

**JS Quality Consult**

Management et Organisation

Jean Simon

Rue Petit Jonckeu, 28

B-4910 POLLEUR

Tél.: +32(0) 87 22 61 07

Fax: +32(0) 87 22 61 08

GSM: +32(0) 475 68 41 95

Email: js@jsqc.be

TVA BE 459-472-172

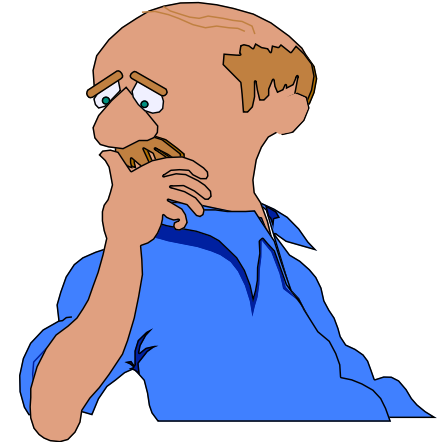
# JCA du 14 octobre 2016

## NOVOTEL Luxembourg Centre

### Notions de risques dans les normes d'accréditation

Gestion de l'impartialité

Gestion des processus



# Ethique et déontologie d'un organisme accrédité

- 1. Compétence :** aptitude à mettre en pratique des **connaissances et un savoir-faire** pour obtenir les résultats escomptés.
- 2. *Impartialité* :** existence d'**objectivité**.
- 3. Confidentialité :** être responsable du management de toutes les **informations obtenues ou générées** pendant la réalisation des activités.

# Gestion de l'impartialité

## Généralités

La structure juridique, l'indépendance financière et la maîtrise de la gestion par la stricte application du système de management permettent d'assurer la conformité aux exigences de la norme.

La direction garantit l'impartialité, l'indépendance technique et l'intégrité de l'organisme dans ses activités et s'interdit expressément toute influence sur les résultats.

L'organisme et tout le personnel rejeteront, sans détours, toute pression extérieure, commerciale, financière ou sous quelque forme que ce soit.

La rémunération du personnel n'est pas liée au nombre d'activités effectuées ni au laps de temps nécessaire à leurs réalisations.

## Que disent les normes ?

### § 4.1.3 ISO/CEI 17020: 2012

**Identifier en continu** les risques susceptibles **de porter atteinte** à son impartialité.

### § 4.2.3 ISO/CEI 17065: 2012

**Identifier régulièrement** les risques susceptibles **de nuire** à son impartialité.

### § 5.2.3 ISO/CEI 17021-1: 2015

**Disposer d'un processus** pour **identifier, analyser, évaluer, traiter, surveiller et documenter** les risques liés aux conflits d'intérêts.

## Que disent les normes ?

### § 4.1.1.3.c ISO/CEI 15189: 2012

Les éventuels conflits d'intérêts **doivent être ouvertement et correctement déclarés**.

### § 4.1.5.d ISO/CEI 17025: 2005

**Avoir des politiques et des procédures** permettant d'éviter l'engagement dans toute activité qui **réduirait la confiance** en son impartialité.

### § 4.1.3 CD2 ISO/CEI 17025

The laboratory shall **identify risks** to its impartiality **on an on-going basis**.

## Notes

- Cette identification doit inclure les risques découlant de ses activités ou de ses relations, ou les relations de son personnel.  
Cependant, ces relations **ne présentent pas nécessairement** un risque pour l'impartialité de l'organisme.
- Une relation présentant un risque pour l'impartialité peut résulter de facteurs tels que la propriété, la gouvernance, le management, le personnel, le partage de ressources, la situation financière, des contrats, la formation, la commercialisation, le paiement de commissions sur les ventes ou autres incitations à l'apport de nouveaux clients, etc...
- L'identification des risques **n'implique pas** une évaluation du risque selon l'ISO 31000.

