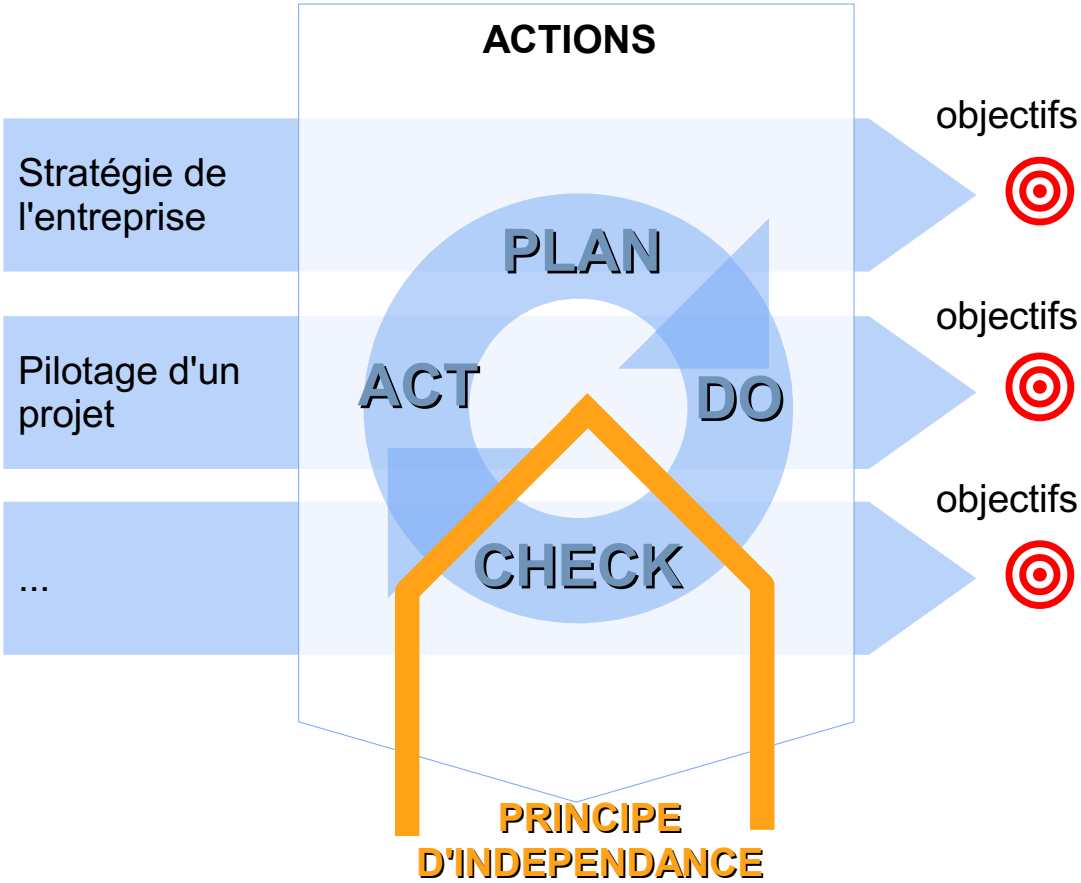
# Contexte d'intervention

→ L'audit



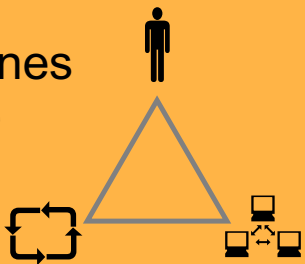
# Contexte d'intervention

→ L'audit → Contexte d'intervention



## Processus d'audit

Focalisation sur les domaines à haut risque de la société



Financier

Opérationnel

Conformité

→ *L'audit* → *Contexte d'intervention*

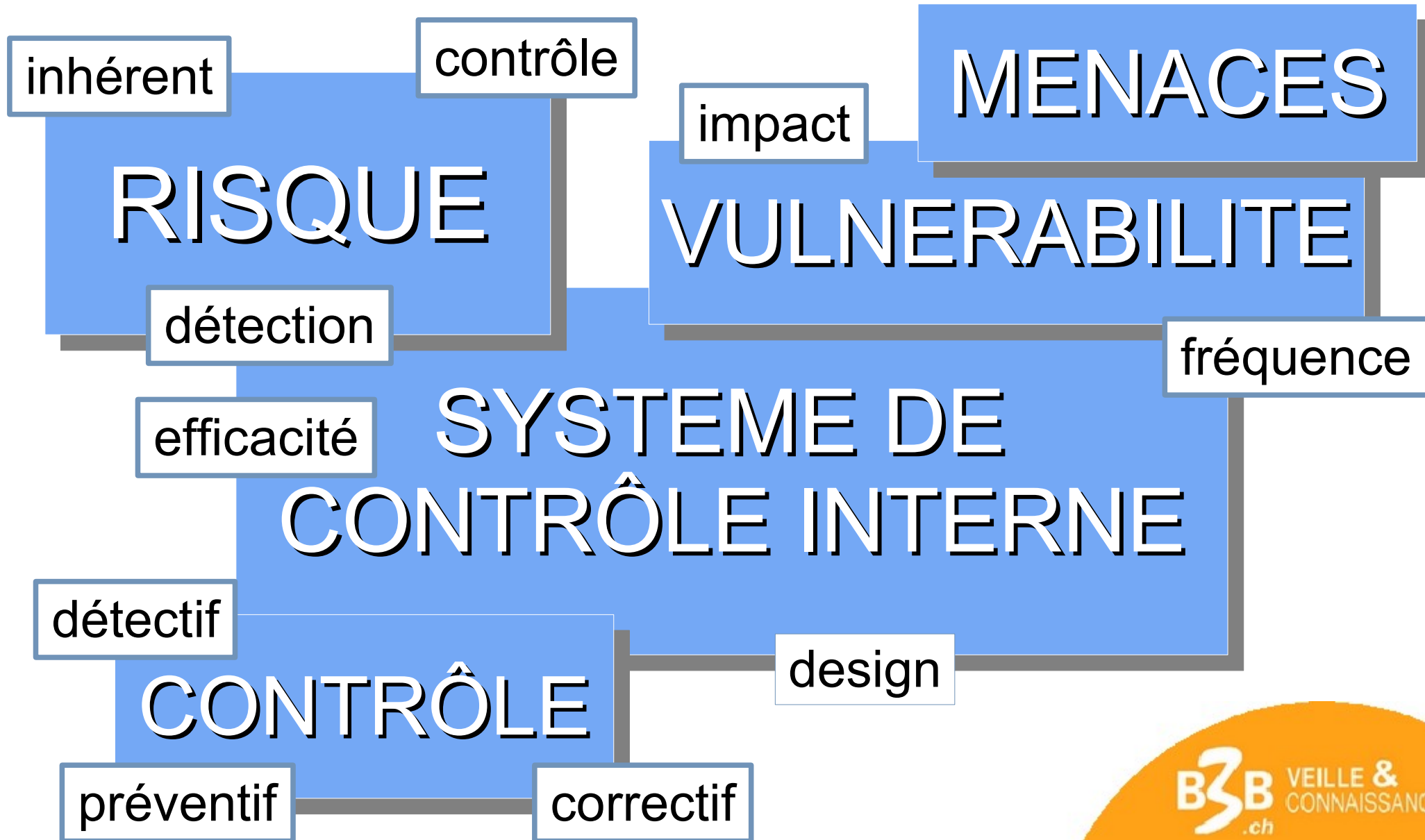
## ▶ Planification à long terme

- Par exemple triennale
- Lié à la planification stratégique de l'entreprise
- Facteurs à considérer
  - Changements de technologies
  - Nouveau principes de contrôle
  - Modification de processus opérationnels
  - Nouvelles contraintes réglementaires
  - ...

## ▶ Planification à court terme

- Annuelle
- Lié à la planification des ressources

→ L'audit



## ▶ Menace

- Tout acte, situation, événement, pouvant être à l'origine de dégâts ou de dommages sur un bien ou à une personne physique ou morale.

