NORME INTERNATIONALE

ISO 19650-5

Première édition
2020-06

Organisation et numérisation des informations relatives aux bâtiments et ouvrages de génie civil, y compris modélisation des informations de la construction (BIM) — Gestion de l'information par la modélisation des informations de la construction —

Partie 5: Approche de la gestion de l'information axée sur la sécurité

Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling —

Part 5: Security-minded approach to information management

Numéro de référence
ISO 19650-5:2020(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 59, *Bâtiments et ouvrages de génie civil*, sous-comité SC 13, *Organisation et numérisation des informations relatives aux bâtiments et ouvrages de génie civil, y compris modélisation des informations de la construction (BIM),* en collaboration avec le Comité technique CEN/TC 442, *Modélisation des informations de la construction (BIM)*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Une liste de toutes les parties de la série ISO 19650 se trouve sur le site web de l'ISO.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

L'environnement bâti connaît une période d'évolution rapide. On s'attend à ce que l'adoption de la modélisation des informations de la construction (BIM) et l'utilisation croissante des technologies numériques dans la conception, la construction, la fabrication, l'exploitation et la gestion des actifs ou des produits, ainsi que la prestation de services, dans l'environnement bâti aient un effet transformateur pour les parties concernées. Il est probable que pour accroître l'efficacité et l'efficience, les initiatives ou les projets qui développent de nouveaux actifs ou de nouvelles solutions, ou qui modifient ou gèrent des actifs ou des solutions existants, doivent devenir plus collaboratifs. Une telle collaboration exige des méthodes de travail plus transparentes et ouvertes et, dans la mesure du possible, le partage et l'utilisation appropriés d'informations numériques.

L'environnement bâti numérique et physique combiné devra permettre d'atteindre les objectifs futurs en matière de fiscalité, de finances, de fonctionnalité, de contribution au développement durable et de croissance. Cela aura un impact sur les processus d'approvisionnement, de réalisation et d'exploitation, y compris une collaboration interdisciplinaire et sectorielle beaucoup plus étroite. Et cela augmentera également le recours aux outils numériques ainsi que la disponibilité de l'information. L'utilisation des technologies informatiques soutient déjà de nouvelles méthodes de travail, telles que le développement de la fabrication en usine hors site et de l'automatisation sur site. Les systèmes cyber-physiques sophistiqués, en utilisant des capteurs (l'élément cybernétique ou de calcul) pour contrôler ou influencer les parties physiques du système, sont capables de travailler en temps réel pour influer sur les résultats dans le monde réel. On s'attend à ce que de tels systèmes soient utilisés pour obtenir des avantages tels qu'une augmentation de l'efficacité énergétique et une meilleure gestion du cycle de vie des actifs en recueillant des informations en temps réel sur leur utilisation et leur état. Ils sont déjà mis en œuvre dans les transports, les services publics, l'infrastructure, les bâtiments, la fabrication, les soins de santé et la défense, et lorsqu'ils sont capables d'interagir comme des environnements cyber-physiques intégrés, ils peuvent être utilisés dans le développement de collectivités intelligentes.

En raison de cette utilisation croissante des technologies de l'information et de la communication et de la dépendance croissante à leur égard, il est nécessaire d'aborder les questions inhérentes de vulnérabilité et donc leurs répercussions sur la sécurité, que ce soit pour les environnements bâtis, les actifs, les produits, les services, les personnes ou les collectivités, ainsi que pour toute information connexe.

