

# Recommandations des contrôles des finances à l'égard des projets informatiques

**Groupe de travail IT Government Audit**

Le groupe rassemble les auditeurs informatiques des administrations publiques suisses

Contact: [info@efk.admin.ch](mailto:info@efk.admin.ch)



# Pourquoi cette brochure?

Les responsables de projet sont soumis à de nombreuses contraintes et doivent conduire leurs projets au succès dans des conditions parfois difficiles.

L'intervention d'un auditeur constitue un défi supplémentaire souvent perçu comme une inutile chicane par les responsables. Les Contrôles des finances estiment important de communiquer de manière ouverte et consé- quente avec les responsables de projet. **Cette brochure est là pour répondre à des questions qui sont fré- quemment posées aux auditeurs.** Elle contient également des informations intéressantes pour les décideurs, les responsables informatiques ou les personnes chargées de l'assurance-qualité.

L'objectif est notamment de déterminer la liste des documents les plus importants pour un auditeur et de définir les questions auxquelles ils doivent répondre. Cette brochure se concentre sur la phase de projet qui constitue un passage important de la vie d'une application.

Il existe en Suisse différentes méthodes de développement (y compris celles qui sont proposées par certains fournisseurs) et la terminologie peut varier de l'une à l'autre. Cette brochure se concentre sur le contenu des documents et vous fournit les références à ces différentes méthodes.

Votre contrôle des finances (communal, cantonal ou fédéral) est à disposition si vous avez des questions complémentaires.

## Les objectifs à atteindre

Malgré la diversité des législations communales, cantonales et fédérale, les objectifs à atteindre par les projets informatiques sont les mêmes partout.

Ces objectifs découlent:

- du principe supérieur de la bonne gestion des crédits accordés (principes d'efficacité et d'efficience),
- du principe de légalité (conformité) et
- du principe de la tenue régulière de la comptabilité (principes d'intégrité, de disponibilité et de fiabilité).

Ces principes recouvrent entièrement les notions classiques de sécurité et de qualité du traitement de l'information.

Le modèle de référence CobiT ([www.isaca.org](http://www.isaca.org)) est souvent utilisé par les auditeurs, en particulier lorsqu'il s'agit d'auditer les contrôles généraux dans le domaine informatique. CobiT retient 7 critères correspondant à ces objectifs.

# Rappel:

## Quels sont les objectifs à atteindre?

<b>efficacité</b> <b>efficience</b>	Atteinte des objectifs fixés initialement Utilisation optimale des ressources
<b>conformité</b>	Respect des lois, réglementations et clauses contractuelles
<b>intégrité</b> <b>confidentialité</b> <b>disponibilité</b>	Exactitude, validité et intégralité des informations Protection contre toute divulgation non autorisée Disponibilité des systèmes, des ressources et des données
<b>fiabilité</b>	Mise à disposition d'informations fiables

## Les documents-clés

La méthode « Hermes » ([www.hermes.admin.ch](http://www.hermes.admin.ch)) définit près d'une centaine de documents qui devraient être élaborés durant la vie d'un projet informatique.

Pour un auditeur, une dizaine d'entre eux sont indispensables, et ce quelle que soit la méthode de développement adoptée (y compris les nouvelles méthodes dites « agiles »!).