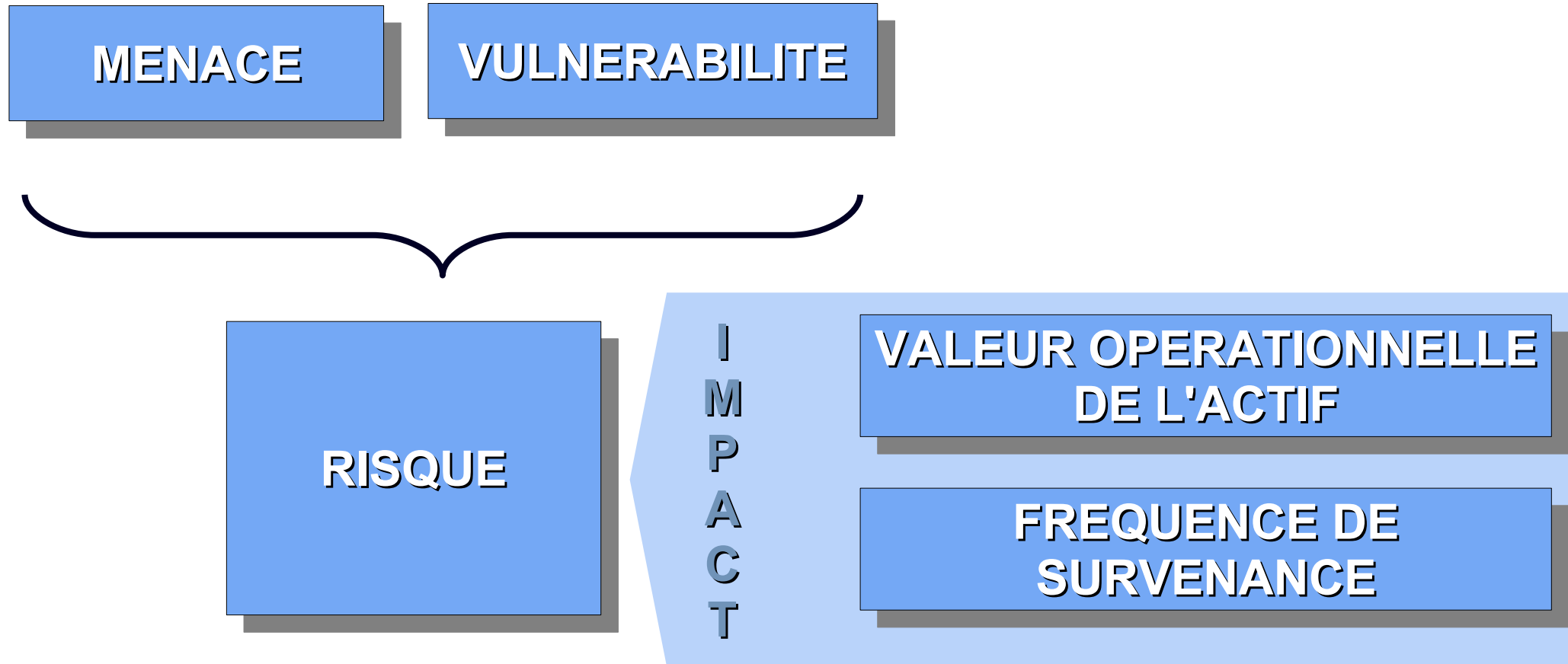


## ▶ Vulnérabilité

- Une vulnérabilité est une faille dans une procédure, un système, le design, l'implémentation d'un contrôle qui peut être exploitée pour abuser la sécurité ou empêcher d'atteindre les objectifs de la société
- Inhérente à l'environnement de la société. Une vulnérabilité peut concerner les bâtiments et les locaux, les logiciels et applications, les systèmes,...

# Risque

→ L'audit → Terminologie



## ▶ Risque

- Evènement qui est susceptible d'entraîner des dommages et/ou des pertes pour l'entreprise concernée

## ▶ Contrôle

- Les contrôles sont des politiques, des procédures, des pratiques et des structures organisationnelles désignées pour mettre à disposition une assurance raisonnable que les objectifs business seront atteints et que les événements non souhaités pourront être prévenus ou détectés et corrigés

→ *L'audit* → *Terminologie*

## ▶ Système de contrôle interne

- Ensemble des contrôle (méthodes et procédures) utilisés dans une société
  - pour la protection des actifs de l'entreprises
  - Comptabilité correcte et conforme
  - Management efficace de la société
  - Conformité avec la stratégie opérationnelle
  - Prévention et la détection d'erreurs et d'irrégularités
  - ...

