INTERNATIONAL STANDARD

ISO 19650-5

First edition
2020-06

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

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

Reference number
ISO 19650-5:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Establishing the need for a security-minded approach using a sensitivity assessment process **3**
4.1 Undertaking a sensitivity assessment process 3
4.2 Understanding the range of security risks 4
4.3 Identifying organizational sensitivities 4
4.4 Establishing any third-party sensitivities 5
4.5 Recording the outcome of the sensitivity assessment 5
4.6 Reviewing the sensitivity assessment 5
4.7 Determining whether a security-minded approach is required 5
4.8 Recording the outcome of the application of the security triage process 6
4.9 Security-minded approach required 7
4.10 No security-minded approach required 7

5 Initiating the security-minded approach **7**
5.1 Establishing governance, accountability and responsibility for the security-minded approach 7
5.2 Commencing the development of the security-minded approach 8

6 Developing a security strategy **9**
6.1 General 9
6.2 Assessing the security risks 9
6.3 Developing security risk mitigation measures 10
6.4 Documenting residual and tolerated security risks 10
6.5 Review of the security strategy 11

7 Developing a security management plan **11**
7.1 General 11
7.2 Provision of information to third parties 12
7.3 Logistical security 12
7.4 Managing accountability and responsibility for security 13
7.5 Monitoring and auditing 13
7.6 Review of the security management plan 13

8 Developing a security breach/incident management plan **14**
8.1 General 14
8.2 Discovery of a security breach or incident 14
8.3 Containment and recovery 15
8.4 Review following a security breach or incident 15

9 Working with appointed parties **15**
9.1 Working outside formal appointments 15
9.2 Measures contained in appointment documentation 16
9.3 Post appointment award 17
9.4 End of appointment 17

Annex A (informative) **Information on the security context** **18**

Annex B (informative) **Information on types of personnel, physical, and technical security controls and management of information security** **20**

Annex C (informative) **Assessments relating to the provision of information to third parties** **24**

Annex D (informative) **Information sharing agreements** **26**

Bibliography **28**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 59, *Buildings and civil engineering works*, Subcommittee SC 13, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM)*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 442 *Building Information Modelling (BIM)*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

A list of all parts in the ISO 19650 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The built environment is experiencing a period of rapid evolution. It is anticipated that the adoption of building information modelling (BIM) and the increasing use of digital technologies in the design, construction, manufacture, operation and management of assets or products, as well as the provision of services, within the built environment will have a transformative effect on the parties involved. It is likely that to increase effectiveness and efficiency, initiatives or projects that are developing new assets or solutions, or modifying or managing existing ones, must become more collaborative in nature. Such collaboration requires more transparent, open ways of working, and, as much as possible, the appropriate sharing and use of digital information.

The combined physical and digital built environment will need to deliver future fiscal, financial, functional, sustainability and growth objectives. This will have an impact on procurement, delivery and operational processes, including greater cross-discipline and sector collaboration. It will also lead to an increased use of digital tools and availability of information. The use of computer-based technologies is already supporting new ways of working, such as the development of off-site, factory-based fabrication and on-site automation. Sophisticated cyber-physical systems, by using sensors (the cyber or computation element) to control or influence physical parts of the system, are able to work in real-time to influence outcomes in the real world. It is anticipated that such systems will be used to achieve benefits such as increases in energy efficiency and better asset lifecycle management by capturing real-time information about asset use and condition. They can already be found in transportation, utilities, infrastructure, buildings, manufacturing, health care and defence, and when able to interact as integrated cyber-physical environments, can be used in the development of smart communities.

As a consequence of this increasing use of, and dependence on, information and communications technologies, there is a need to address inherent vulnerability issues, and therefore the security implications that arise, whether for built environments, assets, products, services, individuals or communities, as well as any associated information.

