

Outil de compréhension du projet de norme NF EN IEC 80001-1 :

Maîtrise des risques des DM connectés et logiciels de santé

<https://doi.org/10.34746/yxb0-qp16>

*Université de Technologie de Compiègne
A21*



Utilisation de la cartographie interactive :

Sélectionner puis cliquer sur l'article pour y accéder :

5.2 Leadership et engagement



Cliquer sur la maison pour revenir au plan complet de la norme :



Cliquer sur la flèche pour revenir à la diapositive précédente :



Table des icônes



Objectifs



Acteurs



Actions



Documents



NF EN IEC 80 001-1

Articles informatifs

1. Domaine d'application

2. Références normatives

3. Termes et Définitions

4. Principes

Articles normatifs


5. Cadre

6. Analyse du risque

Annexes informatives

A.Établissement de correspondances entre le texte de l'IEC 80001-1 et le document réorganisé

B. Recommandations pour les informations dans les documents d'accompagnement



1. Domaine d'application



Ce document est destiné à aider les organisations à spécifier un cadre d'exigences et des recommandations générales sur la gestion des risques avant, pendant et après la mise en relation du système TI de santé et les infrastructures TI de santé.



Les organisations



appliquer une
gestion des risques

traiter la sécurité,
l'efficacité et la
sûreté



Menu



Retour

2. Références normatives



ISO 81001-1 ED2, Health informatics - Health Software and health IT systems safety, effectiveness and security - Part 1 : Foundational principles, concepts and terms



Menu



Retour

3. Termes et Définitions



Les termes et définitions utilisés dans ce document sont extraits de l'ISO 81001-1 ED2 ISO et IEC.



ISO

IEC



comportent et tiennent à jour des bases de données terminologiques utilisable en normalisation consultable sur :



<http://www.electropedia.org>

<http://iso.org/obp>



Conséquence (ISO 31000:2018); Soins de santé (ISO 13940:2015); Risque initial (ISO/IEC/IEEE 15026-1:2019); Vraisemblance (ISO 31000:2018); Processus (IEC 80001-1:2010); Gestionnaire des risques (IEC 80001-1:2010); Plan de gestion des risques (ISO/IEC 16085:2006)



Menu



Retour

4. Principes



Les principes créent et communiquent la valeur, l'objectif et la finalité de la gestion des risques grâce aux propriétés clés dans l'utilisation et la mise en oeuvre des systèmes TI de santé connectés.



Organisation

Organisme
responsable



Prends en compte
dans ces activités la
gestion des risques

Responsable du
processus de gestion
des risques



Menu



Retour



Article 5 : cadre

5.1 Généralités

5.2 Leadership et engagement

5.3 Intégration de la gestion des risques

5.4 Conception / Planification

5.5 Mise en oeuvre

5.6 Evaluation

5.7 Amélioration



Menu



Retour



Suivant

5.1 Généralités



Tous les intervenants et la direction prennent en compte le cadre de la gestion des risques et l'intègrent à d'autres activités et fonctions importantes.



Intervenants
et
Direction



Sont concernés par la nécessité
de cadrer la gestion des risques

Intègrent la gestion des risques à
d'autres activités importants



5.2 Leadership et engagement



La gestion des risques est assurée et évaluée tout au long du cycle de vie du système des technologies de l'information (TI) de santé.



L'organisation

La Direction



établit et adhère à un processus défini pour la gestion des risques

assure la mise en oeuvre de la gestion des risques et évalue son efficacité



Dossier de gestion des risques



Menu



Retour

5.3 Intégration de la gestion des risques



La gestion des risques concerne tous les niveaux et tous les membres d'une organisation (fabricants).



Tous les membres
de l'organisation



Intègrent la gestion des
risques à leurs activités
quotidiennes



Dossier de Gestion des
Risques



Menu



Retour

5.4 Conception / Planification



La planification et le traitement des activités de gestion des risques tout au long du cycle de vie du système TI de santé sont documentés.



