L’analyse de risque SSI et l’évaluation d’impact sur la vie privée (EIVP)

Principes SSI : le fil rouge

« Si vous pensez que seule la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris à la technologie, ni à vos problèmes »

Bruce Schneier (cryptologue, spécialiste en sécurité informatique)

De quoi parle -t- on ?

D'organisation, d'aspects juridiques (lois et règlements), d'usages (ergonomiques, psychologiques …), de moyens (financiers et humains) ET DE TECHNIQUE…

Principes SSI : le fil rouge

Utopie : « vouloir tout sécuriser et partout »

Cerner le périmètre de sécurité pour mieux protéger ce qui a le plus de valeur !
→ Réaliser des états des lieux, des cartographies organisationnelles, techniques, applicatives …

Identifier l'information, les données sensibles

Informatique et Liberté, Sécurité biologique, Protection du Patrimoine Scientifique et Technique, Stratégiques …

Apprécier et gérer les risques

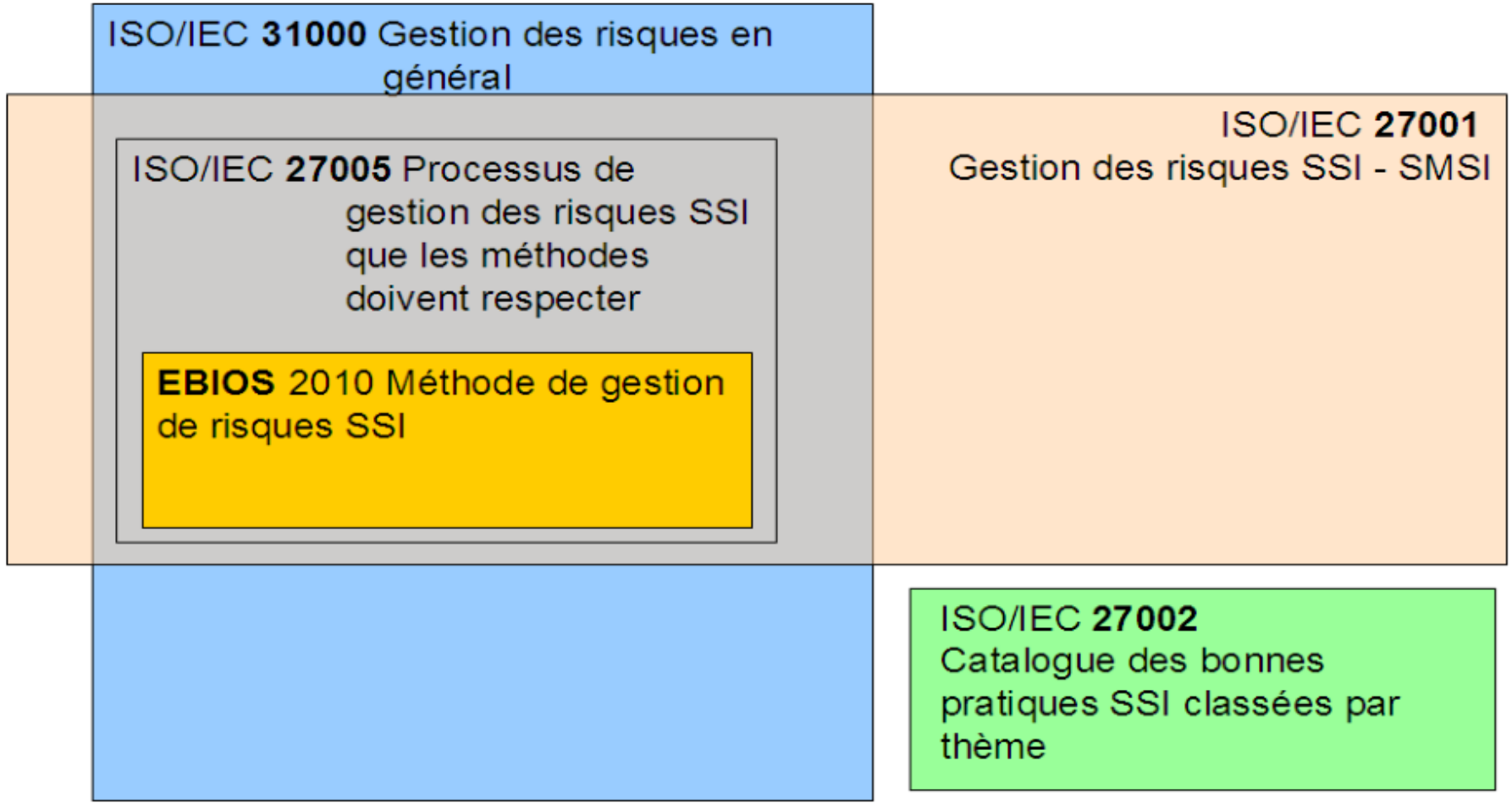
Informatique et Liberté, Sécurité biologique, Protection du Patrimoine Scientifique et Technique, Stratégiques …

