La sécurité de l'information : *et les managers dans tout ça ?*

Cercle Immedia du 13 février 2018

Nicolas Chaine

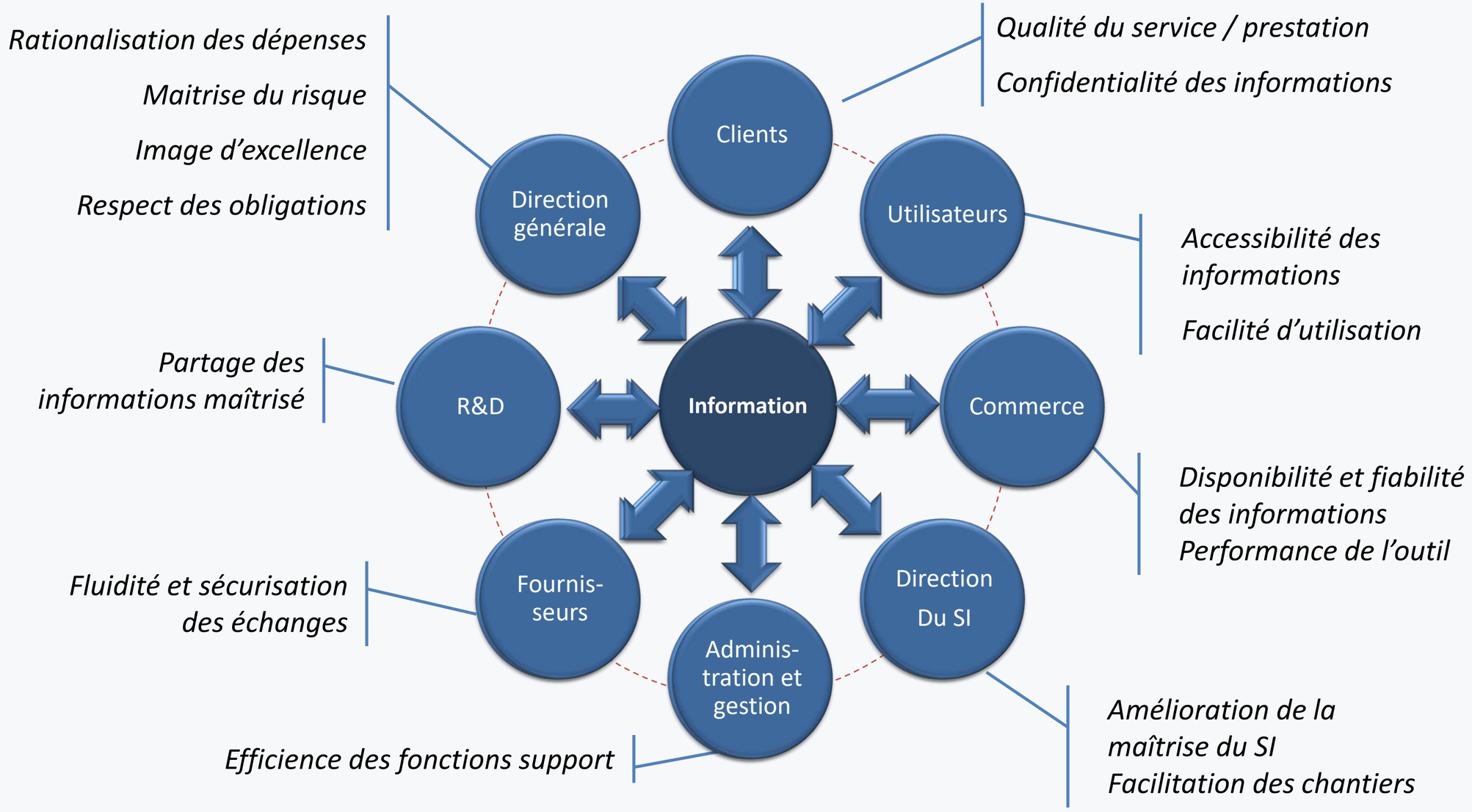
Préambule

ON NE VA PAS PARLER DU RGPD…

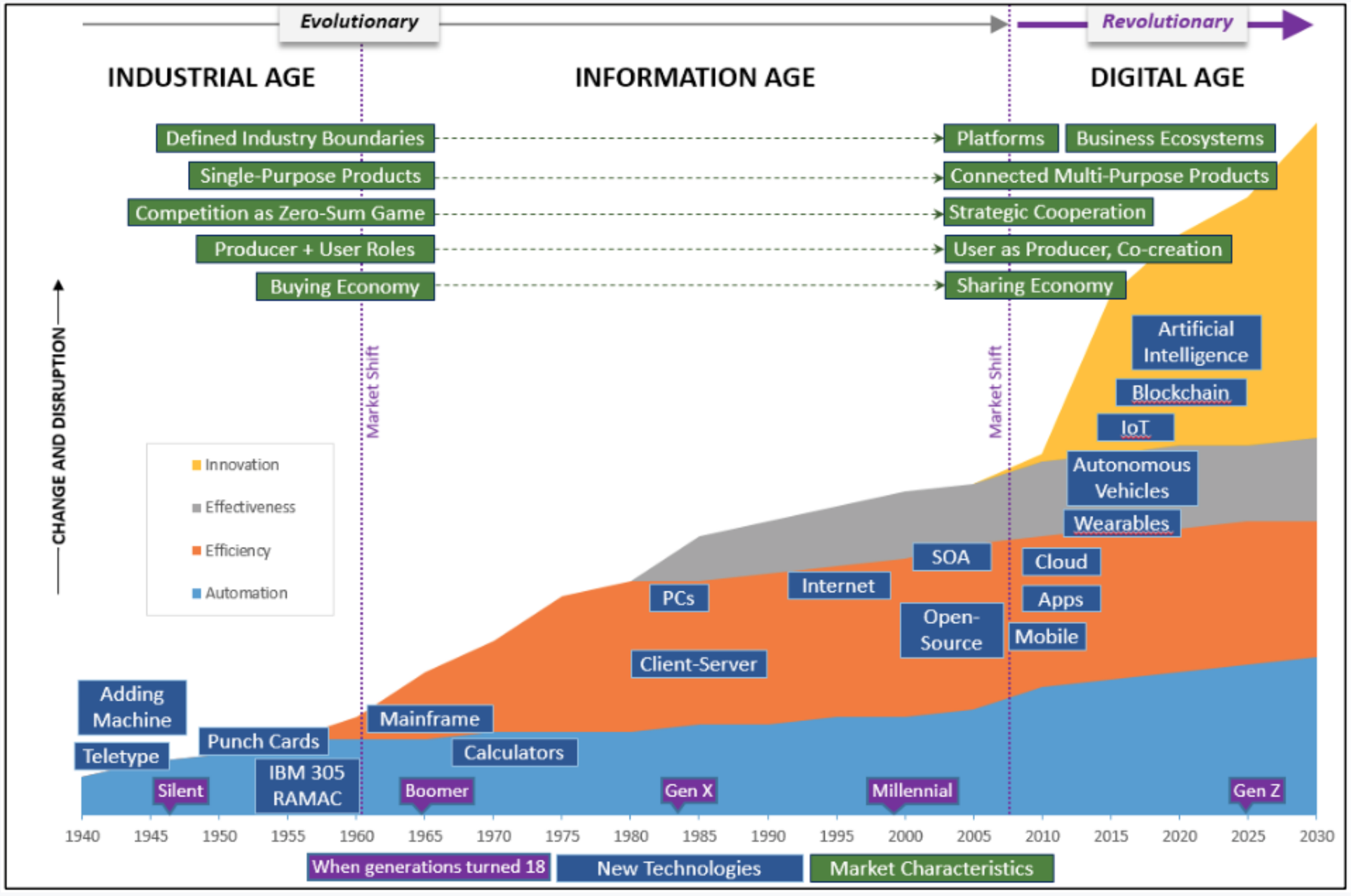
… mais plutôt de sécurité de l'information ☺

Sommaire

En entreprise, on trouve de nombreux acteurs et de nombreux besoins en informations…



… et des systèmes d'information en pleine (r)évolution



Quelques chiffres (inquiétants) autour de la sécurité des SI

- 100% des entreprises déclarent qu'au-delà d'une semaine sans système informatique, elles ne peuvent plus travailler

- Entre 1 et 10% seulement des cas de criminalité informatique sont traités par les services de police ou de justice.

- La sécurité : 3% du budget SI, 1/1000 personnel

- 55% des incidents de sécurité proviennent d'utilisateurs qui effectuent des actions qu'ils ne devraient pas.

Source : Secteur Fiance IBM 2014

- Les dommages liés à la sécurité informatique :
  - En 2003, 25 milliards de dollars…
  - En 2012, plus de 300 milliards de dollars… liés à la seule cybercriminalité (+42% / 2011 !...)
  - En 2015, pour le seul Royaume-Uni et pour la seule cybercriminalité, ce coût a été évalué à 27Md£ !!!...

Au fait… qu’est ce que la sécurité de l’information ?

La sécurité de l'information est un processus visant à protéger des données contre l'accès, l'utilisation, la diffusion, la destruction, ou la modification non autorisés.

La sécurité de l'information n'est confinée ni aux systèmes informatiques, ni à l'information dans sa forme numérique ou électronique. Au contraire, elle s'applique à tous les aspects de la sûreté, la garantie, et la protection d'une donnée ou d'une information, quelle que soit sa forme.

Toutes les mesures techniques, organisationnelles et humaines qui permettent de protéger les informations

Les quatres objectifs fondamentaux de la sécurité de l'information

- Assurer la DISPONIBILITE des services et des données
- Garantir l'INTEGRITE des données
- Assurer la CONFIDENTIALITE des données sensibles
- Assurer la TRACABILITE des actions

Il y a contradiction (fréquente) entre :
Se protéger de ses utilisateurs légitimes / Leur donner les moyens de travailler

Quelles sont les menaces sur la sécurité de l'information ?

- Erreurs
  - Dégradation de performance
  - Erreurs de manipulation
  - Erreurs de saisie
  - Erreurs de configuration
  - Bugs

- Accidents
  - Accident environnemental (incendie, inondation, accident industriel…)
  - Rupture de service
  - Coupure réseau
  - Panne d'équipements
  - Saturation de ressources
  - Perte accidentelle de données

- Actes non malveillants
  - Absence de personnel d'exploitation (grèves, congés, départ de personnel)
  - Utilisation de logiciels sans licence
  - Mauvais usages

- Malveillances
  - Vandalisme, vol et sabotage
  - (interne & externe)
  - Fuite d'information / divulgation
  - Effacement volontaire de données
  - Abus de droits
  - Saturation par un code malveillant
  - Cybercriminalité
  - Intrusion sur le SI

Qui sont les agresseurs ?

