UFC
UNIVERSITÉ
DE FRANCHE-COMTÉ

femto-st
sciences & technologies

Cours Sécurité – L3 Informatique

Partie II – Sécurité des Systèmes d'Information

Chapitre 1 – Menaces et vulnérabilités

Chapitre 2 – Analyse de risque et Test de sécurité

Sommaire du chapitre II.2

- Analyse de risques et définition d'une politique de sécurité
  - Analyse de risque – ISO 27005
  - La méthode EBIOS de l'ANSSI
  - La modélisation CORAS
- Test de sécurité
  - Types de test

Analyse de risque – Pourquoi ?

- On ne peut pas définir une politique de sécurité cohérente si on ne connait pas les risques, et leur conséquences :
  - Quels actifs à protéger ?
  - Quelles menaces ?
  - Quelles vulnérabilités ?
  - Quels scénarios d'attaque ?
  - Quelle stratégie de sécurité ?
- Mesures des risques :
  - Risques humains
  - Risques techniques
  - Risques juridiques

➔ ISO 27005/2011 - Gestion des risques liés à la sécurité de l'information

➔ Méthode EBIOS - ANSSI
Expression des Besoins et Identification des Objectifs de Sécurité

➔ CORAS - SINTEF
Modélisation de la sécurité

RSSI – Un rôle clé dans les entreprises et organismes publics

- RSSI – Responsable de la Sécurité du Système d'Information
- Rôle : définition, mise en œuvre et contrôle des processus de sécurité des systèmes d'information
  - basé sur une **architecture de sécurité des systèmes d'information**
  - et sur une **politique de sécurité des systèmes d'information**.
- Le RSSI participe à la définition de la **stratégie de sécurité** nécessaire pour couvrir les risques et les impacts sur les biens informationnels de l'organisation.

RSSI – Définition de stratégie

RSSI – Définition de stratégie

Responsable de la sécurité des systèmes d'information (RSSI) | Paris, Île de France

Générale de Santé

Missions principales :

- Définir la politique de sécurité des Systèmes d'Information, la maintenir et contribuer à sa mise en place au sein de GDS tant au niveau du siège que des établissements.
- Définir l'organisation des cellules de crise et les déclencher en cas de sinistre de sécurité informatique.
- Définir les normes et standards en matière de sécurité informatique et valider les outils de sécurité utilisés.
- Analyser les risques et menaces y compris au moyen d'audits et de tests et établir les Plans de Prévention afférents.
- Sensibiliser les collaborateurs de Générale de Santé aux enjeux de la sécurité, participer aux actions de formation.
- Contrôler et garantir la bonne application des normes et des standards de sécurité au sein de Générale de Santé.
- Représenter la DSI dans le cadre de la gestion des risques au sein de Générale de Santé.
- Assurer le suivi des évolutions règlementaires et techniques de son domaine.

Responsable de la sécurité des systèmes d'information (RSSI) | Paris, Île de France

Générale de Santé

Profil :

Ingénieur Informatique Bac+5 ayant une dizaine d'années d'expérience dans la sécurité IT

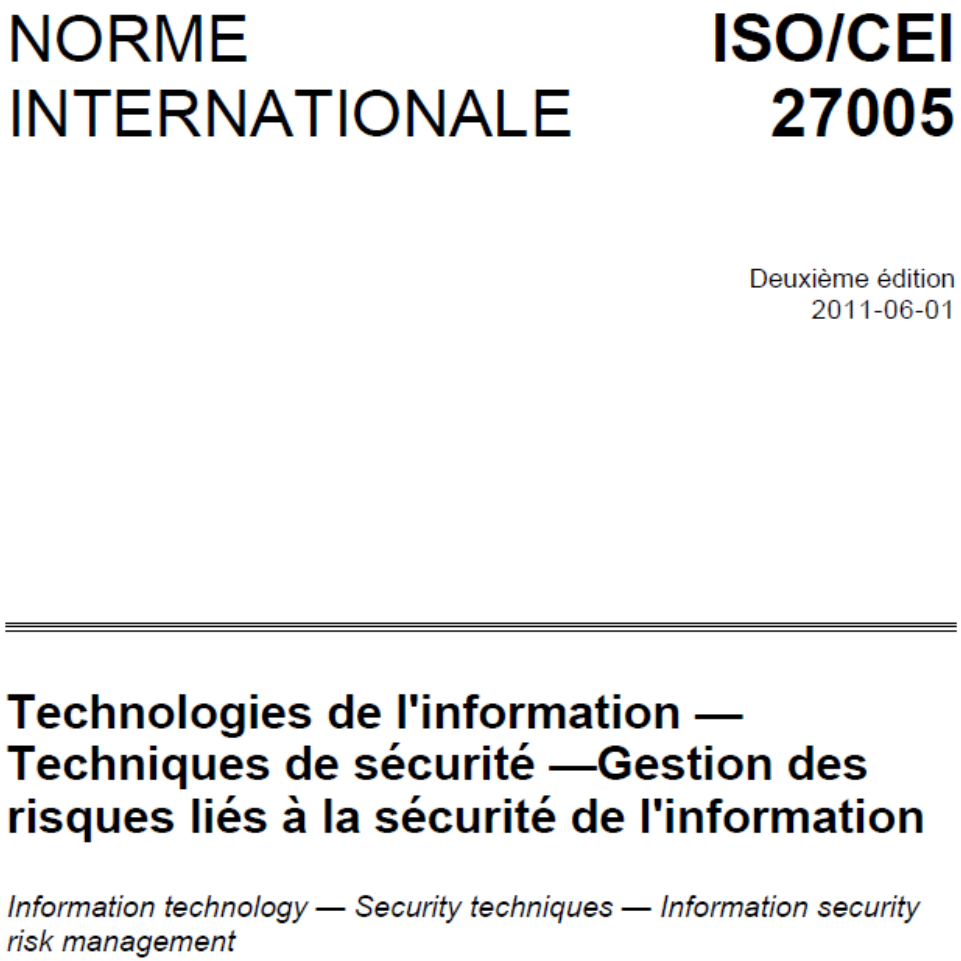
Forte sensibilisation à la sécurité des données

Bonne connaissance des réseaux informatiques

Bonne compréhension et prise en compte des nouveaux usages informatiques et des comportements des utilisateurs ayant un impact sur la sécurité

ISO 27005 - Gestion des risques liés à la sécurité de l'information

- Vocabulaire ISO 27005
- Processus de management du risque
- Evaluation du risque



NORME INTERNATIONALE

ISO/CEI 27005

Deuxième édition
2011-06-01

Technologies de l'information — Techniques de sécurité —Gestion des risques liés à la sécurité de l'information

Information technology — Security techniques — Information security risk management

Terminologie ISO 27005

Terme en français	Terme en anglais	Définition
Analyse de risque	Risk analysis	Processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque. • L'analyse des risques fournit la base de l'évaluation du risque et les décisions relatives au traitement des risques. • L'analyse des risques inclut l'estimation des risques.
Conséquence	Consequence	Effet d'un événement affectant les objectifs. • Un événement unique peut engendrer des conséquences multiples. • Une conséquence peut être certaine ou incertaine et dans le cadre de la sécurité de l'information elle est généralement négative. • Les conséquences peuvent être exprimées de façon qualitative ou quantitative. • Des conséquences initiales peuvent déclencher des réactions en chaîne.

