LES NORMES ISO DE MANAGEMENT DU RISQUE

Dr SO Abdoulaye
JANVIER 2021

OBJECTIF

- Connaitre les normes ISO du management du risque

Dr SO Abdoulaye

JANVIER 2021

PLAN DU COURS

- INTRODUCTION
- NORMES GENERALES
  - ISO 31000
  - ISO Guide 73
  - ISO 9001
- NORMES SPECIFIQUES
  - Sécurité de l'information (famille ISO 27000)
  - Santé et sécurité au travail (ISO 45001)

Dr SO Abdoulaye

JANVIER 2021

INTRODUCTION (1/3)

Naissance de ISO

À Londres, en 1946, **65 délégués de 25 pays** se réunissent à Londres pour envisager l'avenir de la normalisation internationale. **En 1947, l'ISO voit officiellement le jour**

INTRODUCTION (2/3)

- L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO)
- Durant les dernières décennies, plusieurs organismes ont établi un système qualité dans le but de satisfaire leurs clients
- La multiplication des normes est un phénomène qui se généralise

INTRODUCTION (3/3)

Les normes générales du risque :

IS0 31000: **2018** Management du risque: lignes directrices

Guide ISO 73:2009, Management du risque – Vocabulaire

ISO 31010: 2009 : Gestion des risques – Techniques d'évaluation des risques

ISO 9001: 2015 Systèmes de management de la Qualité-Exigences

Les normes spécifiques relatives à la sécurité (santé) :

ISO/CEI 27001 : Système de Management de la Sécurité de l'Information (SMSI) — Exigences

ISO 45001: 2018 Systèmes de management de la santé et de la sécurité au travail -- Exigences et lignes directrices

LES NORMES GENERALES DU MR

Dr SO Abdoulaye

JANVIER 2021

ISO 31000 : 2018

Dr SO Abdoulaye
JANVIER 2021

ISO 31000 : 2018 (1/2)

Management du risque: lignes directrices

- Cette norme fournit des principes et des lignes directrices générales sur le management du risque afin d'harmoniser les processus de management du risque dans les normes existantes et à venir
- Elle offre une approche commune à l'établissement des normes traitant de risques et/ou secteurs spécifiques, sans toutefois remplacer ces normes

Dr SO Abdoulaye

JANVIER 2021

ISO 31000 : 2018 (2/2)

- Recommande que les organismes élaborent, mettent en œuvre et améliorent continuellement un cadre organisationnel dont **le but est d'intégrer le processus de management du risque aux processus de gouvernance, de stratégie et de planification, de management, de rédaction des rapports, ainsi qu'aux politiques, aux valeurs et à la culture d'ensemble de l'organisme**

Dr SO Abdoulaye

JANVIER 2021

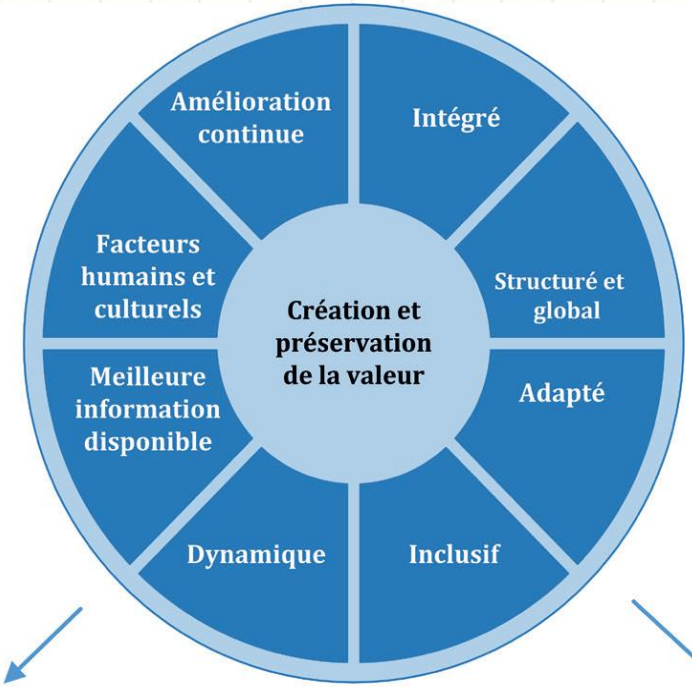
OBJECTIFS DE LA NORME

- Prendre conscience de la nécessité d'identifier et de traiter le risque à travers tout l'organisme
- Améliorer l'identification des opportunités et des menaces
- Encourager un management proactif

