

Organisation de la Sécurité et Implémentation dans l'Entreprise





Organisation de la sécurité et ses métiers dans l'entreprise

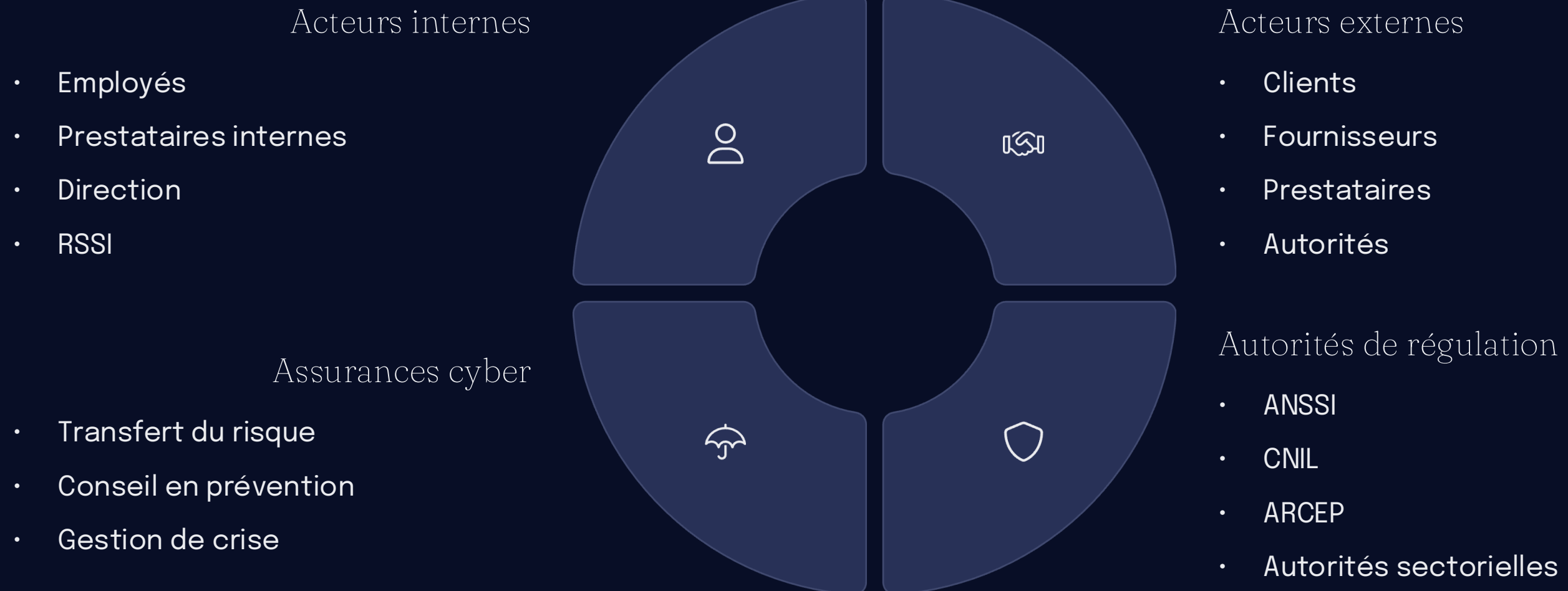
La sécurité de l'information implique de nombreux acteurs, chacun ayant des rôles et responsabilités spécifiques dans l'écosystème de l'entreprise.

Une organisation efficace de la sécurité nécessite une compréhension claire des différents métiers et de leur interaction au sein de l'entreprise.

Acteurs et responsabilités

Cartographie des acteurs

La sécurité de l'information implique de nombreux acteurs, chacun ayant des rôles et responsabilités spécifiques dans l'écosystème de l'entreprise.



Acteurs externes

Clients

Rôle dans la sécurité :

- Utilisateurs finaux des services/produits
- Détenteurs de données personnelles
- Demandeurs d'exigences de sécurité

Responsabilités :

- Respect des conditions d'utilisation
- Protection de leurs accès (identifiants, mots de passe)
- Signalement des incidents suspectés



Interactions :

- Communication des exigences de sécurité
- Notification en cas de violation de données
- Audits de conformité

Fournisseurs et prestataires



Fournisseurs de services cloud

Proposent des services IaaS, PaaS et SaaS avec des responsabilités spécifiques en matière de sécurité selon le modèle de service.