Le risque, une notion difficile à définir

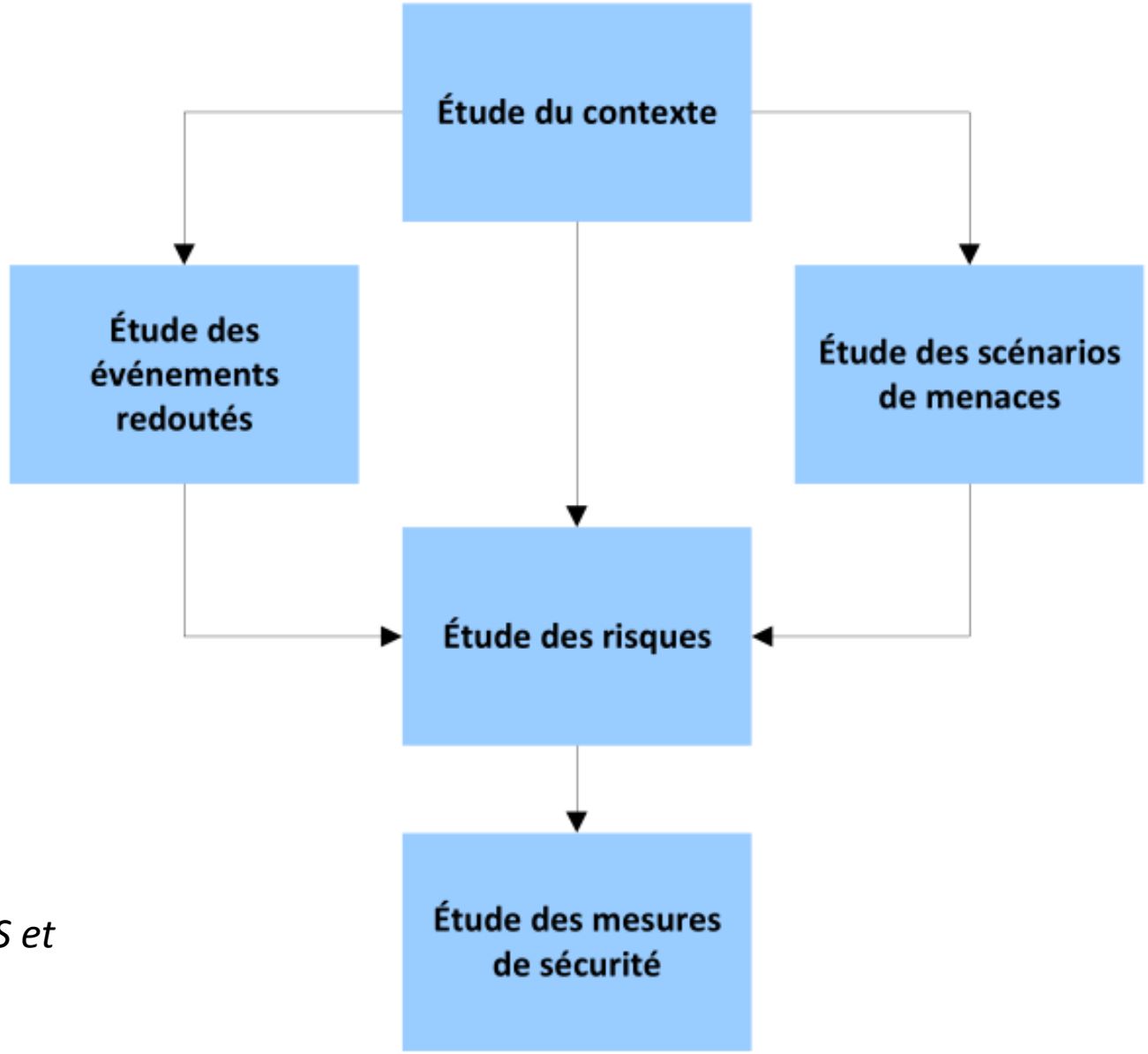
- Norme ISO 27 000 : Effet de l'incertitude sur la réalisation des objectifs
- Norme ISO 27 000 - note 4 : Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (y compris les changements de circonstances) et de sa vraisemblance.
- Norme ISO 27 005 : Possibilité qu'une menace donnée exploite les vulnérabilités d'un bien/actif ou d'un groupe de biens/d'actifs et nuise donc à l'organisation.
- Risque EBIOS : Scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarios de menaces.

