

# Bonnes pratiques d'administration et maintien en condition opérationnelle (MCO)

---

## 2.1. Définition du MCO – Maintien en Condition Opérationnelle

Le Maintien en Condition Opérationnelle (MCO) constitue la **colonne vertébrale de l'administration informatique**. Il désigne l'ensemble des activités techniques, organisationnelles et documentaires destinées à garantir que les infrastructures du Système d'Information (SI) sont disponibles, performantes, sécurisées et conformes aux attentes des utilisateurs et aux engagements de service.

Les 3 grands piliers du MCO :

- **Surveillance** proactive des composants (réseaux, serveurs, cloud)
- **Maintenance** régulière et préventive (mises à jour, sauvegardes)
- **Support** technique de niveau 2 et 3 (résolution d'incidents complexes)

Les infrastructures informatiques modernes sont devenues **critiques pour les organisations**. Une défaillance du réseau, un serveur inaccessible, ou une application non supervisée peut impacter la production, la logistique, la comptabilité ou les services publics. L'AIS joue donc un rôle de **garant de la continuité de service**.

---

## 2.2. Normes et cadres de référence : ISO, ITIL, ANSSI

Un AIS opère dans un cadre structuré, en s'appuyant sur les **référentiels de bonnes pratiques** :

Référentiel	Description	Application pour l'AIS
ITIL (Information Technology Infrastructure Library)	Cadre de bonnes pratiques pour la gestion des services IT (ITSM)	Gestion des incidents, des problèmes, des changements, du catalogue de services
ISO/IEC 20000	Norme internationale pour la gestion des services IT	Alignement avec les processus ITIL, preuve de qualité
ANSSI	Agence nationale française de la sécurité des systèmes d'information	Recommandations pour la sécurité opérationnelle des systèmes
RGPD	Réglementation sur la protection des données personnelles	Journalisation, traçabilité, respect des durées de conservation

Le respect de ces référentiels garantit un **niveau de service optimal, sécurisé et conforme** à la réglementation française et européenne.

---

## 2.3. Processus ITIL essentiels pour le MCO

### a) Gestion des incidents

- Objectif : **restaurer un service aussi rapidement que possible**

- Exemples : perte de connectivité réseau, arrêt d'un serveur
- Outils utilisés : GLPI, OTRS, ServiceNow

#### b) Gestion des problèmes

- Objectif : **identifier la cause racine d'incidents récurrents**
- Exemples : serveur en surcharge régulière, lenteurs en VPN
- Méthodes : analyse des journaux, tests de performance

#### c) Gestion des changements

- Objectif : **planifier, valider, documenter toute évolution**
- Exemples : migration vers une nouvelle version de Windows Server, ajout de VLANs

#### d) Gestion de la configuration

- Objectif : **maintenir une base de données (CMDB) à jour**
- Inventaire des équipements, relations entre composants

#### e) Gestion de la disponibilité

- Objectif : **maximiser le temps de fonctionnement du SI**
- Utilisation d'outils de supervision, tests de bascule, redondance

## 2.4. Outils et plateformes du MCO

L'administrateur utilise plusieurs **outils opérationnels** dans sa démarche de maintien :

Outil	Fonction
<b>GLPI</b>	Gestion des incidents, base de connaissance, parc informatique
<b>Centreon / Zabbix</b>	Supervision technique des systèmes et réseaux
<b>Grafana / Prometheus</b>	Suivi des métriques temps réel, création de tableaux de bord
<b>PowerShell / Bash / Python</b>	Scripts d'automatisation
<b>Ansible / Terraform</b>	Infrastructure as Code (IaC) pour les tâches répétitives
<b>VEEAM / Veritas</b>	Sauvegarde, restauration, réplication
<b>Syslog / Wazuh</b>	Collecte de logs, détection d'événements

## 2.5. Supervision proactive et réactive

La **supervision** permet de **visualiser en temps réel l'état de santé de l'infrastructure**. Deux grandes approches coexistent :

#### Supervision proactive :

- Anticipation des incidents
- Analyse de tendances (montée de charge, erreurs disques)

- Mise en place de seuils d'alerte, escalades automatiques

#### **Supervision réactive :**

- Réception d'une alerte suite à une panne
- Intervention immédiate
- Déclenchement d'un processus de résolution

#### **Les indicateurs clés à suivre :**

- Disponibilité (uptime)
  - Temps de réponse
  - Charge CPU / RAM / disque
  - Latence réseau
  - Journaux d'erreurs
- 

## **2.6. Diagnostic structuré et résolution des incidents**

Lorsqu'un incident est signalé, l'AIS suit une **méthodologie structurée** :

1. **Identification** : Qui est concerné ? Quel est l'impact ?
  2. **Classification** : Criticité, domaine affecté, SLA concerné
  3. **Diagnostic** : Utilisation des outils de logs, supervision, historique
  4. **Action corrective** : Redémarrage, mise à jour, restauration
  5. **Vérification** : Tests de fonctionnement, confirmation utilisateur
  6. **Clôture et documentation** : Trace dans l'outil de gestion d'incident
- 

## **2.7. Planification et documentation des opérations**

Le MCO repose également sur des **opérations planifiées**, comme :

- Sauvegardes quotidiennes
- Tests de restauration mensuels
- Mise à jour des systèmes
- Vérification des certificats SSL
- Archivage des logs selon le RGPD

Chaque action doit être :

- **Documentée** (procédures écrites, guides d'exploitation)
- **Historisée** (via outil ITSM)
- **Automatisée si possible** (via scripts ou planificateurs)

La documentation est un **outil vital de pérennisation**, de formation interne, et de communication avec les équipes techniques.

---

## 2.8. Conformité et sécurité dans le MCO

Le Maintien en Condition Opérationnelle ne peut être séparé de la **sécurité informatique** :

- **PSSI** (Politique de Sécurité du Système d'Information)
- **Conformité RGPD** : accès aux données, durée de conservation
- **Gestion des vulnérabilités** : veille, patch management
- **Auditabilité** : preuves d'accès, journaux sécurisés
- **Tests PRI/PCI** : plan de reprise et de continuité

L'AIS s'assure que chaque action technique **s'aligne sur les exigences de sécurité** définies par la direction informatique et les recommandations de l'ANSSI.

---

## 2.9. Évaluation de la performance des services

L'AIS contribue à mesurer **l'efficacité du SI**, à travers des indicateurs (KPI) :

KPI	Objectif
<b>Taux de disponibilité</b>	99.9% ou plus selon les SLA
<b>MTTR</b> (Mean Time To Repair)	Réduire le temps de résolution d'incident
<b>MTBF</b> (Mean Time Between Failures)	Allonger les périodes sans panne
<b>Satisfaction utilisateur</b>	Questionnaire post-intervention

---

## 2.10. Études de cas pratiques et QCM associés

Dans le cadre de la formation GRETA, plusieurs **misés en situation** sont proposées :

- Rétablissement d'un service suite à un incident serveur
- Planification des sauvegardes automatisées
- Intégration de nouveaux équipements dans GLPI
- Supervision d'une VM Azure via Zabbix

Des **QCM de validation** viennent compléter cette section, couvrant :

- Terminologie ITIL
  - Séquences de traitement d'incident
  - Outils et bonnes pratiques MCO
-