HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

ISO27005
Gestion de risque

Clusif – groupe méthodes / méhari
Paris, 15 mai 2007 matin

Alexandre Fernandez
Hervé Schauer

HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

ISO27005
Gestion de risque

Club EBIOS
Paris, 15 mai 2007 après-midi

Alexandre Fernandez
Hervé Schauer

Préambule

- HSC : pas un expert du domaine de la gestion de risque
  - Simple observateur jusqu'à ce que l'ISO 27001 apparaîsse

- Si rérérence (X.Y.Z) en rouge entre parenthèse ➔ dans la norme
  - Reférence à la norme ISO 27005
  - Pour les références aux autres normes, précision devant
    - ISO 27001, ISO 27002, BS7799-3

- Norme à l'état final du document de travail du comité de normalisation (FCD) de janvier 2007

Sommaire (4)

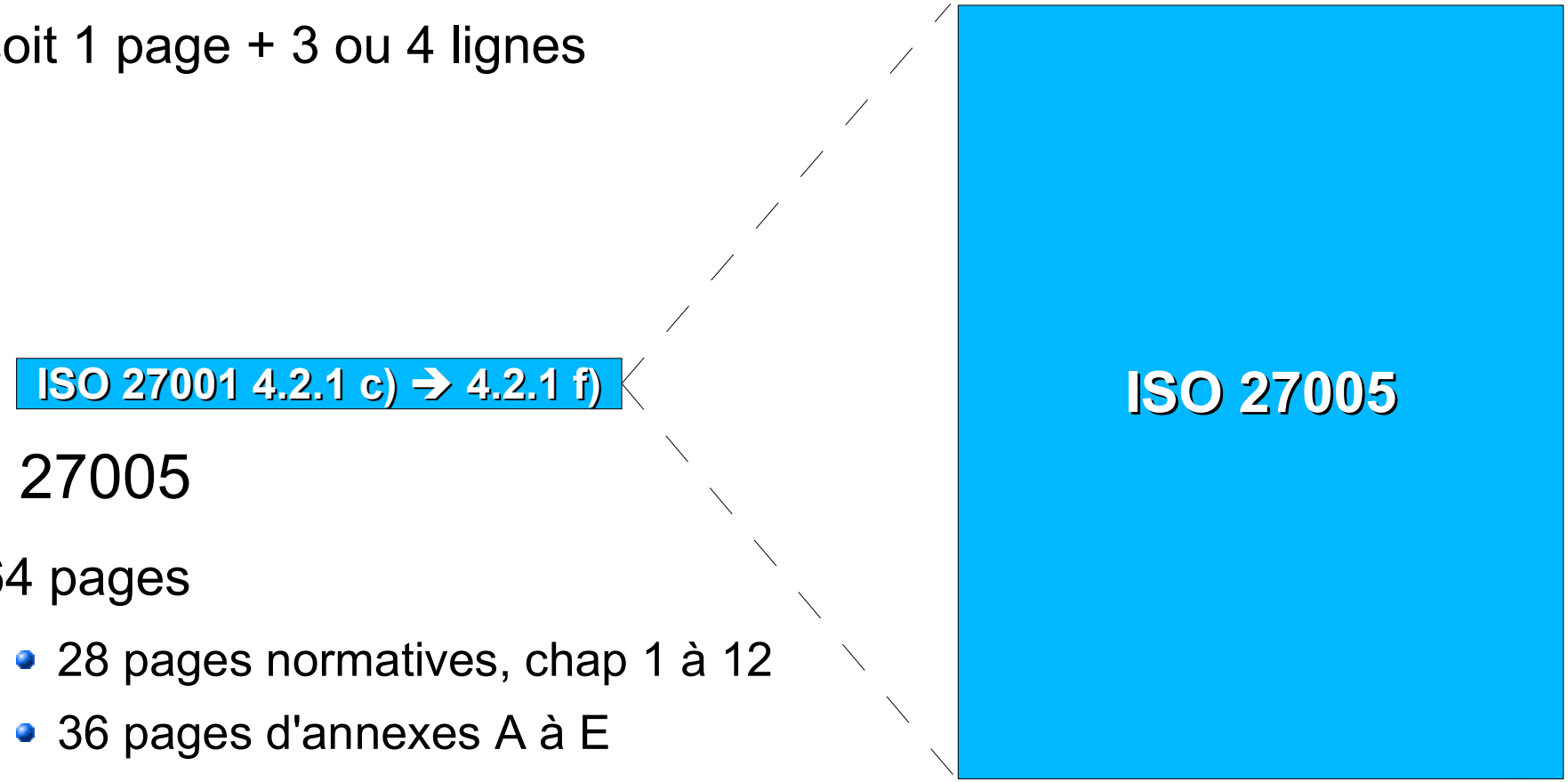
- Introduction
- Historique
- Vocabulaire « Analyse de risque »
- Processus de gestion de risque (6)
- Etablissement du contexte (*context establishment*) (7)
- Appréciation du risque (*risk assessment*) (8)
  - Analyse de risque (*risk analysis*) : Identification des risques (*risk identification*) (8.2.1)
  - Analyse de risque (*risk analysis*) : Estimation du risque (*risk estimation*) (8.2.2)
  - Evaluation du risque (*risk evaluation*) (8.3)

Sommaire (4)

- Traitement du risque (*risk treatment*) (9)
- Acceptation du risque (*risk acceptance*) (10)
- Communication du risque (*risk communication*) (11)
- Surveillance et réexamen du risque (*risk monitoring and review*) (12)
- Outillage
- Conclusion
- Prochains rendez-vous

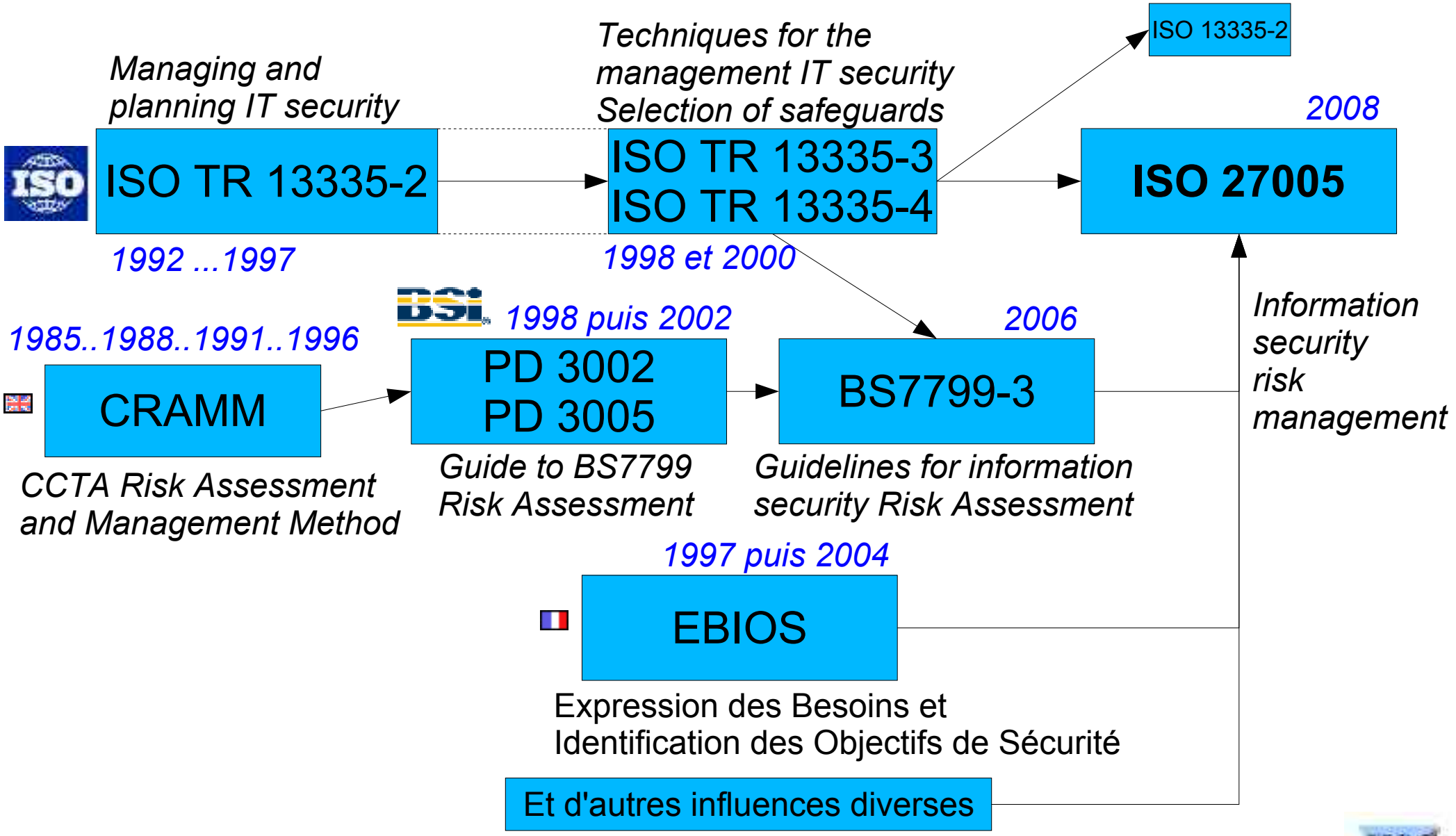
Introduction

- ISO 27005 : Guide de mise en oeuvre de la partie appréciation des risques de la sécurité de l'information de l'ISO 27001
- ISO 27001 4.2.1 c) à 4.2.1 f) 4), plus 4.2.3.d)
  - soit 1 page + 3 ou 4 lignes



- ISO 27005
  - 64 pages
    - 28 pages normatives, chap 1 à 12
    - 36 pages d'annexes A à E

Historique



Vocabulaire « Analyse de risque »

- Choix de traduction
  - *Risk Analysis* ➔ Analyse du risque
  - *Risk Evaluation* ➔ Evaluation du risque
  - *Risk Estimation* ➔ Estimation du risque
  - *Risk Assessment* ➔ Appréciation du risque
- Langage courant
  - Analyse de risque ⇔ *Risk Assessment*
  - Usage impossible à garder sans confusions
    - Pas d'autre traduction possible que *Risk Analysis* ➔ Analyse du risque
    - Confusion avec *Risk Assessment*

Processus de gestion du risque (6) p7

- Définition d'un **processus**
  - Continu et qui s'améliore, donc PDCA
- Processus de **gestion de risque de la sécurité de l'information**
  - (*information security risk management process*)
- Processus applicable
  - A toute l'organisation
  - A un sous ensemble
    - Service, site géographique, etc
  - A tout système d'information
  - A une mesure de sécurité ou un traitement existant ou planifié
    - Exemple : continuité d'activité

Processus de gestion du risque (6) p7

Plan

- Identifier les risques
- Quantifier chaque risque par rapport
  - aux conséquences que sa matérialisation pourrait avoir sur le business
  - à sa probabilité d'occurrence (*likelihood*)
- Identifier les actions appropriées pour réduire les risques identifiés à un niveau acceptable

Do

- Implémenter les actions pour réduire les risques
- Eduquer la direction et le personnel sur les risques et les actions prises pour les atténuer

Act

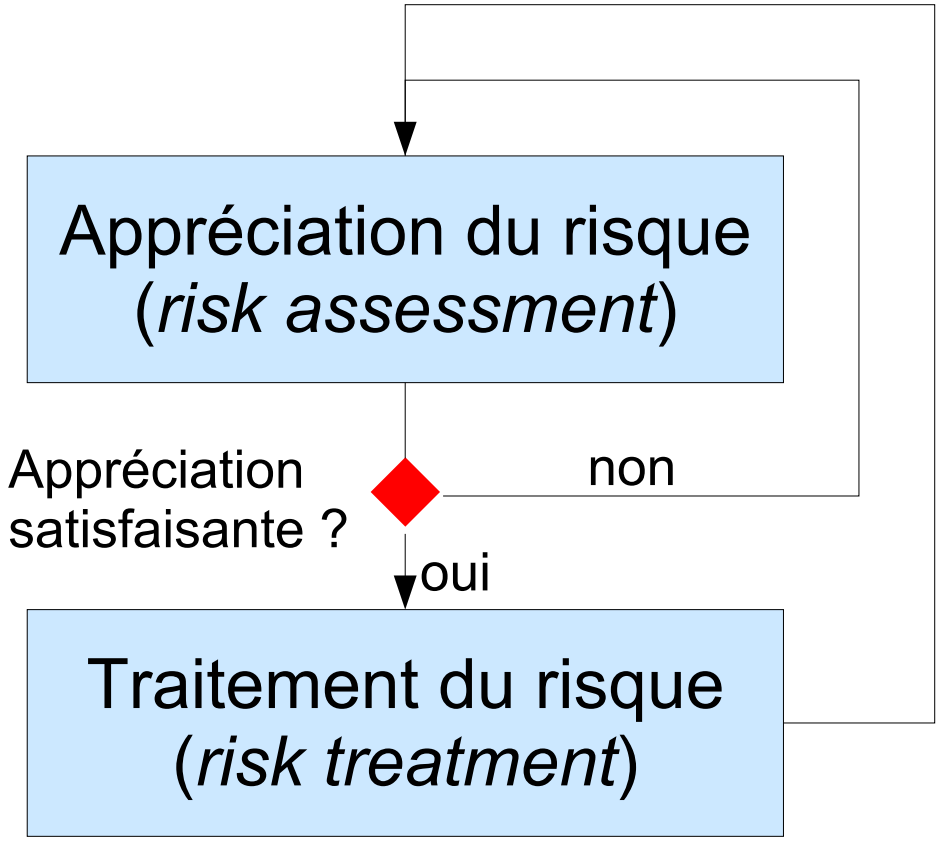
- Rectifier le traitement du risque à la lumière des évènements et des changements de circonstances
- Améliorer le processus de gestion du risque

Check

Surveiller et réexaminer les résultats, l'efficacité et l'efficience du processus

Processus de gestion du risque (6) p8

- Décomposé en deux activités séquencielles et **itératives** { dans ISO 27001 l'**activité** appréciation du risque s'appelle **processus** d'appréciation du risque (8.1)
- Approche itérative
  - Améliore la finesse de l'analyse à chaque itération
  - Garanti une appréciation des risques élevés
  - Minimise le temps et l'effort consenti dans l'identification des mesures de sécurité
- Appréciation des risques satisfaisante ?
  - Passer au traitement du risque