Prestataires de sécurité

Offrent des services comme le SOC externalisé, les tests d'intrusion et l'audit de sécurité pour renforcer la posture de sécurité.



Intégrateurs systèmes

Assurent l'implémentation et l'intégration des solutions de sécurité dans l'infrastructure existante.



Fournisseurs de matériel et logiciels

Développent et maintiennent les outils et solutions de sécurité utilisés par l'entreprise.

Gestion des risques fournisseurs

- Due diligence avant contractualisation
- Clauses de sécurité dans les contrats
- Audits réguliers
- Plans de continuité en cas de défaillance

Assurances cyber

Rôle

- Transfert du risque financier
- Conseil en prévention
- Gestion de crise

Types de couvertures

- Dommages directs (pertes de données, interruption d'activité)
- Responsabilité civile (violation de données personnelles)
- Frais de gestion de crise
- Cyber-extorsion (ransomware)



Obligations

- Déclaration exacte des risques
- Mise en place de mesures de sécurité minimales
- Notification rapide des sinistres

Autorités de régulation



ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information - Autorité nationale en matière de cybersécurité, elle définit les standards et accompagne les organisations.



CNIL

Commission Nationale de l'Informatique et des Libertés - Veille à la protection des données personnelles et au respect du RGPD.



ARCEP

Autorité de Régulation des Communications Électroniques et des Postes - Régule les télécommunications et les services postaux.



Autorités sectorielles

ACPR pour la finance, ARS pour la santé - Définissent des exigences spécifiques à leur secteur d'activité.

Interactions

- Déclarations obligatoires
- Audits de conformité
- Sanctions en cas de manquement

Acteurs internes

Employés

Catégories :

- Utilisateurs standards : Usage quotidien des SI
- Utilisateurs privilégiés : Administrateurs, développeurs
- Personnel sensible : RH, finance, direction

Responsabilités communes :

- Respect de la charte informatique
- Protection des informations confidentielles
- Utilisation appropriée des ressources
- Signalement des incidents



Sensibilisation :

- Formation initiale à l'embauche
- Campagnes de sensibilisation régulières
- Tests de phishing
- Exercices de crise

