Cybersécu

Notions générales:

- Principes de Peter: Selon ce principe, « dans une hiérarchie, tout employé a tendance à s'élever à son niveau d'incompétence », avec pour corollaire que « avec le temps, tout poste sera occupé par un employé incapable d'en assumer la responsabilité »
- KISS: Keep It Simple, Stupid → ligne directrice de conception qui préconise la simplicité dans la conception et que toute complexité non indispensable devrait être évitée dans toute la mesure du possible
- SMART: Specific, Measurable, Achievable, Relevant and Time-bound, en français spécifique, mesurable, atteignable, réaliste et temporellement défini
- Fast-Good-Cheap: cout qualité délais. Il n'est pas possible de faire vite, bien, et pas cher. Seulement deux objectifs peuvent être atteints.
- Matrice d'Einshower: Outil de priorisation des tâches selon important/pas important, urgent/pas urgent: A faire, A planifier, A déléguer, A abandonner
- Loi de Pareto: encore loi des 80-20, est une observation selon laquelle environ 80 % des effets sont le produit de seulement 20 % des causes
- Rationalité limitée: idée selon laquelle la capacité de décision d'un individu est altérée par un ensemble de contraintes comme le manque d'information, des biais cognitifs ou encore le manque de temps.

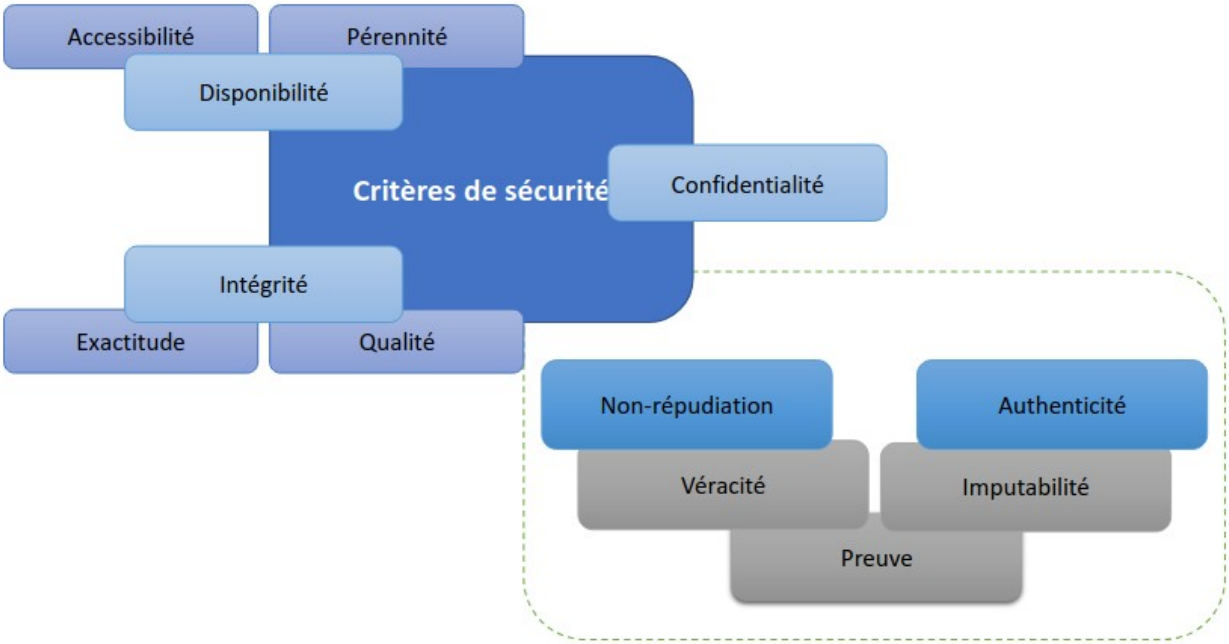
Lexique:

DIC → Disponibilité, Intégrité, Confidentialité
CNIL → Commission nationale de l'informatique et des libertés
RGPD → Règlement Général sur la Protection des Données
ANSSI → Agence Nationale de la Sécurité des Systèmes d'Information
DPO → Data Protection Officer, délégué à la protection des données
RSSI → Responsable sécurité des systèmes d'information
PSSI → Politique de sécurité des systèmes d'information
CTI → Cyber Threat Intelligence, activité liée à la collecte d'informations sur les menaces ou les acteurs de la menace
DPI → Droit de Propriété Intellectuelle
LIO → Lutte Informatique Offensive
LID → Lutte Informatique Défensive
L2I → Lutte Informatique d’Influence
LPM → Loi de Protection Militaire
SMSI → Système de Management de la Sécurité de l'Information
SSI → Sécurité des Systèmes d'Information
PTR → Plan de Traitement du Risque
TI → Technologies de l'information

