

Normes Légales en Matière de Sécurité Informatique en France



Agenda

- Cadre réglementaire français
OIV, OSE et leur contexte juridique
- Obligations et responsabilités
Exigences légales pour les différentes catégories d'organismes
- Institutions et autorités de contrôle
ANSSI et son rôle dans la cybersécurité nationale
- Normes et méthodologies
ISO 27001, méthode PDCA et leur application



Contexte Réglementaire Français

Protéger ses infrastructures critiques et assurer la résilience numérique de ses institutions essentielles.

Ce cadre s'articule autour de plusieurs dispositifs complémentaires, dont les principaux sont les régimes OIV et OSE, qui répondent à des impératifs tant nationaux qu'européens.



Organismes d'Importance Vitale (OIV)

Les OIV constituent la première catégorie d'organismes soumis à des obligations renforcées en matière de cybersécurité en France.



Définition

Organisme public ou privé exerçant des activités indispensables à la survie de la Nation ou dangereuses pour la population



Fondement juridique

Loi de Programmation Militaire (LPM) – Portée strictement française



Nombre

Environ 250 opérateurs répartis dans 12 secteurs d'activité vitaux pour la France

Secteurs d'Activités d'Importance Vitale



Systemes d'Information d'Importance Vitale (SIIV)

Caractéristiques des SIIV

Les Systèmes d'Information d'Importance Vitale sont les systèmes numériques critiques exploités par les OIV, dont la compromission pourrait:

- Nuire gravement au potentiel de guerre ou économique de la France
- Compromettre la sécurité ou la survie de la Nation
- Menacer la sécurité de la population



Ces systèmes sont soumis à des règles de sécurité particulièrement strictes et font l'objet d'une surveillance accrue.

Organismes de Services Essentiels (OSE)

Définition et portée

Les OSE sont des entités fournissant un service essentiel au fonctionnement de la société ou de l'économie, dont la continuité dépend des réseaux et systèmes d'information.

Ce statut provient de la directive européenne NIS (Network and Information Security), transposée en droit français.

122

Opérateurs désignés

En France, répartis dans 11
secteurs d'activité

27

États membres

Applicant la directive NIS
à l'échelle européenne

Secteurs Concernés par le Statut OSE



Énergie

Production, transport et distribution d'électricité, pétrole et gaz



Infrastructures numériques

Points d'échange Internet, DNS, registres de noms de domaine



Secteur bancaire

Établissements de crédit et infrastructures de marchés financiers



Santé

Établissements de soins et laboratoires de référence

Systemes d'Information Essentiels (SIE)

Définition

Les SIE sont les systèmes d'information qui soutiennent les services essentiels fournis par les OSE. Leur compromission pourrait entraîner une perturbation grave du service essentiel.

Chaque OSE doit identifier ses SIE et les déclarer à l'ANSSI dans un délai légal après sa désignation.

Critères de criticité

- Impact sur la continuité du service essentiel
- Nombre d'utilisateurs dépendant du service
- Dépendance d'autres secteurs essentiels
- Impact potentiel en termes de sécurité publique
- Part de marché de l'opérateur

N°	Règle	Délai d'application
I - Règles relatives à la gouvernance de la sécurité des réseaux et SI		
1	Analyse de risque	< 3 ans *
2	Politique de sécurité	1 an
3	Homologation de sécurité	< 3 ans *
4	Indicateurs	2 ans
5	Audits de la sécurité	< 3 ans *
6	Cartographie	1 an
II. Règles relatives à la protection des réseaux et SI		
Section 1 : Sécurité de l'architecture		
7	Configuration	1 an
8	Cloisonnement	2 ans
9	Accès distant	2 ans
10	Filtrage	2 ans
Section 2 : Sécurité de l'administration		
11	Comptes d'administration	2 ans
12	Systèmes d'information d'administration	2 ans
Section 3 : Gestion des identités et des accès		
13	Identification	1 an
14	Authentification	1 an
15	Droits d'accès	1 an
Section 4 : Maintien en conditions de sécurité		
16	Procédure de maintien en conditions de sécurité	1 an
Section 5 : Sécurité physique et environnementale		
17	Sécurité physique et environnementale	1 an
III. Règles relatives à la défense des réseaux et systèmes d'information		
Section 1 : Détection des incidents de sécurité		
18	Détection	2 ans
19	Journalisation	1 an
20	Corrélation et analyse de journaux	2 ans
Section 2 : Gestion des incidents de sécurité		
21	Réponse aux incidents	1 an
22	Traitement des alertes	3 mois
IV. Règles relatives à la résilience des activités		
23	Gestion de crises	1 an

Les Obligations des OSE

Gouvernance

Mise en place d'une gouvernance efficace de la sécurité des réseaux et systèmes d'information

Protection

Déploiement de mesures de protection adaptées aux risques identifiés

Défense

Capacité à détecter et à répondre aux incidents de sécurité

Résilience

Garantie de la continuité des activités essentielles même en cas d'incident

* SIE en service avant désignation de l'OSE : 3 ans.