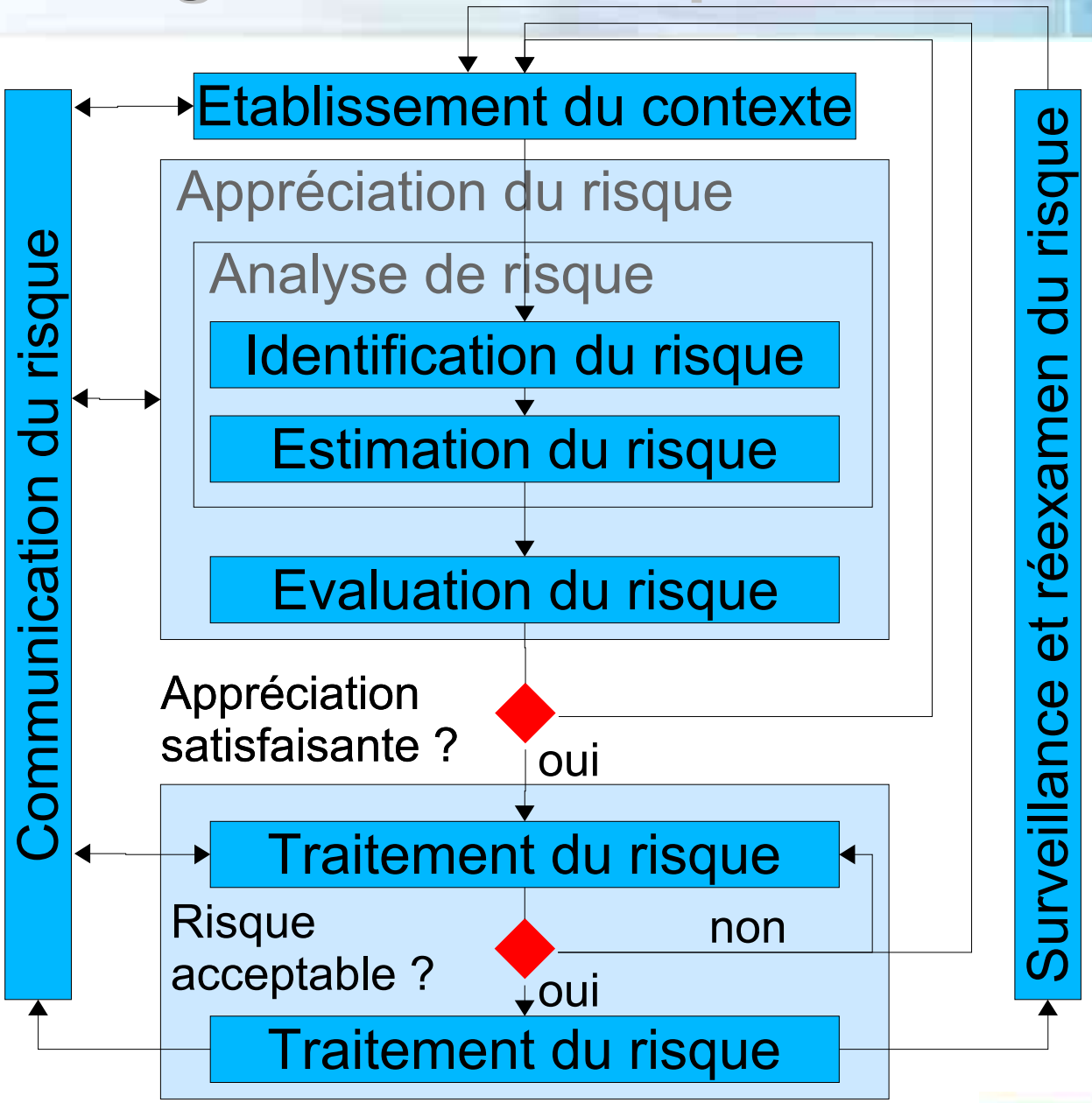


Processus de gestion du risque

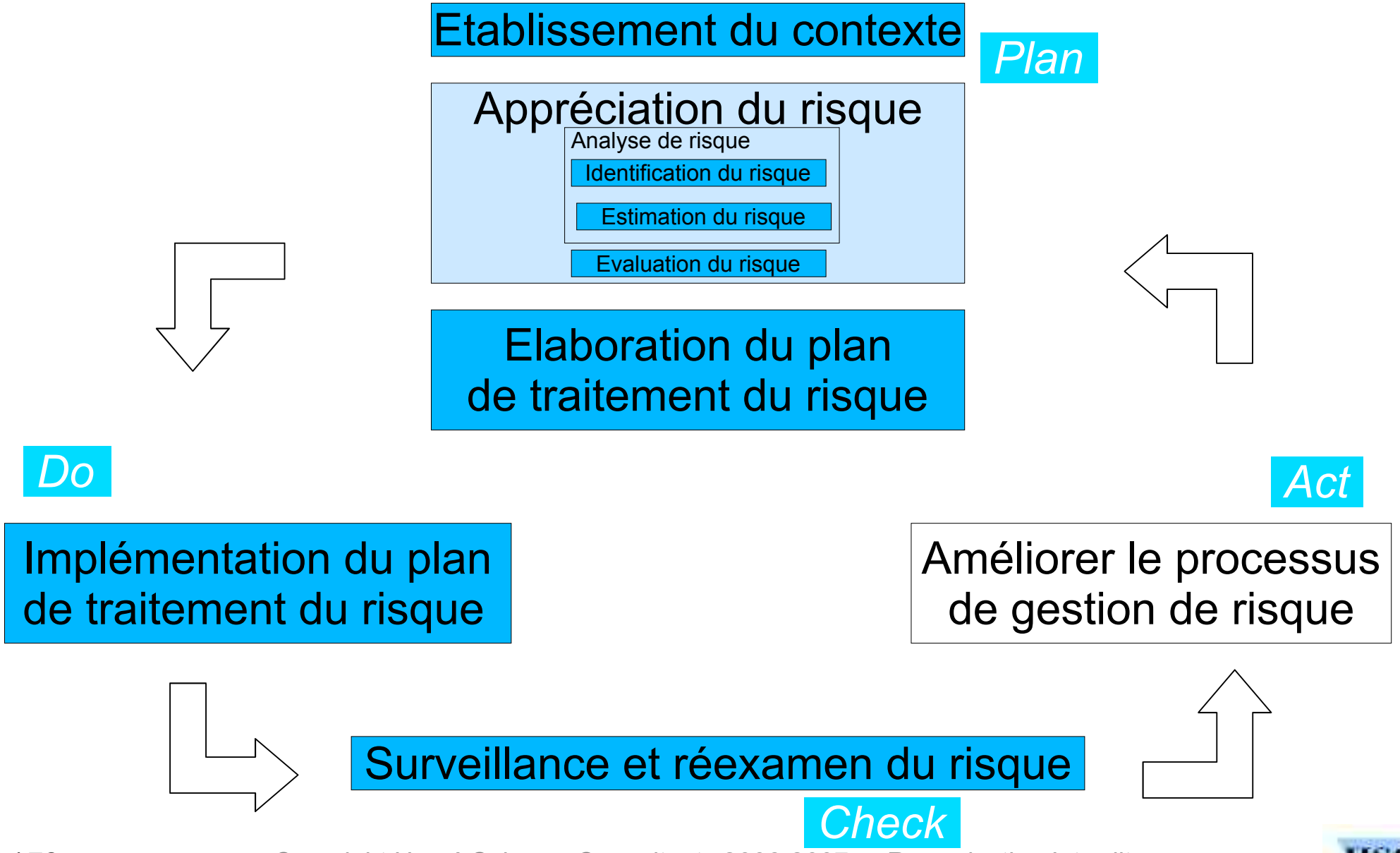
- Appréciation du risque (8)
  - Analyse des risques
    - Mise en évidence des composantes des risques
    - Estimation de leur importance
  - Evaluation des risques
    - Analyse d'ensemble et prise de décision sur les risques
- Traitement du risque (9)
  - Sélection des objectifs et mesures de sécurité pour réduire le risque
  - Refus, transfert ou conservation du risque
- Acceptation du risque (10)
  - Approbation par la direction des choix effectués lors du traitement du risque
- Communication du risque (11)

Processus de gestion du risque (6) p8-9

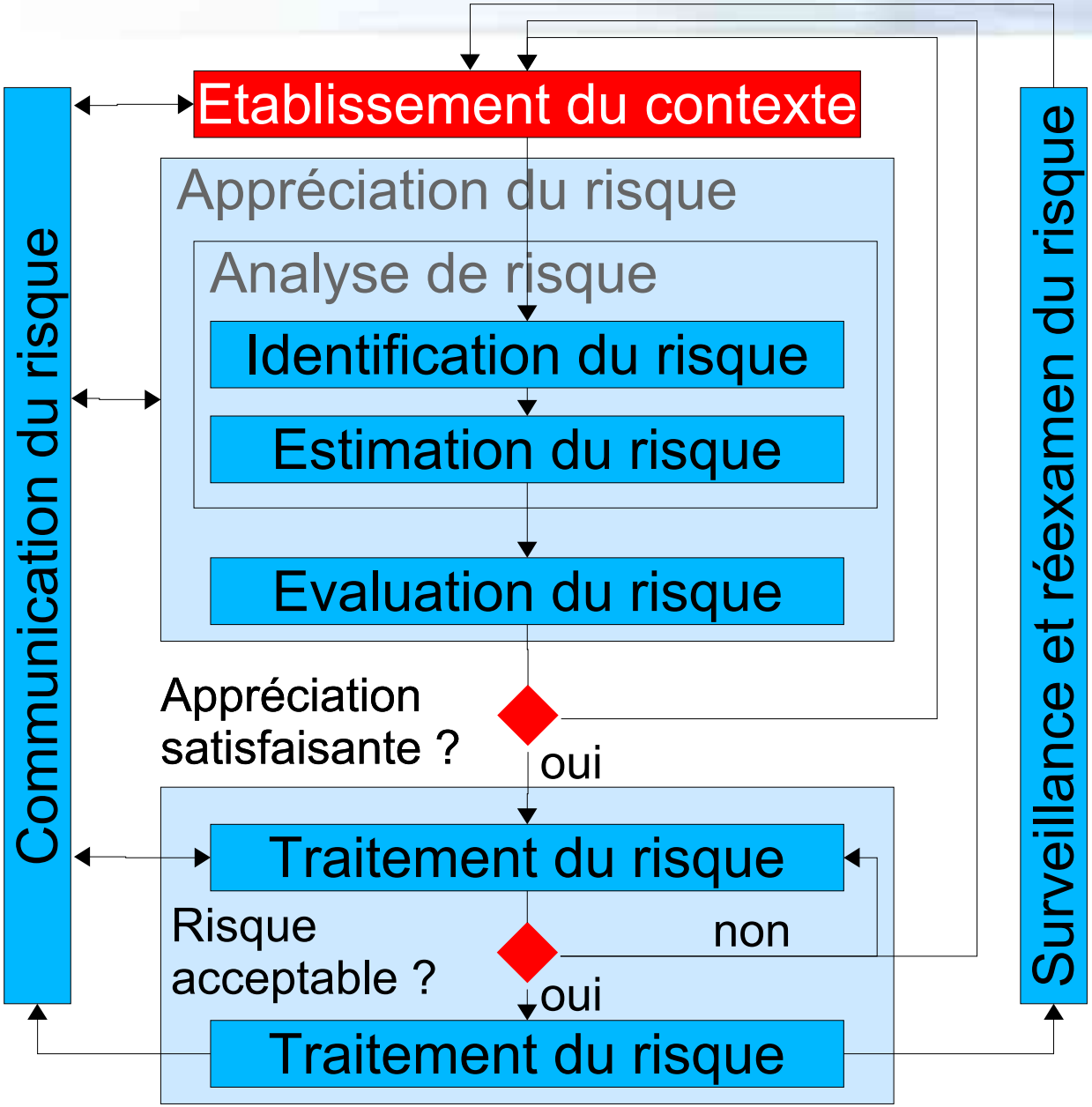
- n° 1
  - Assez d'éléments pour déterminer les actions nécessaires à la réduction des risques à un niveau acceptable ?
- n° 2
  - Risque acceptable ?
- Communication à la hiérarchie et aux équipes opérationnelles à chaque étape
  - Risque identifié utile immédiatement à la gestion des incidents



Processus de gestion du risque (6) p10

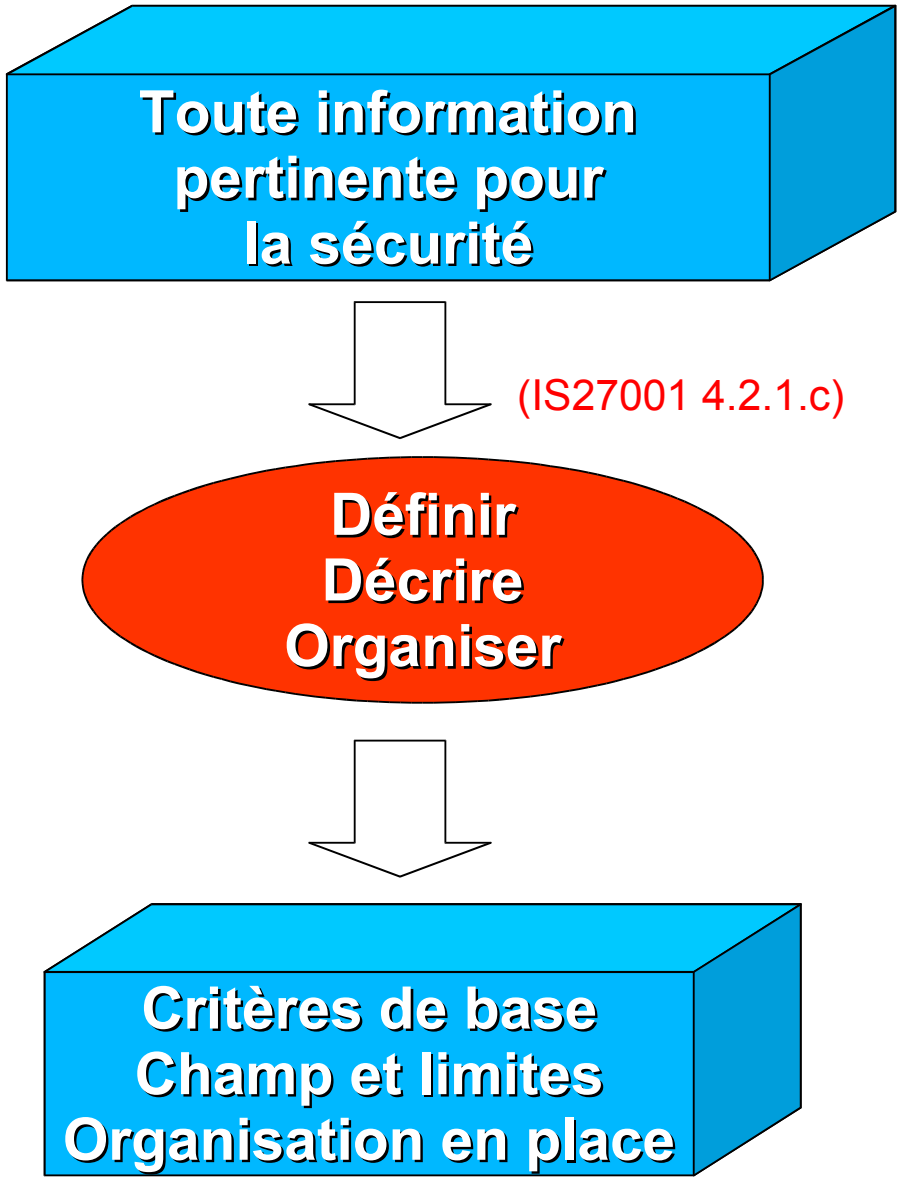


Etablissement du contexte

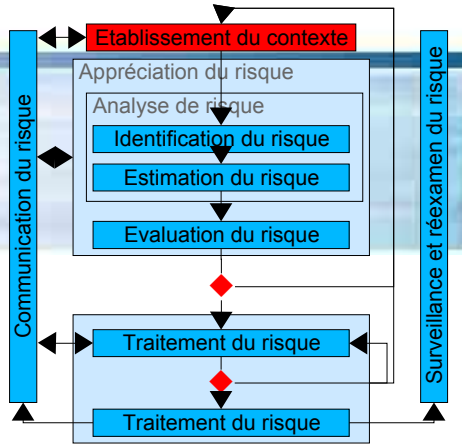


Etablissement du contexte

- Définir ses critères de base (7.2)
- Définir le champ et les limites du processus de gestion du risque (7.3)
- Décrire l'environnement du processus de gestion du risque (7.3)
- Décrire l'objet du processus de gestion du risque (7.3)
- Organiser et gouverner la gestion du risque (7.4)



Etablissement du contexte



- Définir ses critères de base (7.2) :
  - Critères d'évaluation des risques
  - Critères d'impact
  - Critères d'acceptation des risques
  - Disponibilité des ressources
- Critères peuvent changer d'une appréciation à l'autre, d'une itération à l'autre

Etablissement du contexte

- Critères d'évaluation des risques (7.2) :
  - Valeur stratégique du processus métier
  - Criticité des actifs impliqués
  - Conséquences financières en association avec :
    - Obligations légales et règlementaires (*legal and regulatory requirements*)
    - Engagements contractuels (*contractual obligations*)
    - Perception du client et conséquences négatives pour la clientèle
    - Attentes des clients

Etablissement du contexte

- Critères d'impact (7.2) :
  - Niveau de classification du patrimoine informationnel impacté
  - Impact de la violation des critères de sécurité (*breaches of security criteria*)
    - Confidentialité, intégrité, disponibilité, et éventuellement d'autres critères de sécurité
  - Détérioration de l'exploitation (*impaired operations*)
    - Interne ou tierce partie
  - Perte financière et perte de business
  - Pertubation des projets, non-respect des dates limites (*disruption of plans and deadlines*)
  - Dégradation de la réputation (*damage of reputation*)

Etablissement du contexte

- Critères d'impact (B.3) :
  - Différence entre la valeur d'un actif et l'impact ?
  - Incident de sécurité peut affecter
    - Un actif
    - Plusieurs actifs
    - Une partie d'un actif
  - Impact mesure le degré de dommage d'un incident
  - Au départ l'estimation d'un impact sera très proche de l'estimation de la valeur des actifs impactés

Etablissement du contexte

- Critères d'acceptation des risques (7.2) :
  - Métier
  - Légaux et règlementaires
  - D'exploitation
  - Technologiques
  - Financiers
  - Sociaux et humanitaires
- Définir sa propre échelle et son propre seuil d'acceptation des risques (*level of risk acceptance decision*)

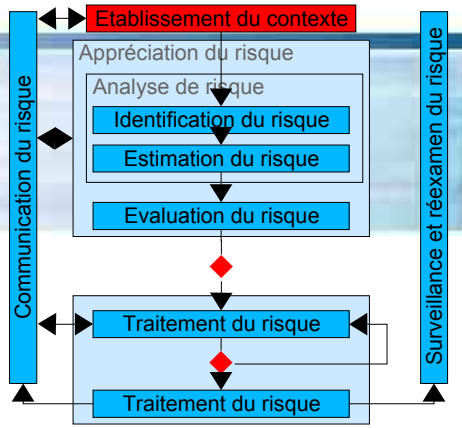
Etablissement du contexte

- Critères d'acceptation des risques :
  - Décrit les circonstances dans lesquelles l'organisation acceptera les risques (BS7799-3 4.2)
  - Correspond au critères de risque (*risk criteria*) (ISO Guide 73) dans d'autres documents
  - Conservation des risques dépendra des critères d'acceptation des risques

Etablissement du contexte

- Disponibilité des ressources pour (7.2) :
  - Réaliser l'appréciation des risques et le plan de traitement des risques
  - Définir et implémenter les politiques et procédures
  - Implémenter les mesures de sécurité sélectionnées
  - Suivre de près les mesures de sécurité
  - Surveiller le processus de gestion des risques

Etablissement du contexte



- Définir le champ et les limites (*scope and boundaries*) du processus de gestion du risque (7.3) :
  - Inclus dans le périmètre du SMSI
  - **Environnement** du processus de gestion du risque
  - **Objet** du processus de gestion du risque
- Processus de gestion du risque applicable à tout type d'objet :
  - Application
  - Infrasructure IT
  - Processus métier
  - Organisation

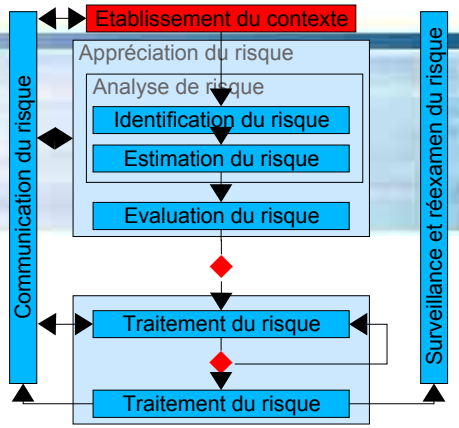
Etablissement du contexte

- Décrire l'environnement du processus de gestion du risque(7.3) :
  - Présentation de l'organisation
  - Ses objectifs stratégiques pour son métier, ses stratégies et ses politiques
  - Politique de sécurité
  - Contraintes affectant l'organisation
  - Liste des obligations légales, règlementaires et contractuelles s'appliquant à toute l'organisation
  - Aire d'application du processus au sens des limites système ou géographiques
  - Architecture du système d'information
  - Justification des exlusions du champ du processus de gestion de risque
  - Environnement socio-culturel