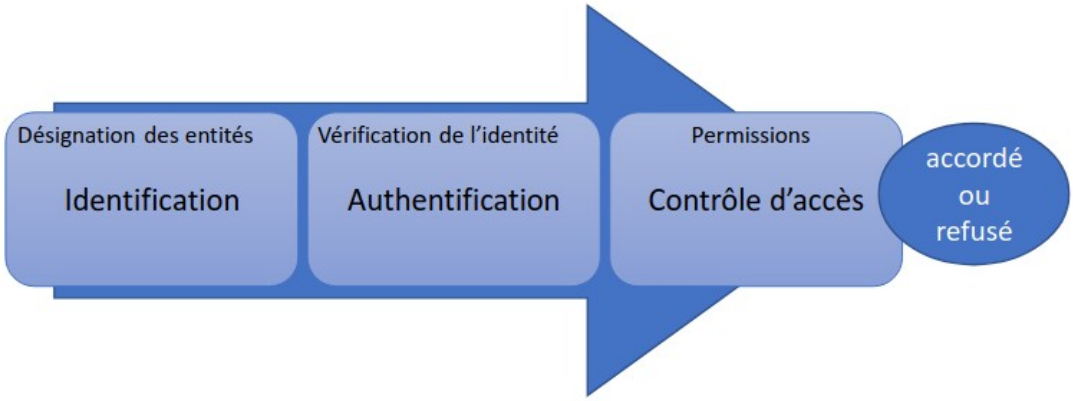
Séance 1:

Ecosystème:

Critères de base des objectifs de sécurité (DIC) → Disponibilité, Intégrité, Confidentialité