Terminologie ISO 27005

Français	Ang.	Définition
Evénement	Event	Occurrence ou changement d'un ensemble particulier de circonstances. • Un événement peut être unique ou se reproduire, et peut avoir plusieurs causes. • Un événement peut consister en quelque chose qui ne se produit pas. • Il peut parfois être fait référence à un événement en tant qu'«incident» ou «accident».
Mesure de sécurité	Control	Mesure qui modifie un risque • Une mesure de sécurité du risque en sécurité de l'information inclut n'importe quel processus, politique, procédure, recommandation, dispositif pratique ou organisation, qui peut être d'ordre administratif, technique, managérial ou juridique et qui modifie le risque en sécurité de l'information. • Une mesure de sécurité du risque n'aboutit pas toujours à la modification voulue ou supposée. • Une mesure de sécurité du risque est également utilisée comme synonyme de protection ou contre-mesure.

Terminologie ISO 27005

Français	Ang.	Définition
Niveau de risque	Risk level	Importance d'un risque, exprimée en termes de combinaison des conséquences et de leur vraisemblance.
Risque	Risk	Effet de l'incertitude sur l'atteinte des objectifs • Un effet est un écart, positif et/ou négatif, par rapport à un attendu, positif et/ou négatif. • Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'une organisation toute entière). • Un risque est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux. • **Un risque en sécurité de l'information est souvent exprimé en termes de combinaison des conséquences d'un événement de sécurité de l'information et de sa vraisemblance (3.9).** • L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance. • Le risque en sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités

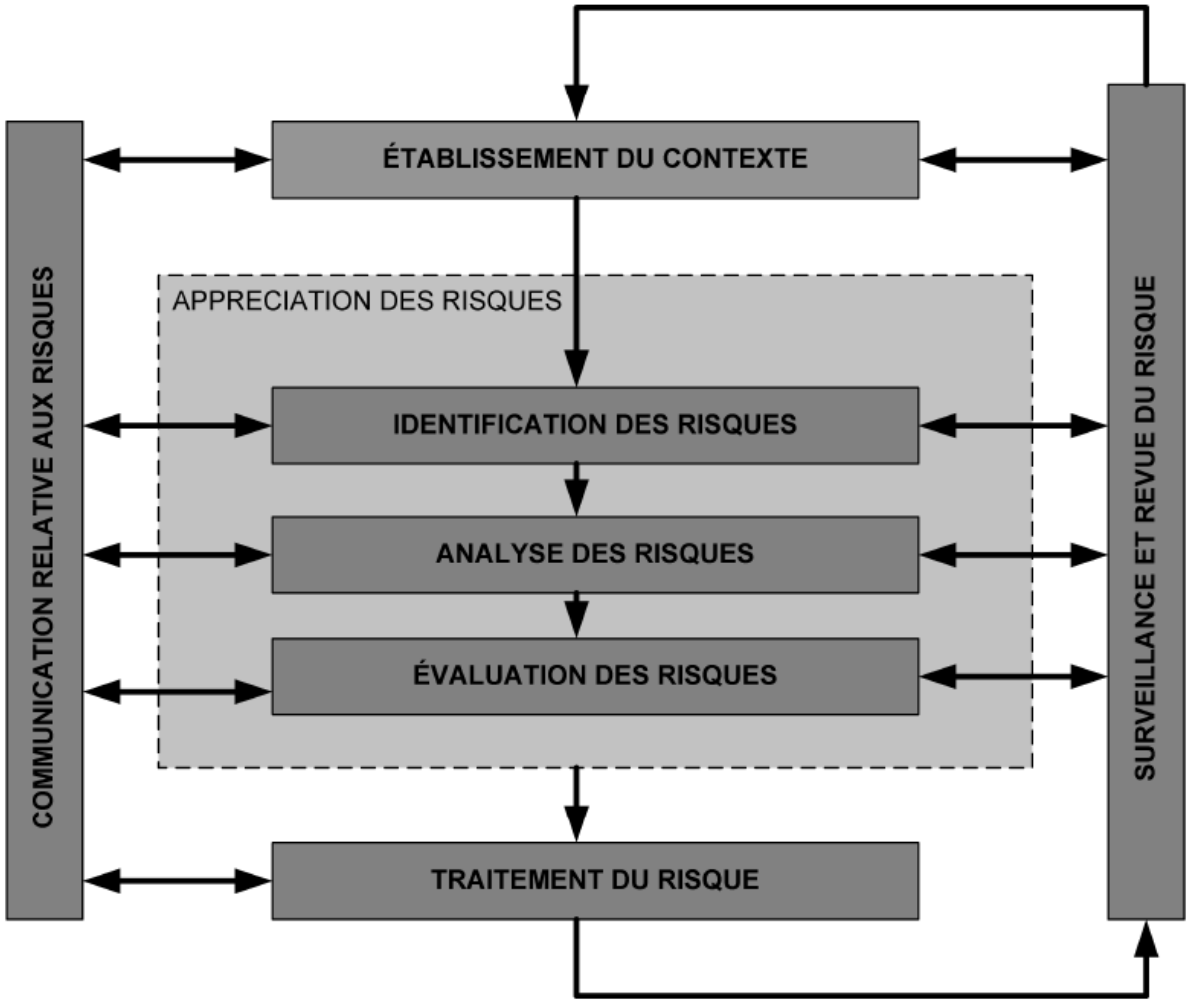
Terminologie ISO 27005

Français	Ang.	Définition
Risque résiduel	Residual risk	Risque subsistant après le traitement des risques. • Un risque résiduel peut inclure des risques non identifiés. • Un risque résiduel peut également être appelé «risque maintenu».
Traitement des risques	Risk treatment	Processus destiné à modifier un risque. • Le traitement des risques peut inclure: o un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque; o la prise ou l'augmentation d'un risque afin de saisir une opportunité; o l'élimination de la source de risque; o une modification de la vraisemblance; o une modification des conséquences; o un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque); et o un maintien du risque fondé sur une décision argumentée. • Les traitements des risques portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque». • Le traitement des risques peut créer de nouveaux risques ou modifier des risques existants.

Terminologie ISO 27005

Français	Ang.	Définition
Vraisemblance	Likelihood	Possibilité que quelque chose se produise. • Dans la terminologie de la gestion des risques, le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée). • Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie de la gestion des risques, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

