

Méthodologie de la sécurité informatique

(Système de Management de la Sécurité de l'Information)

université d'Alger 1 -
Benyoucef Benkhedda

Introduction:

Sécuriser un tel système signifie:

- ✓ **Evaluer** les risques et leur **criticité** (cartographie des risques)
- ✓ Les **choix** de sécurité Étape difficile
- ✓ Mettre en œuvre les protections, et **vérifier** leur efficacité.

“Tout est basé sur la DÈCISION”

information security management system :



"An **information security management system (ISMS)** is a set of **policies** and **procedures** for systematically managing an organization's sensitive data. The goal of an ISMS is to **minimize risk** and ensure business continuity by pro-actively limiting the impact of a security breach."

An ISMS typically addresses **employee behaviour** and **processes** as well as **data** and **technology**. It can be targeted towards a particular type of data, such as customer data, or it can be implemented in a comprehensive way that becomes part of the company's culture."

- Techtarget.com

Intégration de la sécurité :

- 1. Intégrer la sécurité au sein d'une organisation**
- 2. Intégrer la sécurité dans les projets**
- 3. Politique de la sécurité des systèmes d'information (PSSI)**
- 4. Difficultés liées à la prise en compte de la sécurité**



1. Intégrer la sécurité au sein d'une organisation

1. Intégrer la sécurité au sein d'une organisation

Afin d'évaluer le niveau de sécurité attendue, les questions suivantes peuvent être posées :

- Qu'est ce que je veux protéger ?
- De quoi je veux me protéger ?
- A quel type de risques mon organisation est exposée ?
- Qu'est ce que je redoute ?
- Quelles sont les normes qui s'appliquent à mon organisation ?

1. Intégrer la sécurité au sein d'une organisation

L'organisation peut s'inspirer de la famille de norme internationale **ISO 2700x** et des guides nationaux (référentiel de sécurité informatique 2016)

27001

- Systèmes de management de la sécurité de l'information

27002

- Code de bonnes pratiques

27004

- Mesures du management de la sécurité

27005

- Gestion des risques

27035

- Gestion des incidents de sécurité

27037

- Traitement des preuves numériques (*forensics*)

...

- ...

2016

Référentiel de Sécurité
Informatique



1. Intégrer la sécurité au sein d'une organisation

Classification des informations

	Intitulé	Explication	Exemple	Risque
C1	Accès libre	Tout le monde peut y accéder	Informations publiées sur le site internet	Aucun
C2	Accès à l'organisation	Seul le personnel de l'organisation est autorisé à accéder à l'information	Nom, adresse des partenaires et fournisseurs de l'organisation	Atteinte à l'image, gêne passagère
C3	Diffusion limitée	Au sein de l'organisation, seul un groupe de personnes est autorisé comme les membres du même projet	Plan technique d'un nouveau laboratoire ; Listes des personnes admissibles avant publication officielle...	Situation à risques ; pertes financières acceptables
C4	Confidentiel	L'information est accessible à une liste très restreinte d'utilisateurs à titre individuel	Contenu des brevets déposés ; Recherche en cours ; N° de sécurité sociale et noms...	Pertes financières inacceptables, poursuites judiciaires

1. Intégrer la sécurité au sein d'une organisation

Classification des informations

Sur la base des niveaux de confidentialité définis, les mesures suivantes peuvent être implémentées :

- Une politique de gestion des informations est définie :
 - Création d'un modèle de document indiquant le niveau de confidentialité ;
 - Sensibilisation du personnel et des partenaires à cette politique.
- Les informations de niveau « **Confidentiel** » doivent être :
 - envoyées par mail de manière chiffrée et le mot de passe communiqué par SMS aux destinataires ;
 - stockées localement dans des conteneurs chiffrés.
- Les informations de niveau « **Diffusion limitée** » doivent être échangées au travers d'un système documentaire collaboratif ayant des accès nominatifs contrôlés, par exemple MS SharePoint.

2. Intégrer la sécurité au niveau du projet



2. Intégrer la sécurité au niveau du projet

Il s'agit de bien distinguer entre **la sécurité du système d'information** qui est un des objets du projet et **la sécurité du projet en lui-même** (diffusion et traitement des informations).

Concernant la sécurité du SI en lui-même :

- Toute activité étant gérée en mode projet, une bonne intégration de la sécurité dans l'organisation nécessite l'intégration de la sécurité dans chaque projet dans le respect de la réglementation ;
- Isoler les traitements de données sensibles au sein de projet pour avoir une meilleure maîtrise des risques et des mesures de sécurité à mettre en œuvre pour réduire ces risques.