Plaisantins :
- S'amusent

Compétiteurs :
- Relèvent des défis
- Collectionnent des exploits

Vandales :
- Cherchent à détruire

Espions et/ou voleurs :
- Motivations politiques
- Motivations économiques

La sécurité physique des SI est souvent la première étape

- Les dispositifs de sécurité physique préservent les biens matériels contre des malveillances et des accidents matériels

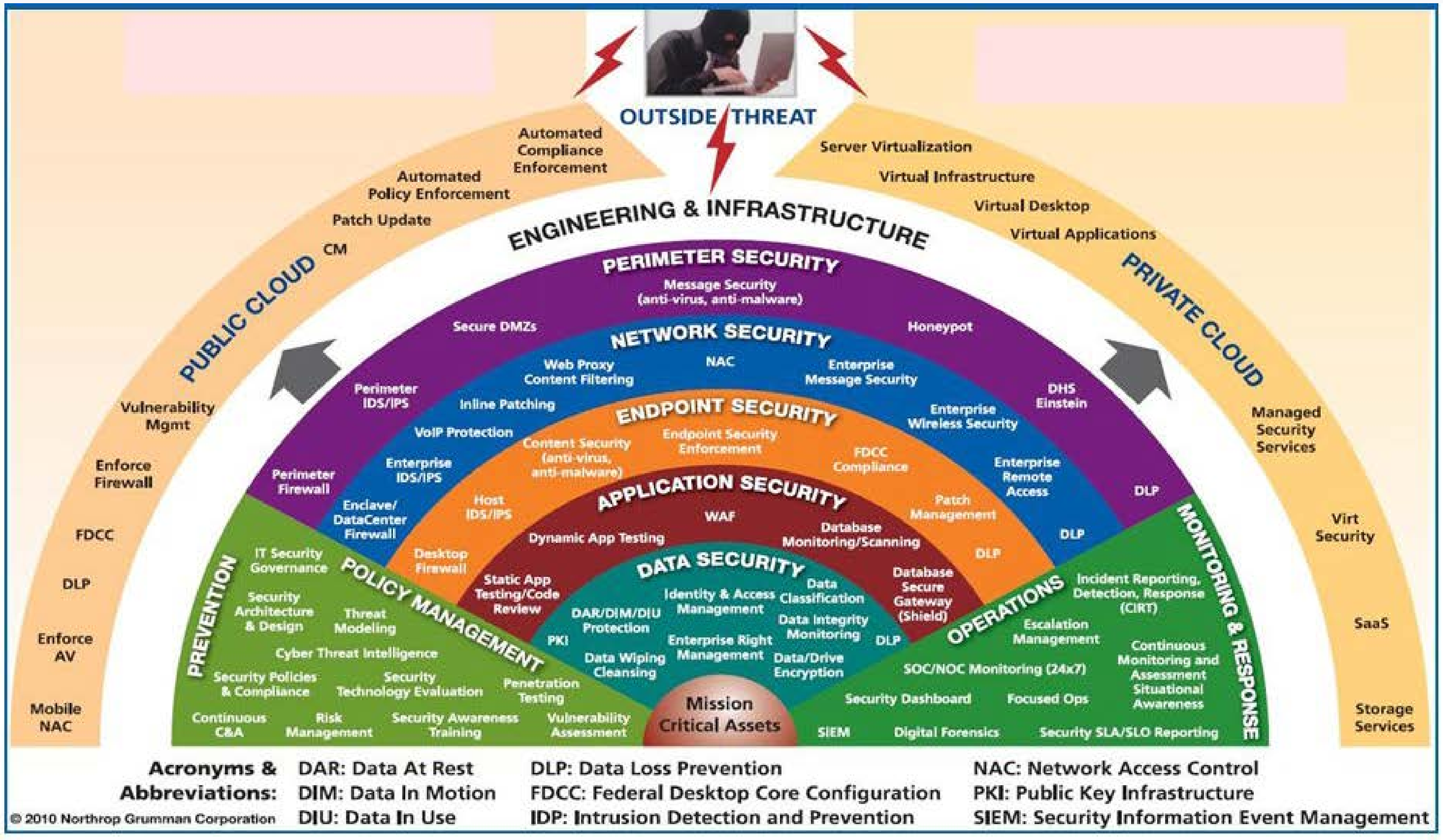
- Les dispositifs de sécurité physique sont de plusieurs natures :
  - protection des locaux informatiques : extincteurs, surélévation des planchers, …
  - protection des matériels informatiques : onduleurs, climatisation, groupes électrogènes, …
  - protection contre le vol : contrôle d ’accès, coffre-fort, etc.

Les dispositifs de sécurité logique sont très nombreux

- Les dispositifs de sécurité logiques préservent les ressources informatiques immatérielles contre des erreurs et des malveillances immatérielles

- Les dispositifs de sécurité logique sont de plusieurs natures (en vrac…) :
  - Les antivirus
  - L'évitement
  - La protection contre l'intrusion
  - La protection contre les « spams »
  - La protection contre les « exploits »
  - Le contrôle des erreurs
  - La technologie RAID
  - Les firewall
  - La sécurité des bases de données
  - La cryptographie
  - …

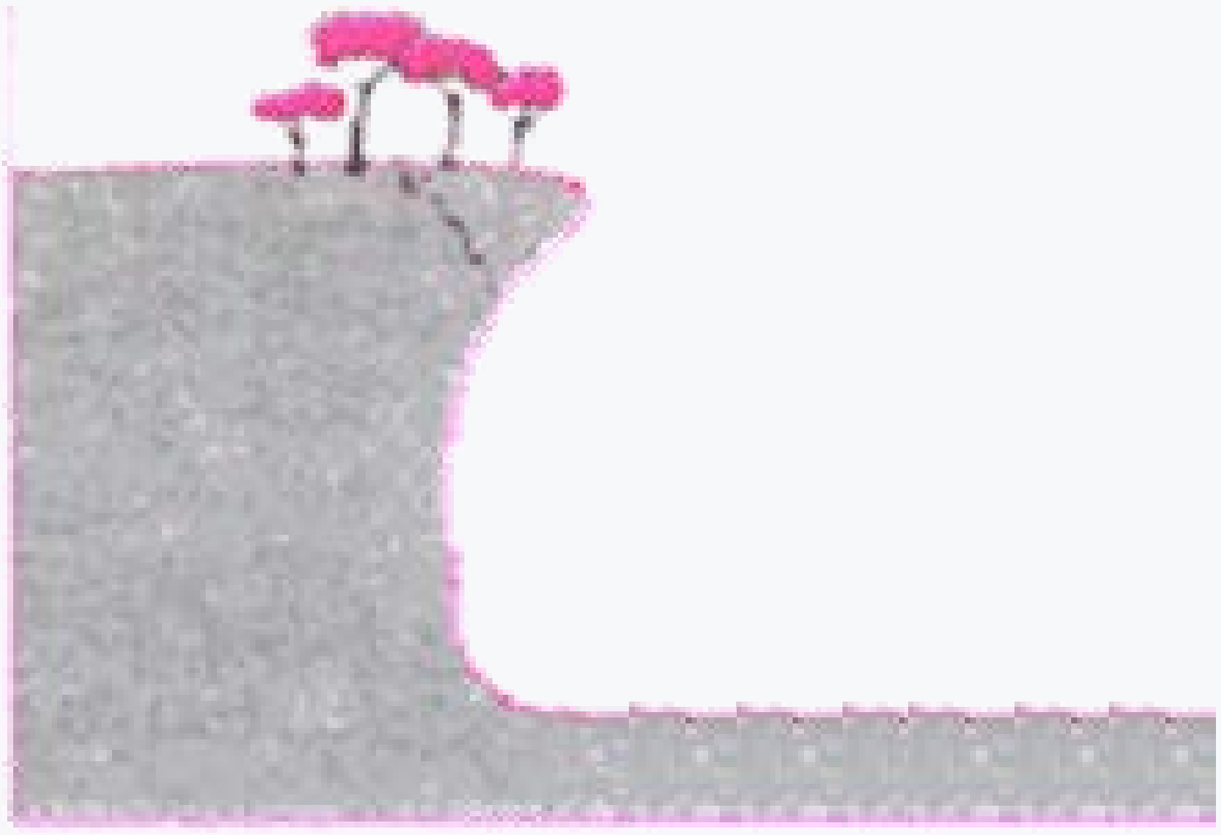
En synthèse, la sécurité des SI consiste à tout mettre en œuvre pour protéger les actifs clés de l'entreprise



Sommaire

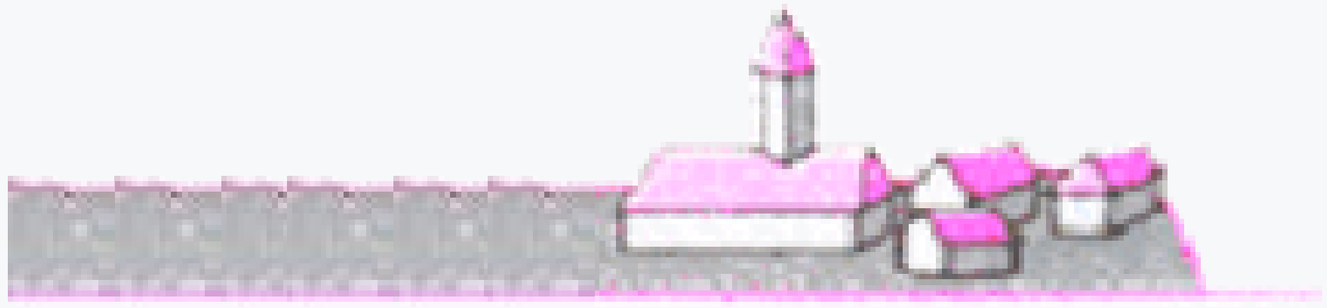
La sécurité de l’information est avant tout une gestion des risques
Comment apprécier un risque ?