Le responsable
qualité



Rédige la planification des risques qui comprend :

- un cadre d'analyse du risque
- les critères d'acceptation des risques définis
- une liste des procédures, politiques et ressources pertinentes exigées
- toute référence à des documents d'accompagnement éventuel



Dossier de
Gestion des
Risques



Menu



Retour



5.4 Conception / Planification

5.4.1 Généralités

5.4.2 Dossier de gestion des risques

5.4.3 Comprendre l'organisation et l'écosystème socio technique

5.4.4 Articulation de l'engagement en matière de gestion des risques

5.4.5 Attribution de rôles, autorités, responsabilités et imputabilités dans l'organisation

5.4.6 Allocation de ressources

5.4.7 Etablissement de la communication et de la consultation



5.4.1 Généralités



Un plan de gestion des risques adapté au domaine d'application est établi dès le début d'un projet dans le but de documenter et planifier les activités de gestion des risques tout au long du cycle de vie du système TI de santé



L'organisation



Établit un plan de gestion des risques en début de projet

Enregistre et planifie les activités de gestion des risques tout au long du cycle de vie



Plan de gestion des risques



Suivant



Menu



Retour

5.4.2 Dossier de gestion des risques



Un dossier de gestion des risques est établi dès le début d'un projet, documenté, maintenu à jour et accessible facilement tout au long du cycle de vie du système TI de santé.



L'organisation



Établit un DGR en début de projet

Maintient le DGR tout au long du cycle de vie

Assure que le DGR est récupérable en cas de défaillance



Dossier de Gestion des Risques



Menu



Retour

5.4.3 Comprendre l'organisation et l'écosystème socio technique



Tous les éléments, matériels et immatériels, actifs ou passifs, positifs et négatifs, internes et externes pouvant impacter la gestion des risques du système TI de santé doivent être identifiés pour ensuite être pris en compte et maîtrisés.



L'organisation



Établit et maintient



Une liste définie d'éléments d'actifs connectés au système TI de santé



Menu



Retour

5.4.4 Articulation de l'engagement en matière de gestion des risques



Un plan de gestion des risques est établi par la direction qui en assure le suivi et l'évaluation de son efficacité.



Direction de l'organisation



Veille à l'adhérence et à la conformité

Autorise le déploiement du système TI de santé



Plan de Gestion des Risques



Menu



Retour

5.4.5 Attribution de rôles, autorités, responsabilités et imputabilités dans l'organisation



Les rôles et responsabilités sur la gestion des risques sont attribués et communiqués par la direction à des personnels compétents. Un gestionnaire de la gestion des risques du système TI de santé est nommé dont les responsabilités sont connues de tous.



Direction de l'organisation

Gestionnaire des risques

L'organisation



Identifie le gestionnaire des risques et assure que l'ensemble des rôles et responsabilités du personnel sont définis et appliqués

Veille au respect du processus de gestion des risques

Reporte les résultats



Dossier de Gestion des Risques

Suivant



5.4.6 Allocation de ressources



Les ressources nécessaires à la maîtrise de la gestion des risques du système TI de santé sont mobilisables facilement, mobilisées en temps utile et adaptées aux besoins.



Direction de l'organisation



Fournit les ressources suffisantes

S'assure de la qualification du personnel impliqué



5.4.7 Etablissement de la communication et de la consultation



Des moyens efficaces existent pour collecter, partager et conserver les informations utiles à la gestion des risques auprès des intervenants internes ou externes.



L'organisation



Etablit des moyens de partage



Collecte d'informations chez les intervenants internes et externes



5.5 Mise en oeuvre



Le succès de la gestion des risques du système TI de santé est garanti par l'engagement des intervenants, une planification rigoureuse des actions, la mobilisation des ressources nécessaires et l'adaptation permanente aux incertitudes dans la prise de décision.



