BS EN ISO 19650-5:2020

BSI Standards Publication

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

bsi.

National foreword

This British Standard is the UK implementation of EN ISO 19650-5:2020. It is identical to ISO 19650-5:2020.

The technical content of this BS EN ISO 19650-5 is intended as a replacement for content found in PAS 1192-5:2015. PAS 1192-5:2015 has been withdrawn.

The UK participation in its preparation was entrusted to Technical Committee B/555, Construction design, modelling and data exchange.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2020

ISBN 978 0 539 01039 8

ICS 35.240.67; 91.010.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2020.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 19650-5

July 2020

ICS 35.240.67; 91.010.01

English Version

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 19650-5:2020)

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 (ISO 19650-5:2020)

Organisation von Daten zu Bauwerken - Informationsmanagement mit BIM - Teil 5: Spezifikation für Sicherheitsbelange von BIM, der digitalisierten Bauwerke und des smarten Assetmanagements (ISO 19650-5:2020)

This European Standard was approved by CEN on 15 June 2020.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (EN ISO 19650-5:2020) has been prepared by Technical Committee ISO/TC 59 "Buildings and civil engineering works" in collaboration with Technical Committee CEN/TC 442 “Building Information Modelling (BIM)” the secretariat of which is held by SN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2021, and conflicting national standards shall be withdrawn at the latest by January 2021.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 19650-5:2020 has been approved by CEN as EN ISO 19650-5:2020 without any modification.

This page deliberately left blank

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 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.

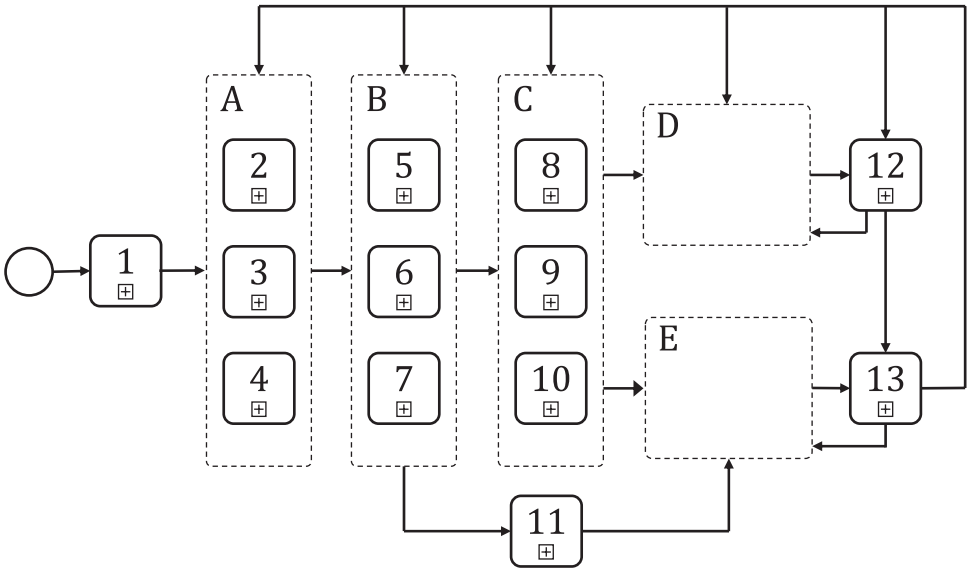
This document provides a framework to assist organizations in understanding the key vulnerability issues and the nature of the controls required to manage the resultant security risks to a level that is tolerable to the relevant parties. Its purpose is not in any way to undermine collaboration or the 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