Introduction à l'analyse de risque



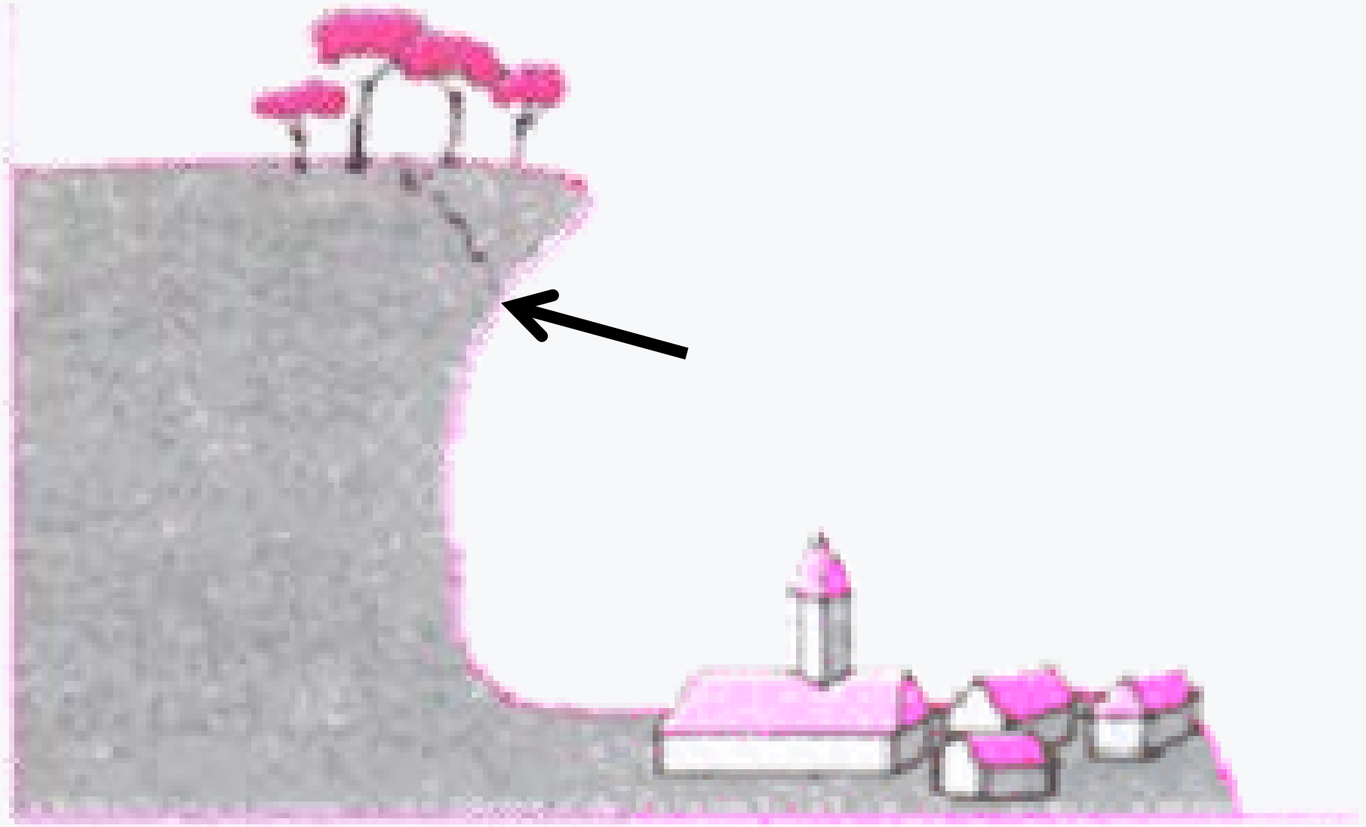
La menace

Introduction à l'analyse de risque



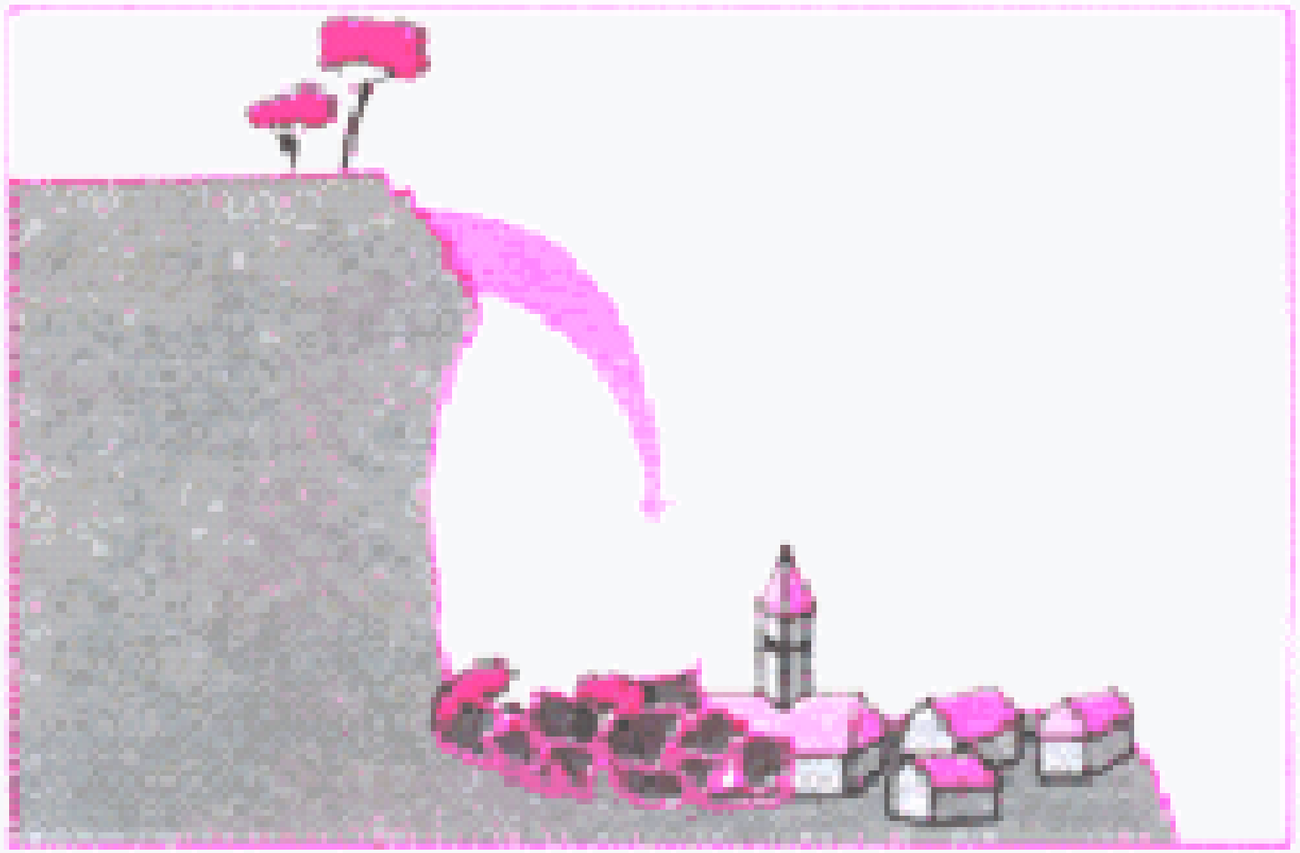
L’actif

Introduction à l'analyse de risque



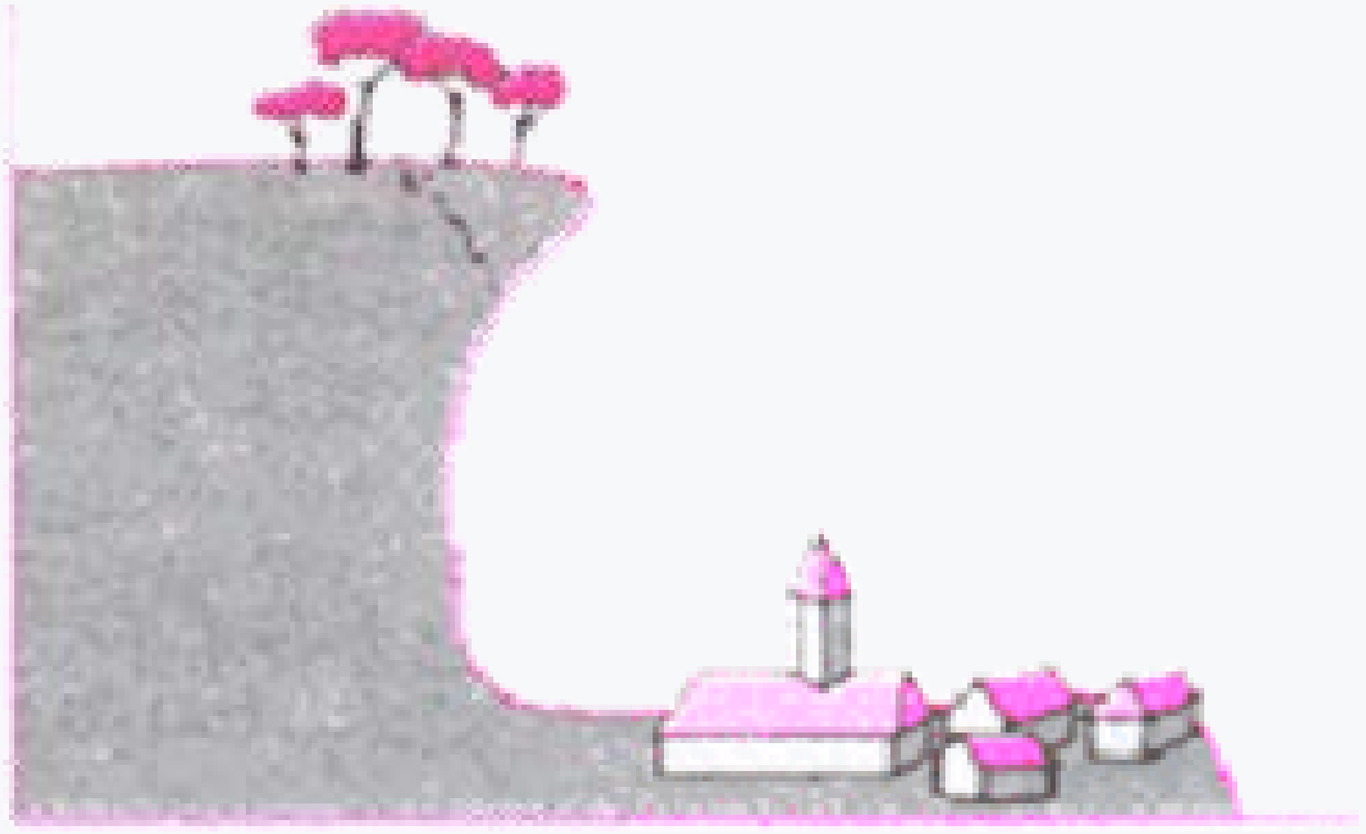
La vulnérabilité

Introduction à l'analyse de risque



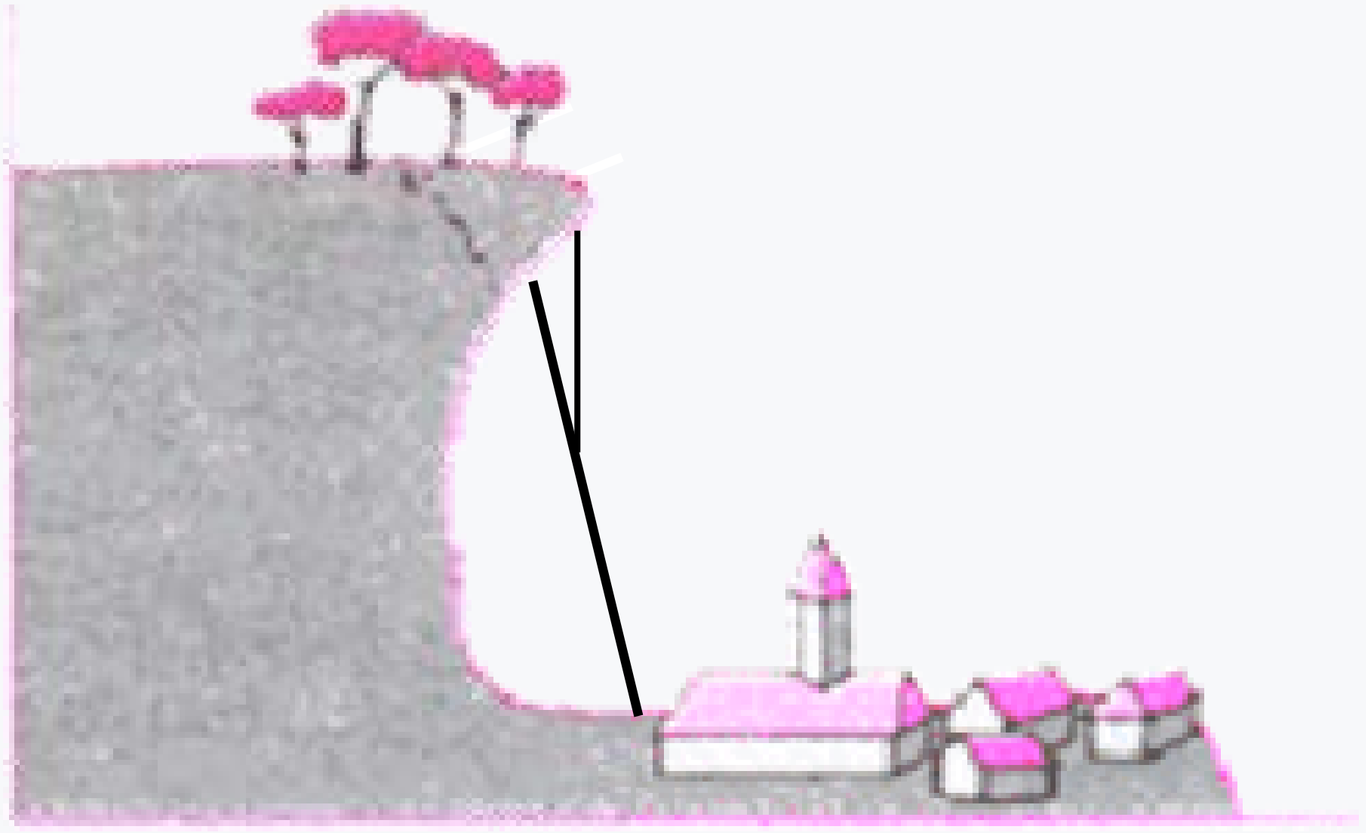
Le risque

Introduction à l'analyse de risque