# Risque

→ L'audit → Terminologie

**MENACE**

**VULNERABILITE**

**RISQUE**

**SYSTEME DE  
CONTROLE  
INTERNE**

**IMPACT -  
VALEUR OPERATIONNELLE**

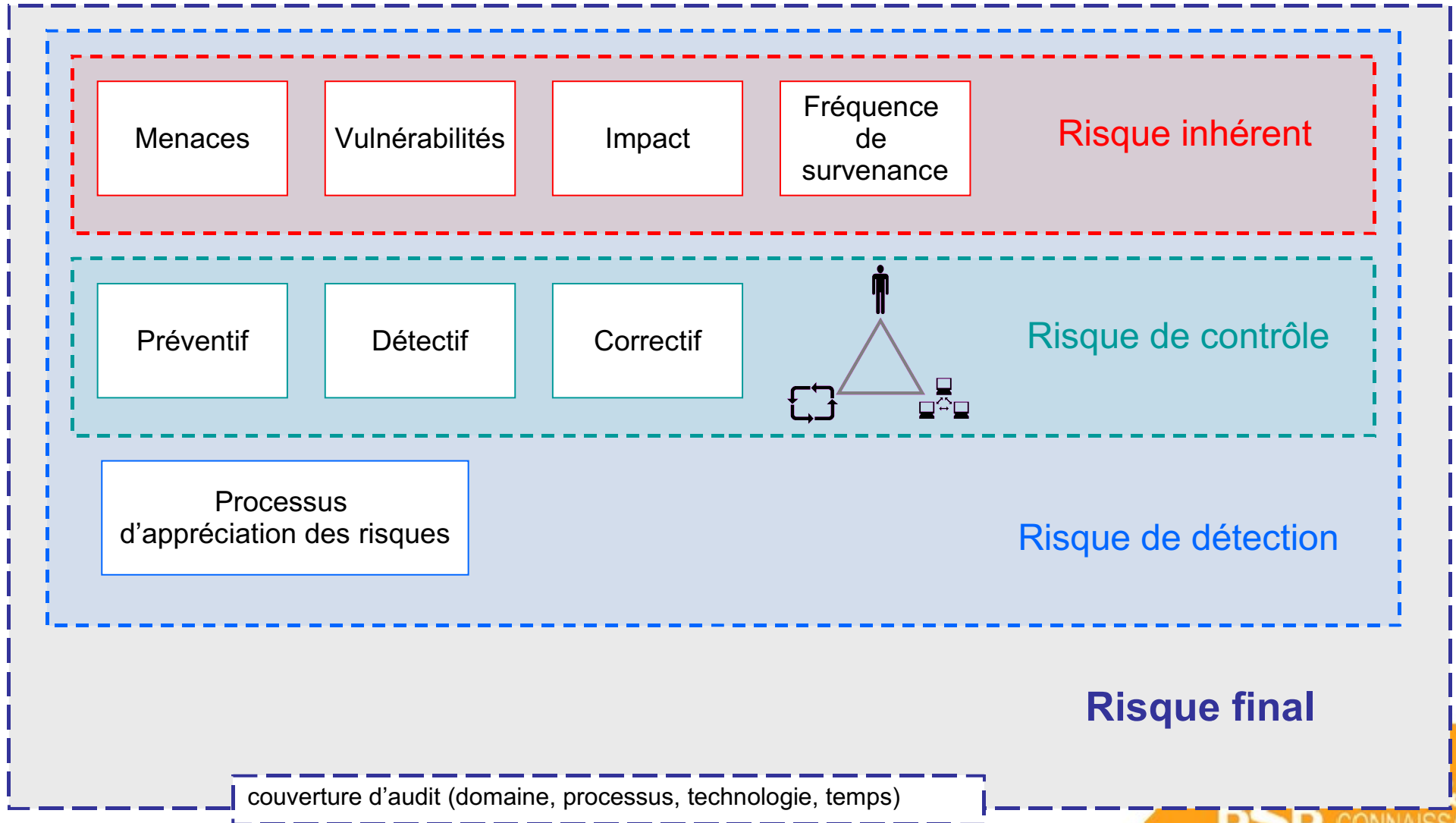
**FREQUENCE DE  
SURVENANCE**

**B3B** VEILLE &  
CONNAISSANCE  
.ch

*Intelligence économique  
pour la Banque et la Finance*

# Construction du risque

→ L'audit

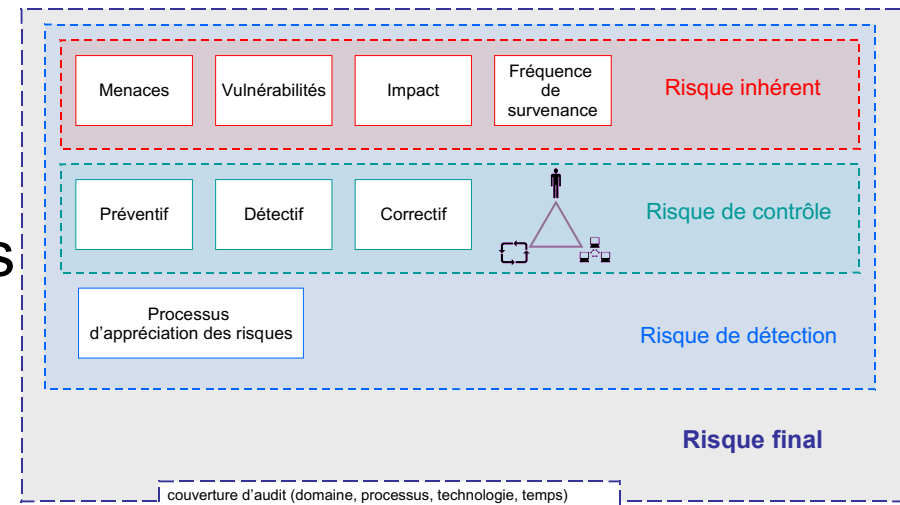


# Risques inhérents

→ L'audit → Construction du risque

## ► Risque inhérent:

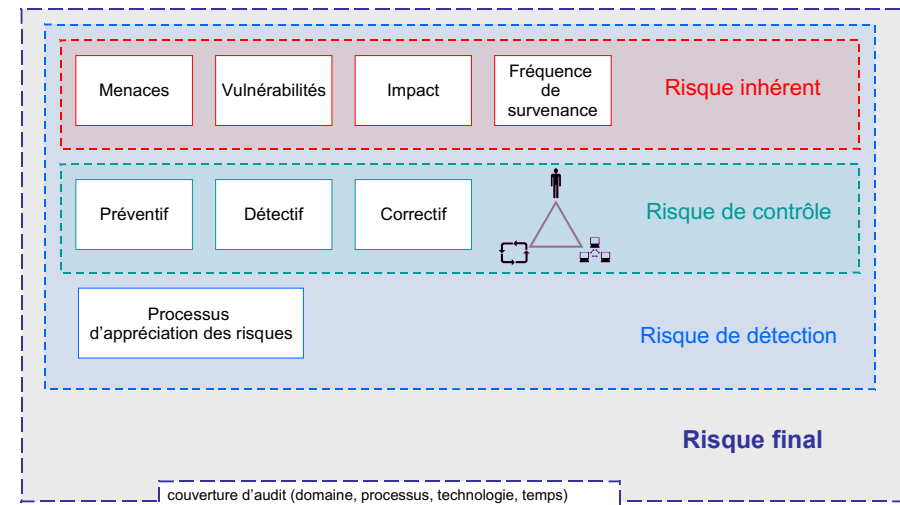
- Type de produits ou de services
- Situation de concurrence
- Industrie
- Taille et états financiers de la sociétés
- Développement technologique
- Environnement informatique
- ...



# Risques de contrôle

→ L'audit → Construction du risque

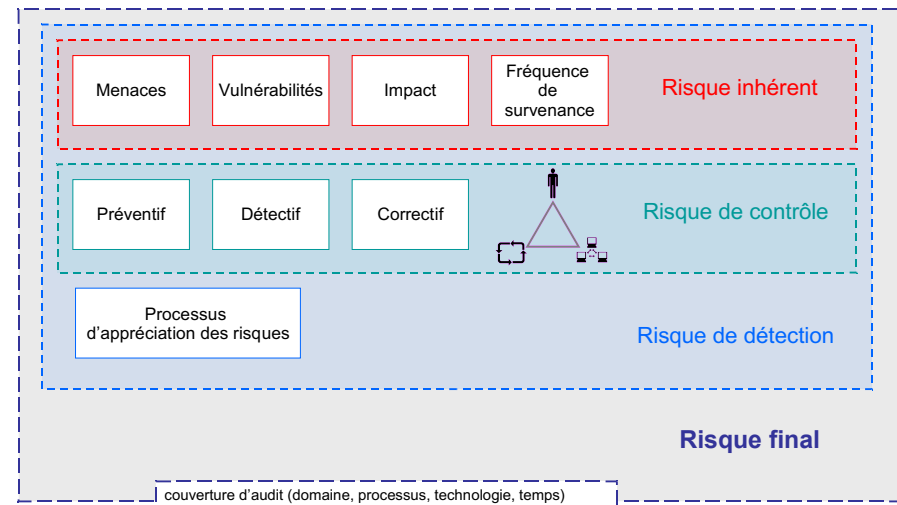
- ▶ Culture d'entreprise
- ▶ Activités / industries
- ▶ Réorganisation, fusions, acquisition, outsourcing
- ▶ Staff, personnes et organisation
- ▶ Gestion des changements
- ▶ Manque de directives et de documentations
- ▶ Ségrégation des tâches
- ▶ ...



# Risques de détection

→ L'audit → Construction du risque

- ▶ Erreur non détectée
- ▶ Indicateurs inefficaces
- ▶ Planning d'audit inadéquat
- ▶ Résultats d'audit interprétés de manière incorrecte
- ▶ Constats non pondérés de manière correcte
- ▶ ...

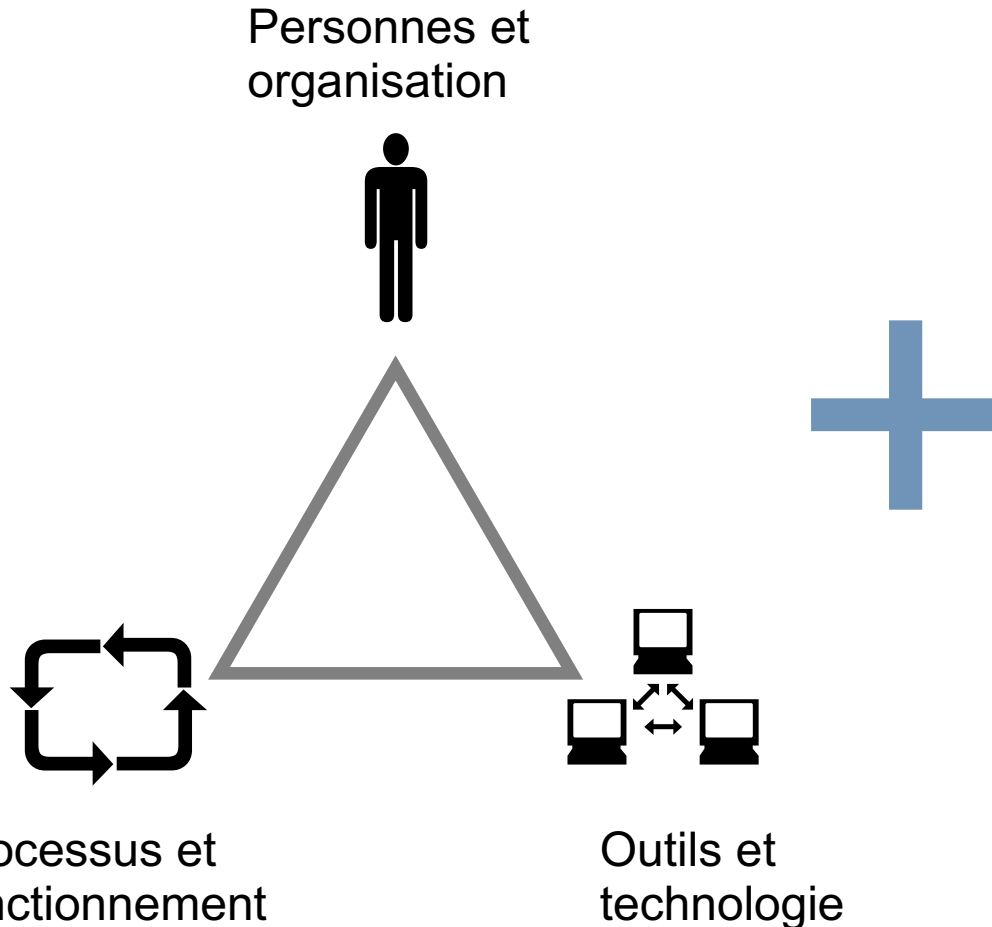


# L'approche audit

- *Compréhension de l'environnement*
- *Identification des risques*
- *Identification des contrôles*
- *Appréciation des risques*
- *Communication des résultats*
- *Suivi des constatations*

# 1. Compréhension de l'environnement

→ *L'approche d'audit*



*Dimensions à considérer*

- ▶ Identifié?
- ▶ Défini?
- ▶ Validé?
- ▶ Documenté?
- ▶ Implémenté?
- ▶ Surveillé?
- ▶ Revu?

→ *L'approche d'audit*

→ *1. Compréhension de l'environnement*

▶ Interviews

- Direction
- Personnes clés
- Employés

▶ Revue de documentation (papier et électronique)

- Politiques, standards et procédures
- Mode d'emploi
- ...

▶ Observation

- Mode opératoire
- Responsabilité, limites d'activités
- ...