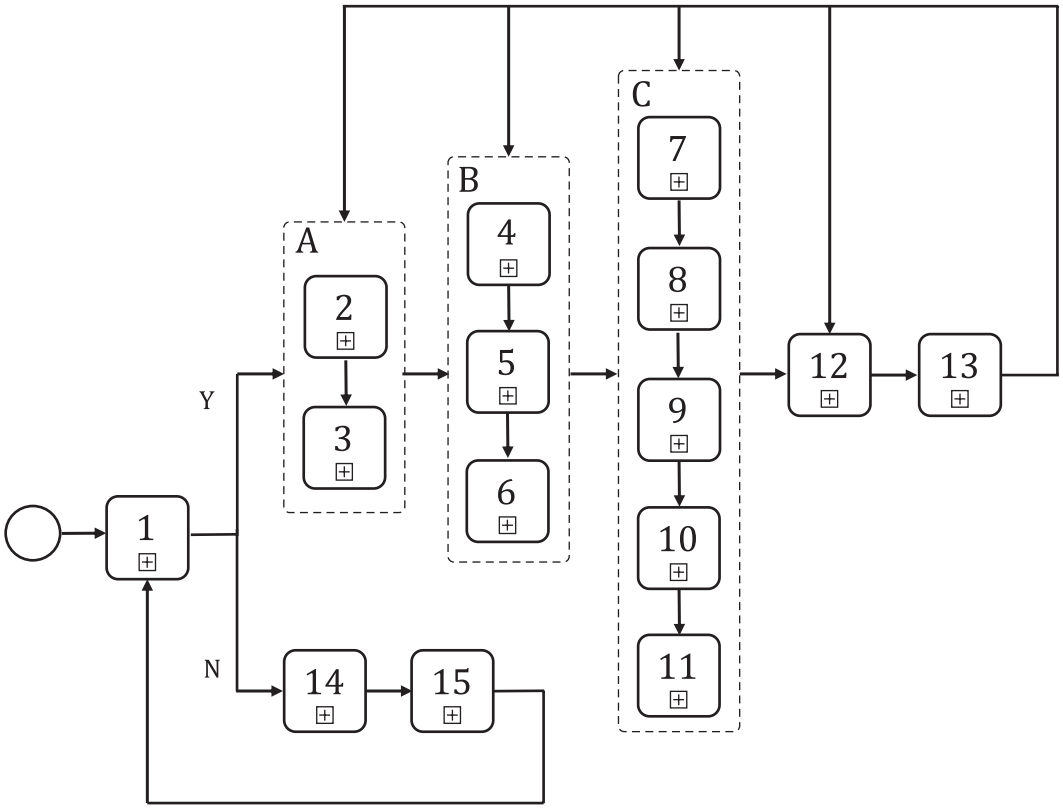
A coordinated and consistent strategies and policies
B coordinated and consistent plans
C coordinated and consistent information requirements
D activities undertaken during the operational phase of assets
E activities undertaken during the delivery phase of the asset (see also ISO 19650-2)
1 organizational 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.

INTERNATIONAL STANDARD **ISO 19650-5:2020(E)**

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.

4.2 Understanding the range of security risks

4.2.1 The top management of an organization involved in:

a) initiating a project to develop a new asset(s), product(s) or service(s) or modify/enhance an existing one;

b) managing, operating, re-purposing or disposing of an asset(s); and/or

c) the provision of an asset-based service(s),

shall determine the range of security risks that arise through greater availability of information, integration of services and systems, and the increased dependency on technology-based systems.

4.2.2 Information on the types of security risks that should be considered are contained in Annex A.

4.2.3 Where two or more organizations are involved, the top management of each organisation shall follow 4.2.1 in a coordinated manner.

NOTE Such an arrangement of multiple organizations can occur in a city/community, a large, multi-purpose development or in the provision of a transport system.

4.3 Identifying organizational sensitivities

4.3.1 Taking into consideration the range of security risks that exist, the organization(s) cited in 4.2.1 and 4.2.3 shall determine whether an initiative, project, asset, product or service, as well as any associated information, in whole or in part, and whether planned or existing, shall be considered sensitive.

NOTE Wherever the term "organization(s)" is used in the reminder of this document, it refers to the organization(s) referred to in 4.2.1 and 4.2.3.

4.3.2 A built asset shall be considered sensitive, as a whole or in part, if it:

a) comprises critical national infrastructure, identified by the local or national government;

b) fulfils a defence, law enforcement, national security or diplomatic function;

c) is a commercial site involving the creation, processing, trading or storage of valuable materials, currency, pharmaceuticals, chemicals, petrochemicals, or gases or the provision or production of enablers for production of these materials;

d) constitutes a landmark, nationally significant site or crowded place;

e) is used, or is planned to be used, to host events of security significance.