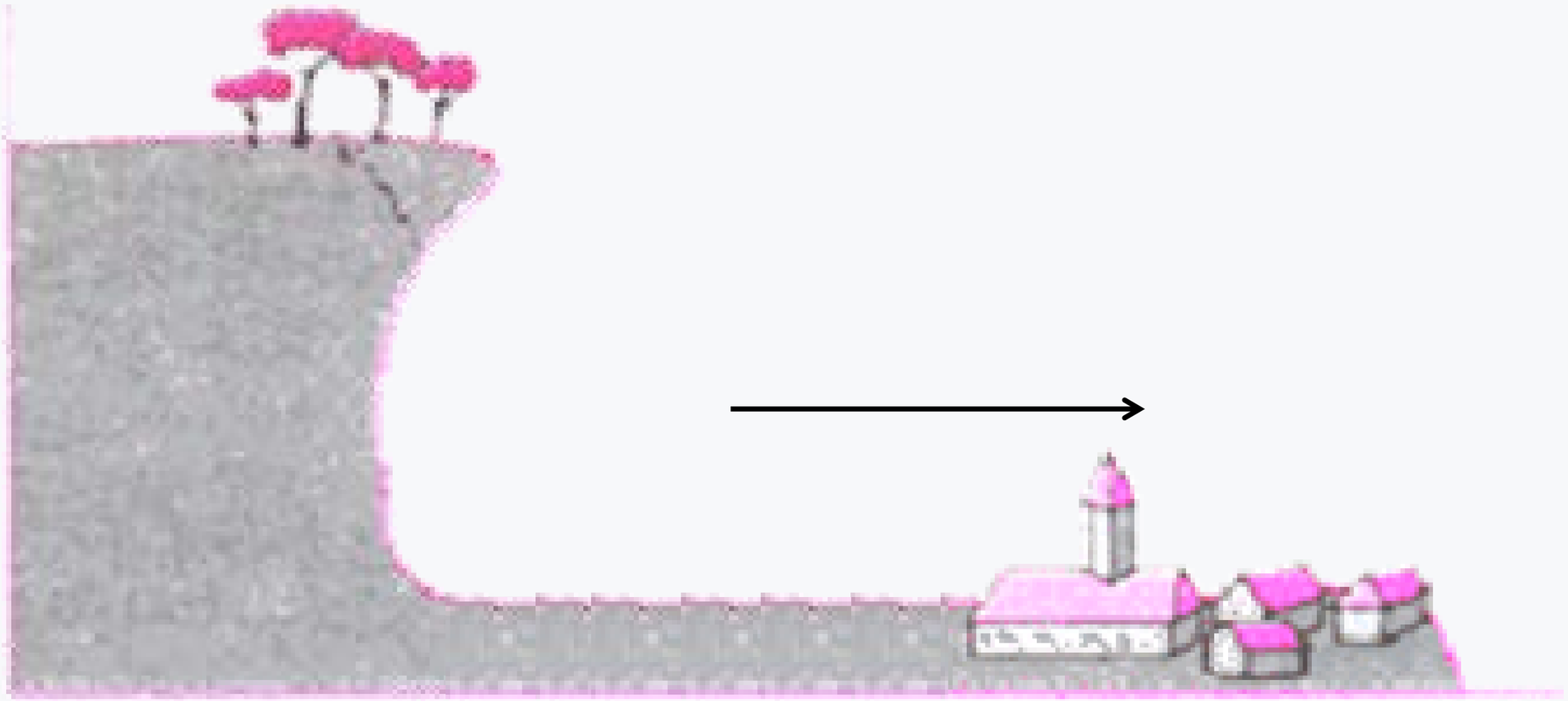
Accepter le risque

Introduction à l'analyse de risque



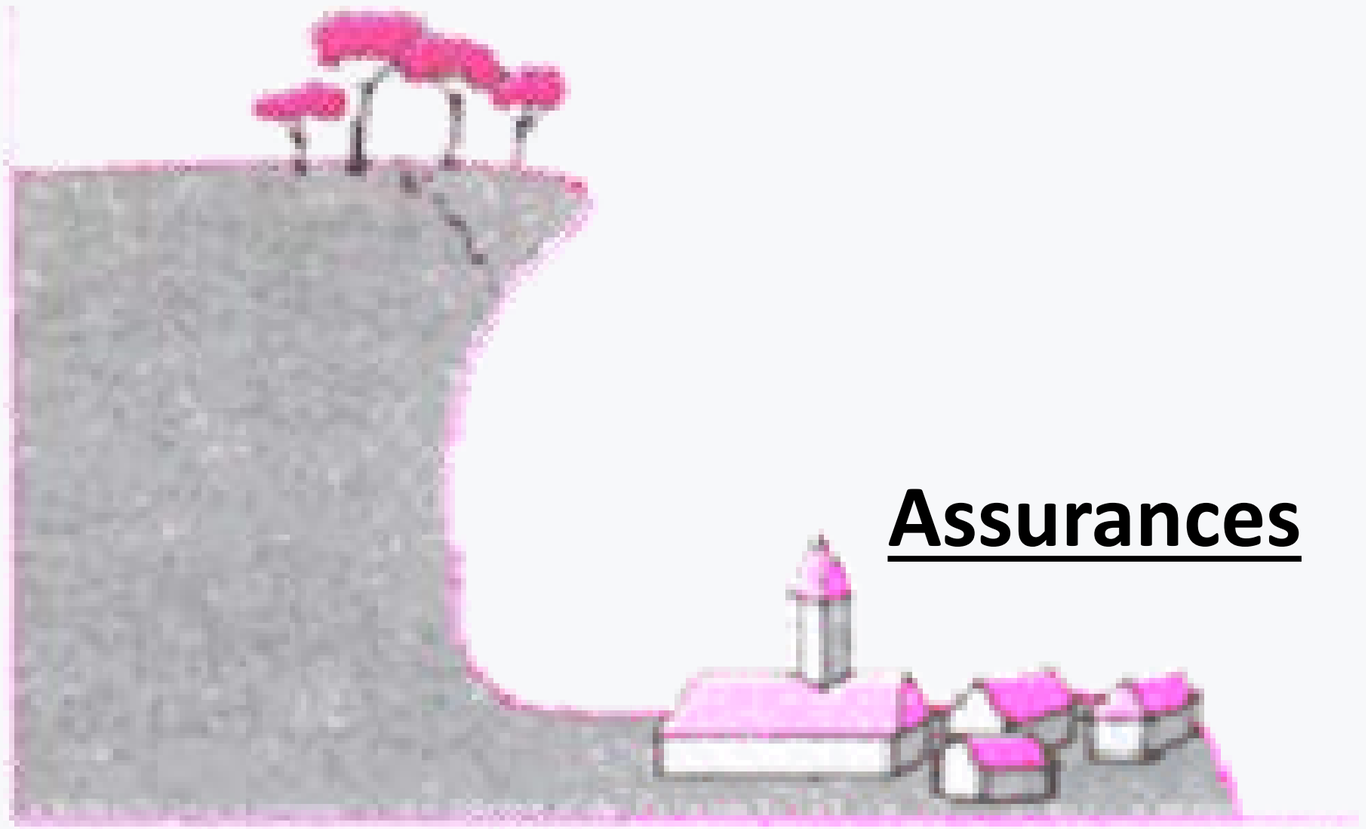
Réduire le risque

Introduction à l'analyse de risque



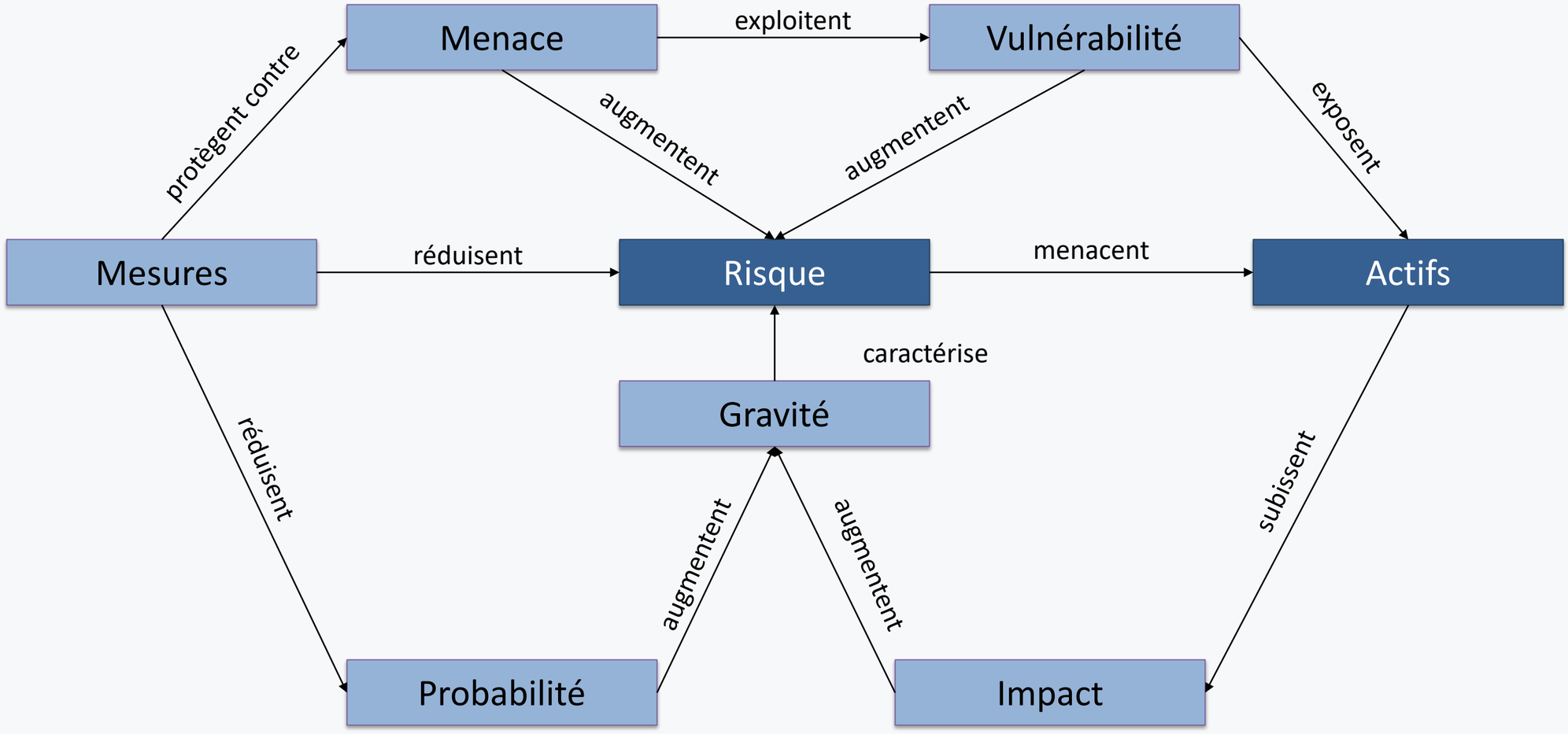
Contourner/éviter le risque

Introduction à l'analyse de risque



Transférer le risque

La sécurité de l'information est avant tout une gestion des risques pour éviter de dégrader ses actifs