## Définitions

§ 4.2.4 ISO 17021-1: Les menaces qui pèsent sur l'impartialité peuvent inclure les suivantes, sans s'y limiter :

a) les **intérêts personnels** :

cette menace est due au fait qu'une personne ou une entité **agisse dans son propre intérêt**. Son intérêt financier **représente une menace susceptible de compromettre l'impartialité** d'une certification;

b) l'**autoévaluation** :

cette menace est due au fait qu'une personne ou une entité **évalue son propre travail**. Auditer le système de management d'un client auquel l'organisme de certification a prodigué des conseils en matière de système de management **crée un risque dû à l'autoévaluation**;

## Définitions

§ 4.2.4 ISO 17021-1: Les menaces qui pèsent sur l'impartialité peuvent inclure les suivantes, sans s'y limiter :

c) la **familiarité** (ou confiance) :

cette menace est due au fait d'**entretenir une trop grande proximité** relationnelle **ou** de **faire trop confiance** aux personnes auditées **plutôt que de rechercher des preuves** lors des audits;

d) l'**intimidation** :

cette menace est due au fait qu'une personne ou une entité **éprouve la sensation de subir des pressions** directes ou insidieuses, par exemple la **menace d'être remplacée ou dénoncée** à sa hiérarchie.

## Que faire en cas de risque identifié ?

### § 4.1.3 ISO/CEI 17020: 2012

L'organisme d'inspection doit pouvoir **démontrer** comment il l'**élimine** ou le **minimise**.

### § 4.2.3 ISO/CEI 17065: 2012

L'organisme de certification doit pouvoir **apporter la preuve** de la manière dont il **élimine** le risque ou le **limite** au minimum.

### § 5.2.3 ISO/CEI 17021-1: 2015

L'organisme de certification doit **documenter et apporter la preuve** de la manière dont il **élimine** ou **limite** ces menaces au minimum **et documenter tout risque résiduel**.

## Exemple pratique

Risques	Sous-risques	Mesures prises	Elimination Limitation du risque
Intérêts personnels	Filiale de l'organisme comme client.	Pas de prestation fournie.	Elimination
	Membre d'un Comité interne postule comme client.	Pas de prestation fournie.	
	Liens professionnels de l'organisme avec un postulant.	Pas de prestation fournie.	
Autoévaluation	L'auditeur/inspecteur a déjà travaillé pour le client (< 2 ans).	Code de conduite : révéler tout conflit d'intérêt.	Limitation
		Liste annuelle des clients des auditeurs / inspecteurs (pour freelance).	
		Audit confié à un autre auditeur/inspecteur si déjà travaillé pour le client.	
Familiarité	Proximité de l'auditeur/inspecteur vis-à-vis du client.	Code de conduite : révéler tout conflit d'intérêt.	Limitation
	Proximité relationnelle ou faire trop confiance aux personnes auditées / inspectées.	Limiter les interventions d'un même auditeur / inspecteur dans le temps (ex. : max. 3 ans). Supervision régulières des auditeurs/inspecteurs.	
Intimidation	Pressions directe ou insidieuse.	Code de conduite : révéler tout conflit d'intérêt. Information à la Direction.	Limitation

## *Identifier en continu ?*

Les facteurs de risque identifiés à chaque étape du processus opérationnel (depuis la demande jusqu'à l'émission du rapport/certificat) sont passés en revue pour évaluer le risque de perte éventuelle de l'impartialité et prendre, le cas échéant, une décision quant à la suite à donner.

Lorsqu'un risque est détecté à la revue de contrat, la situation est analysée pour savoir si ce risque peut être maîtrisé et si le processus opérationnel peut être poursuivi.

Cette analyse de risque est évaluée au minimum lors des réunions périodiques trimestrielles et lors des revues de direction.

## Approche par les risques

### § 4.14.6 ISO/CEI 15189 : 2012 Gestion des risques

Le laboratoire doit **évaluer l'impact des processus de travail** et défaillances potentielles **sur la sécurité des résultats des examens**

et

doit **modifier les processus** pour **réduire ou éliminer** les risques identifiés, et **documenter les décisions** et actions menées.

## NEW Concept ISO 17025

### § 8.5 CD2 ISO/CEI 17025: *Actions à mettre en œuvre face aux risques et opportunités*

Le laboratoire **doit déterminer** les **risques** et **opportunités** associés à ses activités.

Le laboratoire **doit planifier** :

- a) les **actions à mettre en œuvre** face aux risques et opportunités,
- b) Comment :
  - 1) **intégrer** et **mettre en œuvre ces actions** au sein de son SMQ,
  - 2) **évaluer l'efficacité** de ces actions.

Les **actions** mises en œuvre face aux risques et opportunités **doivent être proportionnelles à l'impact** potentiel sur la validité des activités du laboratoire.

**Le risque est inhérent à toute activité humaine :**

- Traverser une rue,
- Investir en bourse,
- Changer d'employeur,
- Partir en vacances,
- Pratiquer une activité sportive.