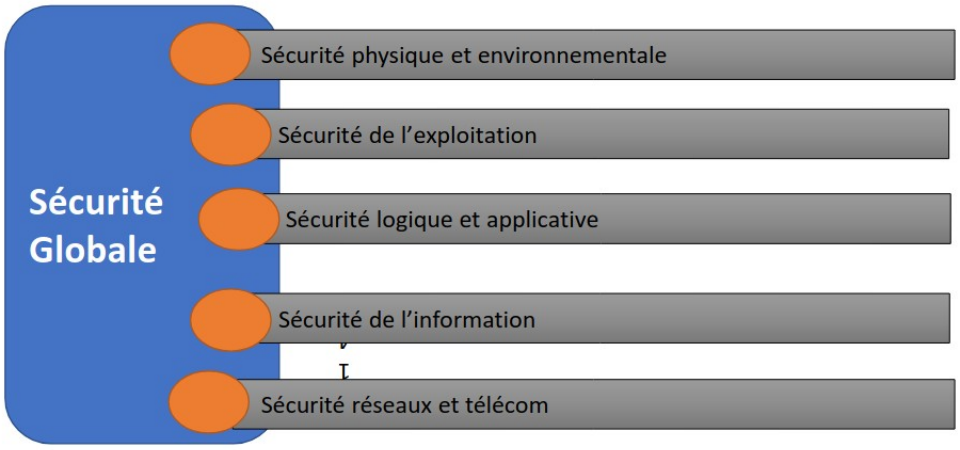


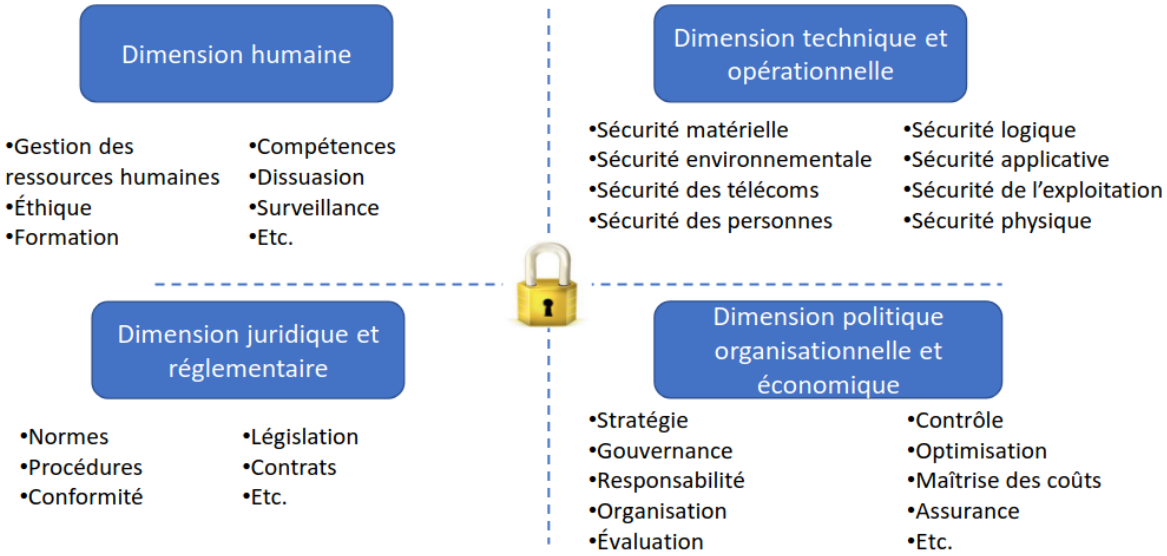
Non-répudiation → fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu



Cyberespace → Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. (autre nom d'internet)
Cybersécurité → État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.
Cyberdéfense → Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

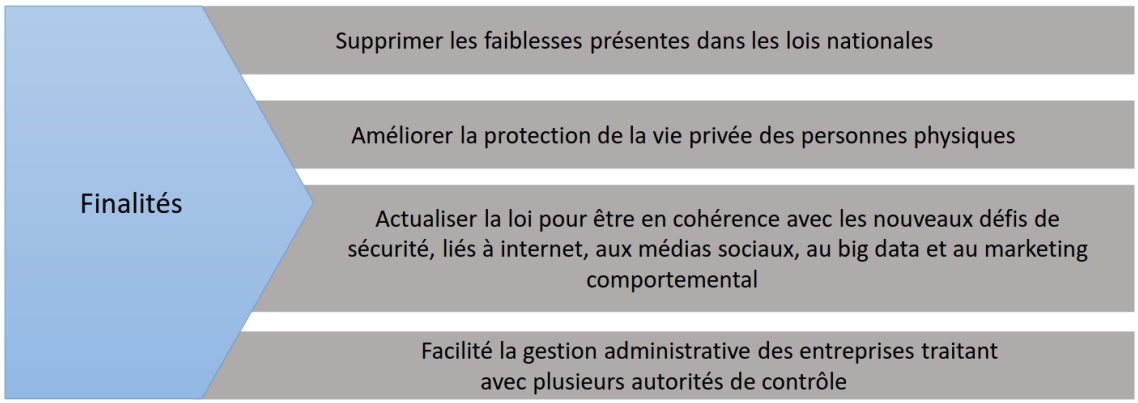
Sécurité informatique d'une entreprise assurée par une politique de sécurité, motivation et formation du personnel, mise en place de mesures proactives et réactive, mesure de sécurité par les axes managériaux, juridiques et techniques





Identité numérique:

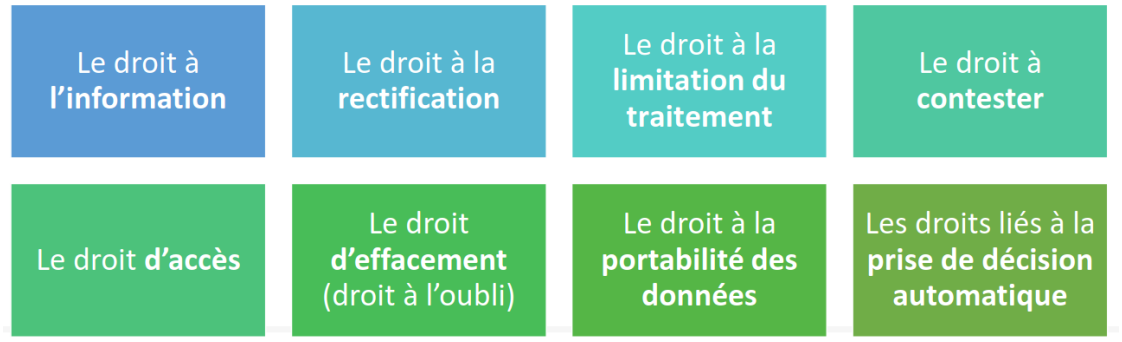
Les rares textes législatifs ou réglementaires qui font référence à l'identité numérique ne traitent en définitive que de la notion de « données personnelles »
En France c'est la CNIL qui protège les données à caractère personnel
Ce n'est pas un droit constitutionnel
RGPD énumère des exigences précises concernant la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et à la libre circulation de ces données



Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Le RGPD a identifié six principes à appliquer lors de la collecte ou du traitement des données, mentionnés au chapitre II du RGPD :

Droits accordés par le RGPD aux personnes concernées :



Séance 2:

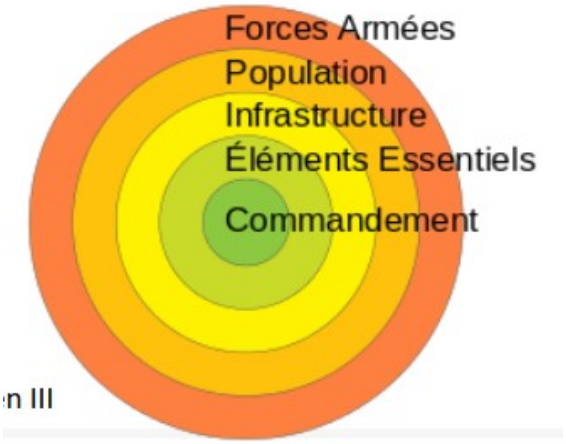
Intelligence économique, géopolitique

IE → Intelligence collective, maîtrise protection et exploitation de l'information
Cycle de l'information → détection, collecte, exploitation, diffusion. La veille englobe toutes ces étapes

Analyse PESTEL → politique, économique, sociologique, technologique, environnemental, légal. Groupes de forces macro-environnementales susceptibles d'influer sur les activités d'une organisation
Analyse SWOT → Strengths (forces), Weaknesses (faiblesses), Opportunities (opportunités), Threats (menaces). Positionne l'organisation dans son environnement global d'une manière plus dynamique
Cinq forces de Michael Porter → acteurs à surveiller parmi les concurrents directs, les nouveaux entrants, les fabricants de produits de substitution, les clients, les fournisseurs

Le niveau de protection de l'ensemble est égal à son élément le moins protégé.
Agir sur l'attitude et le comportement du public: La méthode employée pour façonner l'opinion se nomme «relations publiques».
Processus d'influence: identification des cibles → définition du message et identification des relais → choix du moment d'action → surveillance et ajustement

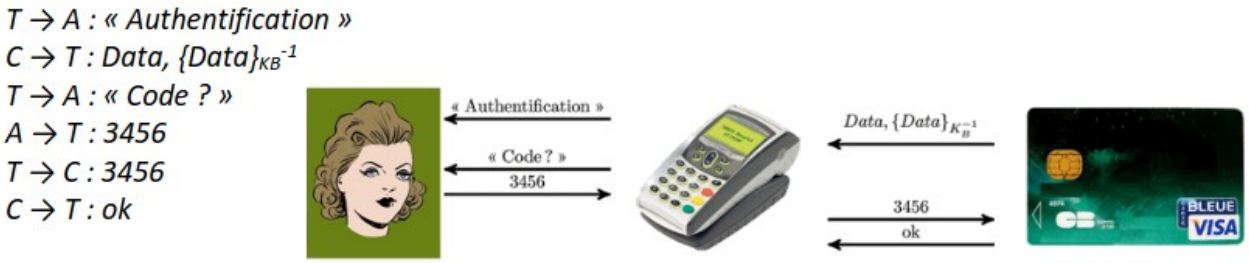
Théorie des cinq cercles de John A.Warden: le cyberespace lie les 5 cercles et donc les attaques cyber permettent d'atteindre la capacité à prendre des décisions sans action physique