Prestataires internes

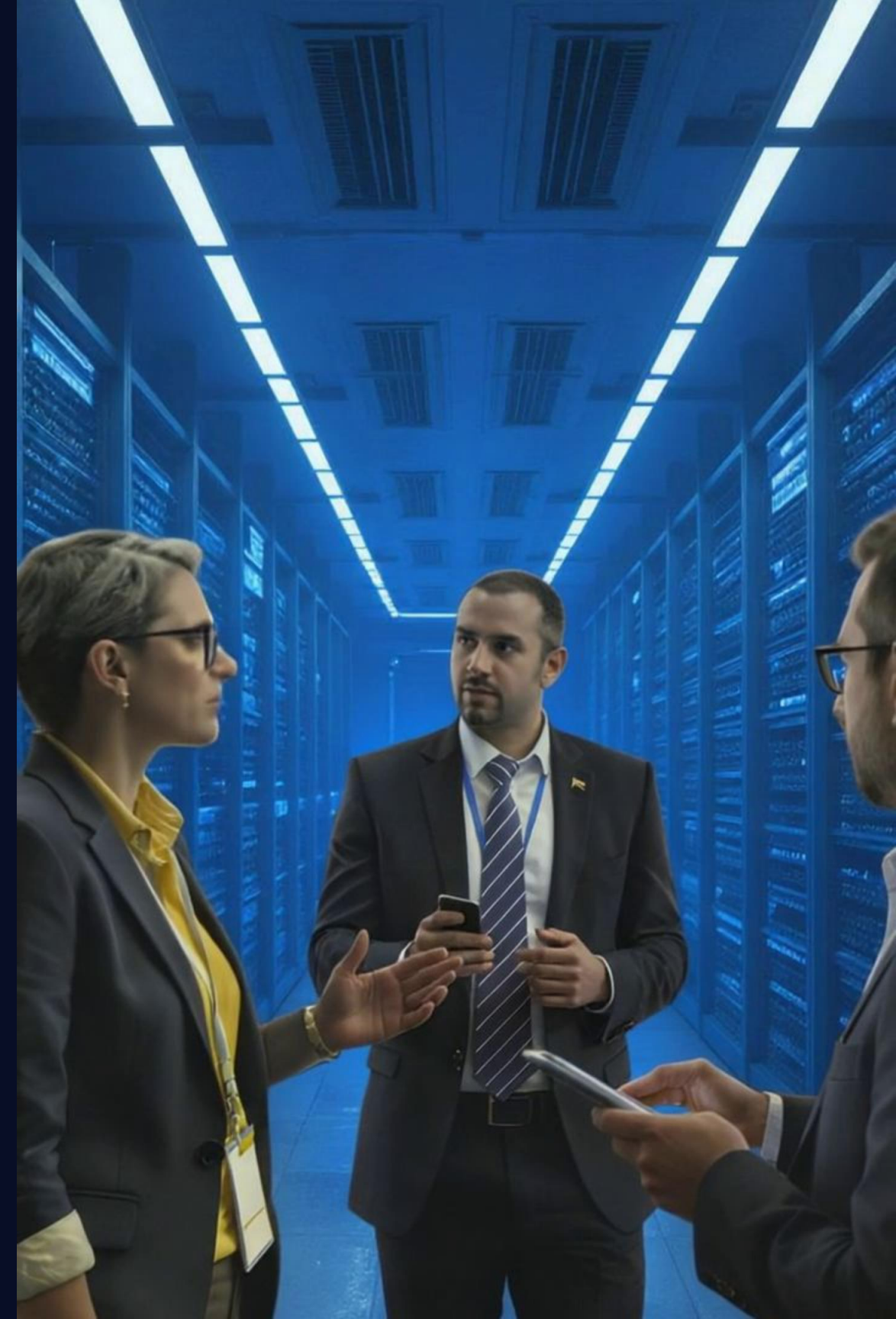
1 Types de prestataires internes

- Consultants et intérimaires
- Personnel de maintenance
- Stagiaires et alternants

2 Spécificités de gestion

- Accès temporaires et limités
- Clauses de confidentialité renforcées
- Supervision accrue
- Retrait des accès en fin de mission

Les prestataires internes représentent un risque particulier pour la sécurité de l'information car ils ont souvent besoin d'accéder à des systèmes sensibles tout en étant temporairement rattachés à l'organisation. Une gestion rigoureuse de leurs accès et de leurs responsabilités est essentielle.



Le RSSI (Responsable de la Sécurité des Systèmes d'Information)

Définition et positionnement

Le RSSI est le garant de la sécurité des systèmes d'information de l'organisation. Il définit, met en œuvre et maintient la politique de sécurité.

Positionnement organisationnel :

- Rattachement à la Direction Générale : Indépendance et vision transverse
- Rattachement à la DSI : Proximité technique mais risque de conflit d'intérêts
- Rattachement au Risk Management : Approche globale des risques



Missions principales du RSSI



Stratégiques

- Définition de la politique de sécurité (PSSI)
- Alignement avec la stratégie business
- Gestion du budget sécurité



Opérationnelles

- Gestion des incidents de sécurité
- Coordination des projets sécurité
- Veille sur les menaces



Gouvernance

- Reporting à la direction
- Relations avec les autorités
- Gestion de la conformité



Support

- Sensibilisation et formation
- Conseil aux métiers
- Expertise technique



Relations avec les directions métiers

DSI (Direction des Systèmes d'Information)

Nature de la relation :

- Collaboration étroite mais indépendante
- Le RSSI challenge les choix techniques
- La DSI implémente les mesures de sécurité

Points de collaboration :

- Architecture sécurisée
- Gestion des vulnérabilités
- Plans de continuité IT
- Projets d'infrastructure



Points d'attention :

- Équilibre entre sécurité et performance
- Gestion des urgences opérationnelles
- Budget et ressources partagés

Relations avec les autres directions



DRH (Direction des Ressources Humaines)

- Recrutement : Vérification des antécédents
- Formation : Plans de sensibilisation
- Sanctions : Violations de la politique de sécurité
- Départs : Retrait des accès et confidentialité



DAF (Direction Administrative et Financière)

- Budget : Justification des investissements sécurité
- ROI : Mesure de l'efficacité des contrôles
- Assurances : Négociation des polices cyber
- Conformité : Respect des obligations légales



Direction Marketing/Communication

- Protection de l'image de marque
- Gestion de crise : Communication externe
- Données clients : Conformité RGPD
- Présence digitale : Sécurité des sites web



Direction juridique

- Conformité réglementaire
- Gestion des contrats fournisseurs
- Litiges et contentieux
- Protection de la propriété intellectuelle



Gouvernance de la sécurité

Définition et principes

Gouvernance de la sécurité : Ensemble des structures, processus et mécanismes permettant d'assurer que la sécurité de l'information est gérée et alignée avec les objectifs de l'organisation.