La sécurité doit être prise en compte dans **toutes les étapes** d'un projet

2. Intégrer la sécurité au niveau du projet

Exemple d'intégration

Phases

Sécurité

<ul style="list-style-type: none">Perception d'un besoinExpression des besoinsCréation d'un projet	<ul style="list-style-type: none">Formalisation de besoins fonctionnelsÉtude de marchéÉtude de faisabilitéAnalyse de coûtPlanificationIdentification des entrée/sortie	<ul style="list-style-type: none">Développement logiciel ou matérielConstruction de prototypeTests utilisateursDocumentation	<ul style="list-style-type: none">Déploiement dans l'environnement de productionTest de performanceMaintien en Condition OpérationnelleExploitation	<ul style="list-style-type: none">Libération des ressourcesFin du projet
<p>Étude / Initialisation</p>	<p>Conception</p>	<p>Implémentation / Prototype / Test</p>	<p>Exploitation / Maintenance</p>	<p>Fin de vie</p>
<ul style="list-style-type: none">Analyse de risques amontConsultation des équipes sécurité	<ul style="list-style-type: none">Analyse de risquesProposition de mesures de sécuritéIdentification des risques résiduelsExpressions de besoins de sécuritéEstimation de coûts	<ul style="list-style-type: none">DéveloppementPrise en compte des bonnes pratiquesTop 10 OWASP¹Validation sécuritéContrôle des mesures de sécurité	<ul style="list-style-type: none">Maintien en condition de sécuritéGestion des incidentsAnalyse ForensiqueSauvegardeSupervision de sécuritéVeille de sécuritéAudit (technique, opérationnel)Tests d'intrusionRésilience	<ul style="list-style-type: none">Archivage des informationsEffacement sécuriséRéversibilitéMise au rebutObsolescence des configurations

¹Open Web Application Security Project

2. Intégrer la sécurité au niveau du projet

Différentes approches d'intégration

- **Sécurité prise en compte en fin de développement**

- Intégration des solutions de sécurité après finalisation du projet (après développement d'une application par exemple)
- **Problèmes de coût, des délais et des efforts supplémentaires**

Exemple d'un projet de construction d'une nouvelle salle devant héberger les serveurs de l'organisation :

- L'audit de sécurité fait le constat que :
 - Les baies de stockage des serveurs ne se ferment pas à clé ;
 - Pas de mécanisme de contrôle d'accès (lecteur de badge) prévu tracer les accès ;
 - Pas de redondance (alimentation, accès de télécommunications) des équipements ;
 - Aucune alarme anti-intrusion ou incendie n'est prévue ;
 - L'arrivée de câbles dans la salle est exposée à des actes de malveillances ;
 - La salle est construite en zone inondable.
- Conséquences :
 - Rachat de matériel et d'équipements => **coût supplémentaire** ;
 - Re-câblage de la salle, et travaux de génie civil à prévoir ;
 - Relocation de la salle ou reconstruction => **coût supplémentaire très importante**.

2. Intégrer la sécurité au niveau du projet

Différentes approches d'intégration

- **L'approche par l'analyse et le traitement du risque**

L'analyse de risques doit être effectuée en amont du projet mais doit aussi évoluer au fur et à mesure de l'exploitation du système et fonction de l'évolution des risques.

L'analyse de risque consiste à :

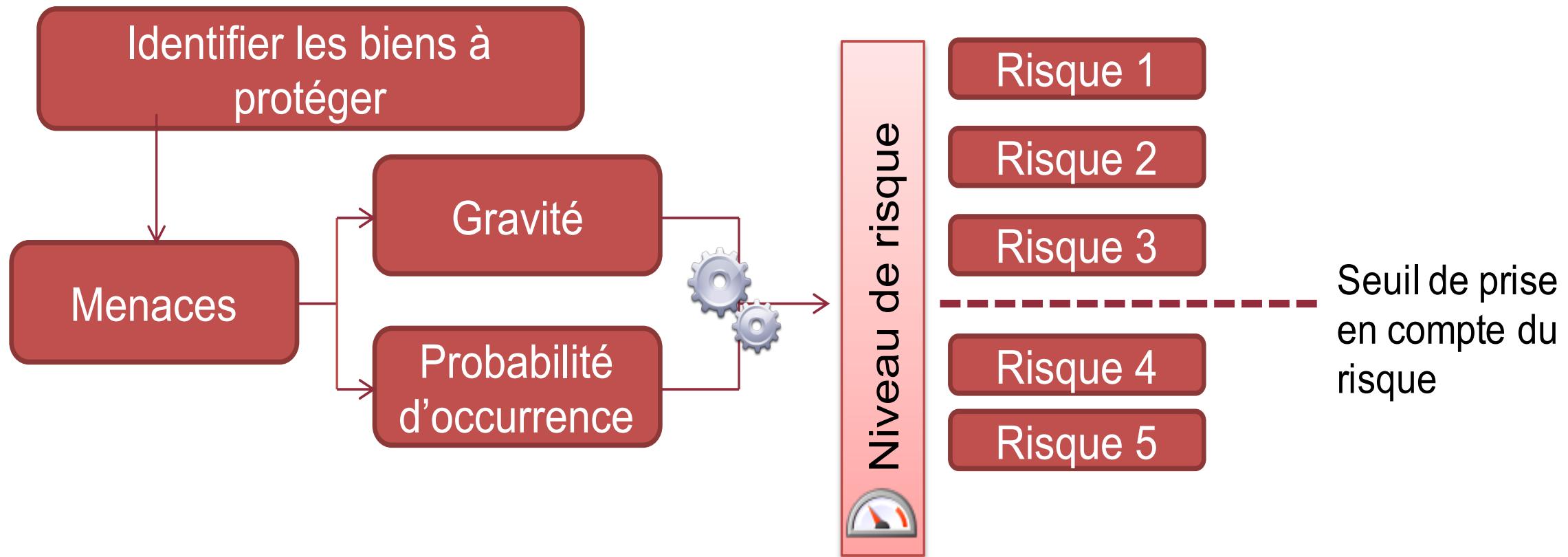
- identifier les biens à protéger,
- analyser de la fréquence et la gravité du danger pour évaluer la criticité du risque,
- établir une hiérarchisation des risques : fréquence vs gravité,
- établir un seuil d'acceptabilité pour chacun de ces risques,
 - seuil au-delà duquel le risque doit être pris en compte par les mesures de sécurité.
- identifier des mesures de sécurité.