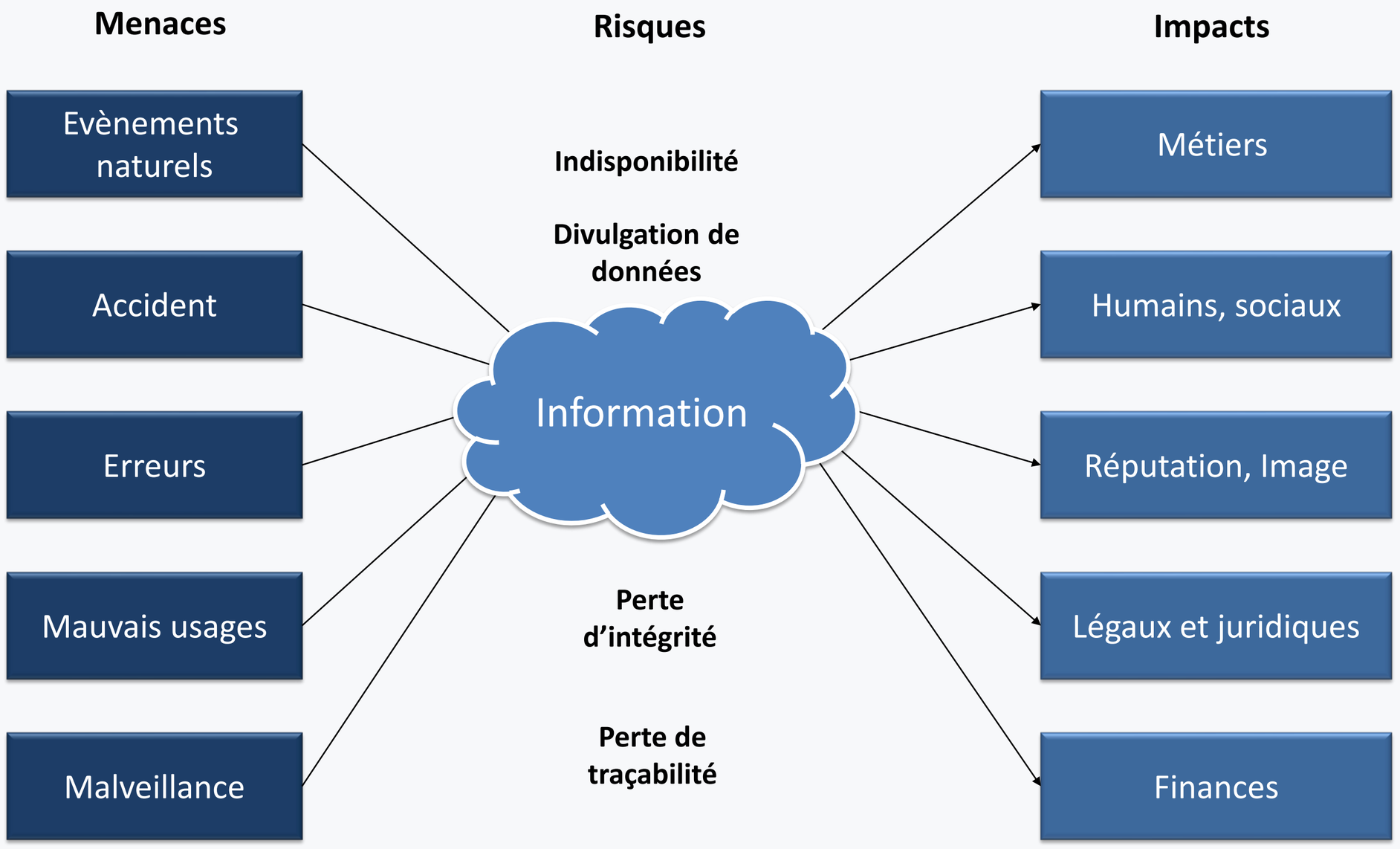
Il existe différents types de risques liés à l'information dans les entreprises

- **Risques opérationnels** : risque de pertes directes ou indirectes résultant de dysfonctionnements ou d'erreurs du système d'information, des processus, des personnes ou d'événements extérieurs
  - Exemples : mouvements sociaux, incapacité des dirigeants, catastrophe industrielle

- **Risques sur le système d'information** : risque d'atteinte aux critères de l'information
  - Critères : efficacité, efficience, fiabilité, conformité, disponibilité….
  - Exemples : absence de stratégie SI, non maîtrise des niveaux de service, résistance au changement

- **Risques de la sécurité de l'information** : risque d'atteinte aux critères fondamentaux de sécurité de l'information
  - Critères : disponibilité, intégrité, confidentialité, traçabilité
  - Exemples : perte de données, divulgation d'informations, absence de traçabilité, abus ou usurpation de droits

Quels risques et quels impacts liés à la sécurité de l'information ?



Pour piloter ces risques, il existe plusieurs méthodes de gestion des risques

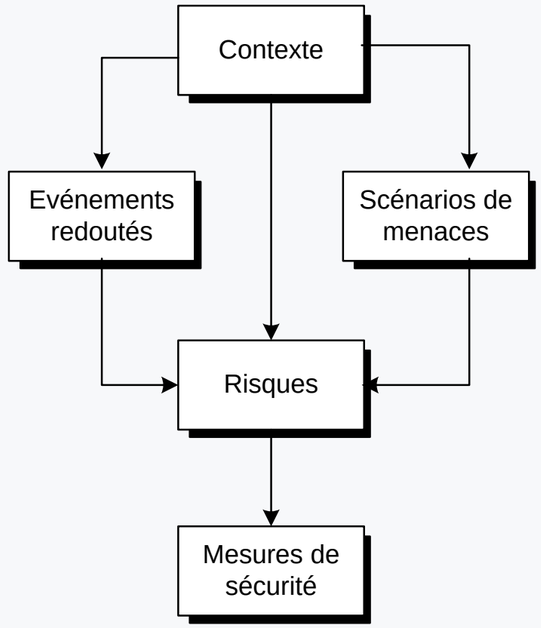
Méthode	Création	Popularité	Auteur	Soutenue par	Pays	Outils disponibles	Etat
EBIOS	1995	***	DCSSI	Gouvernement	France	Logiciel gratuit	
Mehari	1995	***	CLUSIF	Association	France	Logiciel Risicare	
Marion	1980	**	CLUSIF	Association	France		AB
Melissa		**	DGA	Armement	France		AB
Octave	1999	**	UCM	Universitaire	Etats-Unis	Logiciel payant	
Cramm	1986	**	Siemens	Gouvernement	Angleterre	Logiciel payant	
Score	2004		AC	Secteur privé	France	Logiciel payant	
Callio	2001		Callio. Tech.	Secteur privé	Canada	Logiciel payant	
COBRA	2001		C&A	Secteur privé	Angleterre	Logiciel payant	
ISAMM	2002		Evosec	Secteur privé	Belgique		
RA2	2000		aexis	Secteur privé	Allemagne	Logiciel payant	

Un exemple : Fiche d'identité de la méthode EBIOS

EXEMPLE

Fiche d'identité

- Nom Complet : Expression des Besoins et Identification des Objectifs de Sécurité
- Date de naissance : 1995
- Lieu de naissance : Direction Centrale de la Sécurité des Systèmes d'Information (ANSSI actuelle)
- Pays de naissance : France
- Langue : Français, Anglais, Allemand, Espagnol



Démarche EBIOS

Etude du contexte
Définir le cadre de la gestion des risques, préparer les métriques et identifier les biens.

Etude des événements redoutés
Apprécier les événements redoutés identifiés par les métiers de l'organisme en termes de gravité et de vraisemblance.

Etude des scénarios de menace
Apprécier les scénarios de menaces envisageables pour chaque bien support en termes de vraisemblance.

Etude des risques
Apprécier et évaluer les risques et identifier les objectifs de sécurité par rapport à ces risques.

Etude des mesures de sécurité
Formaliser les mesures de sécurité à mettre en œuvre et mettre en œuvre les mesures de sécurité.

Contenu de la méthode

- Biens essentiels et biens supports
- Sources de menace
- Menaces
- Impacts
- Vulnérabilités
- Mesures de sécurité

Démarche

- L'établissement du contexte
- L'appréciation des risque
- Le traitement des risques
- La validation du traitement des risques
- La communication et la concertation relatives aux risques
- La surveillance et la revue des risques