L'Organisation



Prend des décision afin de
limiter les nouvelles
incertitudes



Menu

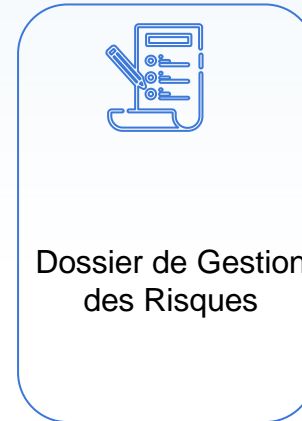
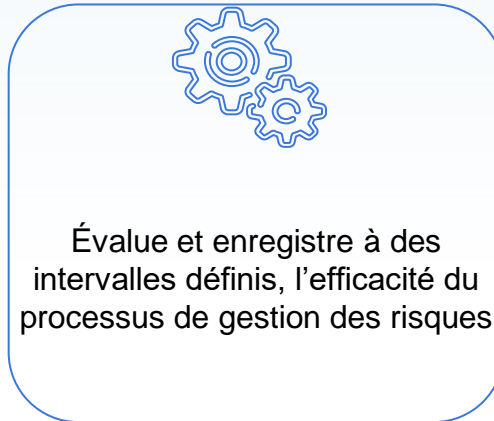
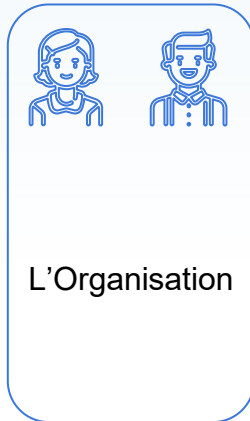


Retour

5.6 Evaluation



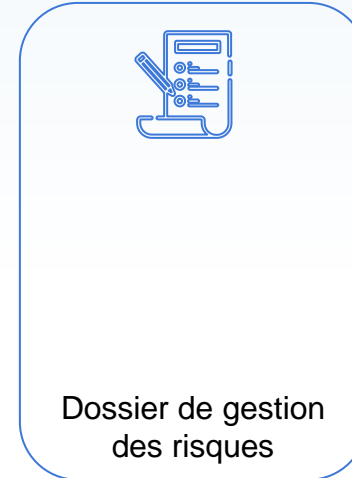
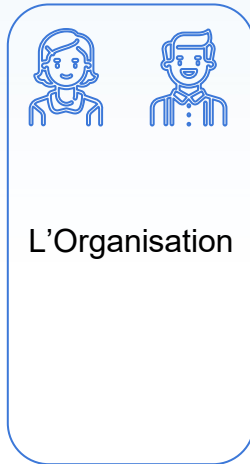
Des évaluations périodiques sur la conformité et l'efficacité de la gestion des risques sont réalisées et enregistrées dans le dossier de gestion des risques.



5.7 Amélioration



L'organisation favorise l'amélioration continue du processus de gestion des risques et enregistre toute preuve d'amélioration dans le dossier de gestion des risques.





6. Analyse du risque

6.1 Exigences générales

6.2 : Exigences spécifiques
au cours de la vie



Menu



Retour



Suivant




6.1 Exigences générales

6.1.1 Généralités

6.1.2 Analyse du risque

6.1.3 Evaluation du risque

6.1.4 Maîtrise du risque



Menu



Retour

6.1.1 Généralités



Un plan de gestion des risques cliniques est établi dès le début d'un projet, documenté, surveillé dans ses écarts et enregistré dans le dossier de gestion des risques tout au long du cycle de vie du système TI de santé. Un cas d'assurance est établi dès le début du projet



L'organisation

Les organismes responsables



Etablit et maintient

Enregistre et incorpore le Plan de Gestion des Risques dans



Plan de Gestion des Risques


Dossier de Gestion des Risques



Menu



Retour



6.1.2 Analyse du risque

6.1.2.1 Généralités

6.1.2.2 Définition de l'objet et du domaine d'application du Processus

6.1.2.3 Identification des dangers

6.1.2.4 Estimation du risque



6.1.2.1 Généralités



Une analyse de risque est réalisée sur tous les aspects du système TI en santé (architecture, technologie, fonctionnalités, usage prévu...) de manière multidisciplinaire avec l'ensemble des parties-prenantes directes ou indirectes au système.