Les mesures ainsi identifiées peuvent constituer un cahier de charges sécurité pour le projet qui soit réalisé en interne ou externalisé.

2. Intégrer la sécurité au niveau du projet

Différentes approches d'intégration

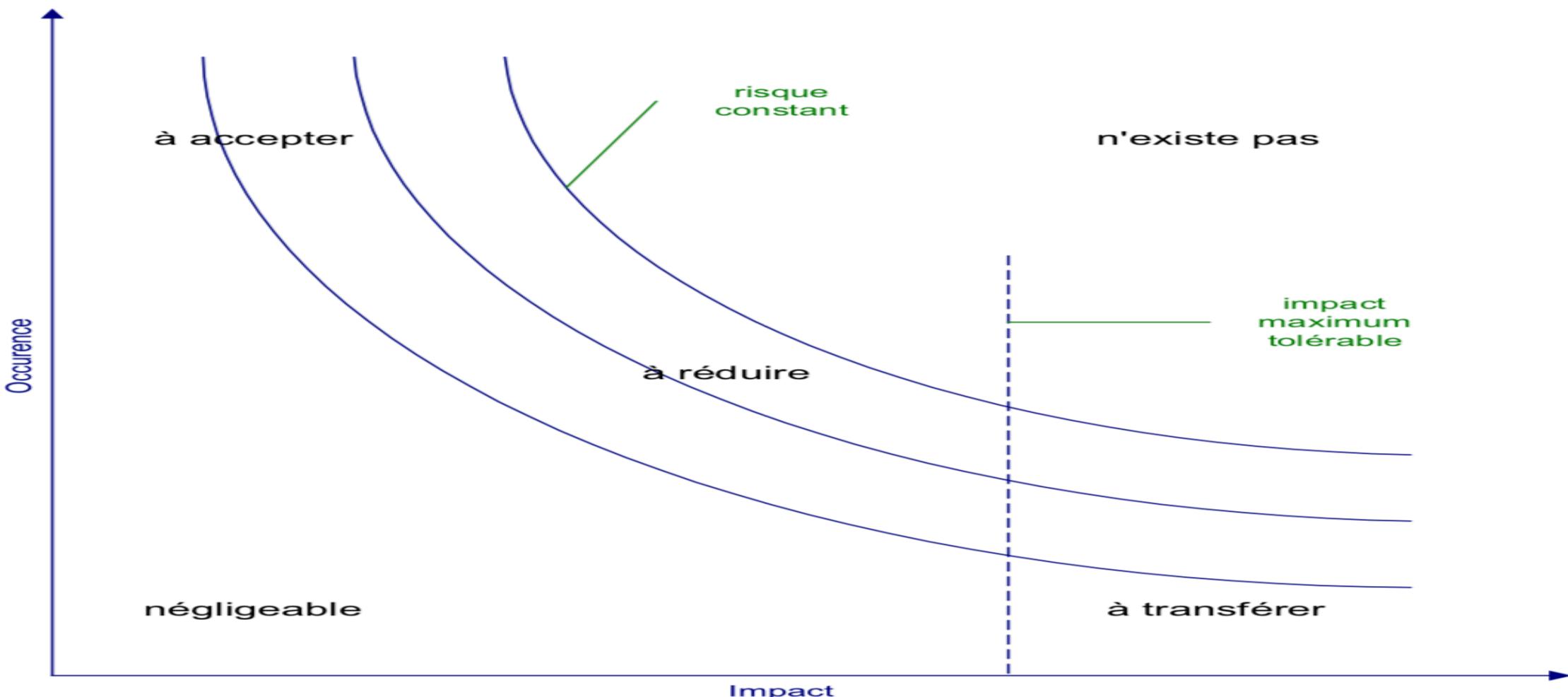
- L'approche par l'analyse et le traitement du risque



2. Intégrer la sécurité au niveau du projet

Différentes approches d'intégration

- L'approche par l'analyse et le traitement du risque (zones de risque)



2. Intégrer la sécurité au niveau du projet

Différentes approches d'intégration

- **Plan d'action du SSI**

Le défi vis-à-vis de la mise en place des mesures de sécurité est **asymétrique** entre « attaquer » et « défendre » :

- L'attaque peut réussir par l'exploitation d'une seule vulnérabilité ;
- Tandis que la défense doit prendre en compte l'ensemble du système.