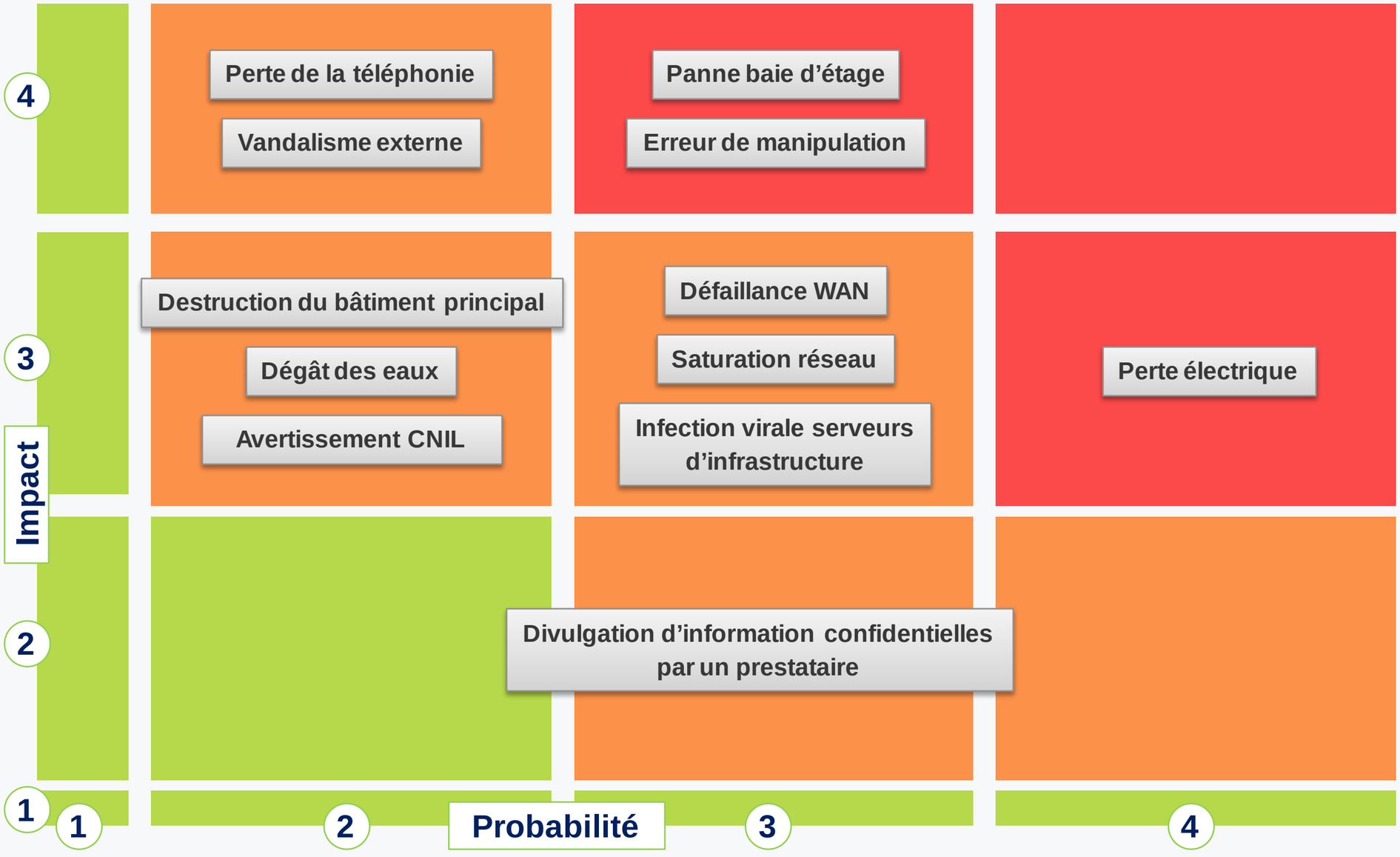
Quelles questions se poser pour l'analyse de risque ?
Un exemple de questionnaire à adapter en gestion de risques projet

EXEMPLE

- Questions générales
  - Projet stratégique ? A forte visibilité ?
- Utilisateurs
  - Quel canal d'accès à l'application ?
  - Quel type de population ? Combien ?
- Confidentialité des données
  - Quel type de données sont manipulées (données à caractère personnel, données client, données de santé, données financières, données stratégiques…) ?
- Intégrité
  - Quel impact en cas d'altération des informations manipulées ?
- Disponibilité
  - Combien de temps l'application peut-elle être indisponible ?
  - En cas d'incident, quelle perte de données [illegible] acceptable ?
- Preuve / traçabilité
  - Y-a-t-il des exigences particulières en sur les traces attendus sur le système ?
  - Existe-t-il des contraintes d'archivage légale ?
- Architecture / mise en œuvre
  - Est-ce un progiciel ou un développement spécifique ?
  - L'hébergement est-il externalisé?
  - Y-a-t-il des flux avec des éléments externes à l'organisation ?
  - Les technologies pressenties sont-elles standards (technologies éprouvées, nouvelles technologies…)

Exemple de synthèse d'une analyse de risque

EXEMPLE



Sommaire

Qu’est-ce qu’un SMSI et pourquoi le mettre en place ?
(Système de Management de la Sécurité de l’Information)

Car c’est un modèle permettant de mettre en place une **organisation efficace et pérenne de la sécurité** afin de répondre à des enjeux importants

Garantir la confiance	Augmenter la performance
Gérer les risques	Asseoir la crédibilité
Assurer la conformité	Garantir la qualité
Préserver l’image	Etre certifié ISO 27001

Comment ?

ISO 27005

ISO 27005 : gestion des risques
- Identification des risques
- Evaluation de ces risques
- Traitement des risques retenus

ISO 27003

ISO 27003 : guide d'implémentation
- Exemples types et recommandations pour la planification d'un SMSI

Impulsion initiale

« Nous souhaiterions mettre en place un SMSI »

Planifier

Phase de définition du contexte:
- La vision sécurité de l'organisation
- Les objectifs à atteindre
- Les moyens mis à disposition
- Analyse des risques
- La stratégie de mise en œuvre
- La politique de sécurité

ISO 27002

ISO 27002 : guide des bonnes pratiques
- Pistes et recommandations pour la gestion globale de la sécurité de l'information

ISO 27003

ISO 27003 : guide d'implémentation
- Exemples types et recommandations pour l'implémentation d'un SMSI

Déployer

Phase d'implémentation :
- Mise en œuvre de la politique de sécurité

SMSI
ISO 27001

Phase de révision et de mise à jour du SMSI:
- Corriger
- Adapter
- Améliorer

Améliorer

ISO 27004

ISO 27004 : mesurage
- Guide de préparation d'un programme de mesure de l'efficacité d'un SMSI ainsi que des métriques à choisir et à mettre en place

Phase de contrôle et de mesure d'efficacité du SMSI:
- Mise en place de tableaux de bords
- Mise en place de métriques de la sécurité
- Evaluation périodique de la sécurité

Contrôler

ISO 27007

ISO 27007 : audit des SMSI
- Recommandations relatives à la conduite d'audits internes et externes

ISO 27008

ISO 27008 : audit des contrôles
- Recommandations relatives à la conduite d'audits portés sur les contrôles ou groupe de contrôles implémentés au sein d'un SMSI

Légende:

En vert, cycle PDCA principal tel qu'il est utilisé dans la norme ISO 27001.
En orange, les autres normes qui gravitent autour de l'ISO 27001.

Amélioration continue

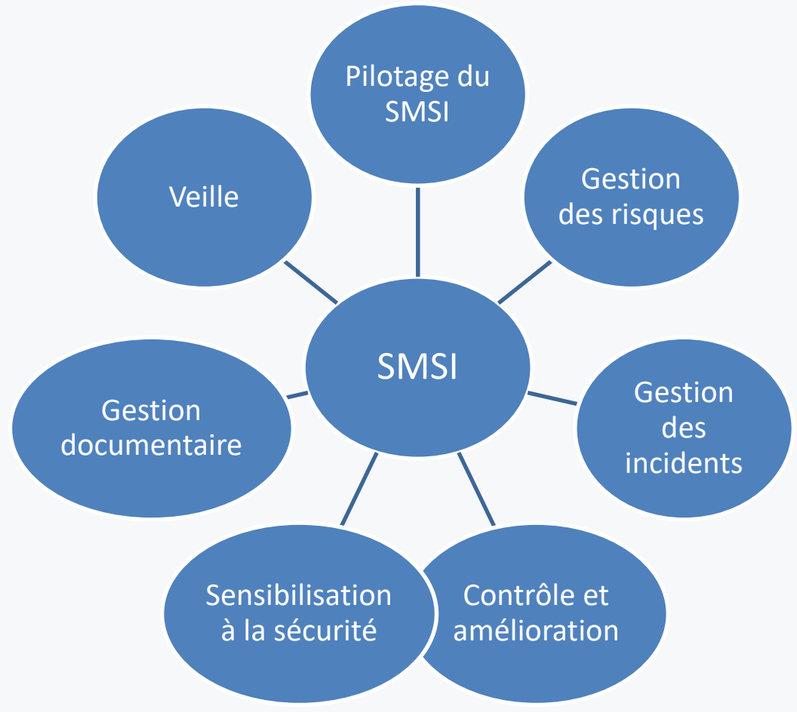
La norme ISO 27001 pose les bases d'un SMSI

- Elle professionnalise la démarche sécurité
- Elle garantie l'adéquation entre les mesures mises en œuvre et les risques identifiés, pour une meilleure maîtrise des coûts
- Elle est certifiante
- Elle est reconnue internationalement
- Elle est référencée par ITIL
- Elle est complétée par une famille de normes (la famille ISO 27000)

- C'est une norme qui établit une démarche, mais ne l'outille pas
  - Le choix de la méthode d'analyse pour cartographier les risques est libre
  - Des exemples précis et riches sont proposés en annexe
    - Liste type de menaces
    - Exemples de vulnérabilités
    - Tableau de classification des actifs
    - ….

Organisation internationale de normalisation

Les 7 processus essentiels de la norme ISO 27001



La norme ISO 27002 est un guide de bonnes pratiques

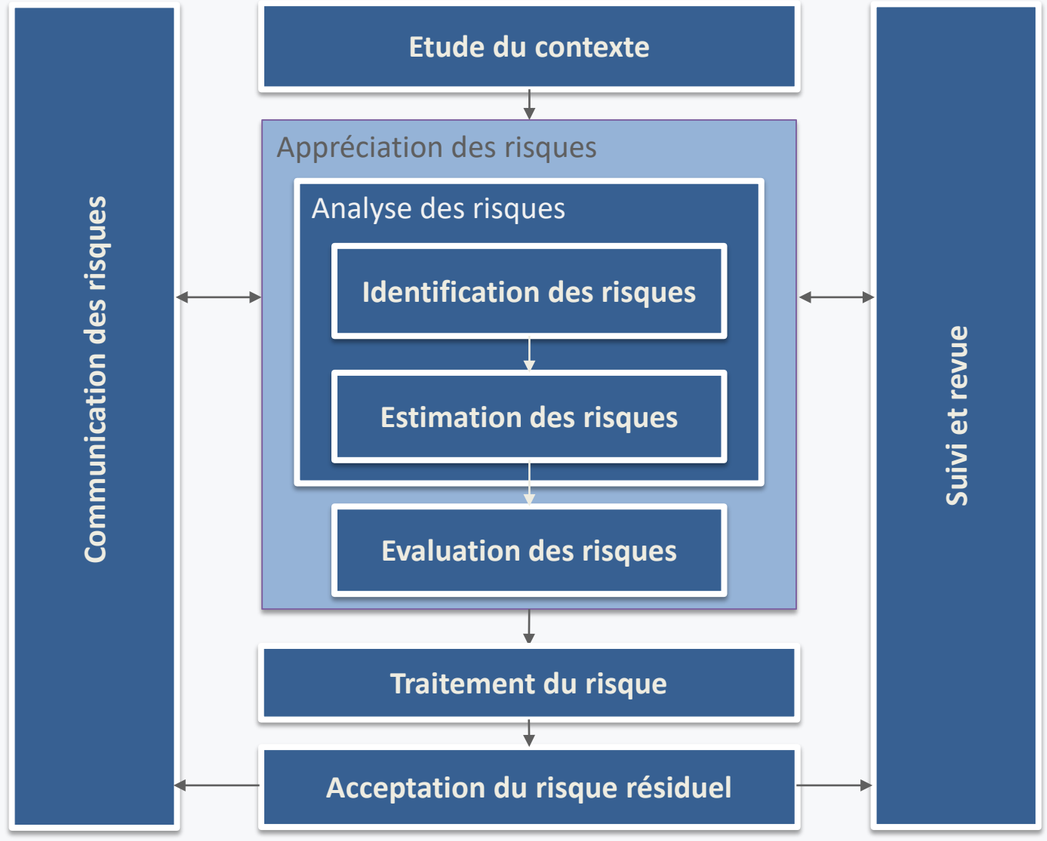
Organisation internationale de normalisation

La norme ISO 27005 explique en détail comment conduire l'appréciation des risques et le traitement des risques

