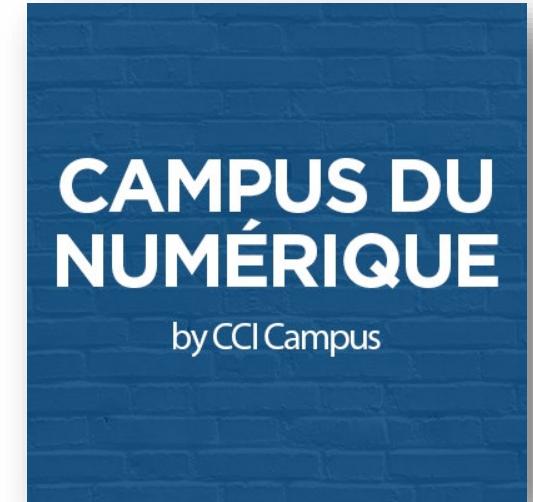


Manager en Ingénierie Informatique

- Management des Systèmes d'Information

Gabriel BETETA

gbeteta@ccicampus.fr



Gouvernance des Systèmes d'Information

1. Gouvernance
2. Les normes et les référentiels SI et des audits des systèmes d'information
3. SMSI
4. PSSI

La gouvernance informatique

Définition : La gouvernance des systèmes d'information consiste à fixer des objectifs pour orienter l'évolution du système d'information de l'entreprise et à contrôler son fonctionnement. Il s'agit de définir la manière dont le système d'information contribue à la création de valeur en lien avec la stratégie suivie et de mettre en place des dispositifs de contrôle (tableaux de bord, etc.).

Parmi les outils utilisés, **ITIL** (*IT Infrastructure Library*), **COBIT** (*Control Objectives for Information and related Technology*, contrôle de l'information et des technologies associées) et les normes **ISO 270xx** permettent d'assurer le contrôle du système d'information et de le faire évoluer en fonction de la stratégie de l'entreprise tout en tenant compte des besoins en sécurisation des systèmes et des données.

Pour optimiser la gouvernance, il faut :

- lever les facteurs de blocage au niveau des relations de pouvoir entre acteurs,
- définir la stratégie et en maîtriser l'exécution,
- mettre en place une structure avec des fonctions et des processus appropriés

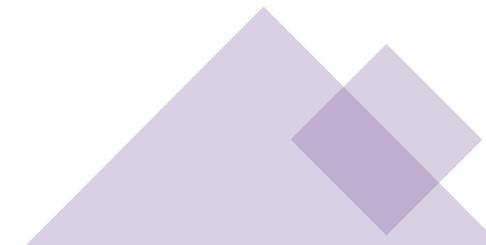
L'ISACA (*Information Systems Audit and Control Association*) définit 5 domaines fondamentaux de la gouvernance des SI :





Pour compléter ce tableau, il serait malvenu d'oublier les professionnels de l'informatique et des télécommunications qui sont souvent en position de « subir » les audits et qui, en général de culture « technique » ou « ingénieur », veulent voir prises en compte les « règles de l'art », c'est-à-dire souvent les contraintes de leur métier. Pour eux, le modèle est à rechercher chez les grands instituts de normalisation technique qui font avancer l'industrie tous les jours : l'*Institute of Electrical and Electronics Engineers* (IEEE) en est un exemple. L'Union internationale des télécommunications (UIT) toujours aussi active malgré son grand âge (elle fut créée en 1865 sous le nom de l'Union télégraphique internationale), est certainement l'exemple le plus abouti d'une coopération internationale qui débouche sur des normes qui sont utilisées tous les jours par tous sur tous les continents.

Mais l'informatique ce n'est pas seulement du « hard » (matériel) ou des échanges de messages électroniques, c'est aussi, et de plus en plus, du service et, dans ce domaine, le leadership de la normalisation a été pris depuis de nombreuses années par l'*International Organization for Standardization* ou Organisation internationale de normalisation (ISO), par exemple avec les célèbres normes ISO 9000 et suivantes.



1. Norme (source : Afnor)

C'est un référentiel élaboré en **consensus** par l'ensemble des acteurs d'un marché : producteurs, utilisateurs, laboratoires, pouvoirs publics, consommateurs etc., et reflétant l'état de la technique et des contraintes économiques à un moment donné.

La **norme** est un document **d'application volontaire et contractuelle**.

La **Directive 98/34/CE** indique que la **norme** est « *une spécification technique approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire* ».

2. Normalisation (source : Afnor)

Le processus de **normalisation** a pour objet la publication de normes et documents normatifs, aussi bien à l'échelle nationale, européenne ou internationale.

En France, le **décret n° 84-74 modifié** du ministère de l'industrie et de la recherche, fixant le statut de la **normalisation**, précise que :

« La **normalisation** a pour objet de fournir des documents de références comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux. »

Ce texte définit le système de normalisation français et en confie la gestion à l'Afnor (Association française de normalisation).

Afnor est le membre français des structures de normalisation internationale (ISO – Organisation internationale de normalisation) et européenne (CEN – Comité européen de normalisation).

3. Standard ou standardisation

Ces termes sont souvent utilisés comme synonymes de norme et normalisation du fait de l'origine anglo-saxonne de ces termes.

En revanche, pour beaucoup d'auteurs francophones, le « standard » n'a pas la reconnaissance officielle de la « norme ». Il doit être envisagé comme une « norme » de fait, qui a vocation à être validée par l'organisme en charge de la normalisation.

Pour les anglophones, seul le terme « standard » existe et recouvre les deux sens.

4. Référentiel

Un référentiel contient des informations de référence. Toute information identifiée comme information de référence doit obligatoirement faire l'objet d'une définition explicite permettant notamment :

- d'apporter une vision claire et précise du contour de cette information de référence (aucune ambiguïté ne doit exister sur les limites et le contenu de cette information de référence) ;
- une adhésion de tous sur la définition et le contour qu'elle porte (partage de la définition).

5. Certification

La certification est une reconnaissance écrite, par un organisme indépendant du fabricant ou du prestataire de service, de la conformité d'un produit, service, organisation ou personnel à des exigences fixées dans un référentiel. La certification doit être effectuée dans le cadre européen par un organisme accrédité. En France c'est le Comité français d'accréditation (Cofrac) qui délivre les accréditations.

Les accords multilatéraux dont le Cofrac est signataire facilitent les échanges des produits et des services : une accréditation obtenue en France est reconnue dans tous les pays signataires en Europe et dans le monde. L'État français reconnaît le Cofrac comme « instance nationale d'accréditation ».

6. Usages de la profession, état de l'art, règles de l'art...

Tous ces termes font référence à des pratiques professionnelles qui sont reconnues comme correctes et qui doivent assurer dans les métiers de services un niveau de prestation conforme aux attentes du client. Il est à noter que les tribunaux peuvent avoir à apprécier la conformité de cette « obligation de moyens » dans le cas d'un conflit client-fournisseur. Le rôle des instances professionnelles est donc important pour fixer ces usages. Le législateur confie d'ailleurs à certaines d'entre elles le soin de les rédiger (par exemple pour la profession réglementée d'avocat).

« Dans le respect des dispositions législatives et réglementaires en vigueur, le Conseil national des barreaux unifie par voie de dispositions générales les règles et usages de la profession d'avocat. »

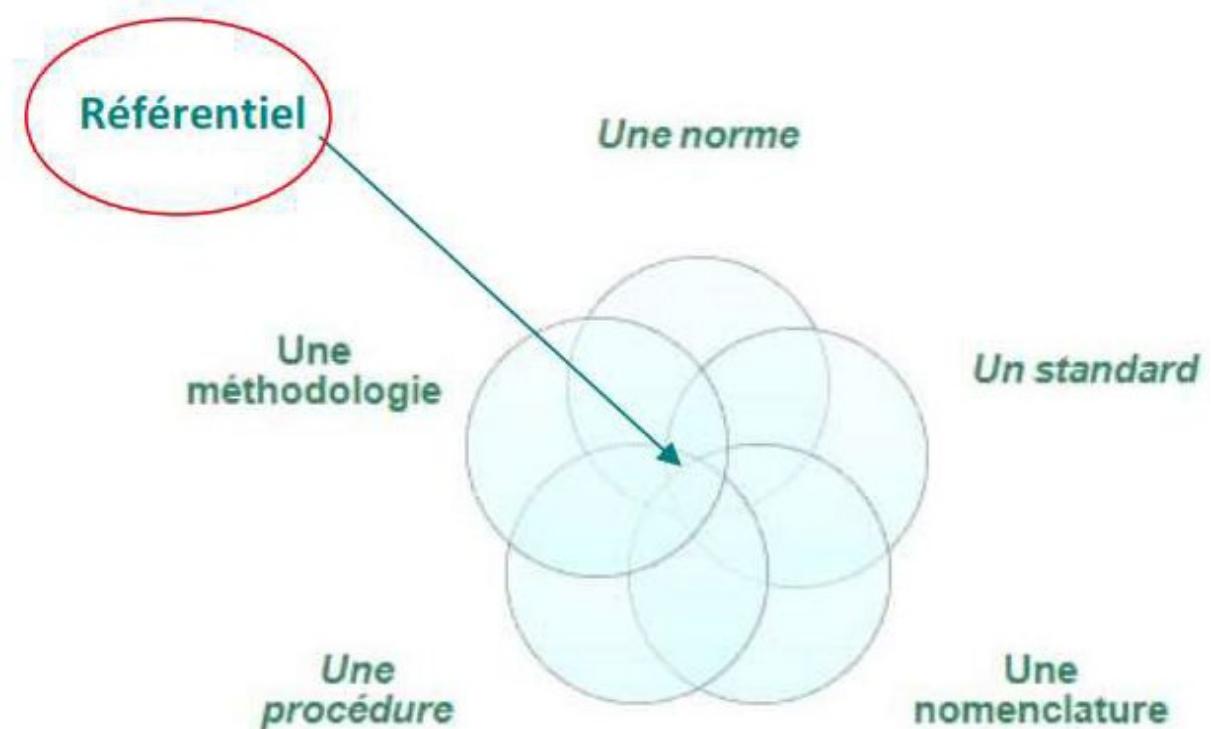
C. trav., art. 22.