Structures de gouvernance

Comité de sécurité

Composition : RSSI (animateur), Représentants des directions métiers, DSI, Risk Manager, DPO

Missions : Validation de la politique de sécurité, Arbitrage des priorités, Suivi des indicateurs, Décisions d'investissement

Fréquence : Mensuelle ou trimestrielle

Comité de crise

Activation : En cas d'incident majeur

Composition : Direction générale, RSSI, Directions impactées, Communication, Juridique

Processus de gestion des incidents

Planification et préparation

- Politique de gestion des incidents
- Procédures documentées
- Formation des équipes

Détection et reporting

- Mécanismes de détection
- Canaux de reporting
- Classification initiale

Évaluation et décision

- Analyse de l'incident
- Catégorisation
- Priorisation

Réponse

- Confinement
- Éradication
- Récupération

Apprentissage

- Analyse post-incident
- Amélioration des processus
- Partage d'expérience

Implémentation de la sécurité

Volet organisationnel : L'analyse du risque

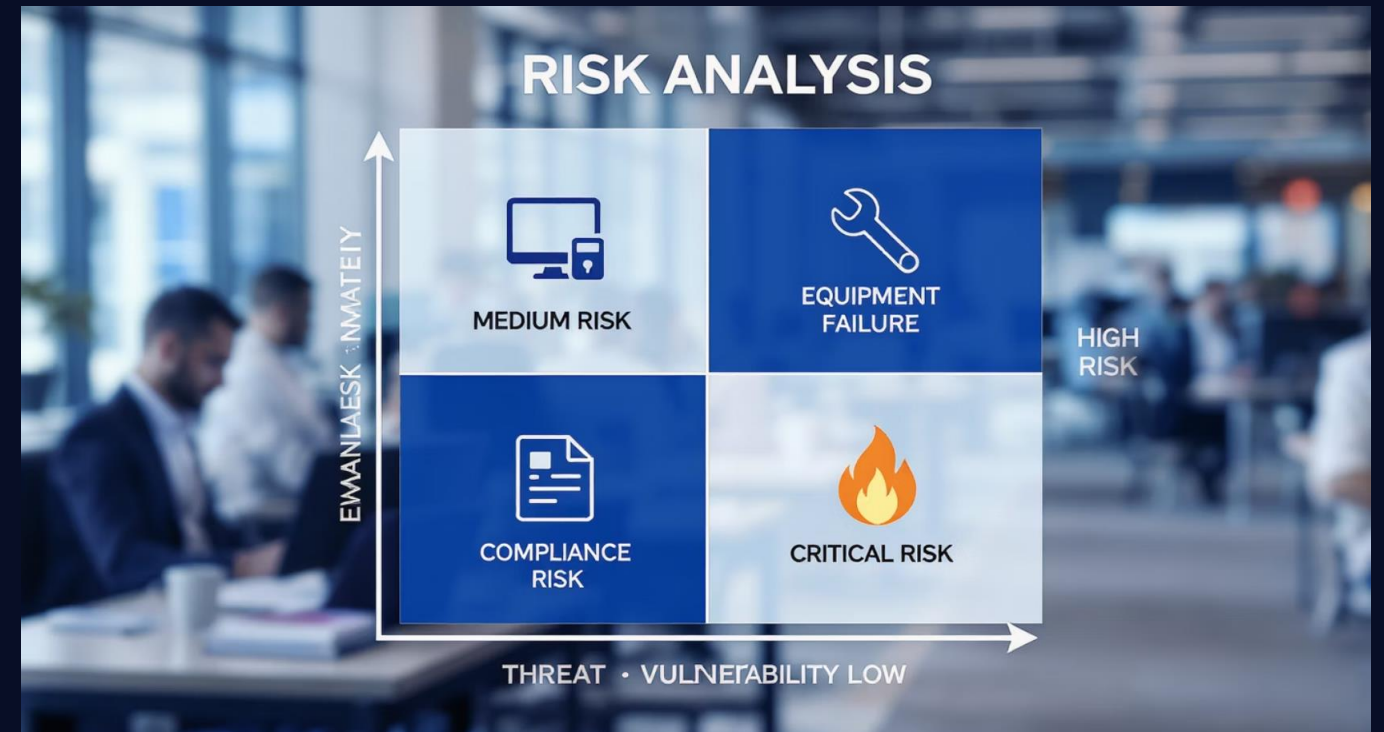
Définition et concepts fondamentaux

Le risque en sécurité de l'information

Définition : Le risque est la possibilité qu'une menace exploite une vulnérabilité d'un actif et cause ainsi un préjudice à l'organisation.