NOTE The fact that a built asset does not fall within the criteria described does not preclude the application of a higher level of security if the organization(s) wishes to adopt this.

4.3.3 An asset, product or service shall be considered sensitive if there is sufficient risk that it is, or can be, used to significantly compromise the integrity, safety, security and/or resilience of an asset, product or service, or its ability to function.

4.3.4 An asset, product or service shall also be considered sensitive if the risk to the safety, security and/or privacy of individuals or communities or their personal information exceeds the risk appetite of the organization(s).

4.3.5 If there is any uncertainty as to whether or not an initiative, project, asset, product or service is sensitive, the organization(s) shall seek advice from appropriate security experts who can demonstrate competence in the required areas.

NOTE Information on obtaining suitable security advice is contained in Annex A.

4.4 Establishing any third-party sensitivities

4.4.1 An assessment of an initiative, project, asset, product or service shall also consider whether access will be, or has already been, gained to information about other organizations, their assets, products or services that is not otherwise publicly available.

NOTE As an example, information not otherwise publicly available that can be sensitive can arise from physical surveys of underground structures, infrastructure networks and systems on private land.

4.4.2 The organization(s) shall, unless prohibitive for commercially or locally sensitive reasons, consult with the affected organization(s) to establish whether any of that information is sensitive, and where this is the case, what measures need to be applied to its capture, processing, storage, sharing and disposal and destruction.

4.5 Recording the outcome of the sensitivity assessment

The organization(s) shall record and retain the outcome of each sensitivity assessment process, including where there is no identified sensitivity, and recognize that the outcome may itself be sensitive.

4.6 Reviewing the sensitivity assessment

4.6.1 The organization(s) shall establish a suitable mechanism for performing periodic and event-driven reviews that check whether there has been any change to the sensitivity of an initiative, project, asset, product or service, whether for political, economic, social, technological, legal or environmental reasons.

4.6.2 A review shall also be undertaken when there is a significant change to the initiative, project, asset, product or service, including:

a) the ownership, use or occupancy of a built asset;

b) the processes or systems used in the management of a built asset or the production of an asset or product;

c) the information collected, processed and/or stored;

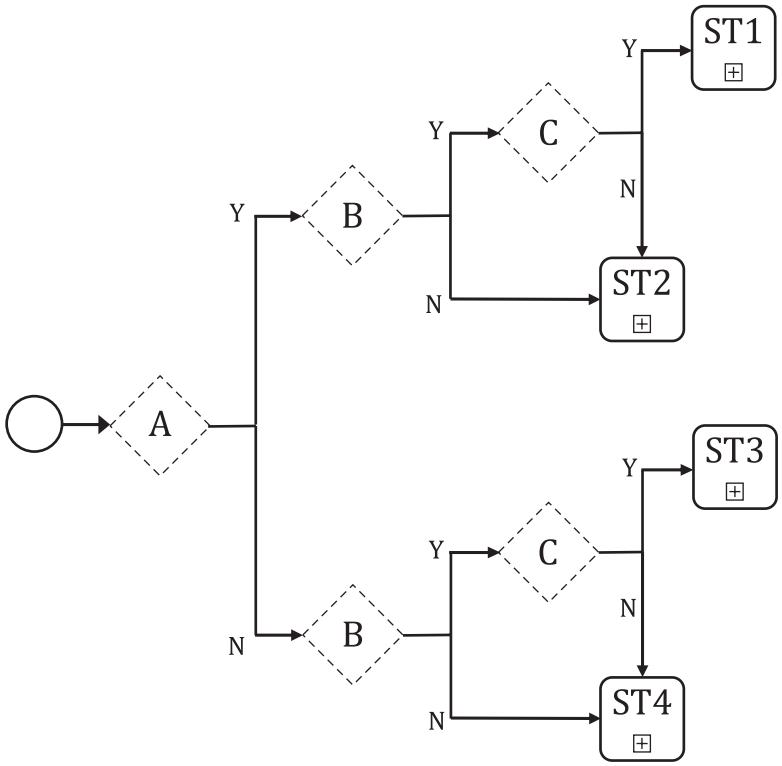
d) the service delivered; or

e) the security context.

4.6.3 Additional event-driven reviews shall be undertaken when events occur that reveal vulnerabilities not previously anticipated.