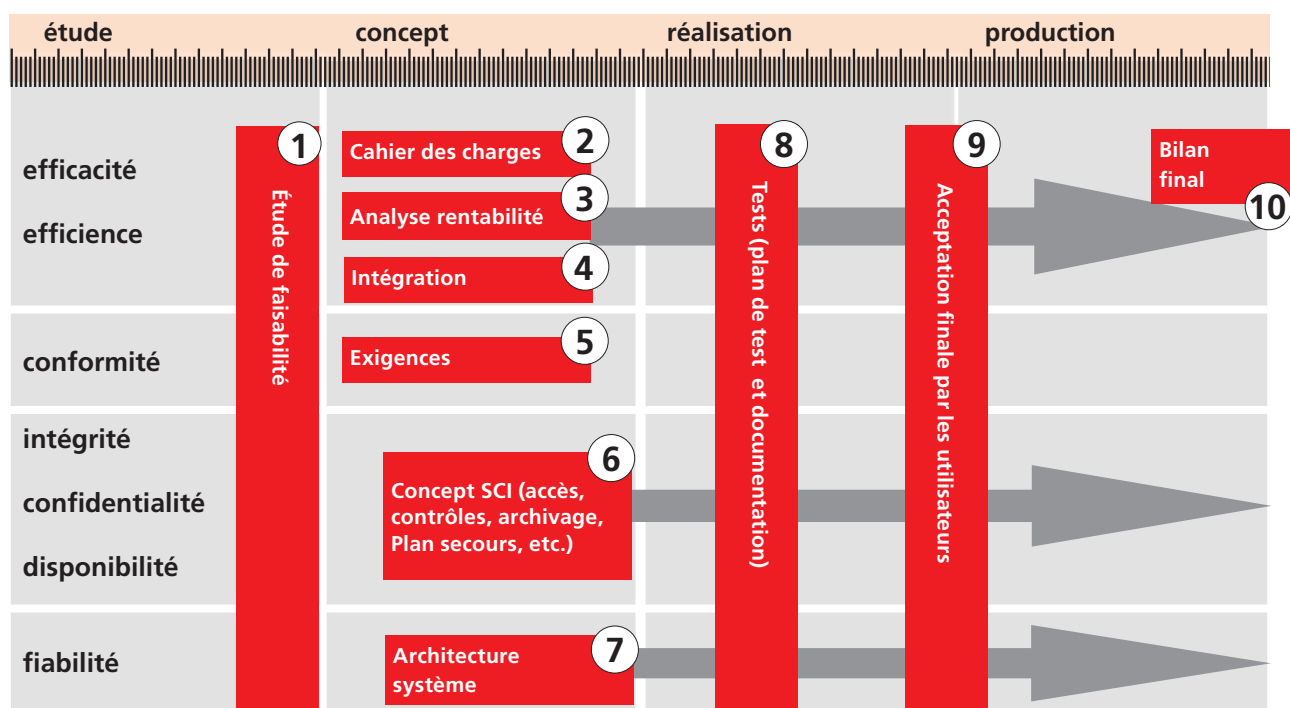
Les exigences formelles à leur égard sont cependant élevées:

- Ils doivent être validés et signés.
- Ils doivent être disponibles à un moment précis du projet (une étude de faisabilité intervenant après la phase de concept n'a plus d'utilité)
- Pour certains d'entre eux, ils doivent être tenus à jour non seulement durant tout le projet mais après le passage en production jusqu'au démantèlement final de l'application (l'architecture du système ou le concept du système de contrôle interne par exemple)

**Les recommandations se concentrent sur les documents produits par le projet**



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



## Communication des dix documents-clé

Le Contrôle des finances souhaite-il recevoir une copie de chacun de ces documents? En principe non, il les consultera le cas échéant à l'occasion d'un audit du projet ou de la future application.

Il est en revanche essentiel que le Contrôle des finances ait connaissance de l'existence de chaque projet informatique d'importance\*, raison pour laquelle:

- tous les « mandats de projets » doivent lui être transmis systématiquement et spontanément ,
- un inventaire toujours actualisé des projets en cours doit être tenu à sa disposition.

\* les directives communales, cantonales et fédérales respectives définissent ce qui doit être compris comme un « projet informatique d'importance »

## Les liens vers les principales sources citées

Hermes SE/DS (édition 2003), Hermes SA/VAS (édition 2005), <http://www.hermes.admin.ch>

Ordonnance concernant la tenue et la conservation des livres de comptes (Olico, RS 221.431)

[http://www.bk.admin.ch/ch/f/rs/221\\_431/index.html](http://www.bk.admin.ch/ch/f/rs/221_431/index.html)

CobiT Version 4.0, <http://www.isaca.ch>

Manuel suisse d'audit (MSA) et normes de la Chambre Fiduciaire suisse <http://www.treuhand-kammer.ch>

PRINCE 2 [www.ogc.gov.uk/prince](http://www.ogc.gov.uk/prince)

# 1. Etude de faisabilité



Quels sont les objectifs du système ?  
Quelles sont les solutions envisageables ?