Processus de documentation

*Qualité de l'information  
et quantité d'information*

→ *L'approche d'audit*

→ *1. Compréhension de l'environnement*

## ▶ **Pertinente**

- Alignée sur les objectifs de l'audit
- En relation logique avec les constatations et les conclusions

## ▶ **Reliable**

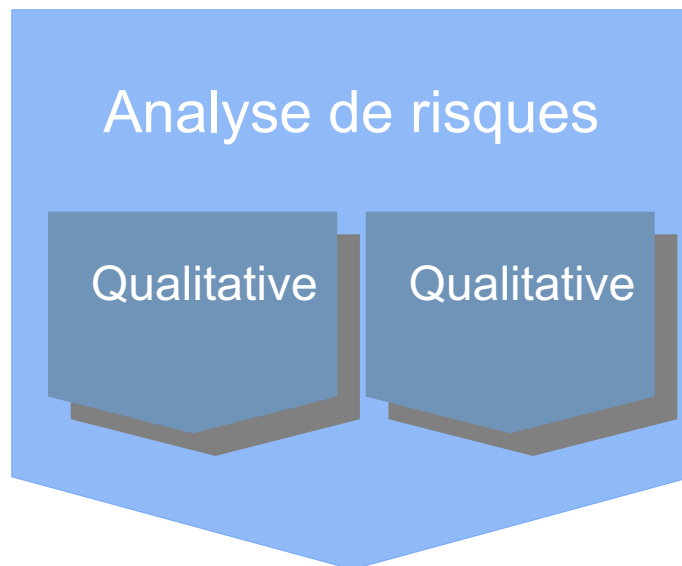
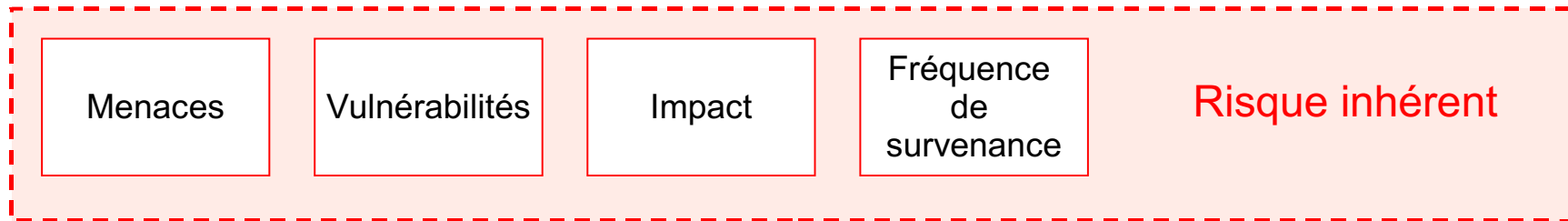
- Valide (temps, domaine, source indépendante, etc.)
- Factuelle
- Objective (interprétation)

## ▶ **Suffisante**

- Complète
  - Adéquate
  - Convaincante
- ▶ Conduirait un autre auditeur aux mêmes conclusions

## 2. Identification des risques

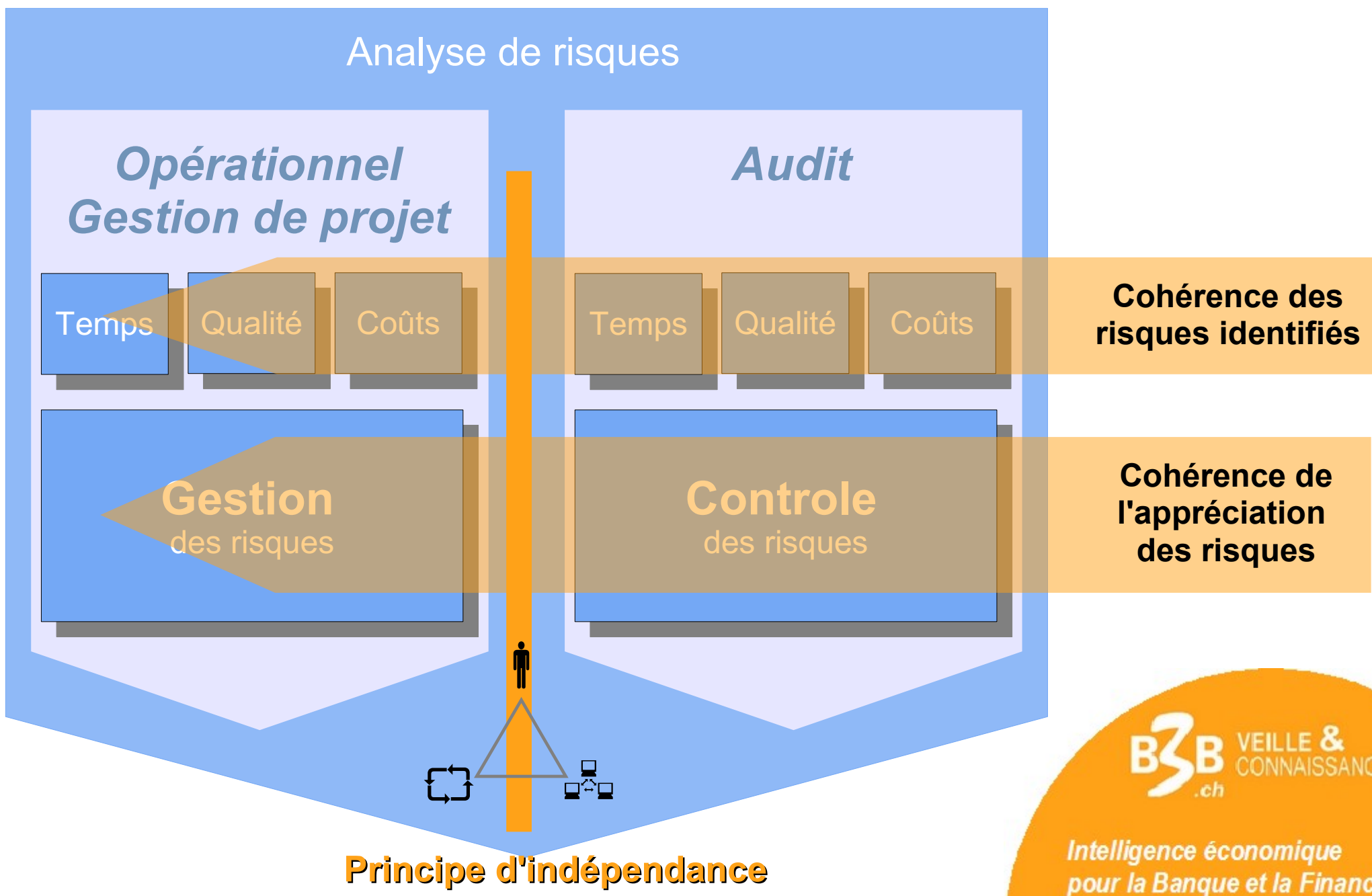
→ *L'approche d'audit*



- Aide à la planification de l'évaluation des contrôles
- Confirme les objectifs d'audit

# Gestion du risque vs contrôle du risque

→ L'audit → 2. Identification des risques



# Référentiels et outils

→ L'approche d'audit → 2. Identification des risques

Normes assurance qualité  
(ISO, PRINCE2 , ITIL,...)

Normes d'audit  
(NAS, COBIT, COSO,...)