Formule classique :

Risque = Menace × Vulnérabilité × Impact



Composantes :

- **Actif** : Tout élément ayant de la valeur pour l'organisation
- **Menace** : Cause potentielle d'un incident non désiré
- **Vulnérabilité** : Faiblesse d'un actif
- **Impact** : Conséquence sur l'organisation

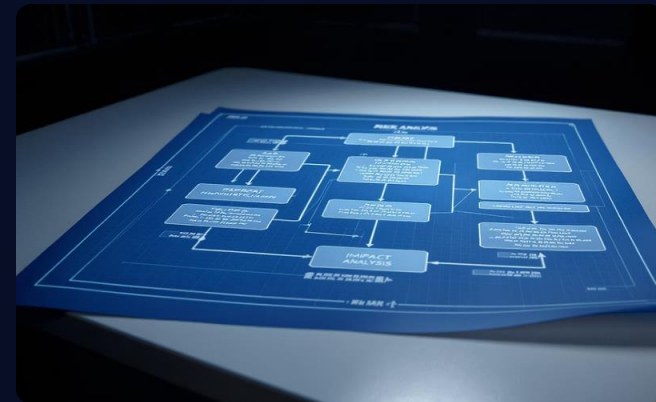
Panorama des méthodes d'analyse de risque



EBIOS Risk Manager

Origine : Méthode française développée par l'ANSSI

Caractéristiques : Approche par scénarios, Focus sur les risques intentionnels, Intégration de la menace cyber



MEHARI

Origine : Méthode du CLUSIF (Club de la Sécurité de l'Information Français)

Principes : Évaluation de la gravité et de la potentialité, Base de connaissances de scénarios, Questionnaires d'audit détaillés



ISO 27005

Nature : Norme internationale pour la gestion des risques

Processus : Établissement du contexte, Appréciation du risque, Traitement du risque, Acceptation du risque, Communication et concertation, Surveillance et réexamen



OCTAVE

Origine : Carnegie Mellon University

Approche : Auto-évaluation par les équipes, Focus sur les actifs informationnels critiques, Workshops collaboratifs

Processus d'analyse de risque

Établissement du contexte

- Contexte externe : réglementaire, menaces sectorielles
- Contexte interne : organisation, objectifs métiers
- Critères de risque : échelles d'impact, niveaux de vraisemblance

Identification des vulnérabilités

- Types : techniques, organisationnelles, physiques
- Sources d'information : audits, tests d'intrusion, retours d'expérience



Identification des actifs

- Actifs primaires : processus métiers et informations
- Actifs supports : systèmes, réseaux, locaux, personnel
- Valorisation : Confidentialité, Intégrité, Disponibilité, Preuve

Analyse des menaces

- Sources de menaces : humaines, environnementales, techniques
- Caractérisation : motivation, capacités, opportunités

De l'analyse de risque à la PSSI et schéma de sécurité

La PSSI (Politique de Sécurité des Systèmes d'Information)

Définition et objectifs

Définition : Document de référence définissant la stratégie de sécurité de l'organisation, les principes, les règles et les responsabilités.

Objectifs :

- Formaliser l'engagement de la direction
- Définir le cadre de gouvernance
- Établir les principes directeurs
- Clarifier les responsabilités



Structure type d'une PSSI



Préambule



- Contexte et enjeux
- Périmètre d'application
- Engagement de la direction

Organisation de la sécurité



- Rôles et responsabilités
- Instances de gouvernance
- Processus de décision

Principes de sécurité



- Classification de l'information
- Contrôle d'accès
- Protection des données
- Continuité d'activité

Règles de sécurité



- Utilisation des ressources
- Gestion des accès
- Protection physique
- Développement sécurisé