Un plan d'action des mesures de sécurité à mettre en place à l'issue de l'analyse de risques devrait respecter le principe de « **défense en profondeur** » qui recommande :

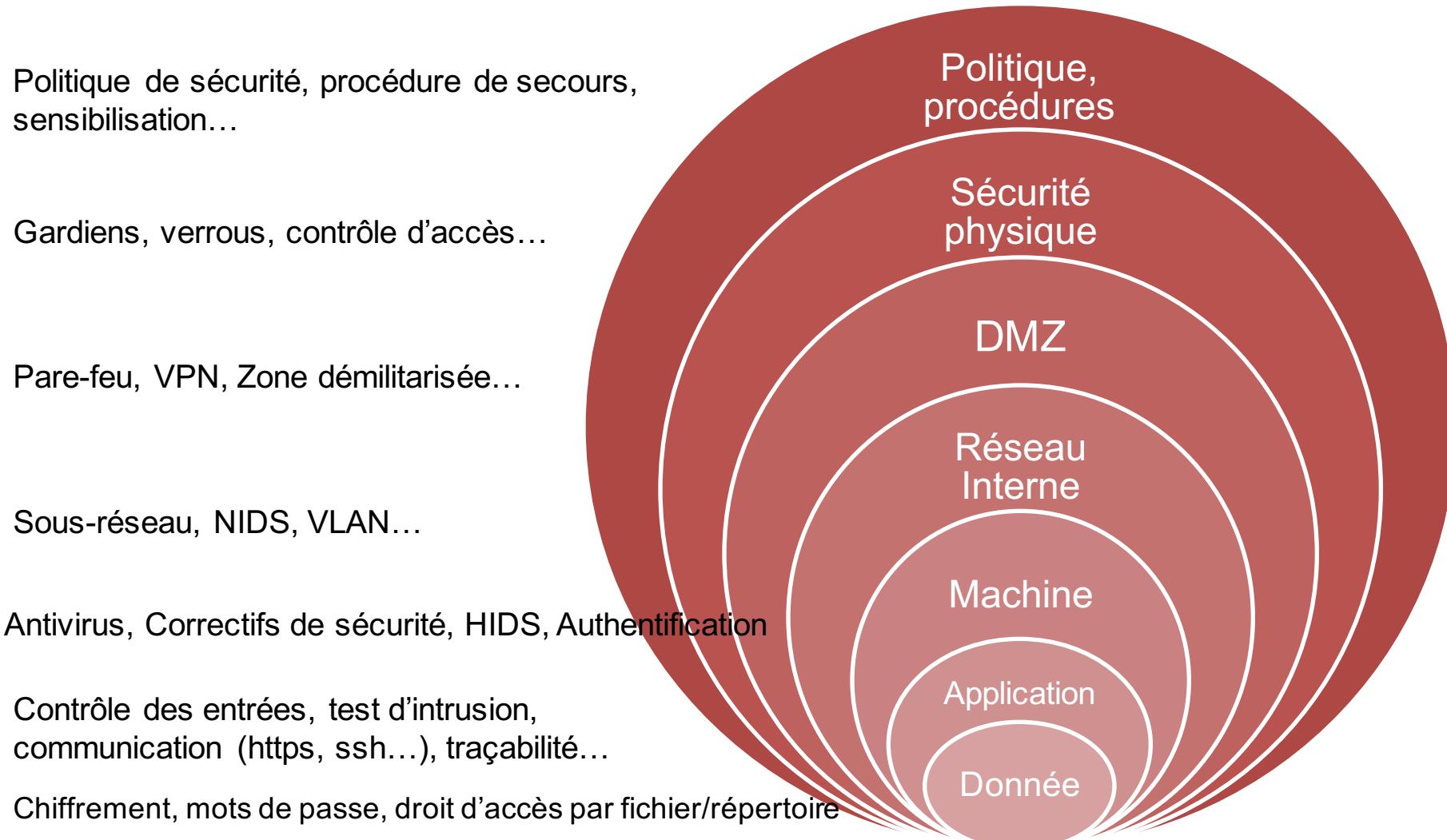
- d'avoir plusieurs lignes de défenses indépendantes ;
- que chaque ligne constitue une barrière autonome contre les attaques ;
- que la perte d'une ligne de défense implique qu'on passe à un niveau de défense plus fort.

Ce plan d'action est élaboré et décrit dans un document appelé « **politique de sécurité du système d'information (PSSI)** »

2. Intégrer la sécurité au niveau du projet

Différentes approches d'intégration

- Plan d'action du SSI



3. Politique de sécurité de système d'information (PSSI)

3. Politique de sécurité de système d'information (PSSI):

- ✓ Un **plan** d'actions définies pour maintenir un certain niveau de sécurité.
- ✓ L'ensemble des **orientations** suivies par une entité en termes de sécurité.
- ✓ Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information .