Etablissement du contexte

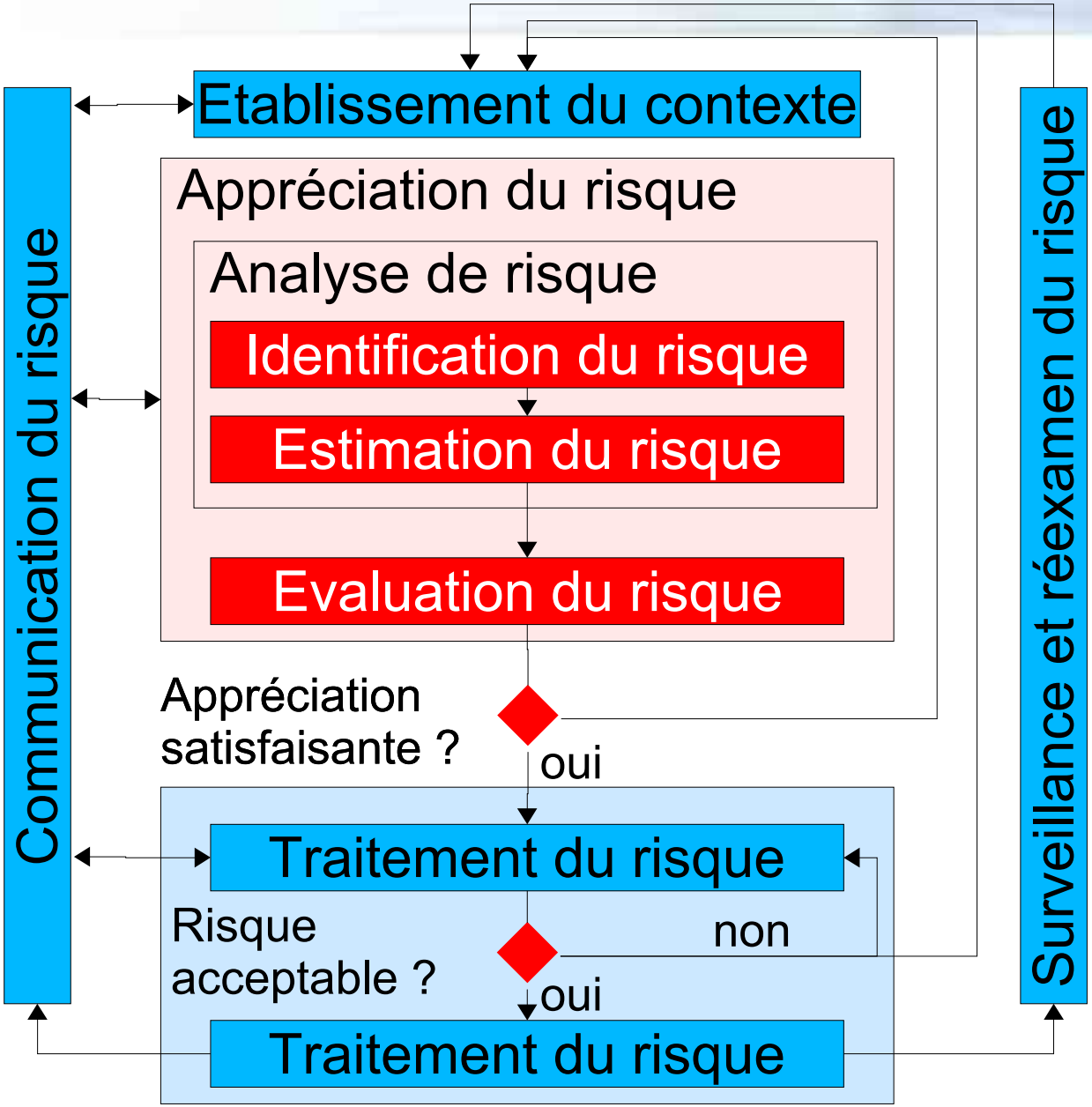
- Décrire l'objet du processus de gestion du risque (7.3) :
  - Présentation du champ
  - Constituants
  - Objectifs
  - Description fonctionelle
  - Mesures de sécurité déjà en place ou prévues
  - *Borders and barriers*
  - Interfaces et échanges avec l'environnement
  - Organisation et responsabilités
  - Postulats (*assumptions*)
  - Contraintes spécifiques
  - Références règlementaires spécifiques

Etablissement du contexte



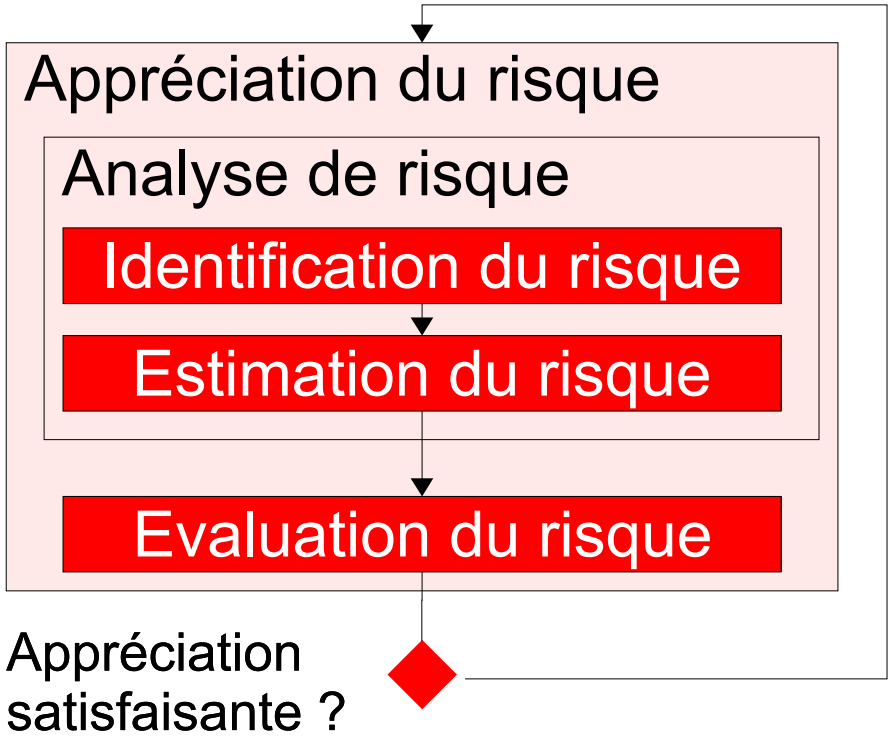
- Organiser et gouverner la gestion du risque (7.4) :
  - Approbation par la direction générale (Cf IS27001 5.1.f)
  - Identification des parties impliquées (*involved parties*)
    - Dont les dépositaires d'enjeux (*stakeholders*)
  - Définition des rôles et responsabilités
    - Dans toutes les entités concernées par le processus de gestion du risque
  - Etablissement des liens nécessaires entre les parties impliquées
    - Particulierement avec les fonctions de gestion du risque de haut niveau
    - Gestion des risques opérationnels
  - Répartition des tâches et activités, y comprit la documentation
  - Gestion de ressources
  - Définition des chemins d'escalade de décision
  - Définition des enregistrements devant être conservés

Appréciation du risque



Appréciation du risque

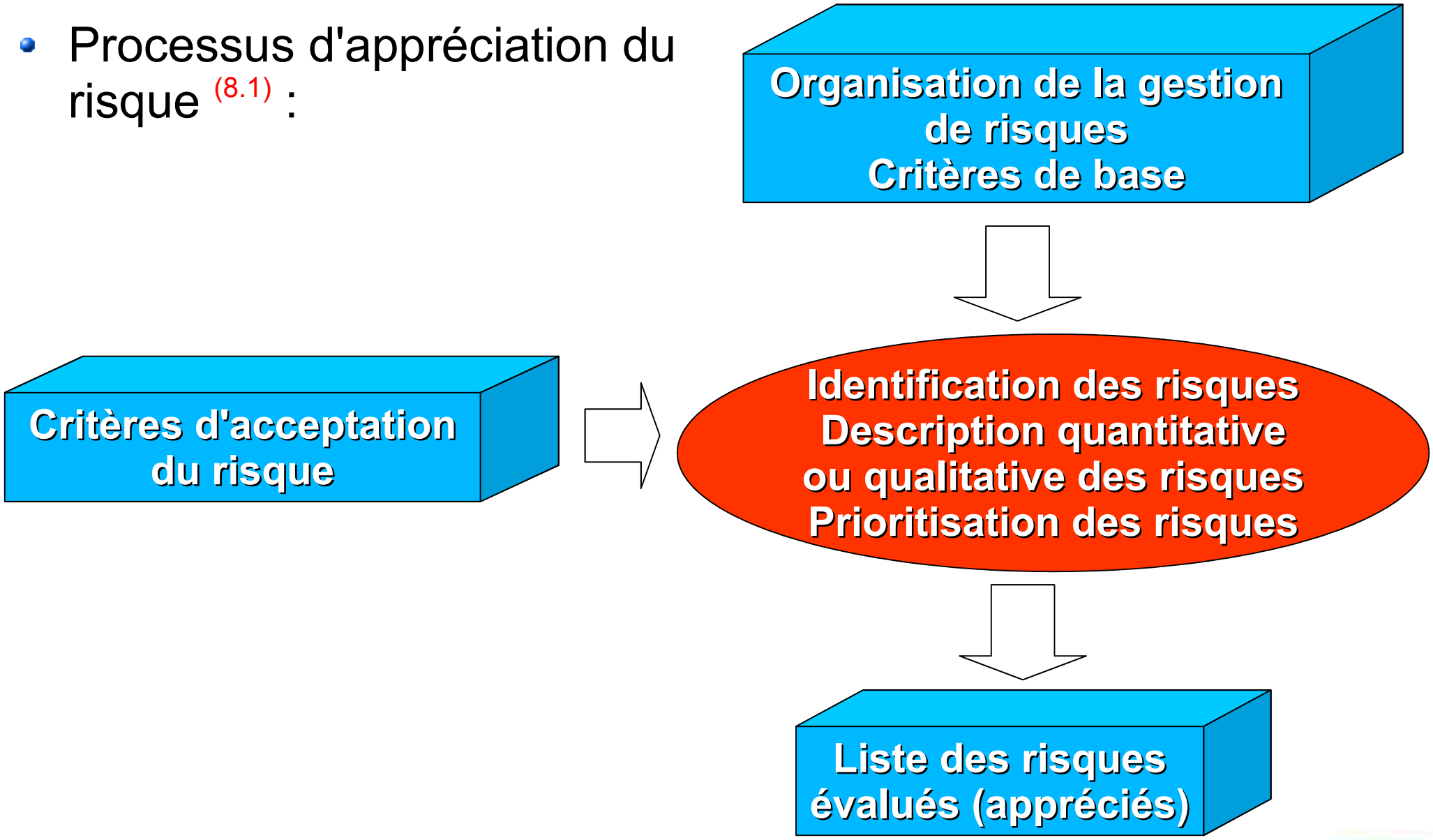
- Appréciation du risque (8.1) :
  - Déterminer la valeur des actifs
  - Identifier les menaces et les vulnérabilités
  - Identifier les mesures de sécurité existantes et leurs effets sur le risque identifié
  - Quantifier les conséquences potentielles
  - Prioritiser et ordonnancer les risques



- Itérations de l'appréciation (8.1)
  - Haut-niveau
  - De plus en plus en profondeur

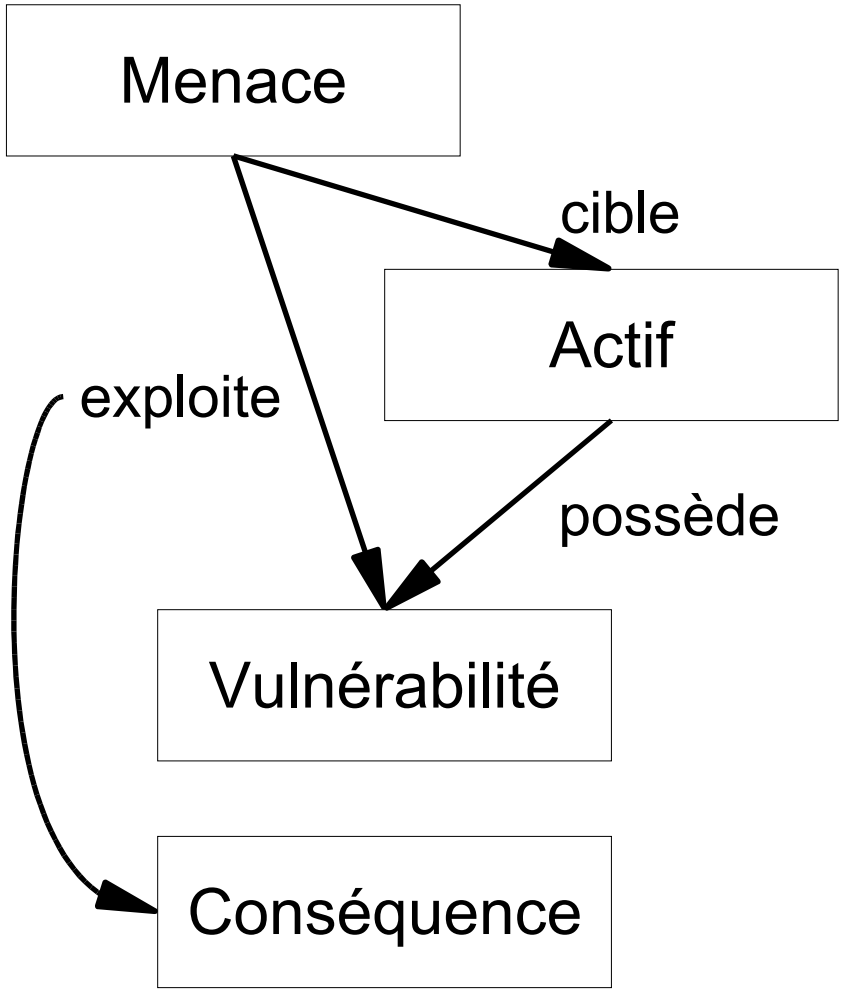
Appréciation du risque

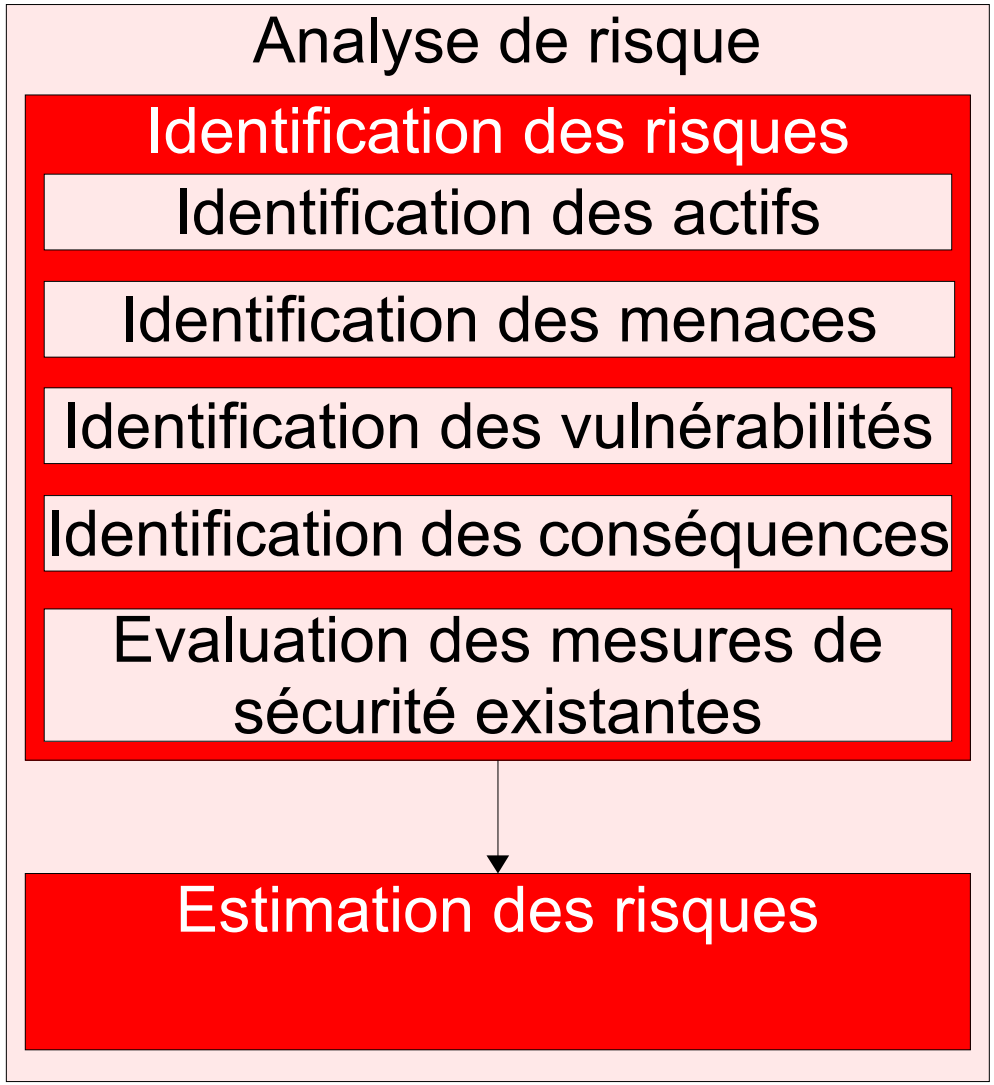
- Processus d'appréciation du risque (8.1) :