Dr SO Abdoulaye

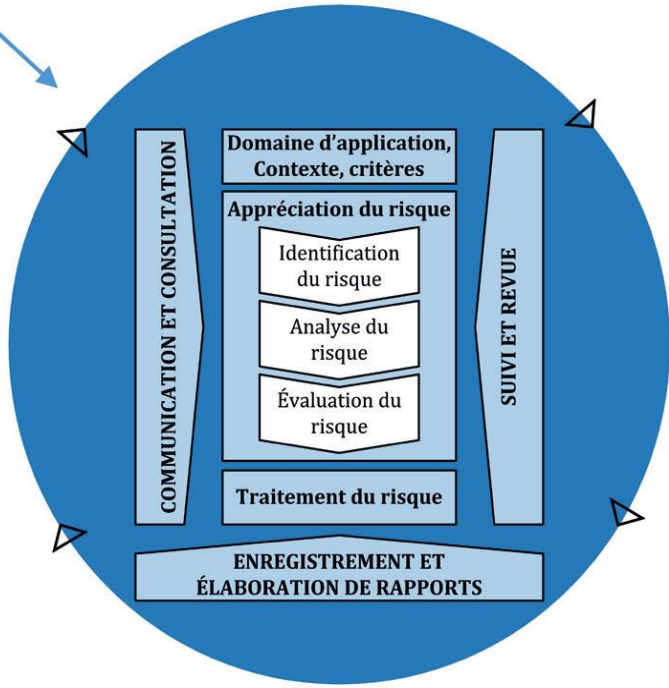
JANVIER 2021

Principes, cadre organisationnel et processus



Principes (partie 4)

Cadre organisationnel (partie 5)



Processus (partie 6)

STRUCTURE DE ISO 31000 (1/3)

1 Domaine d'application

2 Références normatives

3 Termes et définitions

4 Principes

5 Cadre organisationnel

- **Leadership et engagement**
- **Intégration (**à la stratégie d'ensemble**)**
- **Conception**
  - Compréhension de l'organisme et de son contexte

STRUCTURE DE ISO 31000 (2/3)

- Engagement en matière de management du risque
- Attribution des rôles, pouvoirs et responsabilités au sein de l'organisme
- Affectation des ressources
- Établissement d'une communication et d'une concertation

- **Mise en œuvre**
- **Évaluation**
- **Amélioration**
  - Adaptation
  - Amélioration continue

Dr SO Abdoulaye
JANVIER 2021

STRUCTURE DE ISO 31000 (3/3)

6 Processus (cf. technique du management du risque)

- **Communication et consultation**
- **Périmètre d'application, contexte et critères**
- **Définition du domaine d'application**
- **Contexte interne et externe**
- **Définition des critères de risque**
- **Appréciation du risque**
    - Identification du risque
    - Analyse du risque
    - Évaluation du risque
    - Traitement du risque
    - Sélection des options de traitement du risque
    - Élaboration et mise en œuvre des plans de traitement du risque
    - Suivi et revue
    - Enregistrement et élaboration de rapports

GUIDE ISO 73:2009

Dr SO Abdoulaye
JANVIER 2021

GUIDE ISO 73:2009

- Le Guide ISO 73:2009, Management du risque – Vocabulaire (cf. documentation)
- Cette norme complète ISO 31000 en fournissant un ensemble de termes et définitions relatifs au management du risque

Dr SO Abdoulaye

JANVIER 2021

ISO CEI 31010:2009

Dr SO Abdoulaye
JANVIER 2021

ISO CEI 31010:2009

- Gestion des risques – Techniques d'évaluation des risques
- Destinée à l'évaluation des risques
- Traite des concepts de l'évaluation des risques, des processus et de la sélection des techniques d'évaluation des risques
- Eclairage sur des risques pouvant gêner la réalisation des objectifs et leur permet d'évaluer l'adéquation et l'efficacité des contrôles déjà mis en place

ISO 9001: 2015

Dr SO Abdoulaye
JANVIER 2021

ISO 9001: 2015 (1/7)

- L'approche par les risques est l'une des grandes nouveautés de la norme ISO 9001:2015.
- La norme ISO 9001:2015 prône une approche systématique intégrale pour les risques dans le processus de la conception et de la mise en œuvre du SMQ

Dr SO Abdoulaye
JANVIER 2021

ISO 9001: 2015 (2/7)