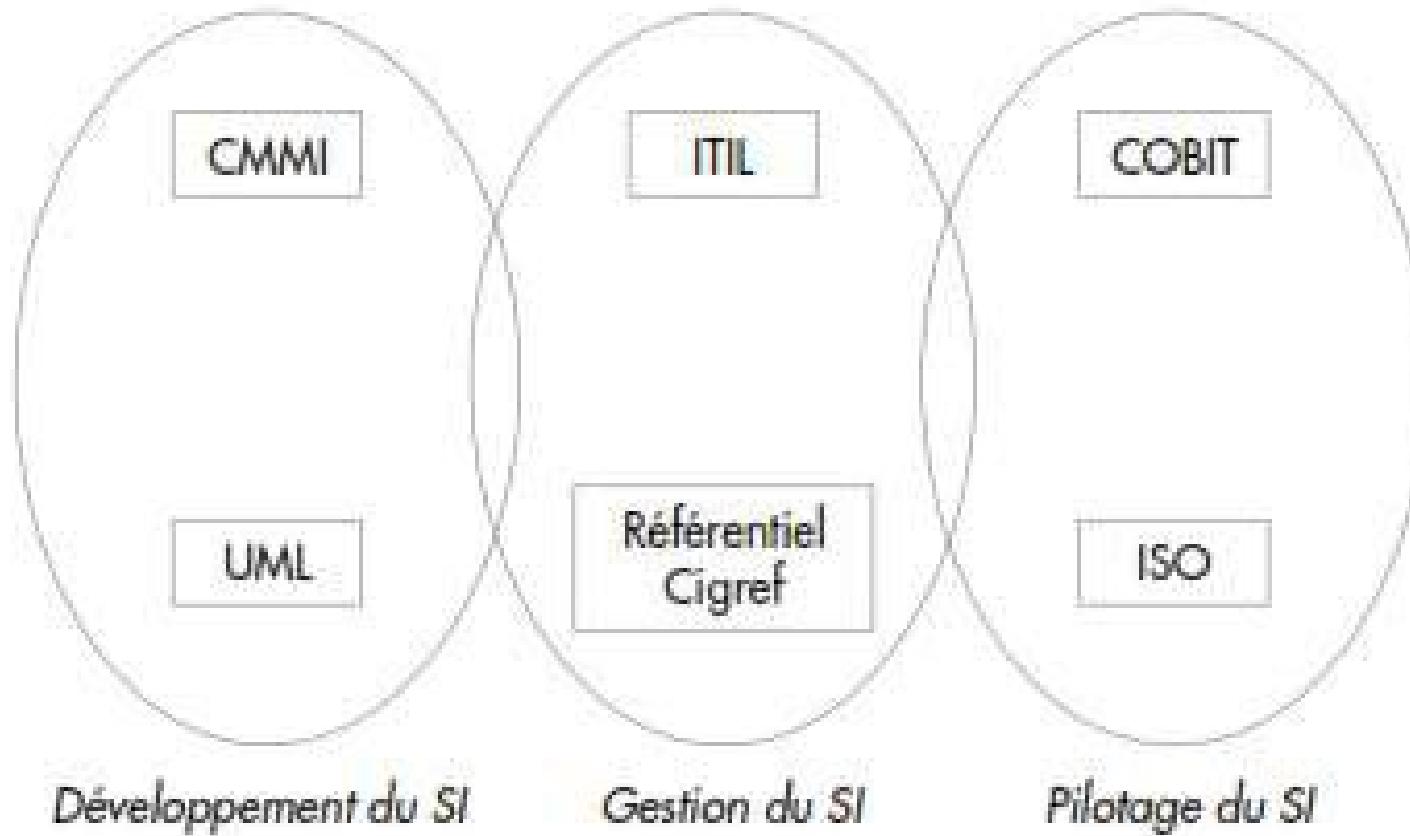
7. Code de déontologie

Document écrit qui regroupe l'ensemble des règles et devoirs qui régissent une profession, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients ou le public. Désormais, de nombreuses professions se sont dotées, avec ou sans l'aval des pouvoirs publics, d'un tel code. Par exemple, les commissaires aux comptes : décret n° 2005-1412 du 16 novembre 2005 portant approbation du Code de déontologie de la profession de commissaire aux comptes.

Référentiels, Méthodes, démarche qualité et normes

- ▶ Référentiels : collection de bonnes pratiques sur un sujet donné
- ▶ Norme : édité par une instance de normalisation indépendante (ex: ISO)
- ▶ Standard : Référenciel largement utilisé et reconnu
- ▶ Nomenclature : permet de décomposer une problématique en éléments homogènes
- ▶ Méthodologie : démarche structurante pour réaliser une tâche donnée





- COBIT, le référentiel de l'ISACA ;
- ISO 17799, devenue ISO 27000 depuis 2005 pour le management de la sécurité informatique ;
- ITIL, une création britannique, désormais devenue une norme ISO 20000 ;
- CMMI, la rationalisation du développement informatique, référentiel développé par l'Université Carnegie-Mellon.

Pilotage

Gouverner le SI de la DSi

Piloter Organisation

Gérer le système de management
•IC-dVAL

Garantir la bonne exécution des Missions
•Val IT, IC-dVAL

Identifier et capitaliser les bonnes pratiques
•5 steps (Valéo)

Gérer le budget IT
•CobiT, PMBok,
•ITIL / ISO 20000,
•Val IT, IC-dVAL

Etablir les plans de recrutement et gestion des compétences
•CobiT, PMBok
Nomenclature CIGREF
Val IT, eSCM, IC-dVAL

Gérer les risques
•CobiT
•PMBok
•COSO
•eSCM

Opérationnel

Fournir un service SI

Construire

Exploiter

Gérer les demandes : Val IT

Gérer les services : CobiT, ITIL, ISO 20000, eSCM

Gérer les changements : CobiT, PMBok, ITIL, eSCM

Gérer les exigences :
•CMMI, Val IT

Gérer les incidents
•CobiT, ITIL,
ISO 20000

Trouver des solutions Informatiques aux enjeux métiers
•CobiT

Gérer les problèmes
•ITIL, ISO 20000,
CMMI

Choisir les projets / Conduire un projet
•CobiT, CMMI, PMBok,
Prince 2, Val IT

Gérer les mises en production
•CobiT, CMMI, ITIL,
ISO 20000

Développer, faire évoluer mettre en œuvre la solution : CMMI, ITIL

Gérer les configurations
•CobiT, ITIL

Gérer les configurations
•CobiT, CMMI, PMBok

Assister les clients
•CobiT, ITIL

Support

Permettre le bon fonctionnement du SI

Gérer les activités support

Gérer les achats et les relations fournisseurs
•PMBok, ISO 20000, eSCM

Gérer la facturation
•CobiT, Référentiel CIGREF benchmarking

Gérer la sécurité et la continuité
•ISO 27001, CobiT, ITIL, ISO 20000

Gérer la communication
•CobiT, PMBok, ITIL, ISO 20000, COSO

Gérer les normes et la documentation : Val IT

Gérer la conformité juridique et normative
•CobiT, ISO 27001, COSO

Assurer la qualité : CobiT, PMBok, CMMI

Gérer les ressources humaines
•Nomenclature CIGREF, IC-dVAL

Assurer la veille technico-fonctionnelle

Gérer la capacité : CobiT, ITIL, ISO 20000

Gérer la disponibilité : CobiT, ITIL

Gouvernance des Systèmes d'Information

Les normes et les référentiels SI et des audits des systèmes d'information

SI et qualité. ISO 9001 est la base de l'ensemble de ces normes. Elle apporte la vision processus, la démarche système, la notion de cycle de vie et l'amélioration continue avec la roue de Deming ou PDCA (*Plan, DO, Check, Act*). La direction générale doit être impliquée dans toutes les actions de l'entreprise.

La qualité se traduit en :

- ISO 20 000, pour le système de management des services ;
- ISO 27001 pour le système de management de la sécurité.

L'entrée dans le **cycle de vie** est opérée par le client qui exprime un besoin sous forme de service en SI. Le client n'est pas toujours capable d'exprimer son besoin. C'est le rôle d'ITIL (version 4 actuellement) ou de ISO 20 000, équivalent de ITIL version 2. ITIL impose de placer le client au cœur du système tout en respectant les principes d'ISO 9001. ITIL se décompose en cinq livres destinés à différents acteurs.

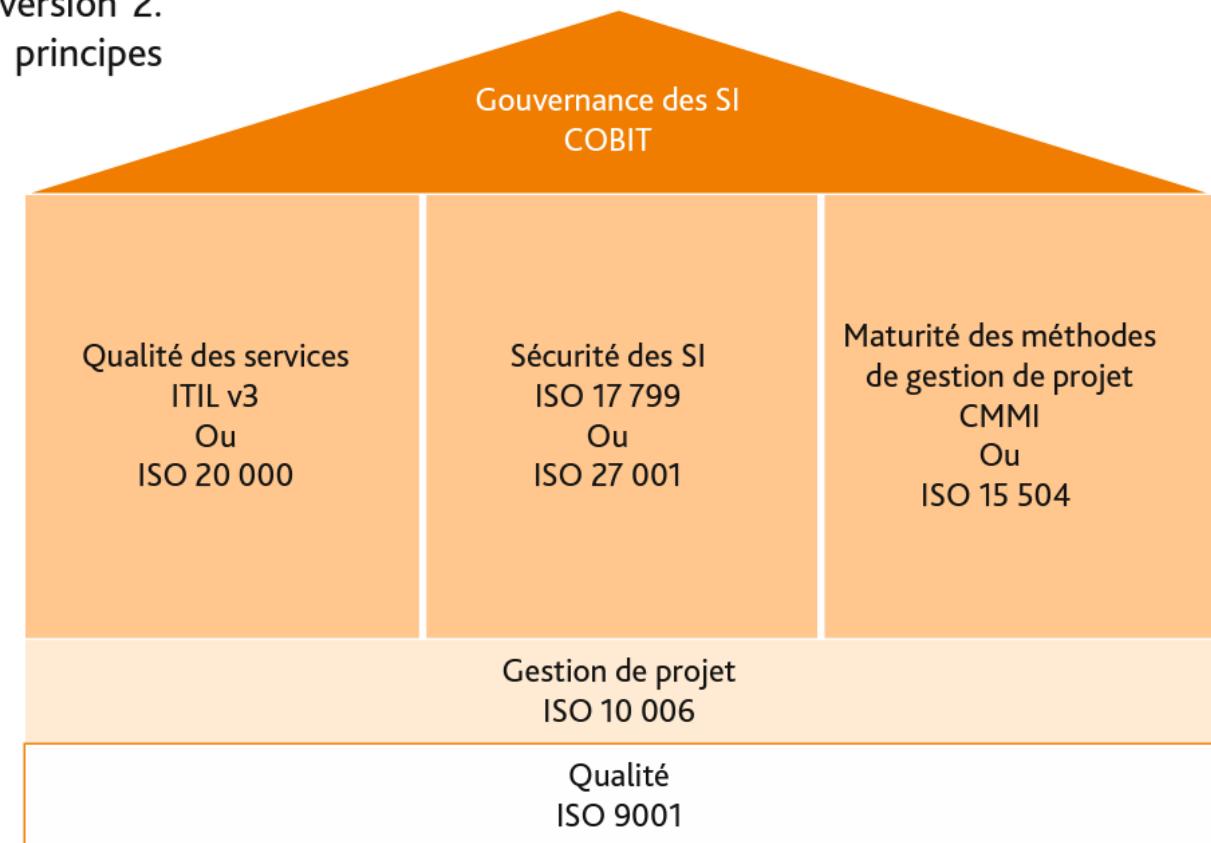
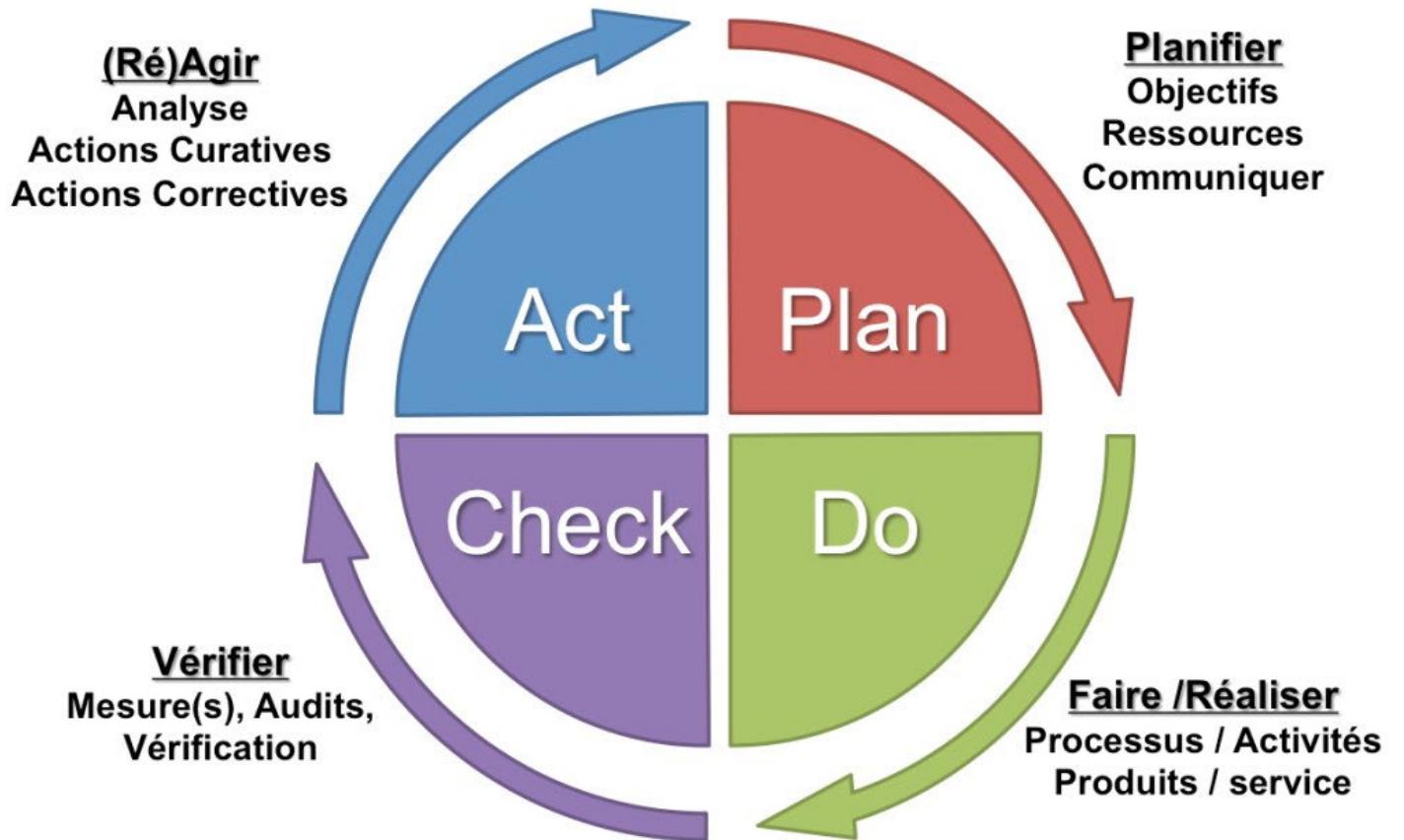