Analyse de risque

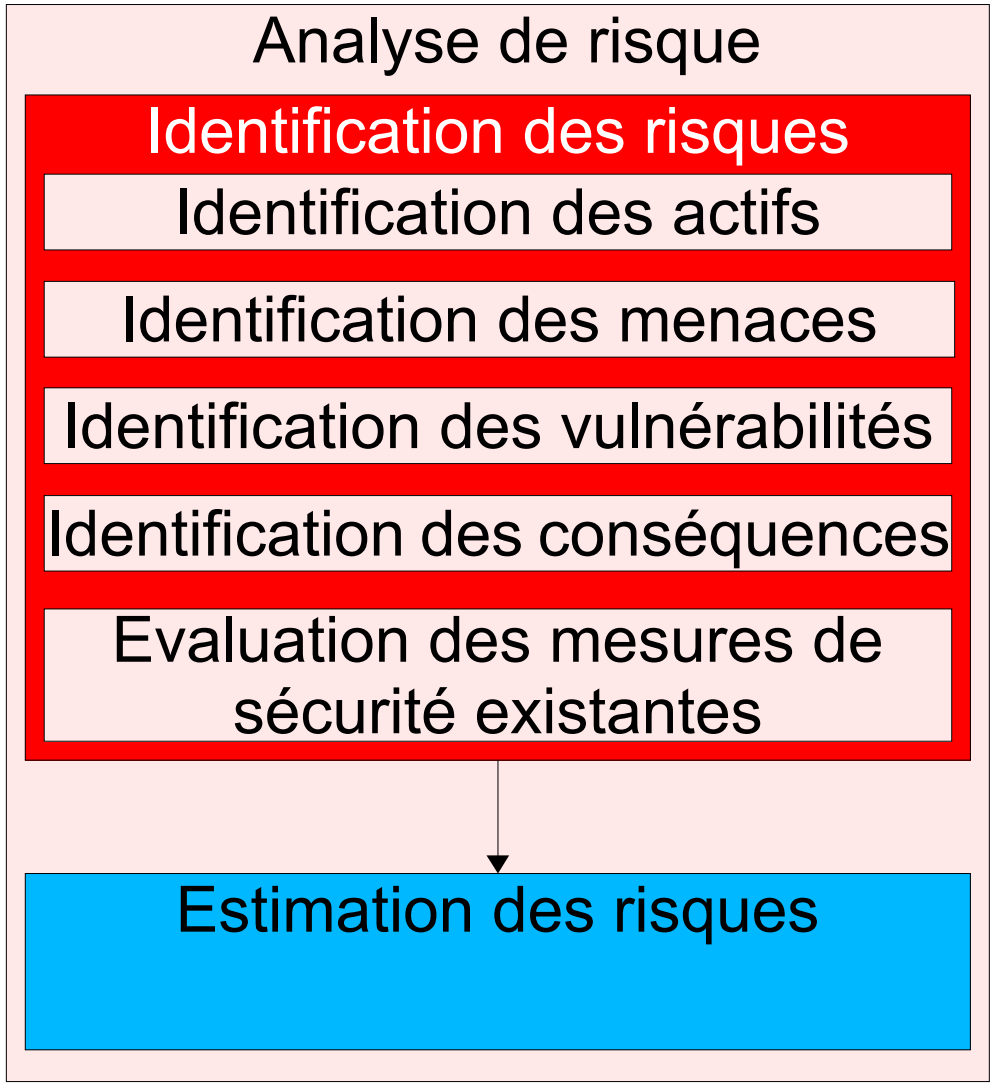
- Analyse de risque (8.2) :





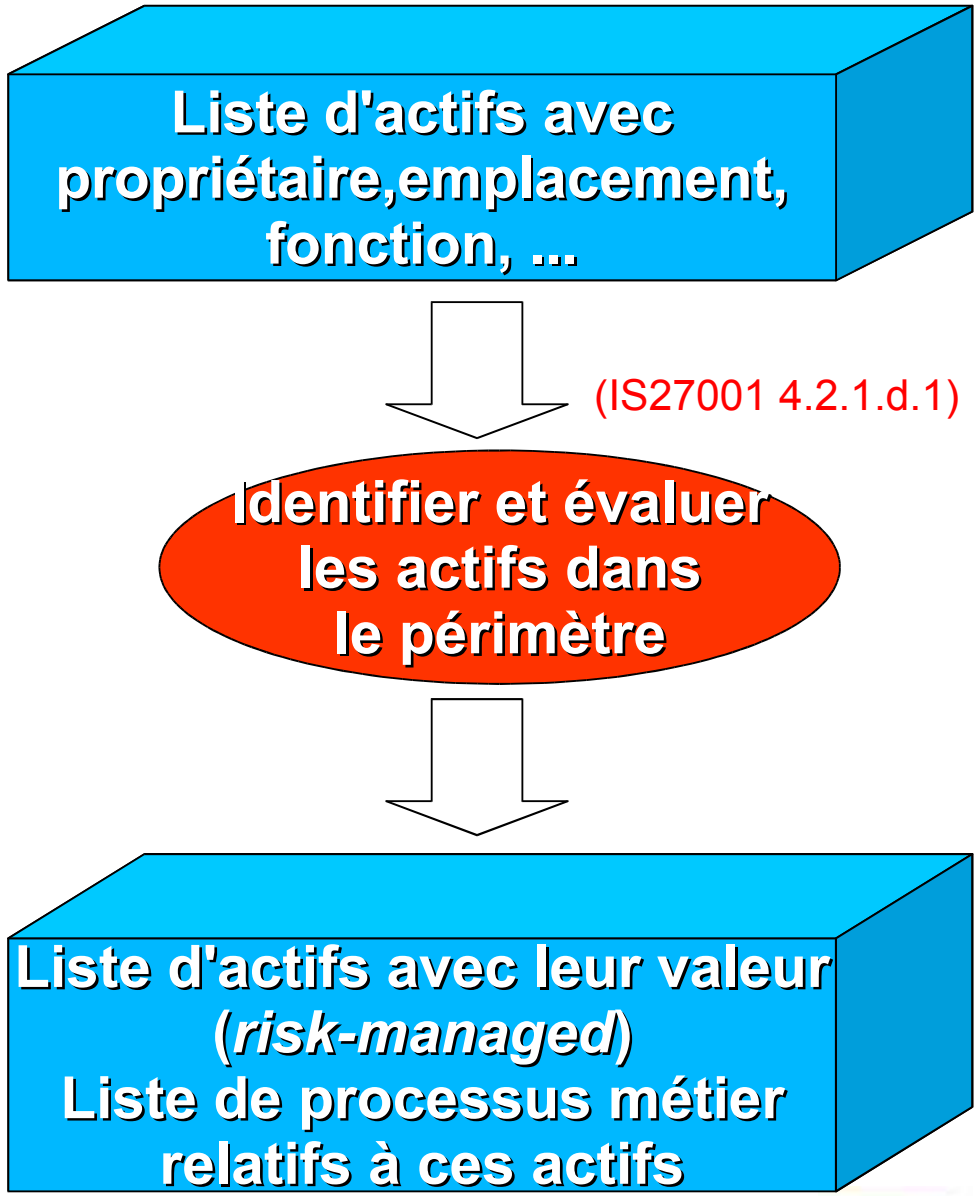
Identification des risques

- Identification des risques (8.2.1) :



Identification des risques

- Identification et évaluation des actifs (8.2.1.1) :
  - Actifs non-identifiés à l'issue de cette activité ne seront pas classés ➔ même compromis cela n'affecte pas l'objet du processus de gestion de risque (B.1.1)
  - Propriétaire de l'actif ➔ responsable et redevable pour cet actif (8.2.1.1)
    - Production, développement, maintenance, usage, sécurité, ...
    - Pas au sens droit de propriété

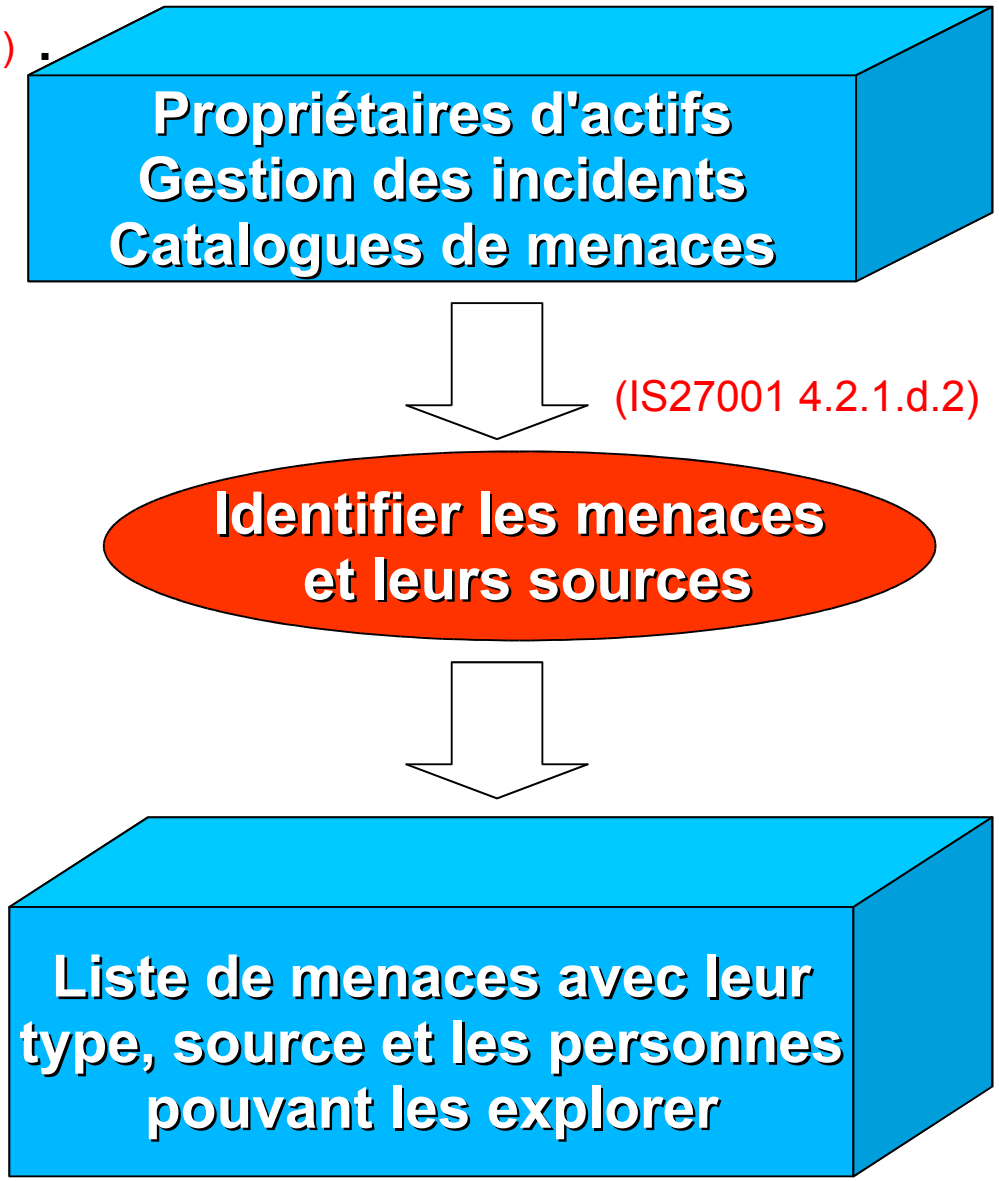


Identification des risques

- Evaluation des actifs (B.2) :
  - Définir une échelle et des critères d'évaluation des actifs
  - Evaluer les actifs
  - Indiquer à chaque évaluation le critère utilisé et l'auteur de l'évaluation
  - Assigner une valeur finale à chaque actif
  - Homogénéiser l'ensemble des évaluations
  - Produire une liste d'actifs avec leur valeur

Identification des risques

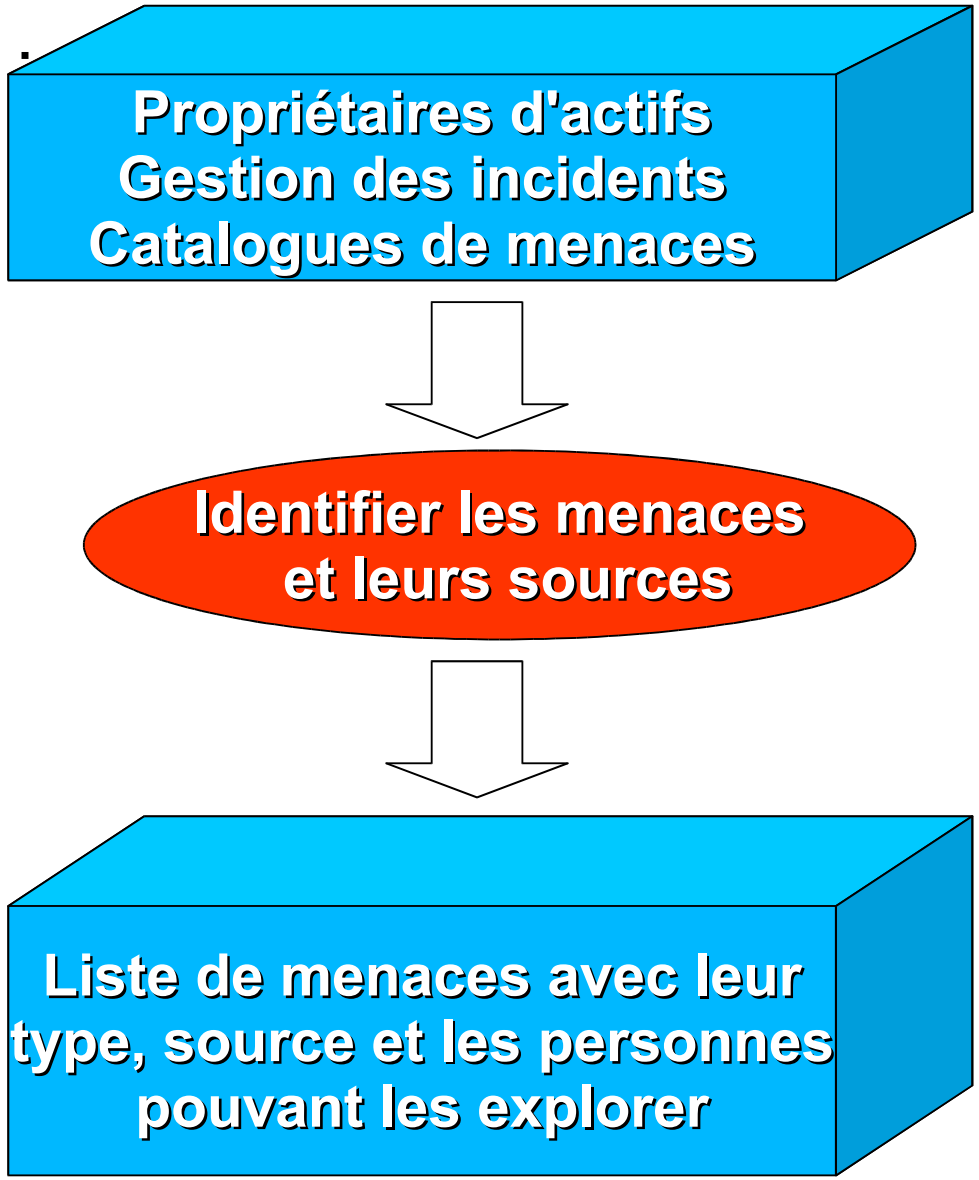
- Identification des menaces (8.2.1.2) .
  - En priorité les menaces d'origine accidentelles et délibérées
  - De manière générique et par type
    - Compromission de l'information, pannes techniques, actions non-autorisées
  - Source
    - Qui et quoi cause la menace
  - Cible
    - Quels éléments du système peuvent être affectés par la menace



Identification des risques

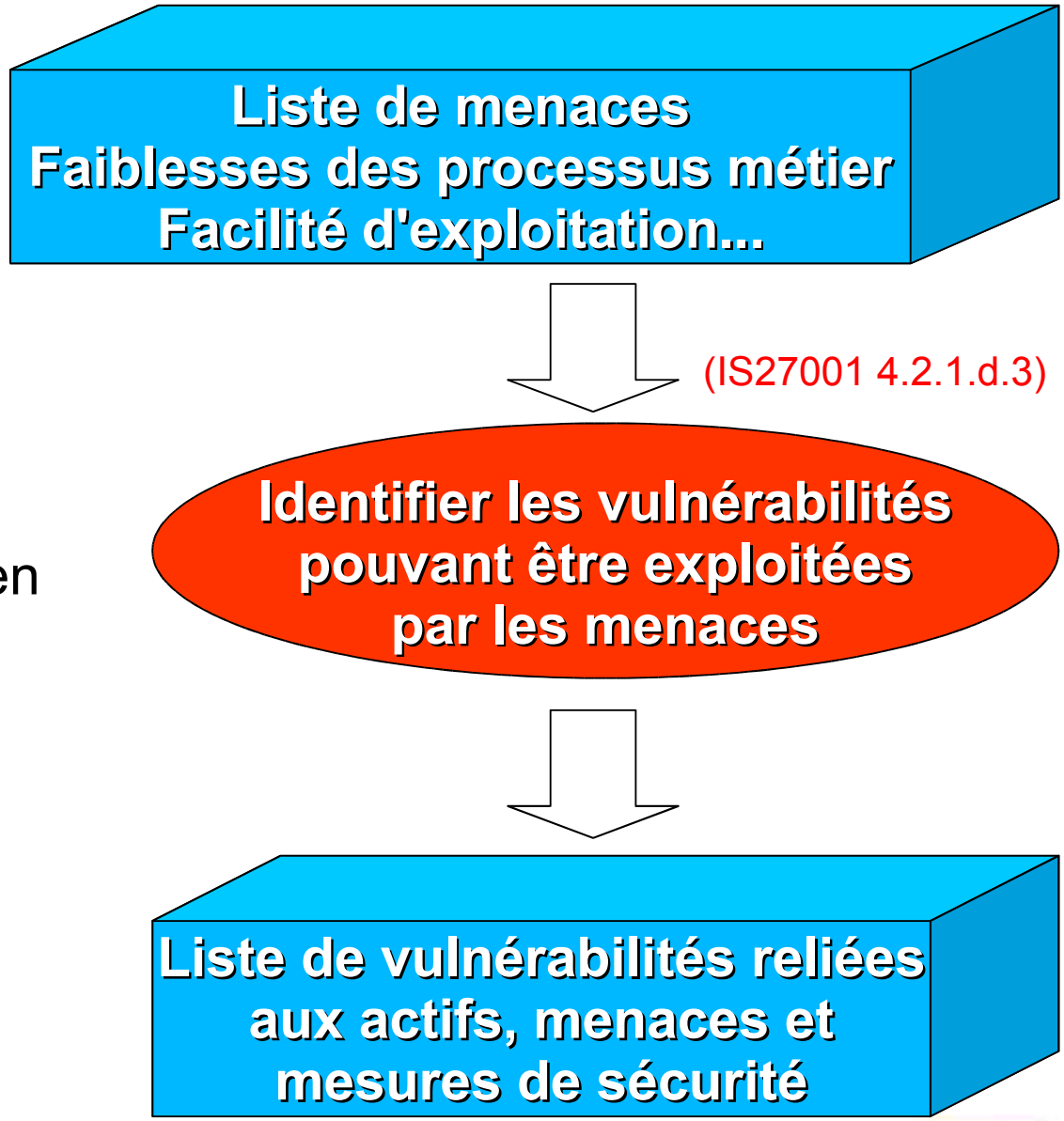
- Identification des menaces (8.2.1.2) .
  - Par interviews
    - Propriétaires d'actifs, utilisateurs, ressources humaines, services opérationnels, spécialistes en sécurité, sécurité physique, juridique...
    - Autorités gouvernementales, météorologie, companies d'assurance...