- Un élément peut être à la fois une menace et un bien à protéger !
- La confrontation des risques entre eux ainsi que la réduction d'un risque qui peuvent créer de nouveau risque.

Apprécier les risques : *Utiliser une méthode !*



Apprécier les risques : *Utiliser une méthode !*



Méthode EBIOS de l'ANSSI

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est un outil complet de gestion des risques SSI conforme au RGS et aux dernières normes ISO 27001, 27005 et 31000.

L'analyse des risques

Disponibilité
Confidentialité
Intégrité

Risque =

combinaison

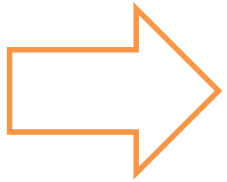
(préjudice estimé
par la MOA ou porteur d'enjeu;

probabilité d'occurrence estimé
par la MOE ou informatique)

Au mélange des genres
(MOA, MOE)

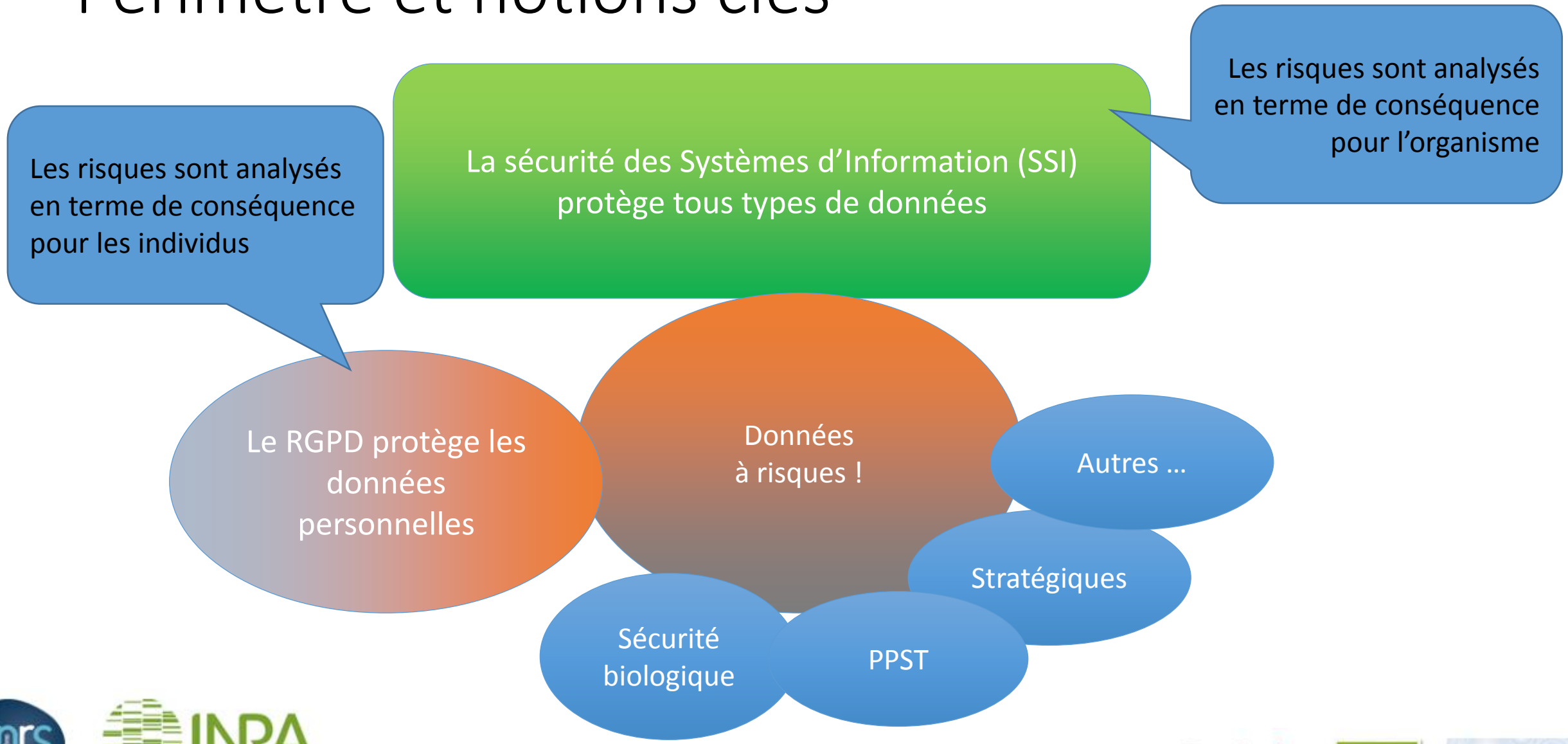
L’analyse des risques

- ✓ Identifier les risques (inacceptables) afin de s’en prémunir
- ✓ Le risque est :
  - réduit ou supprimé ou transféré
  - accepté ou pas par les **responsables**
- ✓ Besoins de sécurité -> mesures (Politique SSI)
- ✓ Mise en œuvre ; contrôles audits

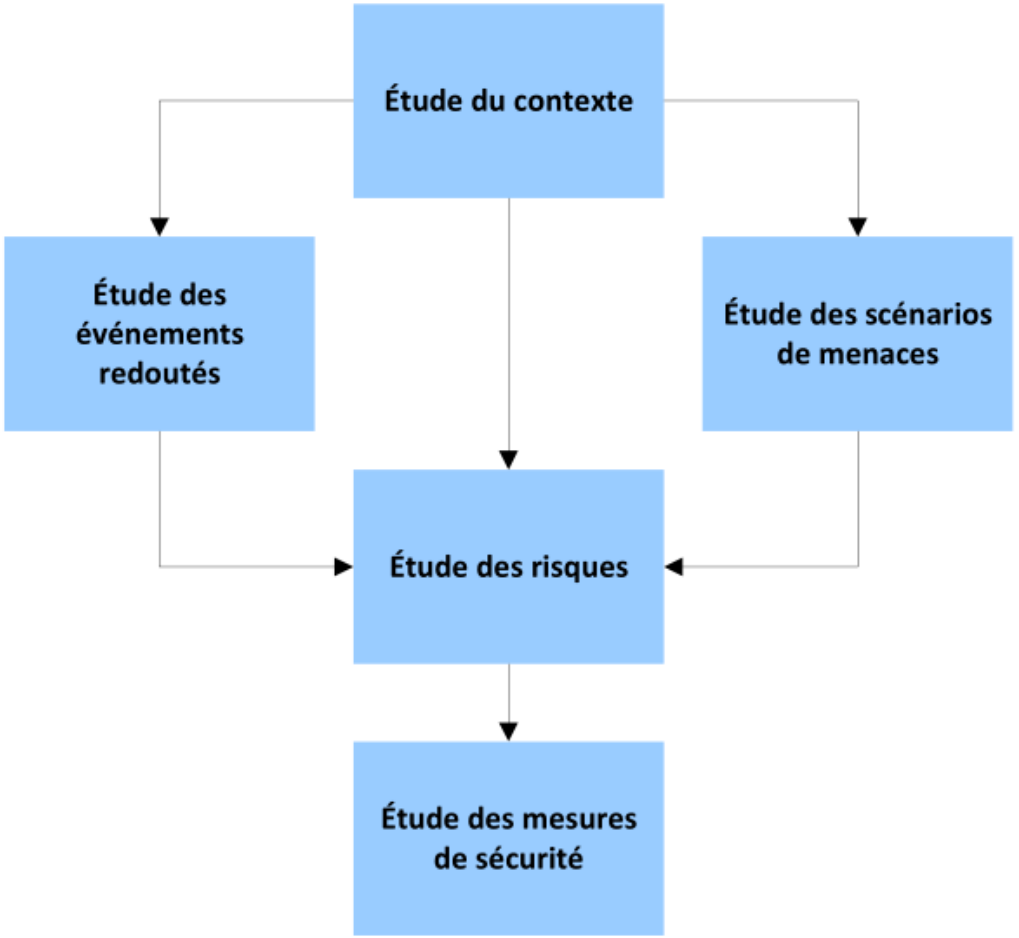


- ✓ Étude de contexte
- ✓ Étude d’Impact sur la Vie Privée (EIVP)
  - Ou analyse d’impact relative à la protection des données (AIPD)
  - Ou Privacy Impact Assessment (PIA)
- ✓ Analyse risque SSI