Processus de gestion des risques ISO 27005



Etablissement du contexte – 1/2

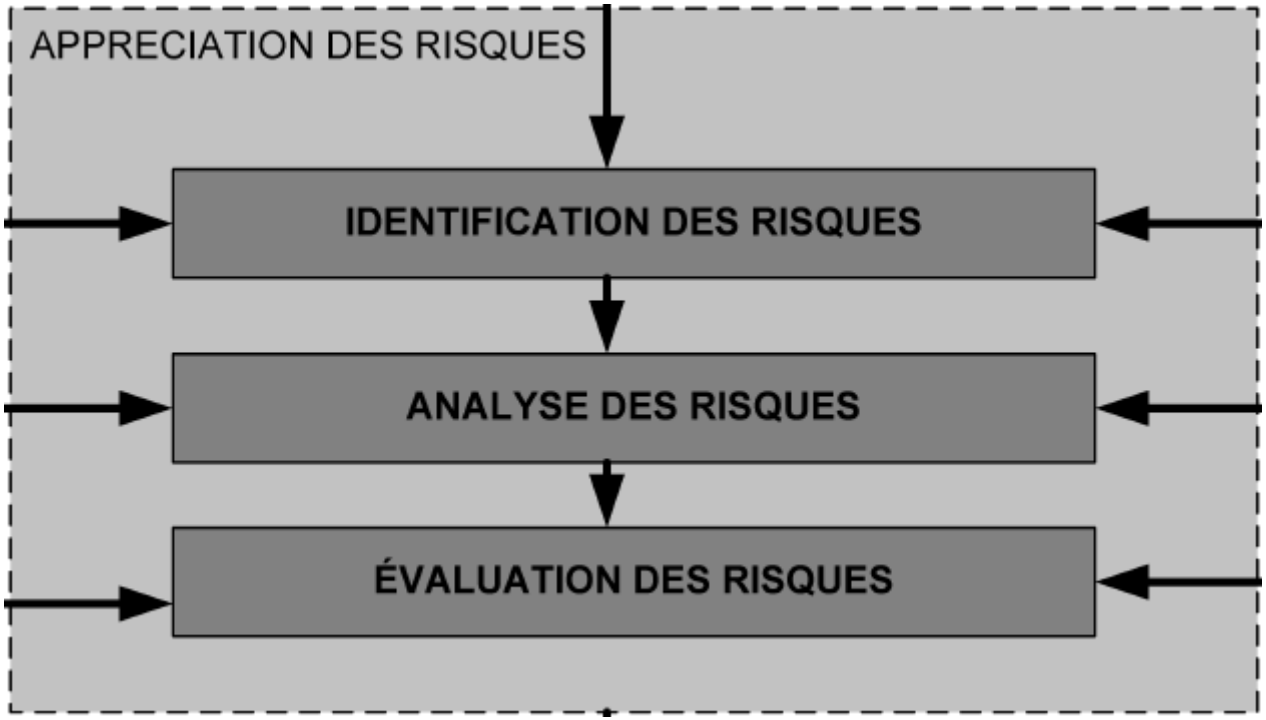
- **Contexte externe et Contexte interne.**

- **Contexte externe** : l'environnement externe dans lequel l'organisation cherche à atteindre ses objectifs. Le contexte externe peut inclure:
  - l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local;
  - les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisation; et
  - les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

Etablissement du contexte – 2/2

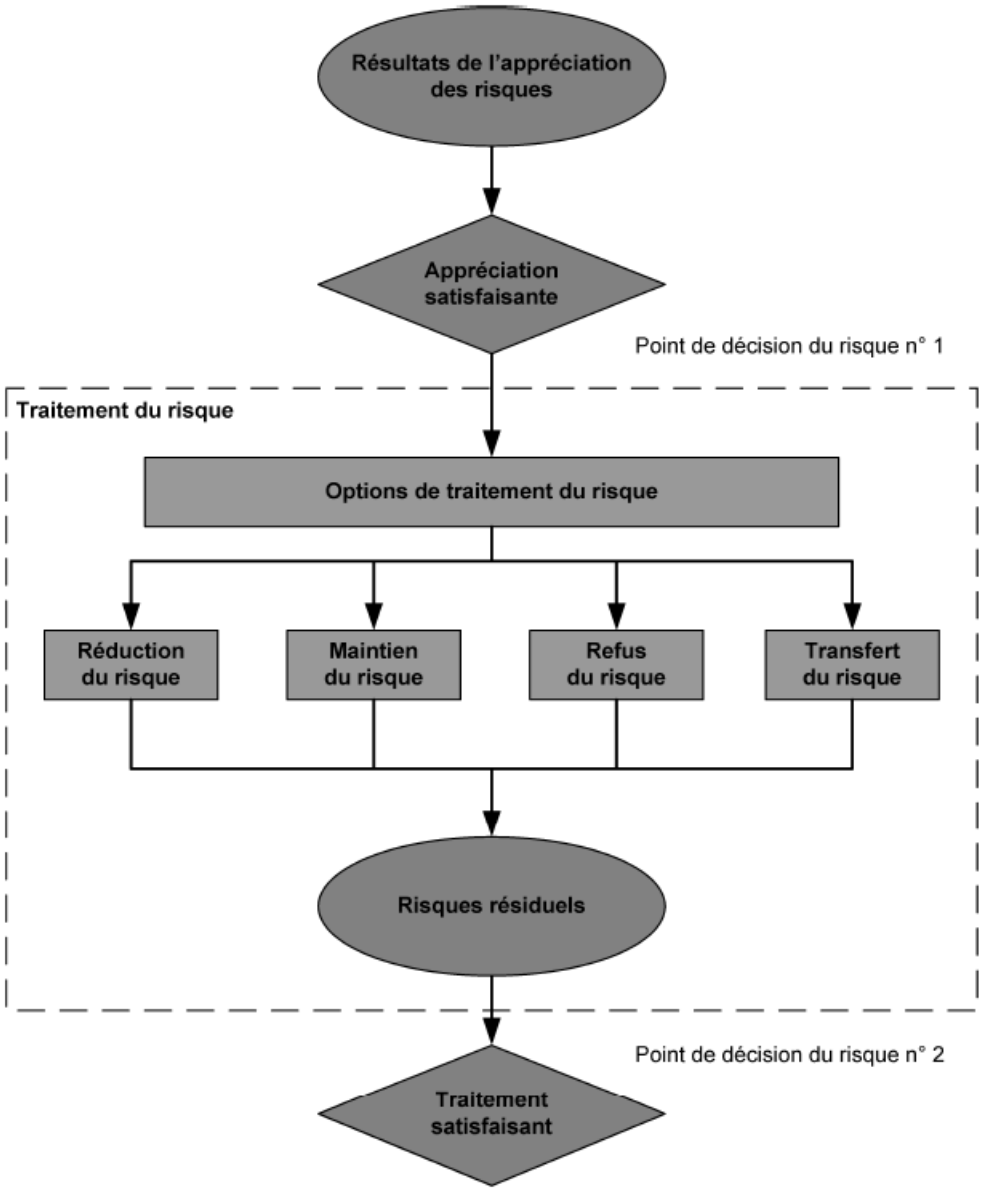
- **Contexte interne** : l'environnement interne dans lequel l'organisation cherche à atteindre ses objectifs. Le contexte interne peut inclure:
  - la gouvernance, l'organisation, les rôles et responsabilités;
  - les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers;
  - les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies);
  - les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels);
  - les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs;
  - la culture de l'organisation;
  - les normes, lignes directrices et modèles adoptés par l'organisation; et
  - la forme et l'étendue des relations contractuelles.

Appréciation des risques – ISO 27005



Traitement du risque

- 4 options de traitement du risque :
  - Réduction du risque
  - Maintien du risque
  - Refus du risque
  - Transfert du risque



Communication relative aux risques

Objectifs de la communication :

- partager les résultats obtenus grâce à l'appréciation des risques et présenter le plan de traitement des risques;
- éviter ou réduire à la fois l'occurrence et les conséquences des violations de sécurité de l'information dues à un manque de compréhension mutuelle entre les décideurs et les parties prenantes;
- aider au processus de prise de décision;
- obtenir de nouvelles connaissances en sécurité de l'information;
- assurer une coordination avec d'autres parties et prévoir des réponses destinées à réduire les conséquences des incidents pouvant survenir;
- responsabiliser les décideurs et les parties prenantes quant aux risques;
- améliorer la sensibilisation à la sécurité de l'information.