- Recenser et analyser les exigences envers le système
- Elaborer des propositions de solution (variantes)
- Comparer les coûts, les risques et les avantages de ces variantes

Quelles sont les exigences envers le projet et l'organisation ?  
Le projet est-il réalisable ?  
Le projet peut-il passer à la phase de conception (mandat de projet) ?

Responsable:  
Service utilisateur (appuyé par le Service informatique pour les questions techniques)

## Références utiles (liste non-exhaustive!)

Hermes : Chap. 3.3 (SE et SA)  
POSAT ZH : Ablaufschritt 2  
CobiT 4.0 : AI 1.3  
PRINCE 2 : Processus SU

# 2. Cahier des charges



Quels sont les objectifs à atteindre?  
Quelles sont les attentes des utilisateurs?

- Quelles sont les fonctionnalités?
- Quels sont les volumes à traiter?

Quelles sont les contraintes à respecter?  
Quels sont les moyens techniques nécessaires à l'atteinte de ces objectifs?

Responsable:  
Service utilisateur (appuyé par le Service informatique pour les questions techniques)

## Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 5.3.47, SA Chap. 3.4.1, 5.3.50  
POSAT ZH : Ablaufschritt 3  
CobiT 4.0 : PO 10.5, AI 1.1  
PRINCE 2 : Processus IP

### 3. Analyse de la rentabilité



Quels sont les coûts complets du projet (y compris les dépenses connexes, par exemple: coût de la migration des données, augmentation de la capacité des installations, formation des utilisateurs, etc...)?  
Comment apprécier quantitativement et qualitativement l'utilité escomptée?  
Quelle est la rentabilité du projet?  
Quels sont les scénarios envisageables propres à modifier la rentabilité du projet?

Responsable:  
Service utilisateur

#### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 5.3.92, SA Chap. 5.3.98  
POSAT ZH : Ablaufschritt 5  
CobiT 4.0 : AI 1.1, AI 1.2, AI 1.3  
PRINCE 2 : Processus DP et CS

### 4. Intégration dans l'environnement informatique



Le projet s'intègre-t-il harmonieusement dans la stratégie et l'architecture IT de l'entreprise?  
Le projet ne fait-il pas double-emploi avec un autre projet ou une application existante?  
Existe-t-il des synergies avec d'autres projets?  
Le projet respecte-t-il les standards adoptés par l'entreprise?  
Quelles interfaces automatiques ou manuelles sont prévues ?

Responsable:  
Service informatique

#### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 5.3.83, SA Chap. 5.3.31, 5.3.89  
POSAT ZH : Ablaufschritt 8  
CobiT 4.0 : PO 2, AI 1.3  
PRINCE 2 : Processus SB

## 5. Exigences à respecter



Quelles sont les exigences internes (conventions, procédures, normes de qualité)?

Quelles sont les exigences externes (lois, ordonnances, directives, contrats) éventuellement spécifiques à certaines branches (protection des données, publication, procédures d'achat, banques, best practices Good xxx Practice, etc.)?

Quelles sont les conséquences de ces exigences en terme de procédures ou d'équipements (architecture, sécurité, etc...)?

Responsable:

Service utilisateur (appuyé par le Service informatique pour les questions techniques)

### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 3.4.4, 5.3.31, 5.3.80, SA Chap. 5.3.32, 5.3.87

POSAT ZH : Ablaufschritt 1

CobiT 4.0 : PO 2, ME 3

## Exemples d'exigences à respecter (liste non exhaustive)

### Domaine du personnel

- Fiscales (certificat de salaire, impôt à la source, etc..)
- Relatives aux assurances sociales (AVS, AC, APG, etc..)
- Relatives à la protection des données (concept le droits d'accès, déclaration le confidentialité etc.)

### Domaine financier

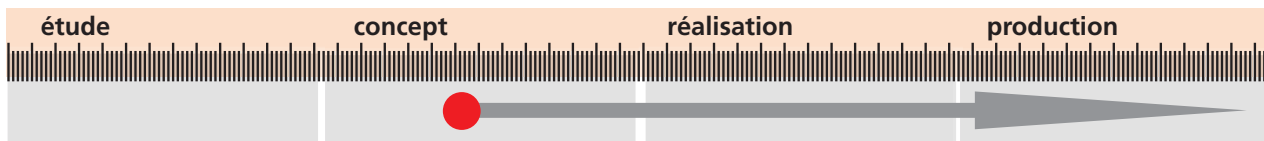
- Relative à la tenue des livres et à la conservation des pièces (Olico)
- Relatives au blanchiment

### Domaine de la santé

- Relative à la comptabilité analytique dans les hôpitaux
- Relative à la traçabilité des produits et médicaments
- Relative à la protection des données

Etc....