Organisation internationale de normalisation

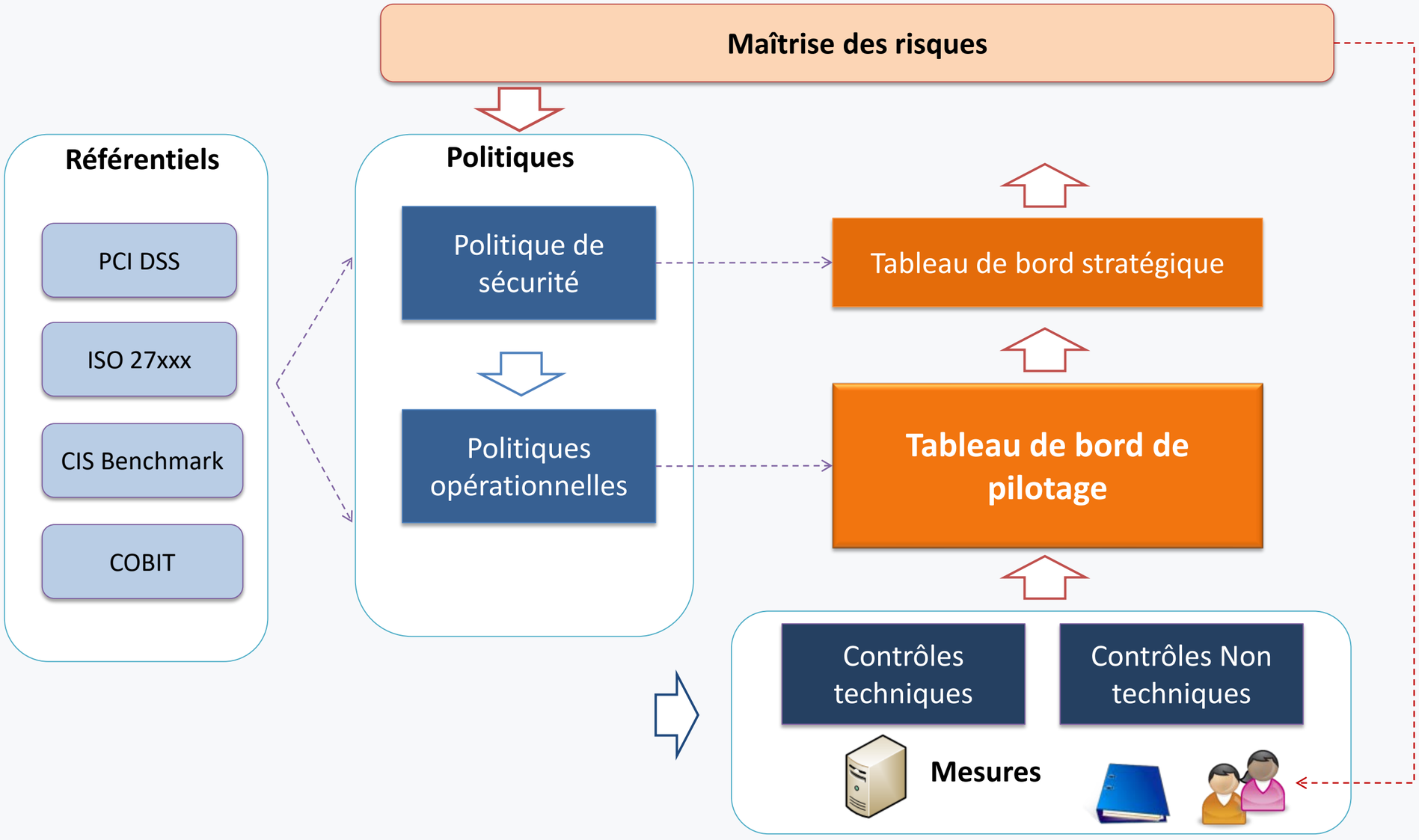
- La norme ISO 27005 propose une démarche pour l'appréciation des risques et le traitement des risques
- Elle vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001
- Elle est applicable à tous types d'organisation et prend en compte les évolutions d'organisation

Processus de gestion de risques selon l'ISO 27005



Sommaire

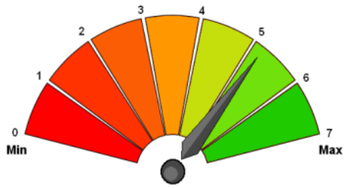
Le pilotage de la sécurité de l'information se fait par la mesure de la conformité

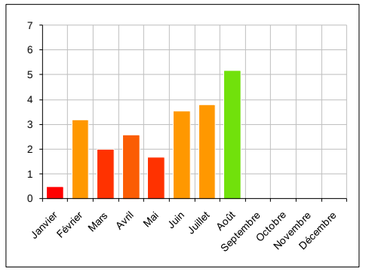


Exemples de tableaux de bord – Synthèse

EXEMPLE

Synthèse | **Protection antivirale** | **Correctifs de sécurité** | **Gestion des droits** | **Sauvegardes** | **Lutte anti-intrusion** | **Plan d'actions**





Les indicateurs ci-dessus montrent, pour le premier, le niveau de conformité pour la période en cours et , pour celui en dessous, l'évolution de ce niveau de conformité sur l'année.

Le niveau de conformité se détermine par des valeurs allant de 0 à 7. 7 est la valeur représentant le niveau le plus élevé. Un code couleur unique entre les deux graphiques permet l'association du niveau global et sa valeur.

Synthèse bimestrielle

Le niveau de conformité globale obtenu lors de l'audit n°3 est assez bon et en nette hausse par rapport à celui obtenu lors du précédent audit.

Cette hausse de votre niveau de conformité est principalement due à la mise en œuvre des actions présentes dans notre précédent rapport. Cette mise en œuvre des actions s'est traduite par la mise à jour des signatures antivirales sur 60% de vos machines et par un déploiement des correctifs de sécurité majeurs, sur l'ensemble des machines.

Nous vous encourageons à poursuivre vos efforts dans la mise en œuvre des plans d'actions fournis avec nos rapports, afin de continuer à améliorer votre niveau de sécurité.

Ce mois, le plan d'action comporte une nouvelle action. Elle concerne le **nombre peu élevé de vos serveurs référencés dans l'outil de sauvegarde**. Nous vous invitons à consulter le détail de cette nouvelle action et à la mettre en œuvre le plus rapidement possible, étant donnée sa criticité.

Si vous souhaitez plus d'informations sur ce rapport ou si vous avez des questions, nous vous invitons à vous rapprocher de notre intervenant chez vous.

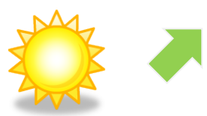
Protection Antivirale

L'antivirus est déployé sur l'ensemble de vos machines.
Toutefois, nous recensons plusieurs machines ne disposant pas de la dernière version des signatures antivirales.

Gestion des correctifs de sécurité

Plusieurs des derniers correctifs de sécurité majeurs n'ont pas été déployés sur vos serveurs.

Gestion des sauvegardes



Toutes les machines de votre parc informatique sont référencées dans l'outil de sauvegarde et tous les tests de restauration ont été concluants.

Gestion des droits

Il existe un nombre important de comptes administrateurs dans votre domaine. Aucune revue des droits des utilisateurs n'a été organisée depuis un an.

Lutte anti-intrusion

Le test d'intrusion a permis de constater une net amélioration du niveau de protection sur le périmètre testé. La plupart des plans d'action identifiés ont été réalisés.

Seuils	Orage	Pluie	Nuage	Eclaircie	Soleil
	0,3	0,5	0,7	0,85	1
Visuels utilisés					

Envoyer par mail Imprimer

Exemples de tableaux de bord– Protection antivirale

EXEMPLE

Synthèse | **Protection antivirale** | Correctifs de sécurité | Gestion des droits | Sauvegardes | Lutte anti-intrusion | Plan d'actions

Informations générales

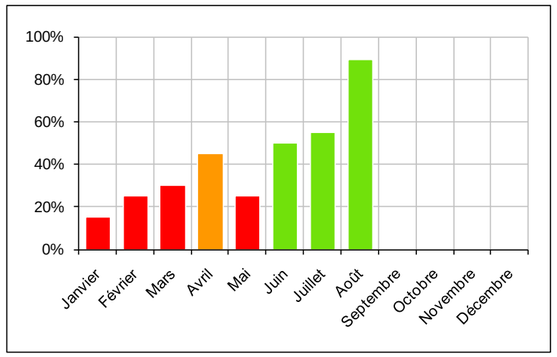
550 Utilisateurs

500 Postes de travail

30 Serveurs

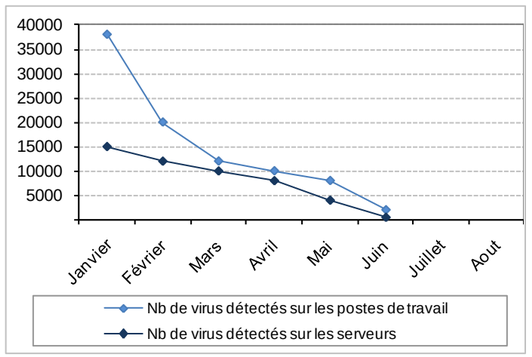
3500 Mails reçus par jour

2000 Spams bloqués par jour



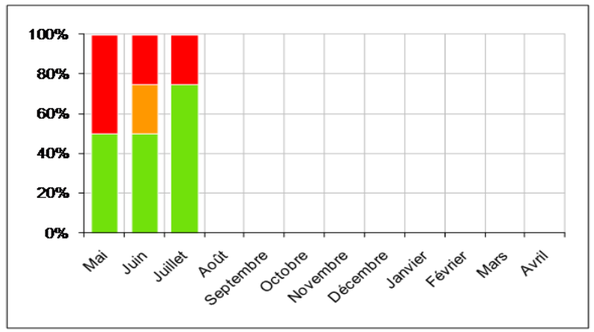
Evolution du nombre de machines protégées

Nombre de machines disposant de la dernière version des signatures antivirales



Evolution du nombre d'incidents viraux

Nombre de menaces virales détectées par l'antivirus



	Fonction de sécurité	Niveau	Tendance
1	Antivirus à jour	Information	→
2	Correctifs Microsoft à jour	Information	→
3	Comptes restreints	Information	↗
4	Firewall actif	Faille	→