4.7 Determining whether a security-minded approach is required

The organization(s) shall apply the security triage process outlined in Figure 3 to determine whether a security-minded approach is required in relation to the initiative, project, asset, product or service.



Key

A Is the initiative, project, asset, product or service, as well as any associated information, in whole or in part, whether planned or existing, considered sensitive (see 4.3)?

B Will access be, or has already been, gained to information about another organization, its assets, products or services that is not otherwise publicly available (see 4.4.1)?

C Is the information about another organization, its assets, products or services considered sensitive (see 4.4.2)?

Y yes

N no

ST1 protect sensitive information regarding initiative, project, asset, product or service as well as third-party sensitive information by applying Clause 5 to Clause 9

ST2 protect sensitive information regarding initiative, project, asset, product or service by applying Clause 5 to Clause 9

ST3 protect third-party sensitive information by applying Clause 5 to Clause 9. Protect any sensitive commercial and personal information

ST4 protect any sensitive commercial and personal information

NOTE ST is the abbreviated term for "security triage".

Figure 3 — The security triage process

4.8 Recording the outcome of the application of the security triage process

The organization(s) shall record the outcome (ST1, ST2, ST3 or ST4) of the application of the security triage process for each initiative, project, asset, product or service to which it is applied, including where there is no identified need for a security-minded approach beyond protection of sensitive commercial and personal information.

4.9 Security-minded approach required

Where an initiative, project, asset, product or service:

a) has been determined to be sensitive, whether in whole or in part; and/or

b) will be holding third-party information that has been identified as sensitive,

the top management of the organization(s) shall, following the requirements of this document, develop and implement an appropriate and proportionate security-minded approach.

4.10 No security-minded approach required

Where an initiative, project, asset, product or service is not considered sensitive and does not have access to other third-party sensitive information, the organization(s) shall consider whether there are business benefits to be derived from applying a security-minded approach.

NOTE 1 It is prudent that organizations take appropriate steps to minimize threats arising from fraud and other criminal activity and from cyber security incidents.

NOTE 2 It is likely that baseline security measures relating to personal information and commercial information will be required within the terms of the appointment or legislation.

NOTE 3 Unless the organization(s) wishes to adopt any higher level of security, there is no necessity for the requirements of the Clause 5 to Clause 9 to be applied to the initiative, project, asset, product or service as currently assessed.

5 Initiating the security-minded approach

5.1 Establishing governance, accountability and responsibility for the security-minded approach

5.1.1 Where an organization is developing a security-minded approach, the top management shall define the individual at top management level accountable for the security-minded approach to be adopted.

5.1.2 Where two or more organizations are developing a collaborative security-minded approach, the top management of each organization shall establish a formal mechanism for:

a) creating the required governance structure, ensuring it is legally constituted and that the relationship of this structure with the relevant organizations is formally documented and agreed on;

b) agreeing on a party or parties to lead on the development of the approach and where this leadership function is split between organizations, ensuring there is clarity over accountabilities and responsibilities;

c) appointing those individuals who shall be accountable for the security-minded approach to be adopted; and

NOTE 1 The individuals are appointed to exercise the legal rights and fulfil the obligations of their respective organization.

d) reviewing and, where appropriate, updating the governance structure and appointments.

NOTE 2 Having an agreed collaborative security-minded approach is more robust than one where those organizations work in isolation.

5.1.3 The organization(s) implementing a security-minded approach shall define the individual(s) responsible for:

a) providing a holistic view of the security threats and vulnerabilities arising out of the use of, and reliance on, information and communications technologies relevant to the initiative, project, asset, product or service;

b) offering guidance and direction on the handling of the resultant security risks;

c) managing the development of a security strategy or, where the organization already has a security strategy, managing the embedding of a record of the additional security risks and mitigation measures arising out of the use of, and reliance on, information and communications technologies relevant to the initiative, project, asset, product or service; (see Clause 6);

d) managing the development, and assisting in the implementation of, a security management plan or, where the organization already has a security management plan, managing the embedding of the relevant additional policies and processes into it (see Clause 7);

e) assisting in embedding the necessary security requirements into any procurement and appointment documentation;

f) promoting a security-minded culture so that all staff understand their security responsibilities and behave in a secure manner;

g) briefing relevant third parties on appropriate aspects of the security policies and processes;

h) advising on the need for, and undertaking, the reviewing and auditing of the relevant security policies and processes;

i) advising on the need for, and where appropriate, undertaking or commissioning, testing of the relevant security measures; and

j) where appropriate and necessary, seeking advice from appropriate security experts who can demonstrate competence in the required areas, to provide additional guidance.