(*related potential exploring agents*) ←



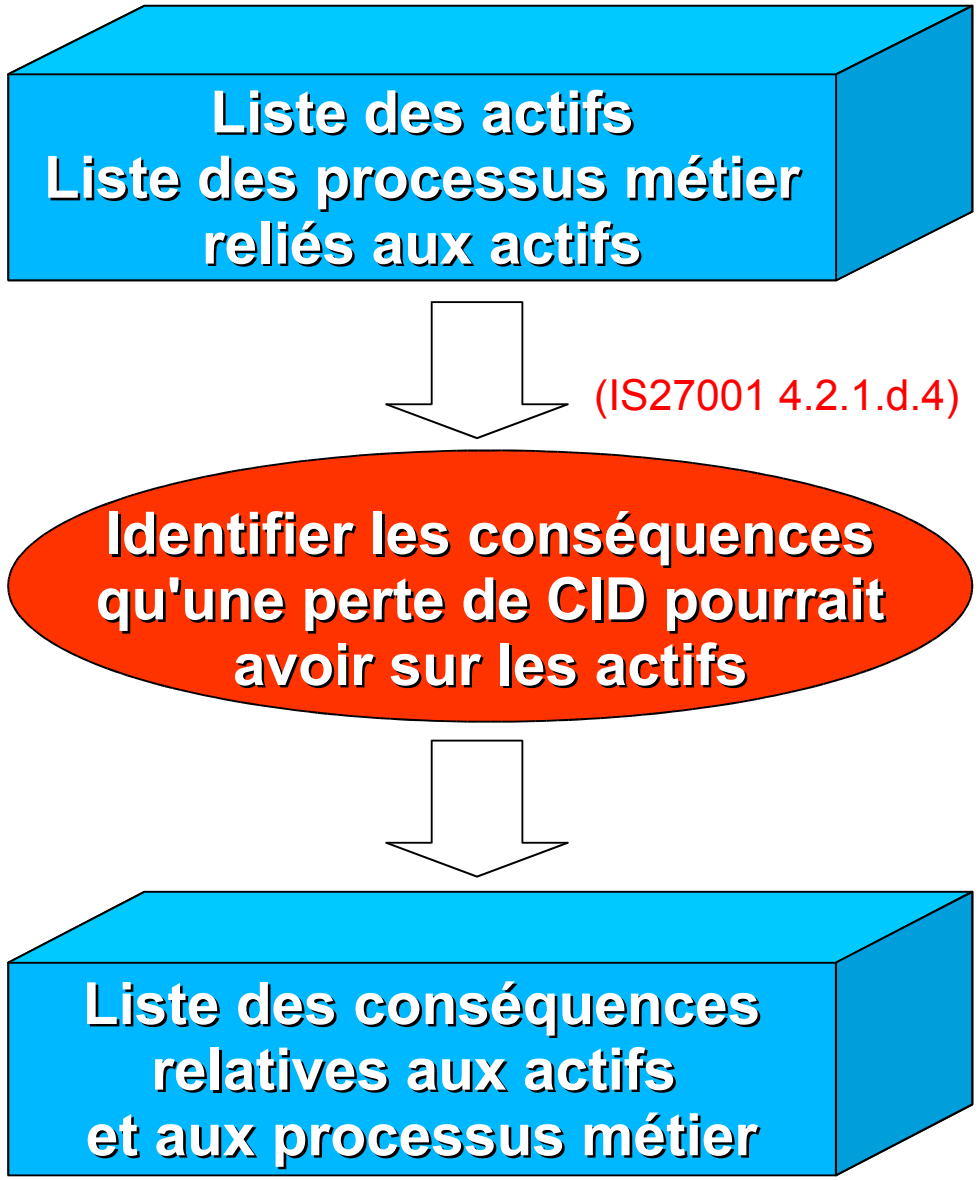
Identification des risques

- Identification des vulnérabilités (8.2.1.3) :
  - Vulnérabilités généralement reliées aux propriétés ou attributs des actifs
  - Vulnérabilités sans aucune menaces doivent être quand même reconnues et suivies en cas de changement plus tard



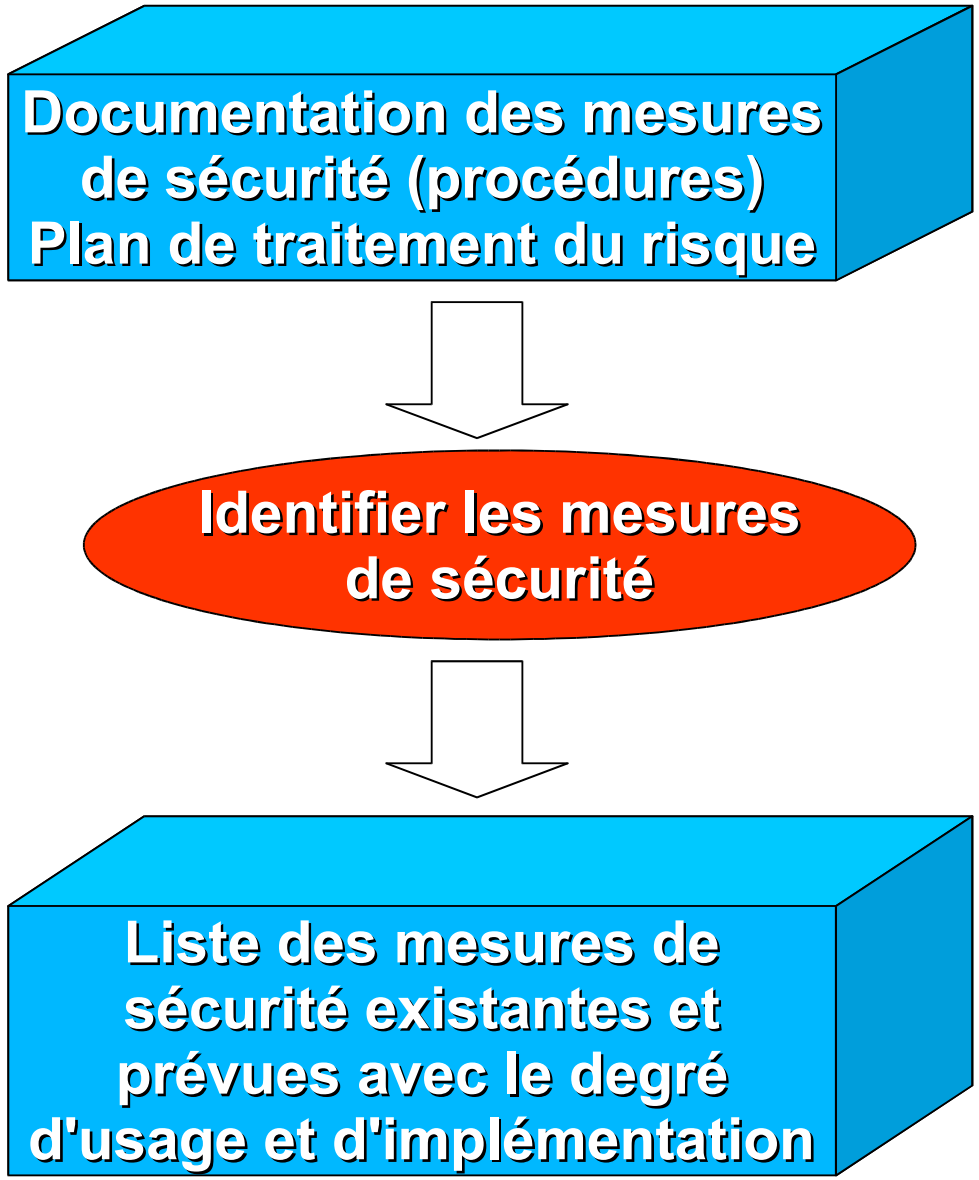
Identification des risques

- Identification des conséquences (8.2.1.4) ou des effets induits :
  - Identification des dommages ou des impacts sur l'organisme
    - Causé par une menace exploitant une vulnérabilité
    - Lors d'un incident de sécurité (cf IS27002 13)
  - Impact mesuré selon les critères d'impact
  - Peut affecter un ou plusieurs actifs
  - Identification des conséquences opérationelles



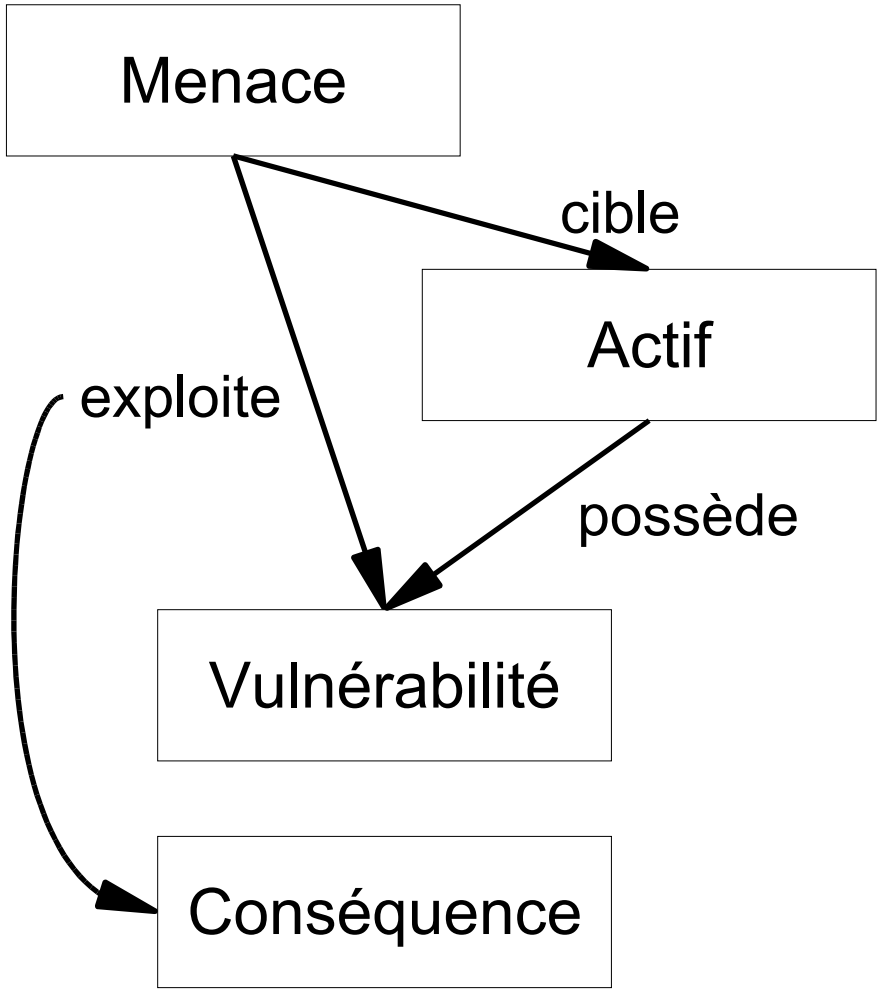
Identification des risques

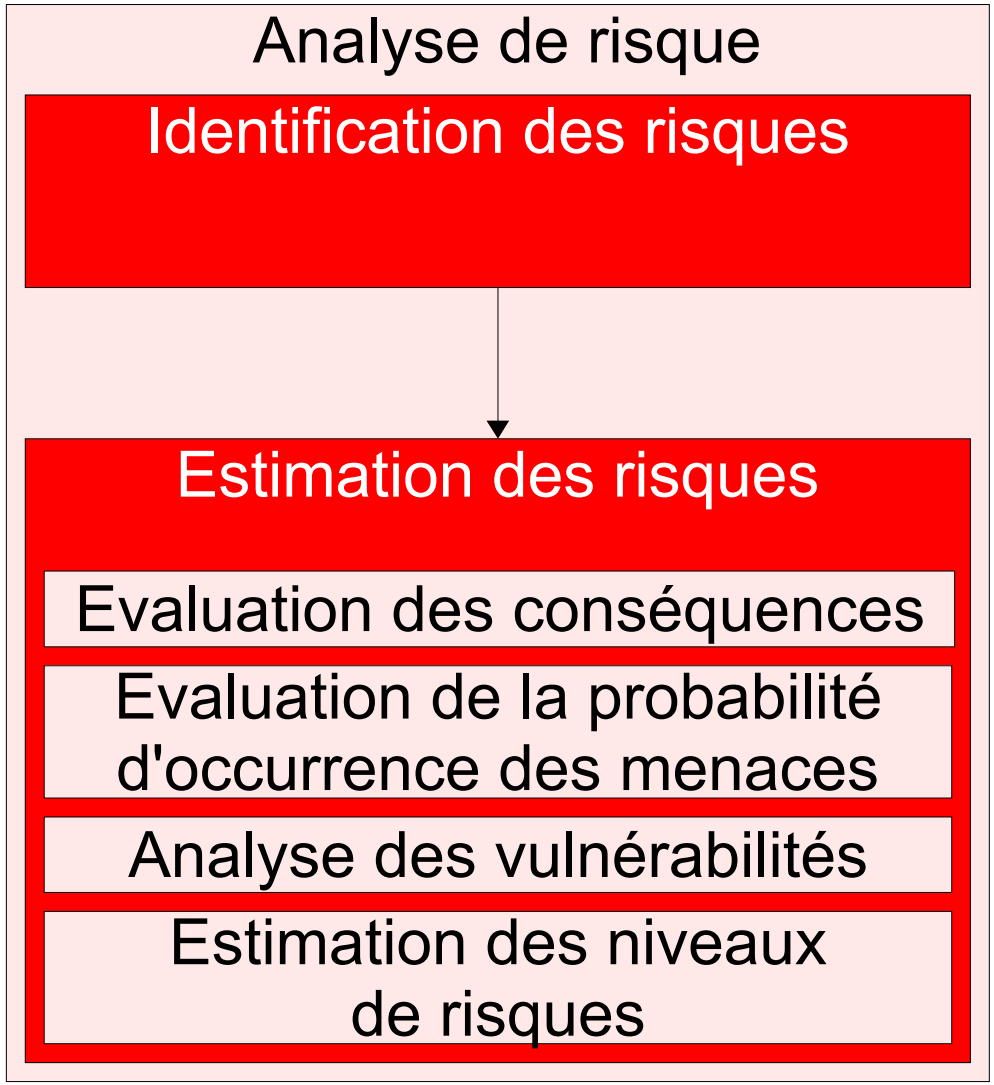
- Evaluation des mesures de sécurité existantes (8.2.1.5) :
  - Evite les redondances
  - Revue du plan de traitement du risque mis en oeuvre, pas du plan élaboré mais pas déjà implémenté
  - Vérification des indicateurs d'efficacité des mesures de sécurité
    - Si une mesure de sécurité ne fonctionne pas comme prévu il peut y avoir des vulnérabilités
  - Interview du RSSI, ...
  - Revue sur site des mesures de sécurité physique



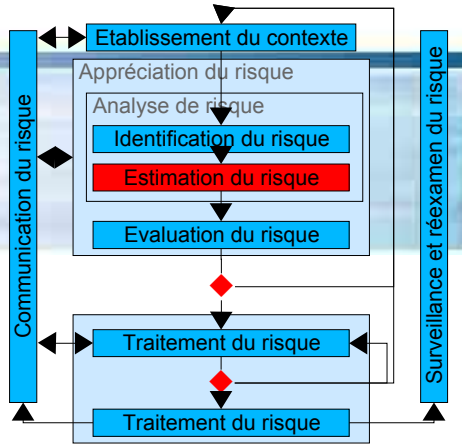
Analyse de risque

- Analyse de risque (8.2) :





