

# Management de la Sécurité

Pr. M.D. El Kettani

ISO 27001 LI

# Plan

- La sécurité de l'information
- La planification du SMSI
- La mise en œuvre de la SMSI
- Le contrôle, l'audit, l'amélioration du SMSI

# Plan détaillé

- La sécurité de l'information
  1. Cadre normatif et réglementaire
  2. Principes fondamentaux de la sécurité de l'information
  3. Systèmes de management de la sécurité de l'information
  4. Analyse préliminaire du projet
  5. Planification du projet
- La planification du SMSI
- La mise en œuvre de la SMSI
- Le contrôle, l'audit, l'amélioration du SMSI

# Plan détaillé

- La sécurité de l'information
- La planification du SMSI
  1. Gouvernance
  2. Analyse des risques
  3. Déclaration d'applicabilité
- La mise en œuvre de la SMSI
- Le contrôle, l'audit, l'amélioration du SMSI

# Plan détaillé

- La sécurité de l'information
- La planification du SMSI
- La mise en œuvre de la SMSI
  1. Gestion documentaire
  2. Design des mesures de contrôle et procédures
  3. Mise en œuvre des mesures de contrôle
  4. Formation, sensibilisation et communication
  5. Gestion des incidents
  6. Gestion des opérations
- Le contrôle, l'audit, l'amélioration du SMSI

# Plan détaillé

- La sécurité de l'information
- La planification du SMSI
- La mise en œuvre de la SMSI
- Le contrôle, l'audit, l'amélioration du SMSI
  1. Monitoring des mesures de contrôle
  2. Mesure de la performance des mesures de contrôle
  3. Audit interne du SMSI
  4. Amélioration continue
  5. Audit de certification

# La sécurité de l'information

1. Cadre normatif et réglementaire
2. Principes fondamentaux
3. Systèmes de management de la sécurité de l'information
4. Analyse préliminaire du projet
5. Planification du projet

# 1. Cadre normatif et réglementaire



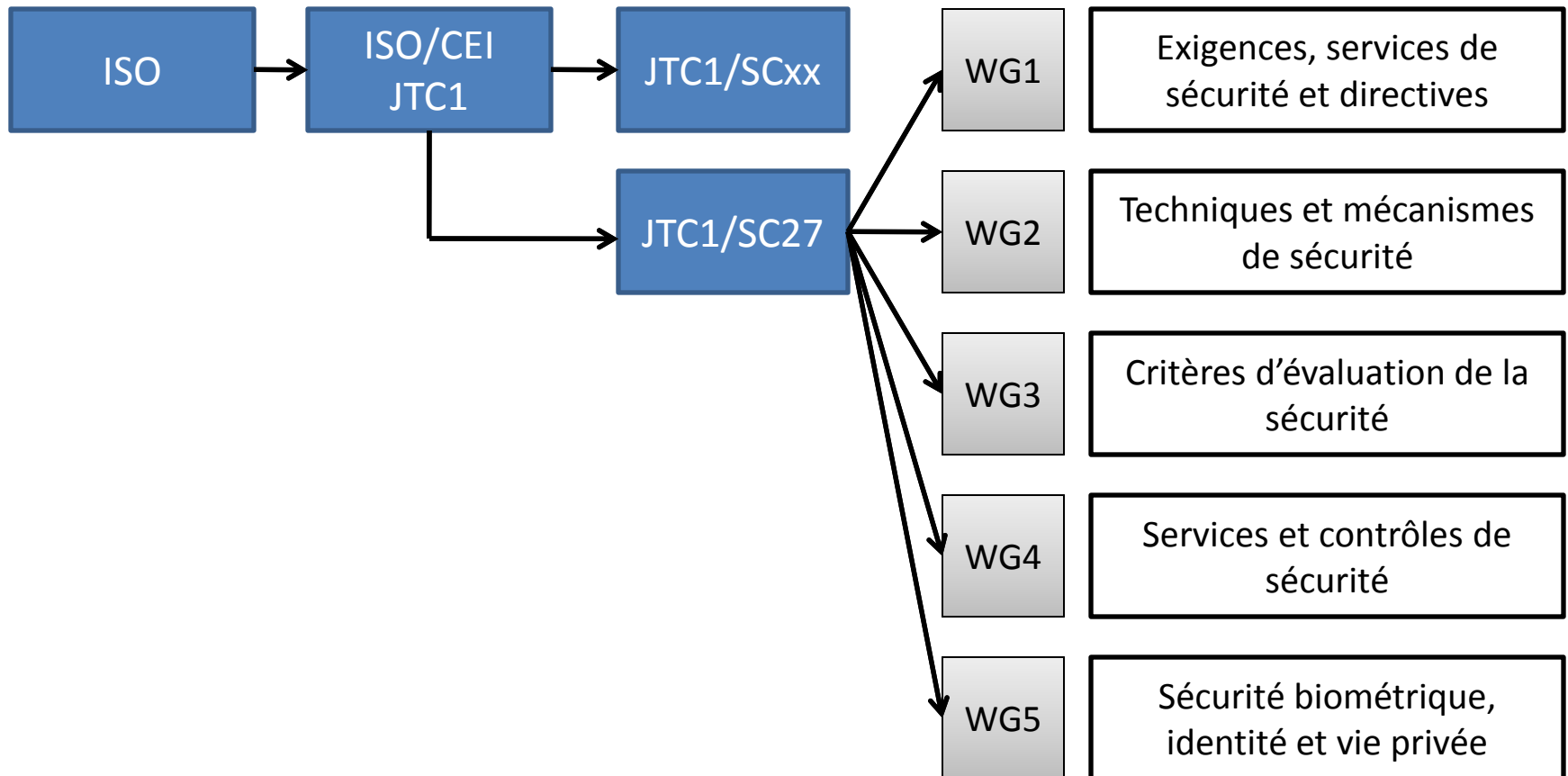
# 1. Cadre normatif et réglementaire

- Organisation Internationale de Normalisation (ISO):
  - Fédération internationale d'organisations normalisatrices nationales de plus de 150 pays
  - Résultats finaux des travaux de l'ISO publiés en tant que normes internationales
  - Plus de 16000 normes publiées depuis 1947

# 1.1. Principes de base des normes ISO

- **Représentation égale:** 1 vote par pays
- **Adhésion volontaire:** ISO n'a pas d'autorité en tant qu'ONG pour leur mise en application
- **Orientation d'affaires:** ne développe que des normes qui comblent des besoins du marché
- **Approche par consensus** des différentes parties prenantes
- **Coopération internationale:** plus de 150 pays membres

## 1.2. Sous-comité ISO/JTC1/SC27



## 1.3. Définitions

- Règlementation
- Politique
- Norme
- Méthodologie
- Lignes directrices
- Procédures

## 1.3. Définitions

- Réglementation:
  - loi officielle qui expose comment quelque chose doit être effectué et établi; ce qui peut, ou ne peut pas être fait

## 1.3. Définitions

- Politique de sécurité:
  - Précise les valeurs d'une organisation, les objectifs et les lignes directrices en matière de sécurité de l'information. Courte et concise, une politique définit la philosophie de haut niveau de l'organisation en matière de sécurité de l'information. Elle précise les directives requises à l'élaboration et à la mise en œuvre d'un programme de sécurité de l'information, ainsi qu'au partage des responsabilités

## 1.3. Définitions

- Norme:
  - Selon le guide ISO/CEI 2, « un document de référence couvrant un large intérêt industriel et basé sur un processus volontaire, approuvé par un organisme reconnu, fourni pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités, ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné »

## 1.3. Définitions

- Méthodologie:
  - Démarche rigoureuse et normalisée s'appuyant sur des outils tels que des questionnaires ou des logiciels spécialisés et permettant de faire l'analyse de la sécurité de l'information. Une méthodologie utilise donc des méthodes, c'est-à-dire des moyens d'arriver efficacement au résultat souhaité. Ce souhait étant habituellement formulé dans une norme, on voit que souvent la méthode sera l'outil utilisé pour satisfaire aux exigences d'une norme



## 1.3. Définitions

- Lignes directrices:
  - Directive importante qui devrait être respectée, bien qu'elle ne soit pas obligatoire. Ce sont des déclarations générales permettant d'atteindre les objectifs de la politique en fournissant l'infrastructure dans laquelle seront implantées les procédures

## 1.3. Définitions

- Procédures:
  - Instructions spécifiques qui expliquent clairement les étapes à suivre afin de déterminer comment la politique, les directives et les normes de soutien seront réellement mises en œuvre dans un environnement d'exploitation

## 1.4. Conformité légale

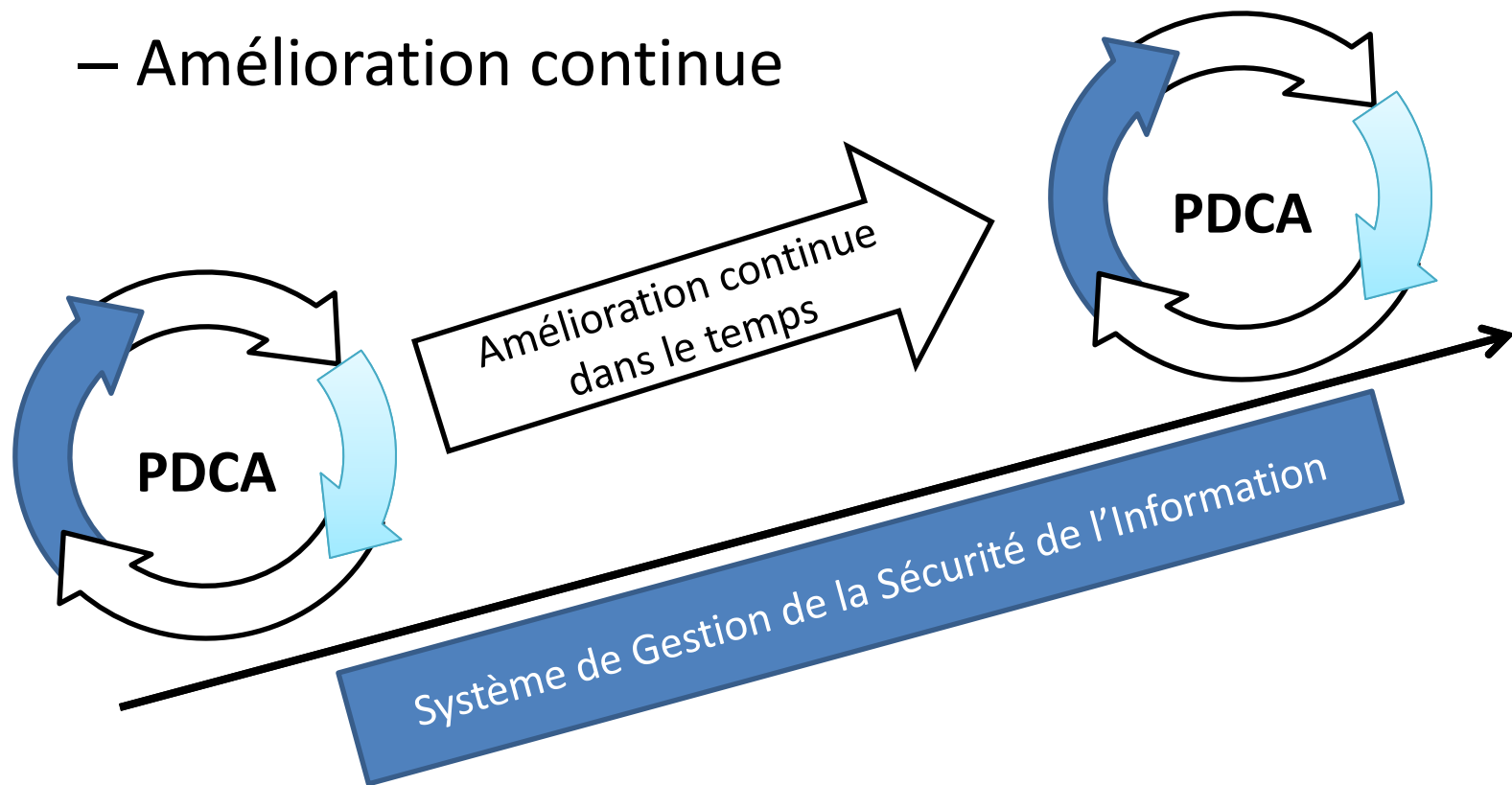
- Les lois applicables et les réglementations doivent être suivies par l'organisation
- Dans la plupart des pays, la mise en œuvre d'une norme ISO est une décision de l'organisation, pas une condition légale
- Dans tous les cas, les lois ont la priorité sur les normes
- Référence : ISO 27002
  - Annexe 15: conformité (15.1 & 15.1.1)

## 1.5. Normes ISO

- Exemples:
  - ISO 9001: qualité
  - ISO 13485: services médicaux
  - ISO 14001: environnement
  - ISO 20000: services TI:
    - ie ITIL, avec en plus sys. de mgt améliorable dans le temps
  - ISO 22000: inspection alimentaires
  - ISO 29001: industrie pétrochimique

## 1.5. Normes ISO

- Principes ISO:
  - Amélioration continue



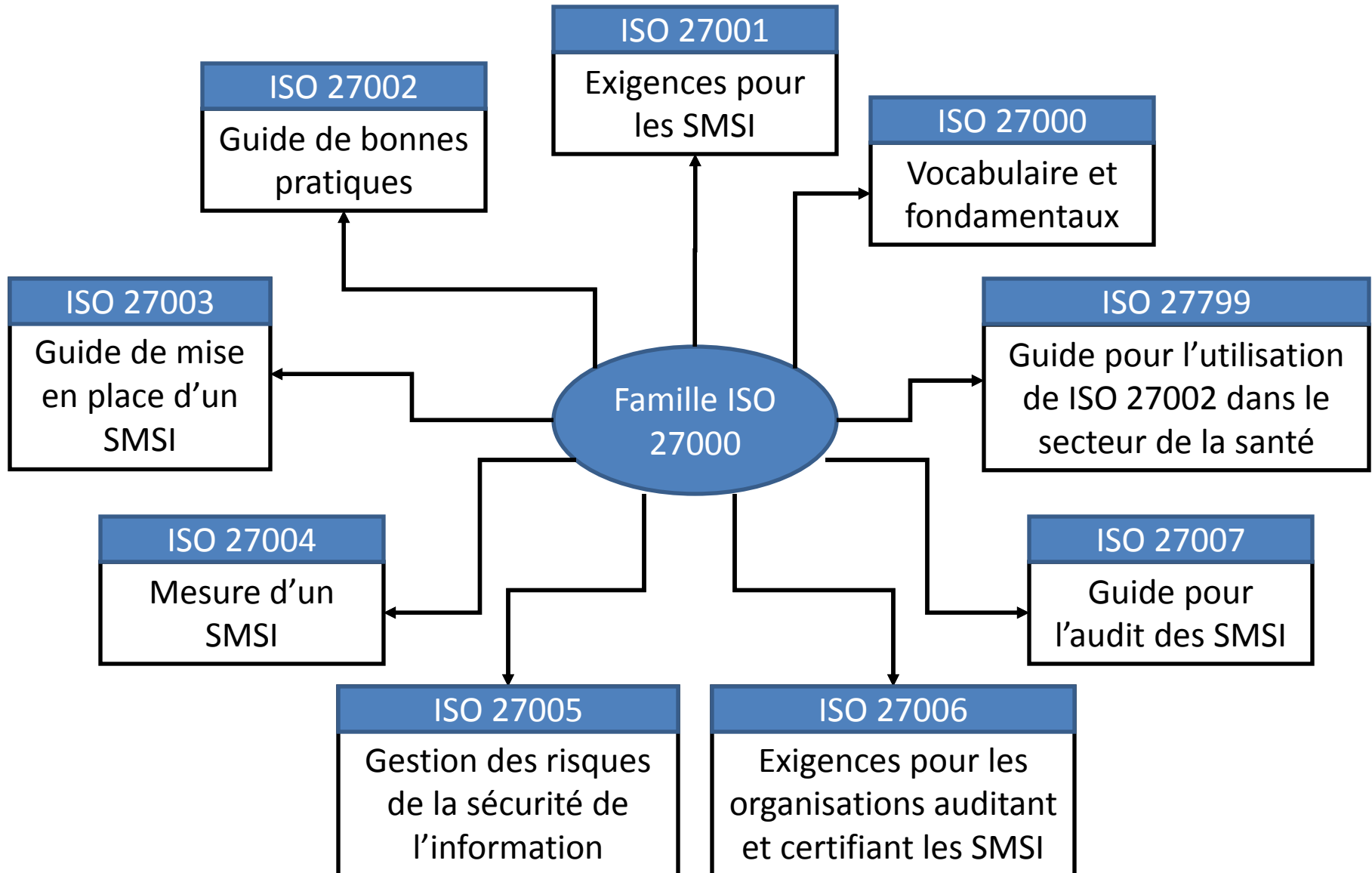
## 1.5. Normes ISO

- Pas d'implémentation parfaite dès le début
- Exemple:
  - A1 (quelques astuces),
  - A2 (quelques contrôles),
  - A3 (optimiser les contrôles)
- Délai: dépend du périmètre (global ou certains process) et des ressources (internes ou clé en main)
- Cas de IAM :
  - 2 ans (50 personnes en interne, + consultants externes), sensibilisation de 11500 personnes
  - Remontée d'information au PDG (tous les 2 jours)
  - Conseiller n°1: adjoint
- Cas de Bank Al Maghrib:
  - 3000 personnes
  - Étude: 6 mois
  - mise en place: 1 an
  - Chemin le plus critique : 4 mois (dépend du ps le plus long)

## 1.5. Normes ISO

- Normes en sécurité:
  - Exemples:
    - ISO 27001: SMSI
    - ISO 27002: bonnes pratiques
    - ISO 18033: cryptographie
    - ISO 18044: gestion des incidents
    - ISO 13335: GMIT (Guidelines for Management of IT Security)
    - ISO 10736: protocoles de transport
    - ISO 15408: critères communs

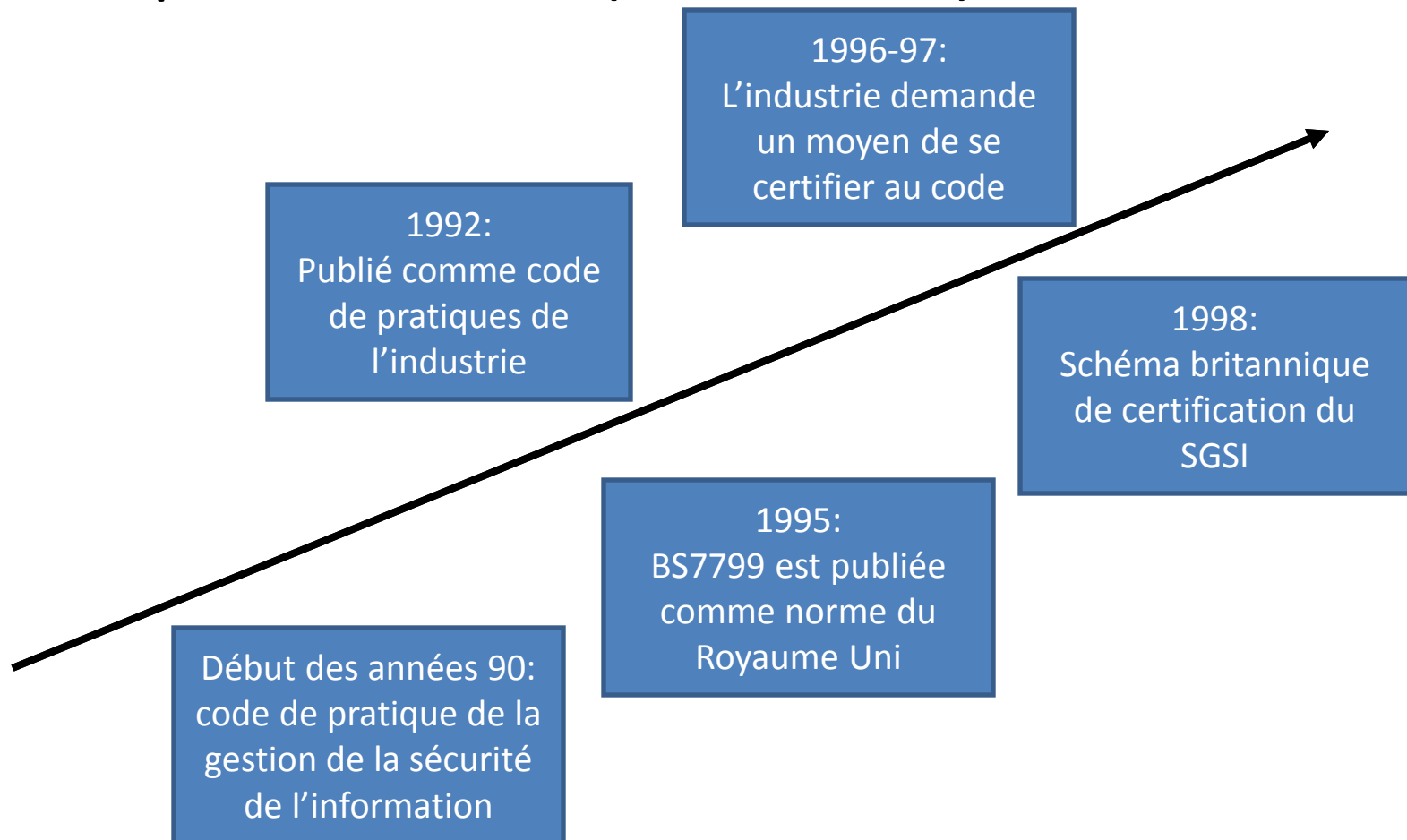
# 1.6. Famille ISO 27000





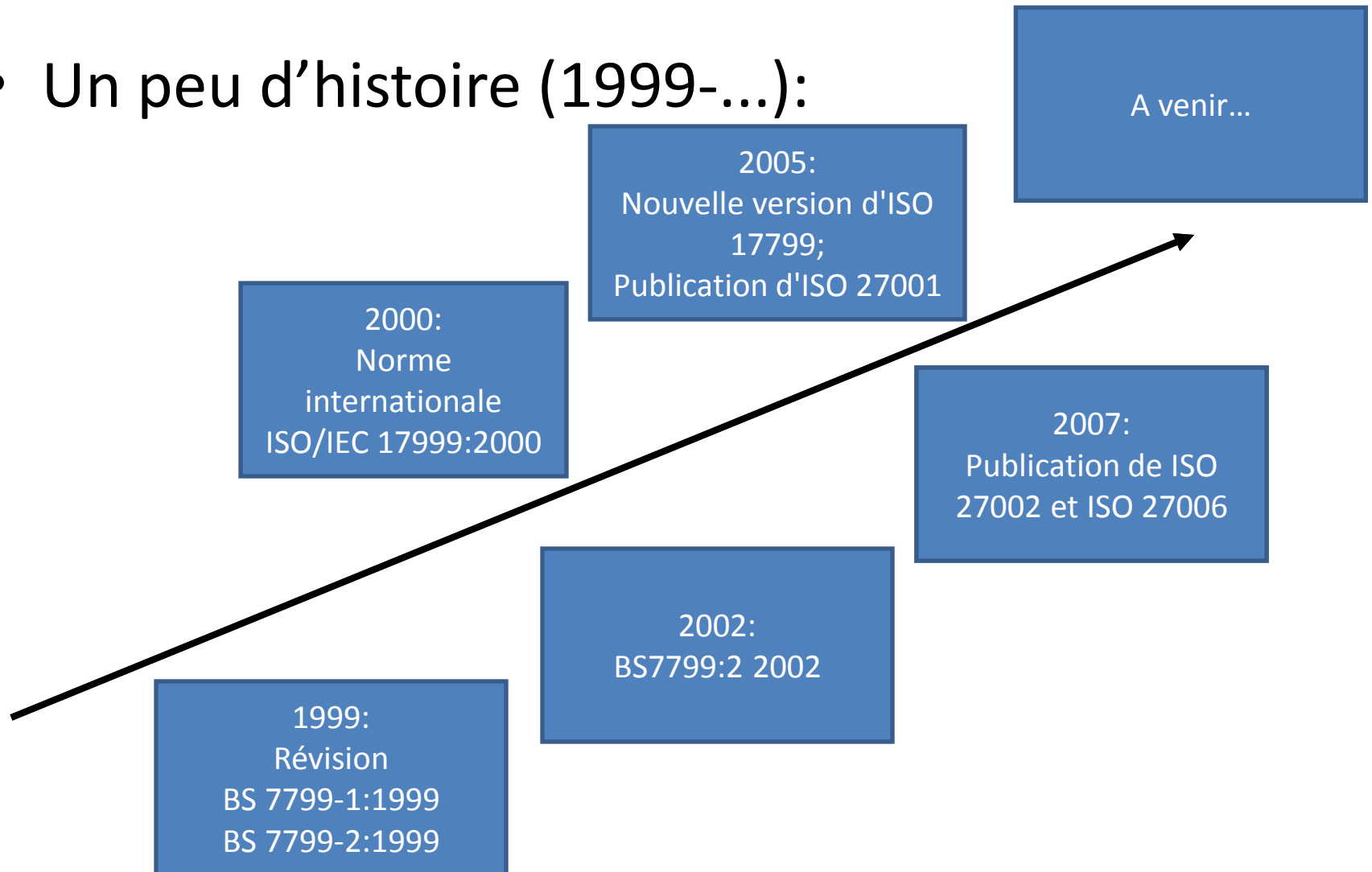
## 1.6.1. ISO 27001

- Un peu d'histoire (1990-1998):