## 6. Concept du système de contrôle interne (SCI)



Quels contrôles automatisés sont-ils nécessaires (validations à la saisie, réconciliations automatiques, listes d'erreurs, etc.)?

Quelles séparations des fonctions sont-elles nécessaires et comment sont-elles répercutées dans la gestion des droits d'accès?

Quelles sont les mesures à mettre en place pour assurer la traçabilité des opérations, y compris la paramétrisation de l'application?

Quelles sont les mesures à prendre pour assurer la continuité de l'exploitation (plan de secours) et la conservation des données (plan d'archivage)?

Responsable:

Service utilisateur (appuyé par le Service informatique pour les questions techniques)

### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 5.3.31, SA Chap. 5.3.32

POSAT ZH : Ablaufschritt 10, 11

CobIT 4.0 : PO 8, AI 1.1, AI 1.2, AI 2.2, AI 2.3, AI 2.4, DS 4, DS 5, DS 11, ME 2

PRINCE 2 : Processus SU

Chambre fiduciaire : NAS 400, Chiffres 3.24233, 3.3222 ss. MSA

## 7. Architecture du système



Comment le système informatique est-il structuré?

Quelle est l'architecture des informations (modèle de données)?

Quelles sont les fonctionnalités du système?

Comment le système s'intègre-t-il dans l'architecture des systèmes existants?

Comment les informations interagissent-elles entre elles?

Quelles sont les interfaces?

Responsable:

Service informatique

### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 5.3.81, 5.3.82, SA Chap. 5.3.88, 5.3.89

POSAT ZH : Ablaufschritt 14

CobIT 4.0 : PO 2, AI 1.3, AI 2.1, AI 2.2, AI 2.5, AI 2.6

## 8. Tests (plan de test et documentation)



Quels sont les objectifs des tests?  
Quels sont les tests prévus (méthodes, utilitaires, critères, cas)?  
Quels sont les ressources et les délais d'exécution?  
Les corrections de dernière minute seront-elles encore testées?  
Comment le déroulement exact des tests et les résultats sont-ils documentés?

Responsable:  
Service informatique (et Service utilisateur)

### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 5.3.85 à 5.3.90, SA Chap. 5.3.91 à 5.3.96  
POSAT ZH : Ablaufschritt 14  
CobIT 4.0 : PO 8, AI 2.8, AI 3.4, AI 5.6, AI 7.2, AI 7.4, AI 7.6, AI 7.7

## 9. Acceptation par les utilisateurs



Quelle est la portée de l'acceptation?  
Qui sont les propriétaires des données et les responsables de l'application?  
Qui est responsable de l'acceptation?  
Sur quels tests se fonde cette acceptation?  
Quelles sont les éventuelles réserves à l'acceptation?

Responsable:  
Service utilisateur

### Références utiles (liste non-exhaustive!)

Hermes : SE Chap. 3.3.6, 3.4.7, 3.5.8, 3.6.7, SA Chap. 3.3.7, 3.4.9, 3.5.11, 3.6.7  
POSAT ZH : Ablaufschritt 14, 15  
CobIT 4.0 : AI 3.1 à 3.3, AI 7.6, AI 7.7, PO 10.6

# 10. Bilan final



- Les objectifs et exigences du projet sont-ils atteints?
- Quels sont les coûts définitifs et les explications pour les écarts éventuels par rapport aux prévisions initiales?
- Quel est le calcul définitif de la rentabilité?
- Quels sont les risques existants après l'implémentation?
- Quelles sont les erreurs survenues après le passage en production?
- Quelles sont les recommandations et mesures proposées?
- Quels sont les enseignements à tirer du projet?