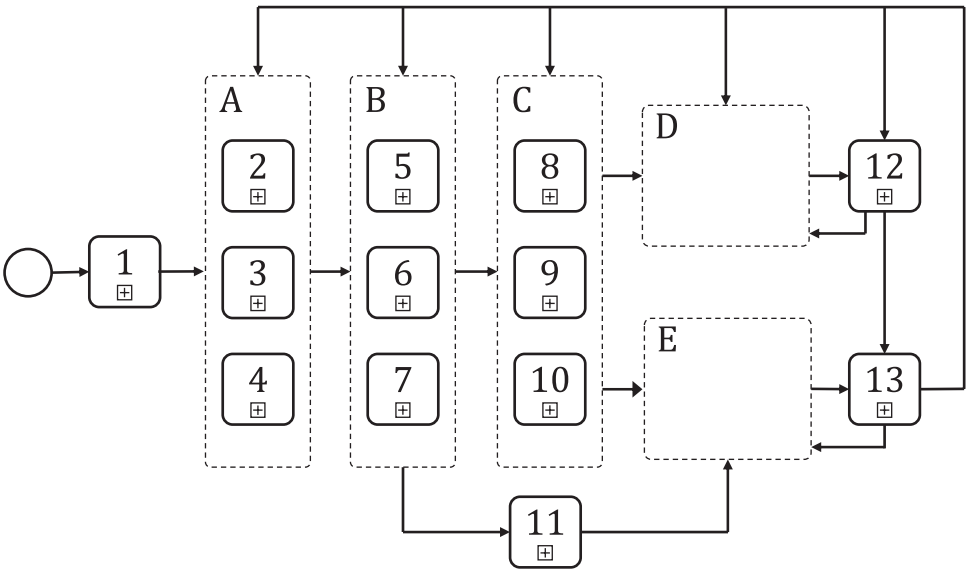
Le présent document fournit un cadre pour aider les organismes à comprendre les questions essentielles de vulnérabilité et la nature des contrôles requis pour gérer les risques pour la sécurité qui en résultent à un niveau tolérable pour les parties concernées. Son but n'est nullement de miner la collaboration ou les avantages que la BIM, d'autres méthodes de travail collaboratif et les technologies numériques peuvent générer.

Le terme « organisme » englobe non seulement les parties désignantes et les parties désignées, comme défini dans l'ISO 19650-1, mais aussi les organismes du côté de la demande qui ne sont pas directement impliqués dans une désignation.

Bien que les exigences en matière de sécurité de l'information pour un organisme, un département d'organisme ou un système individuels soient spécifiées dans l'ISO/IEC 27001, elles ne peuvent pas être appliquées de manière homogène à plusieurs organismes. La BIM et d'autres méthodes de travail collaboratif et technologies numériques impliquent généralement le partage d'informations entre plusieurs organismes indépendants dans le secteur de l'environnement bâti. Par conséquent, le présent document encourage l'adoption d'une approche par les risques, axée sur la sécurité, pouvant être appliquée aussi bien à l'ensemble des organismes qu'au sein de chaque organisme. Le caractère approprié et proportionné de l'approche présente également l'avantage que les mesures n'empêchent pas les petites et moyennes entreprises de participer à l'équipe de production.

L'approche axée sur la sécurité peut être appliquée pendant tout le cycle de vie d'une initiative, d'un projet, d'un actif, d'un produit ou d'un service, qu'il soit planifié ou existant, au cours duquel des informations sensibles sont obtenues, créées, traitées et/ou stockées.

La Figure 1 illustre l'intégration de cette approche axée sur la sécurité à d'autres stratégies, politiques, plans et exigences d'information de l'organisme pour la réalisation numérique des projets et pour la maintenance et l'exploitation numériques des actifs à l'aide de la BIM.