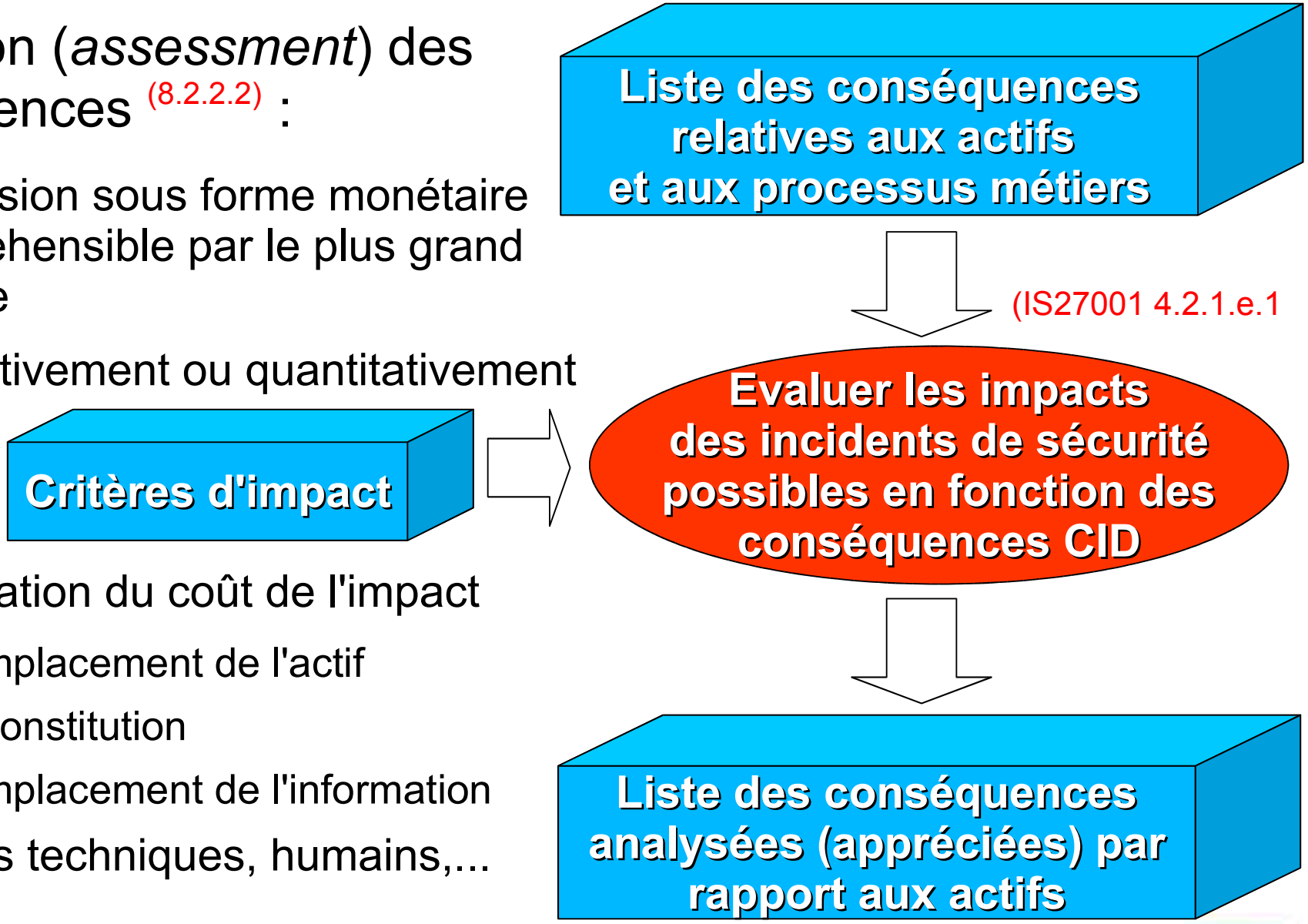
Estimation des risques



- Méthodes d'estimation des risques (8.2.2.1) :
  - Qualitative
    - Magnitude des conséquences exprimée par exemple par faible, moyenne, élevée
    - Utile en l'absence de données permettant une estimation quantitative
    - + Facilité de compréhension
    - - Subjectivité
  - Quantitative
    - Echelle avec des valeurs numériques
    - A faire avec l'historique des incidents
    - + Directement relié aux objectifs de sécurité
    - - Dépend de la validité du modèle

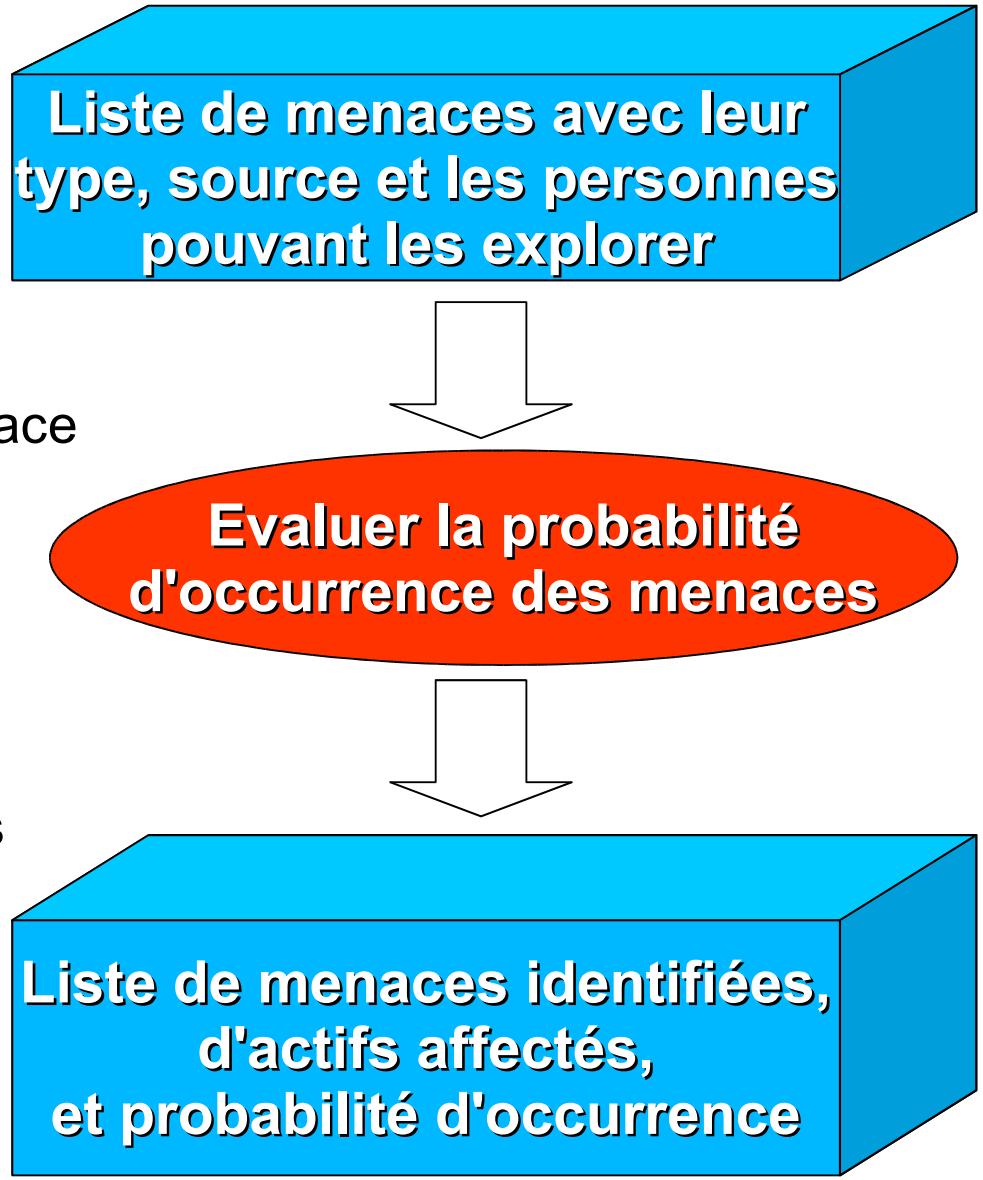
Estimation des risques

- Evaluation (*assessment*) des conséquences (8.2.2.2) :
  - Expression sous forme monétaire compréhensible par le plus grand nombre
  - Qualitativement ou quantitativement
  - Valorisation du coût de l'impact
    - Remplacement de l'actif
    - Reconstitution
    - Remplacement de l'information
  - Critères techniques, humains,...



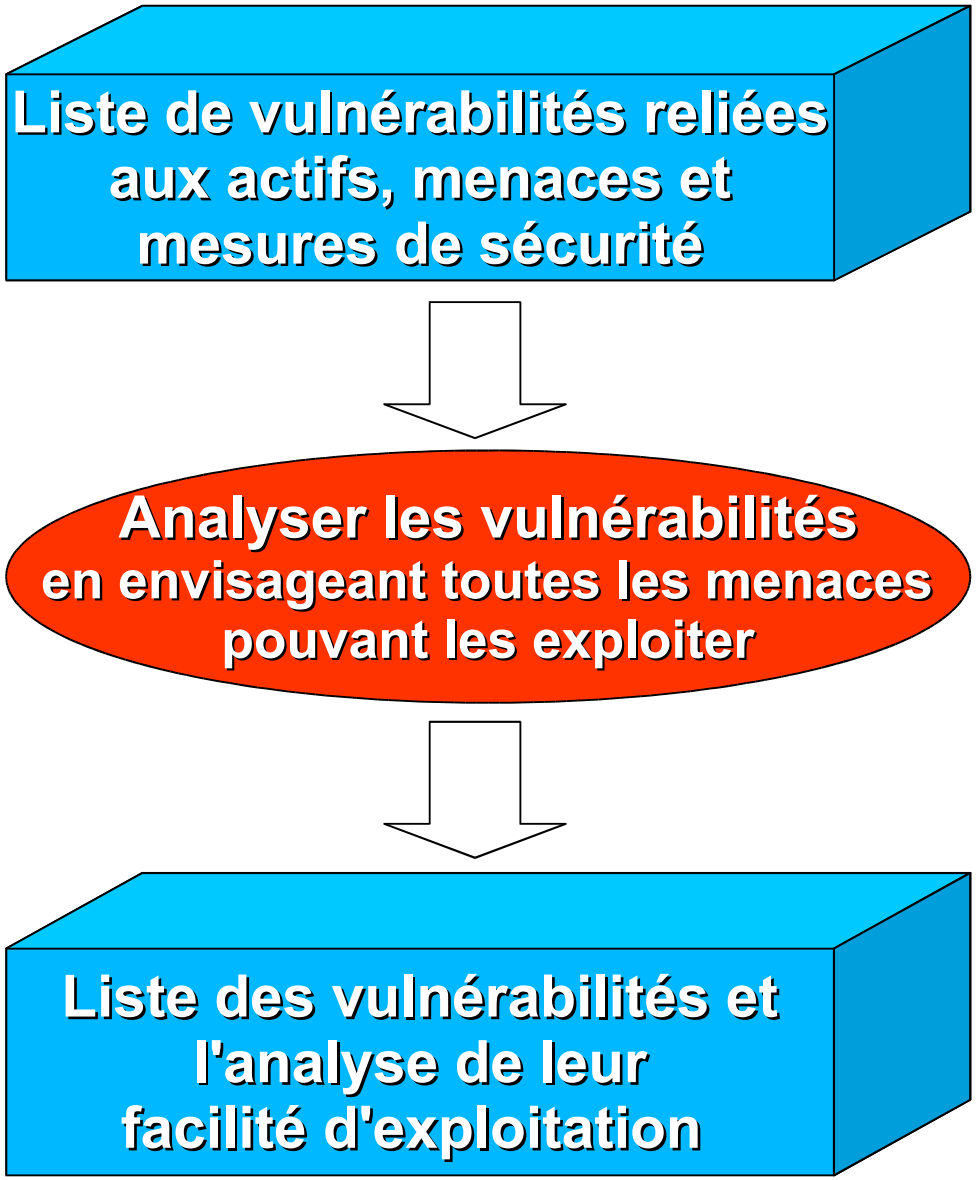
Estimation des risques

- Evaluation (*assessment*) des probabilités d'occurrence des menaces (8.2.2.3) :
  - En prenant en compte :
    - Probabilité d'occurrence de la menace (*threat likelihood*)
    - Motivation, aptitude et ressources des attaquants potentiels et leur perception de l'attractivité et de la vulnérabilité de l'actif
    - Pour les menaces accidentelles les facteurs d'erreurs humaines et de disfonctionnement, géographiques et météorologiques
  - Probabilité d'ocurence faible, moyenne, élevée



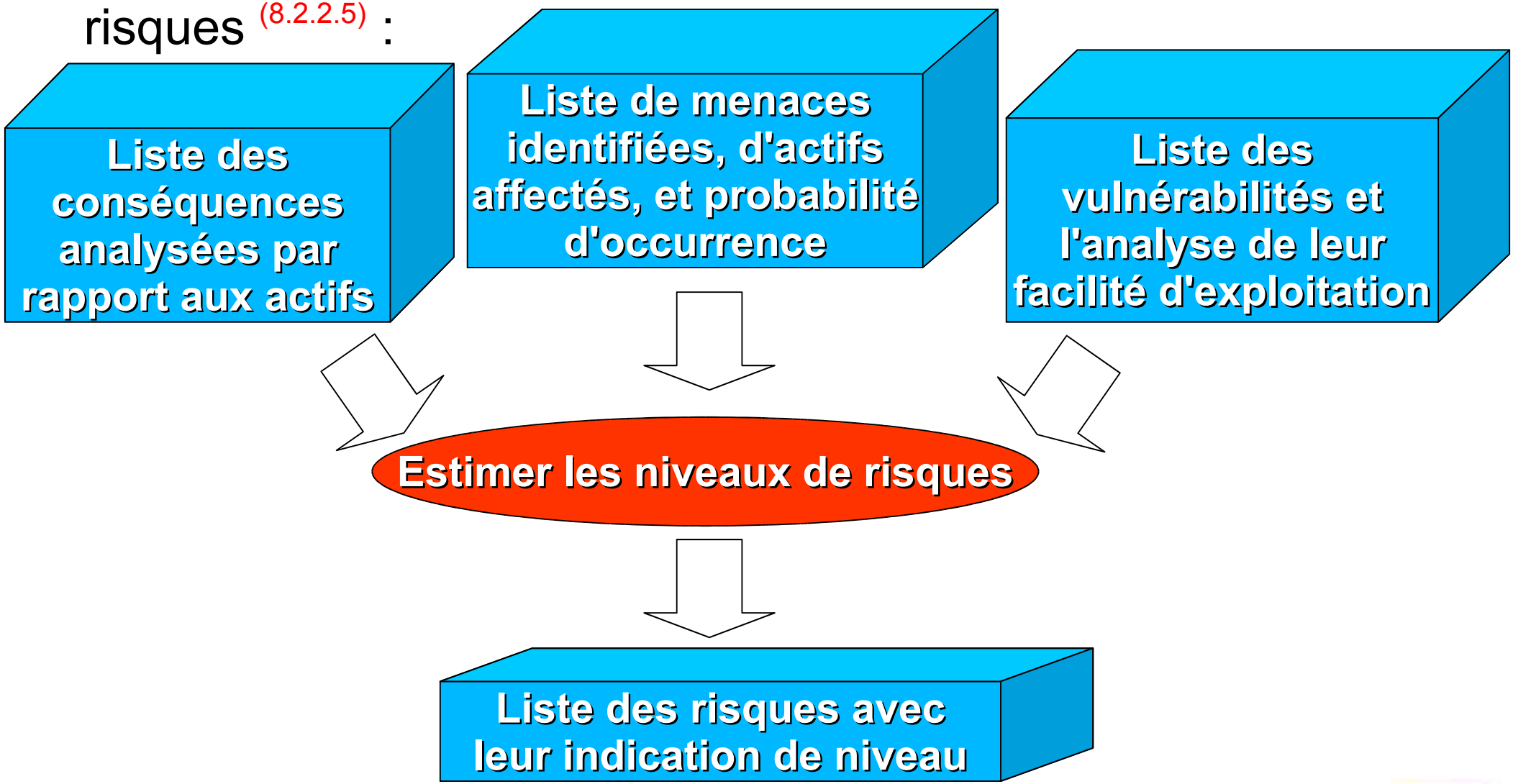
Estimation des risques

- Analyse (*assessment*) des vulnérabilités (8.2.2.4) :
  - En envisageant toutes les menaces pouvant les exploiter
  - Dans une situation donnée
  - En prenant en compte :
    - Facilité d'exploitation
      - Qualitative ou quantitative
    - Mesures de sécurité existantes



Estimation des risques

- Estimation des niveaux de risques (8.2.2.5) :



Estimation des risques

- Estimation des niveaux de risques (8.2.2.5) :
  - Exemple d'une matrice avec des valeurs prédéfinies (E.2.1) :
    - Valeur de l'actif
    - Probabilité d'occurence de la menace (était niveau de menace (BS7799-3 C.5.3))
    - Facilité d'exploitation (était niveau de vulnérabilité (BS7799-3 C.5.3))

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Estimation des risques

- Estimation des niveaux de risques (8.2.2.5) :
  - Exemple d'un ordonnancement des menaces par mesure de risque (E.2.2) :

① Conséquence (était impact (BS7799-3 C.5.4)) en fonction de la valeur de l'actif de 1 à 5

② Probabilité d'occurence de la menace de 1 (faible) à 5 (élevée)

③ Mesure du risque (d) = (b) x (c) conséquence x probabilité d'occurence

④ Ordonnancement des menaces (était incident (BS7799-3 C.5.4)) en fonction des niveaux de risque