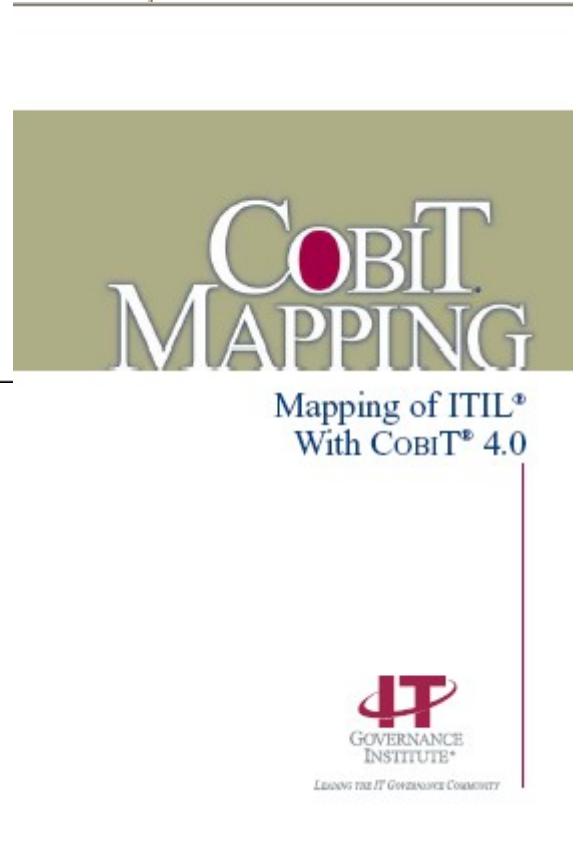
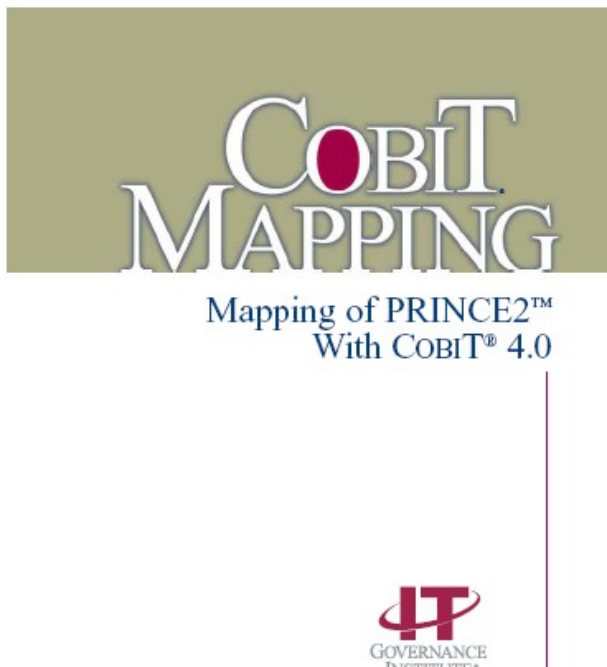
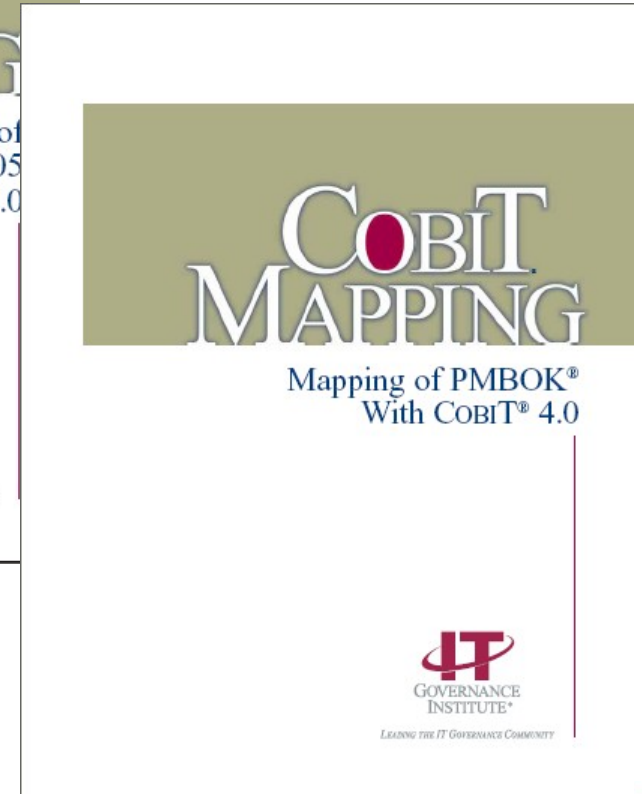
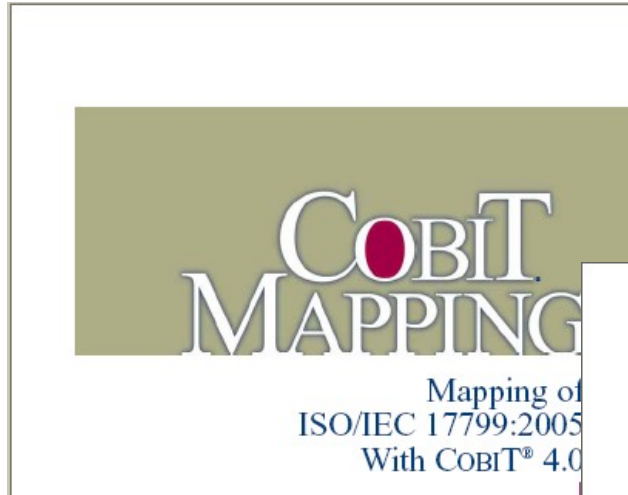
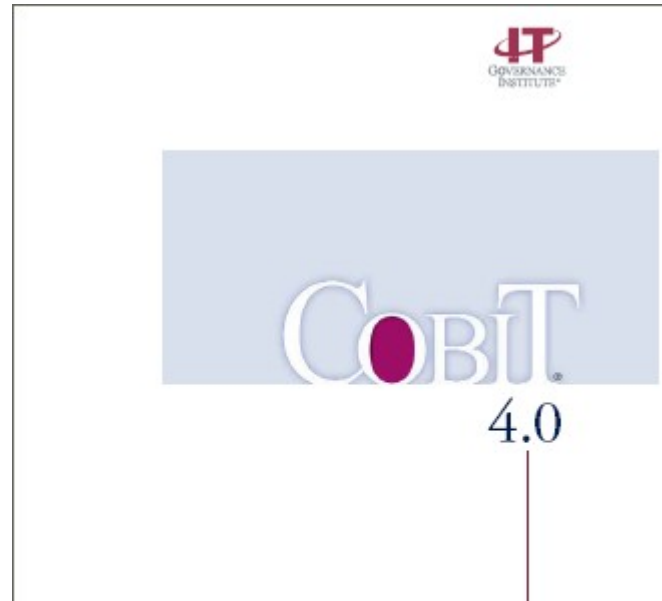
Normes de sécurité  
(ISO 27001, ITsec,...)

Normes, référentiels métier

*Cohérence de  
l'identification et de  
l'appréciation  
des risques*

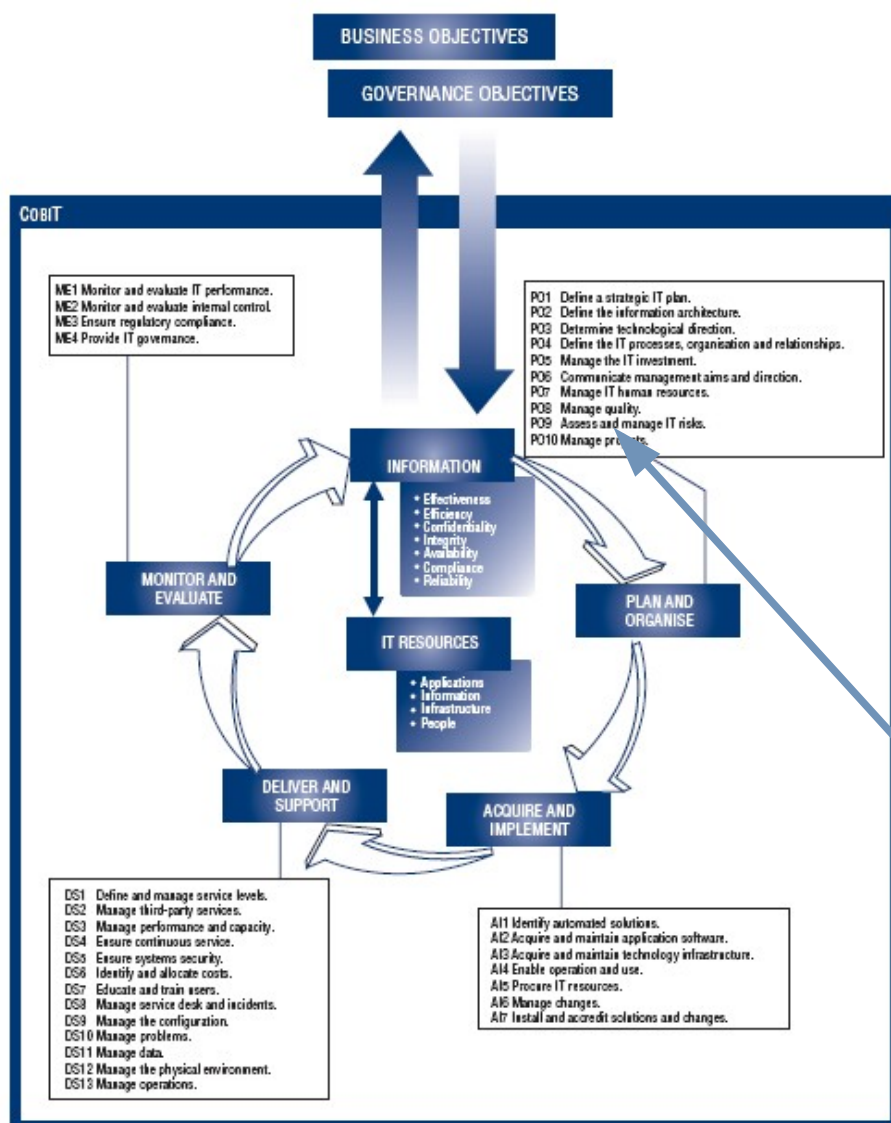
# Référentiels et outils: COBIT

→ L'approche d'audit → 2. Identification des risques



# Vue globale du référentiel

→ L'approche d'audit → 2. Identification des risques → COBIT



## ▶ 4 domaines

- Planning & Organisation
- Acquisition & Implementation
- Delivery & Support
- Monitor & Evaluate

## ▶ 34 Macro-processus

PO-10 Manage Project

# Processus PO 10 – Manage projects (1/3)

→ *L'approche d'audit* → 2. *Identification des risques* → COBIT

**Control over the IT process of**

Processus

**that satisfies the business requirement for IT of**

Objectifs business

**by focusing on**

Objectifs IT

**is achieved by**

Objectifs de contrôles

**and is measured by**

Métriques et indicateurs

→ *L'approche d'audit* → 2. *Identification des risques* → *COBIT*

## ▶ 0 **Non-existent**

- Project management techniques are not used and the organisation does not consider business impacts associated with project mismanagement and development project failures.