## 1.6.1. ISO 27001

- Un peu d'histoire (1999-...):

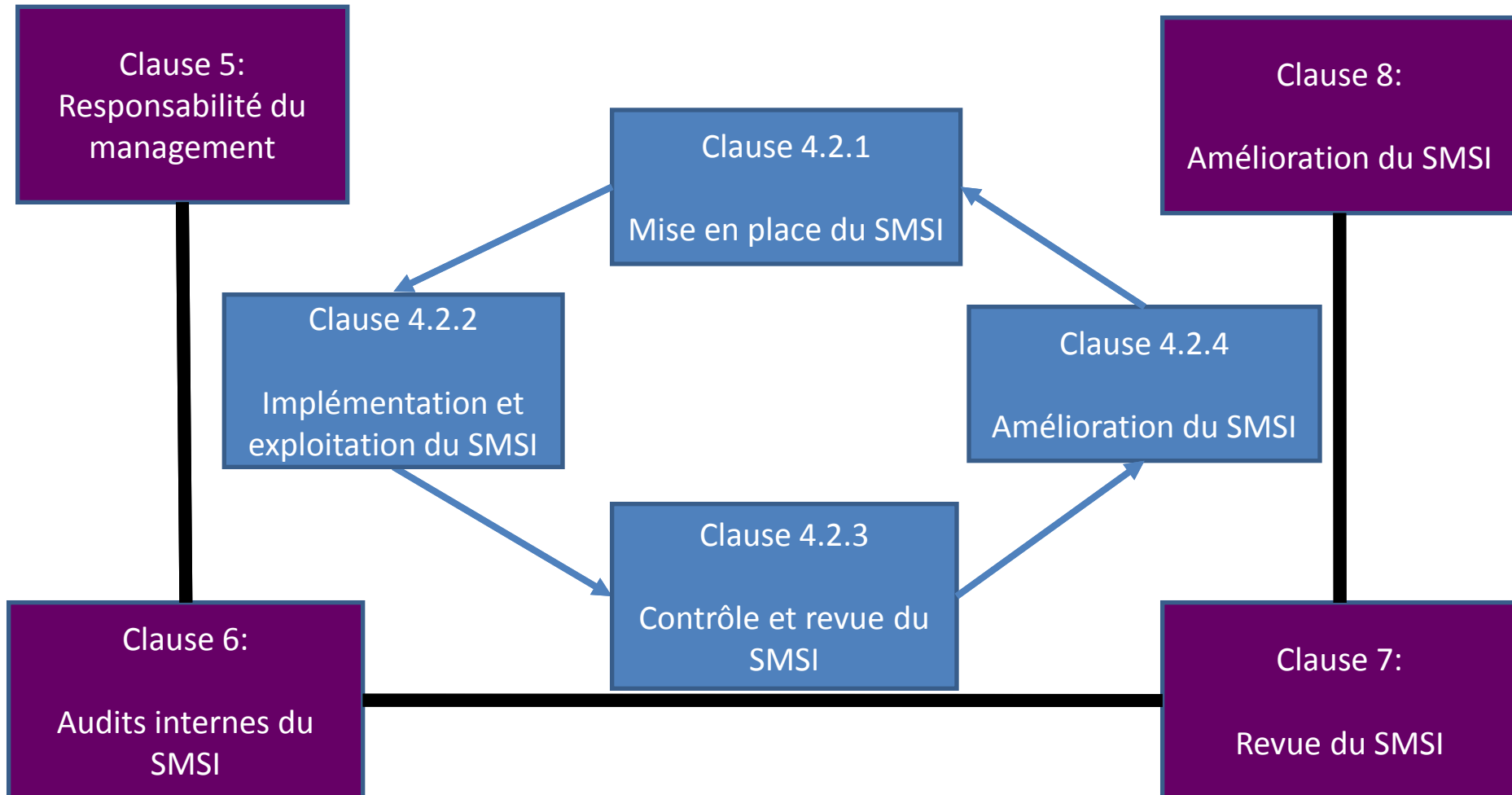


## 1.6.1. ISO 27001

- ISO 27001: gestion de la sécurité de l'information
  - Spécification pour les SMSI:
    - Spécifie les exigences pour la conception, la mise en place et la documentation des SMSI (<> directive)
    - Spécifie les exigences pour la mise en œuvre de contrôles conformément aux besoins des organisations
    - L'annexe A se compose de 11 sections comportant 133 contrôles de ISO 27002
    - Les organismes peuvent postuler à la certification à cette norme
    - Voir clause 0.1

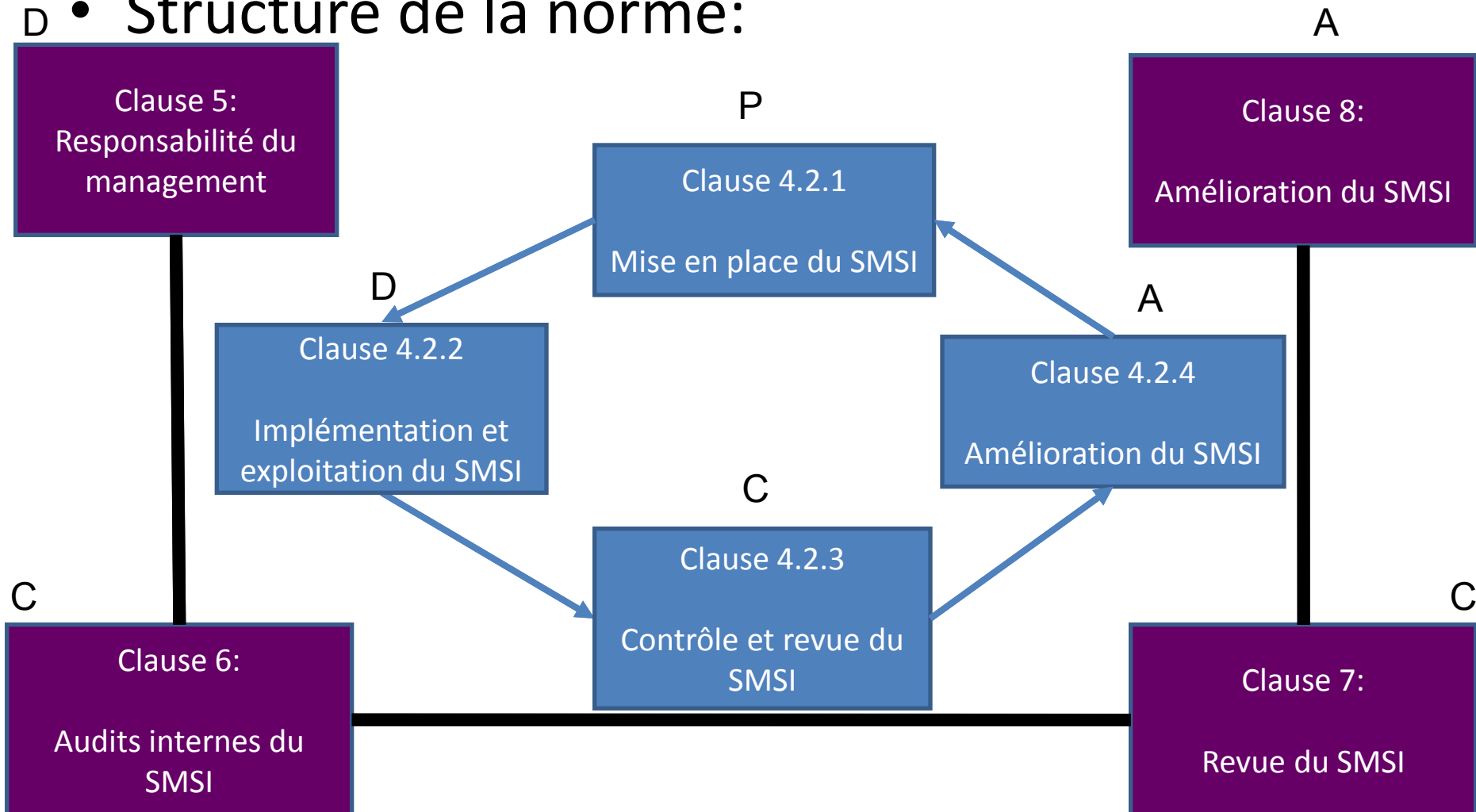
# 1.6.1. ISO 27001

- Structure de la norme:



# 1.6.1. ISO 27001

## D • Structure de la norme:



## 1.6.2. ISO 27002

- ISO/IEC 27002:2007 « technologies de l'information – code de pratiques pour la gestion de la sécurité de l'information JTC1/SC27/WG1 »
  - Basée sur BS 7799-1:2002
  - A utiliser comme document de référence
  - Fournit la gamme complète de contrôles de sécurité
  - Basée sur les meilleures pratiques de sécurité de l'information
  - Composée de 11 sections comportant 133 contrôles (il convient de les mettre en place, certains sont des exigences)
  - Certification ISO 27002 non supportée
  - Voir clauses 5 à 15

## 1.6.2. ISO 27002

- Domaines de ISO 27002 (Annexe 1 ISO 27001)
  - Annexe => Contrôle, Sinon c'est une exigence

A5	Politique de sécurité
A6	Organisation de la sécurité de l'information
A7	Gestion des actifs (classification des informations & des biens)
A8	Sécurité des Ressources Humaines
A9	Sécurité physique et environnementale
A10	Gestion des communications et des opérations
A11	Contrôle d'accès
A12	Acquisition, développement et entretien des Systèmes d'Information
A13	Gestion des incidents de la Sécurité de l'Information (helpdesk avec failles de sécurité. Exemple: vol, sabotage, coupure, etc.)
A14	Gestion de la continuité des affaires (continuité d'activité)
A15	Conformité (légale & réglementation interne de l'entreprise)

## 1.6.3. ISO 27003

- Le but de la norme ISO/IEC 27003 est de fournir de l'aide et des conseils nécessaires à la mise en place d'un système de management de la sécurité de l'information (SMSI)
- Cette norme fournira différentes informations et conseils concernant l'utilisation du modèle PDCA
- Norme très récente
- Voir clauses 1 à 11



## 1.6.4. ISO 27004

- Norme internationale qui devra fournir des conseils sur le développement et l'utilisation d'indicateurs afin d'évaluer l'efficacité des SMSI, et des contrôles utilisés pour mettre en application et contrôler la sécurité de l'information, comme indiqué dans ISO/IEC 27001
- Tableau de bord par rapport aux 133 contrôles (vérifier leur efficacité et leur performance)

## 1.6.4. ISO 27004

- Conseils incluant:
  - Mesures de contrôle
  - Mise en place d'un programme de mesure de sécurité de l'information
  - Rassembler, analyser, et communiquer ces mesures aux dépositaires
  - Utiliser les mesures collectées en tant que facteurs de décision pour les activités du SMSI
  - Faciliter l'amélioration du ps d'évaluation du SMSI
- Voir clauses 6 à 10

## 1.6.5. ISO 27005

- Fournit les techniques pour la gestion des risques de sécurité de l'information
- Inspirée de:
  - ISO Guide 63 (gestion du risque, vocabulaire, lignes directrices pour l'utilisation de la norme)
  - BS7799-3:2006:SMSI
  - ISO 13335: GMIT (lignes directrices pour la gestion de la sécurité de l'information)
  - NIST 800-30 (Guide de la gestion du risque liées aux systèmes d'information)
  - CRAMM (Risk Analysis and Management Method)
- Voir clauses 7 à 12

## 1.6.6. ISO 27006

- « Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems »
  - Définit les conditions générales de gestion d'un organisme de certification pouvant délivrer des certificats de conformité ISO 27001
- Voir clauses 4 à 10

## 1.6.7. ISO 27007

- Titre: « **Technologies de l'information -- Techniques de sécurité -- Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information** »
  - Standard pour les directives de l'audit des SMSI
  - Fournira des conseils pour les auditeurs conduisant des audits des systèmes de management de sécurité de l'information contre ISO/IEC 27001
- Date prévue pour la publication: 15-10-2011

## 1.6.7. ISO 27008+

- ISO 27008 et les suivants :
  - réservés pour la création de normes spécifiques à des industries (télécommunication, santé, automobile, etc.) ou à des domaines spécifiques de la sécurité de l'information (sécurité applicative, cyber sécurité, etc.)
- Exemples:
  - ISO 27012: Directives pour le domaine financier
  - ISO 27013: Directives pour le domaine manufacturier
  - ISO 27015: Directives de certification
  - ISO 27016: Audits et revues
  - ISO 27031: Continuité des affaires pour les TI
  - ISO 27032: Directives pour la cybersécurité
  - ISO 27033: Révision des ISO 18028 (sécurité des réseaux)
  - ISO 27034: Directives pour la sécurité des applications

# Activité

- Exercice 1:
  - En vous basant sur l'histoire, l'organisation, et les processus métier de votre organisation actuelle, déterminez et expliquez les 5 plus grands avantages de l'implémentation de la norme ISO 27001 pour votre organisation, et comment votre organisation peut mesurer ces avantages grâce aux mesures de la performance (indicateurs).

## 1.7. ISO 27001 et les principes de l'OCDE

- L'OCDE a défini des lignes directrices:
  - Promouvoir parmi l'ensemble des parties prenantes une culture de sécurité en tant que moyen de protection des systèmes et réseaux d'information
  - Renforcer la sensibilisation aux risques pour les systèmes et réseaux d'information aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, ainsi qu'à la nécessité de les adopter et de les mettre en œuvre
  - Promouvoir parmi l'ensemble des parties prenantes une plus grande confiance dans les systèmes et réseaux d'information et dans la manière dont ceux-ci sont mis à disposition et utilisés



## 1.7. ISO 27001 et les principes de l'OCDE

- L'OCDE a défini des lignes directrices:
  - Créer un cadre général de référence aidant les parties prenantes à comprendre la nature des problèmes liés à la sécurité, et à respecter les valeurs éthiques dans l'élaboration et la mise en œuvre de politiques, pratiques, mesures et procédures cohérentes pour la sécurité des systèmes et réseaux d'information
  - Promouvoir parmi toutes les parties prenantes, la coopération et le partage d'informations appropriées pour l'élaboration et la mise en œuvre des politiques, pratiques, mesures et procédures pour la sécurité
  - Promouvoir la prise en considération de la sécurité en tant qu'objectif important parmi toutes les parties prenantes associées à l'élaboration et à la mise en œuvre de normes

## 1.7. ISO 27001 et les principes de l'OCDE

- L'OCDE a développé 9 principes de sécurité des systèmes d'information et des réseaux:
  - Sensibilisation
  - Responsabilité
  - Réponse
  - Éthique (non repris dans ISO 27001)
  - Démocratie (non repris dans ISO 27001)
  - Évaluation du risque
  - Conception de la sécurité et mise en œuvre
  - Gestion de la sécurité
  - Réévaluation

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Sensibilisation
    - 1<sup>ère</sup> ligne de défense pour assurer sécurité sys & réseau
    - Risques internes et externes
    - Parties prenantes:
      - Doivent comprendre que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes & réseaux sous leur contrôle mais également à autrui
      - Doivent réfléchir à la configuration de leur système, aux mises à jour disponibles, à la place qu'il occupe dans les réseaux, et aux bonnes pratiques à mettre en place

# 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Sensibilisation
    - Parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité

Phase PDCA correspondante:	Processus SMSI correspondant :
D	4.2.2 & 5.2.2

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Responsabilité des parties prenantes:
    - Tributaires des systèmes & réseaux d'information
    - Doivent comprendre leur resp. ds la sécurité des sys. & rés.
    - En être comptable (en fonction du rôle)
    - Doivent régulièrement examiner et évaluer politiques, pratiques, mesures & procédures pour s'assurer de leur adaptation à l'environnement
  - Cas des développeurs, concepteurs de Puits & Sces:
    - doivent prendre en considération la sécurité Sys & Rés,
    - diffuser les infos appropriées (màj opportunes pour meilleure compréhension par les utilisateurs des fonctions de sécurité et leur responsabilité)

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Responsabilité
    - Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information

Phase PDCA correspondante:	Processus SMSI correspondant :
D	4.2.2 & 5.1

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Réaction
    - Réaction aux incidents de sécurité prompte des parties prenantes dans un esprit de coopération
    - Cause:
      - Inter connectivité des systèmes & réseaux d'information
      - Propension rapide et massive des dommages à se répandre
    - Exigences:
      - Échange approprié d'informations sur menaces et vulnérabilités
      - Mise en place de procédures => coopération rapide et efficace
      - Possibilité d'échanges transfrontaliers si autorisé
    - Objectifs:
      - Prévenir, détecter & répondre aux incidents de sécurité

# 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Réaction
    - Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de la sécurité

Phase PDCA correspondante:	Processus SMSI correspondant :
C	4.2.3 et 6 à 7.3
A	4.2.4 et 8.1 à 8.3



## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Analyse et traitement du risque:
    - Évaluation des risques:
      - Permet de déceler les menaces & vulnérabilités
      - Doit être suffisamment large pour couvrir l'ensemble des
        - » facteurs internes et externes (technologie, etc.)
        - » facteurs physiques & humains
        - » Politiques et services de tierces partiesayant des implications sur la sécurité
      - Permet de déterminer le niveau acceptable de risques

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Analyse et traitement du risque:
    - Évaluation des risques:
      - Facilitera la sélection de mesures de contrôles appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information, compte tenu de la nature et de l'importance de l'information à protéger
      - Doit tenir compte des préjudices aux intérêts d'autrui ou causés par autrui rendus possibles par l'interconnexion croissante des systèmes d'information

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Analyse et traitement du risque
    - Les parties prenantes doivent procéder à des évaluations des risques

Activité	Phase PDCA correspondante:	Processus SMSI correspondant :
Analyse et traitement du risque	P	4.2.1
Réévaluation du risque	C	4.2.3 et 6 à 7.3

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Conception de sécurité et mise en œuvre:
    - Systèmes, réseaux & politiques nécessitent une coordination appropriée => optimiser la sécurité
    - Axe majeur: mesures de protection et solutions adaptées
      - Conçues et adoptées => prévenir ou limiter les préjudices possibles liés aux vulnérabilités et menaces identifiées
      - À la fois techniques et non techniques
      - Proportionnées à la valeur de l'information dans les S&R d'Org
  - Sécurité:
    - Élément fondamental de l'ensemble des Puits, Sces, Sys. & Rés.
    - Partie intégrante de la conception et architecture des systèmes
  - Utilisateur final: sélectionne et configure les Puits & Sces pour ses systèmes

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Conception de sécurité et mise en œuvre:
    - Les parties prenantes doivent intégrer la sécurité en tant qu'élément essentiel des systèmes et réseaux d'information

Phase PDCA correspondante:	Processus SMSI correspondant :
P	4.2.1
D	4.2.2 et 5.2

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Gestion de la sécurité
    - Objectif 1: Couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations
    - Exigences:
      - Fondée sur l'évaluation des risques, Dynamique et Globale
      - Inclure, par anticipation, des réponses aux menaces émergentes
      - Doit couvrir la prévention, détection et résolution des incidents, reprise des systèmes, maintenance permanente, contrôle et audit
    - Objectif 2: Créer un système cohérent de sécurité
    - Exigences:
      - Coordination et intégration des politiques de sécurité, pratiques, mesures et procédures

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Gestion de la sécurité
    - Exigences de la gestion de la sécurité sont fonction de :
      - niveau de participation, et du rôle de la partie prenante,
      - des risques en jeu
      - des caractéristiques du système
  - Conclusion
    - Les parties prenantes doivent adopter une approche globale de la sécurité
    - ISO 27001 : PDCA, prévention, détection, réponse aux incidents, maintenance, révision et audit

## 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Réévaluation
    - Découverte constante de vulnérabilités et menaces nouvelles ou évolutives
    - Parties prenantes:
      - Révision, réévaluation et modification de tous les aspects de la sécurité
      - Faire face à ces risques évolutifs



# 1.7. ISO 27001 et les principes de l'OCDE

- Comparaison avec ISO 27001 - annexe B:
  - Réévaluation
    - Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité

Activité	Phase PDCA correspondante:	Processus SMSI correspondant :
Examens réguliers	C	4.2.3 et 6 à 7.3
Amélioration	A	4.2.4 et 8.1 à 8.3

## 2. Principes fondamentaux

- Principes fondamentaux de la sécurité de l'information

## 2. Définitions

- Actif:
  - Tout élément représentant de la valeur pour l'organisme (clause 3.1) (en tant que support de l'information)
  - Exemples d'actifs (cf ISO 13335):
    - Informations/données, matériel, logiciel, matériel de télécommunication, média (support à l'information), documents, actifs financiers, matériel de production, services, confiance dans les services (paiements), environnement de travail, personnel, image de l'organisation
  - 3 Objectifs des contrôles de sécurité:
    - clause du domaine A7 (A7.1.1, A7.1.2 & A7.1.3)

## 2. Définitions

- Information:
  - Résultat du traitement, de la manipulation, et de l'organisation des données de manière à s'ajouter à la connaissance du récepteur (contexte dans lequel les données sont acquises)
    - Données+information=> connaissance
    - Exemple:fichier plat+logiciel de traitement=>tableau de bord
  - Enregistrement ou « record »: information créée, reçu et maintenue en tant que preuve et source d'information par organisation ou personne dans le but de prouver une transaction ou de servir de preuves dans un cadre légal (source: ISO 15489-1 clause 3.15)

## 2. Définitions

- Catégories d'information :
  - imprimée ou écrite sur papier, stockée électroniquement, transmise par courrier ou par méthode électronique, exposée sur des vidéos corporatives, mentionnée lors de la conversation, etc.
  - Méthode:
    - Identifier les supports de transmission de l'information
    - Objectifs:
      - sécuriser le processus/information métier le plus critique (actif primaire)
      - sécuriser l'homme/logiciel qui traite (actif support)
  - 2 Objectifs des contrôles de sécurité:
    - clauses du domaine A7.2 (A7.2.1 & A7.2.2)

## 2. Définitions

- Sécurité de l'Information:
  - Définition 1: Vise à protéger l'information contre une large gamme de menaces, de manière à garantir la continuité des transactions, à réduire le plus possible le risque et à optimiser le retour sur investissement ainsi que les opportunités en termes d'activité pour l'organisme (ISO/IEC 17799:2005)
    - Voir clauses 0.3 & 0.4 ISO 27002 (exigences et risques)

## 2. Définitions

- Sécurité de l'Information:
  - Définition 2: Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information; d'autres propriétés telles que l'authenticité, l'imputabilité, la non répudiation et la fiabilité, peuvent également être concernées (ISO/IEC 17799:2005)
    - Voir clause 0.1 ISO 17799
      - Mise en œuvre de mesures adaptées regroupant les règles, processus, procédures, structures organisationnelles et fonctions matérielles et logicielles
      - Mesures doivent être spécifiées, mises en œuvre, suivies, réexaminées, et améliorées aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'un organisme
      - Agir de manière concertée avec les autres processus de l'organisme

• Voir clause 0.6 ISO 27002 (base de la sécurité de

## 2. Définitions

- Vulnérabilité:
  - Faiblesse d'un actif ou d'un groupe d'actifs susceptibles d'être l'objet d'une menace (ISO/IEC 13335-1:2004)
  - Elle permet d'attaquer la confidentialité, l'intégrité et/ou la disponibilité de l'information
  - Localisation: logiciel, matériel, procédure
    - Exemples: Brèche dans OS, absence de contrôle d'accès sur serveur, procédure de mäj d'antivirus non efficace, port ouvert sur pare-feu, accès modem non restreint



## 2. Définitions

- Vulnérabilité:
  - Classification:
    - Ressources Humaines:
      - formation insuffisante (sécurité), manque de connaissance, manque de système de surveillance, manque de règlement pour utilisation média, eMail, télécom, personnel non motivé ou contrarié, non remplacement des droits d'accès après fin d'une mission de travail...
    - Environnement physique de l'entreprise:
      - manque de protection physique pour le contrôle d'accès des personnes dans l'enceinte de l'entreprise, Position de l'entreprise dans une zone inondable, sismique, sensible aux désastres naturels, zone de stockage non protégée, sensibilité du matériel à l'humidité, aux variations de température, à la poussière, etc.