SIE mis en service dans un délai de 2 ans maximum après désignation de l'OSE : 2 ans.

SIE mis en service 2 ans ou plus après désignation de l'OSE : avant mise en service en service.

Les Critères de Désignation OSE

Critères principaux

- Fournir un service considéré comme essentiel au maintien d'activités sociétales ou économiques critiques
- La fourniture de ce service dépend des réseaux et systèmes d'information
- Un incident aurait des effets perturbateurs significatifs sur la fourniture du service

Critères sectoriels spécifiques

Chaque secteur dispose de critères additionnels propres à son domaine d'activité:

- Seuils quantitatifs (nombre d'utilisateurs, part de marché)
- Couverture géographique
- Importance stratégique nationale
- Absence d'alternatives disponibles



OIV vs OSE: Domaine d'Application



OIV: Portée nationale

Les OIV relèvent d'un dispositif strictement français, défini par la Loi de Programmation Militaire, et s'inscrivent dans une logique de sécurité et de défense nationales.



OSE: Portée européenne

Les OSE sont issus de la directive européenne NIS, harmonisant les approches de cybersécurité à l'échelle de l'Union Européenne pour le marché unique numérique.

Ces deux dispositifs peuvent se superposer: certains organismes peuvent être à la fois OIV et OSE, et doivent alors se conformer aux deux séries d'obligations.

OIV vs OSE: Les Objectifs

Objectifs des OIV

- Protéger la capacité de survie de la Nation
- Garantir la continuité des fonctions vitales de l'État
- Préserver le potentiel de défense national
- Sécuriser les infrastructures critiques contre tous types de menaces, y compris terroristes

Objectifs des OSE

- Assurer un niveau commun élevé de cybersécurité dans l'UE
- Garantir la continuité des services essentiels au fonctionnement de l'économie
- Renforcer la coopération entre États membres
- Développer une culture de gestion des risques

OIV vs OSE: Responsabilité et Supervision



OIV: Contrôle étatique direct

Supervision directe par l'ANSSI et les ministères de tutelle sectoriels avec des pouvoirs d'inspection étendus et des sanctions pénales possibles



OSE: Coordination européenne

Supervision par les autorités nationales compétentes avec un mécanisme de coordination européen et des sanctions administratives harmonisées



Partage d'information

Obligations de notification d'incidents et participation aux échanges d'informations via des réseaux sectoriels et transversaux

OIV vs OSE: Conclusion Comparative

Critère	OIV	OSE
Origine juridique	Loi de Programmation Militaire (France)	Directive NIS (Europe)
Nombre d'entités	≈ 250	≈ 122
Secteurs	12 secteurs d'activité vitale	11 secteurs de services essentiels
Systèmes concernés	SIIV (Systèmes d'Information d'Importance Vitale)	SIE (Systèmes d'Information Essentiels)
Sanctions maximales	Sanctions pénales possibles	Sanctions administratives jusqu'à 100 000€

Fournisseurs de Service Numérique (FSN)

Définition

Catégorie distincte introduite par la directive NIS, les FSN sont des entreprises qui fournissent des services numériques dans l'Union Européenne.

Ils sont soumis à un régime différent des OIV et OSE, mais doivent également respecter des obligations de sécurité.

Types de services concernés

- Places de marché en ligne
- Moteurs de recherche en ligne
- Services d'informatique en nuage (cloud computing)

Critères d'applicabilité: plus de 50 salariés et un chiffre d'affaires annuel supérieur à 10 millions d'euros.

Synthèse des Régimes Réglementaires

Sigle	Signification	Origine réglementaire	Système d'information	Remarques
OIV	Organisme d'importance vitale	Loi de programmation militaire (LPM). Portée française	SIIV (système d'information d'importance vitale)	12 secteurs d'activité Environ 250 OIV
OSE	Organisme de services essentiels	Directive NIS. Portée européenne	SIE (système d'information essentiel)	11 secteurs d'activité Environ 122 OSE
FSN	Fournisseur de services numériques	Directive NIS. Portée européenne	-	Effectif > 50 salariés et CA > 10 M€

Normes vs Référentiels

Normes

- Documents publiés par des organismes de normalisation (ISO, AFNOR)
- Consensus international ou national
- Caractère volontaire sauf si rendu obligatoire par la réglementation
- Exemple: ISO 27001 pour la gestion de la sécurité de l'information

Référentiels

- Guides de bonnes pratiques élaborés par des autorités ou organismes spécialisés
- Souvent plus détaillés et opérationnels que les normes
- Adaptés à des contextes spécifiques
- Exemple: Référentiel d'exigences de l'ANSSI pour les OIV

Règlement Général sur la Protection des Données (RGPD)

Principes fondamentaux

- Licéité, loyauté et transparence du traitement
- Limitation des finalités
- Minimisation des données
- Exactitude des données
- Limitation de la conservation
- Intégrité et confidentialité
- Responsabilité du responsable de traitement



Le RGPD s'applique à tous les organismes, y compris les OIV et OSE, et complète les exigences de sécurité spécifiques avec des obligations en matière de protection des données personnelles.