Légende

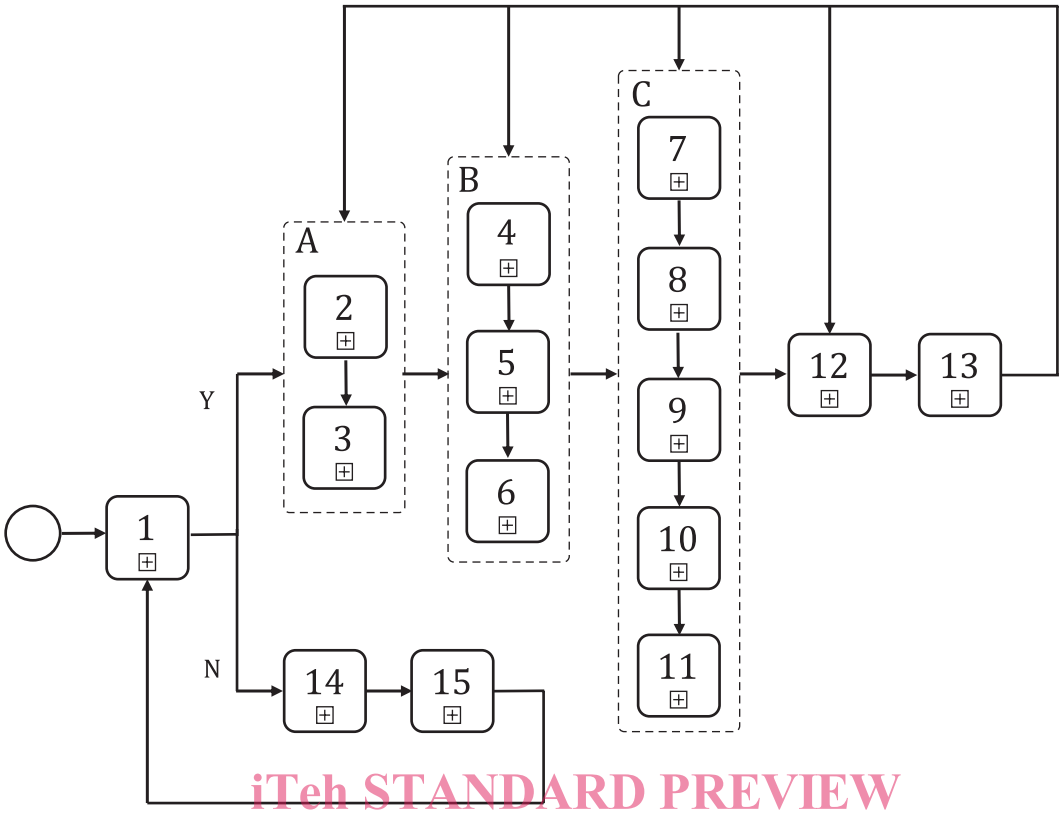
A stratégies et politiques coordonnées et cohérentes
B plans coordonnés et cohérents
C exigences d'information coordonnées et cohérentes
D activités entreprises pendant la phase d'exploitation des actifs
E activités entreprises pendant la phase de réalisation des actifs (voir également l'ISO 19650-2)
1 plans et objectifs de l'organisme
2 plan stratégique/politique de gestion d'actifs (voir l'ISO 55000)
3 stratégie de sécurité
4 autres stratégies et politique de l'organisme
5 plan de gestion d'actifs (voir l'ISO 55000)
6 plan de gestion de la sécurité
7 autres plans de l'organisme
8 exigences d'information d'actif (AIR)
9 exigences d'information de sécurité (faisant partie du plan de gestion de la sécurité)
10 exigences d'information de l'organisme (OIR)
11 analyse stratégique de rentabilité et programme stratégique
12 utilisation opérationnelle d'actif
13 mesurage des performances et actions d'amélioration

NOTE L'énumération en A, B et C n'implique aucun ordre.

Figure 1 — Intégration de l'approche axée sur la sécurité dans le processus plus large de BIM

NOTE Se référer à l'ISO 19650-1 pour les concepts et principes, y compris les OIR et AIR, afin de mieux comprendre l'importance de la sécurité dans le cadre de la série ISO 19650.

Le processus permettant de décider de la nécessité et, le cas échéant, de la mise en œuvre d'une approche axée sur la sécurité en matière de gestion de l'information est résumé à la Figure 2.



Légende

A initier une approche axée sur la sécurité

B élaborer une stratégie de sécurité

C élaborer un plan de gestion de la sécurité

O oui

N non

1 à l'aide du processus de tri en matière de sécurité, déterminer si une approche axée sur la sécurité est requise

2 établir des dispositions relatives à la gouvernance, aux obligations et à la responsabilité de l'approche axée sur la sécurité

3 commencer l'élaboration de l'approche axée sur la sécurité

4 évaluer les risques pour la sécurité

5 élaborer des mesures de réduction des risques pour la sécurité

6 documenter les risques tolérés pour la sécurité

7 élaborer des politiques et des processus pour mettre en œuvre les mesures de réduction des risques pour la sécurité

8 élaborer des exigences d'information de sécurité

9 élaborer des exigences relatives à la fourniture d'informations à des tierces parties