## 2. Définitions

- Vulnérabilité:
  - Classification:
    - Communication et Opérations de gestion:
      - Interface utilisateur compliquée, contrôle des changements inadéquats, gestion du réseau inadéquate, manque de procédures de back-up, aucune séparation des fonctions & contrôle du copiage
    - Contrôle d'accès:
      - Séparation inadaptée du réseau informatique, manque de mécanismes d'identification et d'authentification, aucune ou mauvaise politique de contrôle d'accès, aucune révision des droits d'accès utilisateurs, etc.
    - Maintenance, développement et acquisition des SI:
      - Manque de contrôle des données E/S, aucun contrôle du téléch. & installation de logiciels, protection inadéquate des clefs cryptographiques, manque de validation des données traitées, etc.

## 2. Définitions

- Menace :
  - Cause potentielle d'un incident indésirable pouvant affecter une organisation (ISO/IEC 13335-1:2004)
  - Danger potentiel pour l'information ou pour le système d'information. Elle peut se traduire par un voleur/attaquant qui exploite une vulnérabilité

## 2. Définitions

- Menace :
  - Plusieurs formes:
    - Intrus ayant accès au réseau par un port du pare-feu, accès aux données non conforme à la politique de sécurité, tornade anéantissant une infrastructure, employé faisant une erreur involontaire pouvant porter atteinte à la confidentialité et à l'intégrité de l'information, Pirate informatique
    - Incendie, attaque terroriste, séisme, inondation, foudre, tempête, ouragan, désastres naturels, interruption momentanée des activités, détérioration ou panne des médias, vandalisme, vol, etc.

## 2. Définitions

- Menace :
  - Plusieurs formes:
    - Mise en péril des actifs, espionnage industriel, perte de l'information, faille de sécurité, accès au réseau d'une personne non autorisée, dommages causés par des tests de pénétration, dommages causés par les sous-traitants, fournisseurs, collaborateurs, erreur humaine
    - Disfonctionnement de la climatisation, disfonctionnement des équipements de confort (climatisation, chauffage, électricité, ...), interruption des activités, erreur d'utilisation, erreur de maintenance, panne du matériel, indisponibilité du matériel

## 2. Définitions

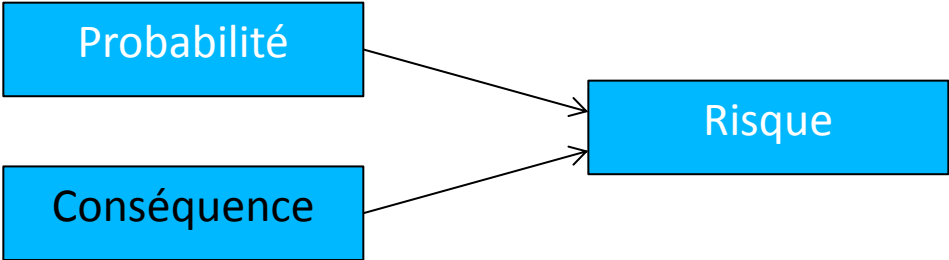
- Menace :
  - Plusieurs formes:
    - Infraction de la législation, rupture des obligations contractuelles, destruction des enregistrements, destruction du plan de continuité de l'entreprise, manque de communication des différents services de l'entreprise, falsification des données, fraude, utilisation illégale de logiciel, interférence, utilisation à mauvais escient des ressources et actifs de l'entreprise, contrefaçon

## 2. Définitions

- Relation entre Vulnérabilité et Menace :
  - identifier objet, puis vulnérabilités, puis menaces

Vulnérabilité	Menace
Entrepôt non protégé et non surveillé	Vol
Interface de saisie compliquée	Erreur de saisie par le personnel
Pas de séparation de tâches	Fraude, Utilisation non autorisée d'un système
Données non encryptées	Vol d'information
Utilisation de logiciels piratés	Poursuite judiciaire, Virus
Pas de revue des droits d'accès	Accès non autorisé par des personnes qui ont quitté l'organisation
Pas de procédure de copies de sauvegarde	Perte d'informations

## 2. Définitions

- Risque :
    - Combinaison de la probabilité de survenance d'un évènement et de ses conséquence (ISO/IEC Guide 73:2002)
- 
- ```
graph LR; A[Probabilité] --> D[Risque]; B[Conséquence] --> D;
```
- The diagram illustrates the components of risk. It features three blue rectangular boxes. On the left, there are two boxes stacked vertically: the top one is labeled 'Probabilité' and the bottom one is labeled 'Conséquence'. Arrows from both of these boxes point towards a single box on the right labeled 'Risque', indicating that risk is a combination of both probability and consequence.
- Voir clauses 3.9 à 3.15 (ISO 27001:2005 – Guide 73)
  - Risque = produit de:
    - Vulnérabilité
    - Menace
    - Impact



## 2. Définitions

- Confidentialité:
  - Propriété que l'information ne soit accessible qu'aux [individus, entités ou processus autorisés] [ $\Leftrightarrow$  actifs] (ISO/IEC Guide 13335-1:2004)
  - Exemple:
    - Problème: les données personnelles des salariés ne doivent être accessibles qu'au personnel du département des RH autorisé (personnel qui en a besoin)
    - Solution: contrôle d'accès / Contrôle: chiffrement
    - Mesures à différents niveaux:
      - Physique: serrures sur les portes, armoires d'archivage, coffre-fort
      - Logique: contrôle d'accès à une information, groupe d'info, fichier

## 2. Définitions

- Confidentialité:
  - Méthodologie pour prévention du risque:
    - Identification des menaces et vulnérabilités
    - Évaluation des risques associés
    - Sélection d'un système de contrôles
    - Mise en place et application
  - Remarque:
    - L'actif tangible prend la valeur de l'information qu'il contient

## 2. Définitions

- Intégrité:
  - Propriété de sauvegarder l'exactitude et la qualité des actifs (ISO/IEC Guide 13335-1:2004)
  - Exemple:
    - les données comptables doivent se conformer à la réalité (complet et exact). L'exactitude se traduit par l'absence d'altération de l'information

## 2. Définitions

- Intégrité:
  - Moyen:
    - Dispositifs de vérification automatique d'intégrité de l'information (dans les lecteurs, médias, systèmes télécom)
    - Contrôles d'intégrité essentiels aux SE, logiciels et applications
      - Évitent la corruption intentionnelle ou involontaire des programmes et données
      - Inclus dans les procédures, réduisent les risques d'erreurs, vol ou fraude
      - Exemples: Contrôles pour la validation des données, Formation des utilisateurs, Contrôles au niveau opérationnel

## 2. Définitions

- Disponibilité:
  - Propriété qu'une information soit accessible et utilisable au moment voulu par une entité autorisée (ISO/IEC Guide 13335-1:2004)
  - Exemple: données relatives à la clientèle accessibles au département marketing
  - Exigences:
    - Système de contrôle (ex. sauvegarde des données)
    - Planification de la capacité
    - Procédures
    - Critères pour l'approbation des systèmes, procédures

## 2. Définitions

- Disponibilité:
  - Exemples de procédures:
    - Procédures de gestion des incidents, la gestion des supports informatiques amovibles,
    - Procédures de traitement de l'information, le maintien et le test d'équipements,
    - Procédures de continuité d'affaires, procédures pour contrôler l'utilisation des systèmes

## 2. Définitions

- **Activité 2: évaluation du risque**
  - Déterminez les menaces et vulnérabilités associées aux situations suivantes. Indiquez ensuite les impacts potentiels, et si les risques affecteraient la confidentialité, l'intégrité, et/ou la disponibilité de l'information. Complétez la matrice de risque et préparez-vous à discuter vos réponses après l'exercice:
    1. L'ancien VP de la comptabilité est embauché par un concurrent
    2. Un disque amovible contenant les sauvegardes du code source des applications développées par une entreprise est introuvable à son bureau de Montréal
    3. Le webmaster ayant développé le site web corporatif d'une entreprise s'occupe des mises à jour et de la mise en production du site
    4. Tous les équipements de télécommunication ont le même mot de passe. Le mot de passe est connu seulement des programmeurs et des techniciens
    5. Votre entreprise externalise le développement de ses produits
    6. Votre entreprise a acheté une liste de 500.000 courriels de clients potentiels d'une compagnie située aux Bahamas afin de commencer une campagne de publicité sur Internet

### 3. Systèmes de management de la sécurité de l'information (SMSI)

- SMSI:
  - Partie du système de gestion **global**, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information (clause 3.7)



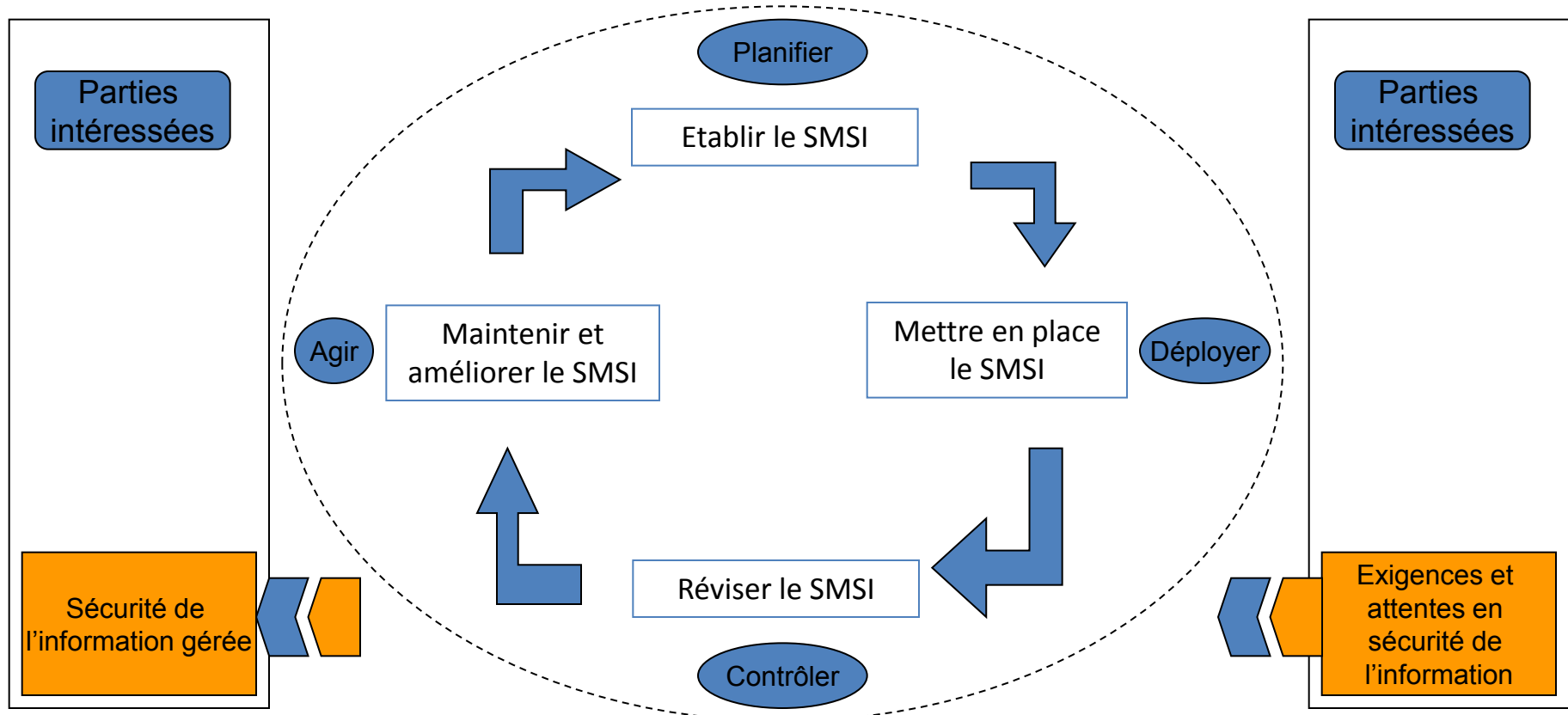
### 3. Systèmes de management de la sécurité de l'information (SMSI)

- SMSI:
  - Exemple:
    - Organisations utilisent des systèmes de gestion pour développer leurs politiques et les mettre en pratiques via des objectifs utilisant:
      - Une structure organisationnelle
      - Des processus systématiques et des ressources associées
      - Une méthodologie d'évaluation
      - Un processus de révision pour s'assurer que les problèmes sont corrigés adéquatement et que les opportunités d'amélioration sont reconnues et mises en œuvre lorsqu'elles sont justifiées
    - Remarque: ce qui est contrôlé doit être mesuré, ce qui est mesuré doit être géré

### 3. Systèmes de management de la sécurité de l'information (SMSI)

- L'approche par processus:
  - ISO 27001 encourage l'adoption d'une approche par processus pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI d'un organisme.
  - Contraire à l'approche par unité organisationnelle
  - Voir (v) clause 0.2 (ISO/IEC 27001:2005) :
    - approche processus (a, b, c & d)

### 3. Systèmes de management de la sécurité de l'information (SMSI)



– Voir (v-vi) clause 0.2 ISO/IEC 27001:2005

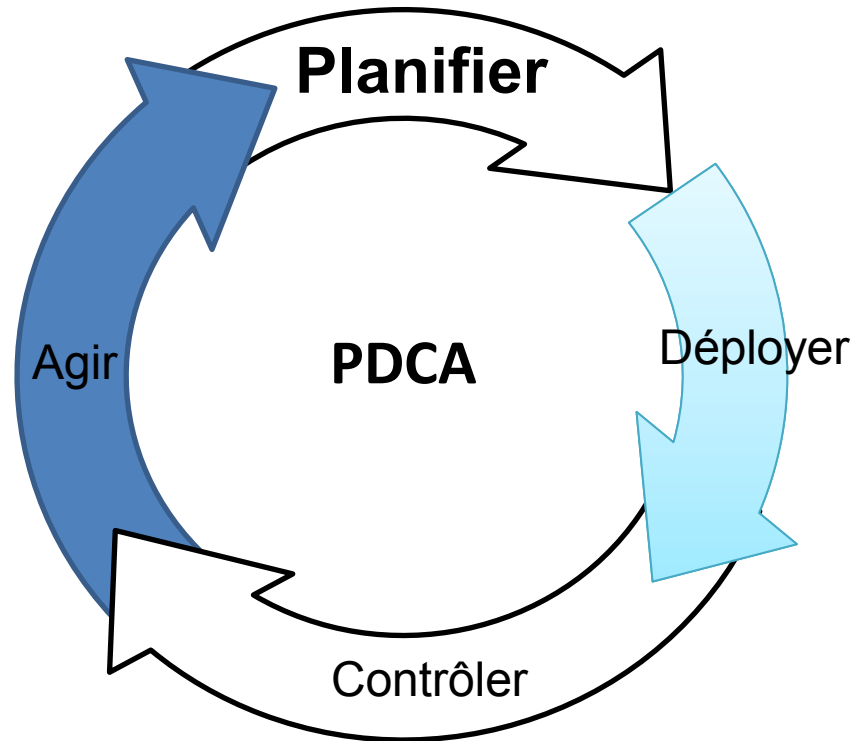
» approche processus (figure & tableau 1)

### 3. ISO27001 : Annexe C

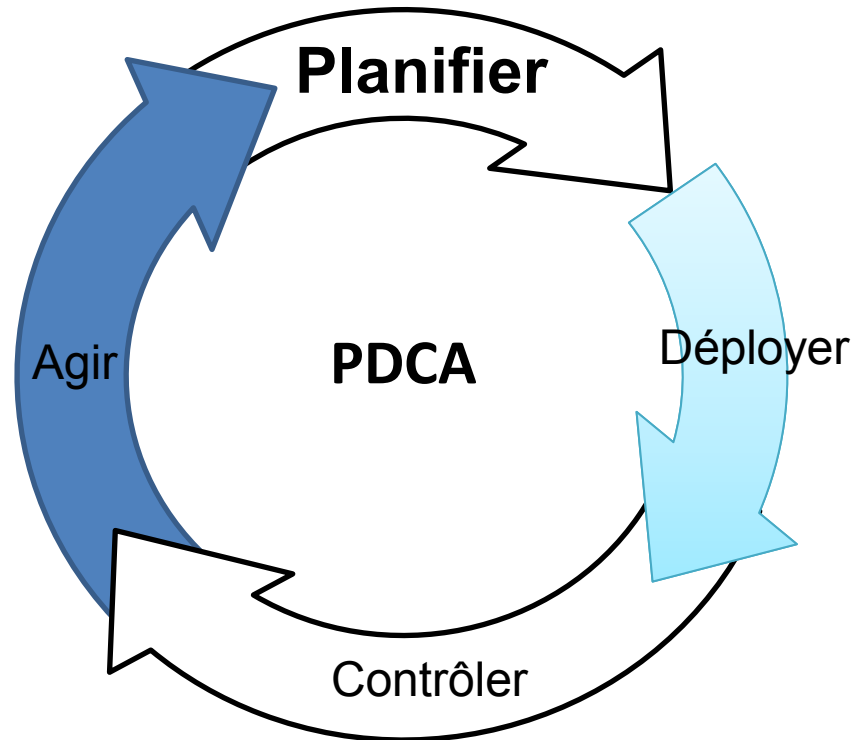
| ISO 27001:2005                      | ISO 9001:2000                          | ISO 14001:2004                      |
|-------------------------------------|----------------------------------------|-------------------------------------|
| 4. SMSI                             | 4. Système de management de la qualité | 4. Système de gestion environnement |
| 5. Responsabilité des gestionnaires | 5. Responsabilité des gestionnaires    | 5. Responsabilité des gestionnaires |
| 6. Audit interne                    | 6. Audit interne                       | 6. Audit interne                    |
| 7. Analyse par les gestionnaires    | 7. Analyse par les gestionnaires       | 7. Analyse par les gestionnaires    |
| 8. Amélioration continue            | 8. Amélioration continue               | 8. Amélioration continue            |

- Voir clause 0.3 (ISO/IEC 27001:2005): compatibilité avec d'autres systèmes
- PAS 99 (Publicly Available Specification): cadre de référence aidant les organisations voulant implémenter un système de management en adéquation avec plus d'une des normes ISO 9001, 14001, 27001, 22000, 20000, ou OHSS 18001 (éviter les conflits, réduire les doublons)

## 3. Planifier



## 3. Planifier

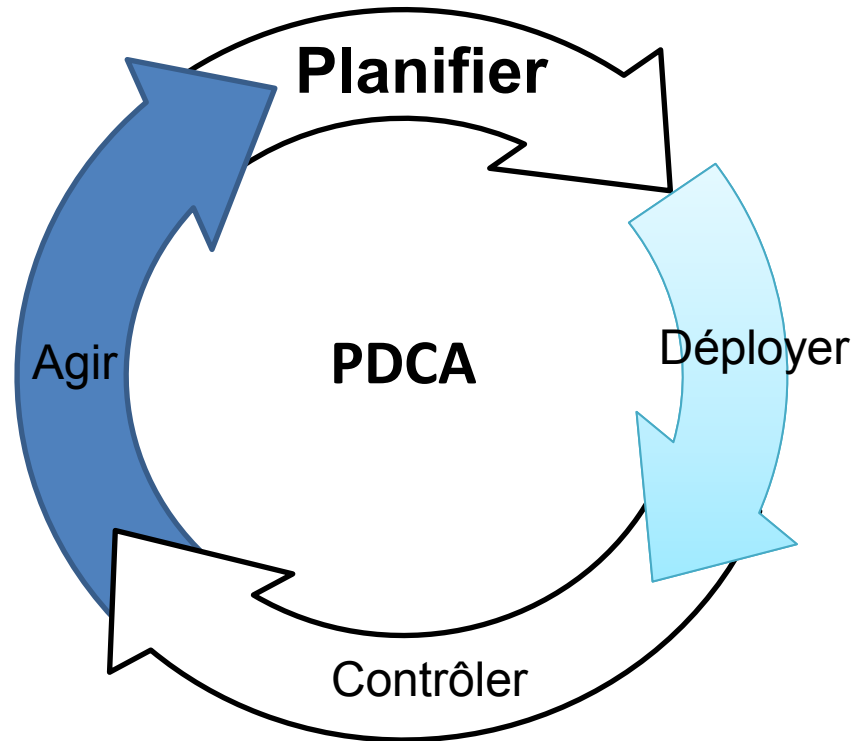


1.1. Etat des lieux

1.2. Analyse des écarts

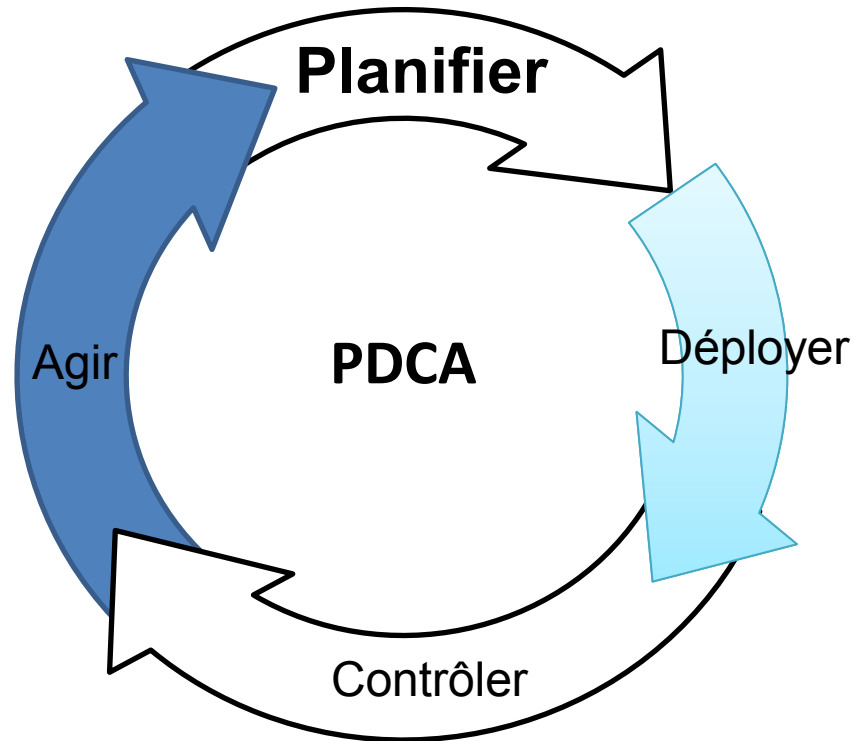
1.3. Business case

## 3. Planifier



- 3.1. Rôles et responsabilités
- 3.2. Domaine d'application et limites
- 3.3. Politique

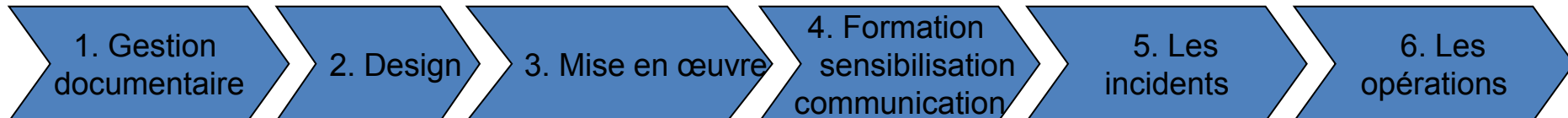
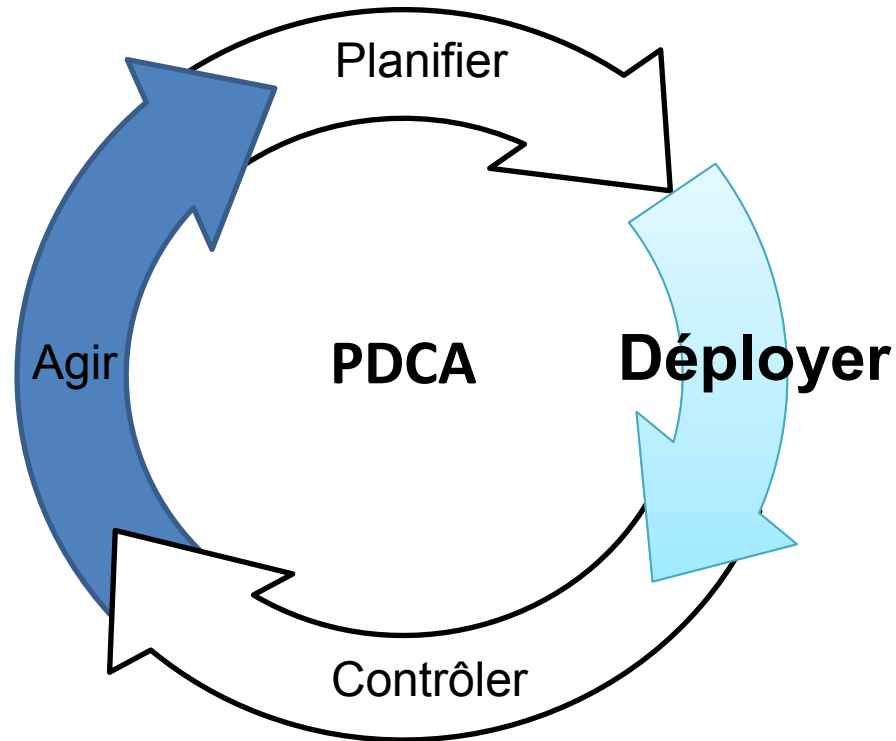
## 3. Planifier