5.1.4 The individual(s) fulfilling the activities listed in 5.1.3 shall have clear reporting lines through to the individual accountable for security within their organization.

NOTE These functions can be fulfilled by a suitably qualified and experienced individual who can undertake or be responsible for security and other duties within the organization or can be a suitable expert employed by the organization.

5.1.5 It shall be acceptable for specific security tasks or duties to be delegated on a day-to-day basis by other individuals (for example, personnel security to human resources, cyber security to the IT manager and asset or physical security to the asset manager or facilities manager). However, the individual(s) defined as fulfilling the activities listed in 5.1.3 shall remain responsible for the operational effectiveness of each of these aspects of security.

5.2 Commencing the development of the security-minded approach

5.2.1 For a planned initiative, project, asset, product or service, the security-minded approach shall be developed as early as possible in the planning stages.

NOTE Information relating to the development that is put into the public domain can be of interest for hostile reconnaissance from the earliest stages in the design process.

5.2.2 Where a sensitive initiative, project, asset, product or service already exists, the security-minded approach shall be developed as soon as is reasonably practicable, and shall take into consideration the extent to which information is already in the public domain.

5.2.3 Where a project relates to the delivery phase of an asset using BIM, the security-minded approach shall be developed alongside the requirements described in ISO 19650-2.

5.2.4 Where the activity relates to the operational phase of an asset using BIM, the security-minded approach shall be developed alongside the requirements described in ISO 19650-3.

6 Developing a security strategy

6.1 General

6.1.1 The organization(s) shall develop and maintain a security strategy which shall include:

a) a record of the outcome of the application of the security triage process;

b) the governance, accountability and responsibility arrangements for the security-minded approach;

c) the assessment of the specific security risks to the organization(s) arising from the greater availability of information, integration of services and systems, and the increased dependency on technology-based systems (see 6.2);

d) the potential risk mitigation measures to address those security risks and the mitigation measures to be implemented (see 6.3);

e) a summary of the tolerated security risks and residual tolerated security risks (see 6.4); and

f) the mechanisms for reviewing and updating the security strategy (see 6.5).

NOTE Principles, a framework and a process for managing risk at a general level are provided by ISO 31000.

6.1.2 The security strategy shall take into consideration the legislative requirements and standards which have been identified as being relevant to the initiative, project, asset, product or service.

6.1.3 The security strategy shall be approved by the top management of the organization(s).

6.1.4 Access to any part of the security strategy that identifies sensitive aspects of the initiative, project, asset, product or service, or details the security risks identified, shall be managed on a strict need-to-know basis, with all such information subject to security measures, appropriate to the level of risk, with regard to its creation, processing and storage.

6.2 Assessing the security risks

6.2.1 The organization(s) shall assess the specific security risks arising from the greater availability of information, integration of services and systems, and the increased dependency on technology-based systems, by assessing:

a) the potential threats;

b) the potential vulnerabilities;

c) the nature of the harm which can be caused to the initiative, project, asset, product or service, as well as to personnel and citizens and to the surrounding environment; and

d) the likelihood that a vulnerability will be exploited and cause that impact.

NOTE In assessing the security risks, it can be appropriate to use the same risk scoring approach in place elsewhere in the organization.

6.2.2 Where information has already been published, the security risk assessment shall take into consideration that once information has been published on the internet or otherwise made publicly available, it is virtually impossible to delete, destroy, remove or secure all copies of it.

6.2.3 Where applicable, the security risk assessment shall include security risks associated with access to other organizations' information that is not otherwise publicly available.

6.3 Developing security risk mitigation measures

6.3.1 The organization(s) shall identify and record possible mitigation measures for each security risk or combination of risks identified.

6.3.2 In identifying and recording possible mitigation measures, the organization(s) shall consider personnel, physical, and technical security controls and requirements around the management of information.