Gestion des incidents



- Détection et signalement
- Traitement et escalade
- Communication de crise

Conformité



- Exigences légales et réglementaires
- Audits et contrôles
- Sanctions

Processus d'élaboration de la PSSI

Initialisation

- Constitution du comité de pilotage
- Définition du périmètre
- Planning et ressources

État des lieux

- Analyse de l'existant
- Identification des écarts
- Benchmark sectoriel

Rédaction

- Ateliers avec les métiers
- Rédaction collaborative
- Validation juridique

Validation

- Revue par les parties prenantes
- Approbation direction
- Communication officielle

Déploiement

- Plan de communication
- Formation des acteurs
- Mise en œuvre progressive

Le schéma directeur de sécurité

Définition

Schéma directeur : Plan pluriannuel (3-5 ans) traduisant la PSSI en projets et actions concrètes.

Composantes

1. **Vision et objectifs stratégiques** : Alignement avec la stratégie d'entreprise, Objectifs de maturité, Cibles de conformité
2. **État des lieux détaillé** : Cartographie des risques actuels, Niveau de maturité par domaine, Écarts de conformité
3. **Feuille de route** : Projets prioritaires, Planning de mise en œuvre, Jalons et livrables



1. **Architecture cible** : Architecture de sécurité, Standards techniques, Patterns de sécurité
2. **Plan de ressources** : Budget prévisionnel, Besoins en compétences, Organisation cible

Déclinaison opérationnelle



Politiques sectorielles

- Politique de gestion des accès
- Politique de sauvegarde
- Politique de classification
- Politique d'usage du SI



Procédures et modes opératoires

- Procédure de création de compte
- Procédure de gestion des incidents
- Guide de développement sécurisé
- Check-lists de sécurité



Standards et référentiels

- Standards de configuration
- Catalogues de mesures
- Matrices de contrôle
- Guides de bonnes pratiques



Approfondissement d'une méthode d'analyse de risque et FEROS

La démarche d'homologation

Contexte réglementaire

Référentiel : Instruction Générale Interministérielle n°300 (IGI 300) et Référentiel Général de Sécurité (RGS)

Objectif : Attester que le système d'information présente un niveau de sécurité adapté aux enjeux et conforme aux exigences.

Périmètre :

- Systèmes traitant d'informations sensibles
- SI en interface avec des tiers
- Applications critiques



La fiche FEROS

Définition

FEROS : Fiche d'Expression Rationnelle des Objectifs de Sécurité

Rôle : Document de synthèse présentant l'analyse de risque et les mesures de sécurité retenues pour l'homologation.

Structure détaillée de la fiche FEROS

1

Présentation du système

- Nom et description du SI
- Finalités et enjeux métiers
- Périmètre fonctionnel et technique
- Acteurs et utilisateurs
- Interfaces avec d'autres SI

2

Analyse du contexte

- Contexte réglementaire applicable
- Contraintes spécifiques
- Durée de vie prévue
- Budget et ressources

3

Biens essentiels et analyse des menaces

- Tableau des biens essentiels avec besoins DICT
- Sources de menaces identifiées
- Scénarios de menace retenus
- Évaluation de la vraisemblance



Suite de la structure FEROS

1 Analyse des vulnérabilités

- Vulnérabilités techniques
- Vulnérabilités organisationnelles
- Vulnérabilités physiques

