SLOVENSKI STANDARD
oSIST prEN ISO 19650-5:2019

01-september-2019

Organizacija in digitalizacija informacij v gradbeništvu - Upravljanje informacij z BIM - 5. del: Varnostni pristop k upravljanju informacij (ISO/DIS 19650-5:2019)

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 (ISO/DIS 19650-5:2019)

Organisation von Daten zu Bauwerken - Informationsmanagement mit BIM - Teil 5: Spezifikation für Sicherheitsbelange von BIM, der digitalisierten Bauwerke und smarten Assetmanagement (ISO/DIS 19650-5:2019)

Organisation des informations concernant les ouvrages de construction -- Gestion de l'information par la modélisation des informations de la construction (ISO/DIS 19650-5:2019)

Ta slovenski standard je istoveten z: **prEN ISO 19650-5**

ICS:

35.240.67	Uporabniške rešitve IT v gradbeništvu	IT applications in building and construction industry
91.010.01	Gradbeništvo na splošno	Construction industry in general

oSIST prEN ISO 19650-5:2019 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 19650-5

ISO/TC **59**/SC **13** Secretariat: **SN**

Voting begins on:
2019-07-05

Voting terminates on:
2019-09-27

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

ICS: 35.240.67; 91.010.01

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 19650-5:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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 on 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 the following URL: 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)*.

A list of all parts in the ISO 19650- series, published under the general title *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM)*, can be found on the ISO website.

Introduction

The built environment is experiencing a period of rapid evolution. It is anticipated that the adoption of digital engineering, including 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 in order to increase effectivity and efficiency, initiatives or projects that are developing new assets or solutions, or modifying or managing existing ones, must become much more collaborative in nature to increase effectivity and efficiency. Such collaboration requires more transparent, open ways of working, and, as much as possible, the appropriate sharing and use of digital information.

Digital built environments will need to deliver future fiscal, financial, functional, sustainability and growth objectives. This is likely to have an impact on procurement, delivery and operational processes including far greater cross-discipline and sector collaboration, significantly increasing the 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, could 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.

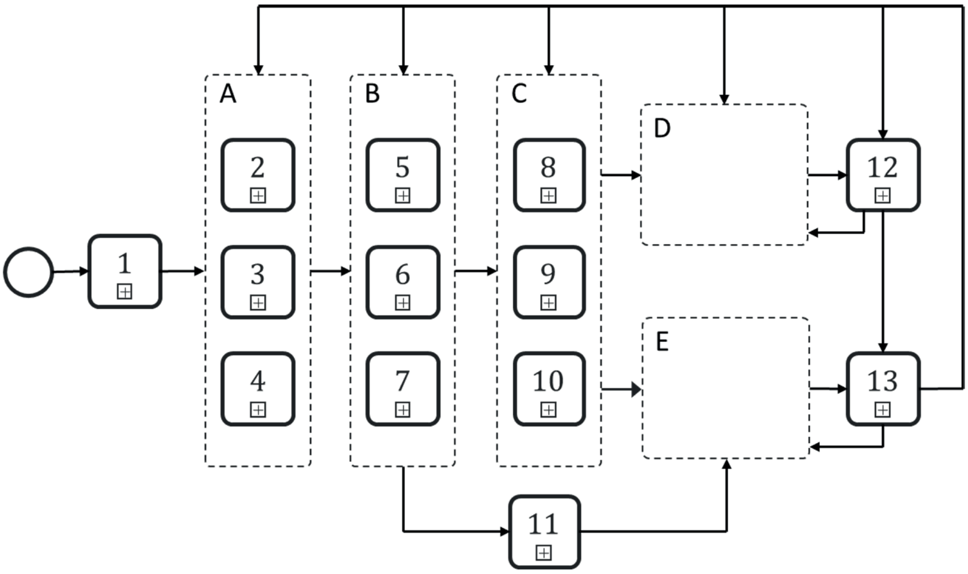
This standard provides a framework to assist organizations in understanding the key vulnerability issues and the nature of the controls required to manage the resultant security risks to a level that is tolerable to the relevant parties. Its purpose is not in any way to undermine collaboration or the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

While information security requirements for an individual organization are set out in ISO/IEC 27001, digital engineering generally involves the sharing of information between a broad range of organizations. ISO/IEC 27001 therefore cannot be applied to these organizations as a whole. This standard 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, maintenance and operation of projects and assets using BIM.

Implementation of the measures outlined in this standard will assist in reducing the risk of the loss, misuse or modification of sensitive information that could 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.



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 (see also ISO 19650-3)
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
10	Organizational information requirements (OIR)
11	Strategic business case and strategic brief
12	Asset operational use
13	Performance measurement and improvement actions

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

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 standard 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", 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 that 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 standard is intended for use by any organization who is involved in the use of digital engineering and related 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 who wish 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 19650-1:2018, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 1: Concepts and principles*

ISO 19650-2:2018, *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 19650-3:2019, *Organization of information about construction works — Information management using building information modelling — Part 3: Operational phase of the assets*

ISO 55000, *Asset management — Overview, principles and terminology*

3 Terms and definitions

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

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

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

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

3.1
asset
Item, thing or entity that has potential or actual value to an organization**[SOURCE:** ISO 55000:2014**].**

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.

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 or data elements

3.4
need-to-know
legitimate requirement of a prospective recipient of information to know, to access, or to possess any sensitive information represented by these information

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

3.6
safety
the state of relative freedom from threat or harm caused by random, unintentional acts or events

3.7
security
the state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts

3.8
security breach
infraction or violation of security

[SOURCE: ISO 14298:2013]

3.9
security incident
suspicious act or circumstance threatening security