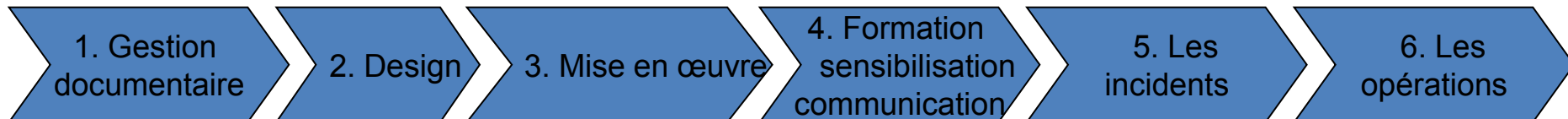
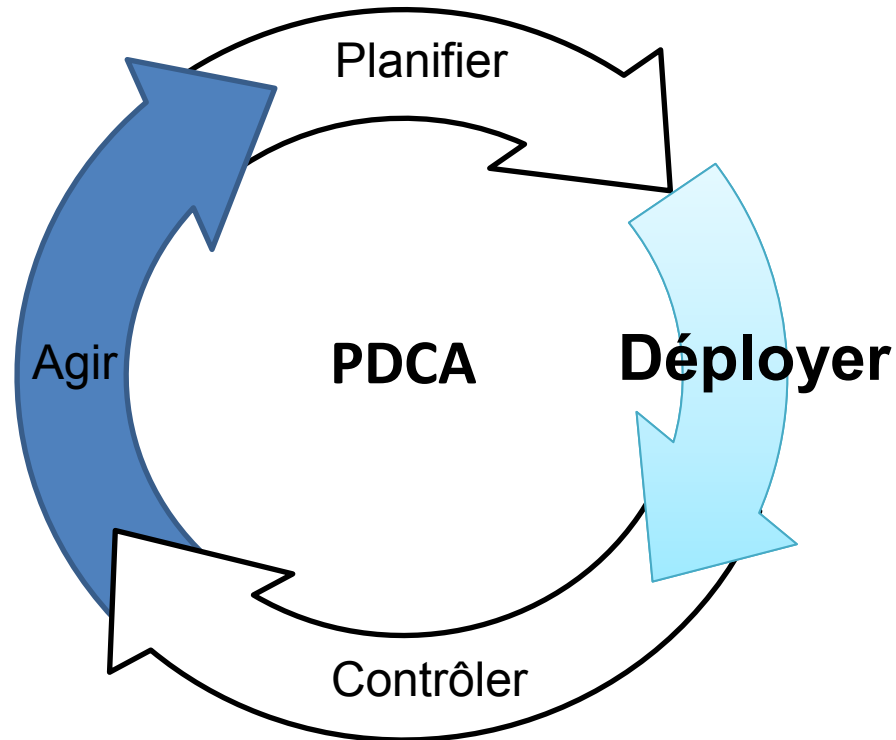
- 4.1. L'approche d'appréciation du risque
- 4.2. Identifier, Analyser, et Évaluer les risques
- 4.3. Le Traitement des Risques



## 3. Déployer

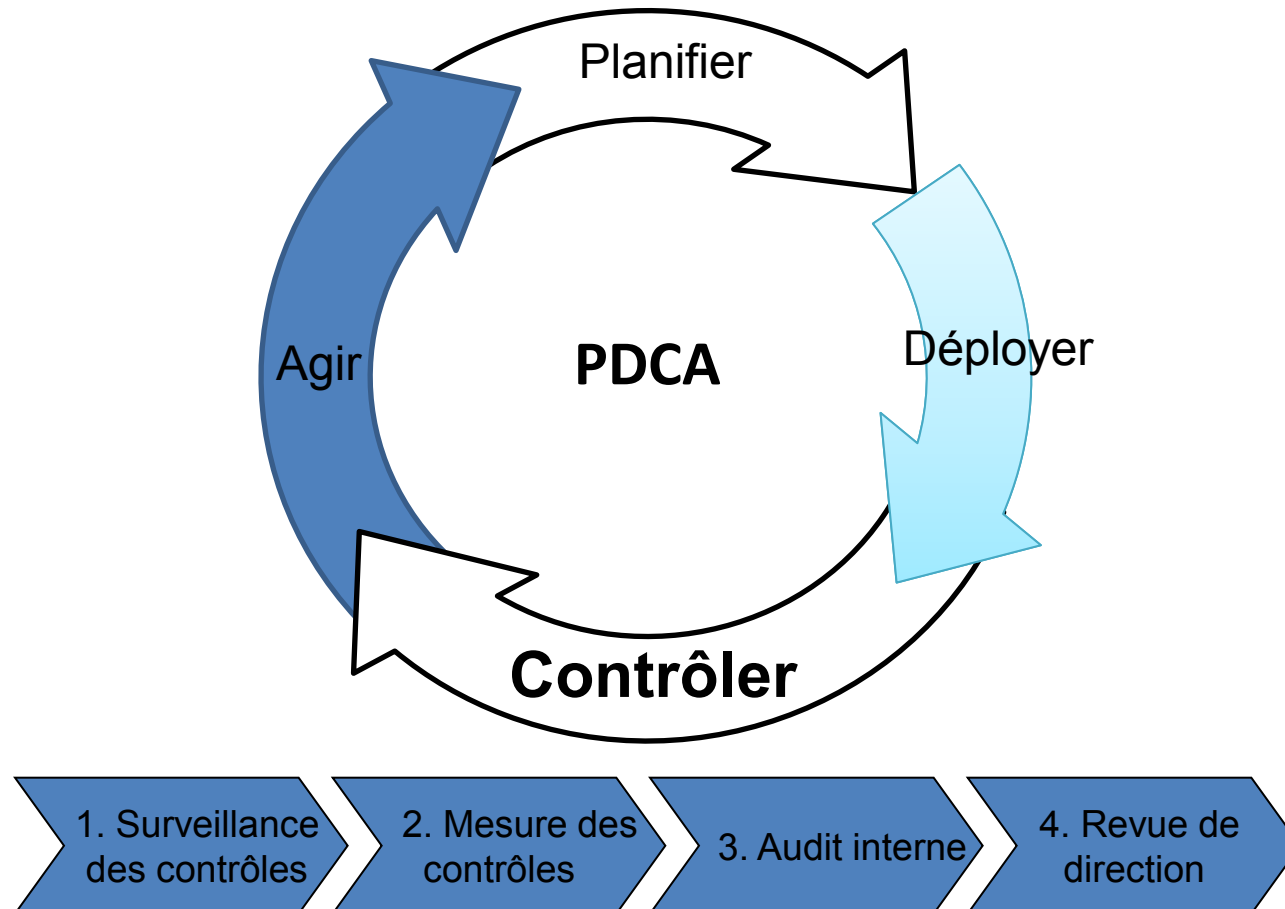


## 3. Déployer



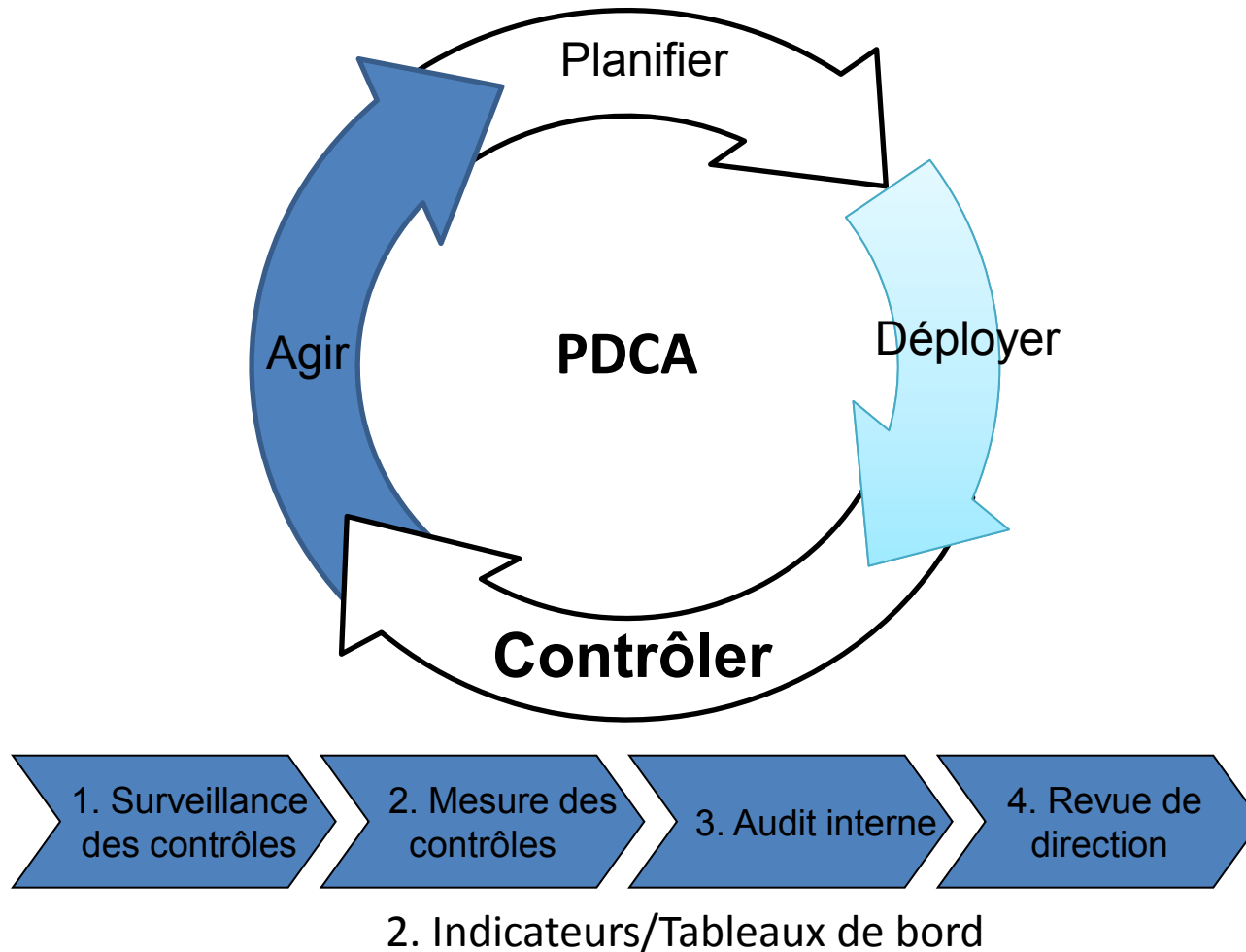
- 1.1. Politique
- 1.2. Cycle de vie
- 1.3. Création des gabarits
- 1.4. Système de gestion

### 3. Contrôler

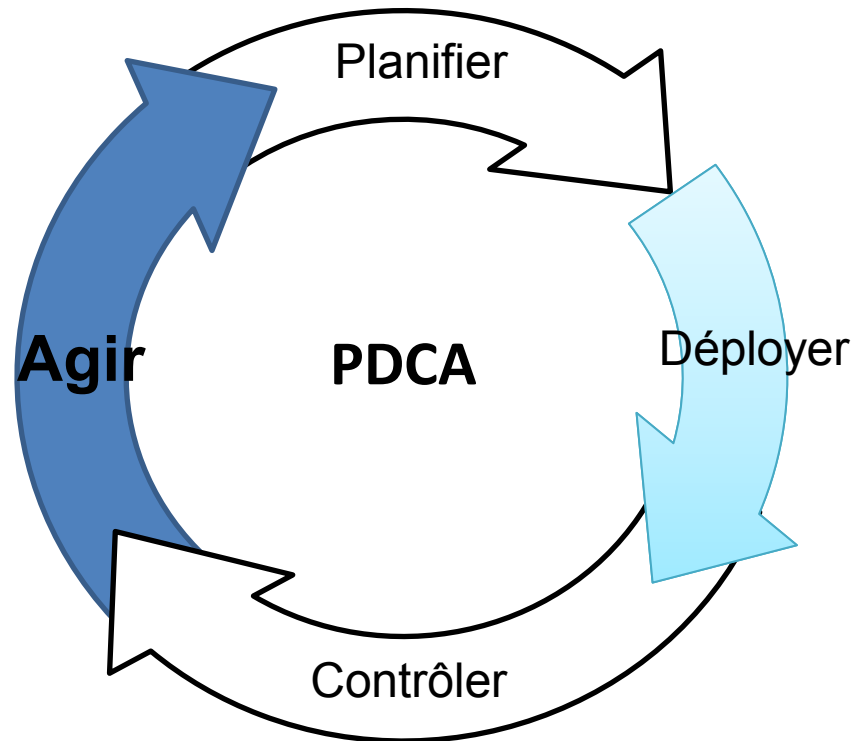


– Améliorer le SMSI

### 3. Contrôler



## 3. Agir

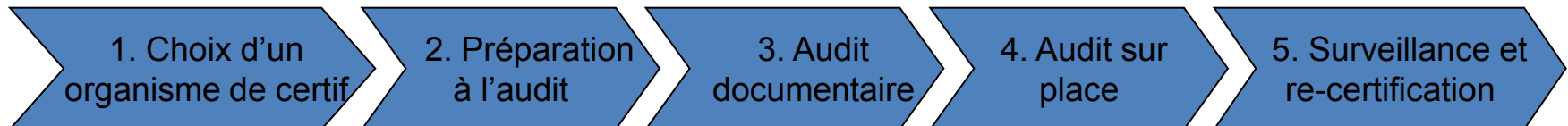
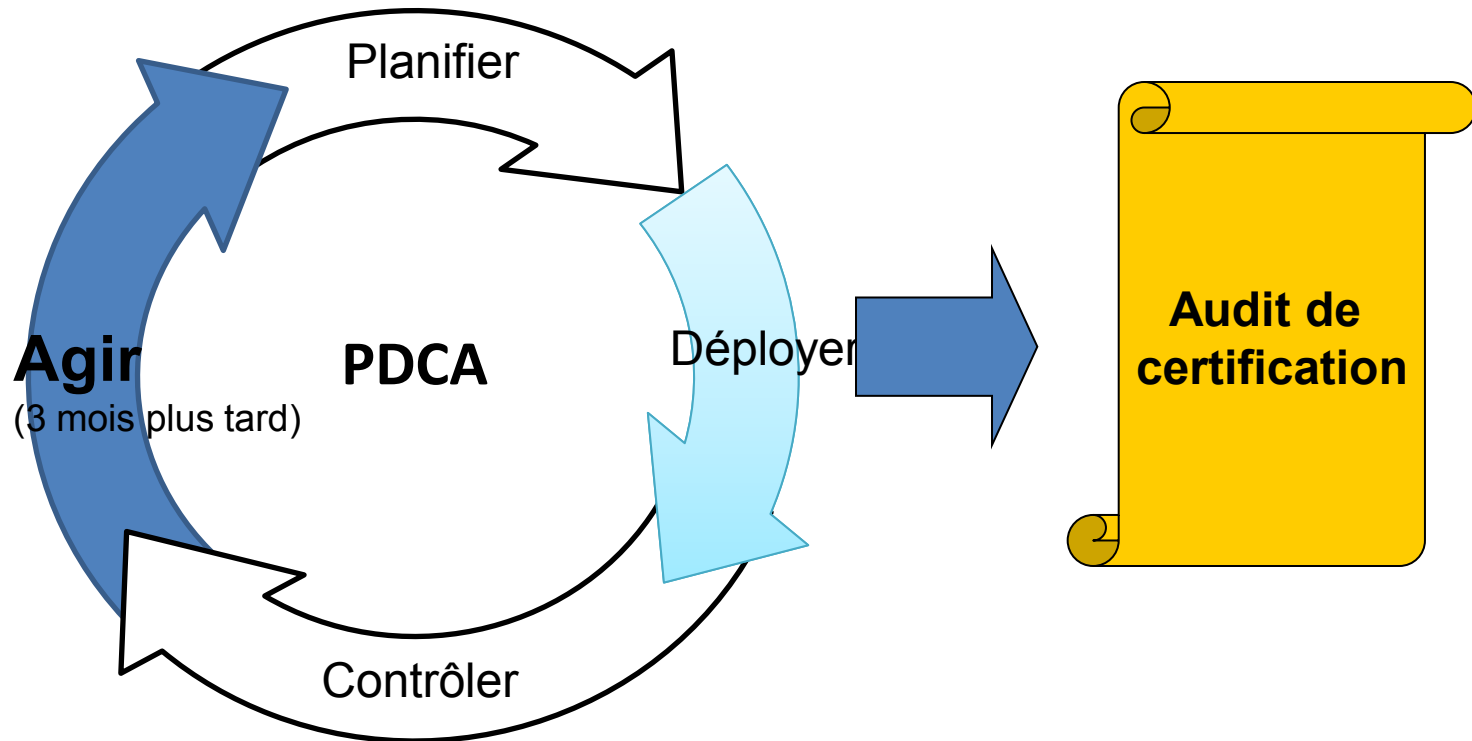


### 1. Amélioration continue

1.1. Identifier les non conformités

1.2. Traiter les non conformités

## 3. Agir



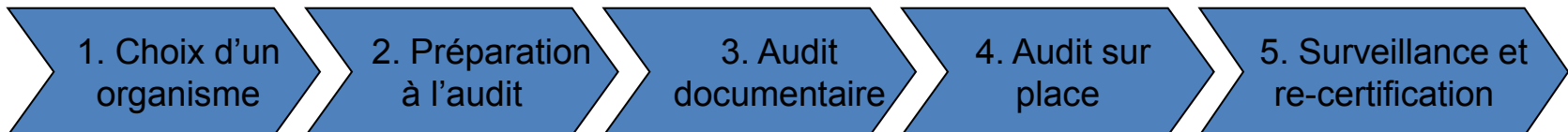
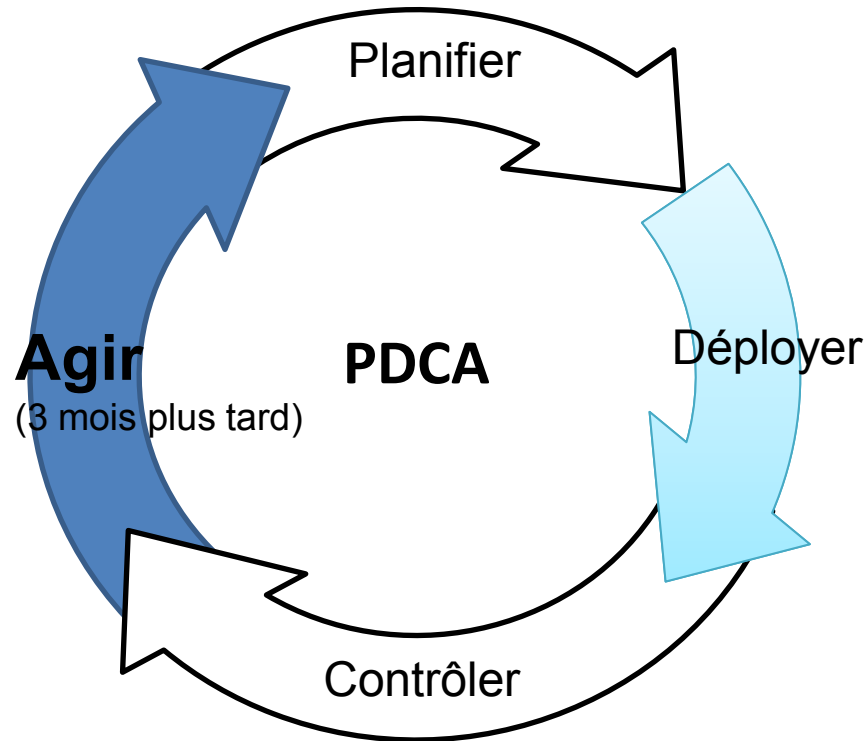
3. Format,

Cycle de vie (validation, etc.),

Contenu (quoi, comment, qui, quand, etc.)

Enregistrement (fruit d'une procédure, via tableau d'émargement)

## 3. Agir



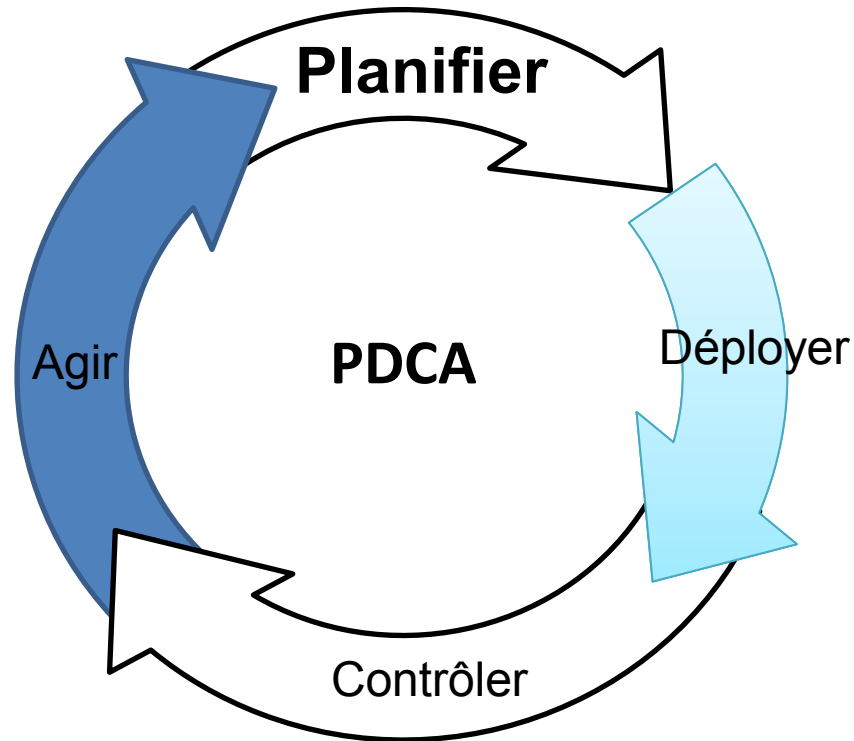
5.1. Surveillance (annuelle)

5.2. Re-certification (tous les 3 ans)

## 4. Analyse préliminaire du projet



## 4. Analyse préliminaire



Niveau de maturité de l'entreprise

Estimation du coût du projet avant le démarrage

## 4. Analyse préliminaire

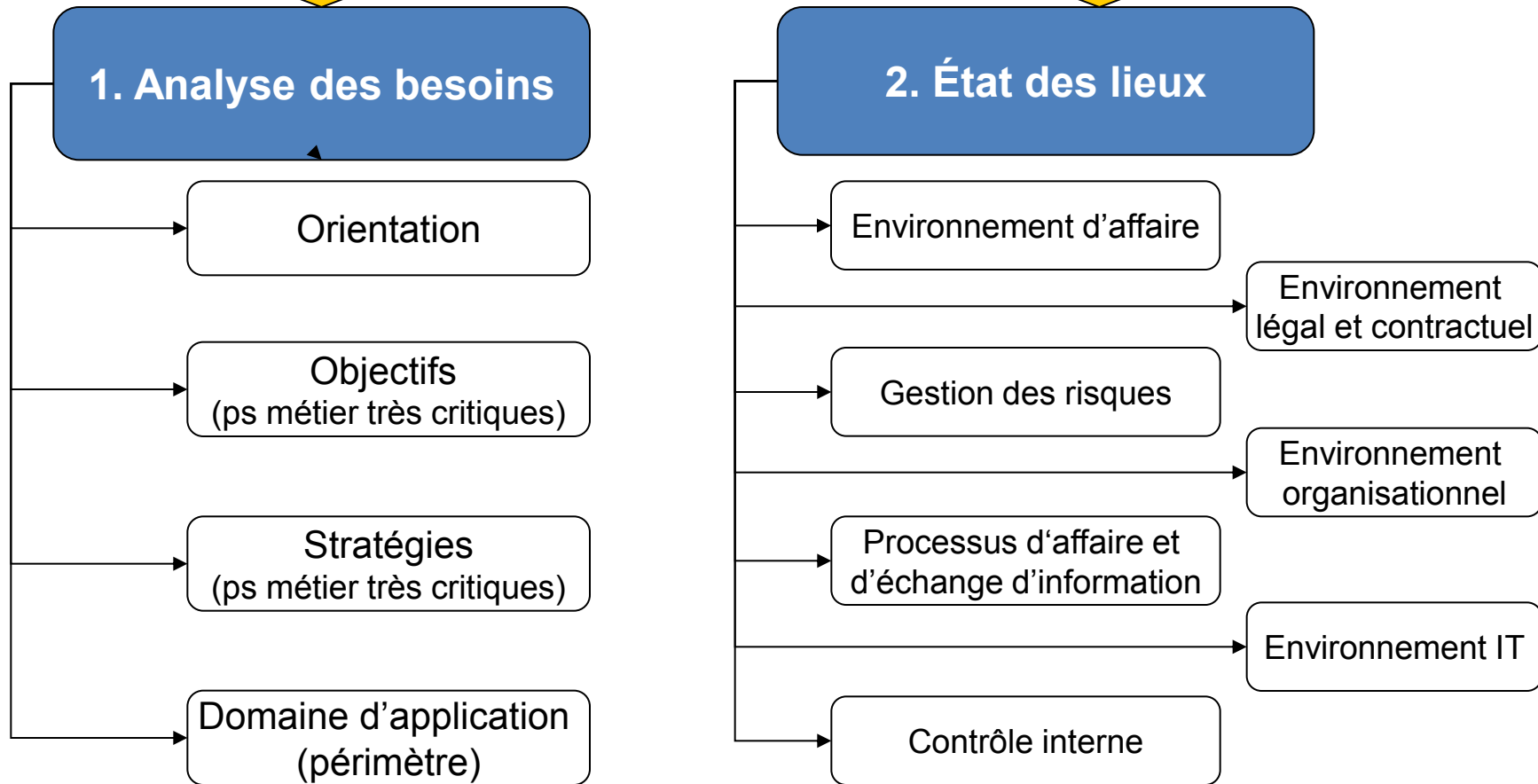
|                             |                                                                                                                        |                                                                         |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Objectifs</b>            | Récolter l'information nécessaire à la planification du projet de SMSI et à son alignement stratégique                 | Vérifier les exigences ISO 27001<br>(terrain vierge, etc.)              |
| <b>Pré requis</b>           | ISO 27001:2005 Clause 4.1<br>Exigences générales                                                                       |                                                                         |
| <b>Personnes impliquées</b> | CISO, CIO, haute direction, gestionnaires TI, propriétaires des principaux processus opérationnels                     | Chief Information Security Officer<br>Recherche des processus conformes |
| <b>Mise en œuvre</b>        | Analyse des besoins de l'organisation,<br>État des Lieux,<br>Analyse des écarts entre l'existant et le but à atteindre | Définir les plans d'action restants pour atteindre l'objectif           |
| <b>Livrables</b>            | Analyse des écarts,<br>Étude de faisabilité,<br>Business Case                                                          |                                                                         |