Intersection RGPD et Sécurité des Systèmes d'Information



Sécurité des traitements

Le RGPD exige des mesures techniques et organisationnelles appropriées pour assurer la sécurité des données personnelles



Notification des violations

Obligation de notifier les violations de données à l'autorité de contrôle dans les 72 heures et aux personnes concernées si risque élevé



Analyses d'impact

Obligation de réaliser des analyses d'impact relatives à la protection des données pour les traitements à risque élevé



Loi Informatique et Libertés

Historique et évolution

Adoptée en 1978, la loi Informatique et Libertés a été la première législation française complète sur la protection des données personnelles.

Elle a été profondément modifiée en 2018 pour s'adapter au RGPD tout en conservant certaines spécificités nationales.



Rôle de la CNIL

La Commission Nationale de l'Informatique et des Libertés est l'autorité administrative indépendante chargée de veiller au respect de la loi Informatique et Libertés et du RGPD en France.

Loi pour la Confiance dans l'Économie Numérique (LCEN)

Objectif et portée

Adoptée en 2004, la LCEN a transposé la directive européenne sur le commerce électronique et encadre diverses activités numériques.

Elle établit le régime de responsabilité des acteurs de l'internet et fixe les obligations en matière de commerce électronique.

Dispositions principales

- Définition et obligations des hébergeurs et éditeurs de contenus
- Encadrement de la publicité par voie électronique
- Régime de la preuve électronique
- Obligations d'identification des sites web commerciaux
- Protection des consommateurs dans les transactions électroniques



Loi relative à la sécurité de l'information

La France dispose d'un cadre juridique étendu concernant la sécurité de l'information, au-delà des régimes OIV et OSE.



Loi de programmation militaire

La LPM 2019-2025 renforce les obligations de sécurité pour les opérateurs critiques et les pouvoirs de l'ANSSI



Loi République numérique

Renforce l'open data, la neutralité du net et introduit des dispositions sur la loyauté des plateformes



Code pénal

Articles 323-1 à 323-8 relatifs aux atteintes aux systèmes de traitement automatisé de données



Code de la défense

Dispositions relatives à la sécurité des systèmes d'information sensibles et à la cryptologie

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Mission et statut

L'ANSSI est l'autorité nationale en matière de cybersécurité. Créée en 2009, elle est rattachée au Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), sous l'autorité du Premier ministre.

Elle constitue l'autorité nationale compétente pour la mise en œuvre de la directive NIS et la supervision des OIV et OSE.



Rôles et Responsabilités de l'ANSSI



Protection

Conception et déploiement de mécanismes de défense des systèmes sensibles de l'État et des infrastructures critiques



Détection

Surveillance permanente, détection et alerte sur les cybermenaces affectant les administrations et opérateurs critiques



Réaction

Coordination de la réponse gouvernementale aux incidents majeurs, assistance technique aux victimes d'attaques



Prévention

Élaboration de recommandations, certification de solutions de sécurité, sensibilisation et formation



Pouvoirs de l'ANSSI

Pouvoirs de contrôle

- Audit et inspection des systèmes d'information des OIV et OSE
- Vérification de la conformité aux règles de sécurité
- Possibilité d'imposer des mesures correctives
- Qualification de prestataires de services de cybersécurité

Pouvoirs en cas de crise

- Déclenchement du plan gouvernemental de vigilance, prévention et protection face aux cybermenaces
- Coordination de la réponse interministérielle
- Possibilité d'imposer des mesures d'urgence aux opérateurs
- Publication d'alertes et de recommandations contraignantes

La Gouvernance Selon la Norme ISO 26000

Principes de la gouvernance

La norme ISO 26000, bien que focalisée sur la responsabilité sociétale, définit des principes de gouvernance applicables à la sécurité de l'information:

- Responsabilité de rendre compte
- Transparence
- Comportement éthique
- Reconnaissance des intérêts des parties prenantes
- Respect du principe de légalité
- Respect des normes internationales de comportement
- Respect des droits de l'homme



Application de la Gouvernance à la Cybersécurité



La Norme ISO 27001

Définition et portée

La norme ISO 27001 est la référence internationale pour la gestion de la sécurité de l'information. Elle spécifie les exigences pour établir, mettre en œuvre, maintenir et améliorer continuellement un système de management de la sécurité de l'information (SMSI).