Les représentants
compétents des différents
corps spécialisés



Définissent les risques

Analysent les risques

Évaluent les risques pour
identifier le danger



6.1.2.2 Définition de l'objet et du domaine d'application du Processus



Le milieu clinique, les utilisateurs et l'usage visé du système TI sont définis ainsi que ses critères de déploiement dans l'infrastructure existante en tenant compte, pour la gestion des risques, des préconisations des fabricants des dispositifs médicaux qui seront connectés. Ces informations sont consignées dans le cas d'assurance et intégrées dans le dossier de gestion des risques



L'Organisation



- Défini le milieu clinique et l'échelle de complexité

L'organisme responsable



- Identifie les utilisateurs, la complexité du déploiement et utilisation prévue du système TI de santé

- Incorpore les résultats d'activité



Cas d'assurance
Documents
d'accompagnements



Dossier de Gestion
des Risques



Menu



Retour



6.1.2.3 Identification des dangers



L'organisation identifie et documente de manière exhaustive et selon une méthode adaptée, les dangers connus ou prévisibles susceptibles d'apparaître tout au long du processus de soins exploitant le système TI de santé dans l'infrastructure existante. Ces informations sont consignées dans le cas d'assurance et intégrées dans le dossier de gestion des risques.



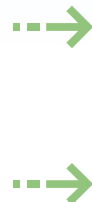
L'Organisation

L'organisme responsable



Identifie et documente les dangers

Identifie, examine et enregistre les vulnérabilités et menaces



Cas d'assurance

Dossier de gestion des risques



Menu



Retour

Suivant

6.1.2.4 Estimation du risque



Pour chaque danger identifié, un risque initial est estimé par les degrés de gravité et de vraisemblance des dommages associés à son apparition. Les estimations faites, avec les méthodes et échelles utilisées, sont consignées dans le cas d'assurance et intégrées dans le dossier de gestion des risques.



L'Organisation



- Estime la gravité de la conséquence du dommage
- Estime la vraisemblance du dommage
- Estime et enregistre le risque résultant
- Incorpore les résultats d'activités de gestion des risques
- Confronte les critères utilisés par l'organisation



Dossier de gestion des risques

L'organisme responsable



Menu



Retour

6.1.3 Evaluation du risque



L'acceptabilité de chaque risque initial est évaluée selon une combinaison de sa gravité et de sa vraisemblance. Elle est incorporée au cas d'assurance et enregistrée dans le dossier de gestion des risques.



L'Organisation



Évalue l'acceptabilité du risque initial et suit les exigences de 6.1.4 si le risque est inacceptable



Incorpore et consigne les résultats des activités de gestion des risques



Dossier de gestion des risques



Menu



Retour




6.1.4 Maîtrise du risque

6.1.4.1 Analyse de maîtrise du risque

6.1.4.2 Analyse benefice-risque

6.1.4.3 Vérification des mesures de maîtrise
du risque

6.1.4.4 Evaluation et compte-rendu du risque
résiduel



Menu



Retour

6.1.4.1 Analyse de maîtrise du risque



Des mesures de maîtrise des risques sont prises pour chaque danger tant que l'acceptabilité du risque résiduel n'est pas satisfaisante. L'apparition éventuelle de nouveaux dangers ou risques est prise en compte et lorsqu'aucune mesure de maîtrise n'est possible, une analyse bénéfico-risque est réalisée. Ces informations sont consignées dans le cas d'assurance et intégrées dans le dossier de gestion des risques.