3. Politique de sécurité de système d'information (PSSI):

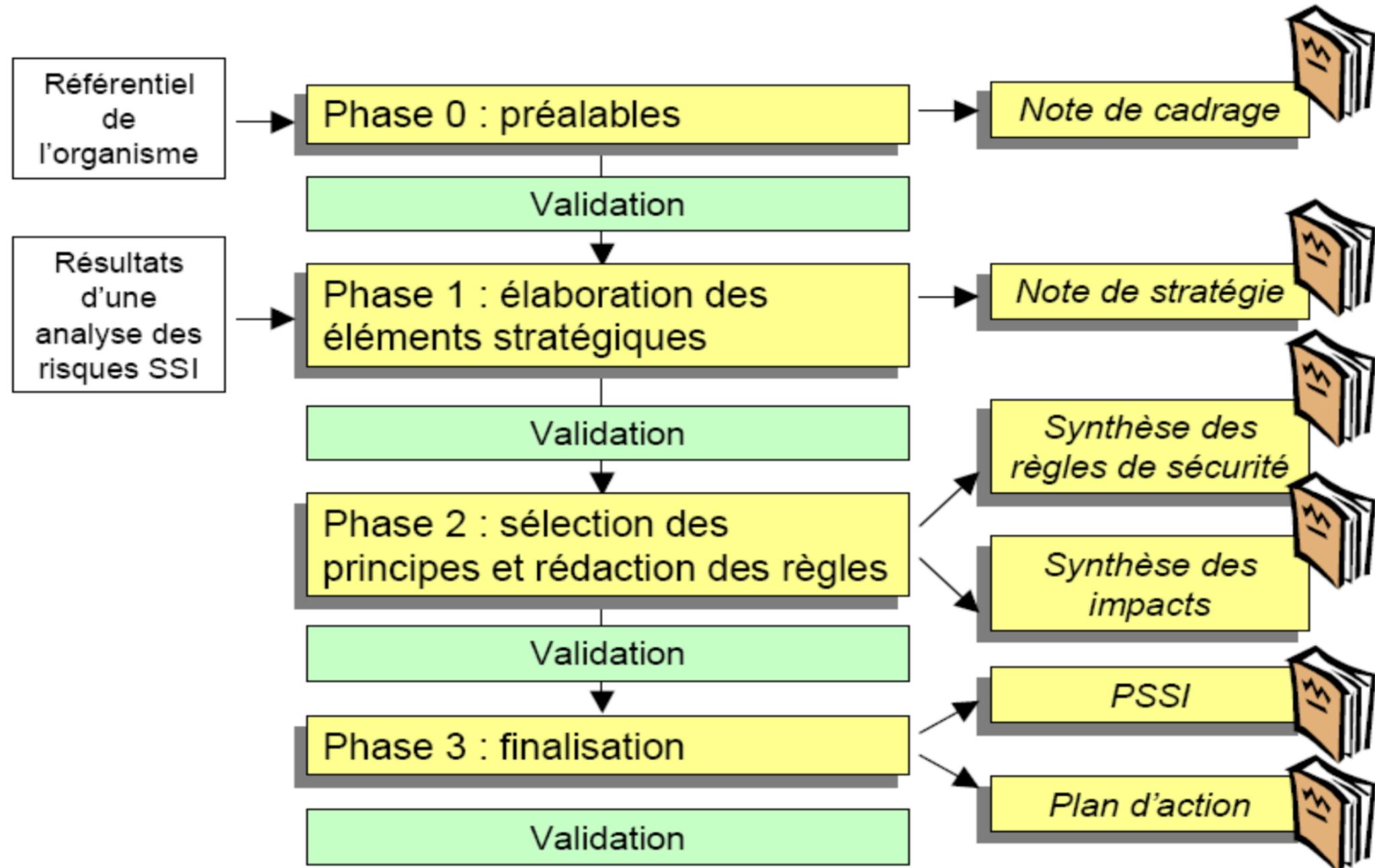
- ✓ La politique de sécurité des systèmes d'information est intrinsèquement liée à la sécurité de l'information.
- ✓ Ne se limite pas à la sécurité informatique.
- ✓ Elle est généralement organisée autour de 3 axes majeurs:
 - physique des installations,
 - la sécurité logique du système d'information
 - la sensibilisation des utilisateurs aux contraintes de sécurité.
- ✓ Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités.

3. Politique de sécurité de système d'information (PSSI):

méthodologie d'élaboration de PSSI:

- ✓ La démarche se base sur:
 - Le **référentiel de l'organisme** :schéma directeur, meilleures pratiques, directives internes...
 - Une **analyse des risques**
- ✓ L'objectif de la méthode consiste à construire un **document** de politique comprenant des **éléments stratégiques** et des **règles de sécurité** pour l'organisme étudié.
- ✓ Les règles de sécurité : définissent les moyens et les comportements définis dans le cadre de la PSSI.

3. Politique de sécurité de système d'information (PSSI):



PSSI (phase 0): préalables

Objectifs de la phase <p>Définir les objectifs et moyens à mettre en œuvre pour l'élaboration de la PSSI et constituer le référentiel documentaire.</p>	
Acteurs de la phase <ul style="list-style-type: none">- Le responsable sécurité ou l'initiateur du projet PSSI	
Éléments en entrée <ul style="list-style-type: none">- Référentiel de l'organisme	Éléments en sortie <ul style="list-style-type: none">- Note de cadrage- Référentiel documentaire
Tâches <ol style="list-style-type: none">1. Décrire l'organisation du projet2. Constitution du référentiel documentaire	
Observations <p>Cette phase doit permettre à la Direction générale de prendre la décision de lancement de l'opération sur la base d'un cadre formalisé d'intervention définissant les objectifs et moyens à mettre en œuvre.</p>	
Validation	
Documents	Validateur
Note de cadrage	Hiérarchie au plus haut niveau, par défaut la Direction Générale

PSSI (phase 0): tache 1 - Organisation du projet

- ✓ consiste à définir l'organisation du "projet PSSI" afin d'élaborer le cadre de réalisation.
- ✓ Démarche:
 - nommer un chef de projet.
 - constituer un comité de pilotage.
 - constituer un groupe d'experts.
 - attribuer un budget.
 - formaliser des objectifs détaillés.
 - établir un calendrier.

PSSI (phase 0): tache 2 - Constitution du référentiel

- ✓ Identifier le référentiel documentaire de l'organisme.
- ✓ Démarche sert à construire:
 - Aspects légaux et réglementaires.
 - Grands principes d'éthique.
 - Le référentiel de sécurité interne.
 - Obligations contractuelles engagé par l'organisme vis à vis de ses clients ou partenaires spécifiques.