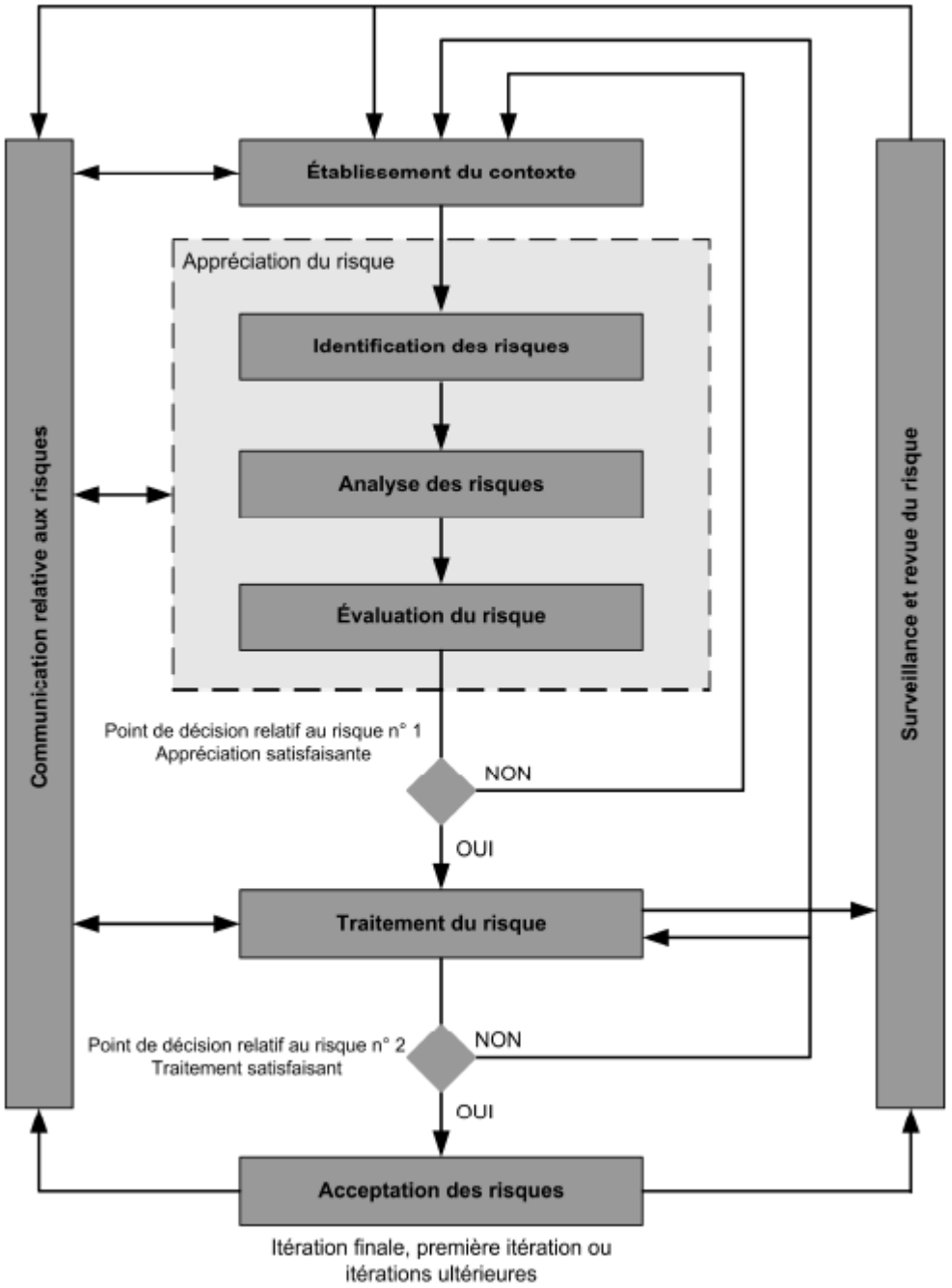
Suivi du risque

- Le monde bouge et les risques évoluent

- Une surveillance et une revue permanents sont nécessaires pour garantir que le contexte, les résultats de l'appréciation et du traitement des risques, ainsi que les plans de gestion, restent adaptés aux circonstances.

Aspects itératifs

- La gestion du risque est un processus itératif



Méthode EBIOS (**E**xpression des **B**esoins de sécurité et **I**dentification des **O**bjectifs **S**écurité)

- Objet
  - EBIOS couvre les aspects sécurité le plus en amont dans le cycle de vie
  - EBIOS conduit à :
    - » L'expression des besoins de sécurité
    - » La spécification des objectifs de sécurité
- Structure (5 modules)
  - Étude du contexte et analyse des enjeux
  - Étude des évènements redoutés
  - Étude des scénarios de menaces
  - Étude de risques
  - Choix des mesures de sécurité

ANSSI
Agence nationale de la sécurité des systèmes d'information

EBIOS

ANSSI | Agence nationale de la sécurité des systèmes d'information

Les bons messages aux décideurs

- Présentation hiérarchique des risques
  arbitrage en connaissance de cause
- Décision face aux enjeux métiers
- Investissement justifié et optimisé
- Fiabilité des processus métiers
- Effort approprié et résultats concrets

La gestion efficace de vos risques SSI

- Implication des métiers
- Cartographie rapide des risques
- Production d'un référentiel cohérent
- Adaptation aux contraintes métiers
- Itération simple quand le SI évolue
- Compatibilité avec ISO 2700x

EBIOS

La méthode de gestion des risques

Une méthode internationale éprouvée

- 15 ans d'expérience
- Traduite en plusieurs langues
- Un réseau d'utilisateur international
- Échange d'expériences au Club EBIOS
- Utilisée par les secteurs privé et public
- Développée et entretenue par l'ANSSI

Pratique

Conseils , exemples et cas concrets

Adaptable

Études optimisées selon les besoins

Outillée

Guides, bases de connaissances, logiciel...