Responsable:  
Service utilisateur

## Références utiles (liste non-exhaustive!)

- Hermes : Chap. 5.3.13 (SE et SA)
- POSAT ZH : Ablaufschritt 16
- CobiT 4.0 : PO 10.6, PO 10.13, PO 10.14, AI 7.12

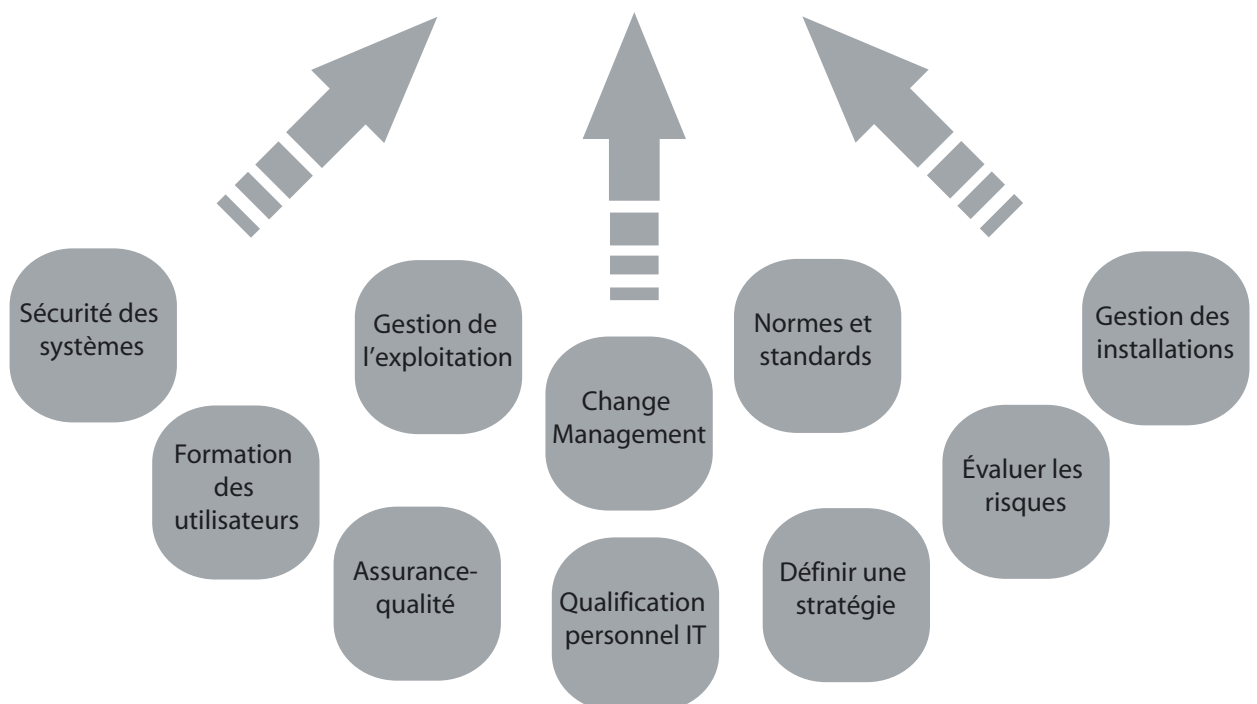
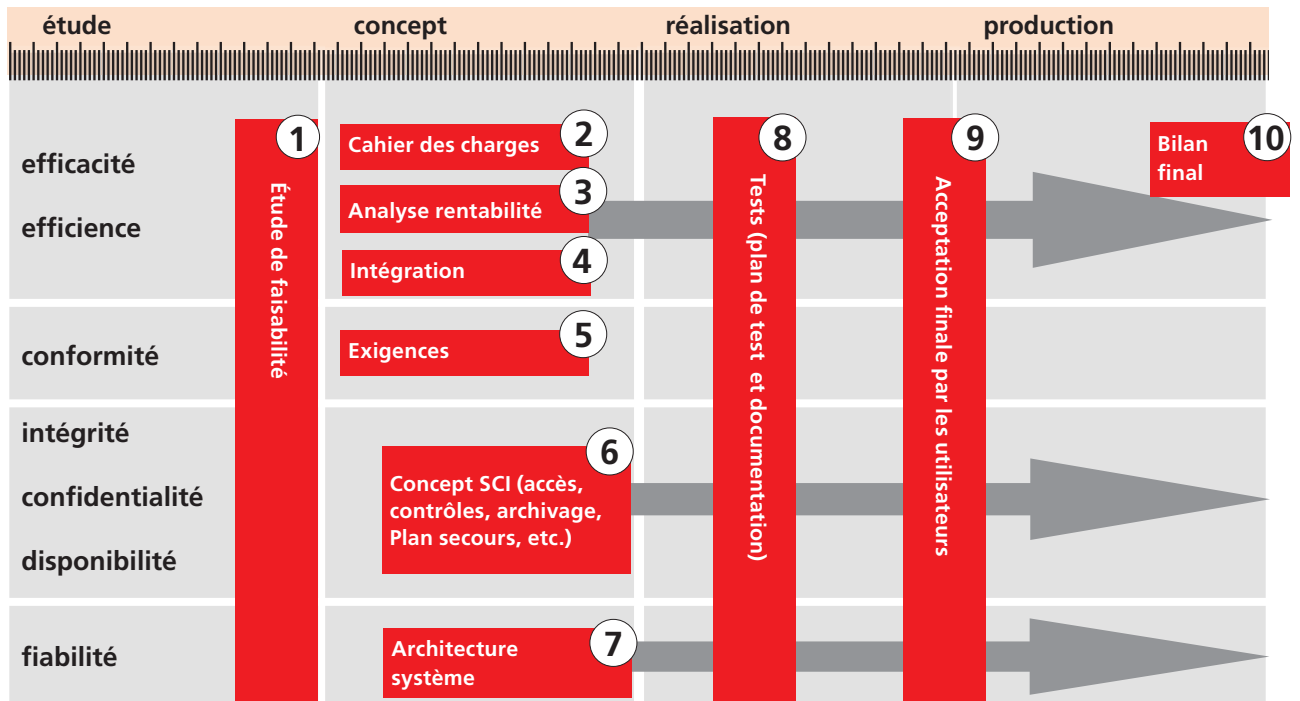
## Ne pas négliger le contexte du projet