Figure 18.3 Cycle de vie et normes

Le PDCA ou la roue de DEMING



Le PDCA repose sur un principe de cycle vertueux qui permet non seulement de résoudre les problèmes identifiés, mais aussi d'engager l'intégration d'innovations dans un contexte contrôlé. Inventée dans les années 1950, cette approche est toujours d'actualité.

Référentiel pour la production informatique et l'assistance aux utilisateurs :

Information Technology Infrastructure Library, bibliothèque structurée composée de bonnes pratiques pour une meilleure gestion du Système d'Information ;



Amélioration continue de services

Gestion de l'amélioration continue de services

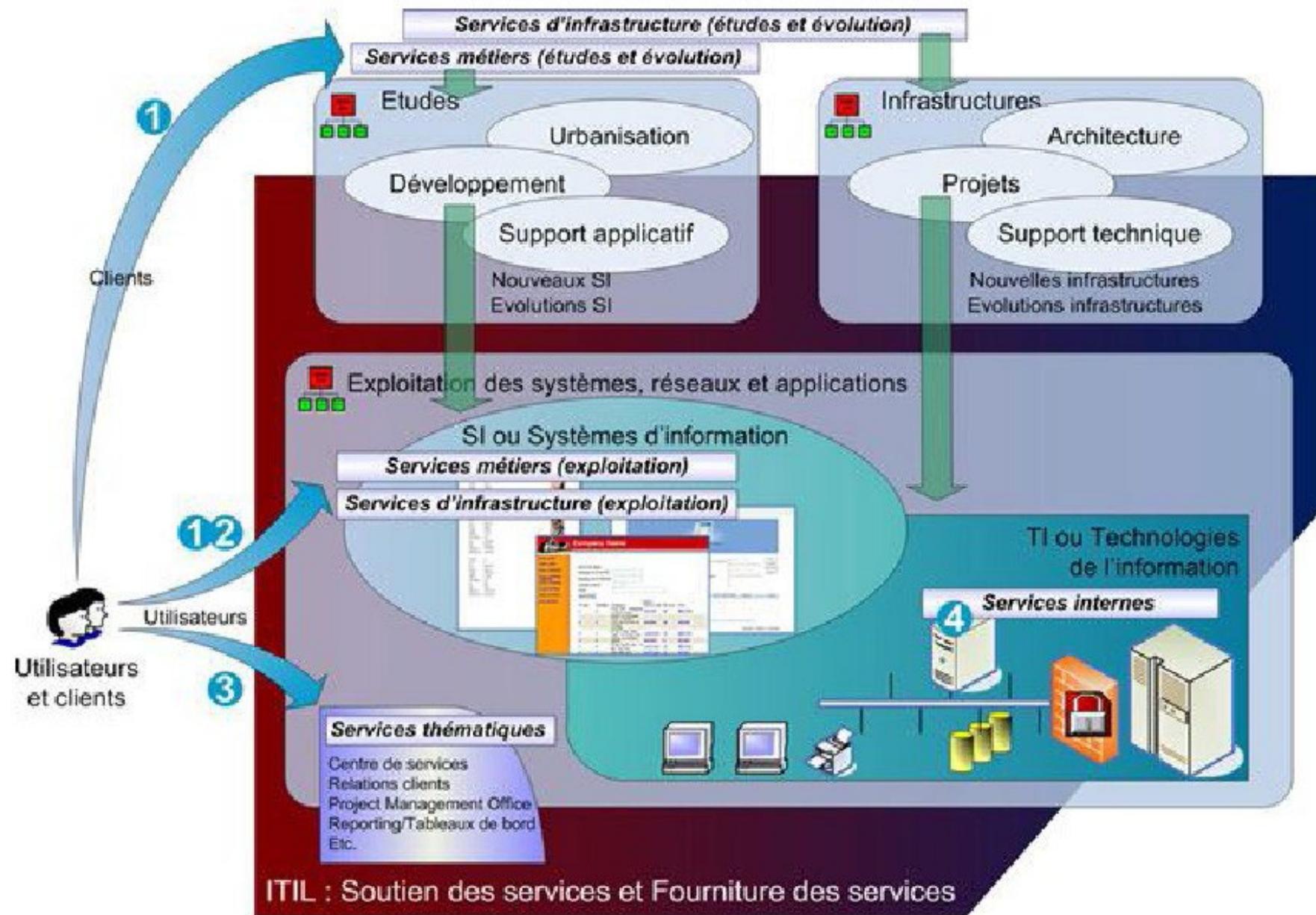
Légende: Phase du cycle de vie d'un service

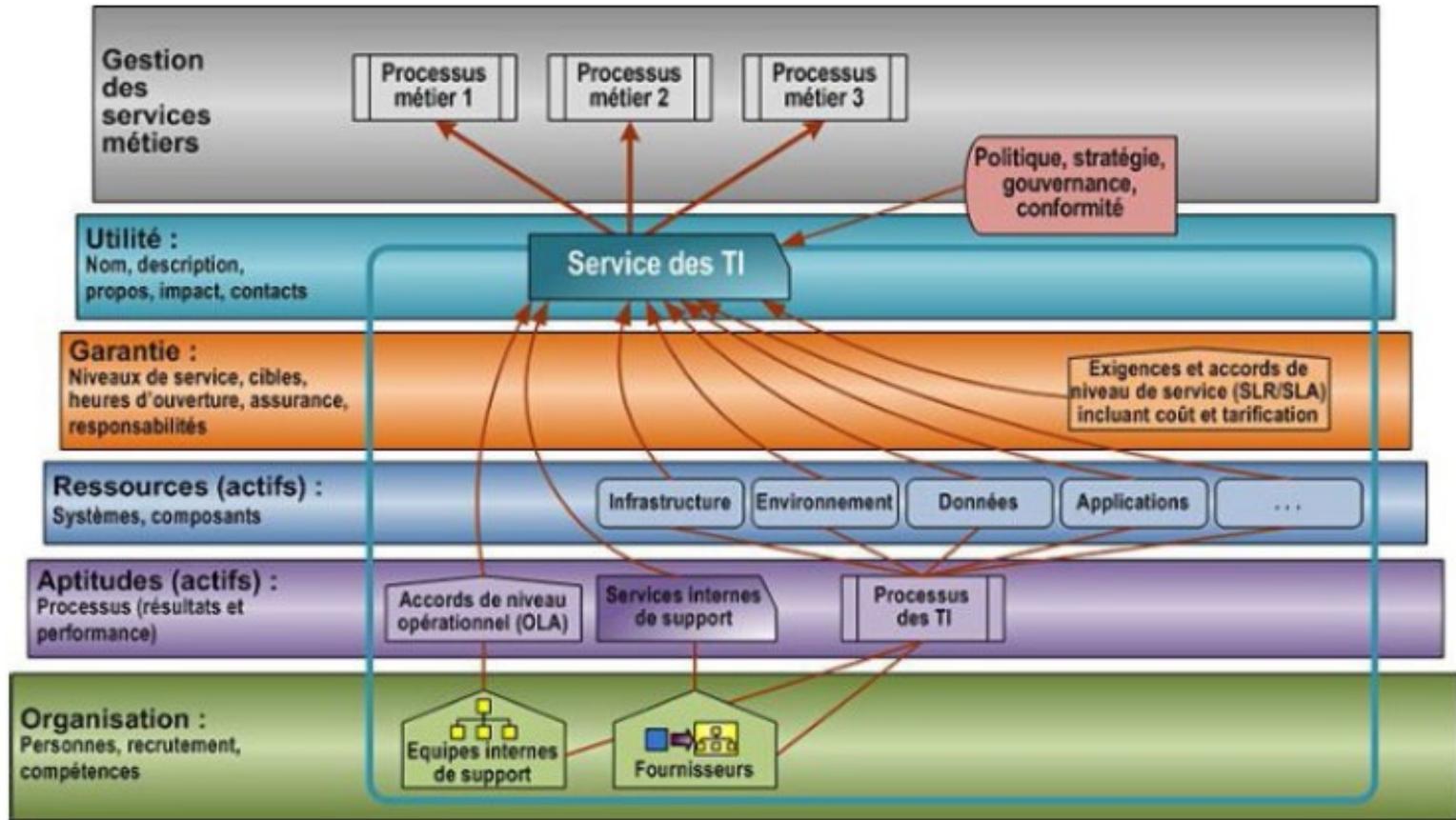
Processus

Fonctions

ITIL

La connaissance des processus informatique qui concourent à la disponibilité et à la continuité de service est essentielle dans le cas ITIL





La conception d'un service doit prendre en compte tous ces aspects :

- les processus métiers : le service doit s'intégrer et faciliter globalement les activités métiers
- l'utilité du service : le service doit fournir une valeur ajoutée sur un processus métier
- la garantie du service : exigences et accords sur le niveau de service, coût et tarification du service
- les ressources informatiques (hors organisation) : infrastructure industrielle (salles informatiques, électricité, climatisation, etc.), les serveurs, les systèmes, les applications, les données, etc.
- les aptitudes (hors organisation) : processus des TI, niveaux de service internes (ou opérationnels)
- l'organisation (domaine à part) : organisation interne et paysage des fournisseurs externes impliqués dans la fourniture du service

CMMI, *Capability Maturity Model Integration*

Référentiel pour le **développement et la maintenance de logiciels** : ensemble structuré de bonnes pratiques constituant un modèle d'évaluation des processus lors de la conception d'applications ;

Accréditations CMMI. Il existe trois accréditations CMMI :

- CMMI-DEV pour la maturité dans le développement d'application ;
- CMMI-ACQ concerne les entreprises qui sous-traitent une partie de leurs interventions. Cette accréditation garantie que le fournisseur ne fera pas baisser la qualité du projet ;
- CMMI-SVC pour les prestations de consulting.