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Estimation des risques

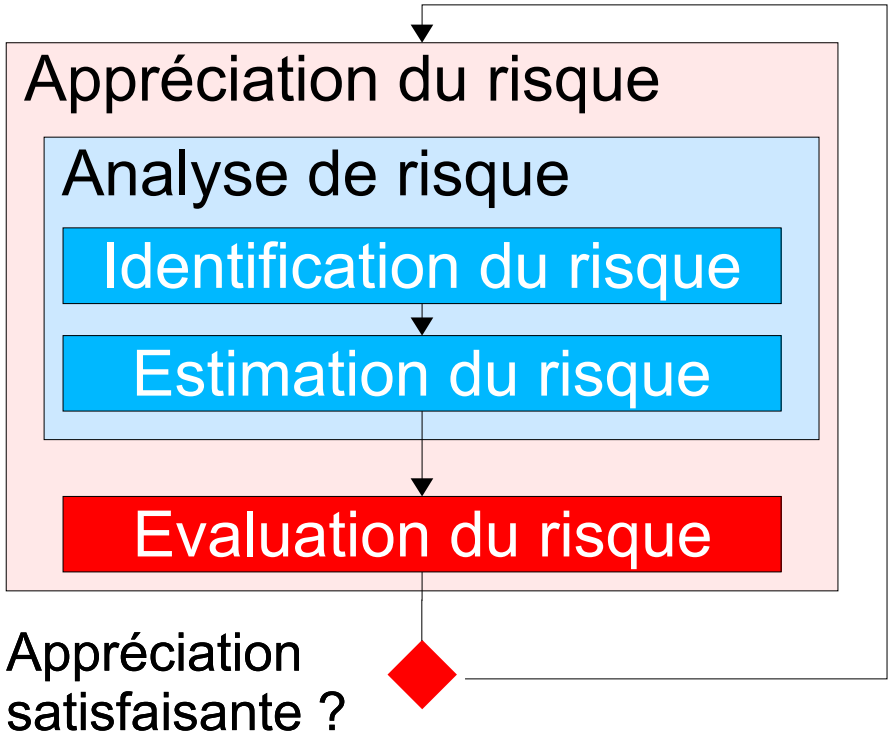
- Estimation des niveaux de risques (8.2.2.5) :
  - Exemple d'une évaluation par probabilité d'occurrence et conséquences possible des risques (E.2.3) :

Levels of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Likelihood Value	0	1	2	1	2	3	2	3	4

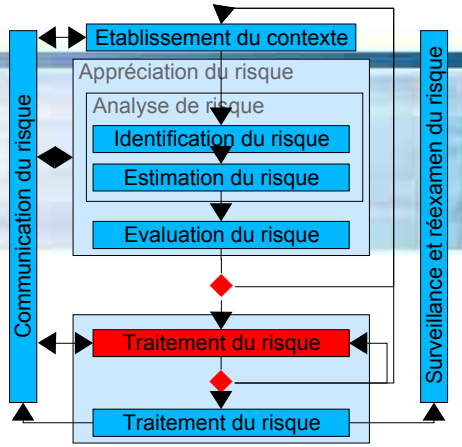
Asset Value	0	1	2	3	4
Likelihood Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Evaluation du risque

- Evaluation du risque (8.3) :



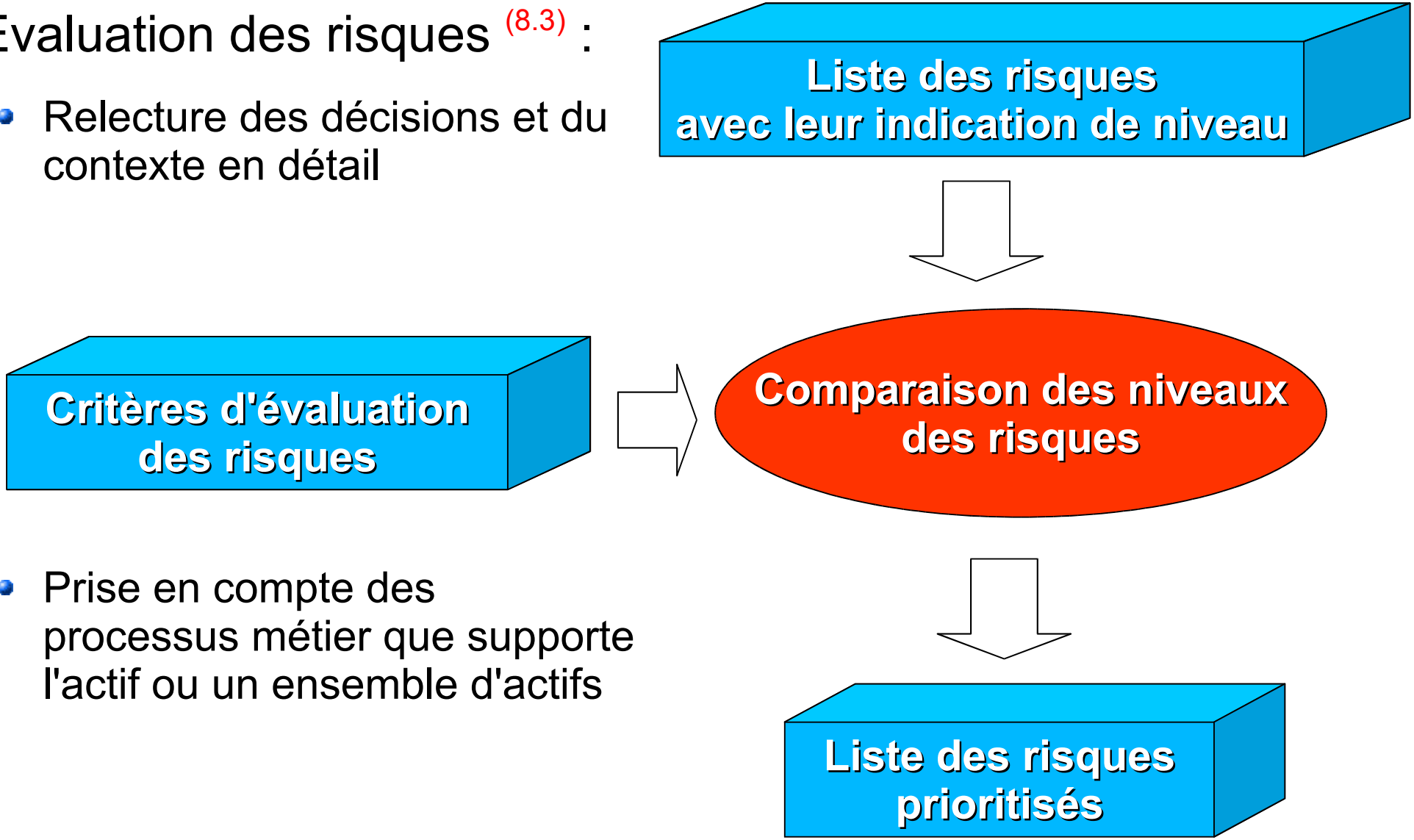
Evalution du risque



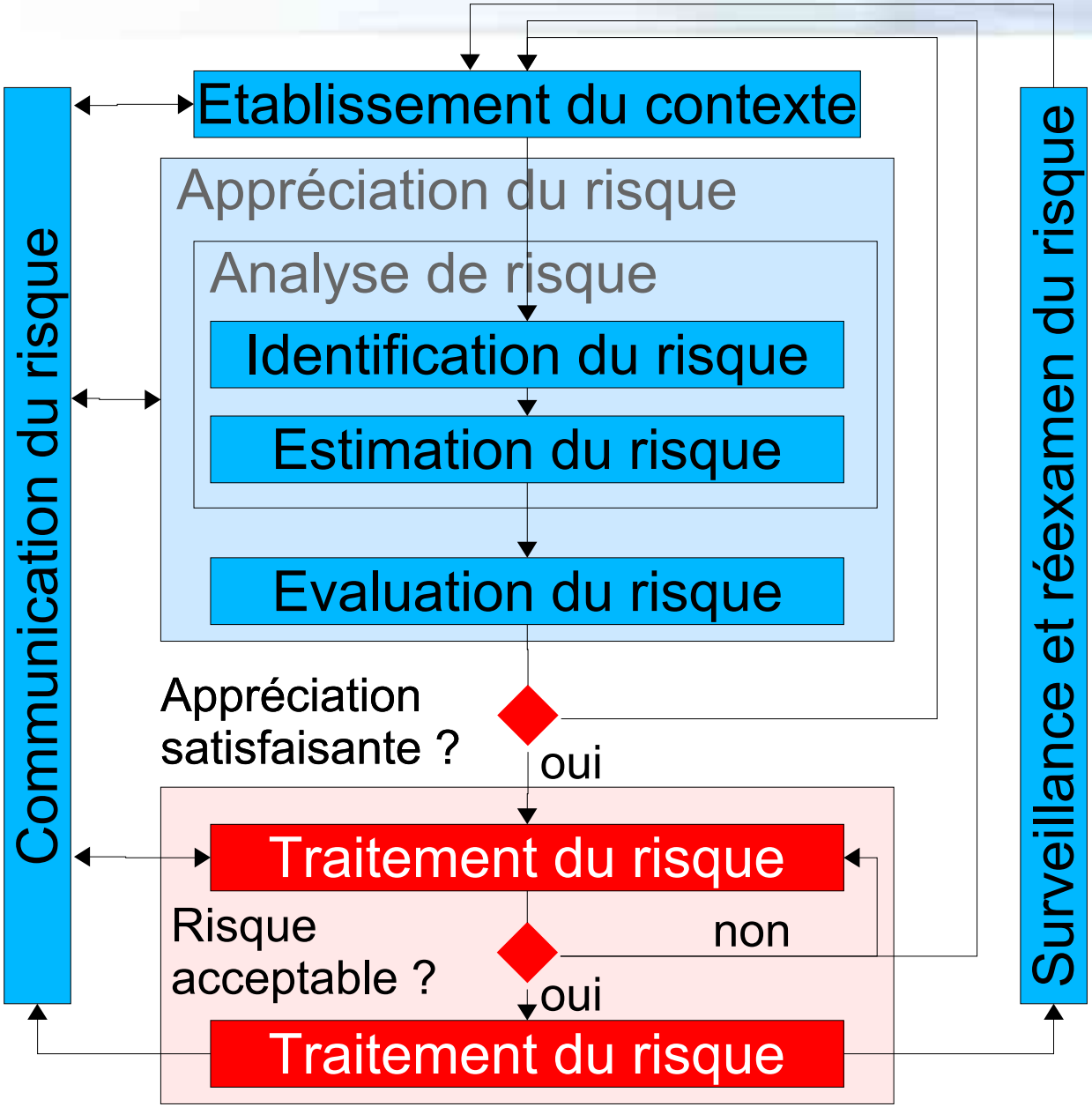
- Evaluation du risque (8.3) :
  - Prise de décisions
    - Si une activité doit être engagée
    - Priorités pour le traitement du risque
  - Utilisation de la compréhension du risque obtenue grâce à l'analyse de risque
  - Prise en compte en plus des risques estimés, des obligations contractuelles, légales et règlementaires

Evaluation du risque

- Evaluation des risques (8.3) :
  - Relecture des décisions et du contexte en détail
  - Prise en compte des processus métier que supporte l'actif ou un ensemble d'actifs

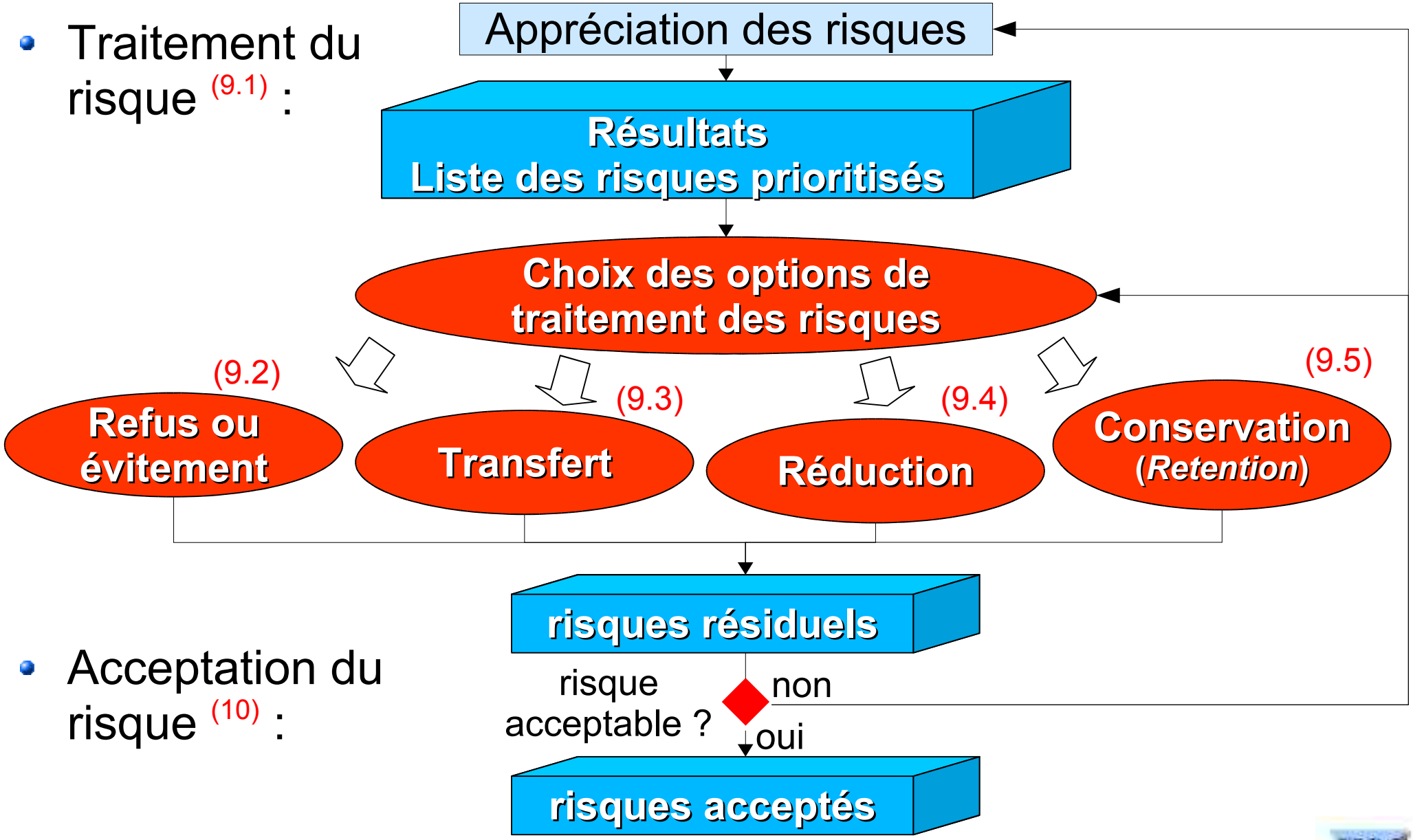


Traitement et acceptation du risque



Traitement et acceptation du risque

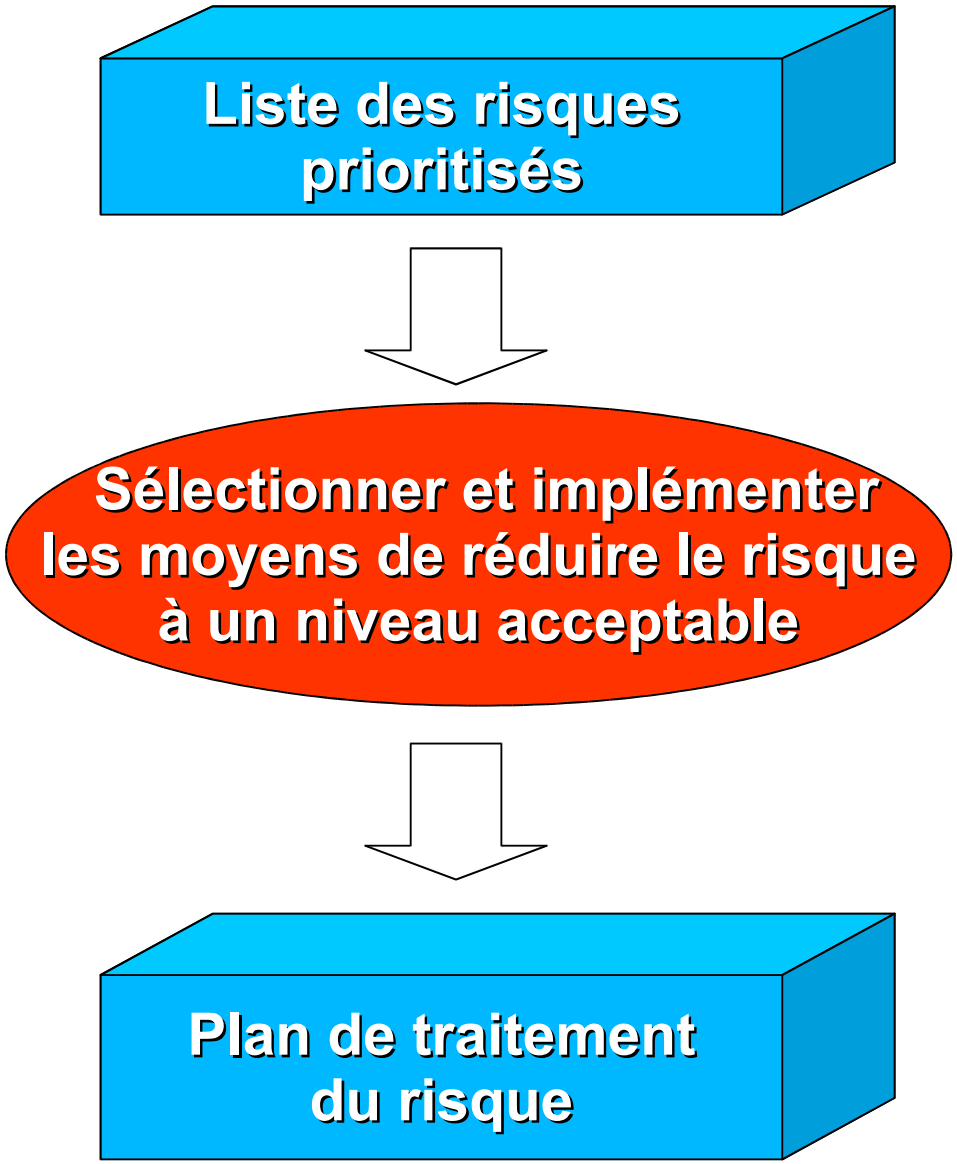
- Traitement du risque (9.1) :



- Acceptation du risque (10) :

Traitement du risque

- Traitement du risque [9.1] :
  - Intégration des coûts
    - Mise en adéquation de coûts par rapport aux bénéfices attendus
    - Forte réduction pour peu de dépenses ?
    - Amélioration très coûteuse ?
  - Prise en compte des risques rares aux impacts importants
    - Qui échappent aux logiques économiques



Traitement du risque

- Traitement du risque (9.1) :
  - Prise en compte des parties concernés
    - Comment les risques sont perçus par les parties concernées
    - Comment communiquer avec les parties concernées

Traitement du risque

- Refus ou évitement du risque (9.2) :
  - Risques considérés trop élevés

Traitement du risque

- Transfert du risque (9.3) :
  - Partage du risque avec des tierces parties
  - Peut créer de nouveaux risques ou modifier les risques existants
    - Nouveau traitement du risque potentiellement nécessaire
  - Transfert à une assurance qui supporte les conséquences
  - Transfert à un sous-traitant qui va surveiller le système d'information pour prendre des actions appropriées en cas d'attaque
  - Attention !
    - Transfert de responsabilité managériale (*responsability*) d'un risque est faisable
    - Transfer la responsabilité légale (*liability*) d'un impact normalement impossible

Traitement du risque

- Réduction du risque (9.4) :
  - Réduction de l'impact d'un risque de manière à ce que le risque soit acceptable
  - Dans la sélection des mesures de sécurité, prendre en compte les **contraintes** :
    - Temps
    - Moyens financiers et TCO de la mesure de sécurité
    - Techniques et opérationelles
      - Exemple : besoins de performance, complexité d'administration, problèmes de compatibilité
    - Humaines et culturelles
      - Exemple : un mot de passe trop long et trop complexe sera écrit
      - Exemple : personne n'appliquera une mesure de sécurité que leur responsable juge innacceptable
    - Moyens humains
      - Sans personnel compétent les mesures de sécurité ne marcheront pas
    - Ethiques, légales, ...