PSSI (phase 1): élaboration des éléments stratégiques

Objectifs de la phase <p>Cette phase, dont les résultats et conclusions doivent impérativement être validés par la Direction Générale, consiste à déterminer les axes stratégiques et les premières grandes orientations à partir desquelles sera déclinée la PSSI. Pour cela, elle doit obligatoirement identifier et prendre en compte le périmètre d'étude, le contexte, les enjeux et orientations stratégiques, le référentiel réglementaire, l'échelle de besoins, les besoins de sécurité des biens à protéger et les origines des menaces afin d'aboutir à une note de stratégie validée par la Direction fixant les grandes orientations de la SSI.</p>	
Acteurs de la phase <ul style="list-style-type: none">- Chef de projet- Représentants de la maîtrise d'ouvrage- Direction Générale- Responsable juridique	
Éléments en entrée <ul style="list-style-type: none">- Référentiel documentaire	Éléments en sortie <ul style="list-style-type: none">- Note de stratégie de sécurité
Tâches <ol style="list-style-type: none">1. Délimitation du périmètre2. Identification des enjeux et orientations stratégiques3. Recensement des lois et règlements applicables4. Définition d'une échelle de besoins en termes de disponibilité, intégrité, confidentialité et éventuellement d'autres critères de sécurité5. Expression des besoins de sécurité des biens à protéger6. Identification des origines des menaces pesant sur l'organisme ou le système étudié (et éventuellement des principaux risques et objectifs de sécurité)	
Observations <p>Il convient d'insister sur l'importance capitale de cette phase et sur la nécessité d'une implication forte de la Direction Générale tant lors de l'identification des besoins et menaces que lors de la validation de la cible et des principaux objectifs à atteindre.</p>	
Validation	
Document	Validateur
Note de stratégie de sécurité	Comité de pilotage puis Direction générale

PSSI (phase 1): tache 1 - Définition du périmètre

- ✓ Décrire les domaines d'activités à couvrir et à affiner le périmètre, notamment les échanges entre les domaines et l'extérieur du périmètre
- ✓ Démarche:
 - lister l'ensemble des domaines d'activités jouant un rôle dans le système
 - sélectionner et décrire les domaines d'activités essentiels au fonctionnement de l'organisme.
 - identifier ceux qui constituent le périmètre de la PSSI et ceux qui en sont exclus.

PSSI (phase 1): tache 2 - Détermination des enjeux et orientations stratégiques

- ✓ présenter les enjeux et orientations stratégiques liés au périmètre de la PSSI.
- ✓ Démarche: prendre en compte
 - la contribution du système d'information à la qualité du service rend
 - la satisfaction des contraintes externes ;
 - la rentabilité économique du projet ;
 - les contraintes (techniques, financières, d'environnement...) et exigences (techniques ou organisationnelles) de l'organisme et du système d'information.

PSSI (phase 1): tache 3 - Prise en compte des aspects légaux et réglementaires

- ✓ présenter l'ensemble du référentiel légal, réglementaire et contractuel applicable au périmètre de la PSSI.
- ✓ Démarche: il est nécessaire de prendre en compte l'ensemble des éléments issus majoritairement du référentiel identifié dans la phase préalable
 - aspects légaux et réglementaires ;
 - grands principes d'éthique ;
 - obligations contractuelles ;
 - obligations contractuelles des prestataires ou partenaires ayant un impact sur le périmètre de la PSSI.

PSSI (phase 1): tache 4 - Elaboration d'une échelle de besoins

- ✓ définir une échelle de mesure utile à l'expression des besoins de sécurité pour les domaines d'activités identifiés.
- ✓ Démarche:
 - sélectionner les critères de sécurité à prendre en compte (disponibilité, l'intégrité et la confidentialité). par exemple: une échelle de confidentialité comme suit:

échelle	désignation
0	public
1	restreint
2	confidentiel avec les partenaires
3	confidentiel et interne
4	secret

PSSI (phase 1): tache 5 - Expression des besoins de sécurité

- ✓ identifier de manière générale les besoins de sécurité associés à chaque domaine d'activités
- ✓ Démarche: exploiter les résultats des étapes précédentes
 - la liste des domaines d'activités (et éventuellement des fonctions et informations) définissant le périmètre de la PSSI.
 - la liste des critères de sécurité retenus .
 - l'échelle de besoins (impacts et valeurs de référence).

PSSI (phase 1): tache 6 - Identification des origines des menaces

- ✓ identifier et caractériser les origines des menaces qui pèsent sur le périmètre de la PSSI.
- ✓ Démarche:Les méthodes d'attaque retenues sont ainsi caractérisées :
 - Les critères de sécurité qui peuvent être affectés sont identifiés
 - Les éléments menaçants qui pourraient les employer peuvent et être caractérisés par :
 - un type.
 - une cause.
 - un potentiel d'attaque estimé.