CMMI est audité avec la méthode SCAMPI. En parallèle, ISO 15 504 propose l'équivalent.



La mise en œuvre d'ITIL permet d'assurer au client la qualité attendue du service. Le modèle CMMI a été créé par l'université américaine Carnegie Mellon. CMMI peut être implémenté de façon continue ; dès qu'un processus est prêt, il est évalué et accrédité, avec la coexistence possible de niveaux différents dans l'entreprise. À défaut, on recourt à une implantation étagée. L'entreprise gagne un niveau de façon globale.

Une échelle de maturité à 5 niveaux ... de l'immaturité vers l'optimisé

5 Les processus sont en **amélioration continue**, l'organisation est en **anticipation** constante

Optimisé

4 Toutes les pratiques clés sont contrôlées par des **mesures** en adéquation avec les objectifs de l'organisation

Quantifié

3 Les **processus** sont définis, gérés, instanciés, et améliorés. Le cadre de production logiciel est défini

Défini, institutionnalisé

2 Les **projets** sont bien gérés, une capitalisation des bonnes pratiques existe d'un projet à l'autre

Discipliné

1 La réussite des projets tient à la qualité de l'équipe et ... à la chance !

Immature



Niveau		Capacité	Résultat
5 Optimisé	Processus d'amélioration continue	Innovation organisationnelle et déploiement Analyse et résolutions des causes	Productivité & Qualité
4 Géré Qualitativement	Management Quantitatif	Management quantitatif des processus Management qualitatifs des logiciels	
3 Défini	Processus de standardisation	Développement des besoins Solution technique Intégration du produit Vérification Validation Focalisation sur l'organisation des processus Organisation de la définition des processus Organisation de la formation Management intégré du produit Management du risque Gestion intégrée de l'équipe Management de l'intégrateur Analyse et résolution de la décision Organisation de l'environnement pour l'intégration	
2 Géré	Gestion de projet basique	Management des besoins Planification Surveillance et contrôle de projet Management des fournisseurs Mesures et analyses Assurance qualité des produits et des processus Gestion de configuration	
1 Initia	Efforts héroïques	Concevoir Développer Intégrer Tester	Risques & Pertes

Le CMMI pour le développement traite des bonnes pratiques relatives aux activités de développement et de maintenance appliquées aux produits et aux services.

Il concerne les pratiques qui couvrent le cycle de vie du produit, de sa conception à sa livraison et à sa maintenance, et met l'accent sur le travail nécessaire pour construire et maintenir l'ensemble du produit.

Gouvernance. Pour la gouvernance des SI, la norme COBIT (*Control Objectives for Information and related Technology*) fait autorité. COBIT définit 37 processus dans cinq domaines (version 5) dépendant les uns des autres (**fig. 18.4**):

- Évaluer, diriger et surveiller pour le respect des règles de gouvernance.
- Aligner, planifier et organiser la gestion informatique.
- Bâtir, acquérir et implanter les applications informatiques.
- Livrer, servir et soutenir l'exploitation informatique.
- Surveiller, évaluer et mesurer pour le processus de contrôle interne entre autres.

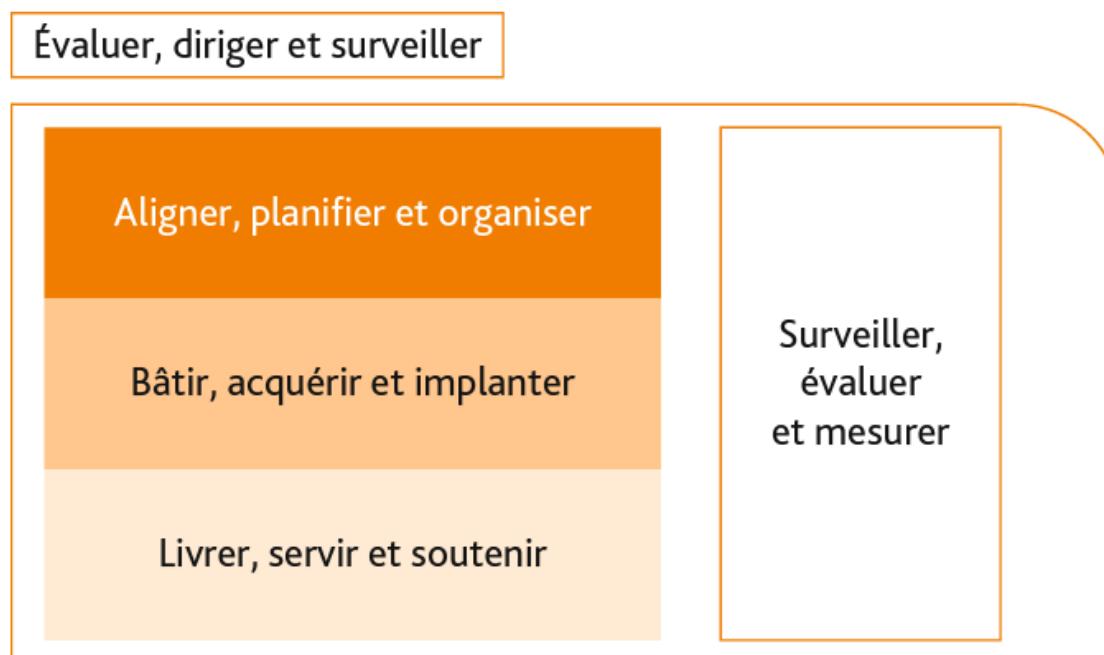


Figure 18.4 Articulation des domaines de COBIT



Conçue par l'ISACA au niveau international et proposée par l'AFAI au niveau français, la norme COBIT est, comme CMMI, basée sur l'amélioration continue et la roue de Demming. Elle constitue une aide à l'auditeur en SI.



BNP Paribas a adopté COBIT, depuis 2007, pour améliorer la gouvernance de ses systèmes d'information et renforcer la gestion des risques liés à la technologie de l'information. La mise en œuvre de COBIT a permis à BNP Paribas d'harmoniser ses processus informatiques, de garantir la conformité réglementaire et d'améliorer la transparence et le contrôle de ses activités technologiques.

Chaque domaine comprend des processus et chaque processus est décomposé en pratique de gestion; COBIT est avant tout un recueil de bonnes pratiques. La norme intègre la **gouvernance des SI** dans la gouvernance de l'entreprise. Les informations récupérées sur les cinq domaines (**fig. 18.5**) concernent le fiduciaire, la qualité et la sécurité. Les domaines sont découplés en processus, eux-mêmes découplés en **activités** exigeant des ressources.

Exemple

- Le personnel, les applications, la technique, l'environnement et les données sont autant de ressources utilisées par les activités.