- La norme ISO 9001:2015 fait référence aux risques 50 fois
- Les risques/opportunités sont cités conjointement 13 fois (dont 8 fois dans les chapitres des exigences)

Dr SO Abdoulaye

JANVIER 2021

ISO 9001: 2015 (3/7)

- Prise en compte des **risques et opportunités** associés au contexte et aux objectifs de l'organisme (Introduction)
- Planifier: établir les objectifs du système, ses processus ainsi que les ressources nécessaires pour fournir des résultats correspondant aux exigences des clients et aux politiques de l'organisme, et identifier et traiter **les risques et opportunités**; (3)

Dr SO Abdoulaye
JANVIER 2021

ISO 9001: 2015 (4/7)

- Pour se conformer aux exigences de la présente Norme internationale, un organisme doit **planifier et mettre en œuvre des actions face aux risques et opportunités** (3)
- La prise en compte à la fois **des risques et des opportunités** sert de base pour améliorer l'efficacité du système de management de la qualité, obtenir de meilleurs résultats et prévenir les effets négatifs
- Prendre en compte **les risques et opportunités** tels que déterminés conformément aux exigences de 6.1;

Dr SO Abdoulaye
JANVIER 2021

ISO 9001: 2015 (5/7)

- L'organisme **doit prendre en compte les risques et opportunités** lors de la détermination des processus nécessaires au système de management de la qualité. (4)
- La direction doit promouvant l'utilisation de l'approche processus et de l'approche par les risques et que **les risques et les opportunités** susceptibles d'avoir une incidence sur la conformité des produits et des services et sur l'aptitude à améliorer la satisfaction du client sont déterminés et pris en compte. (5)

Dr SO Abdoulaye

JANVIER 2021

ISO 9001: 2015 (6/7)

- l'organisme doit déterminer **les risques et opportunités** qu'il est nécessaire de prendre en compte pour donner l'assurance que l'efficacité du SMQ, accroître les effets souhaitables, prévenir ou réduire les effets indésirable et s'améliorer. (6)
- les actions à mettre en œuvre face aux **risques et opportunités** (6)
- Les actions mises en œuvre face **aux risques et opportunités** doivent être proportionnelles à l'impact potentiel sur la conformité des produits et des services (6)

Dr SO Abdoulaye
JANVIER 2021

ISO 9001 (7/7)

- l’efficacité des actions mises en œuvre face aux **risques et opportunités** (6)
- l’efficacité des actions mises en œuvre face **aux risques et opportunités** (voir 6.1) (9)
- L'organisme doit mettre à jour **les risques et opportunités** déterminés durant la planification, si nécessaire lorsqu'il s'agit de traiter les non-conformités et/ou entreprendre des actions correctives (10)

Dr SO Abdoulaye

JANVIER 2021

NORMES SPECIFIQUES

Dr SO Abdoulaye

JANVIER 2021

SECURITE DE L'INFORMATION : LA FAMILLE ISO 27000

Objectifs: protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion

- ISO/CEI 27001 : Système de Management de la Sécurité de l'Information (SMSI) — Exigences
- ISO/CEI 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information
- ISO/CEI 27003 : Système de Management de la Sécurité de l'Information (SMSI) — Guide d'implémentation
- ISO/CEI 27004 : Mesure de la gestion de la sécurité de l'information
- ISO/CEI 27005 : Gestion du risque en sécurité de l'information
- ISO/CEI 27006 : Exigences pour les organismes réalisant l'audit et la certification de Systèmes de Management de la Sécurité de l'Information (SMSI)
- ISO/CEI 27007 : Guide pour l'audit de Systèmes de Management de la Sécurité de l'Information (SMSI)

ISO 27001: 2016

- La norme ISO 27001 : 2016 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI).
- Elle définir une politique de la sécurité des informations.
- Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels.
- La norme énumère un ensemble de points de contrôles à respecter pour s'assurer de la pertinence du SMSI, pour permettre de l'exploiter et de le faire évoluer

Dr SO Abdoulaye

JANVIER 2021

SANTE ET SECURITE AU TRAVAIL

- **OHSAS 18001: 2007**
- **OHSAS 18002:2008**
- **ILO-OSH: 2001**
- **ISO 45001:2018**

Dr SO Abdoulaye

JANVIER 2021

MERCI POUR VOTRE ATTENTION

Dr SO Abdoulaye

JANVIER 2021