Consciemment ou inconsciemment *nous pratiquons* à chaque instant, en faisant des choix, *une gestion du risque*.

La gestion du risque est un *processus clé dans la gestion d'entreprise* comme il l'est pour l'individu.

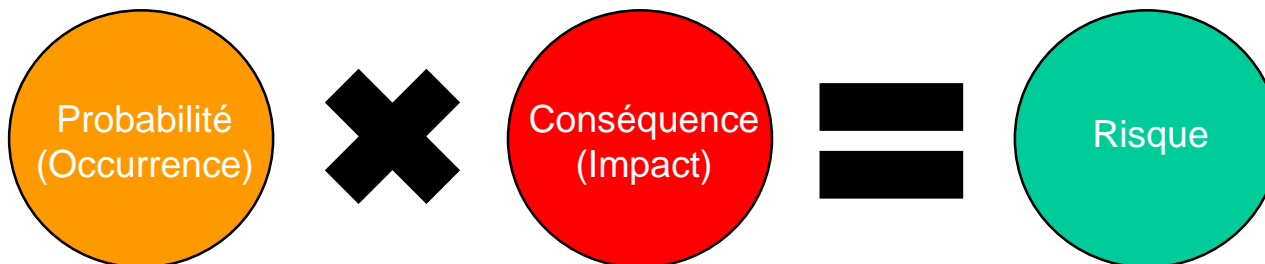
# Risques et Opportunités

Les scénarios à risque peuvent représenter des **opportunités** pour les organisations.

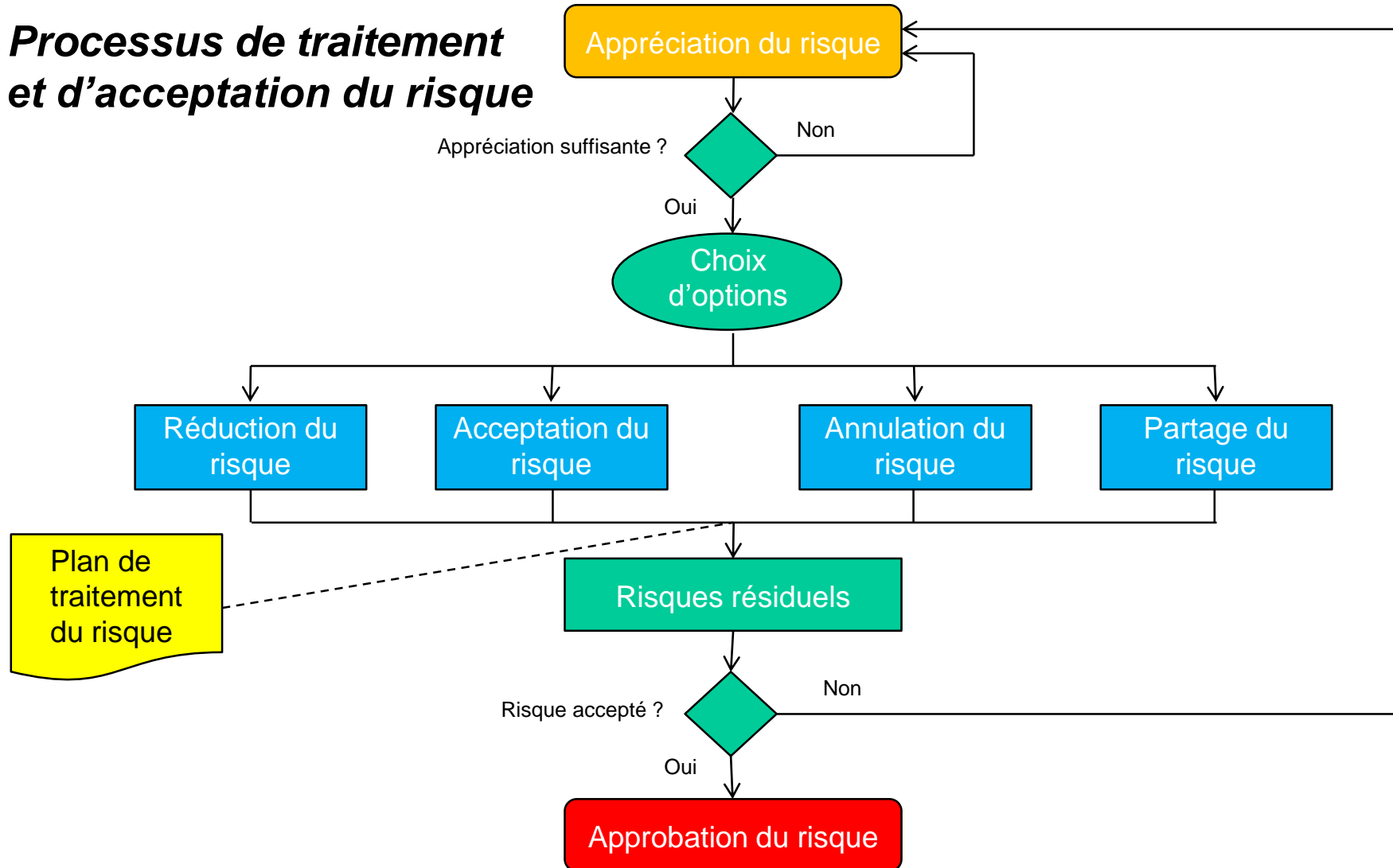
Le principe repose sur la « **prime de risque** », soit un gain ou avantage supplémentaire espéré en participant à une activité plus risquée.