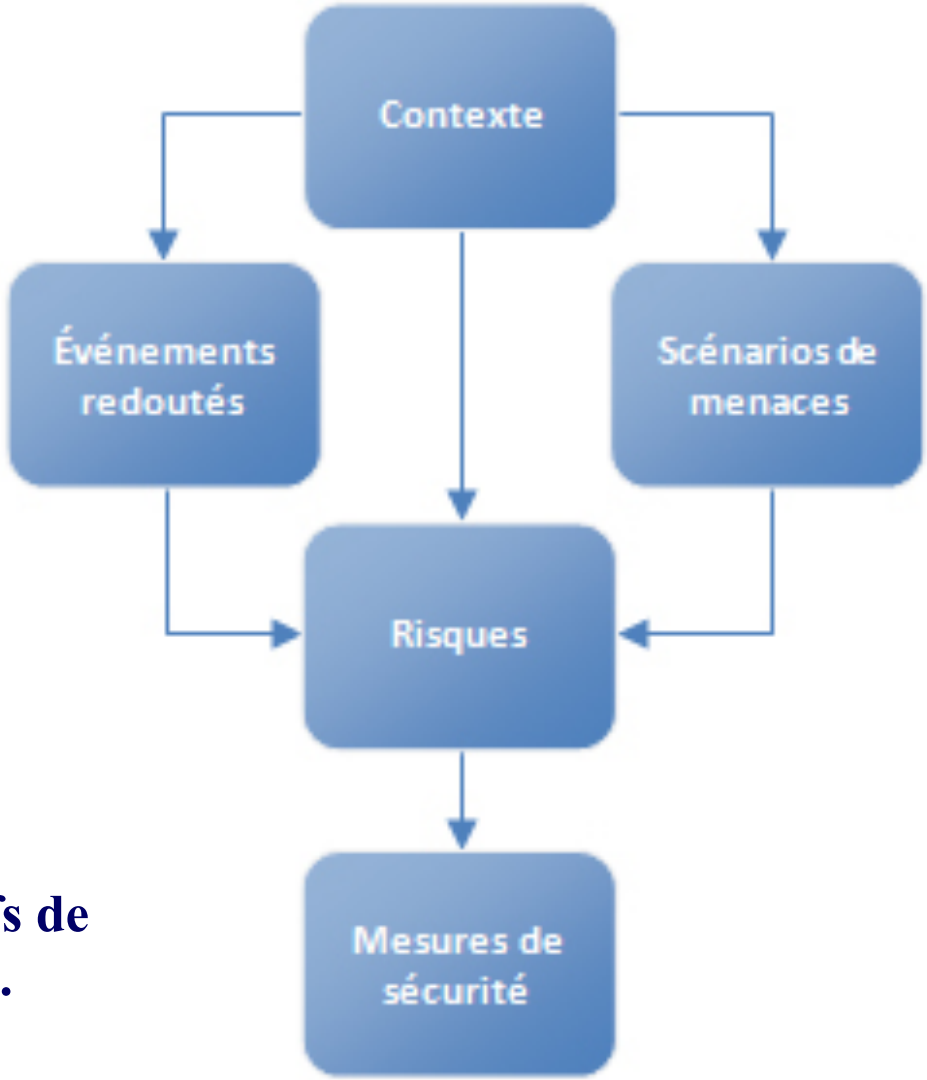
Gratuite

Diffusée sur le site de l'ANSSI

EBIOS – Les étapes de la méthode

ANSSI | Agence nationale de la sécurité des systèmes d'information

1. Etude du contexte
2. Expressions des besoins de sécurité
3. Etude des menaces
4. Identification des objectifs de sécurité
5. Choix des mesures de sécurité



Rédaction de fiches FEROS : Fiche d'Expression Rationnelle des Objectifs de Sécurité (des systèmes d'information).

EBIOS : Étude du contexte et analyse des enjeux

ANSSI Agence nationale de la sécurité des systèmes d'information

- Prise de connaissance du domaine à étudier (environnement physique du système)
- Analyse et formalisation du besoin général
- Enjeux du système pour l'organisme (origine du besoin de sécurité)
  - Poids stratégique du système pour l'organisme
  - Impact de la sécurité du système sur la sécurité globale de l'organisme
  - Pertes maximales que le système peut supporter
- Recensement des informations nécessaires (contraintes,…)

- A l'issue de l'étape, le champ d'investigation de l'étude est clairement défini, les obligations et les différentes contraintes ont été recensées.

EBIOS : Expression des besoins de sécurité

ANSSI Agence nationale de la sécurité des systèmes d'information

- Exigences opérationnelles du système
- Besoins de sécurité associés aux fonctions et données
- Critères : Disponibilité / Intégrité / Confidentialité + autres éventuels (preuve, auditabilité).

- Les besoins de sécurité sont exprimés par les utilisateurs et les responsables du système étudié.
- Ils représentent leurs exigences en matière de sécurité.

EBIOS : Étude des menaces

ANSSI Agence nationale de la sécurité des systèmes d'information

- 4 étapes :
  - Sélection des menaces jugées pertinentes dans le contexte du système
    - » Menaces suffisamment génériques et de haut niveau pour être exhaustives
    - » Caractérisées par leur impact direct sur le système
  - Détermination des vulnérabilités spécifiques au système
    - » Mettent en évidence les possibilités de leur réalisation : **faisabilité** / **facilité de réalisation** (intentionnelle) ou **probabilité** (accidentelle)
  - Identification des risques
    - » Par association des menaces et des vulnérabilités
    - » Risques mis en évidence spécifiques au système utilisé
    - » Caractérisation des risques indépendante de la sensibilité des informations ou des fonctions
  - Confrontation des risques aux besoins de sécurité

EBIOS : Identification des objectifs de sécurité

ANSSI Agence nationale de la sécurité des systèmes d'information

- Prise en compte des contraintes (notamment réglementaires) et de l'application de la politique de sécurité interne
- Les objectifs de sécurité sont associés aux activités du système
- Ils comprennent également l'ensemble des mesures non-techniques, cohérentes avec les mesures techniques.

EBIOS : De quoi dispose-t-on ?

ANSSI Agence nationale de la sécurité des systèmes d'information

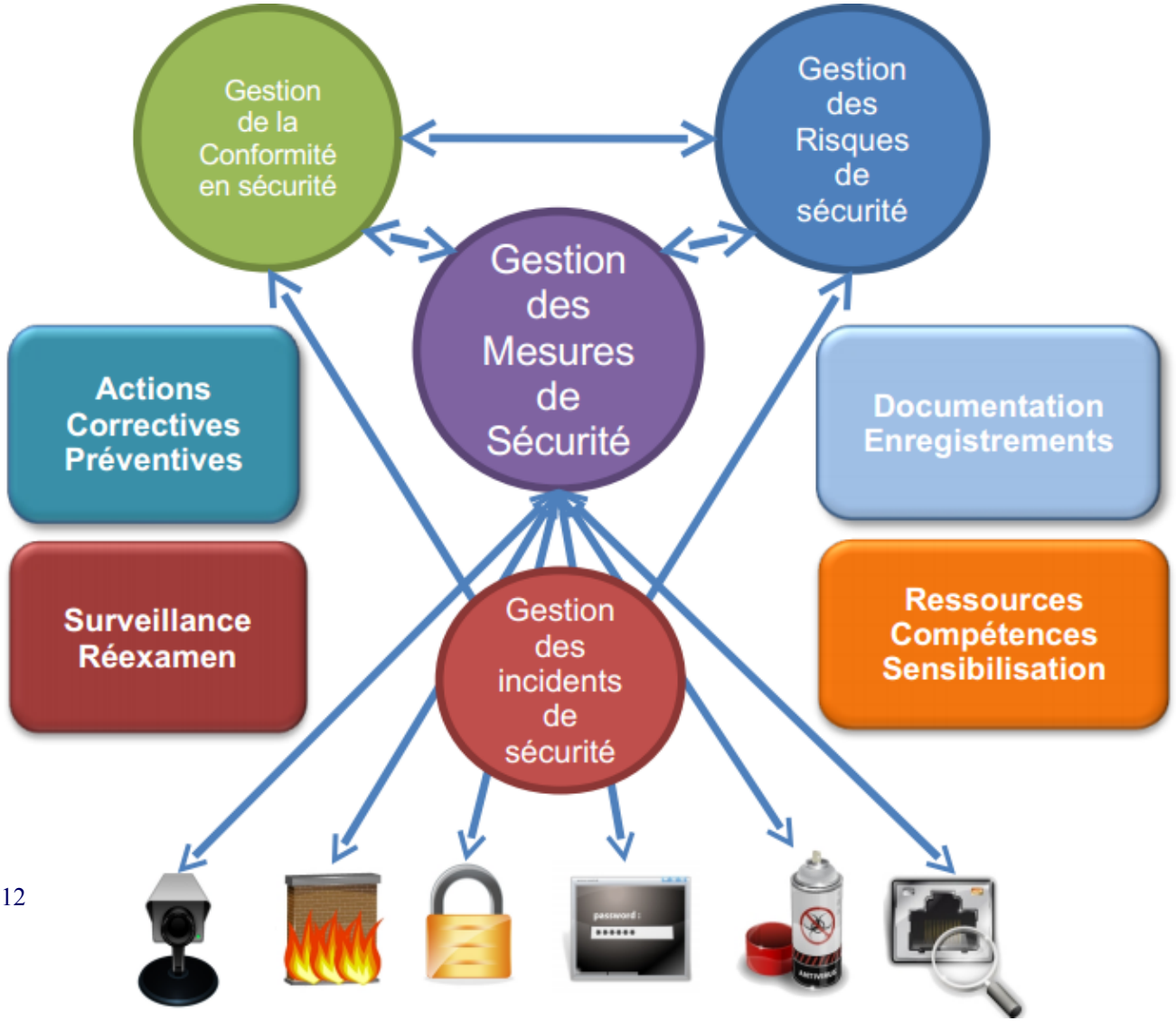
- Le guide EBIOS comprend les quatre parties suivantes :
  - La démarche : ce que le concepteur doit faire
    - » Répertoire des étapes et activités
    - » Synoptiques
  - Les techniques : comment le concepteur doit le faire,
  - Les outils : avec quoi le concepteur doit le faire
    - » Bases de connaissance :
      - Les menaces génériques
      - Les vulnérabilités spécifiques
      - Les classes de fonctionnalités
    - » Répertoire des fiches spécimen
  - Le glossaire