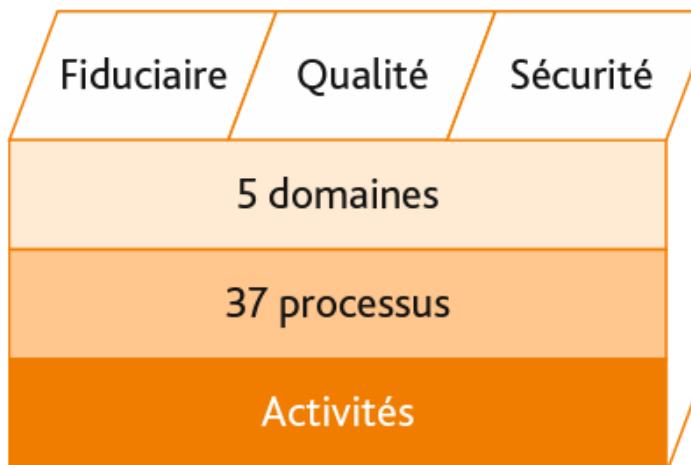


Figure 18.5 Axes de Cobit

OBJECTIFS DE GOUVERNANCE

COBIT

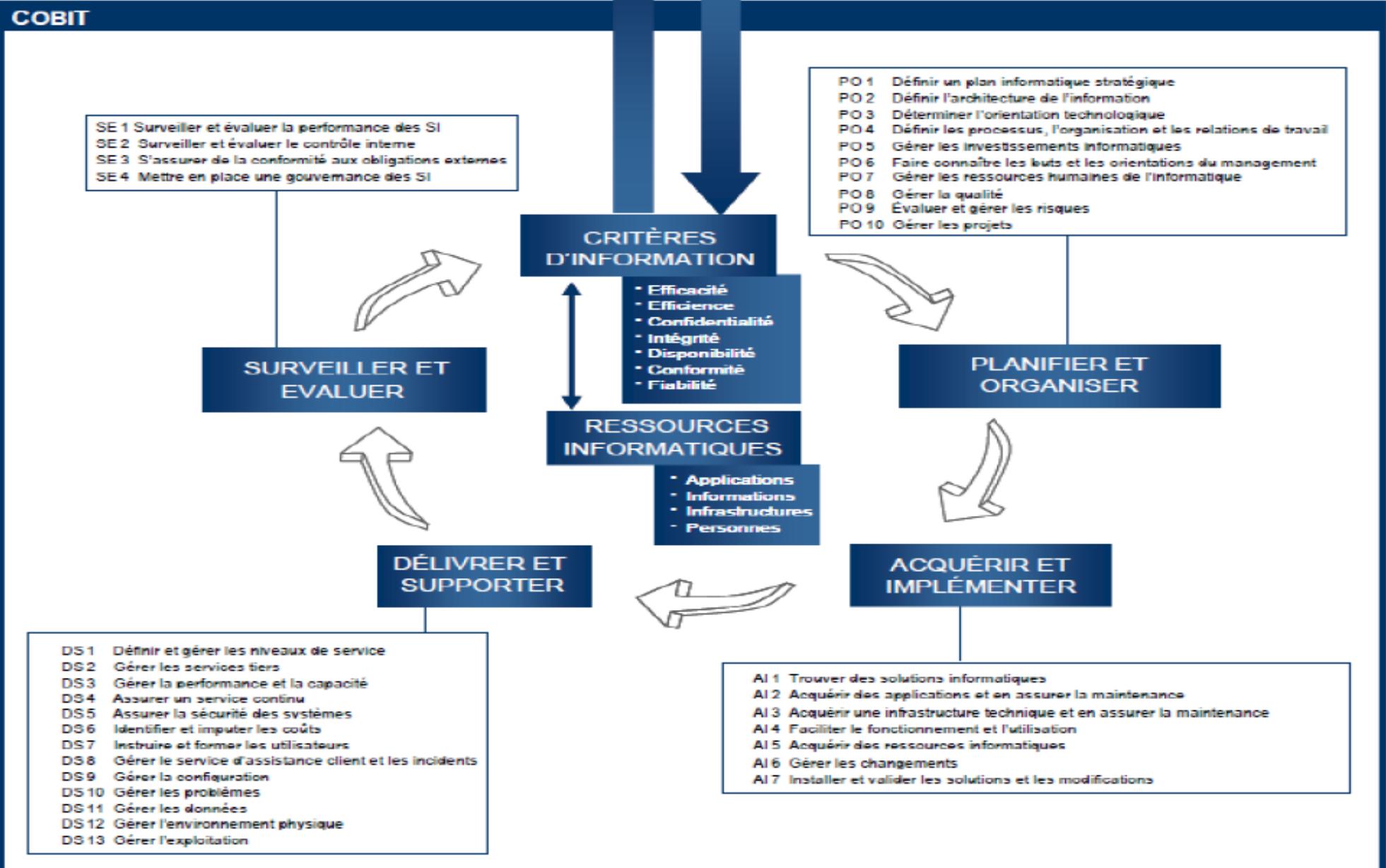


Schéma COBIT

Évaluer, diriger et surveiller

Assurer la définition et l'entretien d'un cadre de gouvernance

Assurer la livraison des bénéfices

Assurer l'optimisation du risque

Assurer aux parties prenantes la transparence

Aligner, planifier et organiser

Gérer le cadre de gestion des TI

Gérer la stratégie

Gérer l'architecture de l'entreprise

Gérer l'innovation

Gérer le portefeuille

Gérer le budget et les coûts

Gérer les relations humaines

Gérer les relations

Gérer les accords de service

Gérer les fournisseurs

Gérer la qualité

Gérer la sécurité

Bâtir, acquérir et implanter

Gérer les programmes et les projets

Gérer les définitions des exigences

Gérer l'identification et la conception des solutions

Gérer la disponibilité et la capacité

Gérer le changement organisationnel

Gérer les changements

Gérer l'acceptation du changement et de la transition

Gérer la connaissance

Gérer les actifs

Gérer la configuration

Livrer, servir et soutenir

Gérer les opérations

Gérer les demandes de services et les incidents

Gérer les problèmes

Gérer la continuité

Gérer les services de sécurité

Gérer les contrôles des processus d'affaires

Surveiller, évaluer et mesurer

Surveiller, évaluer et mesurer la performance et la conformité

Surveiller, évaluer et mesurer le système de contrôles internes

Surveiller, évaluer et mesurer la conformité aux exigences externes

L'utilisation du référentiel CobiT est rassurante pour l'auditeur et l'audité car elle renvoie à une démarche acceptée et validée au niveau international. Elle permet à l'auditeur :

- d'adopter une démarche efficace en se référant, pour la construction et l'application des programmes de travail, à un ensemble reconnu de bonnes pratiques ;
- de structurer la documentation de travail et de la mission ;
- de prendre en compte tous les risques (exhaustivité) ;
- de faciliter les échanges en se référant à un référentiel international ;

Si le recours au référentiel CobiT constitue une véritable opportunité pour l'auditeur, son usage présente des limites. D'une part, le référentiel est avant tout un outil de travail. Il devra donc être adapté aux objectifs de la mission et au contexte de mise en oeuvre. Le référentiel nécessite impérativement une démarche critique de l'auditeur et une appréciation des risques liés au contexte spécifique d'intervention. D'autre part, si le référentiel CobiT reste exhaustif et pertinent pour l'appréciation des risques liés à la fonction informatique, sa portée est considérablement limitée lors de l'évaluation des risques informatiques sous-jacents dans le fonctionnement des autres processus opérationnels ou les risques informatiques particuliers propres, par exemple, à un environnement légal et réglementaire donné.

Le *Service Level Agreement* ou accord sur les niveaux de service

Définition

Vous devez non seulement fixer un niveau de qualité minimum attendu, mais aussi détailler les responsabilités de chacun, par exemple dans l'hypothèse où les services ne seraient pas accessibles comme souhaité. Des pénalités sont prévues en cas de non-respect de l'accord.

Le *Service Level Agreement* (SLA) ou accord sur les niveaux de service (ANS) correspond à un document négocié et signé par le client et le prestataire quant au niveau de qualité attendu et garanti du ou des services qui seront fournis.

1. Les SLA et OLA

Le SLA décrit très précisément le service, les responsabilités du prestataire mais aussi celles du client ainsi que ses besoins (qui sont alors finement détaillés) et les critères d'évaluation et de mesure de la bonne réalisation. La gestion des SLA se fait au sein d'un *Service Level Management* (SLM), ou gestion des niveaux de service. Un SLA peut couvrir plusieurs services ou clients. Il est régulièrement révisé pour prendre en compte les changements technologiques ou législatifs. Il peut constituer une partie du contrat de services, ou être annexé à celui-ci.

Rôle du SLA. Il permet d'établir une relation de confiance entre les deux parties.

Il est indispensable notamment quand la gestion du SI est externalisée, avec des données sensibles hébergées dans le *cloud*, des applications disponibles uniquement en ligne et dont le temps de réponse doit être infiniment petit.

Le Service Level Agreement ou accord sur les niveaux de service

Fonctionnement du SLA. Il s'appuie sur des *Service Level Requirements (SLR)* qui sont des exigences du client pour le service, par exemple la disponibilité. Ces SLR recouvrent les cibles à atteindre et les engagements du fournisseur pour les atteindre. Ils décrivent également les attentes en termes de reprise et de continuité de l'activité si un problème survient.

Il existe de nombreux SLA, en fonction des services. En SI, on les trouve le plus souvent dans trois catégories :

- les SLA liés à l'infrastructure des centres de données et tous les matériels nécessaires à leur fonctionnement comme le réseau, les pare-feux, etc. ;
- les SLA liés aux serveurs pour les systèmes d'exploitation, la mémoire, le stockage, les processeurs, etc. ;
- les SLA liés aux applicatifs pour les logiciels, les bases de données, etc.

2. La mesure de la performance du SI

Afin de s'assurer que le niveau de service attendu est atteint et respecté, il faut mettre en place des **indicateurs de performance**, qu'ils soient mesurables quantitativement ou qualitativement.

Ces indicateurs peuvent également être utilisés comme vitrine pour comparer le niveau atteint par le prestataire par rapport à ses concurrents :

- indicateurs liés à la disponibilité (ex. : temps de réponse moyen, temps d'exécution) ;
- indicateurs liés à la qualité (ex. : délai de prise en charge, pourcentage de résolution).

Le Service Level Agreement ou accord sur les niveaux de service

Les indicateurs dépendent du service traité. Des listes permettent de vérifier ce qui est garanti. Les mesures peuvent être effectuées par le client, par le fournisseur ou – mieux – par un tiers de confiance impartial.

3. Le plan de continuité d'activité (PCA)

Lorsqu'on négocie un SLA, il faut penser à intégrer un **plan de continuité d'activité** ou de gestion des interruptions. En effet, si la performance n'est pas optimum mais dégradée ou que le service est arrêté, il faut pouvoir continuer l'activité. Il est alors nécessaire d'avoir une solution qui prévoie toutes les étapes pour reprendre l'activité ou simplement la poursuivre dans les meilleures conditions.

Exemple

Le basculement sur d'autres serveurs de même qu'un site de substitution peuvent être prévus. Le prestataire garantit alors la continuité ou la reprise d'activité ; il communique la garantie de temps de rétablissement. ▶

B) Les normes et méthodes

L'intégration du *Service Level Agreement* dans les méthodes permet, parce que ces accords suivent le principe de la roue de Deming, une amélioration continue de la qualité des services.

1. ITIL

Le référentiel de bonnes pratiques ITIL positionne le *Service Level Agreement* au cœur de ses processus. En effet, la mise en place de ce document permet de maintenir et d'améliorer progressivement la qualité des services informatiques indispensables et nécessaires au bon fonctionnement des activités de l'entreprise (les SLA doivent alors être modifiables dans cette volonté d'amélioration continue).

Pour ITIL, la distinction entre OLA, SLA et UC est importante pour gagner en clarté et en efficacité. En effet, il est préconisé de rédiger d'abord les OLA et les UC, qui sont la description des exigences des clients et qui seront adaptés en fonction des possibilités techniques et budgétaires, puis les SLA.

2. CMMI

De même qu'ITIL, le référentiel de bonnes pratiques CMMI, modèle de maturité pour la gouvernance des SI, prend en compte les SLA pour appuyer l'atteinte de la maturité. CMMI les intègre par exemple dans les phases de construction et de transition du projet.

3. Ebios

Les *Service Level Agreements* peuvent être des éléments intégrés à la grille d'évaluation.

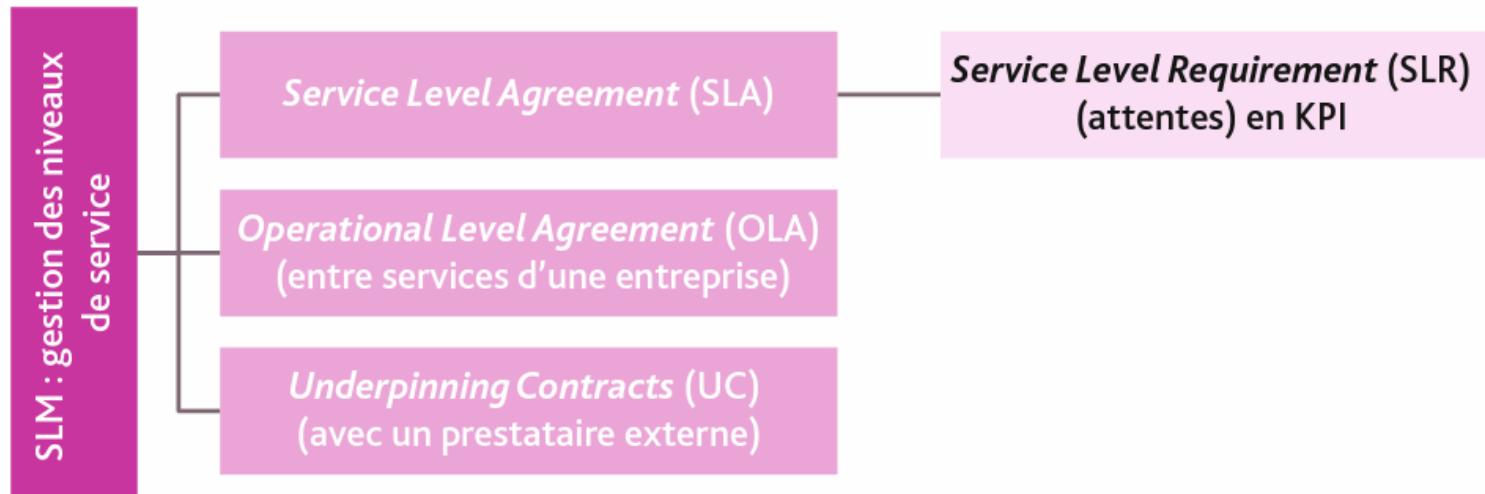


La roue de Deming n'est autre que la représentation graphique de la méthode PDCA (*Plan-Do-Check-Act*), démarche séquentielle visant à améliorer la qualité développée, à l'origine, dans le secteur de la logistique.

4. ISO

Une série de normes ISO (19086) a été développée pour permettre de construire et de mettre efficacement en œuvre ses SLA, notamment pour les services applicatifs.