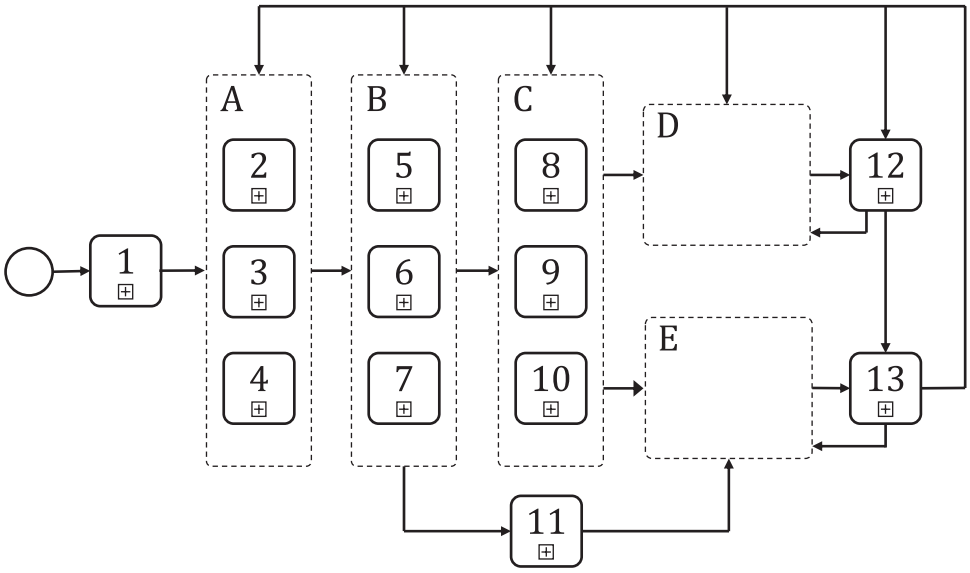
This document provides a framework to assist organizations in understanding the key vulnerability issues and the nature of the controls required to manage the resultant security risks to a level that is tolerable to the relevant parties. Its purpose is not in any way to undermine collaboration or the benefits that BIM, other collaborative work methods and digital technologies can generate.

The term organization captures not only appointing parties and appointed parties, as defined in ISO 19650-1, but also demand-side organizations who are not directly involved in an appointment.

Information security requirements for an individual organization, organizational department or system are set out in ISO/IEC 27001 but cannot be applied across multiple organizations. BIM and other digital collaborative work methods and technologies generally involve the collaborative sharing of information across a broad range of independent organizations within the built environment sector. Therefore, this document encourages the adoption of a security-minded, risk-based approach that can be applied across, as well as within, organizations. The appropriate and proportionate nature of the approach also has the benefit that measures should not prohibit the involvement of small and medium-sized enterprises in the delivery team.

The security-minded approach can be applied throughout the lifecycle of an initiative, project, asset, product or service, whether planned or existing, where sensitive information is obtained, created, processed and/or stored.

Figure 1 shows the integration of this security-minded approach with other organizational strategies, policies, plans and information requirements for the digitally-enabled delivery of projects, and the maintenance and operation of assets, using BIM.