Exemple : Analyse de vulnérabilités

ANSSI Agence nationale de la sécurité des systèmes d'information

Menace	Libellé de la menace	Vulnérabilités	P
M11	PERTE D'ALIMENTATION ENERGETIQUE	• Peu de dispositifs de protection contre les coupures ou variations électriques du réseau EDF ou des groupes électrogènes. • Faiblesse des caractéristiques du système électrique de secours.	2
M12	PERTE DES MOYENS DE TELECOMMNICATION	• Problème de propagation des ondes électromagnétiques (propagation troposphérique) • Facilité d'accès aux boîtiers d'E/S des câbles au niveau des locaux • Défauts d'exploitation du réseau téléphonique ou TD interne • Dysfonctionnement des réseaux externes (phonie, TD...)	2
M13	RAYONNEMENTS ELECTROMAGNETIQUES	• Matériel sensible aux rayonnements électromagnétiques • Câbles inter locaux non protégés; bâtiments éloignés les uns des autres	2
M17	ESPIONNAGE A DISTANCE	• Absence d'organisation de sécurité • Contrôle de périmètre de zone facilement contournable	2
M18	ECOUTE PASSIVE	• Facilité de capter les transmissions à l'extérieur du site : distance de sécurité insuffisante • Matériel comprenant des éléments permettant l'écoute passive • câblage, prises de connexion gérés irrégulièrement	2
M19	VOL DE SUPPORTS OU DE DOCUMENTS	Contrôle d'accès des personnels aux matériels et aux documents rendu difficile en raison de : • la facilité de pénétrer dans les locaux • l'hétérogénéité des personnels (personnels de la société ou du groupe, prestataires informatiques, autres prestataires) • l'absence de coffre-fort • l'absence d'organisation sécuritaire réelle	3

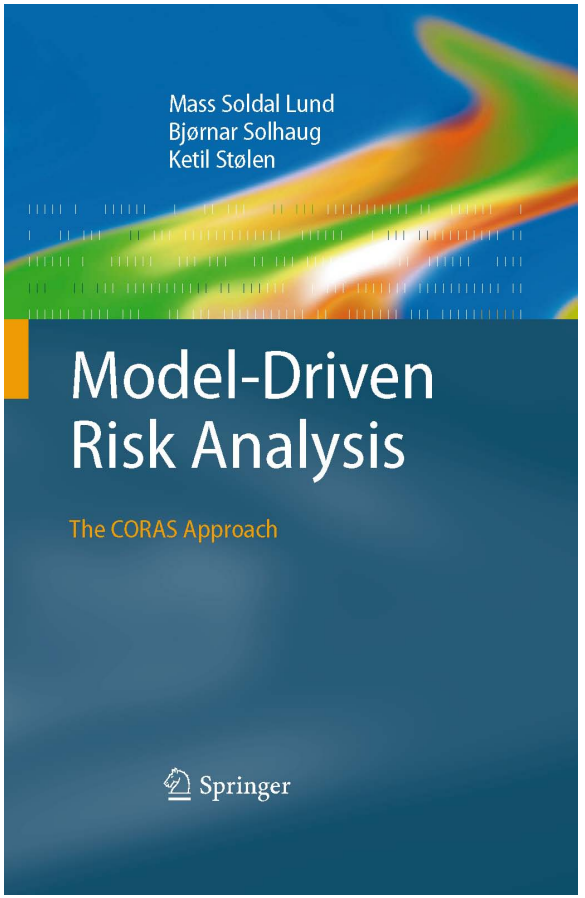
Gestion de la sécurité du Système d'Information - Synthèse



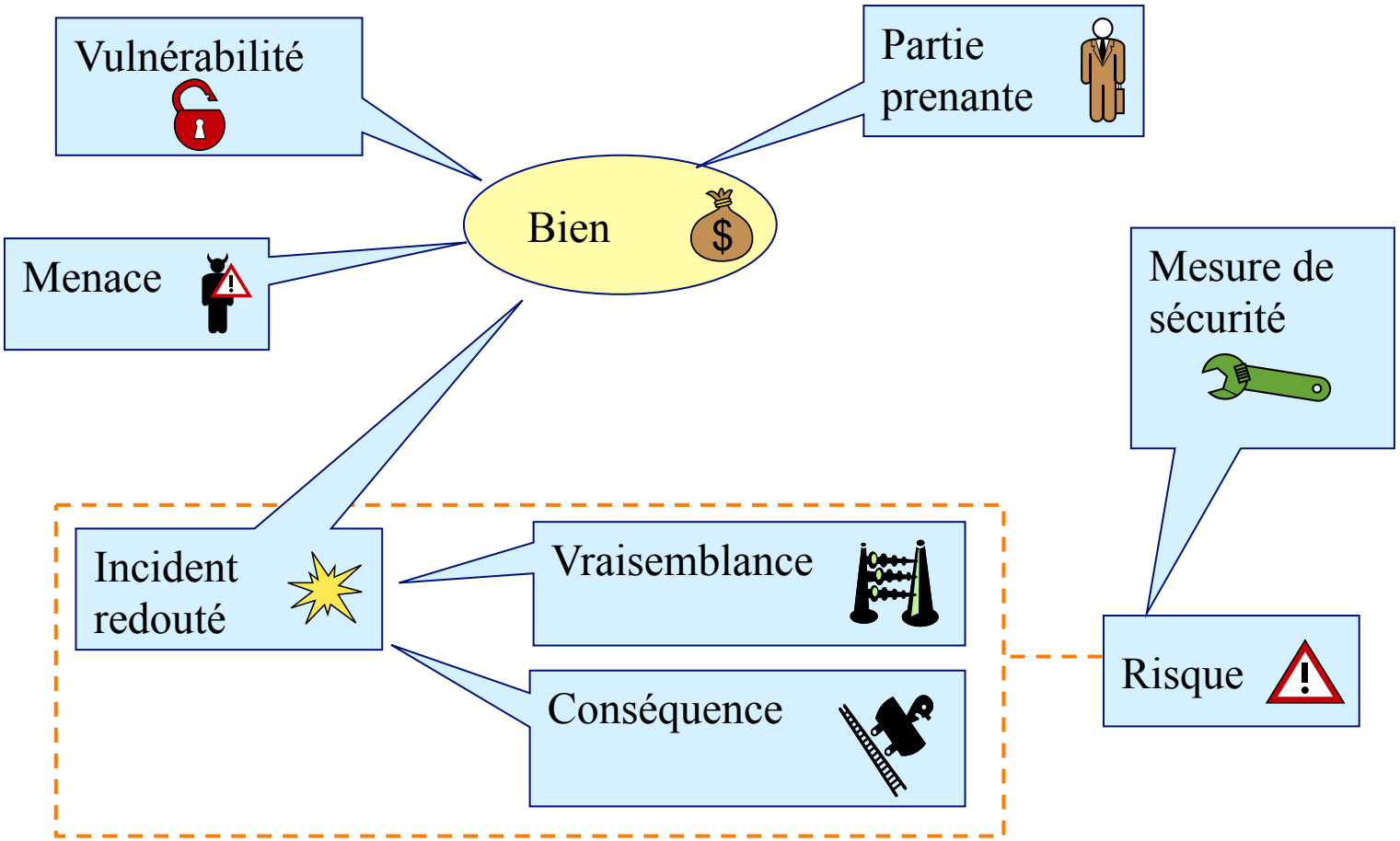
Source : Cabinet Hervé Schauer Consultants 2012