Les accords sur les niveaux de service





**Gouvernance des
Systèmes
d'Information**

SMSI

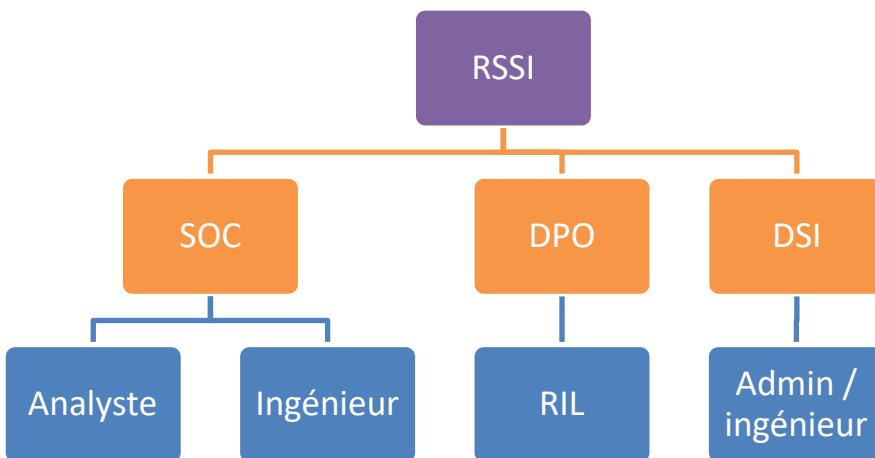
Système de Management de la sécurité de l'information

<https://certification.afnor.org/numerique/lead-implementer-iso-27001>

https://certification.afnor.org/numerique/certification-iso-27001?pk_kwd=certifications%20iso%2027001&gad_source=1



Un système de management de la sécurité de l'information, ou SMSI, comprend les politiques et procédures que votre entreprise met en place pour protéger son contenu, réduire les risques et assurer la continuité de votre activité même en cas de faille du système.



Guide
Recommandations

27000
Vocabulaire

27002
Les bonnes pratiques

27003
Implémentation

27004
Métriques

27005
Gestion de risques

27007
Audit

Normes certifiables

15408
Critères communs

27001
SMSI

Guides pour l'accréditation
ou la certification

17021
Accréditation

27006
Audit SMSI

19011
Audit de SM

17024
Certification
individuelle

RSSI

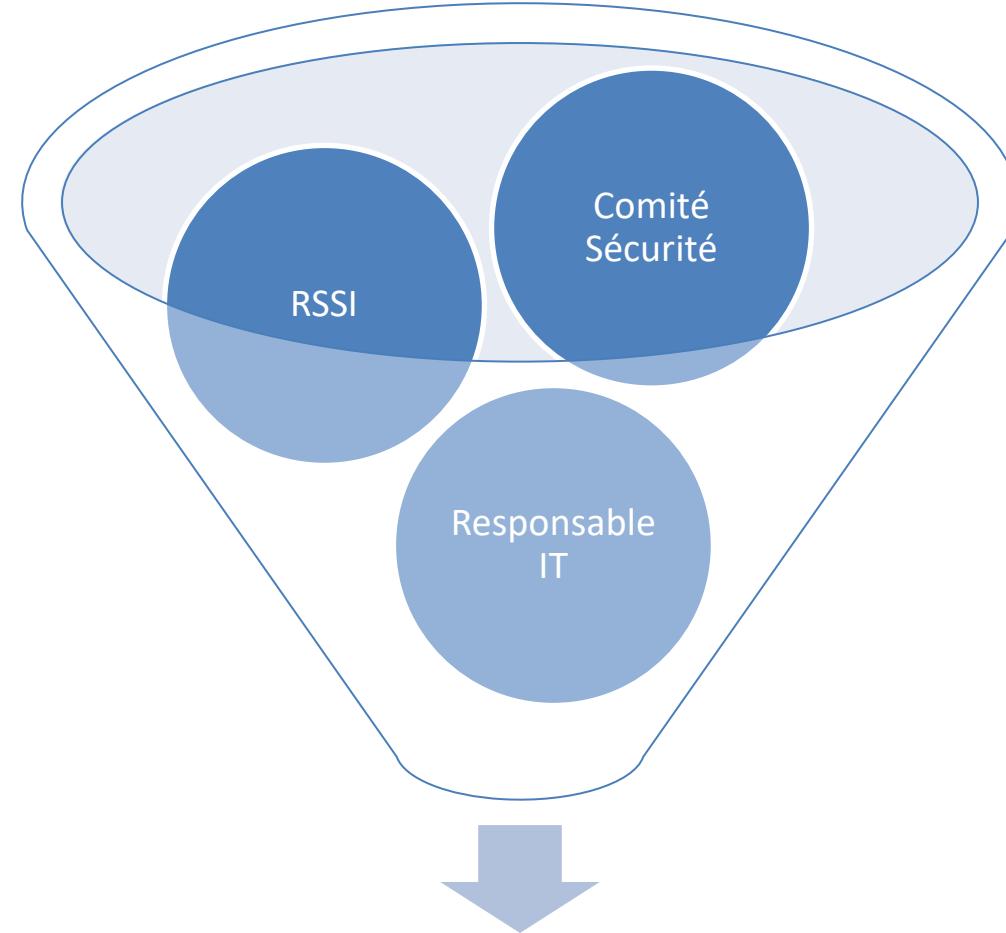
Responsable de la sécurité des systèmes d'information

Définition / évolution de
la politique

Gestion de projet

Contrôle

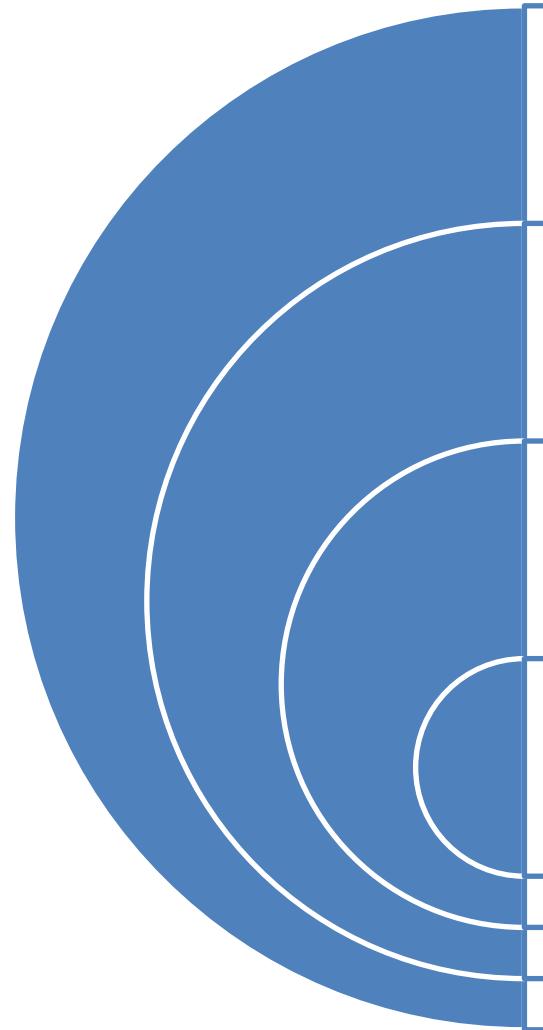
Sensibilisation



Sécurité du SI



- La sécurité a pour objectif de réduire les risques, pour limiter leurs impacts



Réseau Système Données Humain

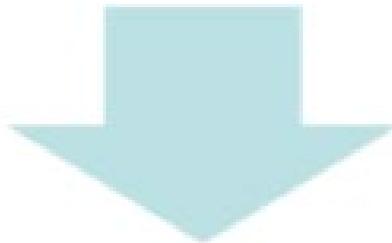
- Firewall
- Segmentation
- VPN
- Sonde IDS
- Wifi

- Anti-virus
- Patch Management
- Vuln Management
- Durcissement OS
- Backup

- Classifier les data
- Analyse de risques

- Formation / Sensibilisation
- PCA / PRA

Sécurité des Systèmes d'Information



Bonnes pratiques

- Organisation
- Formations
- Méthodes
- Procédures
- Directives
- Lois
- Contrôles
- Sanctions
- Technologies



Engagement de responsabilité

- Personne morale
- Direction Générale
- Directions
- Managers
- Personnels
- Partenaires
- Sous-traitants



Gestion du risque

- Relativité des risques
- Valeurs et Enjeux
- Potentialités
- Impacts
- Relativité des règles

Évolution de la maturité SSI



Les bonnes pratiques trouvent leur concrétisation dans les plans de sécurité ou politiques opérationnelles de sécurité

Plans de sécurité

Sécurité physique

- protection anti-incendie ;
- protection électrique ;
- protection d'ambiance du local des machines ;
- contrôle d'accès aux zones protégées.

Sécurité logique

- sécurité des accès ;
- sécurité des échanges ;
- sécurité des infrastructures et des applications.

Détection d'intrusion
Centralisation des logs
Audit / Tests intrusifs

Sécurité de l'organisation

- information des acteurs ;
- définition de règles ;
- organisation de cellules de sécurité ;
- formation de correspondants ;
- définition des moyens de contrôle ;
- réalisation des contrôles
- Procédures.

Plan de secours

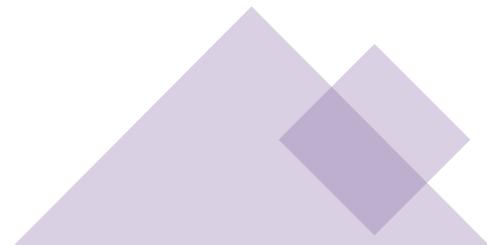
- sauvegardes ;
- plan de secours ;
- plan de reprise d'activité.



Problématique complexe

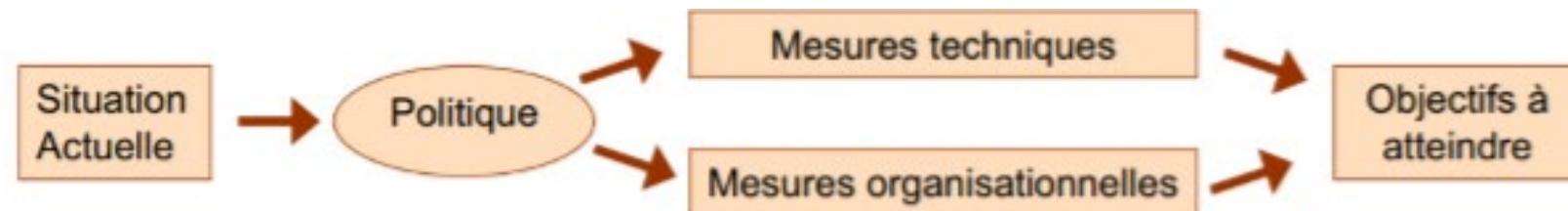
- Concevoir et manager un dispositif de sécurité adapté nécessite :
- Une bonne connaissance des risques
- Une approche globale et transversale faisant interagir les services, DSI / Direction
- Un modèle de conception dynamique qui intègre l'évolution des architectures et des menaces

Le SMSI doit être cohérent avec les objectifs métiers de l'organisme et cohérent avec le système de management de la qualité