NOTE 1 The interplay between personnel, physical and technical controls can be exploited by threat actors if the links across these areas haven't been examined.

NOTE 2 The mitigation measures developed can also seek to preserve or protect commercial, economic and social value.

NOTE 3 Information on the types of security controls and information management factors are contained in Annex B.

6.3.3 In assessing each potential mitigation measure, the organization(s) shall consider:

a) the cost of the mitigation measure and its implementation;

b) the risk reduction that can be achieved and level of residual risk;

c) the predicted cost impact of the mitigation measure;

d) other impacts that the mitigation measure can have on the asset (which can include usability, efficiency and appearance);

e) the potential for the measure to create further vulnerabilities; and

f) whether the measure delivers any other business benefits.

NOTE Business benefits can include reducing overall business risk and ensuring that the value of assets, including information, is understood.

6.3.4 The organization(s) shall use the outcome of the assessment to determine which mitigation measures, if any, are put in place.

NOTE A proportionate mitigation measure is one that is pragmatic, appropriate and cost effective.

6.4 Documenting residual and tolerated security risks

6.4.1 Following the development of the security mitigation measures, the organization(s) shall identify and record any residual security risks.

6.4.2 The organization(s) shall continue the processes of assessing the security risk and developing security risk mitigation measures on these security risks until a point is reached where the individual organization's risk appetite, or the risk appetite of the collective organizations, is not exceeded.

6.4.3 The organization(s) shall document the tolerated security risks.

6.5 Review of the security strategy

6.5.1 The organization(s) shall establish a suitable mechanism for performing periodic and event-driven reviews of the security strategy, including the effectiveness of the mitigation measures in place, to check that it remains fit for purpose.

6.5.2 Event-driven reviews shall be undertaken when political, economic, social, organizational, technological, legal or environmental changes occur that can significantly impact on the initiative, project, asset, product or service, as well as associated information or events occur that reveal vulnerabilities not previously anticipated.

6.5.3 Reviews shall take into consideration the potential impact on existing appointments likely to be affected by significant changes to the mitigation measures, especially where these constitute a change of scope.

6.5.4 Following a review, the security strategy shall be updated to reflect any changes to the threats, vulnerabilities, resultant security risks and/or security risk mitigation measures.

6.5.5 The occurrence of each review shall be recorded and retained as part of the security strategy.

6.5.6 Access to any part of the review that identifies sensitive aspects of the initiative, project, asset, product or service, or details the security risks identified, shall be managed on a strict need-to-know basis, with all such information subject to security measures, appropriate to the level of risk, with regard to its creation, distribution, use, storage, disposal and destruction.

7 Developing a security management plan

7.1 General

7.1.1 The organization(s) shall develop, maintain and implement a security management plan which enables the agreed mitigation measures set out in the security strategy to be implemented in a consistent and holistic manner.

7.1.2 The security management shall, where appropriate, be cross-referenced to other security and relevant management policies and processes which the organization(s) has in place.

7.1.3 The security management plan shall contain, in relation to the organization(s) and its delivery team:

a) the policies that set out the security-related business rules derived from the agreed mitigation measures;

b) the processes that are derived from the security policies and guidance on their consistent implementation;

c) the security information requirements detailing the information which shall be regarded as sensitive and the policies and processes for its creation, distribution, use, storage, disposal and destruction;

d) the requirements relating to the provision of information to third parties (see 7.2);

e) where applicable, logistical security requirements (see 7.3);

f) a security breach/incident management plan (see Clause 8);

g) details of accountability and responsibility for the implementation of the different aspects of the security management plan (see 7.4);

h) monitoring and auditing requirements, including testing of security measures in place (see 7.5); and

i) the mechanisms for reviewing and updating the security management plan (see 7.6).

NOTE Any gaps or omissions in the security management plan will reduce effectiveness of the security strategy and increase the risk of a security breach or incident.

7.1.4 The security management plan shall be used to inform the security requirements embedded into any procurement and appointment documents (see Clause 9).

7.2 Provision of information to third parties

7.2.1 The security management plan shall set the organization(s) requirements for undertaking an assessment prior to sharing and/or publishing of a new, modified or existing information or information model in whole or in part.