PSSI (phase 2): sélection des principes et rédaction des règles

Objectifs de la phase <p>Le travail de cette phase consiste à sélectionner, concevoir, préparer, documenter et valider la déclinaison des principes généraux d'une PSSI et des choix stratégiques de l'organisme. Ce travail se traduit en l'élaboration d'un corpus de règles directement applicables.</p>	
Acteurs de la phase <ul style="list-style-type: none">- Direction générale- Comité de pilotage- Groupe d'experts	
Éléments en entrée <ul style="list-style-type: none">- Note de cadrage- Note de stratégie de sécurité	Éléments en sortie <ul style="list-style-type: none">- Note de synthèse justificative des choix de règles- Note de synthèse des impacts organisationnel et financier
Tâches <ol style="list-style-type: none">1. Sélection des principes2. Construction des règles3. Synthèse et validation	
Observations <p>Les points essentiels à prendre en compte sont la cohérence des règles, leur applicabilité et enfin l'auditabilité de l'ensemble.</p>	
Validation	
Documents	Validateur
Note de synthèse justificative des choix de règles Note de synthèse des impacts organisationnel et financier	Comité de pilotage puis Direction générale

PSSI (phase 2): tache 1 - Choix des principes de sécurité

- ✓ Sélectionner les principes de sécurité à utiliser.
- ✓ Démarche: un choix qui doit être effectuer sur la base de:
 - le référentiel du système d'information
 - la définition du périmètre de la PSSI
 - la liste de besoins de sécurité identifiés
 - la liste des origines de menaces retenues.

PSSI (phase 2): tache 2 - Elaboration des règles de sécurité

- ✓ Instancier les principes retenues en règles de sécurité en se basant sur les éléments déclarés dans la note de cadrage et celle de la stratégie.
- ✓ Démarche: découpage et affinage des principes afin de produire des règles qui doivent refléter:
 - la couverture des origines des menaces retenues.
 - les critères de sécurité (disponibilité, intégrité, confidentialité...) que les origines de menaces concernées peuvent affecter.

PSSI (phase 2): tache 3 - Elaboration des notes de synthèse

- ✓ consiste à synthétiser le travail déjà établi afin de le valider et finaliser le document de la PPSI.
- ✓ Démarche: élaborer une note de synthèse justifiant les principes choisis ainsi que la déclinaison des règles.
- ✓ Généralement, la note de synthèse est élaborée par le groupe des experts à destination du comité de pilotage qui, à son tours, après validation la propose à la direction générale.

PSSI (phase 3): finalisation

- ✓Conduire une étape ultime de validation de la PSSI et du plan d'action associé par la direction générale.

PSSI (phase 3): tache 1 - Finalisation et validation de la PSSI

- ✓ Produire un document descriptif de la PSSI et validé par l'hiérarchie
- ✓ Démarche: consiste à vérifier:
 - la cohérence des règles énoncées.
 - l'exhaustivité de la couverture des risques jugés comme significatifs.
 - la traduction complète de l'ensemble des principes et règles, jugés pertinents pour l'organisme et énoncés dans le référentiel .
 - l'applicabilité des exigences et règles en fonction des pratiques en vigueur au sein de l'organisme.

PSSI (phase 3): tache 2 - Elaboration et validation du plan d'action

- ✓ Assurer l'application de la politique sur le système étudié.
- ✓ Démarche: chaque responsable d'unité opérationnelle ainsi que le responsable de la sécurité doit construire un document descriptif d'un plan d'action permettant de citer les actions prioritaires, par rapport à l'existant, à implémenter
- ✓ La priorité est fixée pour s'assurer la prise en compte des risques les plus significatifs.
- ✓ Le plan d'action sera soumis pour validation au comité de sécurité chargé de la validation et de l'évolution de la politique.



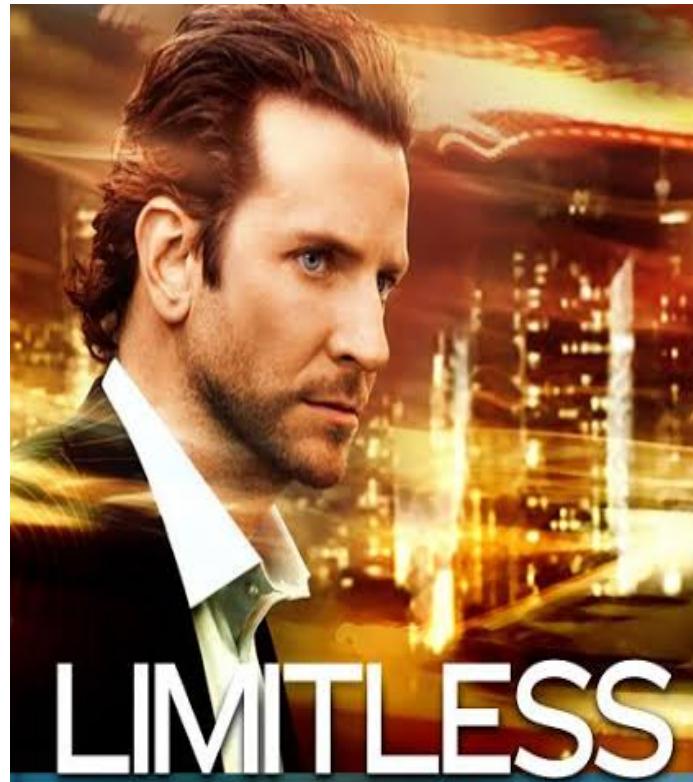
4. Difficultés liées à la prise en compte de la sécurité

4. Difficultés liées à la prise en compte de la sécurité

Une compréhension insuffisante des enjeux...