L'Organisation



- Identifie et évalue les mesure de maîtrise du risque
- Gère tout nouveau danger ou risque accru
- Évalue le risque résiduel et identifie les mesures de maîtrise du risque
- Effectuer une analyse bénéfico risque
- Incorporer les risques



Dossier de gestion des risques



Menu



Retour

6.1.4.2 Analyse bénéfice-risque



Une analyse bénéfices-risques du système TI de santé est réalisée par les personnes ayant les compétences et les responsabilités pour assumer les décisions. Un risque résiduel jugé inacceptable après toutes les mesures possibles de maîtrise est accepté après justification et consignation dans le cas d'assurance. L'ensemble de ces activités sont incorporées dans le cas d'assurance et consignées dans le dossier de gestion ds risques.



L'organisation

L'organisme responsable



Démontre l'acceptabilité des risques résiduels pour chaque dangers

Examine le risque global de tous les dangers non acceptés

Consigne tout risque résiduel non accepté



CAS
d'assurance

Suivant



Menu



Retour

6.1.4.3 Vérification des mesures de maîtrise du risque



Chaque mesure de maîtrise des risques est mise en œuvre et son efficacité est vérifiée, incorporée dans le cas d'assurance et consignée dans le dossier de gestion des risques.



L'Organisation



Met en oeuvre les mesures de maîtrise du risque et vérifie leur efficacité

Incorpore les résultats des activités



Dossier de gestion des risques



Menu



Retour

6.1.4.4 Evaluation et compte-rendu du risque résiduel



Avant tout déploiement ou tout modification d'un système TI de santé, l'organisation prouve l'analyse de l'acceptabilité des risques résiduels ou celle des bénéfiques-risques. Cette activité est incorporée dans le cas d'assurance et consignée dans le dossier de gestion ds risques.



L'Organisation



L'organisme responsable



Examine l'acceptabilité du risque résiduel individuel pour chaque danger et du risque résiduel global

Démontrer l'utilisation d'une analyse bénéfice-risque pour les risques résiduels dépassant les seuils d'acceptabilité


Examine le cas d'assurance du fabricant de système TI de santé pour assurer que le risque résiduel a été pris en compte et que l'acceptabilité des risques résiduels est justifiée



Menu



Retour



6.2 : Exigences spécifiques au cours de la vie

6.2.1 Généralités

6.2.2 Acquisition

6.2.3 Installation, personnalisation et configuration

6.2.4 Intégration, migration de données, transition et validation

6.2.5 Mise en œuvre, optimisation du flux de travaux et formation

6.2.6 Exploitation et maintenance

6.2.7 Mise hors service



Menu



Retour



Suivant

6.2.1 Généralités



Les exigences applicables sont identifiées à chaque phase du cycle de vie du système TI de santé



L'organisation

L'organisme
responsable



Menu



Retour

6.2.2 Acquisition



Lors de l'acquisition d'un système TI de santé, l'organisme responsable(exploitants) associe les principaux acteurs pour évaluer ses bénéfices/risques. Ces activités sont incorporées au cas d'assurance et consignées dans le dossier de gestion des risques.



L'organisme responsable



- Satisfait aux exigences de 6.1.1, 6.1.2 et 6.1.2.3
- Communique le domaine d'application du système TI de santé
- Evaluation des bénéfices-risques des systèmes TI de santé avec les tous intervenants



Dossier de gestion des risques



Menu



Retour

6.2.3 Installation, personnalisation et configuration



L'organisme responsable examine les informations fournies par le fabricant pour configurer au mieux le système TI de santé dans le domaine d'application concerné. Tout défaut potentiel identifié fait l'objet d'une analyse de risque et de mesures de maîtrise. Ces activités sont incorporées au cas d'assurance et consignées dans le dossier de gestion des risques.



L'organisme responsable



- Satisfait aux exigences de 6.1.1, 6.1.2 et 6.1.2.3
- Examine le rapport du CAS d'assurance
- Effectue une gestion des risques et l'incorpore



Dossier de gestion des risques



Menu



Retour

6.2.4 Intégration, migration de données, transition et validation



Pour minimiser les risques liés aux soins lors de de l'intégration du système TI de santé, l'organisme responsable dispose d'un plan global permettant d'identifier toutes les activités à mener et tous les intervenants qu'il est nécessaire d'impliquer. Ces activités sont incorporées au cas d'assurance et consignées dans le dossier de gestion des risques.