- Voir clause 4.1 (ISO 27001:2005)
- Voir clause 5.1.b (ISO 27001:2005)

⇒ Chercher les processus que l'on veut prioriser

# 4. Analyse préliminaire

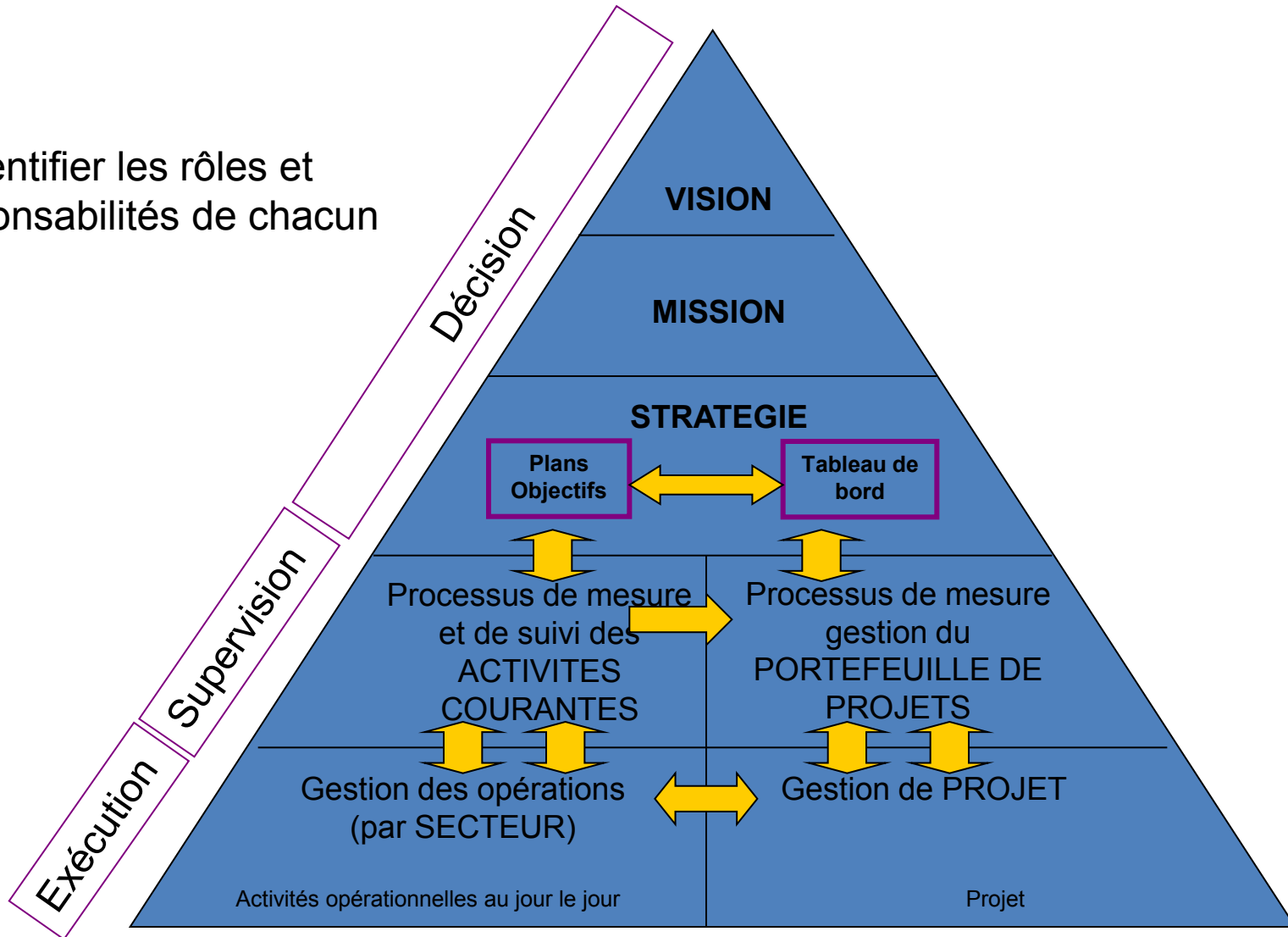
Info. Nécessaire à la planification du projet de SMSI



1. Répondre aux exigences générales de la sécurité de la norme ISO 27001:2005
  2. Déterminer la situation actuelle de l'organisation en terme de sécurité: Évaluation de l'environnement de l'entreprise
- ⇒ Finalité: Mise en évidence de l'écart existant entre le réel et le souhaité

# 4. Comprendre l'organisation

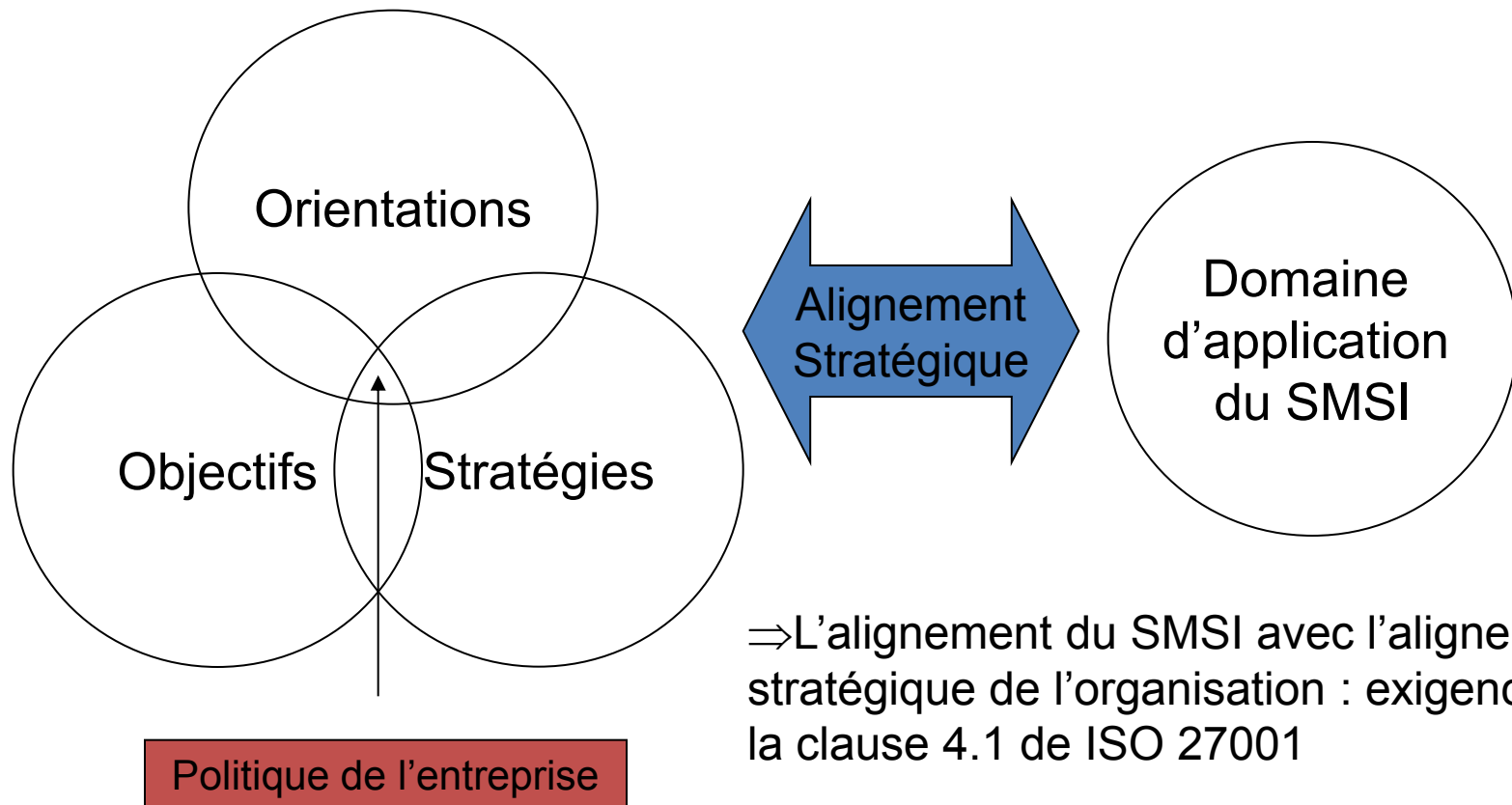
⇒ Identifier les rôles et  
responsabilités de chacun



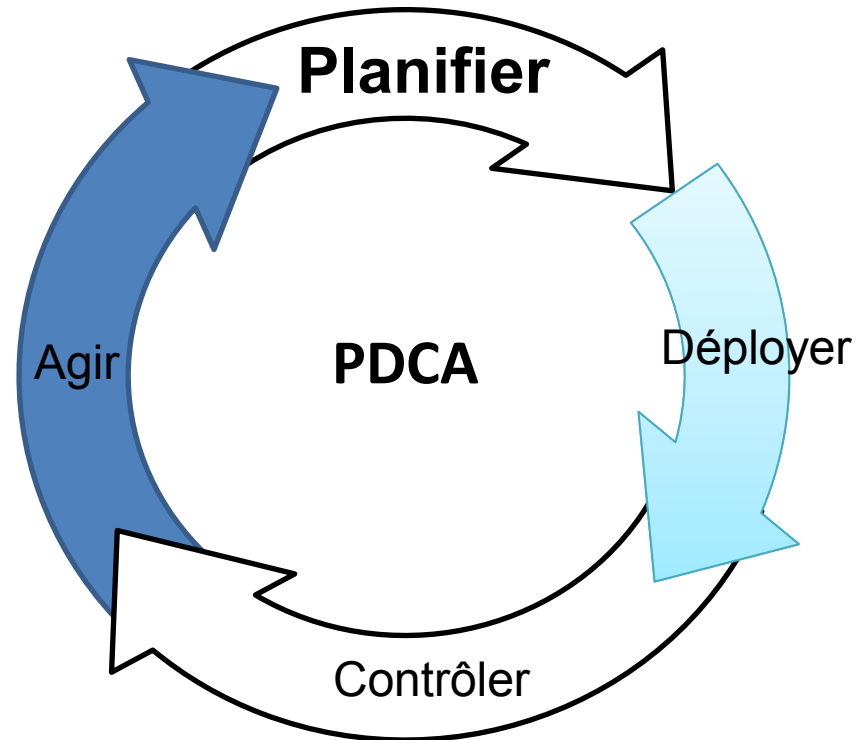
# 4. Analyse des besoins

⇒ Meilleure identification des besoins

⇒ Meilleure mise en œuvre de la politique SMSI dans le domaine d'application



## 4. Analyse des écarts



Niveau de maturité de l'entreprise

Estimation du coût du projet avant le démarrage

## 4. Analyse des écarts

### Objectifs

Déterminer les écarts entre  
l'existant et le but à atteindre

### Pré requis

ISO 27001:2005 Clause 4.1  
Exigences générales

### Personnes impliquées

CISO, gestionnaires des opérations  
Et propriétaires des principaux processus

### Mise en œuvre

Comparer la situation actuelle de l'entreprise avec  
ses besoins et les exigences de la norme ISO 27001

### Livrables

Rapport d'analyse des écarts

| Critère ISO 27002 | Etat actuel | Explication | Qui | # jours | Livable |
|-------------------|-------------|-------------|-----|---------|---------|
|                   |             |             |     |         |         |

## 4. Analyse des écarts

- Outil de comparaison entre performances actuelles et souhaitées (exigences ISO 27001)
- But:

| Critère ISO 27002 | Etat actuel | Explication | Qui | # jours | Livrable |
|-------------------|-------------|-------------|-----|---------|----------|
|                   |             |             |     | Délais  |          |

  - Mesurer le fossé entre les mesures de contrôle actuellement en place et les exigences
  - Mettre en avant les besoins d'amélioration par zone
- Contraintes:
  - Documenter suffisamment pour assurer une analyse efficace
  - Souvent basée sur le benchmarking
- Base pour la mesure des investissements nécessaires en vue de la réalisation du SMSI:
  - Temps, argent, ressources humaines, ressources matérielles



## 4. Échelle de maturité

- La maturité des mesures de contrôle sera classée selon la légende suivante:
  - 0 (Inexistant): les processus de management totalement inappliqués
  - 1 (Initialisé): les processus mis en œuvre au cas par cas sans méthode
  - 2 (Reproductible): les processus suivent un même modèle
  - 3 (Défini): les processus sont documentés et communiqués
  - **4 (Géré): les processus sont surveillés et mesurés (mise en place des processus associés): niveau exigé par ISO 27001**
  - 5 (Optimisé): les meilleures pratiques sont suivies, suite à une amélioration constante, et à la comparaison avec d'autres entreprises (Modèle de Maturité). L'informatique permet d'automatiser les flux de travaux (meilleure qualité, efficacité, et adaptation.

## 4. Questionnaire – Analyse des écarts

| Numéro et objectif du contrôle                                                                                                                                                                                  | Questions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>A.5.1.1</b></p> <p><i>Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernées</i></p> | <p>Votre document de politique de sécurité démontre-t-il:</p> <ul style="list-style-type: none"> <li>•L'engagement de la direction?</li> <li>•Définit-il l'approche de l'organisme pour gérer la sécurité de l'information?</li> </ul> <p>Ce document de politique contient-il les éléments suivants:</p> <ul style="list-style-type: none"> <li>•Une définition de la sécurité de l'information, les objectifs généraux recherchés et le domaine d'application retenue, ainsi que l'importance de la sécurité en tant que mécanisme nécessaire au partage de l'information?</li> <li>•Une déclaration des intentions de la direction soutenant les objectifs et principes de la sécurité de l'information, en conformité avec la stratégie et les objectifs de l'organisme?</li> <li>•Une démarche de définition des objectifs de sécurité et des mesures, intégrant l'appréciation et le management du risque?</li> <li>•Une brève explication des politiques, principes, normes et exigences en matière de conformité qui présentent une importance particulière pour l'organisme (la conformité avec les exigences légales, réglementaires et contractuelles, les exigences en terme de formation et de sensibilisation en matière de sécurité, la gestion de la continuité de l'activité, les conséquences des violations de la sécurité de l'information?</li> <li>•Une définition des responsabilités générales et spécifiques dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'incidents de sécurité?</li> <li>•Des références à la documentation susceptible d'appuyer la politique et devant être respectée?</li> </ul> <p>Cette politique de sécurité de l'information a-t-elle été communiquée à l'ensemble des utilisateurs sous une forme adéquate, accessible et compréhensible?</p> |

## 4. Questionnaire – Analyse des écarts

- Questionnaire:
  - Agit aux niveaux stratégique et opérationnel
  - Analyse les discordances entre les objectifs de contrôle prévus par ISO 27001 et la situation actuelle de l'entreprise
  - Présente les questions auxquelles doit répondre la mise en place du contrôle
  - Couplé avec le gabarit de reporting, il permet de mettre en relief les actions correctives ou préventives à prendre en priorité
  - Favorise la définition de l'orientation stratégique de l'entreprise
  - Composé de
    - 1300 questions
    - ou 133 questions

## 4. Questionnaire – Analyse des écarts

- Activité 3:
  - Pour chaque risque identifié dans l'exercice précédent, fournissez les contrôles appropriés permettant d'atténuer, de transférer ou d'éviter ces risques. Complétez la matrice précédente et soyez prêts à discuter vos réponses pendant le cours.

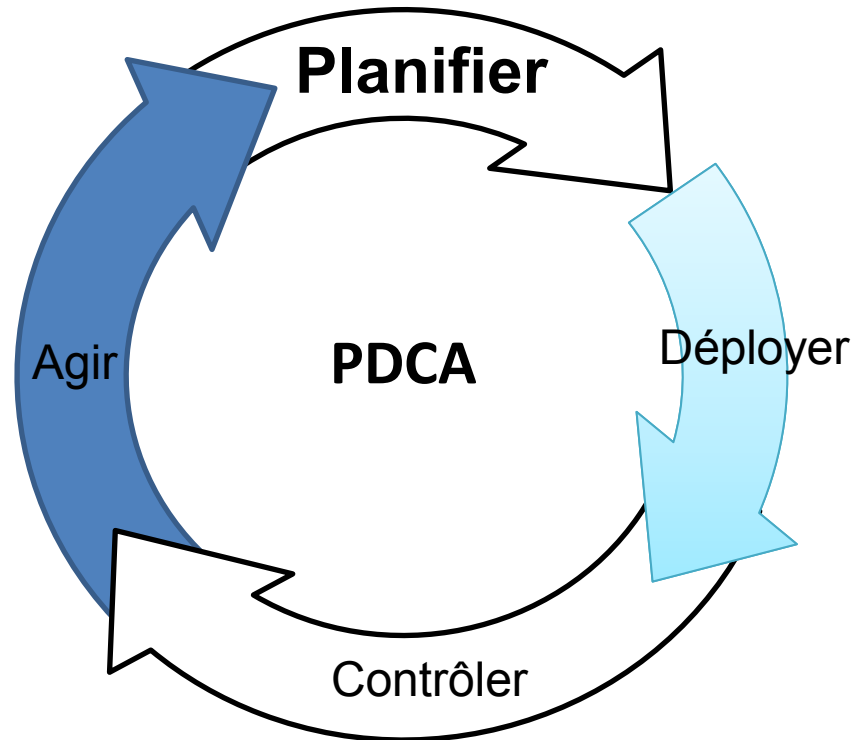
# 4. Gabarit de reporting

| <i>Nom du contrôle</i>                                                                   | <i>Description du contrôle</i>                                                                                                                                                                                                                                                | <i>Description actuelle</i> | <i>M<br/>A<br/>T<br/>U<br/>R<br/>I<br/>T<br/>É</i> | <i>Description des écarts</i> | <i>Degré de complexité</i> | <i>RESPONSABLE</i> |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------------------|-------------------------------|----------------------------|--------------------|
| <i>A.5.1.1<br/>Document de politique de sécurité de l'information</i>                    | <i>un document de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés</i>                                                                                                          |                             |                                                    |                               |                            |                    |
| <i>A.5.1.2<br/>Réexamen de la politique de sécurité de l'information</i>                 | <i>Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, la politique doit être réexaminée à intervalles fixés préalablement en cas de changements majeurs</i>                                                              |                             |                                                    |                               |                            |                    |
| <i>A.6.1.1<br/>Implication de la direction vis-à-vis de la sécurité de l'information</i> | <i>La direction doit soutenir activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement démontré, d'attributions de fonctions explicites et d'une reconnaissance des responsabilités liée à la sécurité de l'information</i> |                             |                                                    |                               |                            |                    |

## 4. Gabarit de reporting

- But:
  - Bien définir le périmètre
  - Court terme:
    - Favoriser l'implémentation de mesures correctives ou préventives pour les actifs avec un risque potentiel élevé
  - Moyen et long terme:
    - Permet de garder une trace des mesures envisagées et des analyses des écarts effectuées
    - Souligner l'amélioration continue mise en place dans l'organisation

## 4. Business case



Niveau de maturité de l'entreprise

Estimation du coût du projet avant le démarrage

## 4. Business case

|                      |                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------|
| Objectifs            | Déterminer la faisabilité du projet et en justifier sa pertinence dans un contexte d'affaires            |
| Pré requis           | ISO 27001:2005 Clause 4.1<br>Exigences générales                                                         |
| Personnes impliquées | CISO, CIO, Analyste financier,<br>Spécialistes et consultants externes                                   |
| Mise en œuvre        | Déterminer les risques projets, les ressources nécessaires, les contraintes, faire une pré-planification |
| Livrables            | Business case                                                                                            |

-Conflit d'intérêt  
-Résistance au changement  
-SI externalisé => engager l'hébergeur de serveurs



## 4. Développer le Business case

- Le business case inclut:
  - Une description détaillée du problème ou de l'opportunité (opportunité d'affaire, image de marque, clientèle, attraction d'autres marchés, etc.)
    - Préparer le projet afin d'obtenir l'engagement de la direction et l'approbation de l'investissement
    - S'appuie sur une étude de faisabilité
    - Fournit une structure pour planifier et gérer le projet, les indicateurs et résultats attendus à partir desquels sera vérifié le succès du projet
  - Une liste de solutions alternatives disponibles (jouer sur les contrôles en cas de manque de moyens)
    - Une analyse des bénéfices, coûts, risques et résultats pour les affaires
    - Une description de la solution préférentielle (timing)
    - Un plan résumé pour la mise en œuvre
    - Le budget

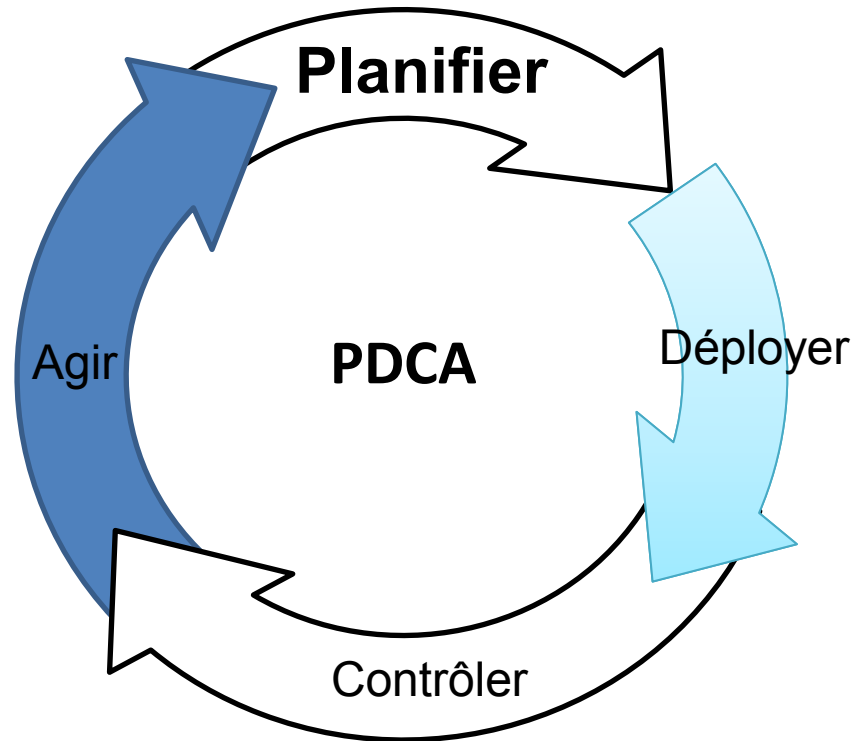
## 4. Développer le Business case

- Le business case répond aux questions suivantes:
  - Quel est le but du projet? A quel besoin de l'utilisateur va-t-il répondre?
  - Quelles sont les solutions qui ont été étudiées?
  - Pourquoi la solution retenue a-t-elle été choisie? Quels sont les risques, les contraintes?
  - Combien cela coûte-t-il? Comment savoir si le projet sera un succès? Comment l'expliquer aux employés, clients, partenaires...? Qui est chargé de ce projet? Est-ce que mon travail sera affecté par ce projet dans le futur?
- Un Business case doit comporter au minimum 5 parties
  - Buts ou objectifs du projet et leur incorporation dans la stratégie de l'org.
  - Les différentes options envisagées
  - La solution choisie
  - La manière dont le projet sera mis en œuvre
  - Les besoins en ressources du projet