2 Analyse des risques

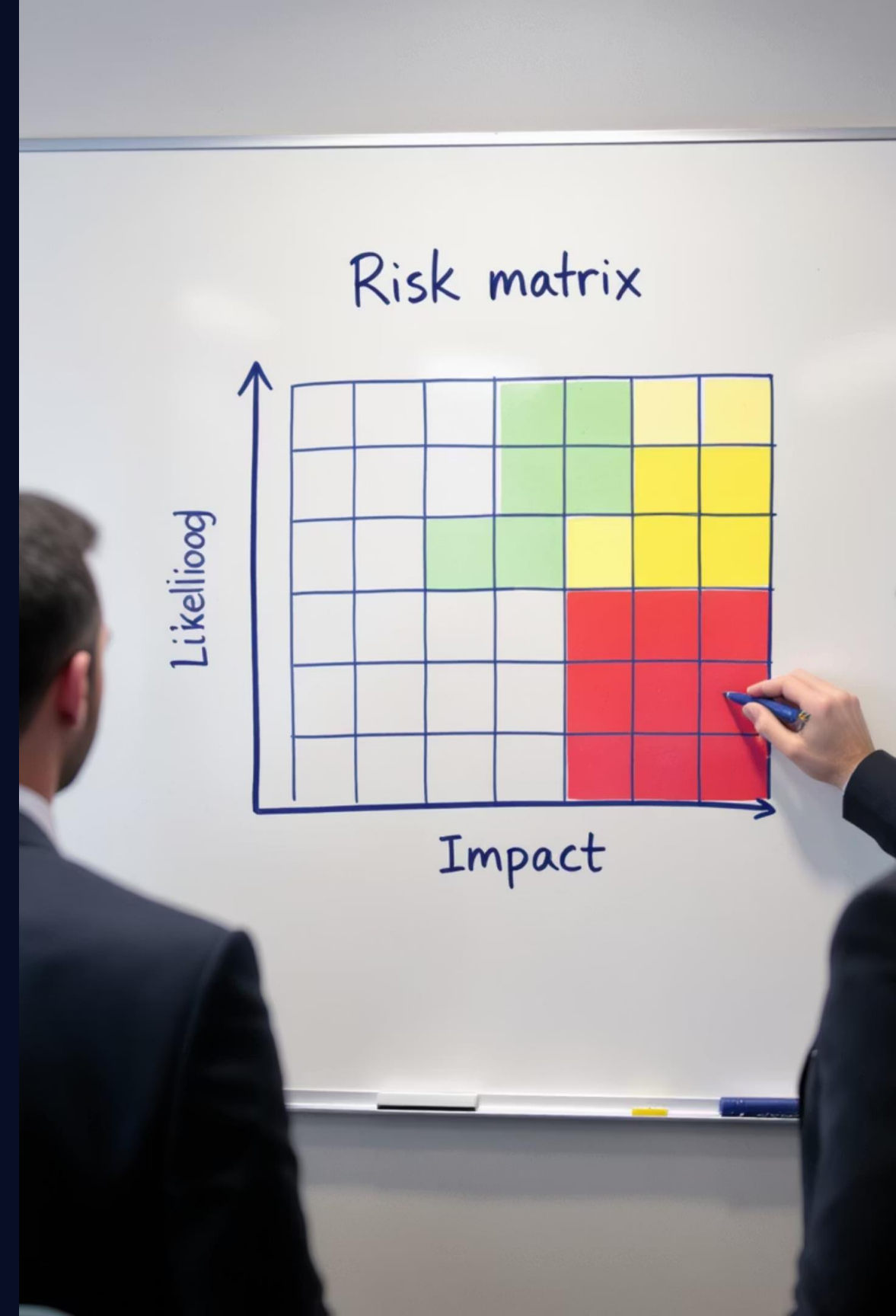
Matrice des risques avec impact, vraisemblance et niveau

3 Mesures de sécurité

- Mesures de prévention
- Mesures de protection
- Mesures de détection
- Mesures de réaction

4 Risques résiduels et plan d'action

- Risques acceptés
- Risques transférés
- Plan de traitement différé
- Actions, responsables et échéances



Déploiement : projets de sécurité, produits et services

Typologie des projets de sécurité



Projets d'infrastructure

- Déploiement d'un SOC
- Mise en place d'une PKI
- Implémentation d'un SIEM
- Architecture Zero Trust



Projets de conformité

- Exigences réglementaires (RGPD, NIS, LPM)
- Certifications (ISO 27001, HDS, PCI-DSS)
- Exigences clients/partenaires



Projets de transformation

- Digitalisation
- Cloud migration
- DevSecOps
- Télétravail massif

Maintien en condition de sécurité et SECOPS

Le maintien en condition de sécurité (MCS)

Définition : Ensemble des activités permettant de maintenir le niveau de sécurité face à l'évolution des menaces et de l'environnement.

Enjeux :

- Adaptation continue aux menaces
- Gestion de l'obsolescence
- Maintien de la conformité
- Optimisation des ressources

Les SECOPS (Security Operations)

Définition : Équipe opérationnelle en charge de la surveillance, détection et réponse aux incidents de sécurité au quotidien.



Missions :

- Monitoring temps réel
- Analyse des alertes
- Réponse aux incidents
- Amélioration continue

Le succès repose sur l'alignement entre les objectifs métiers, les contraintes techniques et les exigences de sécurité, dans une démarche d'amélioration continue.