L'organisme responsable



- Satisfait aux exigences de 6.1.1, 6.1.2 et 6.1.2.3
- Gère l'intégration du système TI de santé
- incorporer les résultats



Dossier de gestion des risques



Menu



Retour

6.2.5 Mise en œuvre , optimisation du flux de travaux et formation



En préalable au déploiement du système TI de santé, l'organisme responsable examine formellement le respect et l'efficacité des exigences du plan de gestion des risques et confirme que la direction les a compris et acceptés, y compris sur les transformations possibles des activités et de formation personnel. Ces activités sont incorporées au cas d'assurance et consignées dans le dossier de gestion des risques.



L'organisme responsable



- Satisfait aux exigences de 6.1
- Confirme que le plan d'action de gestion des risques a été mis en œuvre et que les utilisateurs ont été consignés
- Effectue un examen formel du Système TI de santé avant son déploiement
- Confirme que la direction comprend et accepte le profil de risque du déploiement
- Consigne les résultats des activités de gestion des risques



Dossier de gestion des risques



Menu



Retour



6.2.6 Exploitation et maintenance



Pendant la durée de vie du système TI de santé et à l'occasion de ses modifications, un processus proactif continu évalue son efficacité et permet la maîtrise des incidents selon le plan de gestion des risques. Un registre des incidents et de leur résolution est établi et mis à jour. Ces activités sont incorporées au cas d'assurance et consignées dans le dossier de gestion des risques.



L'Organisation



- Satisfait aux exigences de 6.1. 2, 6.2.3 et 6.2.4
- Démontre le suivi et la gestion efficace des risques
- Apporte des modifications pour garder un niveau de risque acceptable
- Établi et examine un processus de gestion des incidents
- Évalue l'impact de tout incident sur la validité en cours du CAS d'assurance
- Prend des mesures correctives appropriées conformément au PGR lorsque l' incident porte atteinte au CAS d'assurance
- Tient un registre des incidents, y compris de leur résolution
- **Incorpore les résultats des activités de gestion des risques**



Registre des incidents



Menu



Retour

6.2.7 Mise hors service



En cas de mise hors service d'un système TI de santé et son changement par un nouveau système, l'organisme responsable veille à ce que la migration des données entre ces deux systèmes soit sans danger, ne perturbe pas les processus de soins et réponde aux exigences du plan de gestion des risques. Ces activités sont incorporées au cas d'assurance et consignées dans le dossier de gestion des risques.



L'organisme responsable



- Satisfait aux exigences de 6.1.2, 6.1
- Applique son processus de gestion des risques pour prendre en charge le déploiement de tout autre système TI de santé ultérieur
- Examine l'impact de la suppression des fonctionnalités du système TI de santé
- Prend en compte dans la gestion des risques l'impact de la suppression
- Conserve et récupère des informations médicales après mise hors service



Dossier de gestion des risques




Menu



Retour

A.Établissement de correspondances entre le texte de l'IEC 80001-1 et le document réorganisé



Cette annexe est un résumé des exigences de la norme. Un tableau répertorie l'ensemble des éléments articles par articles afin de faciliter la lisibilité des tâches que les acteurs (organisation, organisation responsable, direction de l'organisation, etc) doivent entreprendre pour prétendre à la certification de cette norme.




Menu



Retour

B. Recommandations pour les informations dans les documents d'accompagnement



La présente annexe est fournie à titre de document d'orientation aux organisations souhaitant collecter des informations système auprès de leurs fabricants de dispositifs médicaux. Les sections et le contenu peuvent être revus ou supprimés à la discrétion de l'organisation ou des fabricants de dispositifs médicaux.



Menu



Retour