Périmètre et notions clés



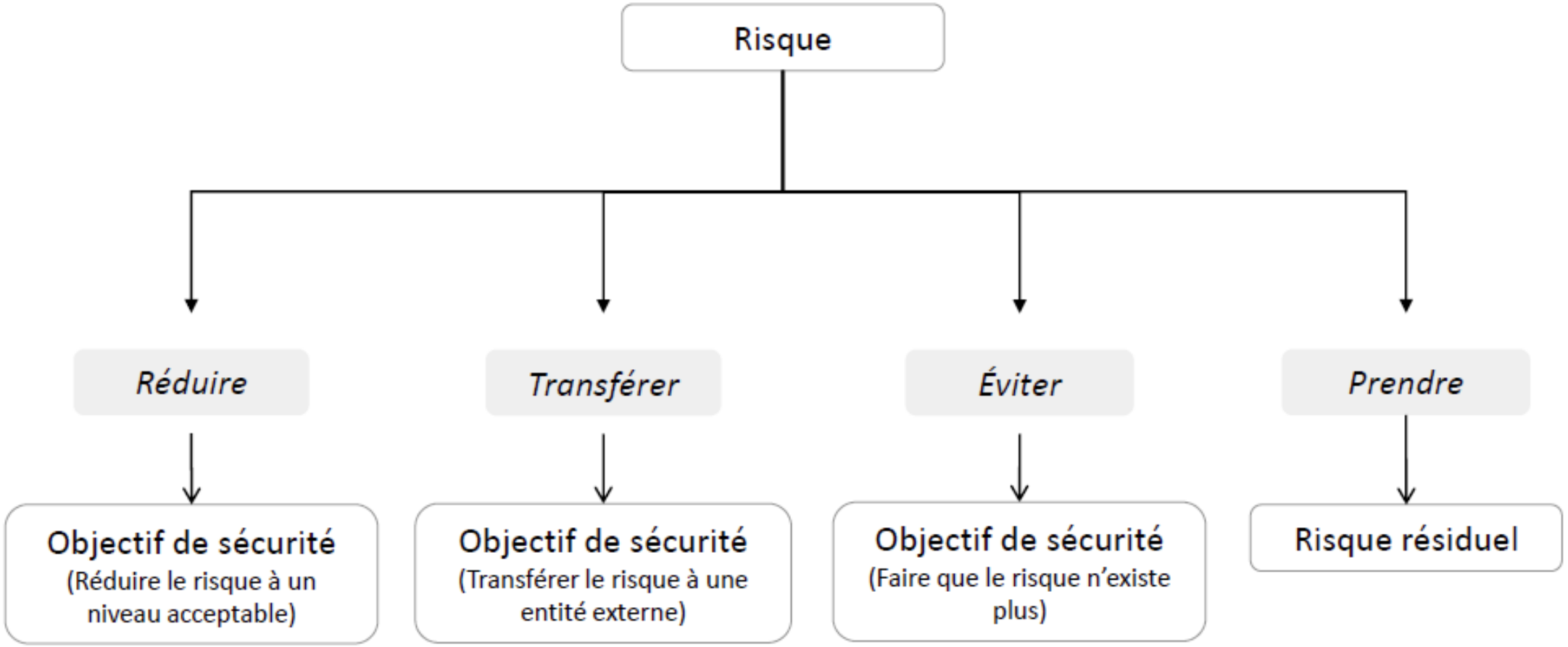
Méthode EBIOS de l'ANSSI



Exemple d'évaluation des risques **après application des mesures existantes**. Les risques rayés correspondent à ceux qui ont été réduits.

Gravité					
	4. Critique		Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres		
	3. Importante		Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre ~~Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver~~	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires
	2. Limitée		Risque lié à l'indisponibilité d'un devis au-delà de 72h Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h Risque lié à l'indisponibilité de visualisations au-delà de 72h Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h	~~Risque lié à l'indisponibilité d'un devis au-delà de 72h~~ ~~Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h~~ ~~Risque lié à l'indisponibilité de visualisations au-delà de 72h~~ Risque lié à l'altération de visualisations sans pouvoir la détecter	~~Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h~~
	1. Négligeable				
		1. Minime	2. Significative	3. Forte	4. Maximale
		Vraisemblance			

Traitement des risques



Un système est sécurisé si :

1. **L'analyse de risque** a été réalisée, le risque résiduel a été accepté par le porteur d'enjeu
2. **Les mesures de sécurité** validées ont été mises en place
3. Le SI se comporte exactement de la manière voulue - et ne fait rien de plus (durcissement des configurations, audit de code …)
4. Le système est **entretenu** (mis à jour)

La sécurité n'est pas une « couche » qu'on rajoute à la fin…

Merci