

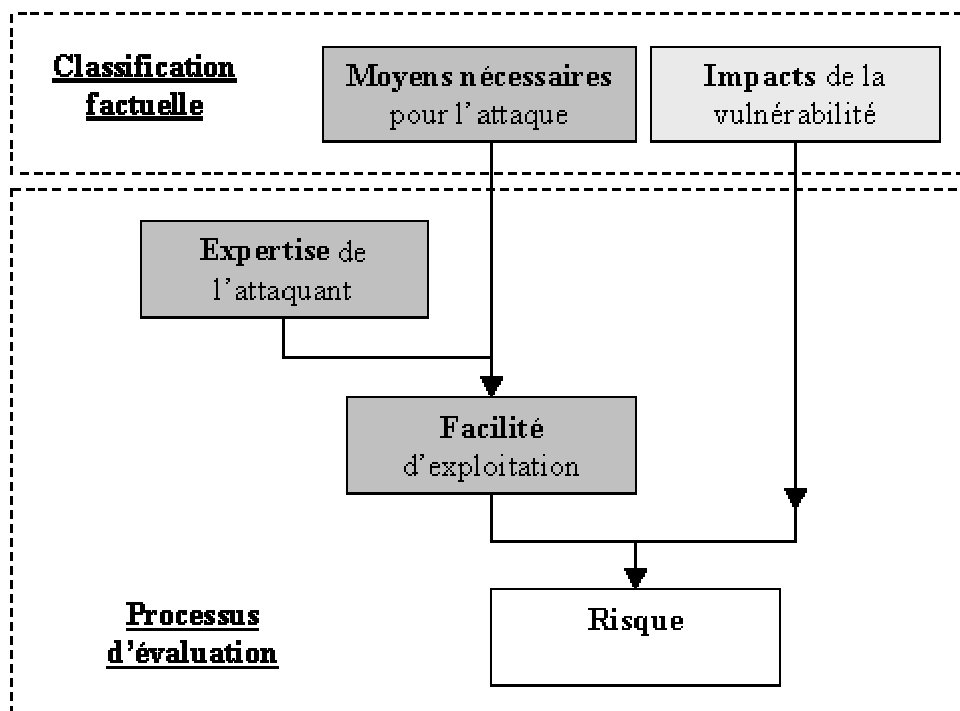
## ➤ Définition des niveaux de confiance pour les avis

A chaque avis de sécurité, le Cert-IST associe un niveau de confiance. Les différents niveaux de confiance possibles sont les suivants :

- **Faillle officielle et testée** : faille émanant d'un organisme officiel (CERT/CC, CIAC, AusCERT, ...) ou d'un constructeur, et testée par le Cert-IST,
- **Faillle officielle** : faille émanant d'un organisme officiel ou d'un constructeur,
- **Faillle testée** : faille n'émanant pas d'un organisme officiel ou d'un constructeur mais testée le Cert-IST,
- **Faillle probable** : faille n'émanant pas d'un organisme officiel ou constructeur n'ayant pas pu être testée mais fortement probable (regroupement d'informations concordantes),
- **Faillle non qualifiée** : faille n'émanant pas d'un organisme officiel ou constructeur, n'ayant pas pu être testée ni recoupée mais présentant une criticité élevée qui justifie sa diffusion avec réserve.

## ➤ Définition de la difficulté de mise en œuvre et du risque pour les avis

Le Cert-IST, en accord avec la métrique définie par le projet EISPP ([www.eispp.org](http://www.eispp.org)), effectue une classification de chaque avis émis de façon à indiquer au lecteur le niveau de risque associé pour le système d'information. Cette évaluation se base sur plusieurs paramètres qui, combinés entre eux, aboutissent à un paramètre unique appelé "**Risque**". Le schéma ci-dessous présente une vue générale de ce processus.



**Le Risque indique au lecteur l'importance de la vulnérabilité, et le degré d'urgence des mesures à mettre en œuvre pour contrer la menace.** Le tableau ci-dessous liste les recommandations du Cert-IST sur l'attitude à tenir en fonction du niveau de risque.

Risque	Recommandation
<b>Très élevé</b>	Agir immédiatement sur tous les systèmes
<b>Elevé</b>	Agir immédiatement sur les systèmes frontaux et les serveurs
<b>Moyen</b>	Les actions peuvent être reportées, mais une opération de maintenance sécurité doit être prévue dès à présent
<b>Faible</b>	Les actions peuvent être reportées jusqu'à la prochaine opération de maintenance sécurité

Les tables ci-dessous décrivent la méthode utilisée pour :

- combiner les **Moyens nécessaires** pour l'attaque avec l'**Expertise** nécessaire à l'attaquant de façon à obtenir la **Facilité d'exploitation** de l'attaque.
- puis combiner cette **Facilité d'exploitation** ainsi obtenue avec l'**Impact** de la vulnérabilité de façon à obtenir le **Risque**

	Moyens			
Expertise	A distance sans compte via un service standard	A distance sans compte via un service annexe	A distance avec compte	Accès physique
Débutant	Trivial	Facile	Modéré	Difficile
Compétent	Facile	Modéré	Difficile	Très difficile
Expert	Difficile	Difficile	Très difficile	Très difficile

	Sévérité de l'impact			
Facilité d'exploitation	Prise de contrôle	Obtention de privilèges Obtention d'un accès	Déni de service Perte d'intégrité Perte de confidentialité	Interruption de service Tremplin Camouflage
Trivial	Très élevé	Elevée	Elevée	Moyen
Facile	Très élevé	Elevée	Elevée	Moyen
Modéré	Très élevé	Elevée	Moyen	Moyen
Difficile	Elevée	Moyen	Moyen	Faible
Très difficile	Elevée	Moyen	Faible	Faible