CORAS – Modélisation graphique de l'analyse de risque

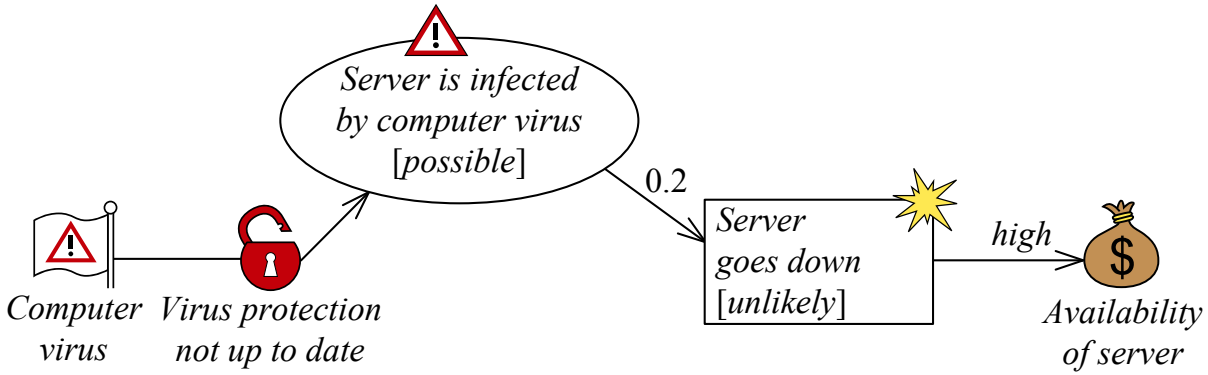
- Développé par le SINTEF – Centre de recherche en Norvège
- Vise la modélisation par diagrammes de l'analyse de risques
- Supporté par un éditeur sous Eclipse en libre accès



Concepts principaux



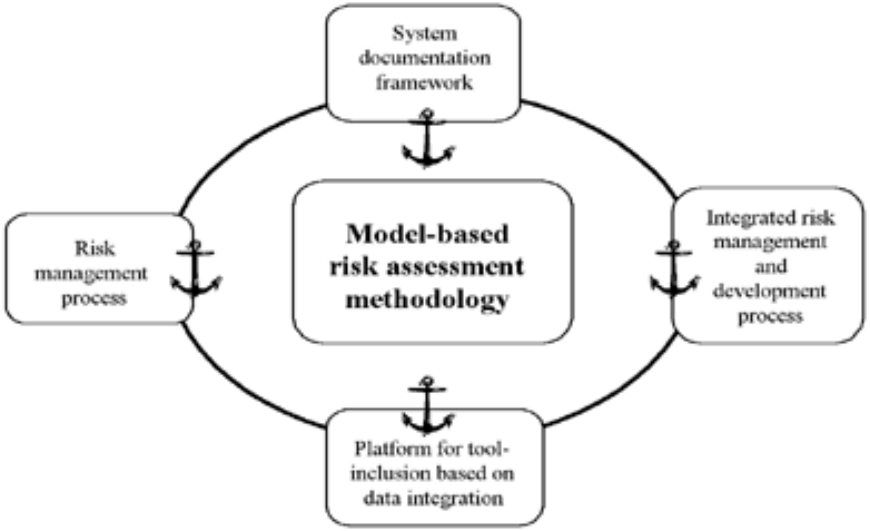
Interprétation d'un diagramme CORAS - Exemple



- Un virus est une **menace non humaine**
- La protection anti-virale pas à jour est une **vulnérabilité**
- Le serveur qui est infecté par un virus est un **scénario de menace** avec une probabilité d'arrivée (0.2)
- La mise hors service du serveur est un **événement redouté**
- La disponibilité du serveur est un **bien** à protéger

CORAS – Modélisation de l'analyse de risques

- Plusieurs types de diagrammes
  - Asset diagrams (Biens à protéger)
  - Threat diagrams (Menaces identifiées)
  - Risk diagrams (Risques identifiés)
  - Treatment diagrams (Mesures de sécurité)
- Permet de prendre en compte différents aspects de l'analyse de risque de sécurité



Exemple: Diagramme de menaces (threat)