Structure et approche

La norme adopte une approche par les risques et s'articule autour:

- Du contexte de l'organisation
- Du leadership et engagement de la direction
- De la planification du SMSI
- Des mesures de support
- Des activités opérationnelles
- De l'évaluation des performances
- De l'amélioration continue

ISO 27001: Les Cibles

Confidentialité
Protection contre l'accès ou la
divulcation non autorisés
d'informations

Preuve
Capacité à démontrer les actions
et événements qui ont eu lieu



Intégrité

Garantie de l'exactitude et de la
complétude des informations et
des méthodes de traitement

Disponibilité

Accessibilité et utilisabilité des
informations et systèmes sur
demande par une entité autorisée

ISO 27001: Due Diligence

Concept et importance

La due diligence en matière de sécurité de l'information désigne l'ensemble des vérifications qu'une organisation prudente et raisonnable doit effectuer pour identifier et gérer les risques liés à la sécurité.

C'est un élément clé de la norme ISO 27001, qui exige une approche systématique d'identification et d'évaluation des risques.

Mise en œuvre

- Identification exhaustive des actifs informationnels
- Évaluation méthodique des menaces et vulnérabilités
- Analyse de l'impact potentiel sur l'activité
- Sélection de mesures de traitement proportionnées
- Documentation des décisions et justifications
- Révision périodique du processus

ISO 27001: Application à la Conformité Réglementaire



Identification des obligations

Recensement des exigences légales, réglementaires et contractuelles applicables à l'organisation



Intégration dans le SMSI

Incorporation des obligations réglementaires dans les politiques et procédures de sécurité



Vérification de la conformité

Audits et contrôles réguliers pour s'assurer du respect continu des exigences



Adaptation aux évolutions

Veille réglementaire et mise à jour du SMSI pour intégrer les nouvelles obligations

ISO 27001 dans un Contexte Plus Global

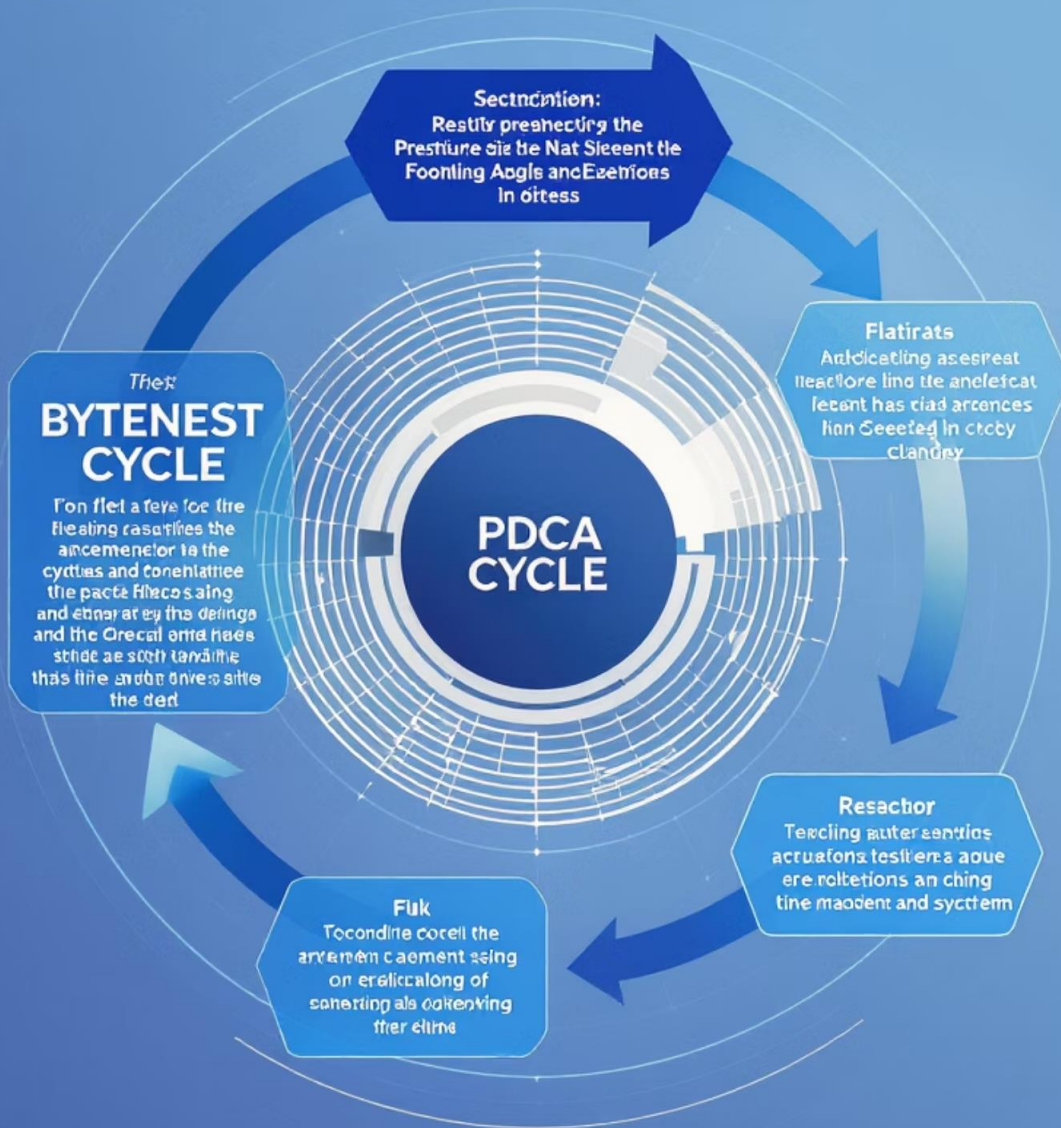
Famille ISO 27000

La norme ISO 27001 s'inscrit dans une famille de normes complémentaires:

- ISO 27000: Vue d'ensemble et vocabulaire
- ISO 27002: Code de bonnes pratiques
- ISO 27003: Guide d'implémentation
- ISO 27004: Mesures
- ISO 27005: Gestion des risques
- ISO 27017/27018: Sécurité du cloud et protection des données personnelles

Synergie avec d'autres référentiels

- ITIL pour la gestion des services informatiques
- COBIT pour la gouvernance IT
- NIST Cybersecurity Framework
- Référentiels sectoriels (HDS pour la santé, PCI-DSS pour les paiements, etc.)
- Exigences spécifiques OIV/OSE de l'ANSSI



Les Principes PDCA

Une méthodologie de perfectionnement de la performance résultant de l'Amélioration Continue



Flattars & Freshalies



Corerabral



Forenciare fate etien
to errationeces nlate

Fondements de la Méthode PDCA

Origine et philosophie

Développée par W. Edwards Deming, la méthode PDCA (Plan-Do-Check-Act) est un processus itératif d'amélioration continue.

Elle repose sur la répétition de cycles courts permettant d'améliorer progressivement la qualité et l'efficacité des processus.

Caractéristiques clés

- Approche systématique et méthodique
- Application sur des solutions existantes pour les optimiser
- Fondée sur des tests empiriques
- Applicable à l'échelle d'un processus ou d'un système entier
- Implique une démarche participative

Les Quatre Étapes du Cycle PDCA

PLAN (Planifier)

Définir les objectifs, le périmètre, les rôles et responsabilités, et développer les procédures nécessaires

ACT (Agir)

Identifier et mettre en œuvre les ajustements nécessaires pour améliorer les services, procédures et systèmes



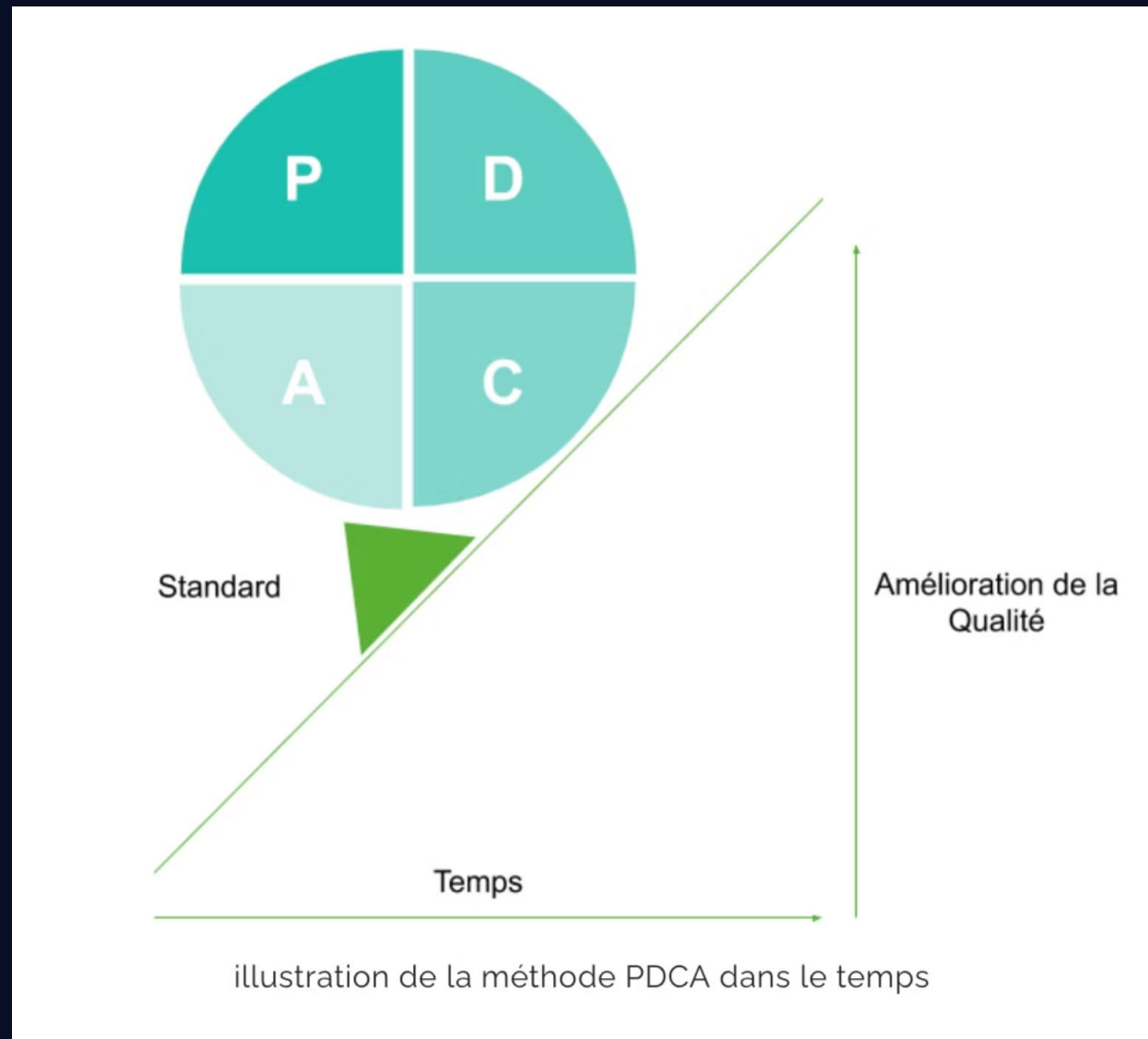
DO (Faire)