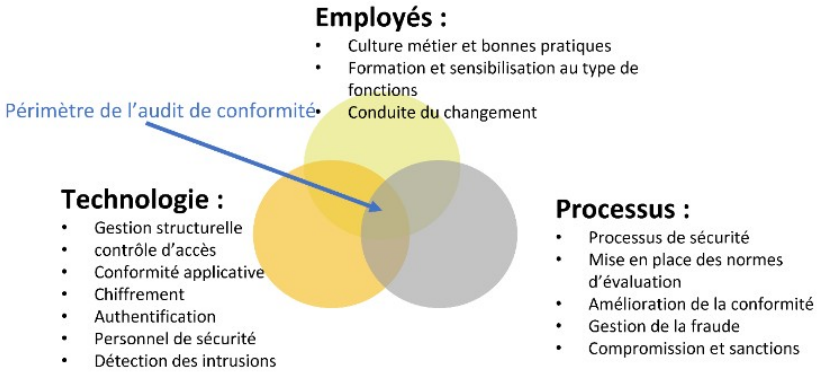


Obligations normatives, réglementaires et juridiques

NIS : Network and Information System Security. Répond aux enjeux: gouvernance, coopération, cybersécurité des OSE, cybersécurité de FSN
OSE → Opérateur de Service Essentiel
FSN → Fournisseur de Service Numérique
ENISA → Agence de l'union européenne pour la cybersécurité
OIV → Opérateurs d'Importance Vitale
Les OSE doivent garantir un socle minimal en termes de cybersécurité. Doit déclarer un responsable auprès de l'ANSSI, identifier ses systèmes d'informations essentiels, appliquer les

règles de sécurité dans les délais impartis, signaler les incidents, être soumis à des contrôles de sécurité
Les FSN doivent signaler les incidents et êtres soumis à des contrôles de sécurité
RGS → Référentiel Général de Sécurité fourni une méthodologie, des règles et bonnes pratiques
Entreprises, clauses de cybersécurité: engagements relatifs à la formation régulière du personnel en matière de sécurité des systèmes d'information, liste d'exigences techniques et engagement sur un niveau de sécurité précis (ex : respect de standards, normes, mise en œuvre de pratiques identifiées, etc.), règles de gestion et de notification des incidents (délais, coopération).
Clé de Luhn → En mathématiques et plus précisément en arithmétique modulaire, la formule de Luhn est utilisée pour ses applications en cryptologie. L'algorithme de Luhn, ou code de Luhn, ou encore formule de Luhn est aussi connu comme l'algorithme « modulo 10 » ou « mod 10 ». C'est une simple formule de somme de contrôle utilisée pour valider une variété de numéros de comptes, comme les numéros de cartes bancaires, les numéros d'assurance sociale canadiens, les numéros IMEI des téléphones mobiles ainsi que pour le calcul de validité d'un numéro SIRET.
PCI-DSS → La norme de sécurité des données de l'industrie des cartes de paiement



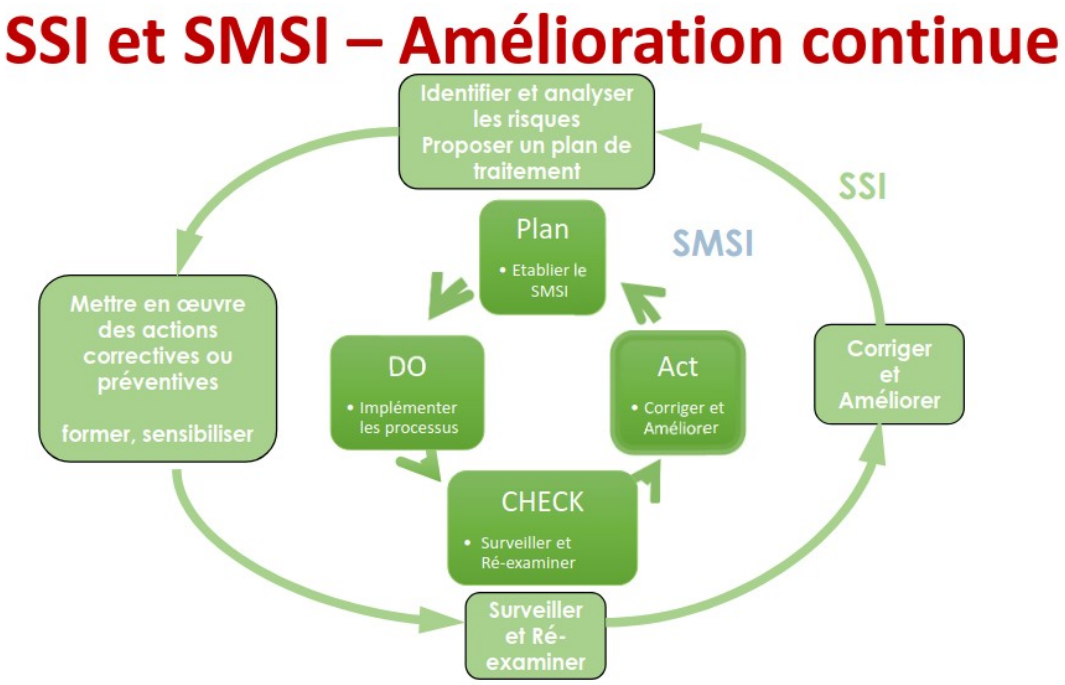


Référentiel de sécurité PCI-DSS

Séance 3:

Norme ISO 27000

Norme de sécurité de l'information
La sécurité est un processus
Les décisions doivent être prises au plus haut niveau
Norme ISO 27001 management de la sécurité et sécurité. Convient à toutes les organisations
PDCA → Modèle de gouvernance Plan → Do → Check → Act



27000 Vue d'ensemble et vocabulaire, 27001 exigences, 27002 code de bonne pratique pour la gestion de la sécurité de l'information, 27003 lignes directrices pour la mise en oeuvre du SMSI, 27004 management de la sécurité de l'information - mesurage, 27005 gestion des risques liés à la sécurité de l'information, 27006 audit de certification

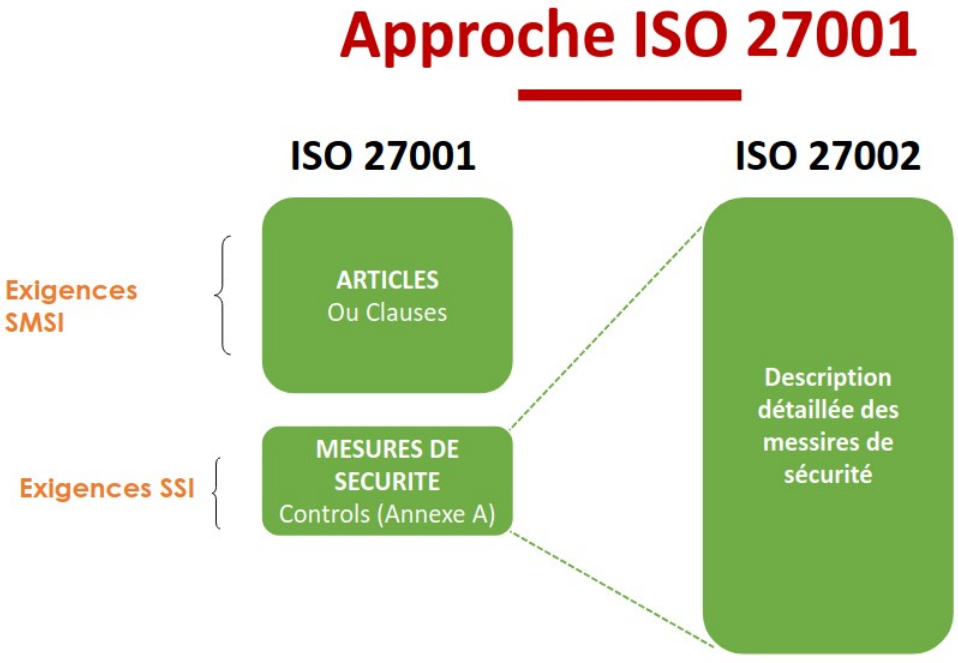
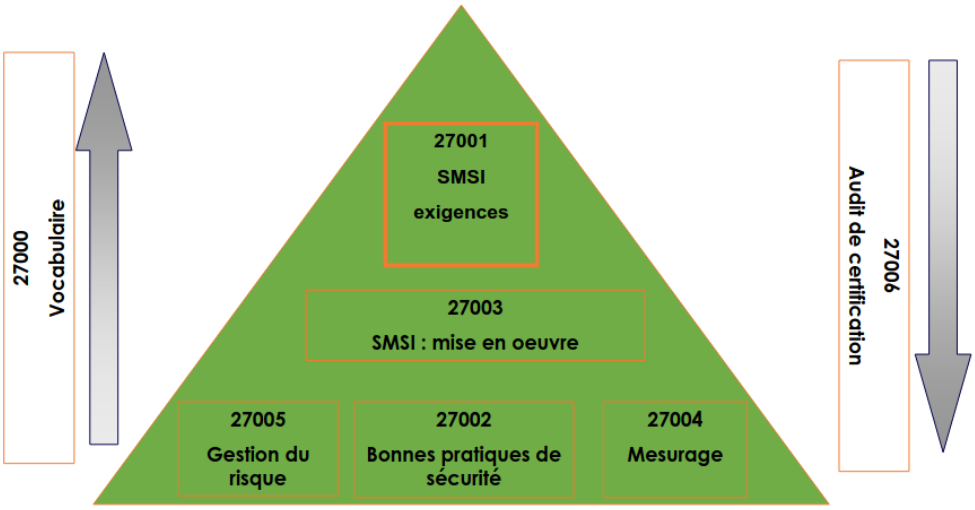
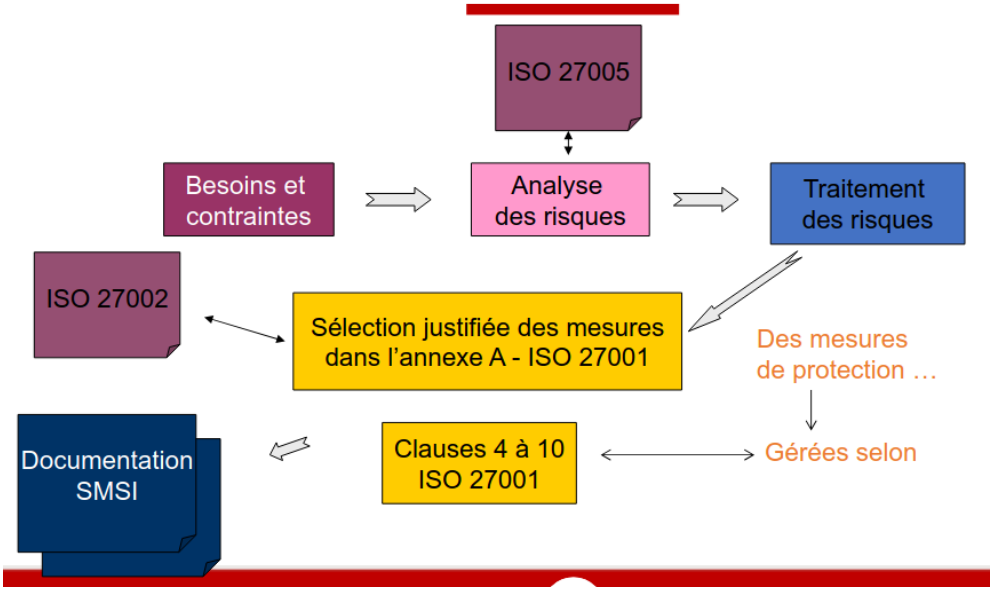