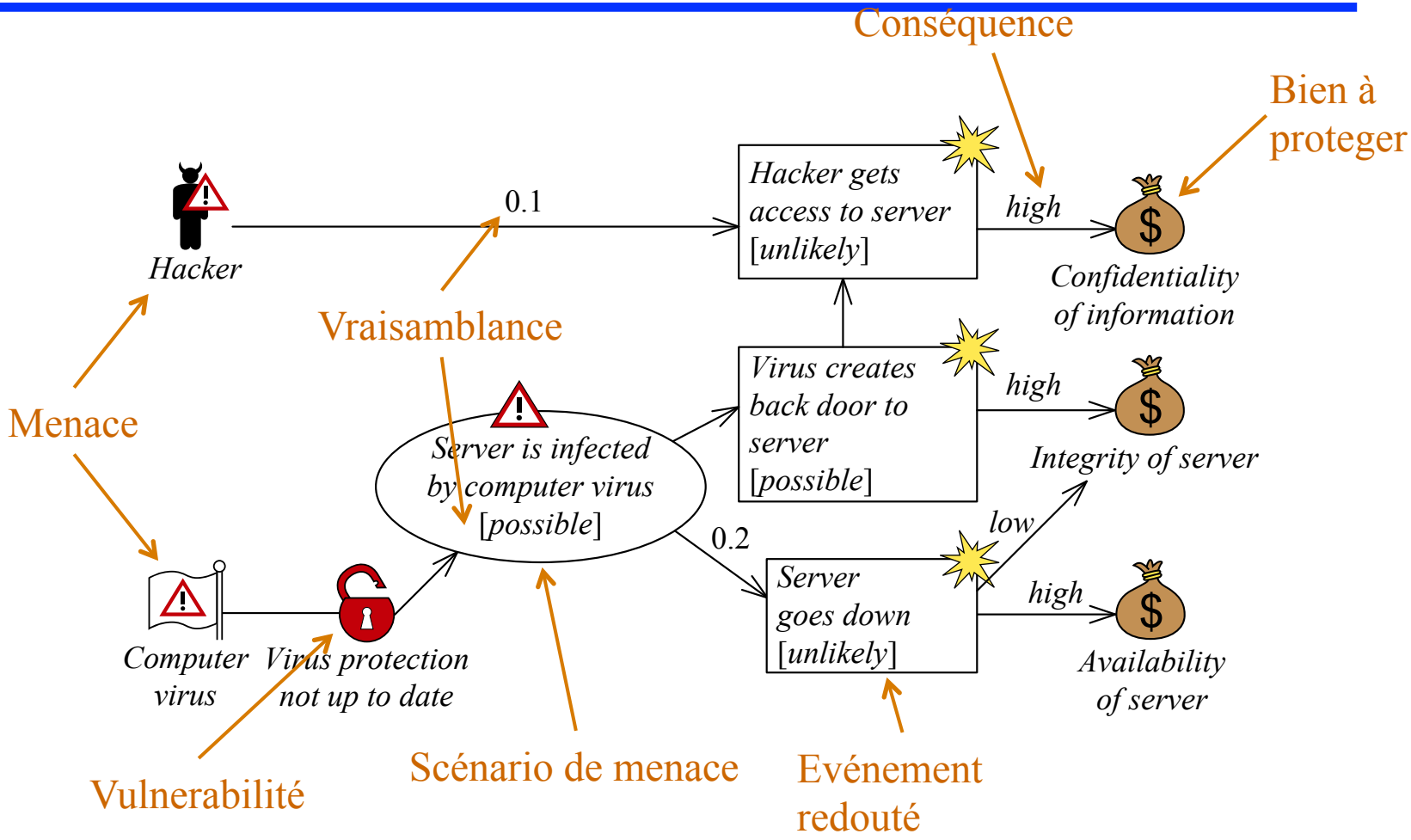
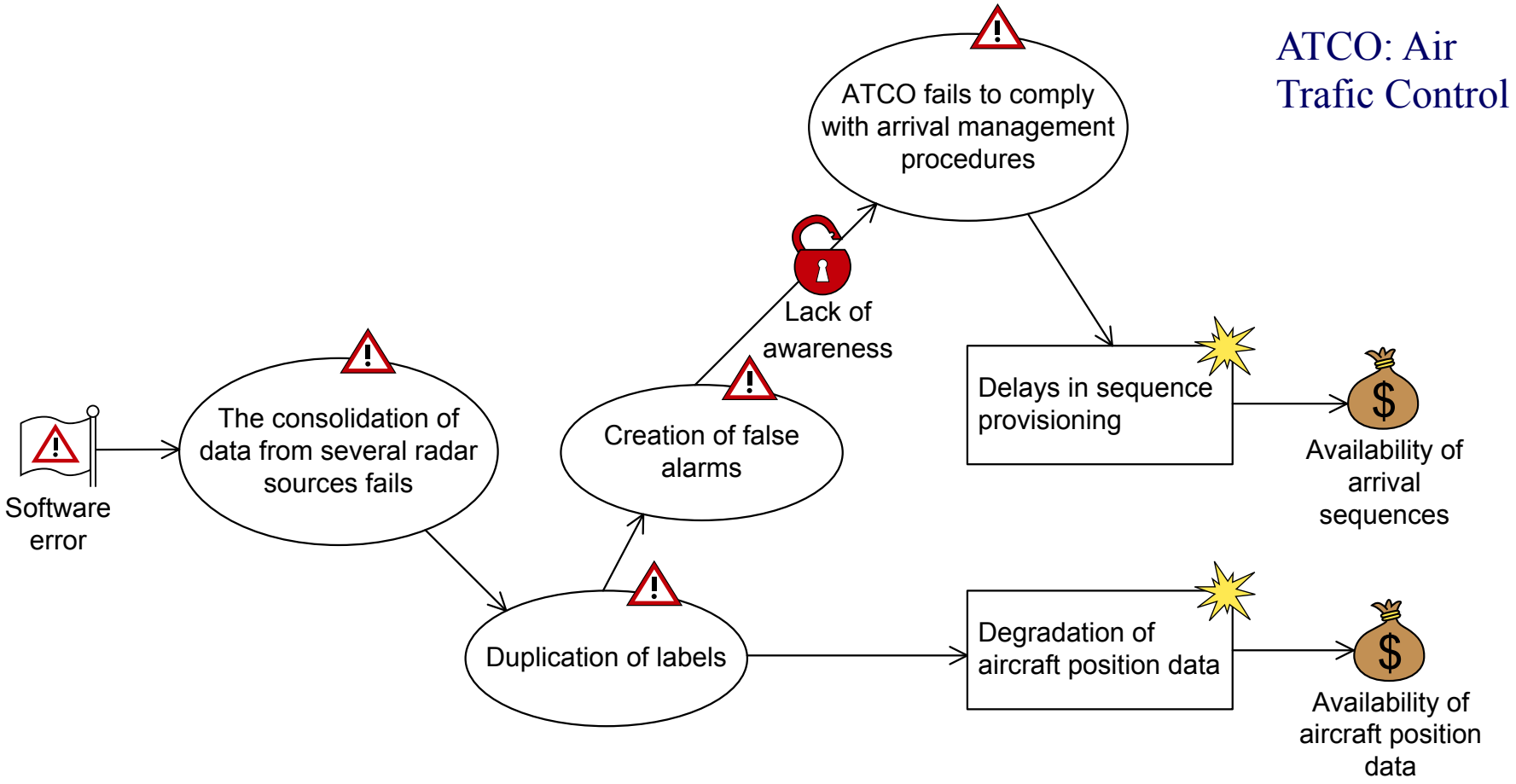


Diagramme de menaces en CORAS – Exemple de système de contrôle de trafic aérien



Sommaire du chapitre II.2

- Analyse de risques et définition d'une politique de sécurité
  - Analyse de risque – ISO 27005
  - La méthode EBIOS de l'ANSSI
  - La modélisation CORAS

- Test de sécurité
  - Types de test

Types de test de sécurité

- Test d'intrusion
- Test de sécurité applicatives / Test de vulnérabilité
- Audit de sécurité

Tests d'intrusion (ou test de pénétratiion ou encore *pentesting*)

- Test d'intrusion
  - Mon système d'information est-il vulnérable depuis Internet ?
  - Mon réseau interne (LAN) est-il sécurisé ? Jusqu'à quel point ?
  - Mon site (ou applicatif) internet est-il sécurisé ?
  - Le nouvel applicatif de l'entreprise est-il vulnérable ou correctement sécurisé ?
- L'analyse peut se réaliser selon trois cas :
  - Le testeur se met dans la peau d'un attaquant potentiel, et ne possède aucune information (black-box testing) ;
  - Le testeur possède un nombre limité d'informations (grey-box testing);
  - Le testeur possède les informations dont il a besoin (white-box testing).

Test de sécurité applicative / Test de vulnérabilité

- Tests applicatifs fondés sur l'analyse des vulnérabilités potentielles au niveau des différentes couches : applications, base de données, serveur, réseau.
- Test des fonctions de sécurité (authentification)
- Peut être réalisé en mode Black-box, Grey-box ou White-box.
- Exemples de tests de vulnérabilité:
  - XSS – Cross-site scripting
  - CSRF - Cross-site request forgery
  - Injection SQL
  - Cookie/ Vol de session

Audit de sécurité

- Typiquement sur la base ISO 27005
- Peut s'appuyer sur les méthodes MEHARI (CLUSIF) ou EBIOS (ANSSI)
- Objectif : analyse partielle ou complète de la sécurité du Système d'information pour analyser les vulnérabilités et mettre en place des mesures de sécurité
- Souvent sous-traité à une entreprise spécialisée
- Peut mettre en œuvre :
  - des tests d'intrusion
  - l'audit du code source
  - l'audit du réseau