Exemple : utilisation d'un logiciel BETA ou le Cloud

- Risques supérieurs (bugs, incompatibilités avec d'autres applications, personnel non formé, etc...)
- Gains de productivité espéré doit être plus grand,



## Processus de traitement et d'acceptation du risque



## Risques détectés et évaluation

## Mesures de prévention et Evaluation Risque après mesures

PROCESSUS PROJET / PRODUIT CONTEXTE	Risque identifié	Probabilité d'apparition du risque P	Gravité des conséquences G	Niveau de Risque R	MESURES PREVENTIVES à appliquer MOYENS DE PROTECTION prévus MOYENS DE DETECTION prévus	Probabilité d'apparition du risque P	Gravité des conséquences G	Niveau de Risque R
<b>Processus Préanalytique</b> Encodage	Erreur de patient	Probable	Grave	<b>CRITIQUE mesure nécessaire</b>	Demander le nom, prénom, date de naissance au patient. Se conformer à la procédure de prélèvement	Peu probable	Grave	<b>A surveiller</b>
<b>Processus Préanalytique</b> Prélèvement	Erreur d'encodage Erreur de patient	Peu probable	Grave	<b>A surveiller</b>	Vérifier la correspondance tubes – demandes – identité du patient. Formation des préleveurs	Peu probable	Grave	<b>A surveiller</b>
<b>Processus Analytique</b> Technique	Automate défaillant sur un ou plusieurs paramètres	Peu probable	Significatif	<b>Acceptable</b>	Réaliser les QC prévus et les actions correctives si nécessaire. Si résultat corrigé, le noter en commentaire.	Peu probable	Significatif	<b>Acceptable</b>
<b>Processus Analytique</b> Prélèvement	Qualité du prélèvement (coagulé, quantité insuffisante...)	Peu probable	Significatif	<b>Acceptable</b>	Eliminer les prélèvements non conformes et si possible en réclamer d'autres.	Peu probable	Significatif	<b>Acceptable</b>
<b>Processus Postanalytique</b> Résultats	Résultats aberrants (hors norme)	Peu probable	Significatif	<b>Acceptable</b>	Comparer les résultats à l'historique si disponible. Validation par le responsable technique.	Peu probable	Significatif	<b>Acceptable</b>
<b>Processus Achat</b>	Pénurie de réactif	Peu probable	Significatif	<b>Acceptable</b>	Gestion rigoureuse du stock. Sélection des fournisseurs	Peu probable	Significatif	<b>Acceptable</b>
<b>Processus Ressources humaines</b>	Manque de personnel en suffisance	Peu probable	Significatif	<b>Acceptable</b>	Gestion des remplaçants compétents	Peu probable	Significatif	<b>Acceptable</b>
<b>Processus Gestion des Equipements</b>	Panne d'équipement d'où arrêt des analyses et retard dans les protocoles	Peu probable	Significatif	<b>Acceptable</b>	Maintenance des équipements. Equipements en back-up	Peu probable	Significatif	<b>Acceptable</b>

### ECHELLE DE RISQUE

Echelle de probabilité	Attendu			<b>CRITIQUE, mesures nécessaires</b>
	Probable		<b>Risque à surveiller</b>	
	Peu probable	<b>Risque acceptable</b>		
		Anodin	Significatif	Grave
		Echelle de gravité		