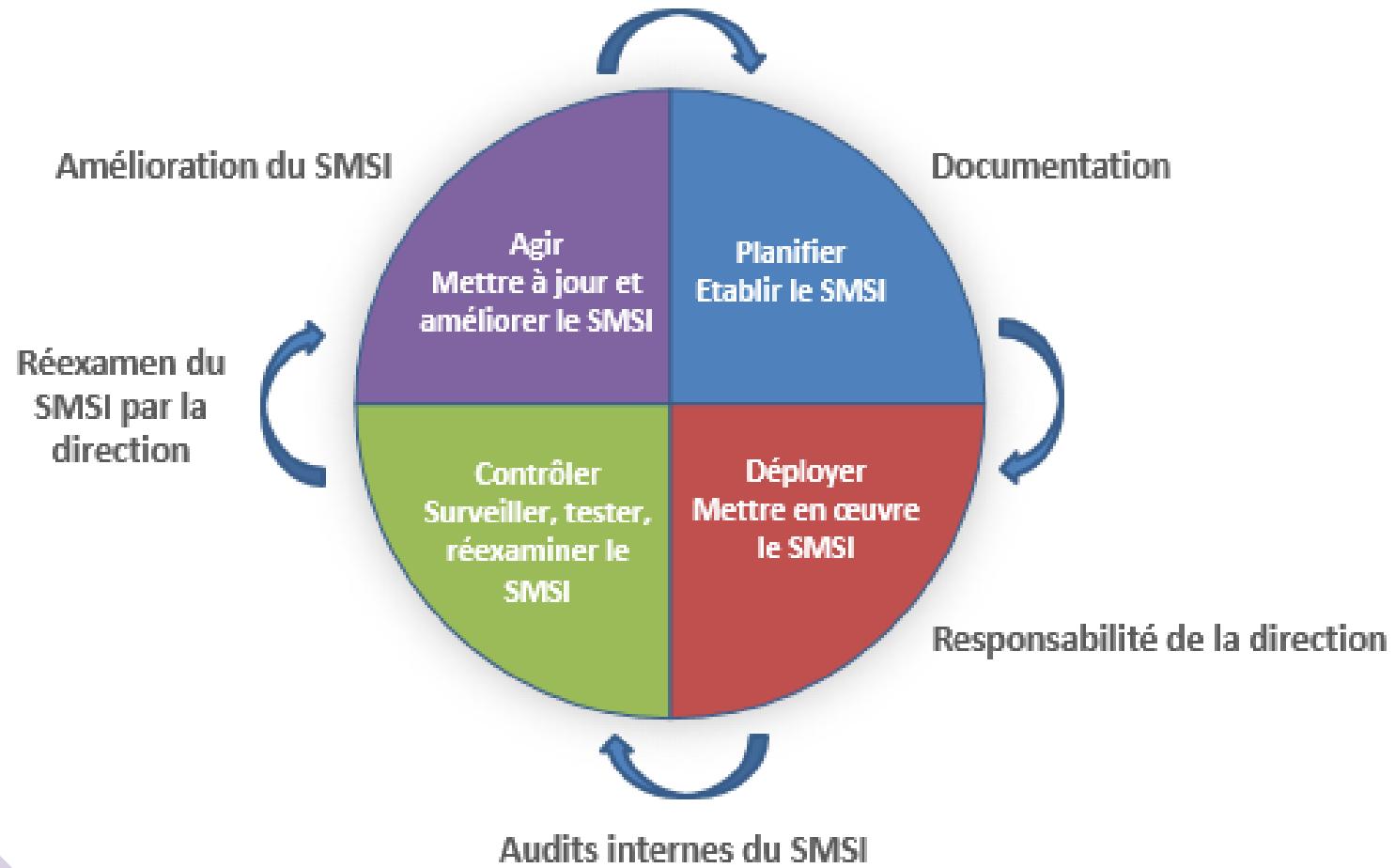


- La sécurité du SI doit être abordée d'une manière globale avec une volonté affichée et un appui de la direction
- Les seules réponses techniques à la problématique sécurité sont insuffisantes si elles ne sont pas consolidées par une approche structurée intégrant les composantes :
 - Stratégique
 - Economique
 - Organisationnelle
 - Humaine

Les priorités portent désormais d'avantage sur les aspects d'organisation et de management



PDCA de la mise en place d'un SMSI selon la norme ISO27001:2005



■ Organisation du document

□ Les chapitres 0 à 3 définissent les généralités de la norme :

- 0. introduction
- 1. Périmètre, modèle PDCA
- 2. Références normatives
- 3. Termes et définitions

□ 4. Les exigences d'un SMSI

□ 5. Les responsabilités de la direction

□ 6. Audits internes du SMSI

□ 7. Contrôle périodique du SMSI par la direction

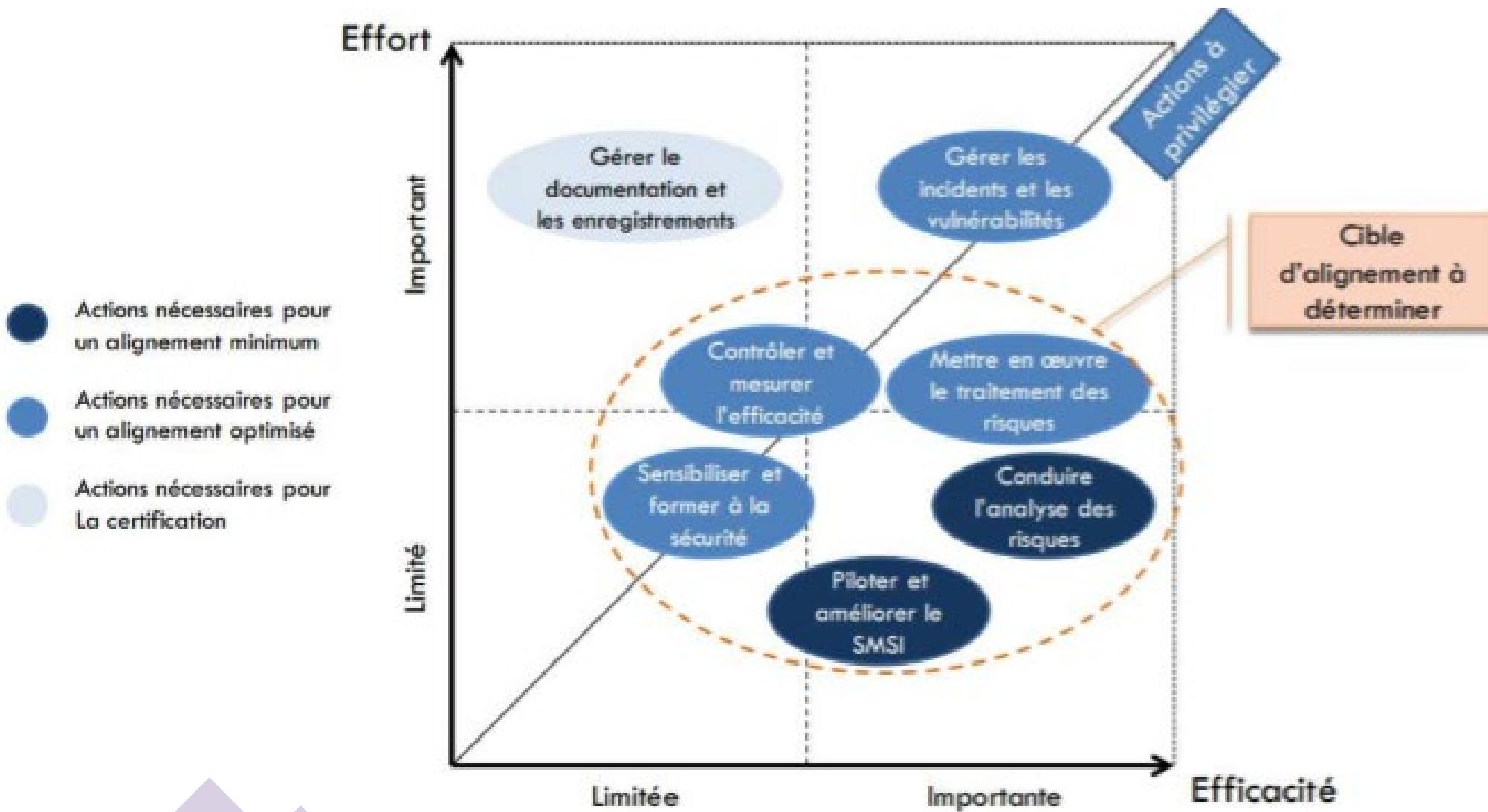
□ 8. Amélioration du SMSI

□ Annexe A. Objectifs de contrôle et contrôles

□ Annexe B. Comparatif OCDE et 27001

□ Annexe C. Correspondance avec les normes ISO 9001:2000 et ISO

Obligatoire pour
une certification
ISO 27001



- **Les contraintes organisationnelles et le budget freinent le RSSI**
- Liste des raisons principales :
 - Manque de budget
 - Manque de connaissance
 - Contraintes organisationnelles
 - Réticence de la direction générale, des métiers ou des utilisateurs
 - Manque de personnel qualifié

Les difficultés de la sécurité

- Les user ont des besoins spécifiques en sécurité IT mais en général ils ont aucune expertise dans le domaine
 - L'utilisateur ne sait pas ce qu'il veut, c'est à l'expert de comprendre
- Performance et confort d'utilisateur Versus Sécurité
 - Les mécanismes de sécurité consomment des ressources additionnelles
 - La sécurité interfère avec les habitudes de travail des usagers
- Ouverture vers le monde extérieur en constante progression

- **Centre de coût VS centre de profil**
 - La justification des dépenses en matière de sécurité n'est pas évidente
 - Le retour sur investissement est un exercice difficile
- **La sécurité n'est pas une fin en soi, mais résulte d'un compromis entre:**
 - Un besoin de protection
 - Le besoin opérationnel qui prime sur la sécurité
 - Les fonctionnalités toujours plus tentantes offertes par les technologies
 - Un besoin de mobilité
 - Des ressources financières et des limitations techniques

Les difficultés de la sécurité

- La sécurité n'est pas une activité ponctuelle
 - elle ne se met pas en œuvre en une seule fois
 - Elle fait partie intégrante du cycle de vie du SI
 - Processus itératif qui n'est jamais fini et doit être corrigé & testé régulièrement

La sécurité absolue est inatteignable, c'est un voyage, pas une destination

Gouvernance des Systèmes d'Information

PSSI

Politique de sécurité du système d'information

<https://cyber.gouv.fr/publications/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation>

- **Définition**

Ensemble des règles formelles auxquelles doivent se conformer les personnes autorisées à accéder à l'information et aux ressources d'un organisation (RFC 2196)

- **Finalité ?**

- Définir les règles du jeu
- Faire accepter et faire respecter les règles du jeu
- Réduire les risques

- **Composantes :**

- Ensemble des principes juridiques, humains, organisationnels et techniques qu'il est recommandé de mettre en œuvre pour créer, gérer, protéger le SI

- **Réussite de mise en œuvre d'une PSSI ?**

- Implication forte de la direction
- En accord avec les directions fonctionnelles et les équipes techniques
- Analyse des risques pleinement étudiée

B. DÉFINITION DE LA PSSI

La PSSI est le document de référence définissant les objectifs poursuivis par l'entreprise en matière de SSI et les moyens mis en œuvre pour les atteindre.

La PSSI édicte un certain nombre de règles, procédures et bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'entreprise.

L'élaboration d'un tel document doit nécessairement être menée comme un véritable projet, *i.e.* associant des représentants des utilisateurs et conduite au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la PSSI est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner le maximum d'impact à la PSSI.

Il existe de nombreuses méthodes permettant de mettre au point une PSSI. Voici une liste non exhaustive des principales méthodes :

- **Mehari** (Méthode harmonisée d'analyse de risques,

<http://www.clusif.asso.fr/fr/production/mehari/>) a été élaborée par la commission Méthodes du Clusif.

La méthode met à disposition des règles, modes de présentation et schémas de décision. Elle propose, au niveau d'une entreprise ou d'une activité, un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de pallier au mieux les failles constatées et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.

- **Ebios** (Expression des besoins et identification des objectifs de sécurité, http://www.ssi.gouv.fr/site_article45.html) a été mise au point par l'ANSSI.