Mettre en œuvre le plan d'actions en allouant les ressources nécessaires (financières, humaines, matérielles)

CHECK (Vérifier)

Surveiller, mesurer et évaluer les résultats par rapport aux objectifs initiaux à travers des audits et contrôles

ÉTAPE 1: Plan (Planifier)



Activités clés de la phase de planification

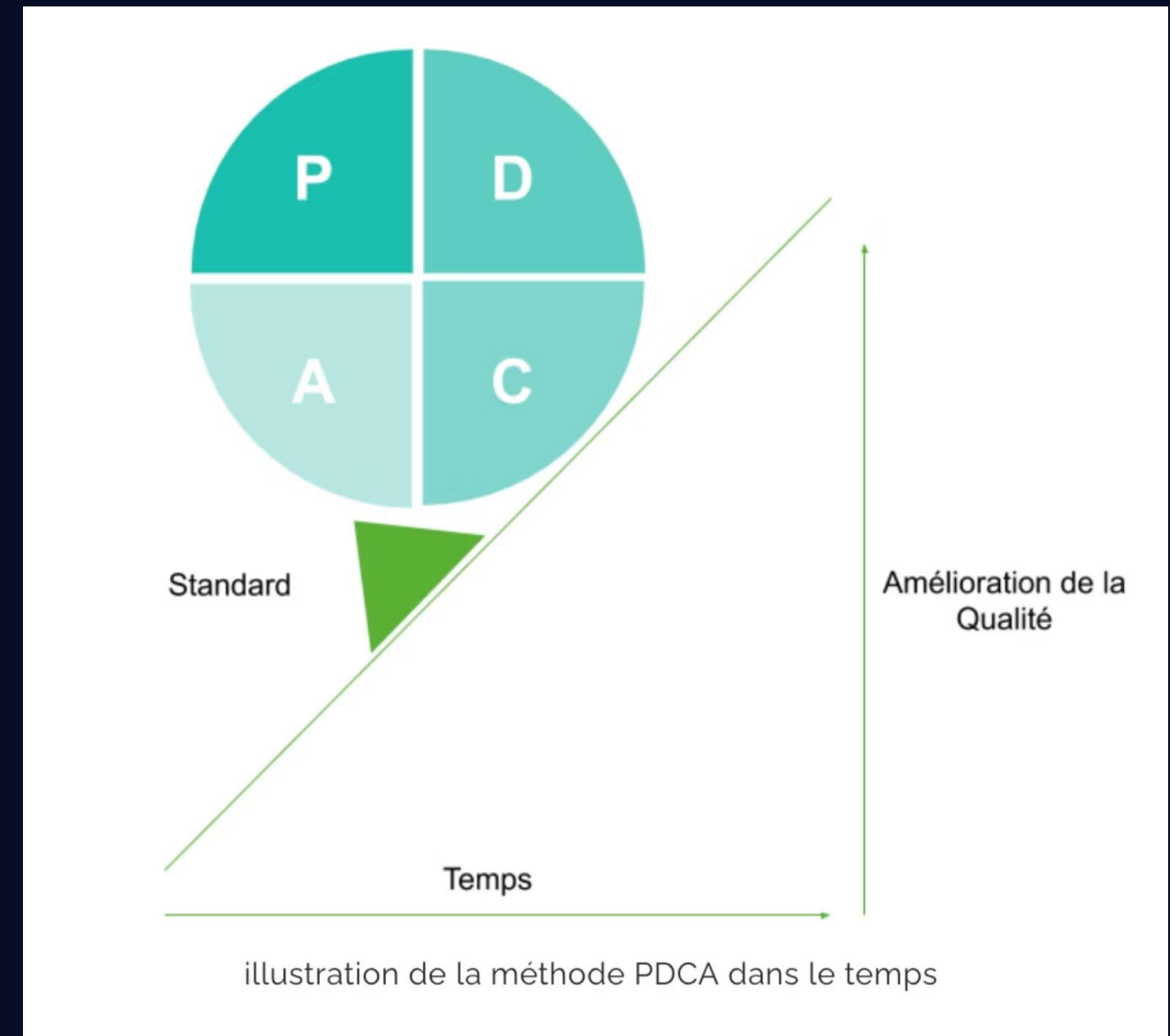
- Définir les buts, les objectifs et le périmètre de l'action
- Déterminer ce qui doit être atteint avec précision
- Établir les rôles et responsabilités des différents acteurs
- Développer les procédures nécessaires
- Identifier les composants techniques et les outils requis
- Définir les interfaces avec les services existants