## 4. Développer le Business case

- Décrire l'approche de mise en œuvre
  - L'activité finale implique dans la création du Business Case est de fournir aux sponsors du projet SMSI la confiance dans le fait que la mise en œuvre de la solution a été bien réfléchie
  - Pour ce faire, décrivez en détails comment le projet sera initié, planifié, exécuté et clôturé
    - Planification: lister phases définition projet/recruter équipe projet/établir bureau projet/décrire processus global de planification pour prouver la bonne coordination du projet/plan de mise en œuvre du SMSI
    - Mise en œuvre: lister activités nécessaires pour produire livrables qui créent solution client
    - Clôture du projet: lister activités impliquées dans la remise de la solution finale au client/libération du personnel/fermeture bureau du projet/révision après mise en œuvre du projet
    - Amélioration du projet: lister activités nécessaires pour accomplir mise en œuvre du projet (programme d'audit interne)
    - Gestion du projet: décrire brièvement la gestion du temps/coûts/qualité/changements/ risque/problèmes potentiels/communications/autorisation&approbations
  - Prouver que le projet est faisable

## 5. Planification du projet SMSI



# 5. Planification du projet SMSI



# 5. Pré-requis de ISO 27001

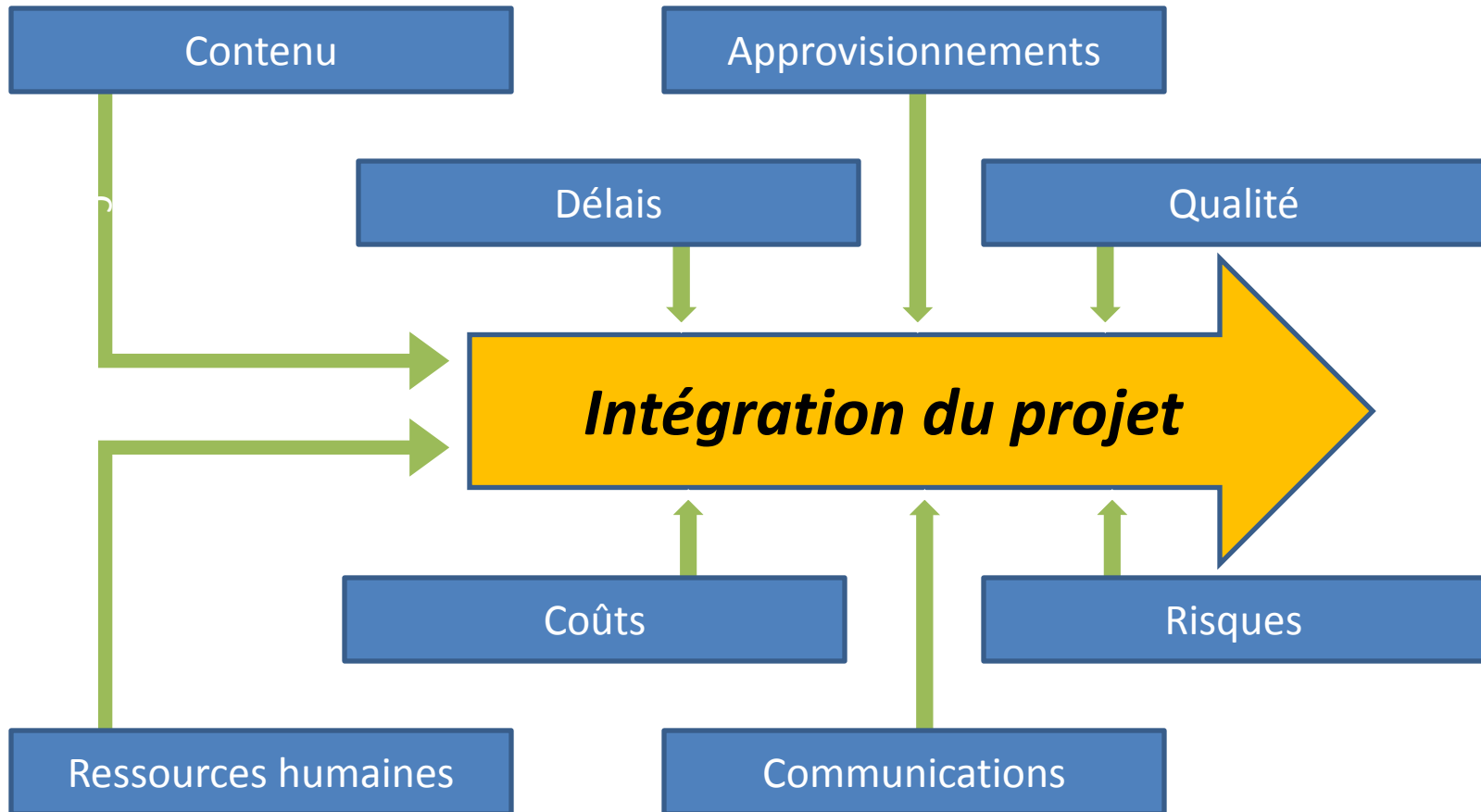
## 4.2.2 Mise en œuvre et fonctionnement du SMSI

- L'organisme doit effectuer les tâches suivantes:
  - a) élaborer un plan de traitement du risque qui identifie les actions à engager, les ressources, les responsabilités et les priorités appropriées pour le management des risques liés à la sécurité de l'information (voir l'Article 5);

### Remarque:

- ISO 27001 ne fournit pas de méthodologie de gestion de projets, ni fait la promotion d'une méthodologie particulière
- ISO 27003 fournira des conseils et de l'aide à l'implantation d'un SMSI (cadre de référence plutôt que méthodologie concrète de gestion de projets)

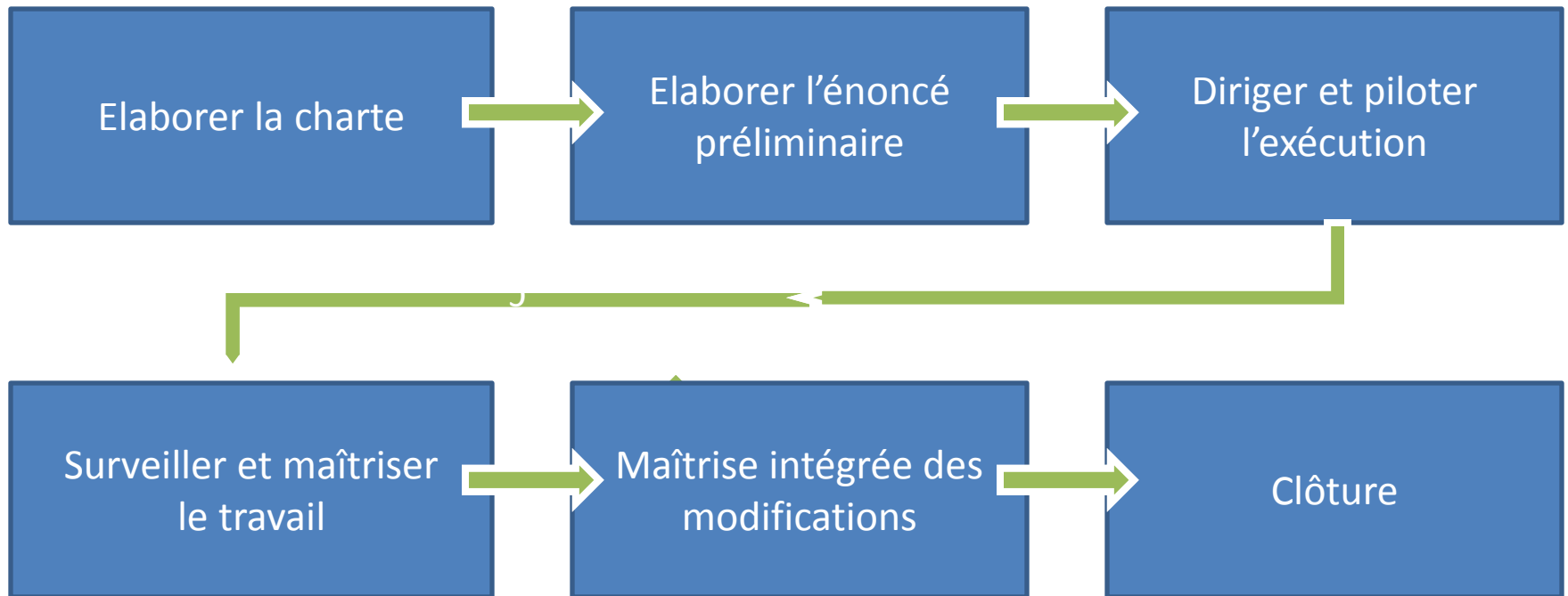
# 5. Pratiques de gestion de projet



- Guide du corpus des connaissances en management de projet, 3<sup>ème</sup> édition, Guide PMBOK, 2004, PMI
- Norme ISO 10006:2003, Système de management de la qualité, lignes directrices pour le management de la qualité dans les projets
- Implication du management en cas de résistance au changement

# 5. Le management de l'intégration de projet

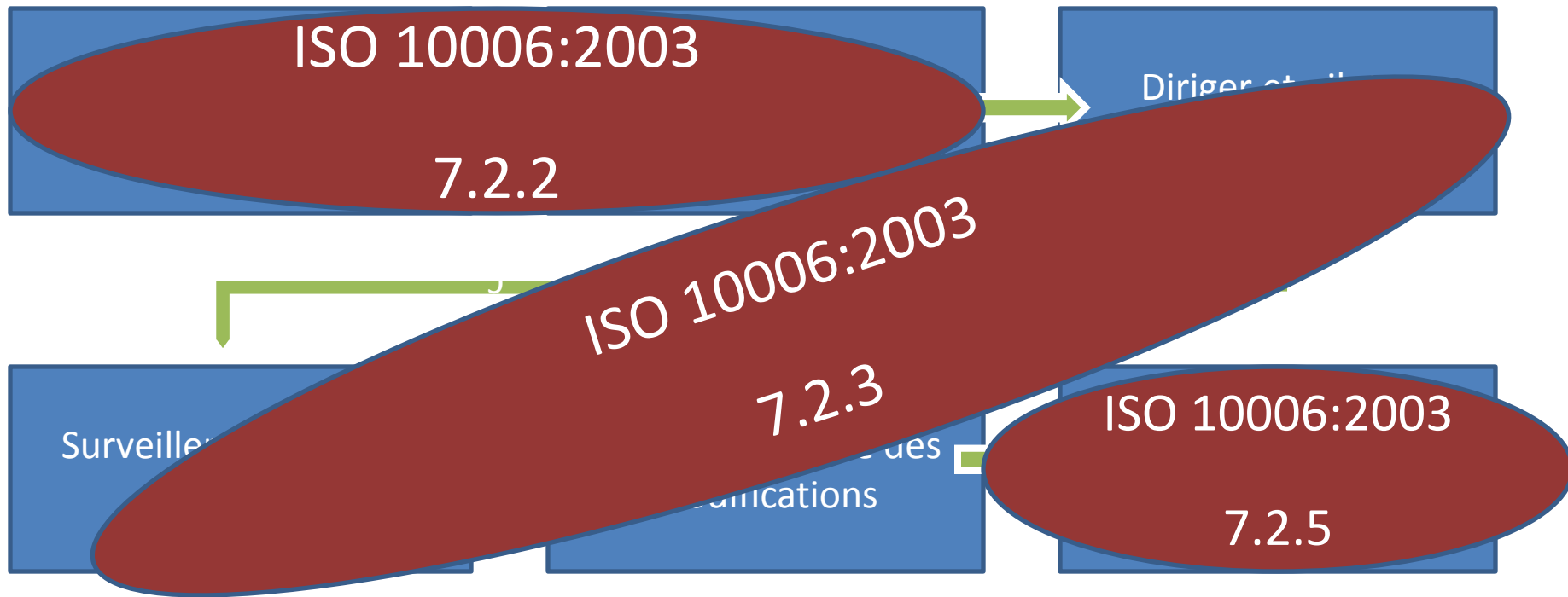
Processus requis pour assurer le bon déroulement du projet





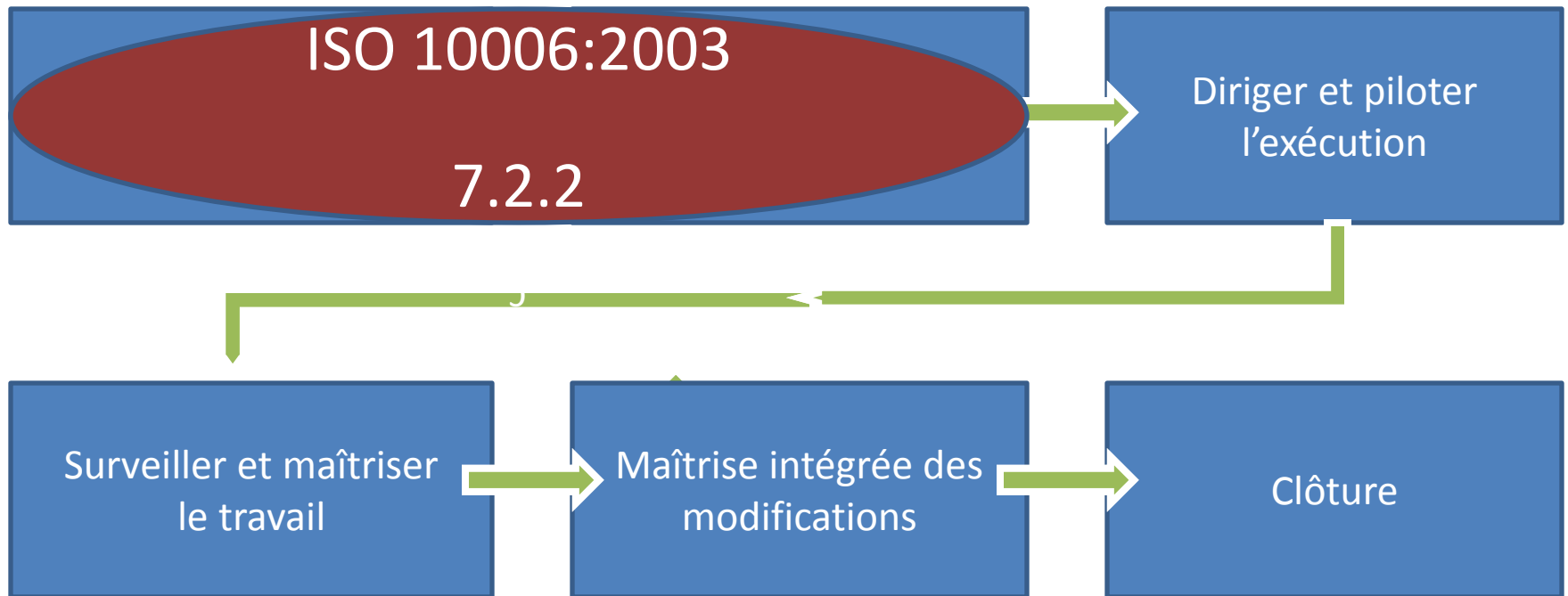
# 5. Le management de l'intégration de projet

Processus requis pour assurer le bon déroulement du projet



# 5. Le management de l'intégration de projet

Processus requis pour assurer le bon déroulement du projet

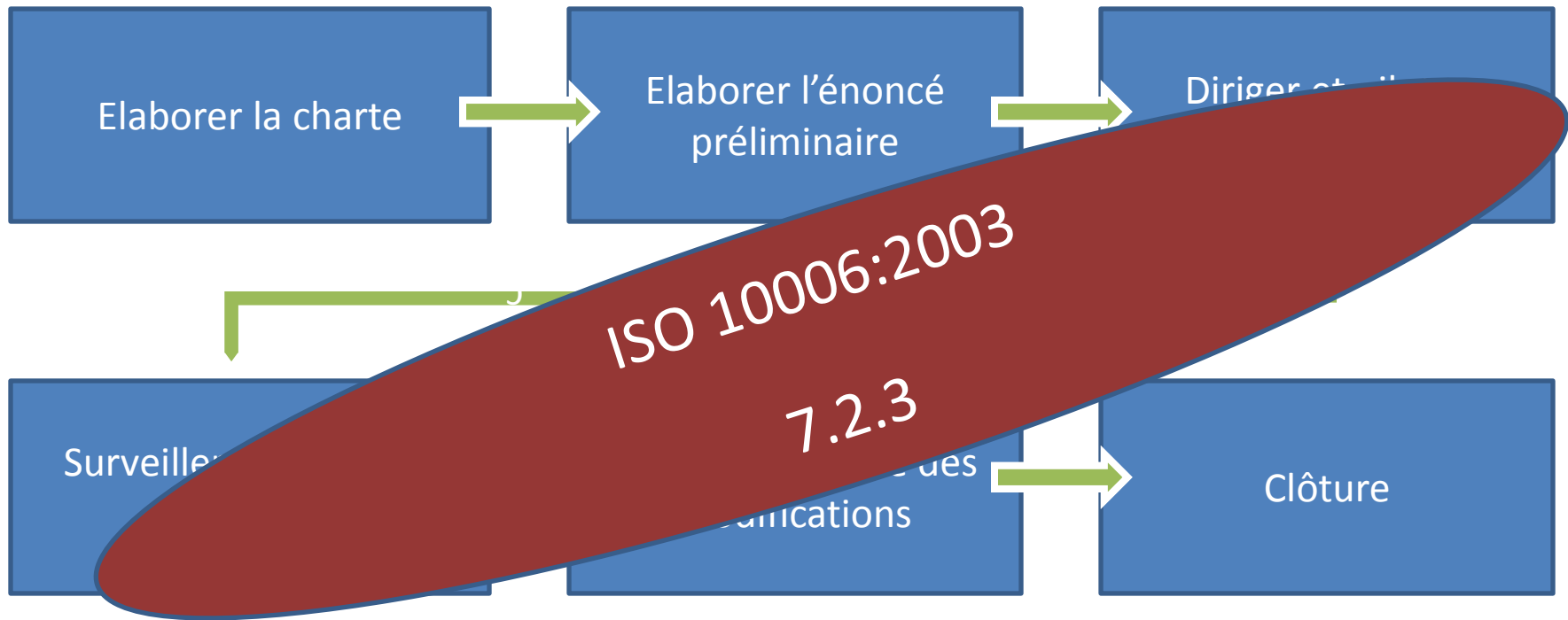


# 5. Le management de l'intégration de projet

- ISO 10006:2003:
  - 7.2.2 Lancement du projet&élaboration du plan de management du projet
    - Élaboration et mise à jour du plan de management du projet
    - Comprend ou fait référence au plan de management du projet
    - Niveau de délai dépend de facteurs tels que la taille ou la complexité du projet
    - Identification parmi les projets déjà réalisés ceux qui se rapprochent le plus du projet à lancer, pour exploiter au mieux l'expérience acquise grâce aux projets précédents
    - Cas des projets relatifs aux réponses aux exigences d'un contrat: procéder à des revues de contrat au cours de l'élaboration du plan de management du projet (s'assurer de la satisfaction des exigences contractuelles ISO 9004:2000, 7.2)
    - Cas des projets ne résultant pas d'un contrat: mener une revue initiale afin d'établir les exigences et confirmer qu'elles sont appropriées et réalisables

# 5. Le management de l'intégration de projet

Processus requis pour assurer le bon déroulement du projet

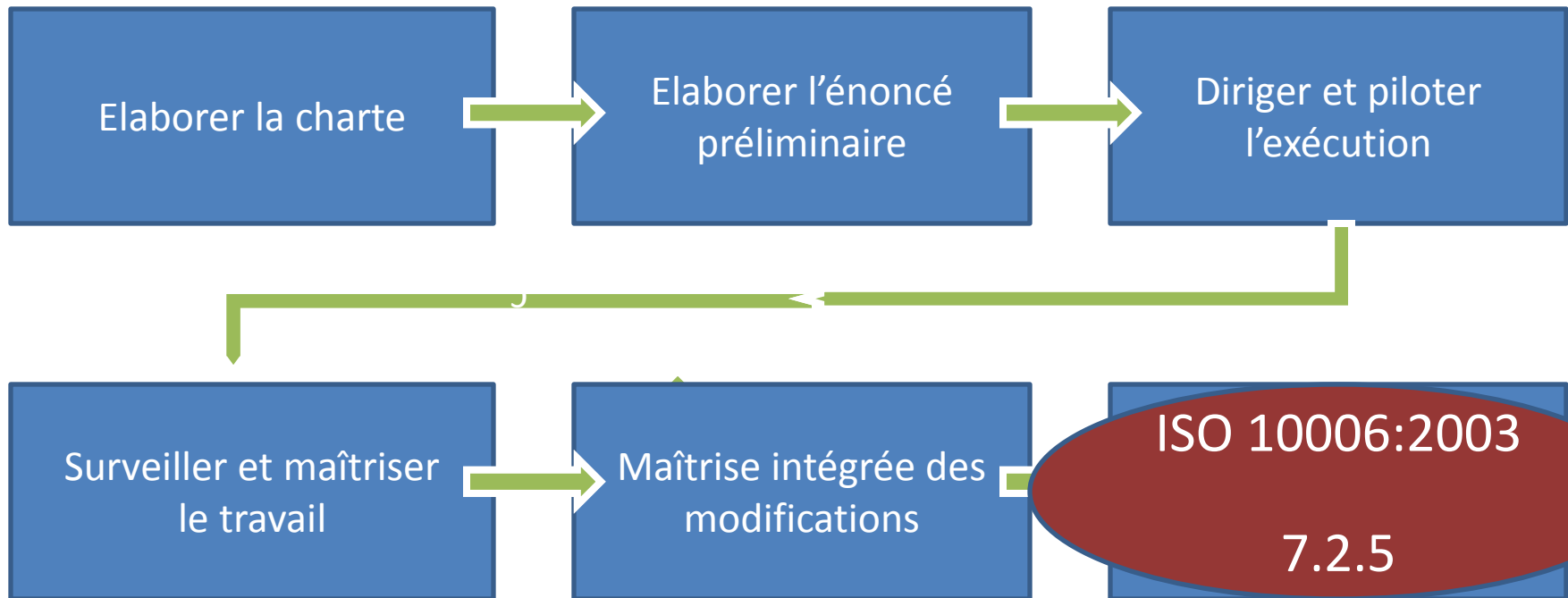


# 5. Le management de l'intégration de projet

- ISO 10006:2003:
  - 7.2.3 Management des interactions
    - Gestion des interactions (non planifiées) au sein du projet, afin de faciliter la coordination planifiée entre processus, dont:
      - Mise en place de procédures visant à à établir le management des interfaces
      - Tenue de réunions de projet impliquant plusieurs fonctions
      - Apport de solutions à des problèmes tels que des conflits de responsabilité ou des modifications apportées à l'exposition à des risques
      - Mesures de performances du projet utilisant des techniques telles que l'analyse de la valeur acquise du réalisé (technique de suivi des performances globales du projet par rapport à un référentiel budgétaire)
      - Réalisation de la mesure de l'avancement afin d'évaluer la situation du projet et de planifier le travail restant à faire
      - => faire appel aux évaluations de l'avancement afin d'identifier les problèmes potentiels d'interface
      - => à noter que les risques sont généralement importants au niveau des interfaces