...liée à un problème d'éducation

L'information a une valeur importante pour l'entreprise, pour les concurrents, pour les États. On parle aujourd'hui de « guerre de l'information ».



4. Difficultés liées à la prise en compte de la sécurité

Une compréhension insuffisante des enjeux...

...liée à un problème de formation

- Des dirigeants qui n'ont pas tous une culture sécurité ;
- Des évolutions vers le poste de « RSSI », sans formation complémentaire adéquate
- Un coût lié à la sécurité qui rebute en période de crise



4. Difficultés liées à la prise en compte de la sécurité

Une compréhension insuffisante des enjeux...

...entraînant de nombreux risques pour l'entreprise ou pour l'organisation

- Perte d'informations essentielles ;
- Arrêt de la production ;
- Détérioration de l'image/réputation ;
- Risques juridiques/réglementaires...

...entraînant de nombreux risques pour les États

- Indisponibilité de services ;
- Perte de crédibilité ;
- Divulgation d'informations sensibles ;
- Risques de conflits avec d'autres États...

4. Difficultés liées à la prise en compte de la sécurité

L'implication nécessaire de la direction

Le chef d'entreprise doit être conscient des enjeux de sécurité pour l'avenir de son entreprise :

- Être **proactif** plutôt que réactif. La PSSI est une réflexion stratégique : Elle permet de prévoir l'avenir de l'organisation ;
- **Prendre le temps** de comprendre, ne pas être absorbé que par ses marchés, ses clients, ses concurrents, son relationnel ;

La sécurité :

- **va au-delà de la technique.** L'humain joue un rôle central ;
- **ne doit pas rester un domaine d'experts.** La sécurité est l'affaire de tous et une préoccupation de tous les responsables ;
- n'est pas seulement une contrainte coûteuse mais **elle est aussi un investissement**, un atout supplémentaire pour l'organisation.

4. Difficultés liées à la prise en compte de la sécurité

Difficulté pour faire des choix en toute confiance

Il est important de faire des choix éclairés en prenant en compte la sécurité.



Vie privée : La NSA s'octroie un backdoor dans tous les systèmes Windows



4. Difficultés liées à la prise en compte de la sécurité

Difficulté pour faire des choix en toute confiance

Il est important de faire des choix éclairés en prenant en compte la sécurité.

Quels sont aujourd’hui les matériels ou logiciels de confiance ?

- Ceux issus de l’industrie nationale vs ceux de nos partenaires de confiance : alliés, fournisseurs ;
- Ceux issus du monde libre (« open source ») ;
- Les matériels qualifiés par l’ANSSI (ARPT en Algérie).

Quels sont les organismes de confiance ?

- Les entreprises nationales ou européennes (mais qui sont les actionnaires) ;
- Nos partenaires de longue date ;
- Les autorités gouvernementales ;
- Les prestataires de service qualifiés par l’ANSSI (ARPT en Algérie).

4. Difficultés liées à la prise en compte de la sécurité

Le délicat équilibre entre productivité et sécurité

Authentification requise pour chaque application dans l'entreprise

- Problème pour l'utilisateur : « J'ai besoin de travailler chaque jour avec 5 applications et je dois à chaque fois y saisir un mot de passe différent ».
- Réaction pour l'utilisateur : « Je note certains mots de passe sur papier ».

Utiliser une application de chiffrement pour partager les fichiers chiffrés avec des partenaires

- Problème pour l'utilisateur : l'interface de Crypt&Share n'est pas ergonomique.
- Réaction de l'utilisateur : « Je vais utiliser Box ou DropBox pour partager les informations avec mes partenaires ».

Les informations classifiées au niveau 4 (niveau de sensibilité le plus élevé) ne doivent pas sortir du S.I.

- Problème pour l'utilisateur : J'ai besoin de l'avis d'un prestataire extérieur sur certaines informations de niveau 4.
- Réaction de l'utilisateur : Déclassification des informations de manière à ne jamais avoir de niveau 4 mais uniquement des niveaux 3 ou 2.

4. Difficultés liées à la prise en compte de la sécurité

Le délicat équilibre entre productivité et sécurité

- **Écouter les utilisateurs** et prendre en compte leurs besoins lors de l'étude de solutions de sécurité :
 - Proposer des mesures en concertation et avec l'adhésion des utilisateurs concernés autant que possible ;
 - **Former les utilisateurs** pour les aider à prendre en main les nouveaux outils et à bien appliquer les mesures.
- **Tester les procédures**, dans le but d'évaluer son efficacité (applicabilité, réalisation des objectifs, risques encourus) :
 - Éviter de multiplier les moyens de protection si ceux-ci ne sont pas respectés ;
 - il faut parfois investir moins dans la sécurité mais avoir des procédures efficaces.
- **Confier la responsabilité de la sécurité à un collaborateur** qui a le pouvoir ou les ressources pour la faire appliquer.
- Choisir les solutions les plus adaptées à **sa propre structure**, à **son fonctionnement**, au niveau de maturité l'entreprise.

Cartographie des métiers et compétence en SSI

Phases

Étude

Conception

Implémentation,
déploiement

Exploitation /
Maintenance

Gestion des
incidents, des crises

Métiers

Ingénieur de sécurité, architecte de sécurité, développeur de sécurité,

Auditeur organisationnel

Auditeur technique

RSSI, Technicien support

Consultant

Analyste dans un SOC

Investigateur numérique