10 élaborer des exigences de sécurité logistique

11 élaborer un plan de gestion des manquements à la sûreté/incidents de sécurité

12 travailler avec des parties désignées dans le cadre de contrats formels ou non pour intégrer l'approche axée sur la sécurité,

y compris l'élaboration d'accords de partage d'informations si nécessaire

13 surveiller, vérifier et examiner

14 protéger toutes les informations commerciales et personnelles sensibles (aucune autre approche axée sur la sécurité requise)

15 examiner si des changements dans l'initiative, le projet, l'actif, le produit ou le service peuvent avoir une incidence sur sa sensibilité

Figure 2 — Processus de mise en œuvre de l'approche axée sur la sécurité exposée dans le présent document

La mise en œuvre des mesures décrites dans le présent document contribuera à réduire le risque de perte, de mauvaise utilisation ou de modification d'informations sensibles qui peuvent avoir une incidence sur la sécurité des personnes, la sécurité et la résilience des actifs, des produits, de l'environnement bâti ou des services fournis par ceux-ci. Elle contribuera également à la protection contre la perte, le vol ou la divulgation d'informations commerciales, d'informations personnelles et de propriété intellectuelle. Tout incident de ce type peut nuire considérablement à la réputation, ce qui se traduit par des opportunités manquées et le détournement de ressources pour mener des enquêtes, trouver des solutions et mener des activités médiatiques, en plus de perturber les activités opérationnelles quotidiennes et d'en retarder l'exécution. De plus, lorsque des incidents se produisent et que des informations ont été rendues publiques, il est pratiquement impossible de récupérer la totalité de ces informations ou d'empêcher la poursuite de leur diffusion.

Organisation et numérisation des informations relatives aux bâtiments et ouvrages de génie civil, y compris modélisation des informations de la construction (BIM) — Gestion de l'information par la modélisation des informations de la construction —

Partie 5: Approche de la gestion de l'information axée sur la sécurité

1 Domaine d'application

Le présent document spécifie les principes et les exigences relatifs à la gestion de l'information axée sur la sécurité à un stade de maturité décrit comme la « modélisation des informations de la construction (BIM) selon la série ISO 19650 », et comme défini dans l'ISO 19650-1, ainsi qu'à la gestion axée sur la sécurité des informations sensibles qui sont obtenues, créées, traitées et stockées dans le cadre de tout autre initiative, projet, actif, produit ou service, ou en relation avec ceux-ci.

Il traite des étapes requises pour créer et développer une culture et un état d'esprit de sécurité appropriés et proportionnés au sein des organismes ayant accès à des informations sensibles, y compris la nécessité de surveiller et de vérifier la conformité.

L'approche décrite est applicable pendant tout le cycle de vie d'une initiative, d'un projet, d'un actif, d'un produit ou d'un service, qu'il soit planifié ou existant, au cours duquel des informations sensibles sont obtenues, créées, traitées et/ou stockées.

Le présent document est destiné à être utilisé par tout organisme concerné par l'utilisation de technologies et de la gestion de l'information dans la création, la conception, la construction, la fabrication, l'exploitation, la gestion, la modification, l'amélioration, la démolition et/ou le recyclage d'actifs ou de produits, ainsi que la prestation de services, dans l'environnement bâti. Il sera également intéressant et pertinent pour les organismes qui souhaitent protéger leurs informations commerciales, leurs informations personnelles et leur propriété intellectuelle.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 19650-2, *Organisation et numérisation des informations relatives aux bâtiments et ouvrages de génie civil, y compris modélisation des informations de la construction (BIM) — Gestion de l'information par la modélisation des informations de la construction — Partie 2: Phase de réalisation des actifs*

ISO 19650-3,[1)] *Organisation et numérisation des informations relatives aux bâtiments et ouvrages de génie civil, y compris modélisation des informations de la construction (BIM) — Gestion de l'information par la modélisation des informations de la construction — Partie 3 : Phase d'exploitation des actifs*

1) En préparation. Stade au moment de la publication : ISO/FDIS 19650-3:2020.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

3.1
actif
item, chose ou entité qui a une valeur potentielle ou réelle pour un organisme

Note 1 à l'article: à l'article : Un actif peut être immobilisé, mobile or mobilier. Il peut s'agir d'un élément individuel d'une installation, d'un véhicule, d'un système d'équipements connectés, d'un espace dans une structure, d'un terrain, d'une infrastructure complète, d'un bâtiment entier ou d'un portefeuille d'actifs, y compris les terrains ou les eaux associés. Il peut également s'agir d'informations sous forme numérique ou imprimée.