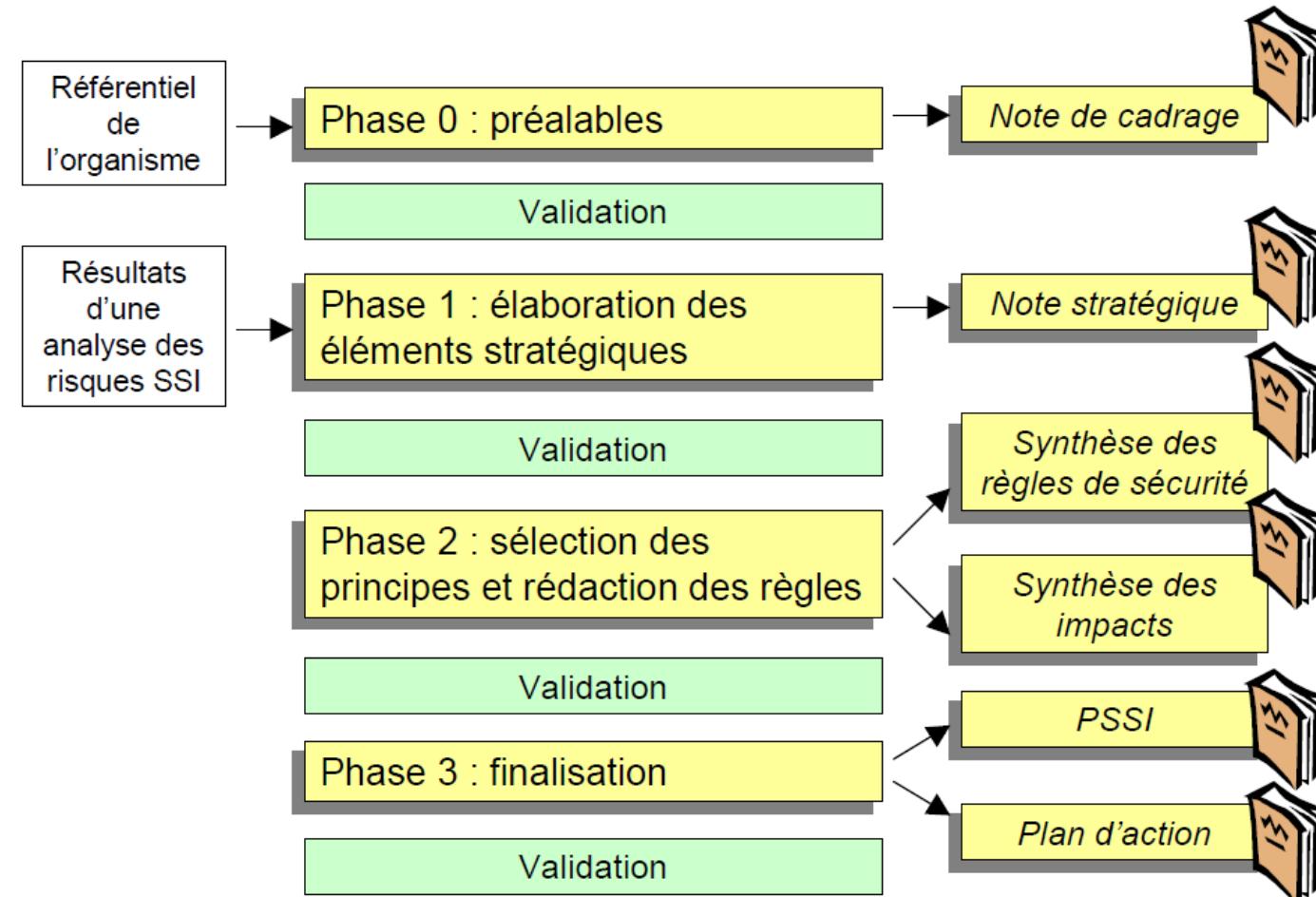
Depuis 2009, **la série de normes ISO 27000** est dédiée au management de la sécurité de l'information (de nombreuses normes sont encore en cours d'écriture). Les normes ISO 27001 et 27002 sont les deux principales normes de la série : la première décrit les exigences à satisfaire pour la mise en place d'un système de management de la SSI, et peut aboutir à plus long terme à une certification de l'entreprise ; la seconde (anciennement ISO 17799) constitue un guide de bonnes pratiques opérationnelles en matière de sécurité de l'information (en définissant onze domaines de SSI, abordant des aspects tant techniques qu'organisationnels, elle propose plus d'une centaine de mesures de sécurité).

Mais des freins et un manque de maturité s'opposent encore à la mise en œuvre d'une PSSI efficace dans les entreprises.

<https://cyber.gouv.fr/la-methode-ebios-risk-manager>

<https://www.m2formation.fr/actions-collectives-opco/>

La démarche d'élaboration de PSSI de la DCSSI est décomposée en quatre phases successives :

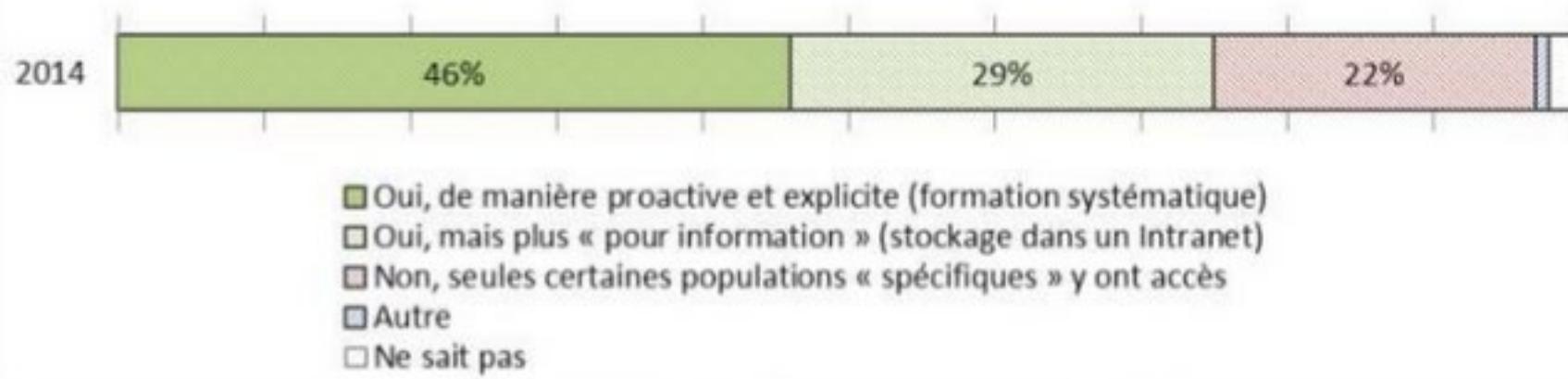


En ce sens, les rapports du Clusif des dernières années ont montré que, plus les dirigeants sont informés de leur responsabilité civile ou pénale, moins ils exigent de justifier une dépense en SSI par un rendement particulier. Ainsi, pour les RSSI, une justification essentielle des investissements en SSI est de se conformer aux réglementations (cet argument est plus avéré dans les grandes entreprises que dans les PME).

EXEMPLE

Bonne pratique : Le RSSI d'un grand groupe manufacturier est rattaché directement au PDG. Il anime et contrôle une structure transversale « sécurité » qui croise et s'impose à chaque grande unité opérationnelle ; cette structure matricielle est doublée d'une structure d'audit indépendante qui couvre également le domaine SSI. Le RSSI a tout pouvoir d'arrêter un dispositif opérationnel s'il juge que la PSSI n'est pas respectée, même si cette décision est susceptible de générer des pertes financières significatives.

La Politique de Sécurité de l'Information de votre entreprise est-elle communiquée à tous les acteurs du SI ?



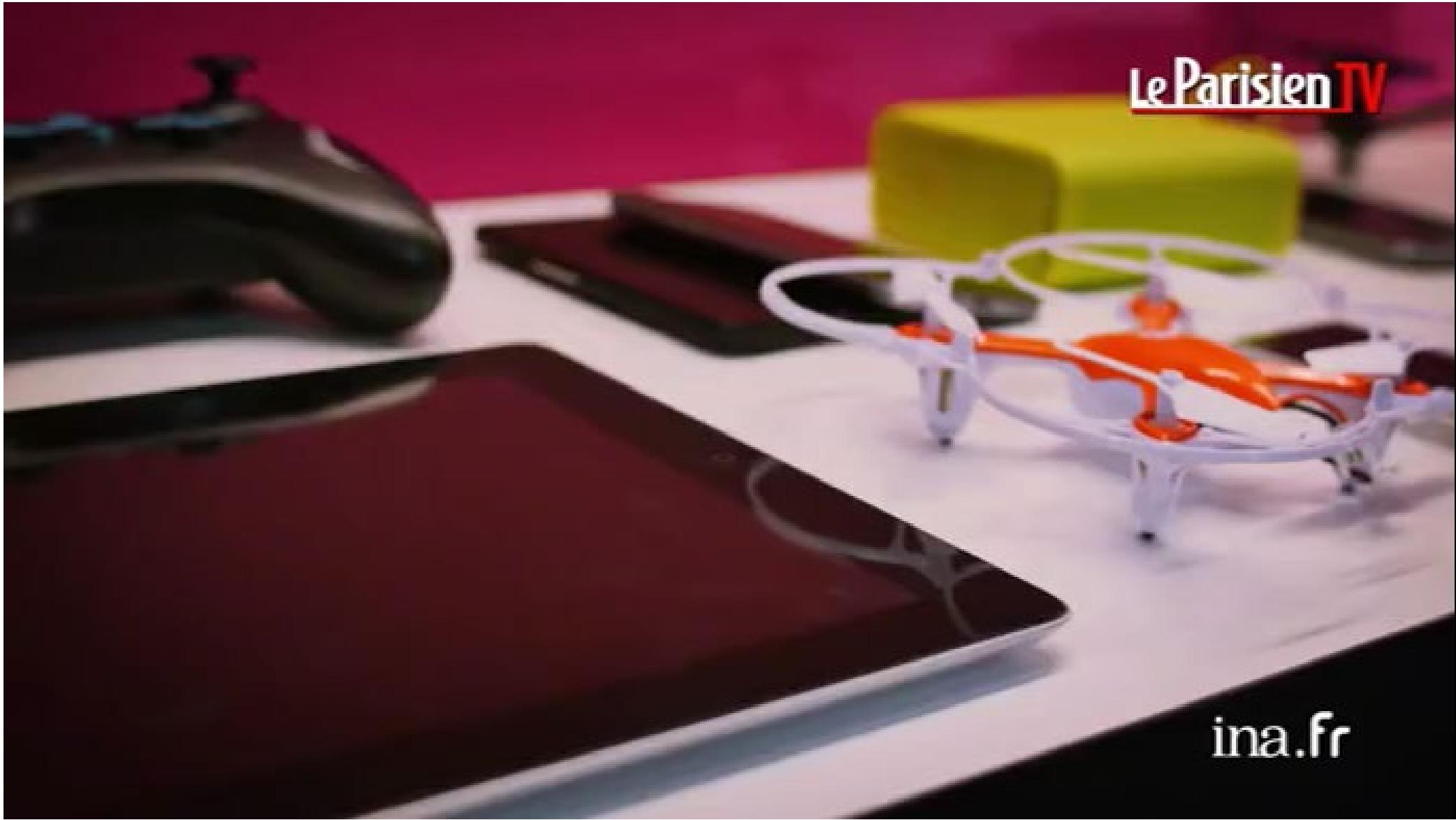
- **Politiques de communication :**
 - Sensibilisation
 - Responsabilisation
 - Formation ciblée par métier
- **Politiques Informatique :**
 - Règles
 - Normes
 - Organisation de la sécurité opérationnelles, études de solutions techniques
 - Intégration de la sécurité dans la conduite de projet (Analyse de risque avant projet)
- **Politiques organisation :**
 - Organigramme, comités de sécurités
 - Management du changement
 - PCA / PRA / Gestion de crise











Le Parisien TV

ina.fr