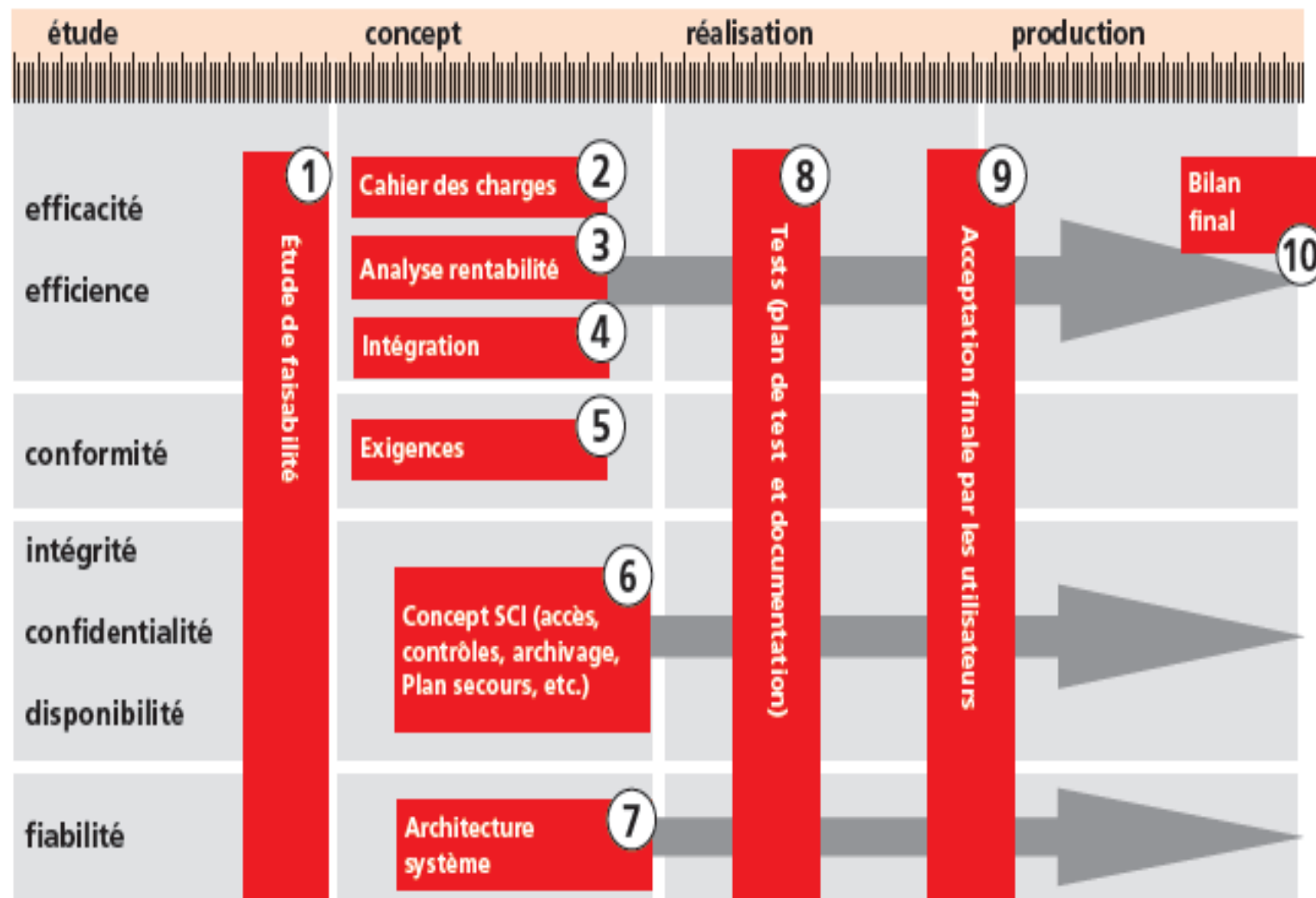
▶ ...

## ▶ 5 **Optimised**

- A proven, full life cycle project and programme methodology is implemented, enforced and integrated into the culture of the entire organisation. An ongoing initiative to identify and institutionalise best project management practices has been implemented. An ...

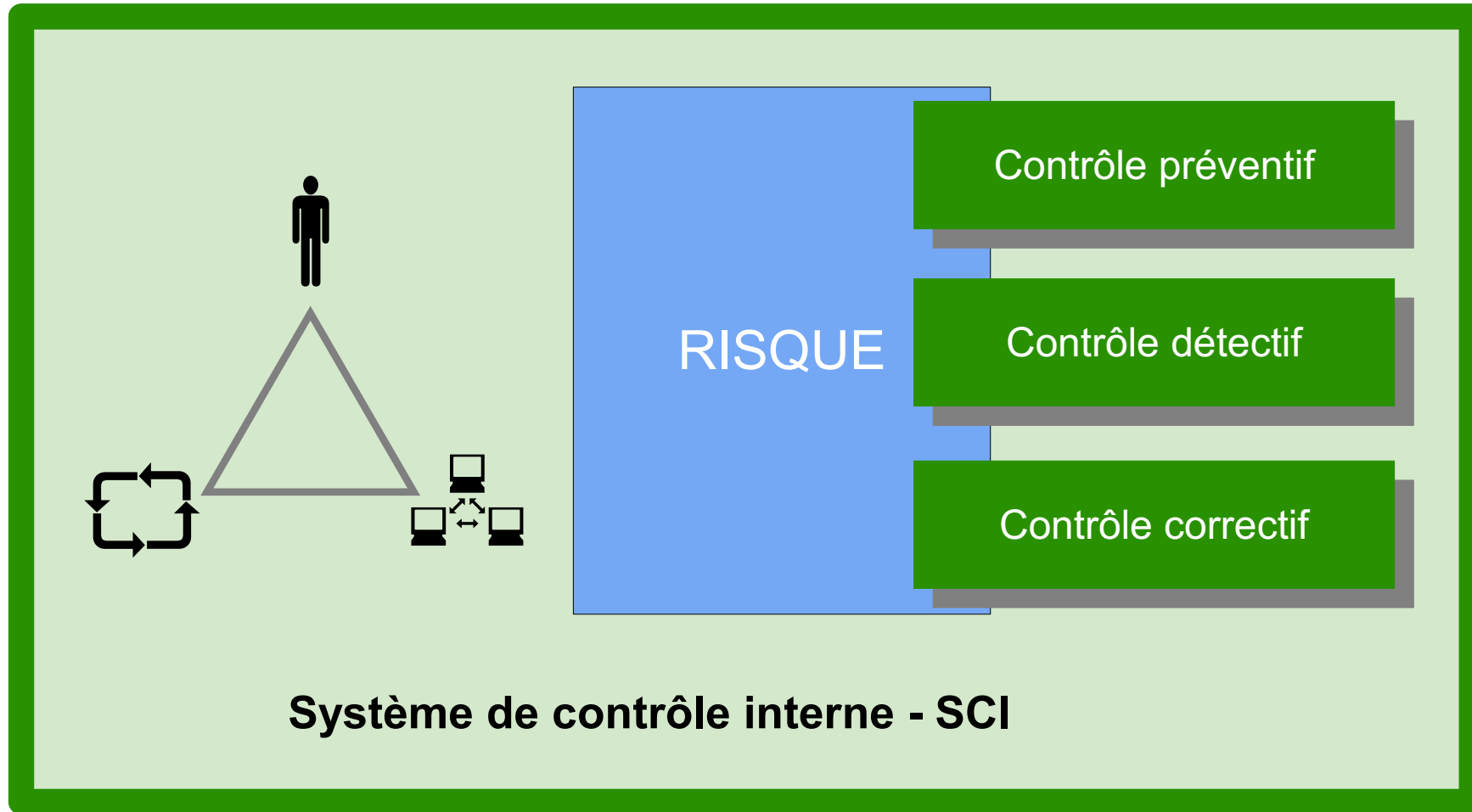
→ L'approche d'audit → 2. Identification des risques → COBIT

## Les 10 documents-clé de la vie d'un projet



# 3. Identification des contrôles

→ *L'approche d'audit*



→ *L'approche d'audit* → 3. *Identification des contrôles*

## ▶ **PREVENTIF**

- Politiques, directives, standards
  - Formation
  - Sensibilisation
  - Ségrégation des tâches
  - Logiciel de contrôle d'accès
  - ...
  -
- ▶ *Détecte les problèmes avant qu'ils surviennent*
- ▶ *Prévient les erreurs, les omissions, les actes malicieux*
- ▶ ...

→ *L'approche d'audit* → 3. *Identification des contrôles*

## ▶ **DETECTIF**

- Contrôle de totaux, reconciliations
  - Messages d'erreur
  - Rapport
  - Indicateurs de tableau de bord
  - ...
- 
- ▶ *Détecte et reporte le problème, tels que les erreurs, les omissions, les actes malicieux*
  - ▶ ...

→ *L'approche d'audit* → 3. *Identification des contrôles*

## ▶ **CORRECTIF**

- Plan de continuité
  - Procédure de backup
  - Procédure de « re-run »
  - ...
- 
- ▶ *Réduit l'impact de la menace*
  - ▶ *Corrige les erreurs découvertes par les contrôles détectifs*
  - ▶ *Modifie le déroulement opérationnel afin de réduire le nombre d'occurrences futures d'un problème*
  - ▶ ...