Niveau de sécurité du serveur antivirus

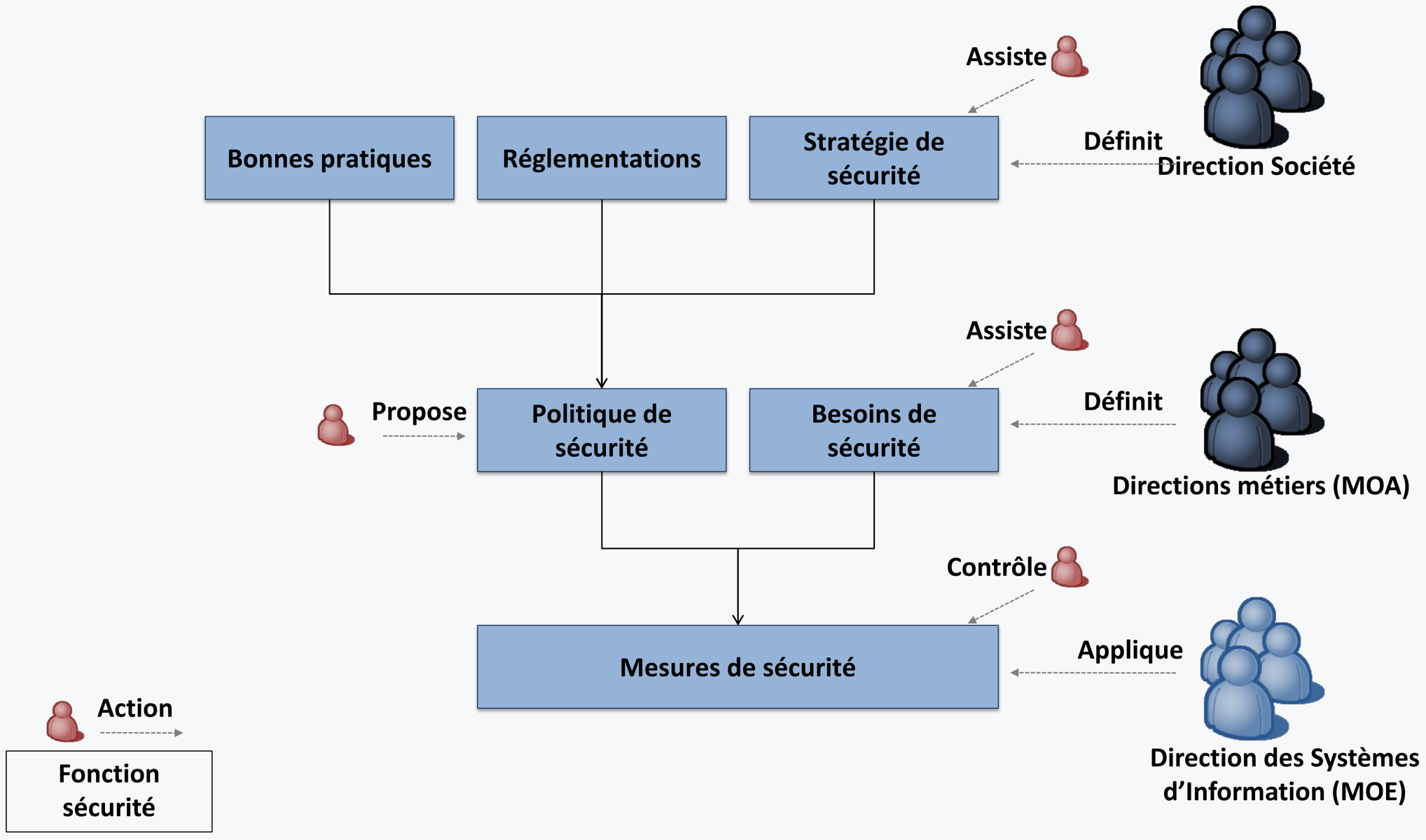
Commentaire

Le niveau de conformité obtenu au cours de cet audit, suit la courbe de progression amorcée depuis trois mois et est donc en nette hausse par rapport à celui obtenu lors du dernier audit. Le nombre d'incidents viraux est, cette fois encore, en nette baisse et l'antivirus est déployé sur l'ensemble de vos machines. Toutefois, nous recensons toujours plusieurs machines ne disposant pas de la dernière version des signatures antivirales.

Envoyer par mail Imprimer

Sommaire

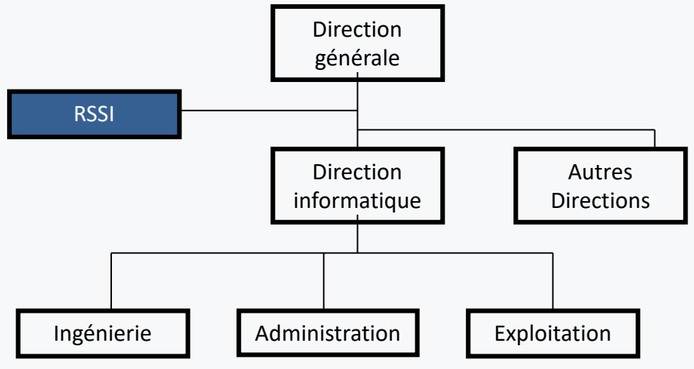
La fonction sécurité est en interaction avec tous les niveaux de l'entreprise



Quel positionnement pour le RSSI dans l'entreprise ?

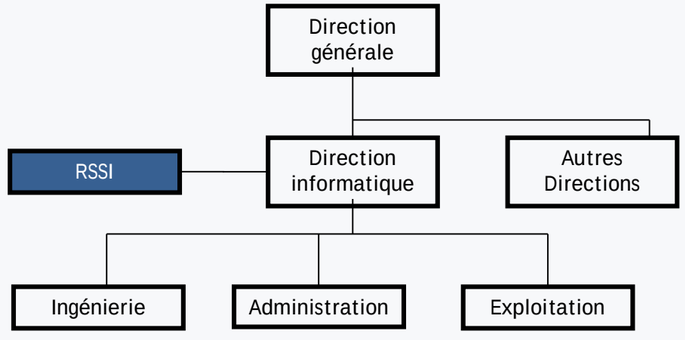
Le positionnement idéal

- En rattachement direct à la Direction Générale
- Le RSSI dispose des pouvoirs nécessaires à son activité
  - Il dispose de la légitimité nécessaire avec les autres directions pour mettre en œuvre les mesures de sécurité
  - Il rend des comptes directement à la Direction Générale



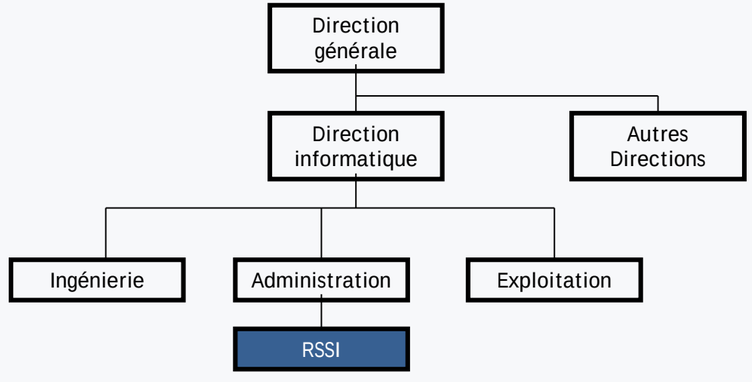
Le positionnement intermédiaire

- En rattachement de la direction informatique
- Positionnement couramment rencontré
- Un pilotage global plus difficile
  - Le RSSI a moins de pouvoir
  - Son budget est lié à celui de la DSI



Le positionnement « 0 »

- Opérationnel
- A peu (pas) de pouvoir
- N'a pas de budget



Synthèse de la fiche d'identité de la fonction sécurité : c’est vaste…

- Analyser les risques et les enjeux
- Définir les référentiels de sécurité
- Accompagner les projets
- Réaliser des audits et des contrôles
- Le pilotage de la sécurité de l'information
- Participer à la gestion des incidents de sécurité, et la gestion de crise
- Assurer la veille autour de la sécurité de l’information
- Communiquer, communiquer, communiquer

Sommaire

A votre avis : quelle est la plus grande menace en entreprise ?

« La plus grande menace pour la sécurité informatique d'une entreprise [...] pourrait être vous »

Kevin Mitnick, premier pirate entré dans le top 10 des criminels les plus recherchés par le FBI

Pourquoi communiquer sur la sécurité de l'information ?

Le post-it collé à l'écran ou sous le bureau

La conversation professionnelle dans un lieu public

Le document confidentiel accessible à tous

La conversation sur un réseau social

Communiquer et répéter sont à la base de la connaissance

« Si vous trouvez que l'éducation coûte cher, essayez l'ignorance »

Abraham Lincoln, seizième président des États-Unis

Sommaire

La sécurité de l’information « on the go »

- La sécurité de l’information ne concerne pas simplement les SI

- La sécurité de l’information est, avant tout, une question de gestion de risques

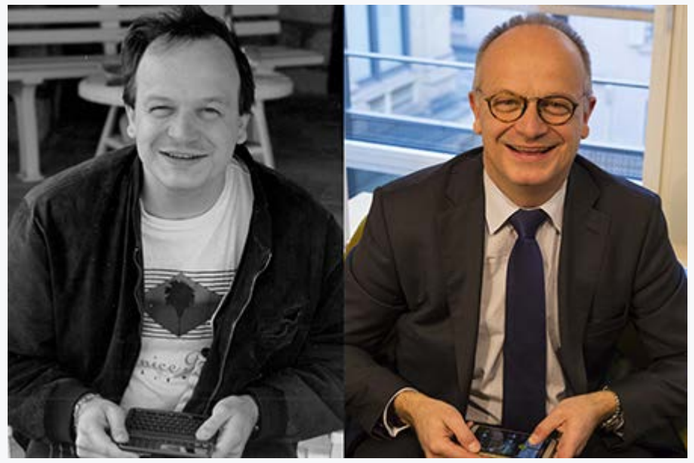
- On ne maîtrise réellement que ce qu’on pilote… il faut donc mettre en place un pilotage de la sécurité de l'information

- Le management doit être impliqué, à TOUS les niveaux de l’entreprise, dans la sécurité de l’information

- Les piliers de la réussite sont : expliquer, communiquer, pratiquer

Nicolas Chaine : Directeur Général de transition / Partner

Stratégie, Ventes & Transformation Digitale – Banque, Assurance et Conseil - Business Development



Nicolas a 49 ans, **Ingénieur** ENSEA, diplômé de l'**ESSEC** et titulaire d'un DEA de Stratégie et Management de l'Université Paris X Nanterre.
Dans son parcours professionnel, Nicolas a occupé à la fois des postes d'**Associé** au sein de grands cabinets de conseil en management (**Gemini consulting**, **Mazars**, **Sopra, AT Kearney**), et des rôles opérationnels de direction générale dans des PME innovantes comme récemment chez **Advens**, acteur majeur et innovant de la cybersécurité, où il était le Directeur Général Adjoint en charge du commerce et des opérations.

Nicolas CHAINE est dirigeant (DG/DGA/Directeur de la transformation) spécialisé dans la mise en œuvre du développement et de la **transformation digitale** des entreprises.
Ses responsabilités incluent la définition de la stratégie, l'évolution et le pilotage opérationnel des organisations, que ce soit sur les aspects commerciaux et produits, recrutement et développement des hommes ou systèmes d'information.
Il connait plus particulièrement le secteur des services B2B à dominante technologique, l'industrie et le secteur financier (**Banque** de détail et **Assurance**).
Nicolas aime partager ses connaissances que ce soit en tant qu'enseignant vacataire à l'ESSEC depuis 1994 ou en tant qu'« advisor » pour plusieurs start-up dans leur positionnement et leur structuration financière.

Il est aussi membre de l'Institut Français des Administrateurs (**IFA**), joueur de tennis et de golf.

Merci!

Bruno CALBRY
Partner

calbry@immedia.fr
T. 01 34 84 50 01
M. 06 77 85 01 81

immédia!
44, rue de la Bienfaisance
75008 - Paris

immédia!
93, rue de la Villette
69003 - Lyon

Nicolas CHAINE
Partner

nchaine@immedia.fr
M. 06 07 34 26 88

immédia!
44, rue de la Bienfaisance
75008 - Paris

C'EST MAINTENANT