Note 2 à l'article: à l'article : La valeur d'un actif peut varier tout au long de sa vie et un actif peut encore avoir de la valeur en fin de vie. La valeur peut être matérielle, immatérielle, financière ou non financière.

[SOURCE: : ISO 55000:2014, 3.2.1, modifiée — Les Notes 1, 2 et 3 originales de l'article ont été supprimées ; de nouvelles Notes 1 et 2 ont été ajoutées.]

3.2
lieu très fréquenté
emplacement ou environnement accessible au public qui peut être considéré comme étant plus exposé au risque d'attaque terroriste en raison de la densité de la foule ou de la nature du site

Note 1 à l'article: à l'article : Les lieux très fréquentés peuvent comprendre les stades, les arènes, les festivals et les salles de concert ; les hôtels et les restaurants ; les pubs, les clubs, les bars et les casinos ; les rues commerçantes, les galeries marchandes et les marchés ; les attractions touristiques ; les cinémas et les théâtres ; les écoles et les universités ; les hôpitaux et les lieux de culte ; les centres commerciaux et les centres de transport. Ils peuvent également inclure des espaces événementiels et des espaces publics tels que les parcs et les places.

Note 2 à l'article: à l'article : Un lieu très fréquenté ne sera pas nécessairement bondé en permanence — la densité de la foule peut varier et être temporaire, comme dans le cas d'événements sportifs ou de festivals en plein air.

3.3
métadonnées
données concernant des données

3.4
besoin de savoir
exigence légitime d'un destinataire potentiel d'informations de connaître, d'accéder ou de posséder une *information sensible* (3.11)

3.5
goût du risque
importance et type de risque qu'un organisme est prêt à saisir ou à préserver

[SOURCE: : ISO 22300:2018, 3.202]

3.6
sécurité
état d'absence relative de *menace* (3.13) ou de préjudice causé par des actes ou des événements aléatoires et non intentionnels

3.7
sûreté
état d'absence relative de *menace* (3.13) ou de préjudice causé par des actes délibérés, indésirables, hostiles ou malveillants

3.8
manquement à la sûreté
infraction ou violation de la *sécurité* (3.7)

[SOURCE: : ISO 14298:2013, 3.30]

3.9
incident de sécurité
acte suspect ou circonstance menaçant la *sécurité* (3.7)

3.10
axée sur la sécurité
compréhension et application systématique de mesures de *sécurité* (3.7) appropriées et proportionnées dans toute situation commerciale afin de décourager et/ou de perturber les comportements ou activités hostiles, malveillants, frauduleux et criminels

3.11
information sensible
information dont la perte, la mauvaise utilisation, la modification ou l'accès non autorisé peut :

— porter atteinte à la vie privée, à la *sûreté* (3.7) ou à la *sécurité* (3.6) d'une ou de plusieurs personnes ;

— compromettre la propriété intellectuelle ou les secrets commerciaux d'un organisme ;

— causer un préjudice commercial ou économique à un organisme ou à un pays ; et/ou

— menacer la sûreté, les affaires intérieures et les affaires étrangères d'une nation

3.12
risque résiduel
risque qui subsiste après la mise en œuvre des mesures de contrôle

[SOURCE: : ISO 16530-1:2017, 3.52]

3.13
menace
cause potentielle d'un incident pouvant entraîner un préjudice

3.14
direction
personne ou groupe de personnes qui oriente et dirige un organisme au plus haut niveau

Note 1 à l'article: à l'article : La direction a le pouvoir de déléguer son autorité et de fournir des ressources au sein de l'organisme.

Note 2 à l'article: à l'article : Dans le cadre du présent document, il convient de considérer la direction comme la fonction et non comme l'activité.

[SOURCE: : ISO 9000:2015, 3.1.1, modifiée — Les Notes 2 et 3 originales de l'article ont été supprimées ; une nouvelle Note 2 a été ajoutée.]

3.15
vulnérabilité
faiblesse qui peut être exploitée pour causer un préjudice