Schéma du positionnement des normes



Estimer le risque (probabilité, impact, gravité) et priorisation, les biens, les vulnérabilités, les actions déjà en place, les acteurs, ce qui est acceptable (acceptation). Evolution permanente donc veille permanente
Tableau de bord SSI permet d'avoir une vision synthétique technique et fonctionnelle aux niveaux décisionnels, de pilotage et opérationnels

Démarche globale 27001



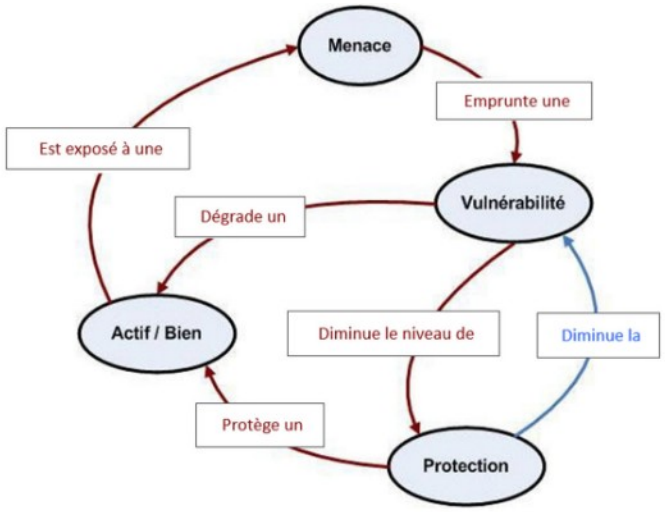
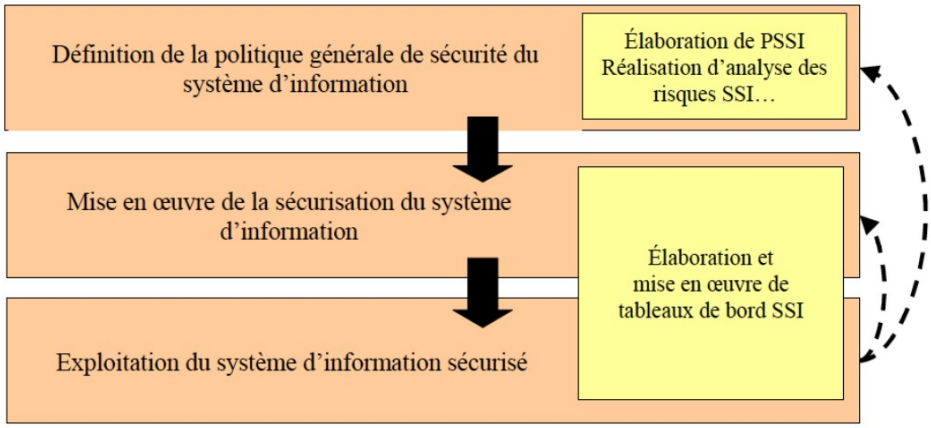