Un projet ne se déroule pas en vase clos. Son succès est directement influencé par le contexte dans lequel il est conduit. Au nombre des facteurs importants: la forte implication des utilisateurs dans le projet, la qualification des personnes intervenant dans le projet, le degré de standardisation de l'entreprise, les systèmes d'assurance-qualité et les procédures garantissant une gestion correcte des différentes versions de programme.

CobiT identifie pour 34 processus informatiques standards les objectifs de contrôle à respecter pour assurer la maîtrise de l'informatique.

Le processus (Distribution et support 8) « Gérer le Service Desk et les incidents » traite par exemple des règles applicables au système de gestion des problèmes, à leur escalade, au suivi de leur résolution et aux pistes d'audit, aux autorisations d'accès temporaires ou en urgence, ainsi qu'aux priorités des traitements d'urgence.

# Tenir compte des facteurs d'influence externes...



# ...et les principes de bonne gestion de projet

## Quelques enseignements tirés d'audits communs des Contrôles des finances:

- La réalisation d'un projet de grande ampleur n'est possible qu'avec du personnel travaillant à plein temps pour ce projet.
- Un projet important doit bénéficier d'un appui politique correspondant.
- Il est essentiel de réorganiser et d'harmoniser avant d'informatiser.
- Raccourcir la durée du projet ou le découper en sous-projets autonomes.
- Eviter les technologies émergentes.
- L'équilibre entre informaticiens et spécialistes métiers doit être adéquat.
- Pas trop d'organes de controlling mais un vrai controlling.
- Identifier et évaluer le plus tôt possible les problèmes, notamment par des tests de faisabilité.
- Identifier correctement les fournisseurs et régler contractuellement leurs relations avec le projet.
- Répercuter contractuellement les éventuelles adaptations de l'organisation de projet.
- Ne pas sous-estimer les problèmes que pose le développement en deux - voire en trois - langues.

## En guise de conclusion

La décision d'intervenir dans un projet informatique appartient au Contrôle des finances. Plusieurs considérations vont guider notre choix, en particulier l'appréciation des risques que présente ce projet par rapport à d'autres projets comparables.

Notre intervention peut prendre la forme d'un examen du projet (en particulier au terme d'une phase de projet) ou d'une prise de position sur des questions particulières (par exemple évaluation du concept SCI avant sa mise en œuvre).

N'hésitez pas à nous soumettre votre problème!