→ *L'approche d'audit* → 3. *Identification des contrôles*

- ▶ Identifier le contrôle et comprendre son fonctionnement
  - Design
  - Point de fonctionnement
    - dans le temps,
    - étape de la procédure,
    - ...
  - Efficacité
- ▶ Habituellement, au minimum 2 contrôles pour couvrir adéquatement un risque

→ *L'approche d'audit* → 3. *Identification des contrôles*

## ▶ Tests de conformité du contrôle

- Détermine si les contrôles internes sont appliqués dans la manière décrite dans la documentations et en accord avec les intentions du management
- Teste le processus

## ▶ Tests de validation du contrôle

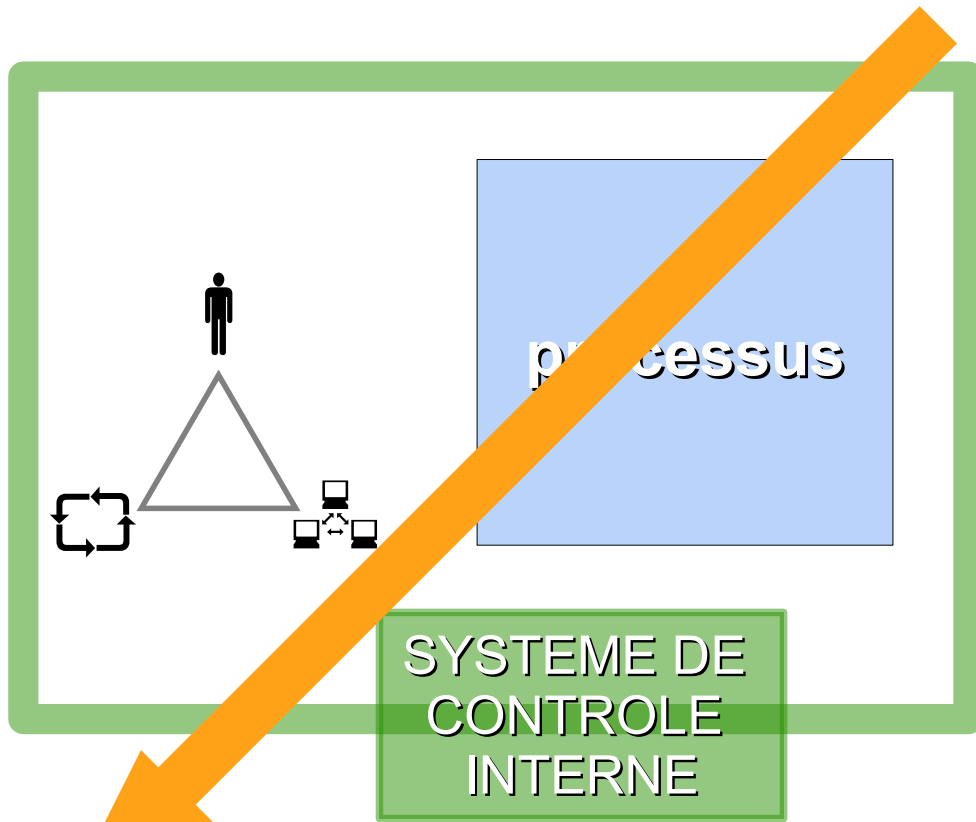
- Confirme l'intégrité du résultat sur la base du fonctionnement réel du contrôle
- Teste la valeur

# Appréciation des contrôles: Tests

→ L'approche d'audit → 3. Identification des contrôles

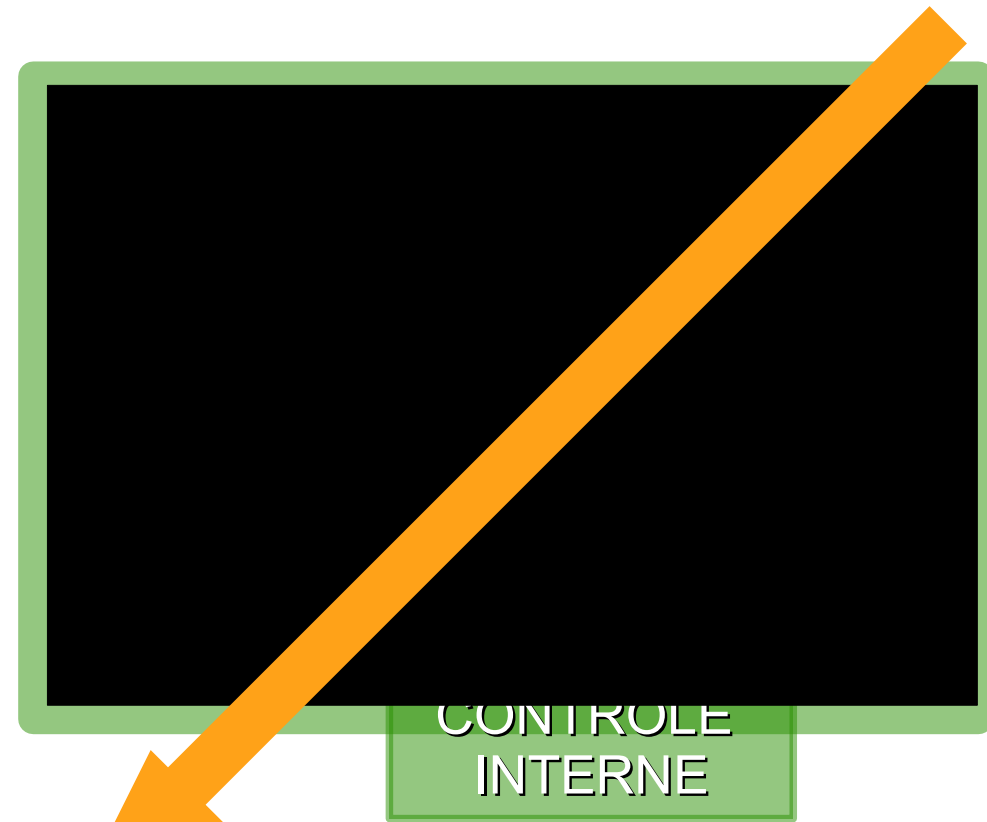
## TESTS DE CONFORMITE

INPUT



## TESTS DE VALIDATION

INPUT

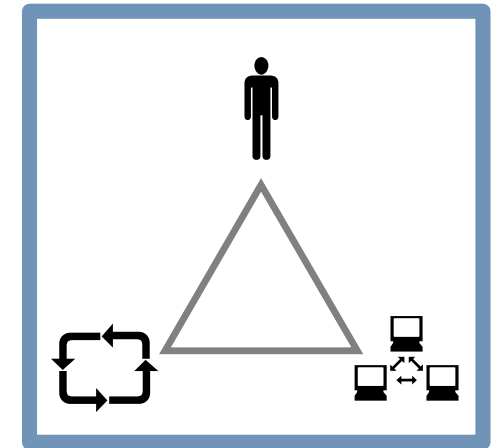
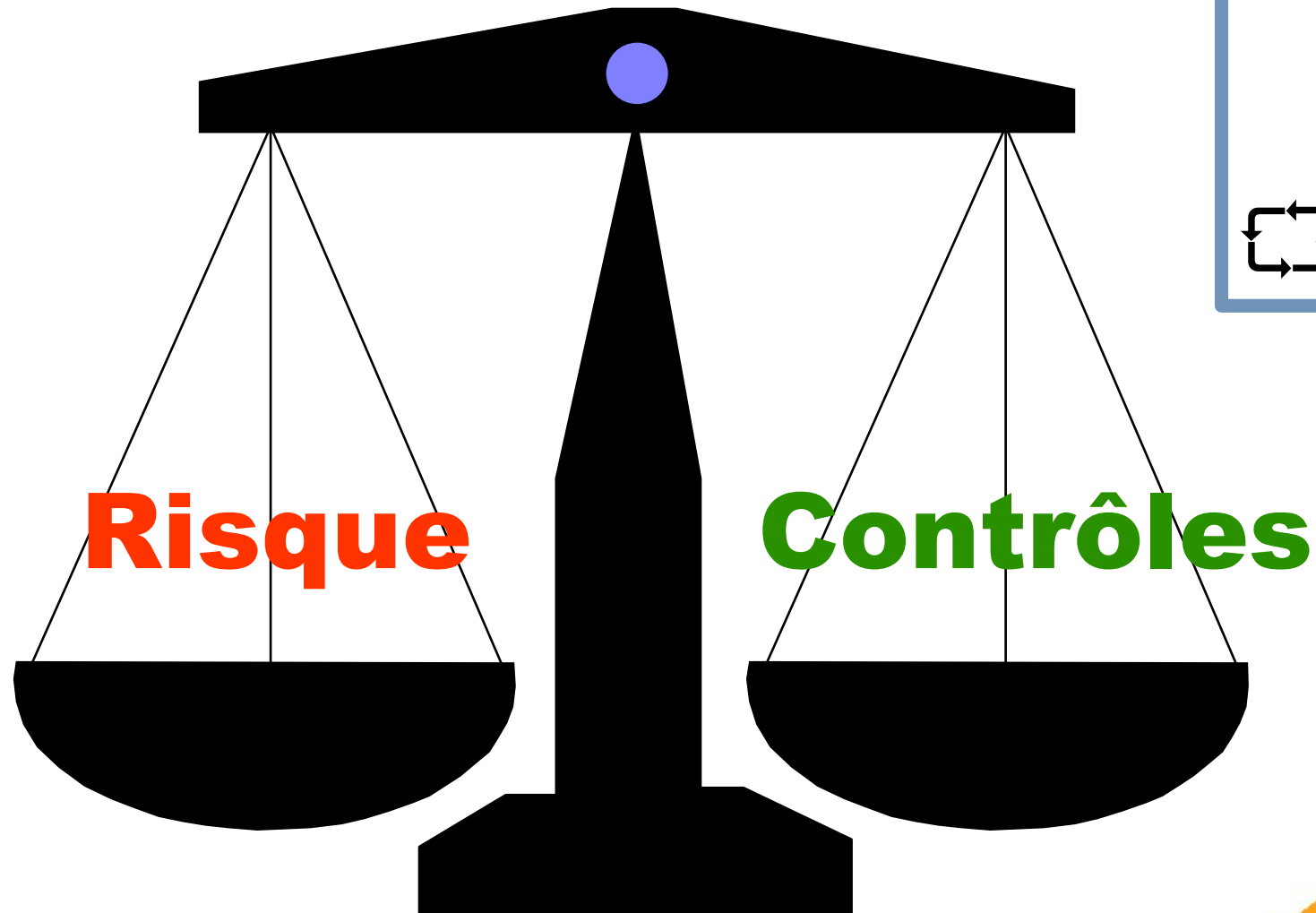