7.2.2 Such an assessment shall be capable of responding to, where applicable:

a) the need to comply with regulatory and statutory process;

b) requests for information received by an organization that is subject to the provisions of public access or transparency legislation; and

c) the need to have material that can be used at public and professional events, in marketing material, in technical, academic or other publications and websites.

7.2.3 An assessment shall consider, as far as is reasonably practicable, whether the information or information model in whole or in part:

a) contains or allows sensitive information, including information about vulnerabilities, to be deduced about an initiative, project, asset, product, service, individual or group/community;

b) when aggregated with existing shared or published material, allows sensitive information to be deduced; and

c) where applicable, contributes to determining the pattern-of-use of an asset(s) and/or the pattern-of-life of individuals or groups/communities not otherwise publicly available.

NOTE Guidance on the areas covered by this type of assessment is contained in Annex C.

7.2.4 Where the assessment finds any of these circumstances to be the case, the organization(s) shall take an appropriate and proportionate risk-based approach to the sharing and/or publication of that information.

NOTE Guidance on potential measures that can be used to reduce the security risks are provided in Annex C.

7.2.5 Access to any part of the assessment that details sensitive information shall be managed on a strict need-to-know basis, with the information contained within it subject to appropriate security measures with regard to its creation, distribution, use, storage, disposal and destruction.

7.3 Logistical security

7.3.1 Where applicable, the security management plan shall set out appropriate and proportionate security measures around the specification, procurement, design, manufacture, transport, installation and commission of any sensitive assets.

NOTE In developing these measures, advice can be sought from specialists.

7.3.2 The organization(s) shall consider:

a) the timing of the installation of any sensitive security-related assets or systems to allow, where possible, access to those assets or areas to be limited to those with a legitimate need;

b) implementing appropriate and proportionate security measures around any sensitive assets and systems which, for logistical reasons, have to be installed earlier than would generally be desirable; and

c) implementing appropriate and proportionate measures to limit, or disrupt the success of, physical hostile reconnaissance.

7.4 Managing accountability and responsibility for security

Each policy in the security management plan shall identify the individual(s) undertaking the security management function(s) that are accountable and responsible for its implementation, management, monitoring and review.

7.5 Monitoring and auditing

7.5.1 The security management plan shall set out the appropriate and proportionate monitoring, auditing and testing measures which shall take place across the lifecycle of the initiative, project, asset, product or service, which shall include assessing, as a minimum, on a risk-based sampling approach:

a) the implementation of all aspects of the security management plan; and

b) the compliance of any delivery team with all relevant aspects of the security management plan.

NOTE 1 A balance needs to be struck between formal verification involving appointed party audits and an honour/trust-based system of verification.

NOTE 2 Where applicable, the compliance of the delivery team with all relevant aspects of the security management plan can form part of the capability and capacity review defined in ISO 19650-1.

NOTE 3 Monitoring and auditing of the security management plan can be informed by standards such as ISO 19011.

7.5.2 The security management plan shall require that only those suitably qualified and experienced shall undertake this monitoring and auditing work.

7.5.3 The organization(s) can delegate some responsibility for compliance verification within the delivery team to a lead appointed party but shall retain accountability for the overall effectiveness of security controls.

7.6 Review of the security management plan

7.6.1 The organization(s) shall establish a suitable mechanism for performing periodic and event-driven reviews of the security management plan, including the security information requirements and security breach/incident management plan, to check that it remains fit for purpose.

7.6.2 Event-driven reviews shall be undertaken following a review of the security strategy, upon a security breach or incident or when political, economic, social, organizational, technological, legal or environmental changes occur that can significantly impact on:

a) the types of security breaches/incidents that can occur;

b) the process to be followed, including the need to collect forensic evidence; and

c) business continuity measures and recovery actions.

7.6.3 Reviews shall take into consideration the potential impact on existing appointments of any changes to policies and processes especially where these constitute a change of scope.

7.6.4 Following a review, the security management plan shall be updated to reflect any changes, as well as to address any identified gaps and shortcomings that lessen the ability of the plan to deliver the level of security risk mitigation required.

7.6.5 Changes to the security management plan shall be communicated within the organization(s) and to the appointed parties.