Key

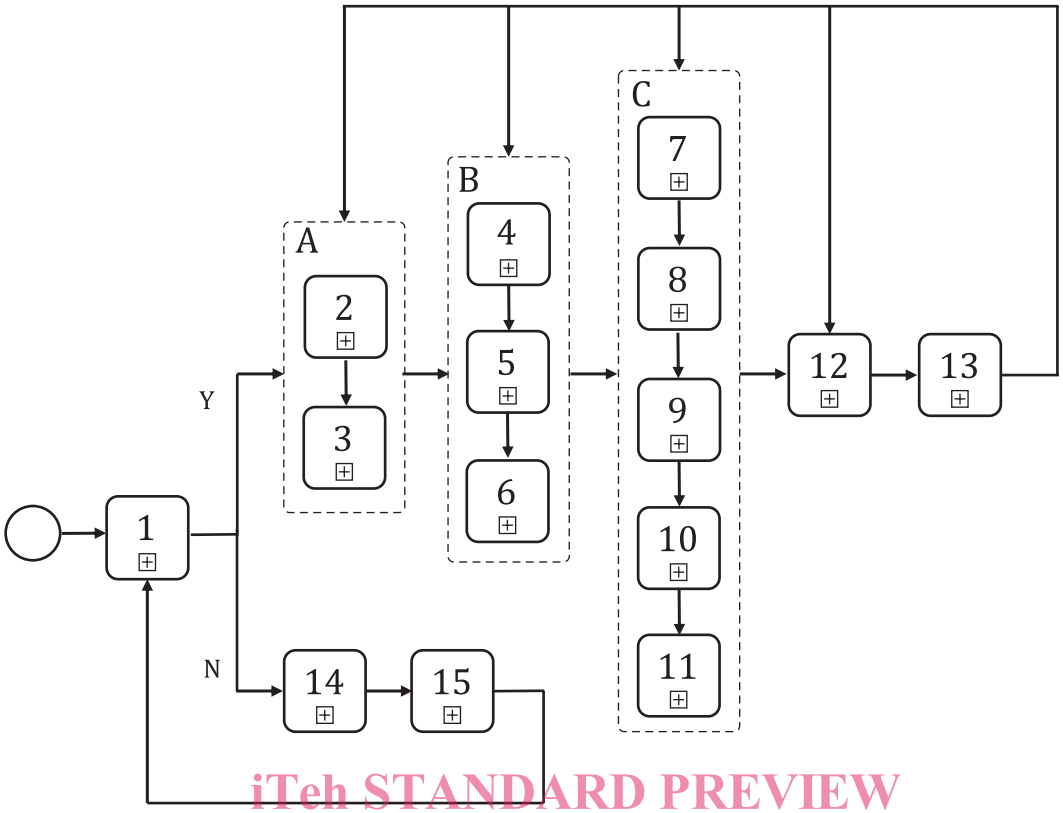
A coordinated and consistent strategies and policies
B coordinated and consistent plans
C coordinated and consistent information requirements
D activities undertaken during the operational phase of assets
E activities undertaken during the delivery phase of the asset (see also ISO 19650-2)
1 organizational plans and objectives
2 strategic asset management plan/policy (see ISO 55000)
3 security strategy
4 other organizational strategies and policy
5 asset management plan (see ISO 55000)
6 security management plan
7 other organizational plans
8 asset information requirements (AIR)
9 security information requirements (which form part of the security management plan)
10 organizational information requirements (OIR)
11 strategic business case and strategic brief
12 asset operational use
13 performance measurement and improvement actions

NOTE No order is implied by the numbering in A, B and C.

Figure 1 — The integration of the security-minded approach within the wider BIM process

NOTE Refer to ISO 19650-1 for concepts and principles including OIR and AIR to assist further understanding of security-mindedness within the context of the ISO 19650 series.

The process for deciding on the need for and, where appropriate, implementing a security-minded approach in relation information management is summarised in Figure 2.



Key

A initiate a security-minded approach
B develop a security strategy
C develop a security management plan
Y yes
N no
1 determine, using the security triage process whether a security-minded approach is required
2 establish governance, accountability and responsibility arrangements for the security-minded approach
3 commence development of the security-minded approach
4 assess the security risks
5 develop security mitigation measures
6 document tolerated security risks
7 develop policies and processes to implement the security mitigation measures
8 develop security information requirements
9 develop requirements relating to provision of information to third parties
10 develop logistical security requirements
11 develop a security breach/incident management plan
12 work with appointed parties in and out of formal contracts to embed the security-minded approach, including the development of information sharing agreements where necessary
13 monitor, audit and review
14 protect any sensitive commercial and personal information (no other security-minded approach required)
15 review if there is change in the initiative, project, asset, product or service which may impact on its sensitivity

Figure 2 — The process for implementing the security-minded approach set out in this document

Implementation of the measures outlined in this document will assist in reducing the risk of the loss, misuse or modification of sensitive information that can impact on the safety, security and resilience of assets, products, the built environment, or the services provided by, from or through them. It will also assist in protecting against the loss, theft or disclosure of commercial information, personal information and intellectual property. Any such incidents can lead to significant reputational damage, impacting through lost opportunities and the diversion of resources to handle investigation, resolution and media activities, in addition to the disruption of, and delay to, day-to-day operational activities. Further, where incidents do occur and information has been made publicly available, it is virtually impossible to recover all of that information or to prevent ongoing distribution.