# 5. Le management de l'intégration de projet

Processus requis pour assurer le bon déroulement du projet

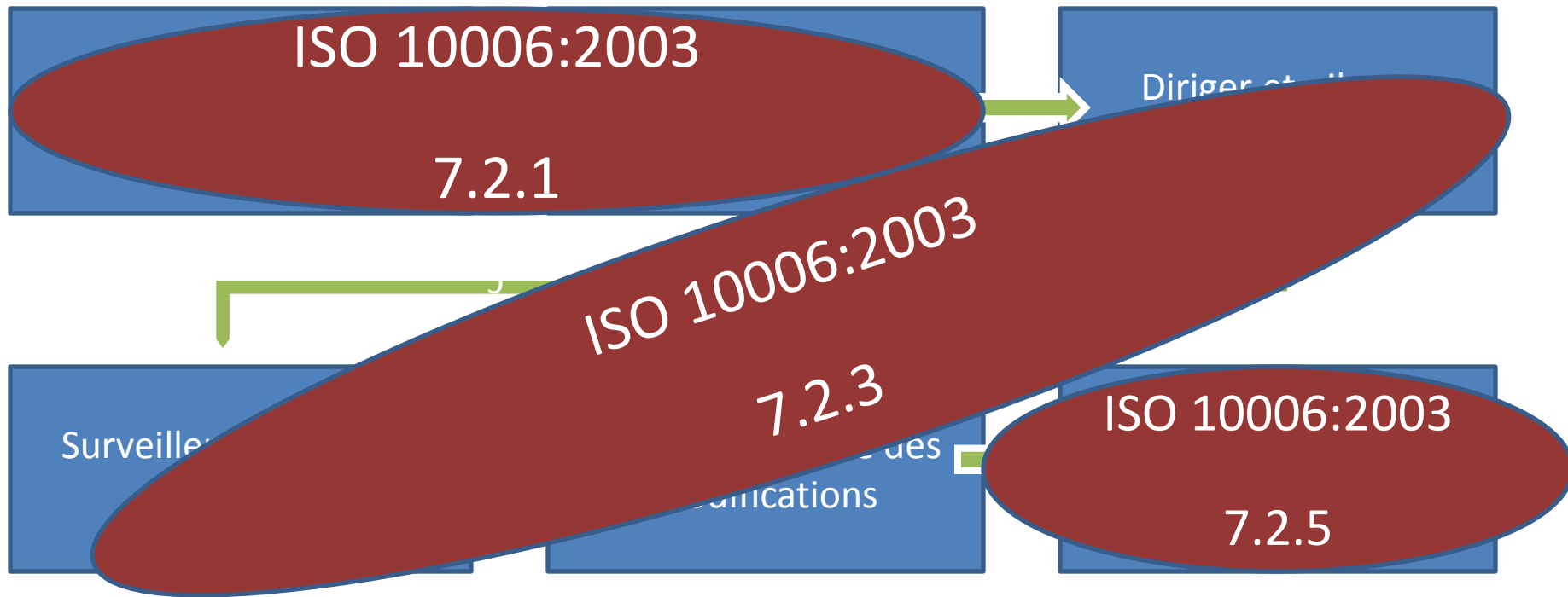


# 5. Le management de l'intégration de projet

- ISO 10006:2003:
  - 7.2.5 Clôture des processus et des projets
    - Le projet est un ps en lui-même, et il convient d'accorder une attention à sa clôture:
      - Définition du processus de clôture des processus et du projet dès la phase de lancement du projet, et l'inclure dans le plan de management du projet (s'appuyer sur l'expérience issue de processus et de projets déjà clos)
    - À tout moment pendant la durée de vie du projet, il convient de :
      - Clore les processus de projets achevés dans les conditions prévues: s'assurer après clôture que tous les enregistrements sont effectués, diffusés au sein du projet et de l'organisme à l'origine du projet, et conservés pendant une durée spécifiée
      - Clore plus tôt ou plus tard également en raison d'évènements imprévus
    - Quelle que soit la raison de clôture, entreprendre une revue complète de ses résultats :
      - prendre en compte les enregistrements pertinents, y compris ceux qui proviennent de l'évaluation de l'avancement et des éléments d'entrée des parties intéressées
      - Attention particulière au retour d'information du client et des autres parties intéressées concernées, et de le mesurer chaque fois que possible
      - Remise d'enregistrements appropriés à partir de cette revue, faisant ressortir les expériences susceptibles d'être utilisées dans d'autres projets et pour l'amélioration continue
    - Remise formelle du produit du projet au client, qui exprime l'acceptation formelle.
      - La clôture sera portée à la connaissance de toutes les parties intéressées

# 5. Le management de l'intégration de projet

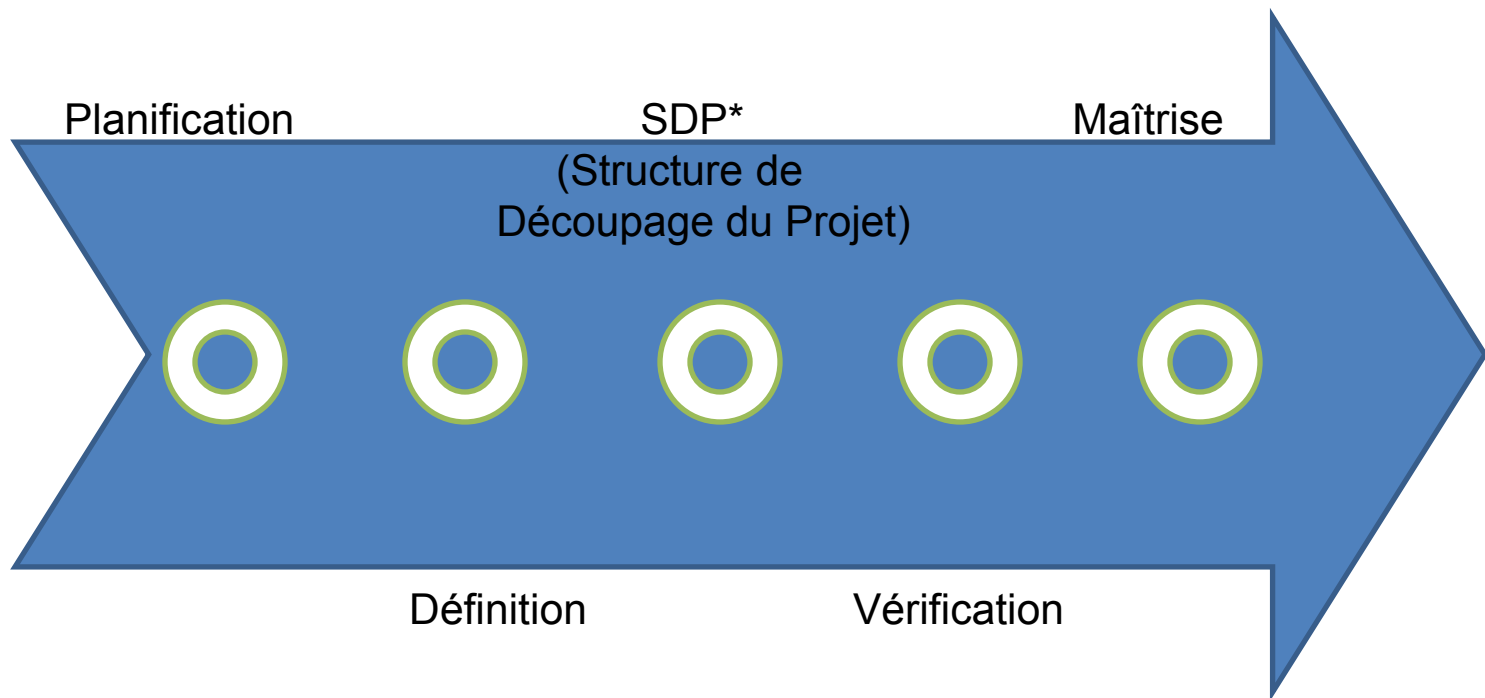
Processus requis pour assurer le bon déroulement du projet





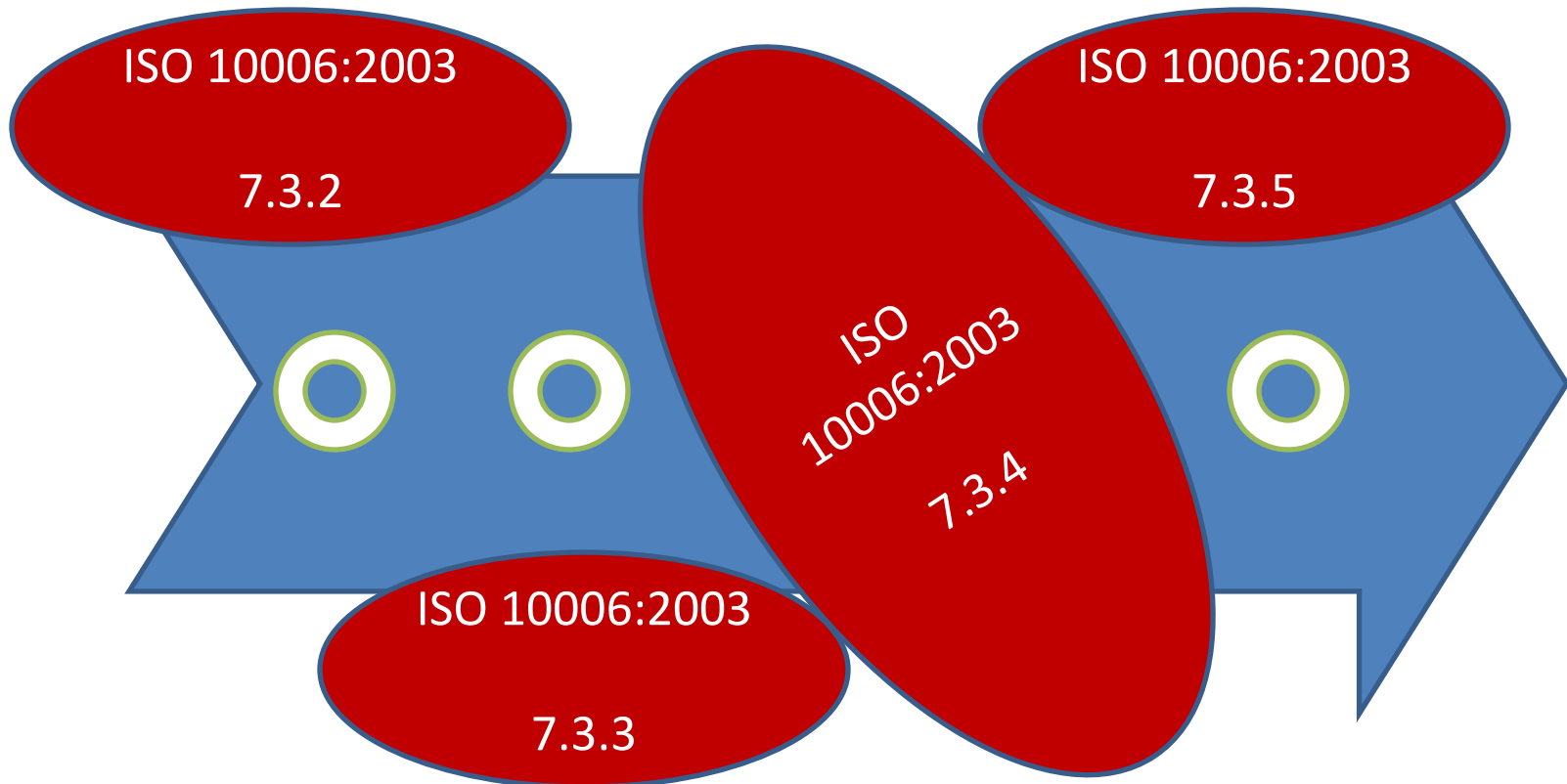
# 5. Le management du contenu de projet

Processus requis pour assurer l'achèvement des livrables du projet



# 5. Le management du contenu de projet

Processus requis pour assurer l'achèvement des livrables du projet



# 5. Le management du contenu de projet

Processus requis pour assurer l'achèvement des livrables du projet

ISO 10006:2003

7 3 2

SDP\*

Maîtrise

## ISO 10006:2003:

### 7.3.2 Elaboration des concepts

- Traduire les besoins et attentes déclarés et généralement implicites du client en matière de processus et de produit en exigences écrites, y compris les aspects statutaires et réglementaires, qui, lorsque le client l'exige, sont manuellement convenues
- Identifier les autres parties intéressées et déterminer leurs besoins
- Traduire ceux-ci en exigences écrites
- Les faire accepter par le client (si c'est approprié)

# 5. Le management du contenu de projet

ISO 10006:2003

- Identifier et documenter aussi précisément que possible les caractéristiques du produit du projet dans des termes mesurables
- Utilisation comme base de conception et de développement
- Spécifier les conditions de mesure de ces caractéristiques ou la manière d'évaluer la

aux exigences

• Si le contenu du contenu de ces  
aure la

ISO 10006:2003

7.3.3

Vérification

# 5. Le management du contenu de projet

- ISO 10006:2003:
  - 7.3.4 Définition des activités:
    - Structuration systématique du projet en activités gérables (respect exigences client pour le produit et le processus) SDP\*
    - Participation du personnel affecté au projet dans la définition de ces activités (profiter de l'expérience de l'organisme en charge, obtenir accord et adhésion)
    - Définir les activités de telle sorte que les résultats soient mesurables
    - Vérifier que la liste des activités est exhaustive
    - Inclure les pratiques de management de la qualité dans les activités, ainsi que les évaluations d' 'avancement,; et la préparation et l'entretien d'un plan de management Vérification
    - Identifier et documenter les interactions entre les activités du projet qui peuvent poser problème entre l'organisme en charge du projet et les parties intéressées

# 5. Le management du contenu de projet

Processus requis pour assurer l'achèvement des livrables du projet

Planification

SDP\*

ISO 10006:2003

7.3.5

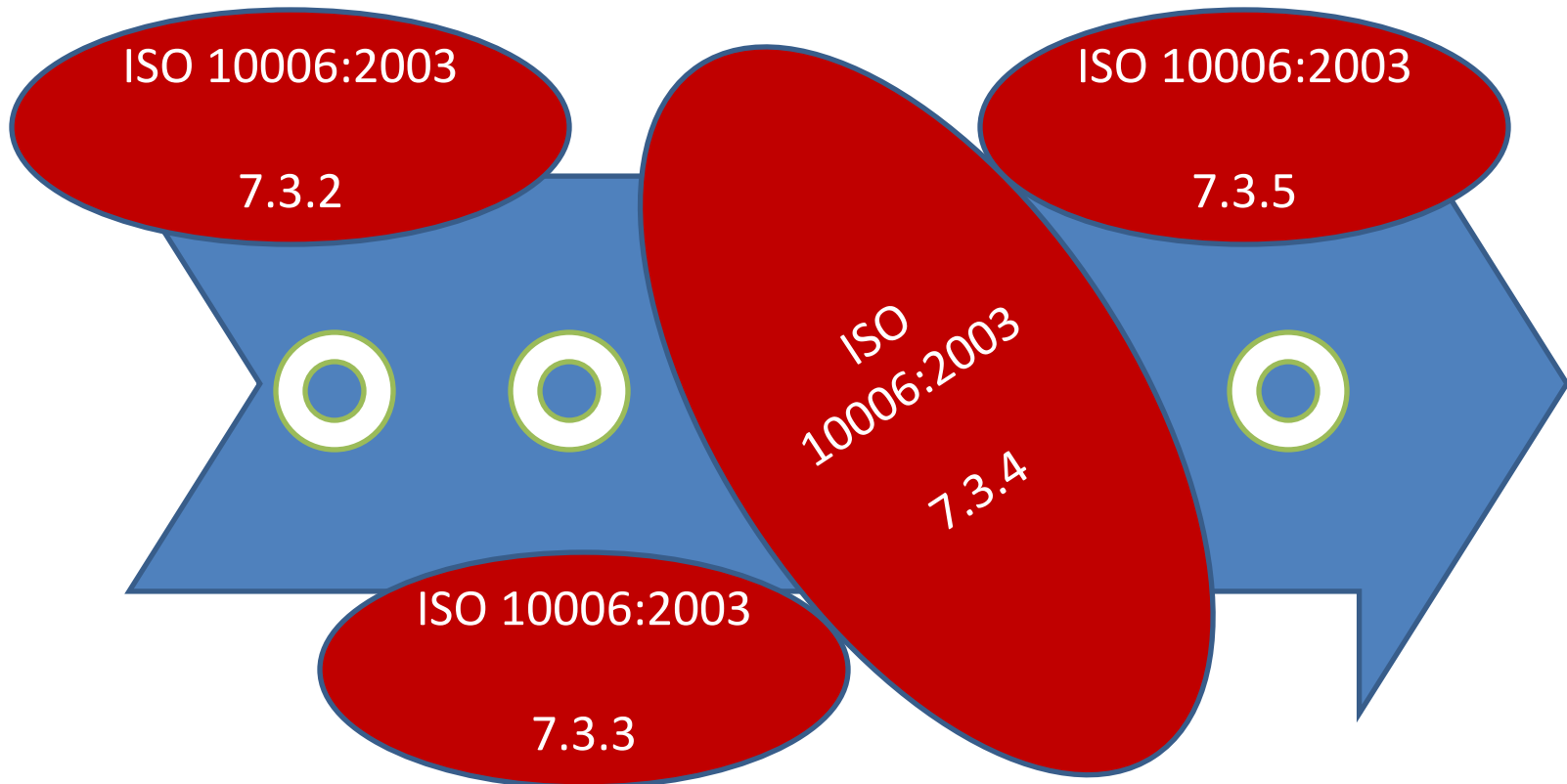
## ISO 10006:2003:

### 7.3.5 Maîtrise des activités

- Mener et maîtriser les activités réalisées au sein du projet conformément au plan de management du projet
- Comprendre la maîtrise des interactions entre les différentes activités afin de réduire les conflits & malentendus au maximum (attention particulière aux produits aux processus impliquant les NTI)
- Mener des revues et évaluer les activités pour identifier les défaillances potentielles et les possibilités d'amélioration (planification des revues adaptée à la complexité du projet)
- Utiliser les résultats des revues dans les évaluations de l'avancement pour évaluer les éléments de sortie des ps et planifier le travail restant
- Consigner par écrit le plan pour le travail restant après révision

# 5. Le management du contenu de projet

Processus requis pour assurer l'achèvement des livrables du projet



# 5. Le management des délais du projet

Processus requis pour assurer l'achèvement du projet à temps

Identification des activités



Séquencement des activités



Estimation des ressources nécessaires aux activités



Estimation de la durée de l'activité



Élaboration de l'échéancier



Maîtrise de l'échéancier



# 5. Le management des délais du projet

Processus requis pour assurer l'achèvement du projet à temps

Identification des activités



Séquencement des activités



Estimation des ressources nécessaires aux activités



Estimation de la durée de l'activité



Élaboration de l'échéancier



Maîtrise de l'échéancier

ISO 10006:2003

7.4.2

ISO 10006:2003

7.4.3

ISO 10006:2003

7.4.4

# 5. Le management des délais du projet

Processus requis pour assurer l'achèvement du projet à temps

Identification des activités



Séquencement des activités



Estimation des ressources nécessaires aux activités

ISO 10006:2003

7.4.2

## ISO 10006:2003:

### 7.4.2 Planification des liaisons entre activités

- Identifier les interdépendances parmi les activités d'un projet
- Passer en revue leur cohérence
- Justifier et documenter tout besoin de modification des données issues du processus d'identification des activités
- Utiliser des diagrammes de réseaux de projet, standards ou éprouvés, pour tirer profit d'expériences antérieures
- Vérifier l'adéquation de ces réseaux au projet

# 5. Le management des délais du projet

## ISO 10006:2003:

### 7.4.3 Estimation des durées

- Faire estimer la durée de chaque activité par le personnel responsable
- Vérifier l'exactitude des estimations de durées (expériences antérieures, possibilité d'application aux conditions du projet en cours)
- Documenter et tracer la traçabilité des éléments d'entrée, depuis leur origine
- Estimation des ressources associées doit accompagner celle des entrées
- Si l'estimation des durées est incertaine, alors évaluation des risques nécessaire (marges pour les risques incorporée dans les estimations pour les risques restants)
- Implication des clients et autres parties intéressées

ISO 10006:2003

7.4.3

Estimation de la durée de l'activité

Élaboration de l'échéancier

Maîtrise de l'échéancier

# 5. Le management des délais du projet

## ISO 10006:2003:

### 7.4.4 Elaboration du planning

- Identifier les éléments d'entrée utiles à l'élaboration du planning
- Vérifier s'il correspondent aux conditions spécifiques du projet
- Tenir compte des activités à longs délais d'exécution ou de longue durée, surtout celles relatives au chemin critique
- Mettre en œuvre les formats de plannings standardisés
- Vérifier la cohérence du rapport entre les estimations des durées et les liaisons des activités
- Remédier à toute incohérence avant de finaliser et publier le planning, qui identifieront les activités critiques ou quasi critiques
- Tenir informé le client et les parties intéressées lors de l'élaboration du planning, et analyser les éléments d'entrée extérieurs
- Fournir les planning pour information, et si nécessaire pour approbation

ISO 10006:2003

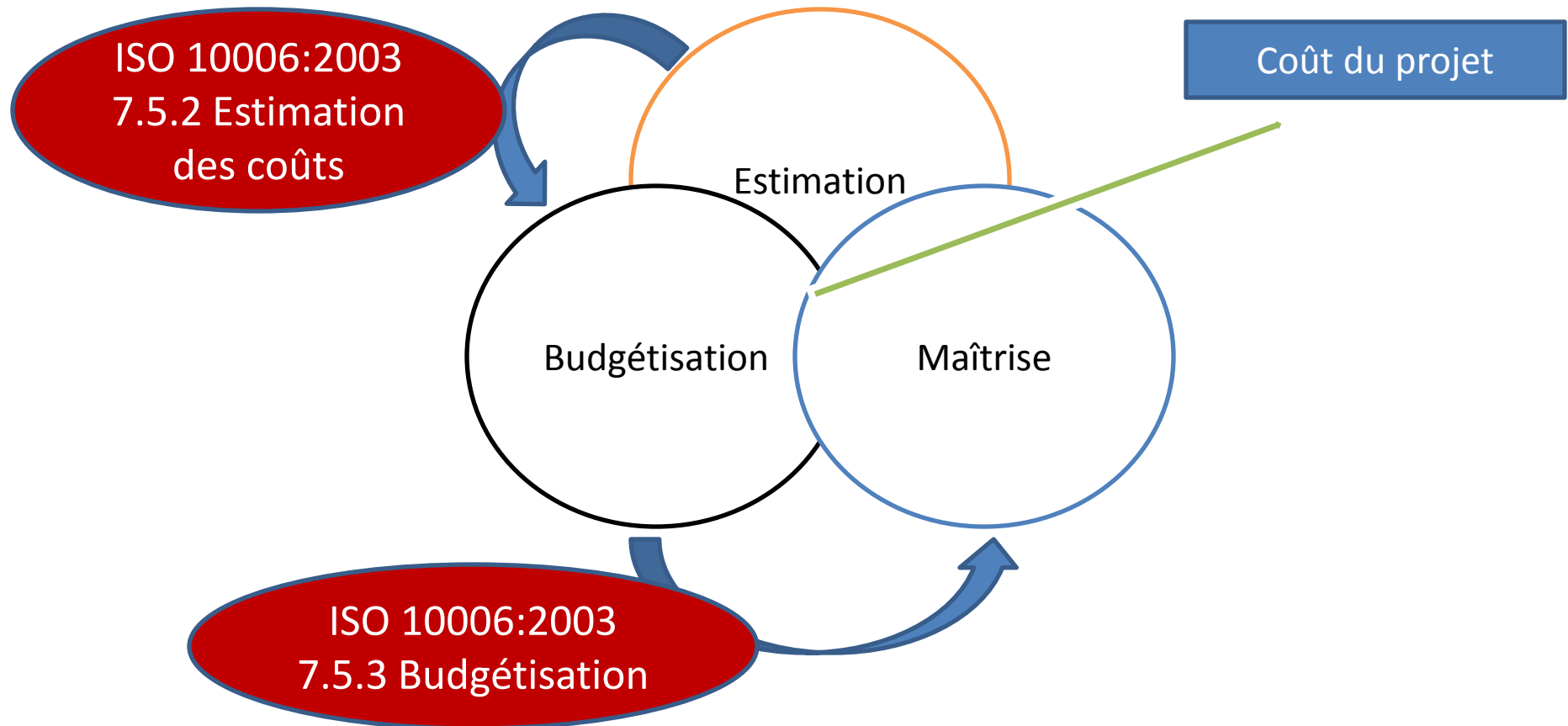
Élaboration de l'échéancier

7.4.4

Maîtrise de l'échéancier

# 5. Le management des coûts du projet

Processus requis pour assurer l'achèvement du projet en respectant le budget alloué



# 5. Le management de la qualité du projet

Processus requis pour assurer l'achèvement du projet selon les critères de qualité définis