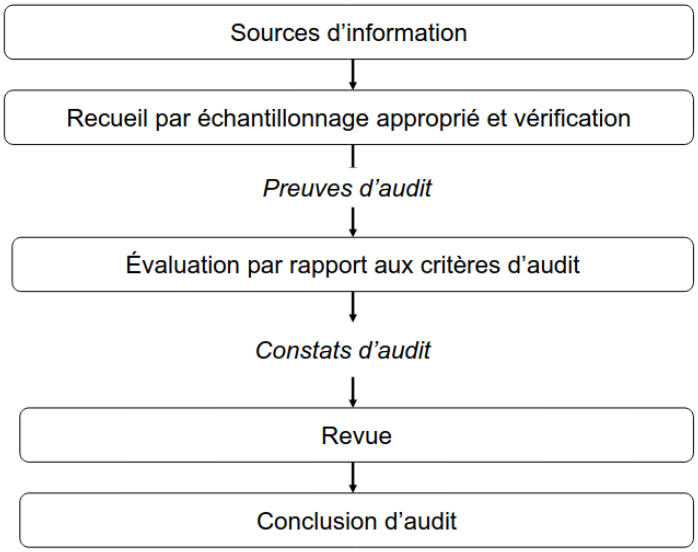
Diagramme de flux du Risque (Source AFAI)



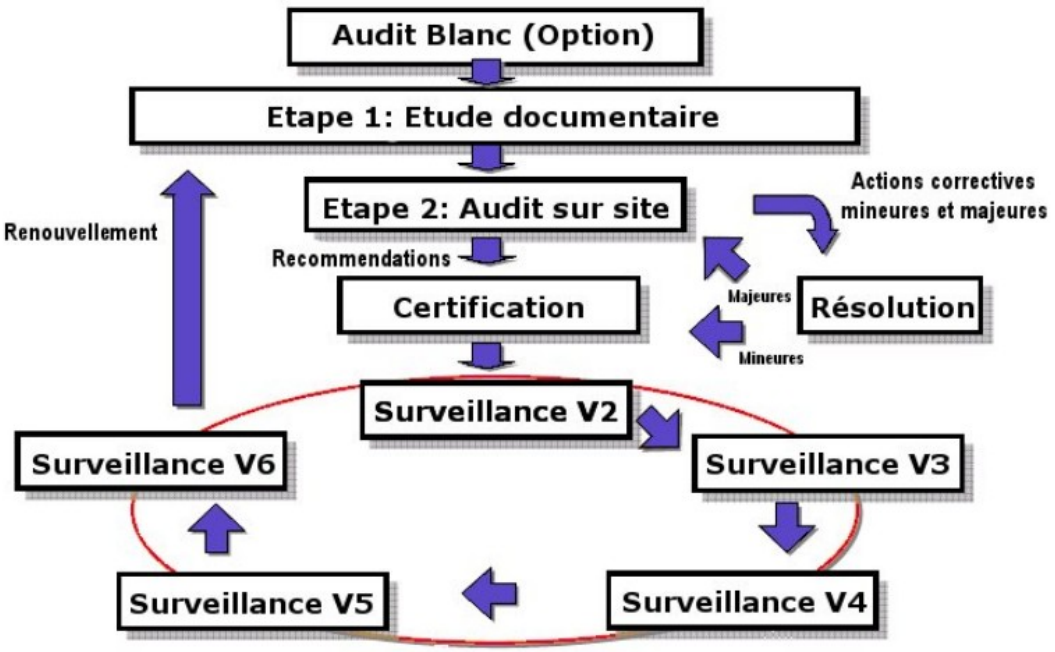
Audit :

Définition : Processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

De la source d'information à la conclusion



Certification ISO 27001



COBIT

Ensemble de recommandations et des process permettant d'évaluer les ressources informatiques qui s'inscrit dans une logique d'alignement et de maturité, par le contrôle et de l'audit. Outil largement utilisé dans la démarche d'IT Gouvernance.