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

1 Scope

This document specifies the principles and requirements for security-minded information management at a stage of maturity described as "building information modelling (BIM) according to the ISO 19650 series", and as defined in ISO 19650-1, as well as the security-minded management of sensitive information that is obtained, created, processed and stored as part of, or in relation to, any other initiative, project, asset, product or service.

It addresses the steps required to create and cultivate an appropriate and proportionate security mindset and culture across organizations with access to sensitive information, including the need to monitor and audit compliance.

The approach outlined is applicable throughout the lifecycle of an initiative, project, asset, product or service, whether planned or existing, where sensitive information is obtained, created, processed and/or stored.

This document is intended for use by any organization involved in the use of information management and technologies in the creation, design, construction, manufacture, operation, management, modification, improvement, demolition and/or recycling of assets or products, as well as the provision of services, within the built environment. It will also be of interest and relevance to those organizations wishing to protect their commercial information, personal information and intellectual property.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 19650-2, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 2: Delivery phase of the assets*

ISO 19650-3[1)], *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 3: Operational phase of assets*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

1) Under preparation. Stage at the time of publication: ISO/FDIS 19650-3:2020.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
asset
item, thing or entity that has potential or actual value to an organization

Note 1 to entry: An asset can be fixed, mobile or movable. It can be an individual item of plant, a vehicle, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets including associated land or water. It can also comprise information in digital or in printed form.

Note 2 to entry: The value of an asset can vary throughout its life and an asset can still have value at the end of its life. Value can be tangible, intangible, financial or non-financial.

[SOURCE: ISO 55000:2014, 3.2.1, modified — The original notes 1, 2 and 3 to entry have been removed; new notes 1 and 2 to entry have been added.]

3.2
crowded place
location or environment to which members of the public have access that can be considered more at risk from a terrorist attack by virtue of its crowd density or the nature of the site

Note 1 to entry: Crowded places can include: sports stadia, arenas, festivals and music venues; hotels and restaurants; pubs, clubs, bars and casinos; high streets, shopping centres and markets; visitor attractions; cinemas and theatres; schools and universities; hospitals and places of worship; commercial centres; and transport hubs. They can also include events and public realm spaces such as parks and squares.

Note 2 to entry: A crowded place will not necessarily be crowded at all times — crowd densities can vary and can be temporary, as in the case of sporting events or open-air festivals.

3.3
metadata
data about data

3.4
need-to-know
legitimate requirement of a prospective recipient of information to know, to access, or to possess *sensitive information* (3.11)

3.5
risk appetite
amount and type of risk that an organization is willing to pursue or retain

[SOURCE: ISO 22300:2018, 3.202]

3.6
safety
state of relative freedom from *threat* (3.13) or harm caused by random, unintentional acts or events

3.7
security
state of relative freedom from *threat* (3.13) or harm caused by deliberate, unwanted, hostile or malicious acts

3.8
security breach
infraction or violation of *security* (3.7)

[SOURCE: ISO 14298:2013, 3.30]

3.9
security incident
suspicious act or circumstance threatening *security* (3.7)

3.10
security-minded
understanding and routinely applying appropriate and proportionate *security* (3.7) measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities

3.11
sensitive information
information, the loss, misuse or modification of which, or unauthorized access to, can:

— adversely affect the privacy, *security* (3.7) or *safety* (3.6) of an individual or individuals;

— compromise intellectual property or trade secrets of an organization;

— cause commercial or economic harm to an organization or country; and/or

— jeopardize the security, internal and foreign affairs of a nation

3.12
residual risk
risk that remains after controls have been implemented

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

3.13
threat
potential cause of an incident which may result in harm

3.14
top management
person or group of people who directs and controls an organization at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: In the context of this document, management should be regarded as the function, not the activity.

[SOURCE: ISO 9000:2015, 3.1.1, modified — The original notes 2 and 3 to entry have been removed; new note 2 entry has been added.]

3.15
vulnerability
weakness that can be exploited to cause harm

4 Establishing the need for a security-minded approach using a sensitivity assessment process

4.1 Undertaking a sensitivity assessment process

The process for undertaking a sensitivity assessment is set out in 4.2 to 4.4.