OUTPUT

OUTPUT

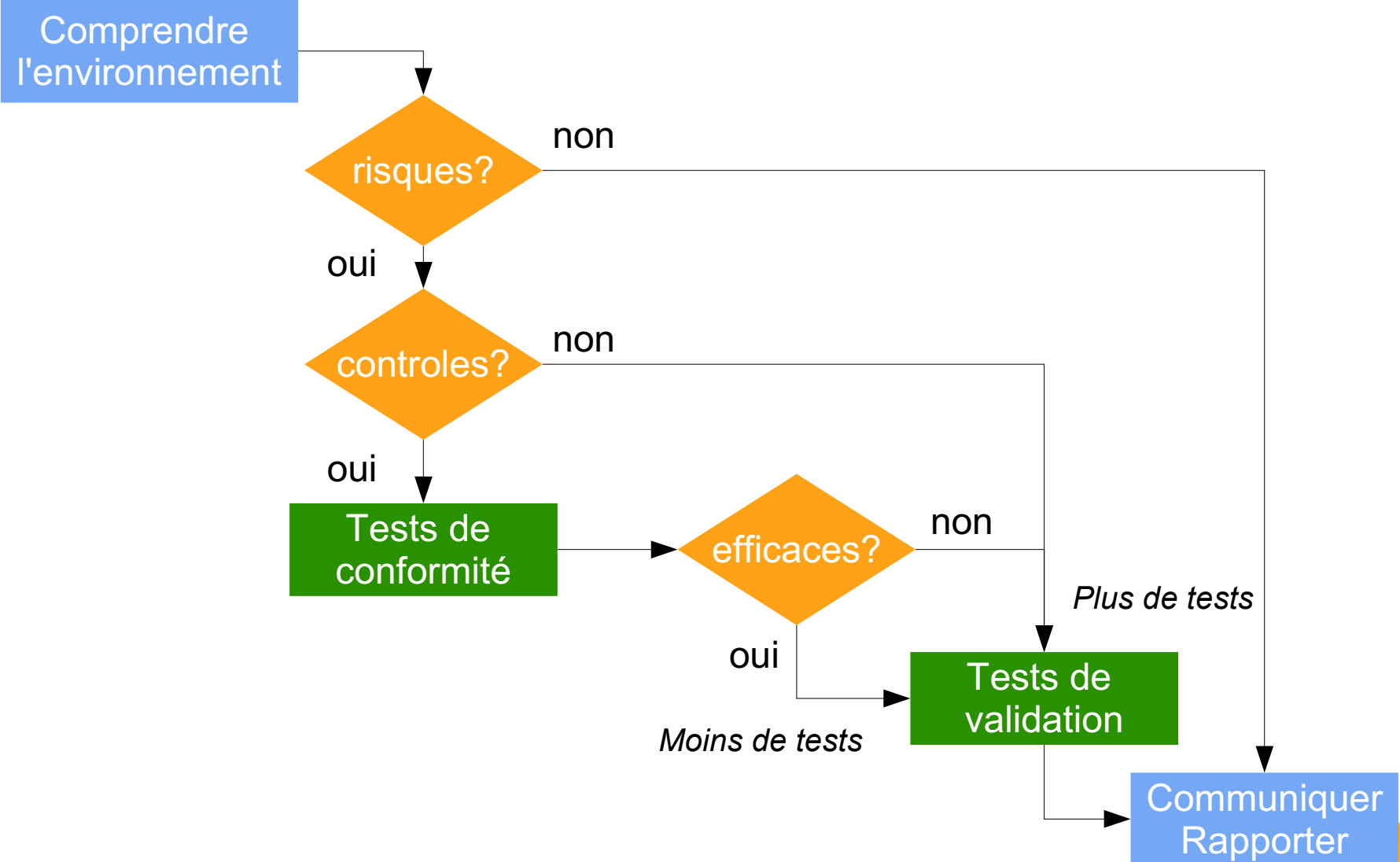
# Niveau de contrôle

→ L'approche d'audit → 3. Identification des contrôles



# Communication des résultats

→ *L'approche d'audit*



## *Audit et services connexes*

	Audit	Services connexes		
Nature du service	Audit	Review (examen succinct)	Procédures d'audit convenues	Compilation d'informations
Niveau d'assurance donné par l'auditeur	Assurance élevée (et non absolue)	Assurance modérée	Pas d'assurance	Pas d'assurance
Rapport	Assurance positive sur les assertions	Assurance négative sur les assertions	Constatations	Identification des informations compilées

- ▶ Communiquer

- Constats et recommandations (importance et priorités)

nBnBgo

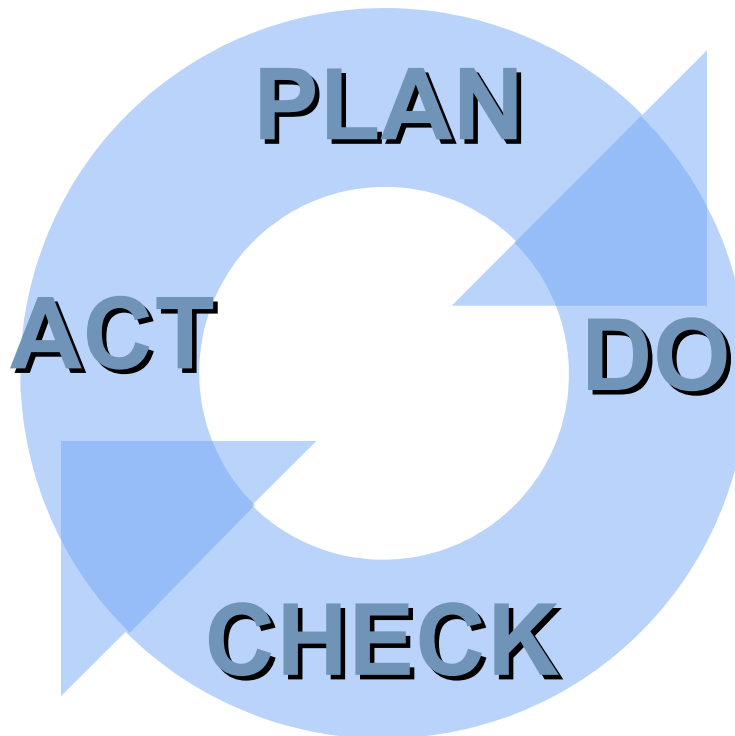
Enti

**B3B** VEILLE &  
CONNAISSANCE  
.ch

*Intelligence économique  
pour la Banque et la Finance*

→ *L'approche d'audit*

- ▶ S'assurer de la mise en oeuvre des recommandations selon les délais convenus



# Conclusion

- ▶ Pour le chef de projet, l'audit permet de
  - S'assurer de la bonne couverture de la gestion des risques
  - S'assurer de la bonne appréciation des risques du projet
  - Valider le design et l'efficacité des contrôles mis en place pour le pilotage du projet
  - Identifier les faiblesses éventuelles
  - Obtenir une nouvelle vision du projet (conseil / advisory)
  - Discuter / échanger avec un spécialiste « indépendant »
  - ...

# *Merci pour votre attention*

Marc Barbezat

*Email:* [marc.barbezat@b3b.ch](mailto:marc.barbezat@b3b.ch)

*Site:* <http://www.b3b.ch/>

*Blog:* <http://blog.b3b.ch/>

**B3B** VEILLE &  
CONNAISSANCE  
.ch

*Intelligence économique  
pour la Banque et la Finance*

- ▶ Recommandations des contrôles des finances à l'égard des projets informatiques  
[http://www.isaca.ch/files/Novena\\_V2\\_f.pdf](http://www.isaca.ch/files/Novena_V2_f.pdf)
- ▶ Normes d'Audit Suisse, Chambre fiduciaire  
[http://www.treuhand-kammer.ch/pix/files/neu\\_ps\\_fr1.pdf](http://www.treuhand-kammer.ch/pix/files/neu_ps_fr1.pdf)
- ▶ Formation CISA en Suisse Romande  
[http://www.iseig.ch/cours/aff\\_cnnx.php?cnnx\\_nRef=97&cnnx\\_nLien=2](http://www.iseig.ch/cours/aff_cnnx.php?cnnx_nRef=97&cnnx_nLien=2)
- ▶ ISACA, Information Systems Audit and Control Association  
<http://www.isaca.ch/> , <http://www.isaca.org/>
- ▶ Banque Cantonale Vaudoise  
<http://www.bcv.ch/>
- ▶ Wikipedia, L'encyclopédie libre  
<http://www.wikipedia.org/>