ÉTAPE 2: Do (Faire)

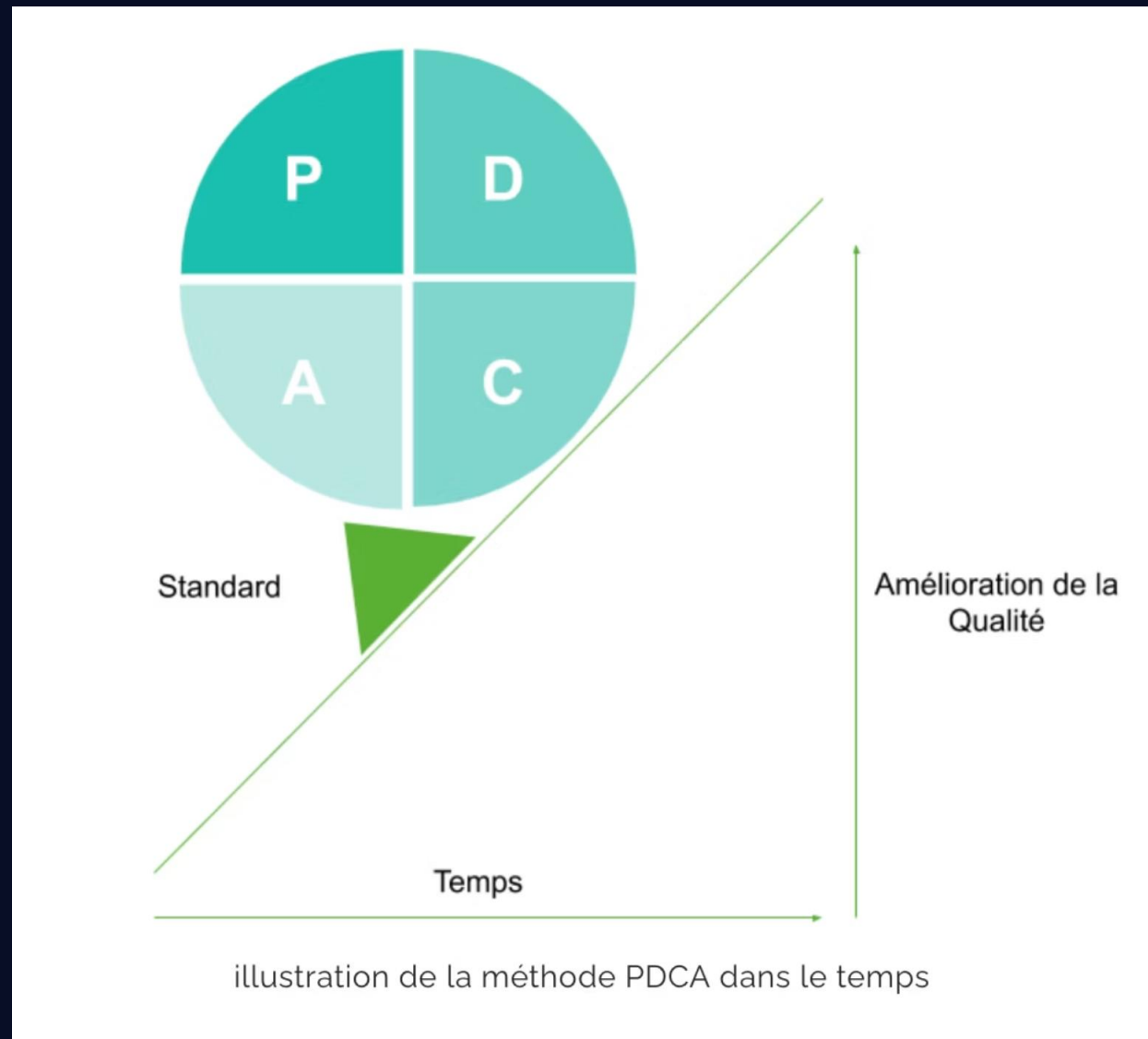
Mise en œuvre opérationnelle

La phase "Do" consiste à exécuter concrètement ce qui a été planifié en mobilisant les ressources appropriées:

- Élaborer un plan d'actions détaillé avec des jalons clairs
- Identifier et obtenir les ressources financières nécessaires
- Mobiliser et former le personnel impliqué
- Acquérir les outils et équipements requis
- Communiquer auprès des parties prenantes
- Documenter les actions entreprises



ÉTAPE 3: Check (Vérifier)



Évaluation des résultats

La phase "Check" permet de mesurer l'efficacité des actions entreprises:

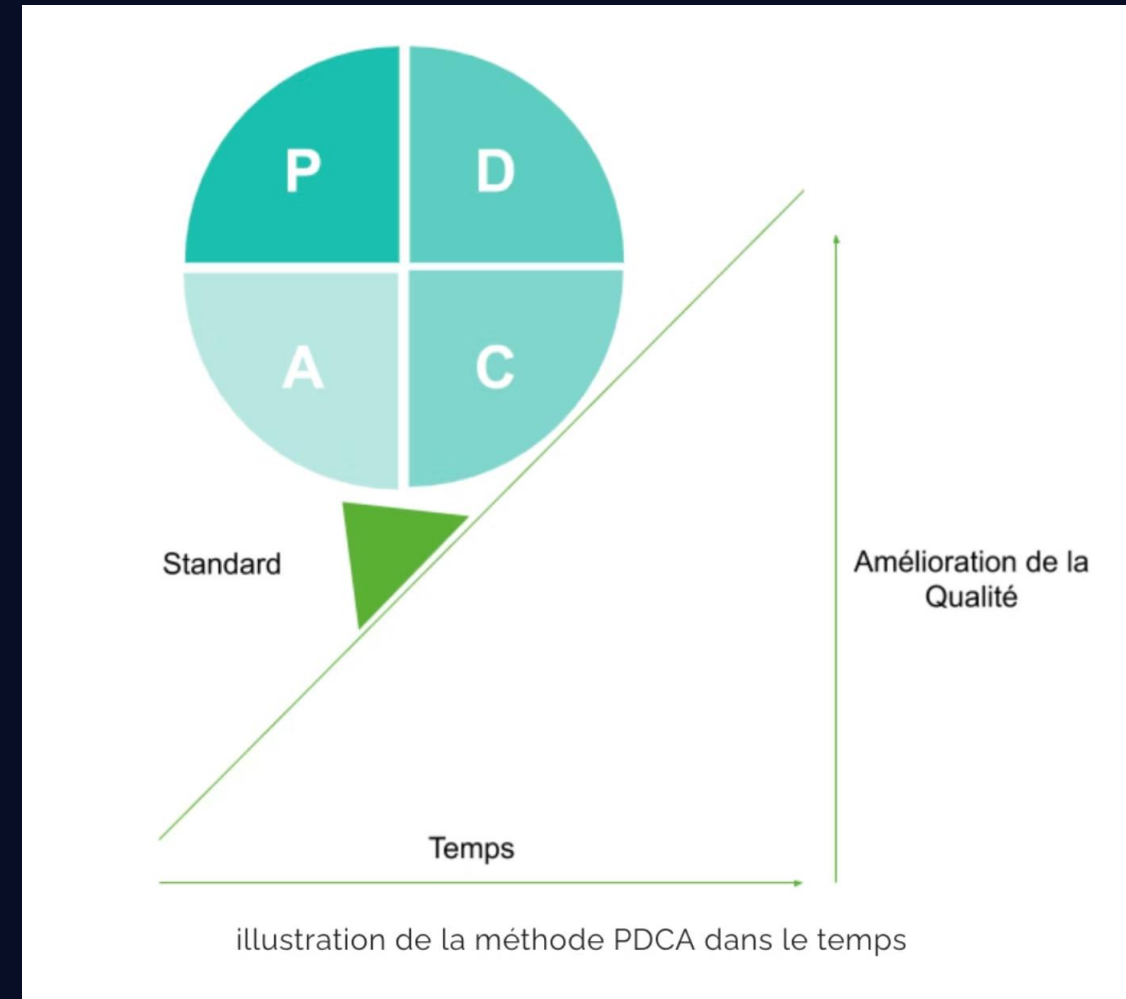
- Surveiller systématiquement l'exécution des activités
- Mesurer les résultats à l'aide d'indicateurs prédéfinis
- Comparer les résultats obtenus avec les objectifs initiaux
- Examiner la documentation produite
- Évaluer les services par des audits internes ou externes
- Identifier les écarts et leurs causes

ÉTAPE 4: Act (Agir)

Amélioration et ajustement

La phase "Act" consiste à utiliser les résultats de l'évaluation pour apporter des améliorations:

- Identifier les ajustements nécessaires pour combler les écarts
- Mettre en œuvre des actions correctives ciblées
- Améliorer les services, procédures ou composants techniques
- Standardiser les bonnes pratiques identifiées
- Communiquer sur les améliorations réalisées
- Préparer le prochain cycle d'amélioration continue



L'étape Act ferme le cycle PDCA et prépare le terrain pour un nouveau cycle, garantissant ainsi une amélioration continue.