Traitement du risque

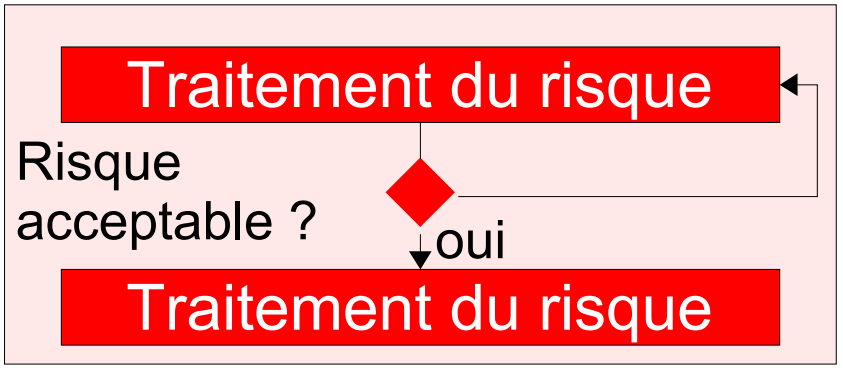
- Réduction du risque (9.4) :
  - Fonctionalités des mesures de sécurité :
    - Correction (*correction*)
    - Elimination (*elimination*)
    - Prévention (*prevention*)
    - Dissuasion (*deterrence*)
    - Détection (*detection*)
    - Recouvrement (*recovery*)
    - Surveillance (*monitoring*)
    - Sensibilisation (*awareness*)

Traitement du risque

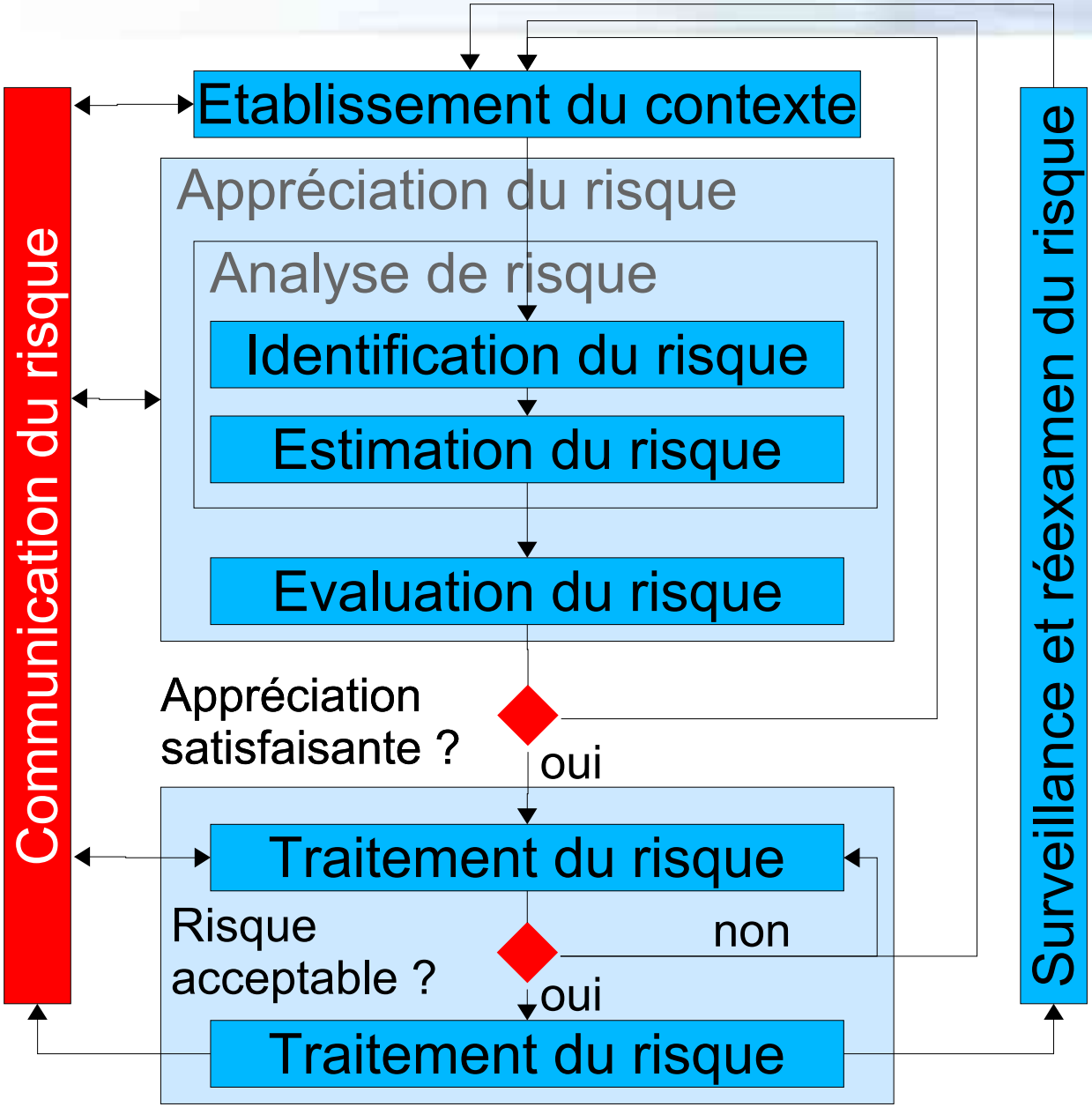
- Conservation du risque (27005 9.5) (27001 4.2.1.f.2) :
  - ISO 27001:2005 : **Acceptation du risque** (*risk acceptance*)
  - ISO 27005 : Devenu **Conservation du risque** (*risk retention*)
    - Conservation, maintien ou rétention du risque, ou prise de risque
  - Risque peut être conservé car le niveau de risque est inférieur aux critères d'acceptation des risques
  - Risque peut être conservé par rapport aux intérêts que celà procure
  - Doit être basé sur l'analyse des coûts du traitement du risque face aux coûts de reconstruction
  - Vérifier que le responsable prenant une décision de conservation de risque a réeellement le pouvoir de le faire

Acceptation du risque

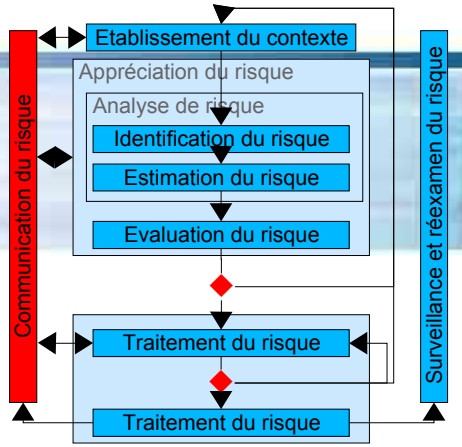
- Acceptation du plan de traitement des risques (10)
- Par la direction générale
  - Soit le plan de traitement du risque est réussi
  - Soit la direction générale accepte le risque en toute connaissance de cause
    - Manque de budget
    - Contraintes de temps
    - Bien que le risque soit au-delà des critère d'acceptation des risques
- Enregistrement formel



Communication du risque

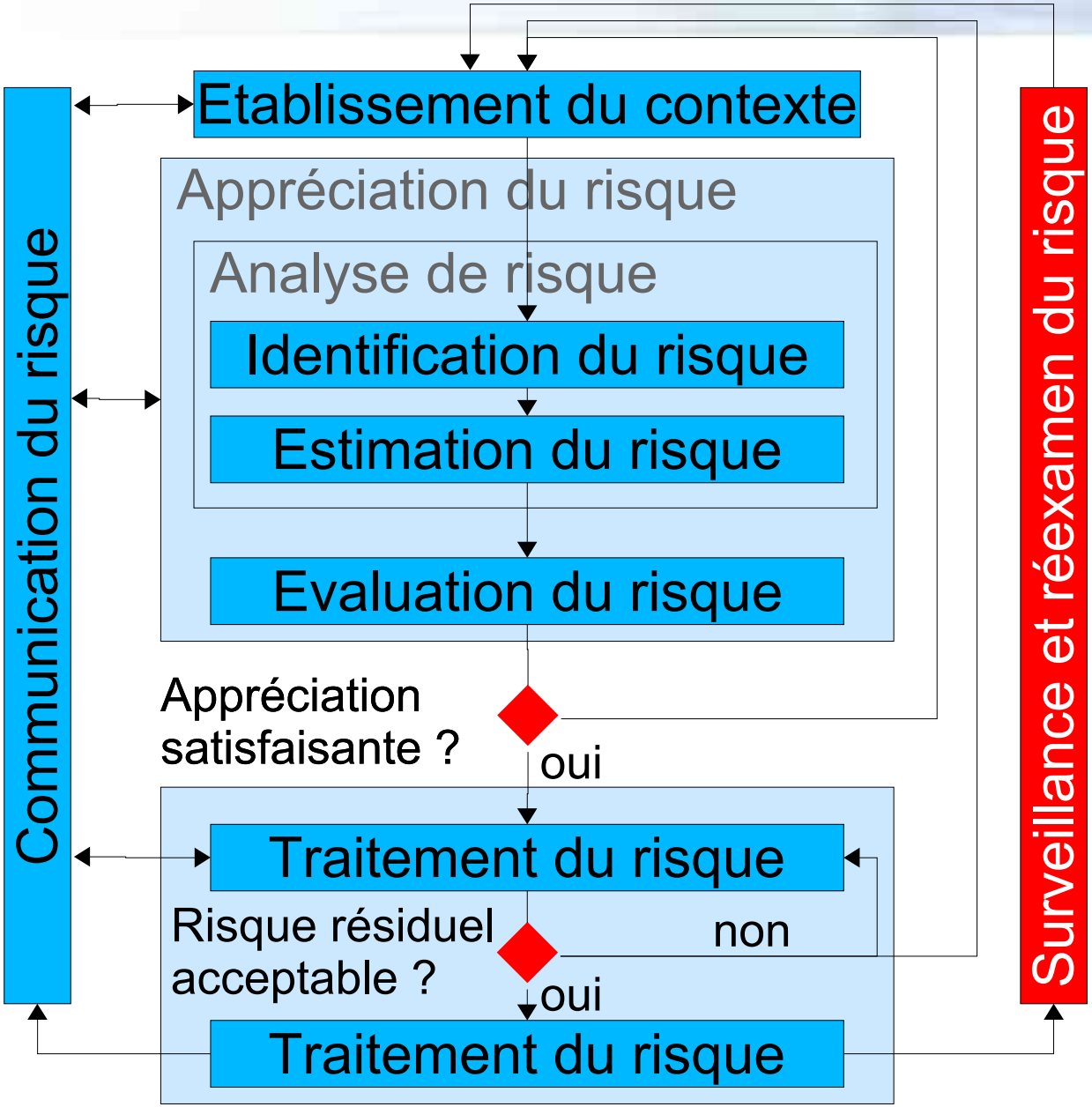


Communication du risque



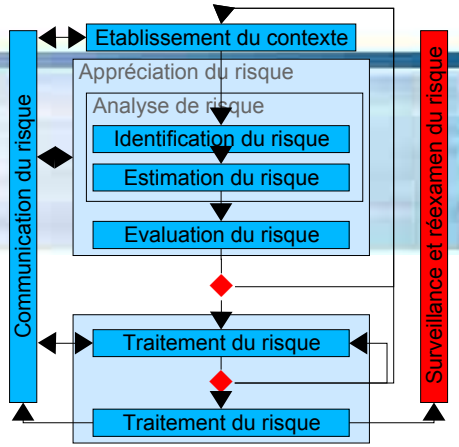
- Communication du risque de sécurité de l'information (*information security risk communication*) [(11)] :
- Echange et partage d'information sur les risques entre :
  - Processus de gestion de risque
  - Décisionnaires (*decision-makers*) et les dépositaires des enjeux (*stakeholders*)
- Activité continue
- Permet de :
  - Réduire les incompréhensions avec les décisionnaires
  - Obtenir de nouvelles connaissance en sécurité
  - Améliorer la sensibilisation

Surveillance et réexamen du risque



(IS27001 4.3.2.d)

Surveillance et réexamen du risque



- Surveillance et réexamen des éléments du risque (12.1) (suivi des risques) :
  - Valeur des actifs
  - Impacts
  - Menaces
  - Vulnérabilités
    - Vulnérabilités nouvelles
  - Potentialité ou probabilité d'occurrence (*likelihood*)
    - Exploitation de vulnérabilités qui ne l'étaient pas auparavant

Surveillance et réexamen du risque

- Surveillance et réexamen du processus de gestion de risques (12.2) :
  - Contexte légal et environnemental
  - Concurrence
  - Approche de l'appréciation du risque
  - Valeur et catégories des actifs
  - Critères d'impact
  - Critères d'évaluation des risques
  - Critère d'acceptation des risques
  - TCO (*Total Cost of Ownership*)
  - Ressource potentiellement disponibles

Outillage

- Ageris Software SCORE ISMS
  - Supporte actuellement Mehari, EBIOS, AS/NZS 4360:2004
  - Intégration ISO 27005 en cours sur la base du FCD actuel
  - Interface web

- Sûrement d'autres projets dont je n'ai pas connaissance

Conclusion

- Norme ➔ **consensus** entre les acteurs du marché
- ISO 27005
  - Ne peut être plus complet que toutes les méthodes qui l'ont précédé
  - Représente le noyau commun accepté par tous
  - Peut être complété en allant rechercher ailleurs
- Méthodes d'analyse de risques existantes
  - Peuvent continuer à évoluer et innover
  - Peuvent contribuer à l'amélioration de la norme ISO 27005
  - Peuvent complèter la norme
  - A terme certaines méthodes pourront se dirent "conformes à la norme ISO 27005"

Conclusion

- ISO 27005 = Méthodologie complète
  - Structure sa démarche
  - Autonome
- Correspond strictement au respect de l'ISO 27001
  - Nécessaire pour la mise en place d'un SMSI
  - Nécessaire pour une certification
- Entrera dans la gestion de risque en général
  - Normalisations ISO de tous les types de risques : financiers, industriels, routiers, santé, ...
- Vocabulaire
  - Compréhensible et plutôt proche du langage courant

Conclusion

- ISO 27005 est d'ores et déjà incontournable au niveau international
  - Du fait de l'ISO 27001
- ISO 27005 manque d'expériences pratiques en France
- ISO27005 permet une gestion des risques simple, pragmatique, adapté aux réalités des affaires
  - Pas un processus linéaire
    - Pas une étape infaisable sans avoir fait la précédente
    - Possible de démarrer au milieu et d'y aller progressivement
  - Rien d'obligatoire dans le formalisme
    - Seules les étapes imposées par l'ISO 27001 doivent être suivies
    - Le fait qu'elles ont été suivies doit être montrable

Prochains rendez-vous

- **Formation ISO27001 Lead Auditor** :
  - Certification ISO27001 Lead Auditor par **LSTI**
  - **http://www.hsc.fr/services/formations/**

Paris : 18-22 juin
Rennes : 10-14 sept.
Luxembourg: 24-28 sep
Lyon : 3-7 décembre
Toulouse : février 2008
Nantes : avril 2008

- **Formation ISO27001 Lead Implementer** :
  - Inclus la formation ISO 27005
  - Certification Lead Implementer par **LSTI**
  - **http://www.hsc.fr/services/formations/**

Paris : 21-25 mai
Luxembourg: 12-16 nov

Questions ?

Herve.Schauer@hsc.fr
www.hsc.fr

ISO 27005 à son club !
Paris, Toulouse, ITIL, ...
www.club-iso27001.fr
Club ISO 27001

Acronymes

- ALE : *Annual Loss of Expectancy*
  - Pertes annuelles prévisibles à partir de la fréquence de survenance d'un incident et coût financier de son impact
- CID : Confidentialité, Intégrité, Disponibilité
  - Trois principaux critères de sécurité
- TCO : *Total Cost of Ownership*
  - Coût total associé au cycle déploiement / maintenance