ISO 10006:2003  
4.2.1 Principes  
de Management  
de la Qualité

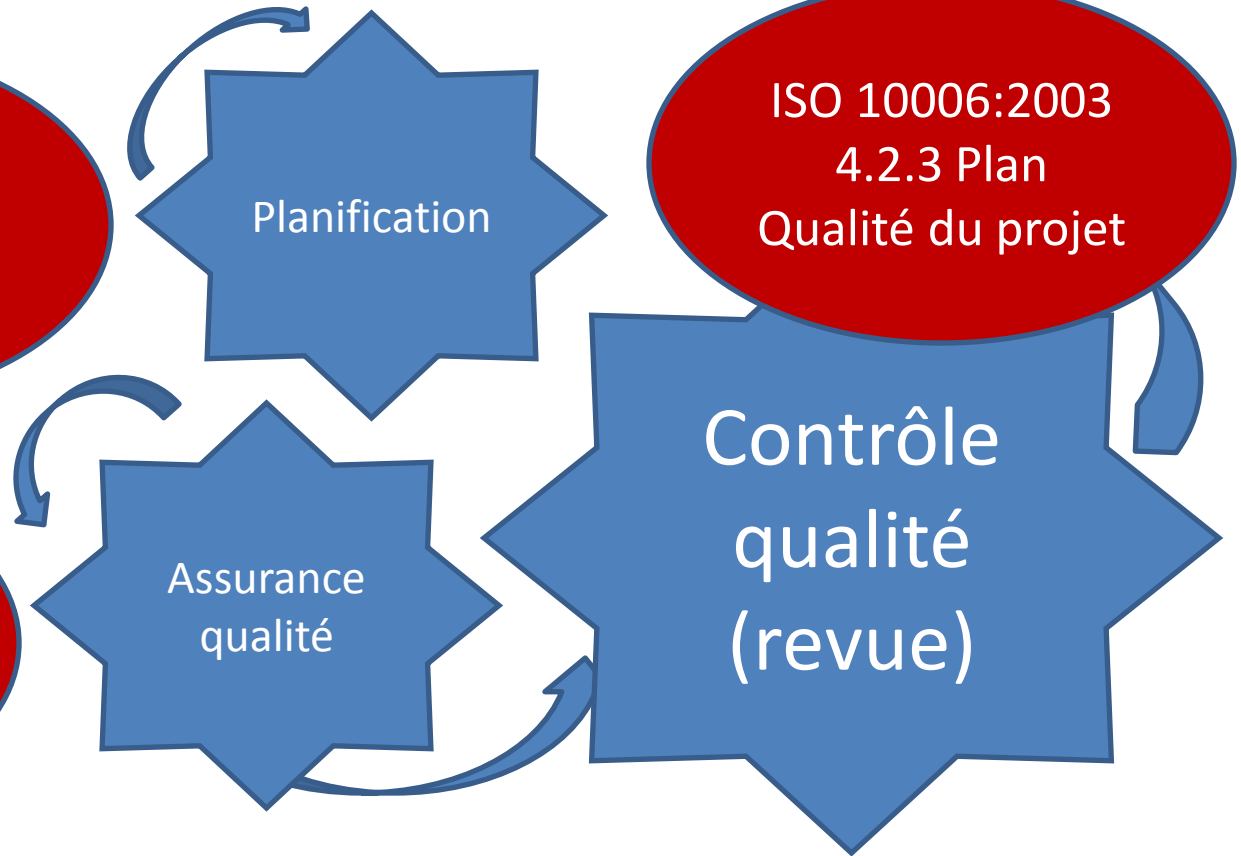
ISO 10006:2003  
4.2.2 Système de  
Management de  
la Qualité du  
Projet

Planification

ISO 10006:2003  
4.2.3 Plan  
Qualité du projet

Assurance  
qualité

Contrôle  
qualité  
(revue)



# 5. Le management des ressources humaines du projet

Processus requis pour assurer l'achèvement du projet selon les critères de qualité définis

Planification des ressources humaines

Former l'équipe de projet

Développer l'équipe de projet

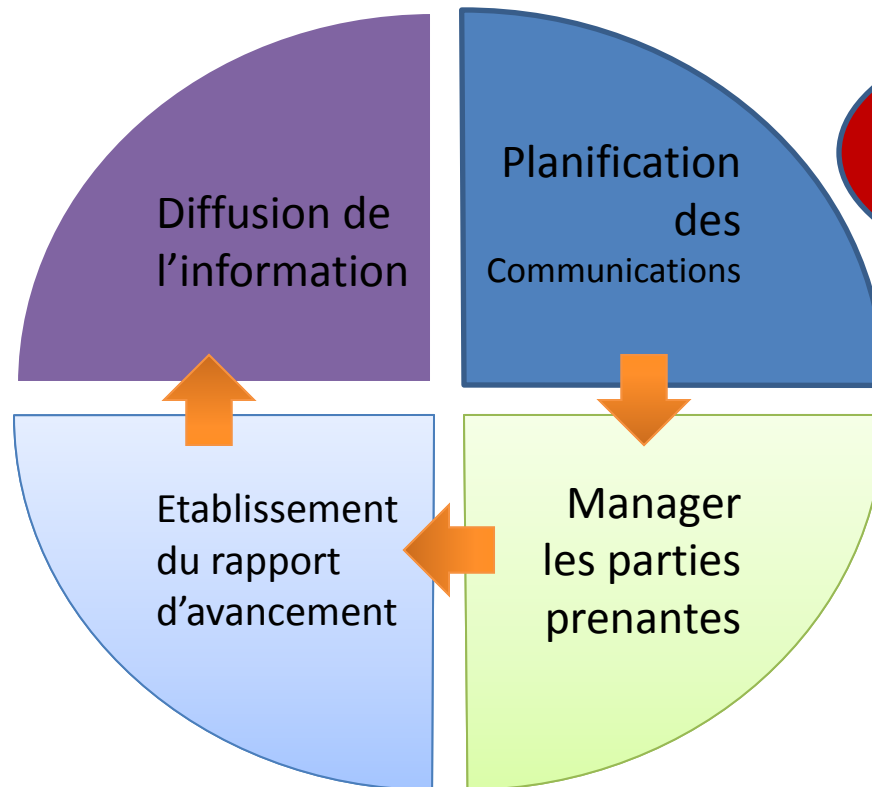
Diriger l'équipe de projet

ISO 10006:2003  
6.2.2 Etablissement de la  
structure organisationnelle  
du projet

ISO 10006:2003  
6.2.3 Affectation du  
personnel

# 5. Le management des communications du projet

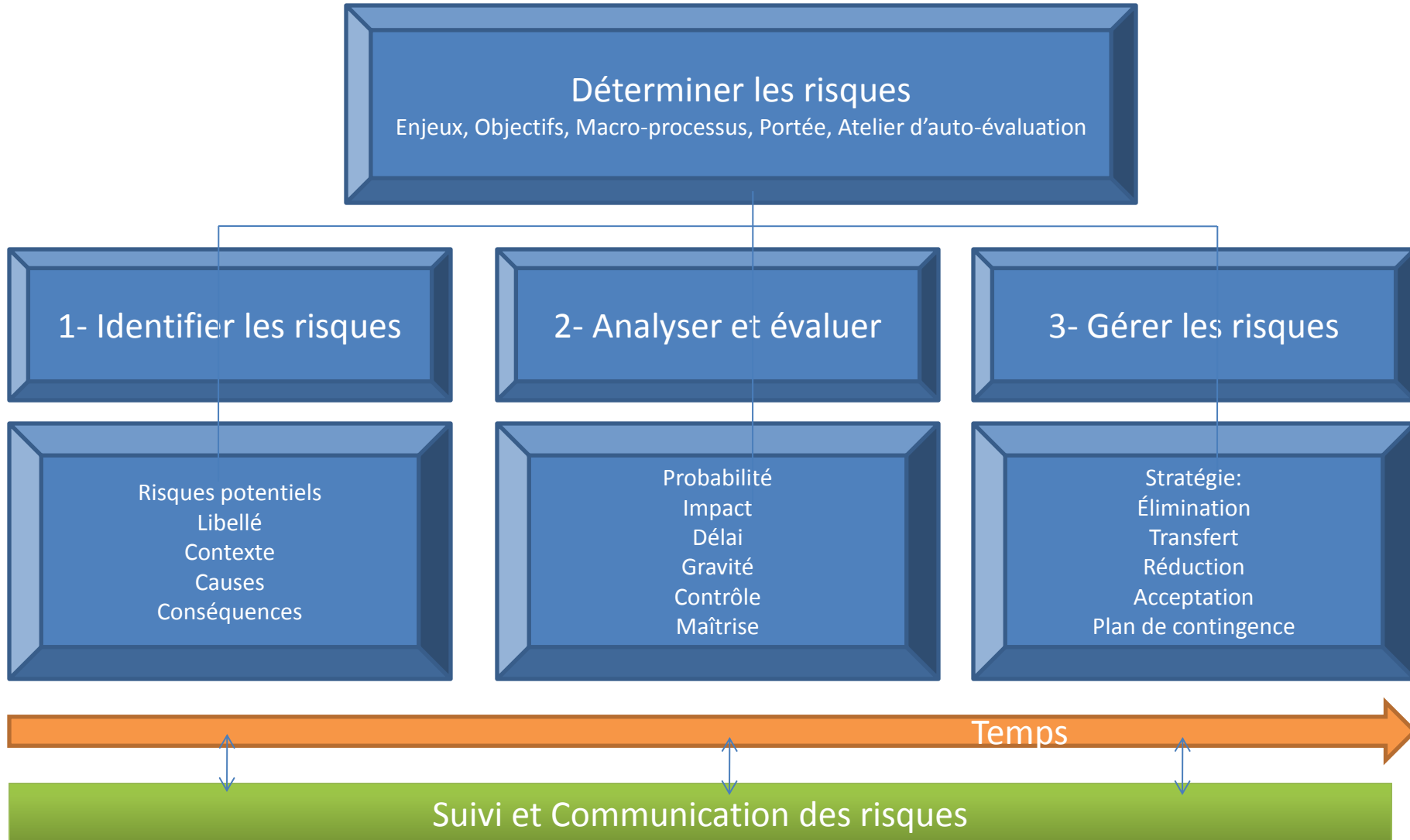
Processus requis pour assurer de la génération, collection, dissémination, stockage et disposition ultime des informations du projet dans le temps et de manière appropriée



**ISO 10006:2003**  
**7.6.2 Planification**  
**de la**  
**communication**



# 5. Management des risques



# 5. Management des risques

## **Exercice 4: Risques de projet SMSI**

- Listez les principaux risques reliés à un projet de mise en œuvre d'un SMSI en vous appuyant sur vos connaissances en gestion de projet et sur les facteurs propres au SMSI
- Déterminez les 3 risques qui sont selon vous les plus importants et proposez une solution de gestion de chacun de ces risques

# 5. Management des approvisionnementnements du projet

Procédure nécessaire pour le domaine d'application du projet

•Planifier les approvisionnementnements

•Planifier les contrats

•Solliciter des offres ou des propositions des fournisseurs

•Choisir les fournisseurs

•Administration du contrat

•Clôture du contrat

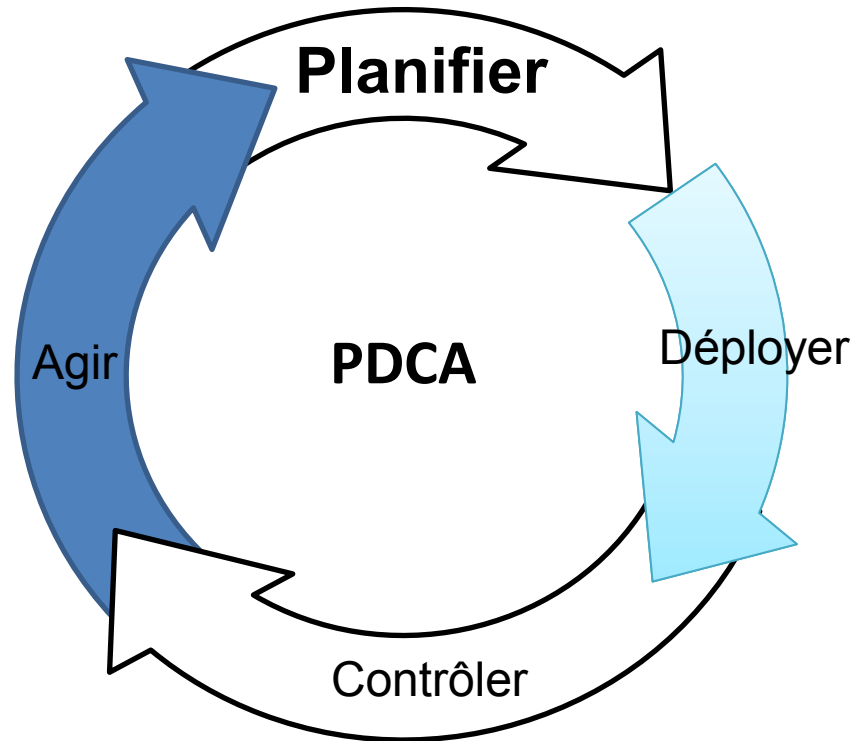
ISO 10006:2003  
7.8.2 Planification et  
maîtrise des achats

ISO 10006:2003  
7.8.3 Documentation des  
exigences d'achat

# La planification du SMSI

1. Gouvernance
2. Analyse des risques
3. Déclaration d'applicabilité

# 1. Gouvernance du SMSI



3.1. Rôles et responsabilités

(nommer RSSI, Auditeurs, Opérationnels d'analyse de risque)

3.2. Domaine d'application et limites

3.3. Politique

# 1. Gouvernance du SMSI

|                             |                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Objectifs</b>            | Mettre en œuvre le cadre de gouvernance du SMSI                                                                                           |
| <b>Pré requis</b>           | ISO 27001:2005 Clause 5<br>Responsabilité de la Direction                                                                                 |
| <b>Personnes impliquées</b> | CISO, CIO, haute direction                                                                                                                |
| <b>Mise en œuvre</b>        | Comités de gouvernance, de pilotage et d'audit du SMSI, domaine d'application et politique du SMSI, rôles&responsabilités de la direction |
| <b>Livrables</b>            | Politique de gouvernance du SMSI et autres documents associés (chartes des comités, comptes rendus de réunions...)                        |

# 1. Pré requis ISO 27001

# 1. Définition de la gouvernance



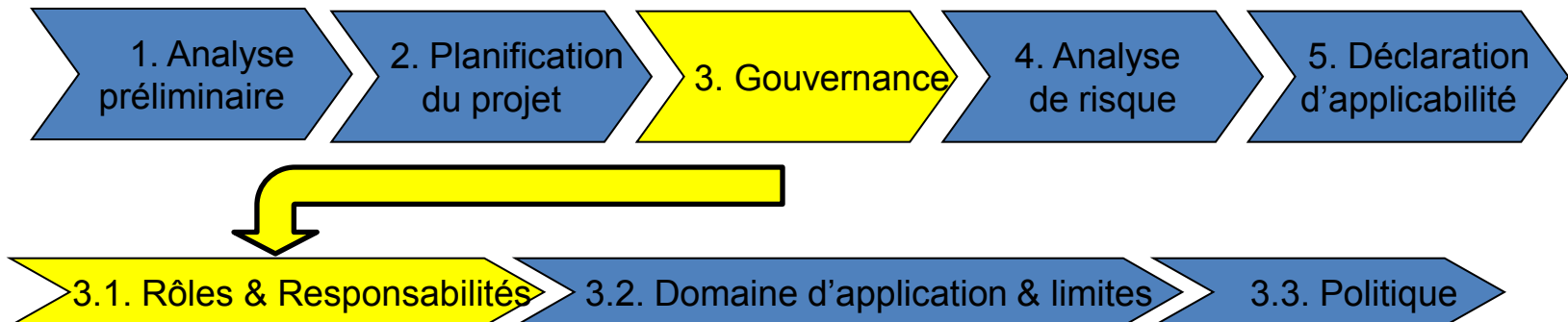
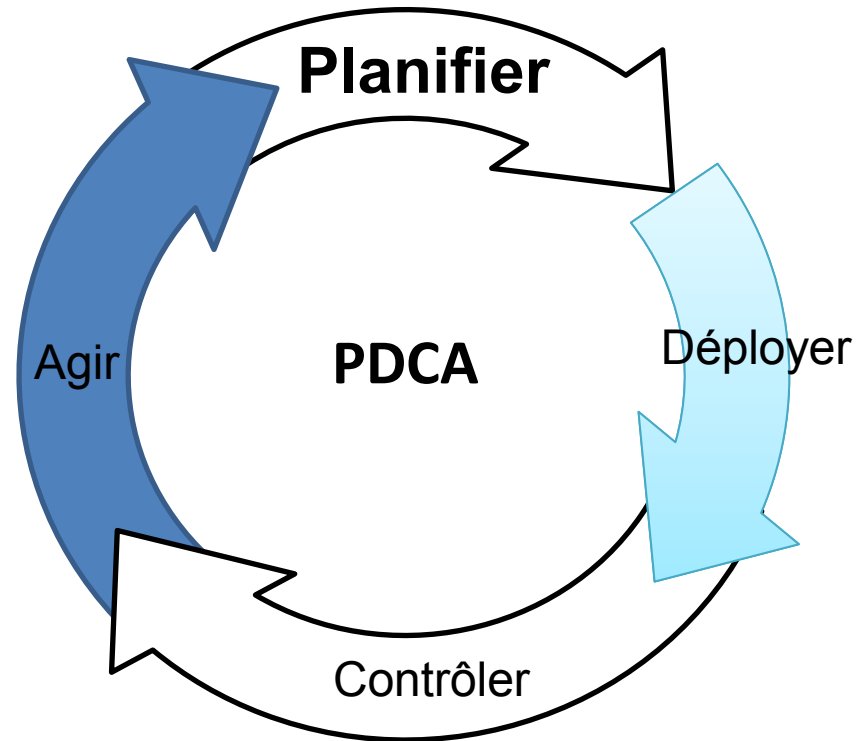
# 1. Définition : Gouvernance de la sécurité de l'information

# 1. Activités de gouvernance SMSI

# 1. Intégrer le modèle COBIT

# 1. Modèle de gouvernance

# 1. Rôles et Responsabilités



# 1. Rôles et responsabilités

|                             |                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Objectifs</b>            | Mettre en œuvre le cadre de gouvernance du SMSI                                                                                           |
| <b>Pré requis</b>           | ISO 27001:2005 Clause 5<br>Responsabilité de la Direction                                                                                 |
| <b>Personnes impliquées</b> | CISO, CIO, haute direction                                                                                                                |
| <b>Mise en œuvre</b>        | Comités de gouvernance, de pilotage et d'audit du SMSI, domaine d'application et politique du SMSI, rôles&responsabilités de la direction |
| <b>Livrables</b>            | Politique de gouvernance du SMSI et autres documents associés (chartes des comités, comptes rendus de réunions...)                        |

# 1. Mise en œuvre

# 1. Mise en œuvre : comité de direction

|                                          |  |
|------------------------------------------|--|
| <b>Objectif</b>                          |  |
| <b><i>Niveau<br/>d'intervention</i></b>  |  |
| <b><i>Missions</i></b>                   |  |
| <b><i>Membres</i></b>                    |  |
| <b><i>Fréquence des<br/>réunions</i></b> |  |



# 1. Mise en œuvre : comité de pilotage

|                                          |  |
|------------------------------------------|--|
| <b>Objectif</b>                          |  |
| <b><i>Niveau<br/>d'intervention</i></b>  |  |
| <b><i>Missions</i></b>                   |  |
| <b><i>Membres</i></b>                    |  |
| <b><i>Fréquence des<br/>réunions</i></b> |  |

# 1. Mise en œuvre : comité opérationnel

|                                          |  |
|------------------------------------------|--|
| <b>Objectif</b>                          |  |
| <b><i>Niveau<br/>d'intervention</i></b>  |  |
| <b><i>Missions</i></b>                   |  |
| <b><i>Membres</i></b>                    |  |
| <b><i>Fréquence des<br/>réunions</i></b> |  |

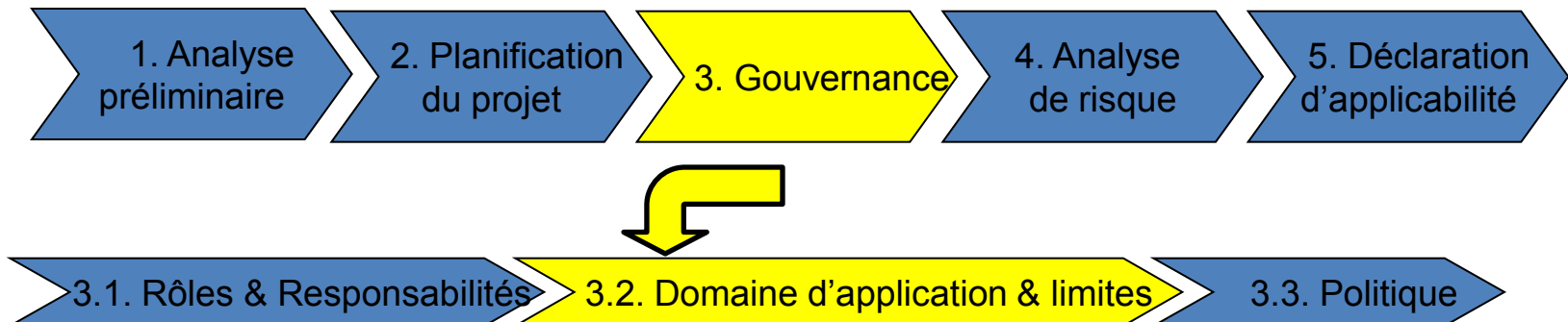
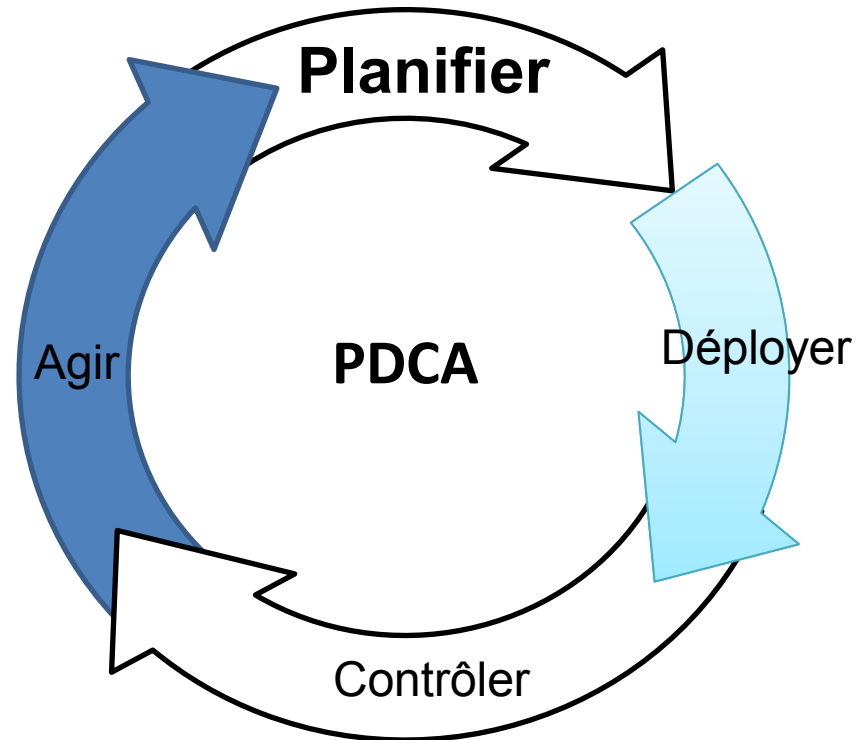
# 1. Mise en œuvre : comité d'audit

|                                          |  |
|------------------------------------------|--|
| <b>Objectif</b>                          |  |
| <b><i>Niveau<br/>d'intervention</i></b>  |  |
| <b><i>Missions</i></b>                   |  |
| <b><i>Membres</i></b>                    |  |
| <b><i>Fréquence des<br/>réunions</i></b> |  |

# 1. Autres comités potentiels

# 1. Rôles et responsabilités des principaux responsables

# 1. Domaine d'application



# 1. Domaine d'application et limites du SMSI

|                             |                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Objectifs</b>            | Mettre en œuvre le cadre de gouvernance du SMSI                                                                                           |
| <b>Pré requis</b>           | ISO 27001:2005 Clause 5<br>Responsabilité de la Direction                                                                                 |
| <b>Personnes impliquées</b> | CISO, CIO, haute direction                                                                                                                |
| <b>Mise en œuvre</b>        | Comités de gouvernance, de pilotage et d'audit du SMSI, domaine d'application et politique du SMSI, rôles&responsabilités de la direction |
| <b>Livrables</b>            | Politique de gouvernance du SMSI et autres documents associés (chartes des comités, comptes rendus de réunions...)                        |

# 1. Pré requis de ISO 27001



# 1. Définition

# 1. Environnement interne et externe

# 1. Les domaines d'applications possibles

# La planification du SMSI

1. Gouvernance
2. Analyse des risques
3. Déclaration d'applicabilité

# La planification du SMSI

1. Gouvernance
2. Analyse des risques
3. Déclaration d'applicabilité

# La planification du SMSI

1. Gouvernance
2. Analyse des risques
3. Déclaration d'applicabilité

# La planification du SMSI

1. Gouvernance
2. Analyse des risques
3. Déclaration d'applicabilité

# La mise en œuvre de la SMSI

1. Gestion documentaire
2. Design des mesures de contrôle et procédures
3. Mise en œuvre des mesures de contrôle
4. Formation, sensibilisation et communication
5. Gestion des incidents
6. Gestion des opérations



# Le contrôle, l'audit, l'amélioration du SMSI

1. Monitoring des mesures de contrôle
2. Mesure de la performance des mesures de contrôle
3. Audit interne du SMSI
4. Amélioration continue
5. Audit de certification