➢ Définition des niveaux de risques pour les avis

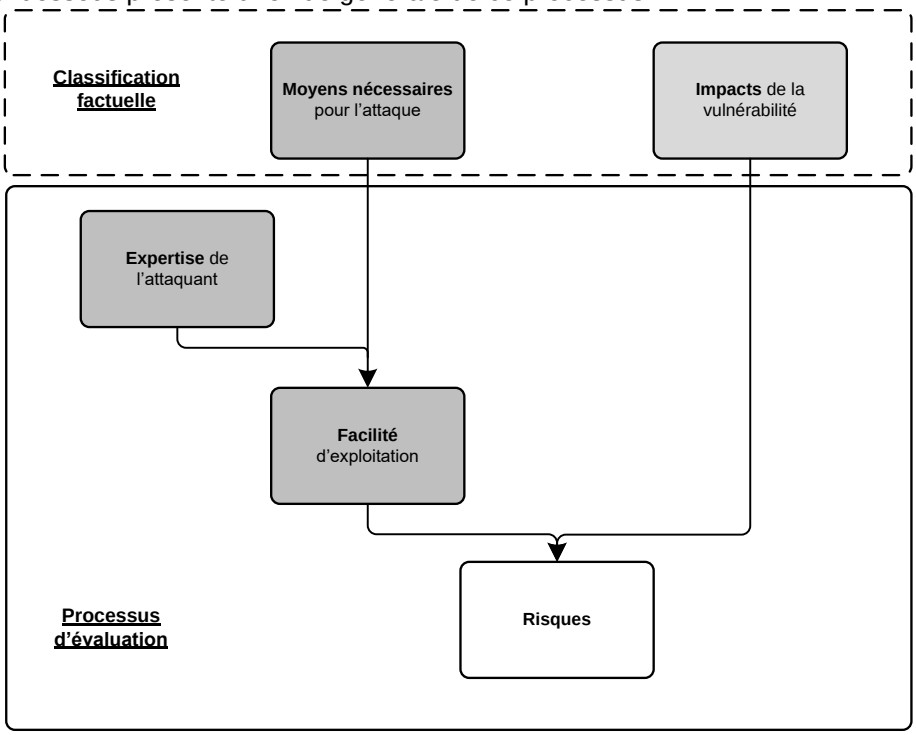
Dans ses avis de sécurité le Cert-IST propose 2 métriques pour évaluer le niveau de risque :

La métrique **CVSS** (depuis 2007)
La métrique définie par le projet **EISPP** (depuis 2003)

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.

CVSS est un standard défini par le FIRST (voir ce guide). Il utilise une dizaine de critères pour évaluer le risque sous forme d'une note décimale variant de 0 (pas de risque) à 10 (risque maximum). Son interprétation est assez complexe. Le Cert-IST fournit pour chaque avis le score CVSS de base et le score temporel en respectant la **version 3 de CVSS**.

Le risque **EISPP** est plus intuitif et a été défini par le projet Européen EISPP (www.cert-ist.com/eispp). Il utilise 3 paramètres qui, combinés entre eux, aboutissent à un paramètre unique appelé "**Risque**". Le schéma ci-dessous présente une vue générale de ce processus.



Le tableau ci-dessous liste les recommandations du Cert-IST sur l'attitude à tenir en fonction du niveau de risque.

Risque	Recommandation
Très élevé	Agir immédiatement sur tous les systèmes
Elevé	Agir immédiatement sur les systèmes frontaux et les serveurs
Moyen	Les actions peuvent être reportées, mais une opération de maintenance sécurité doit être prévue dès à présent
Faible	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	Elevé	Elevé	Moyen
Facile	Très élevé	Elevé	Elevé	Moyen
Modéré	Très élevé	Elevé	Moyen	Moyen
Difficile	Elevé	Moyen	Moyen	Faible
Très difficile	Elevé	Moyen	Faible	Faible

Fin du document