7.6.6 The occurrence of each review shall be recorded and retained as part of the security management plan.

8 Developing a security breach/incident management plan

8.1 General

8.1.1 The organization(s) shall create and maintain a security breach/incident management plan as part of the security management plan which shall include:

a) an assessment of the types of security breaches/incidents that can occur and the potential risks that can arise which impact upon the organization(s), its function, assets, and reputation, to personnel and third parties;

b) the process to be followed on discovery of a security breach/incident, including one that nearly occurred (see 8.2);

c) business continuity measures and recovery actions affording the same level of security as the systems in use on a day-to-day basis including, where applicable, the collection of evidence for law enforcement purposes (see 8.3);

d) the review process to be carried out following a security breach or incident (see 8.4); and

e) the mechanisms for reviewing and updating the security breach/incident management plan (see 8.5).

8.1.2 Parts of the security breach/incident management plan can be covered by other existing plans or national-specific actions and where this is the case, these plans or actions shall be cross-referenced.

8.1.3 Parts of the security breach/incident management plan that record the risks to the organization(s) shall be managed on a strict need-to-know basis, with the information contained within those parts subject to appropriate security measures with regard to its creation, distribution, use, storage, disposal and destruction.

8.2 Discovery of a security breach or incident

The organization(s) shall set out the steps to be taken in the event of a discovery of a security breach or incident which shall include:

a) the persons or roles to be contacted immediately and their contact details;

b) the processes used to identify the concerned parties;

c) the mechanisms for notifying concerned parties and information to be provided; and

d) handling any third party, regulator, media or public interest in the event of a security breach or incident.

8.3 Containment and recovery

The organization(s) shall set out the steps to be taken in the event of a security breach/incident to contain and recover from the event that include:

a) measures for reducing further damage or loss;

b) assessment of what has been lost, compromised, damaged or corrupted;

c) circumstances under which a collection of evidence for law enforcement purposes is required and the approach; and

d) forensic readiness measures required to enable, when required, the capture of forensic information about an incident for use by law enforcement, and/or detailed analysis of the root causes of the incidents.

Under circumstances where it is necessary to collect evidence for law enforcement purposes, all evidence (i.e. both physical and digital) that may aid an investigation to identify the cause of the event and the perpetrators, shall be preserved and collected before any recovery actions are taken, unless the immediate need for such actions is critical to life.

NOTE It is important that forensic evidence is collected before recovery actions are taken, as these actions can destroy or contaminate the digital forensic evidence.

8.4 Review following a security breach or incident

8.4.1 Following the initial containment and recovery actions, the organization(s) shall undertake an assessment of the ongoing risk. This assessment shall examine the causes of the event, identify potential countermeasures, and assess the residual risk as well as any potential new or exacerbated risk arising from the event.

8.4.2 The relevant policies and processes shall be updated to reflect the findings of the assessment and to prevent or reduce the risk for a re-occurrence.

8.4.3 The organization(s) shall require, where applicable, relevant members of its delivery team to collaborate with it to undertake an appropriate and proportionate post-incident evaluation of the event and the response.

9 Working with appointed parties

9.1 Working outside formal appointments

9.1.1 The organization(s) shall put in place information sharing agreements, or equivalent, when working outside formal appointments (for example during tendering) if access is going to be granted to sensitive information.

NOTE Further information on information sharing agreements is contained in Annex D.

9.1.2 The information sharing agreement, or equivalent, shall include the organization(s) requirements for the retention, disposal and destruction of sensitive information.

9.1.3 When the process of tendering appointments requires the release of sensitive information, the organization(s) shall implement appropriate and proportionate protection measures and/or separate processes, while ensuring that sufficient information is available.

9.1.4 The organization(s) shall, as part of the appointed party selection process, assess all tender documentation to establish how it is intended that the security requirements set out in the security management plan would be met.

9.1.5 The organization(s) shall assess the security understanding, capability, competence and experience of the organizations for an appointment, as well as any security training, coaching and support requirements.

9.2 Measures contained in appointment documentation

9.2.1 The organization(s) shall manage its delivery team security risks by having in place provisions in the appointment documentation which support all of the relevant security policies and processes contained within the security management plan, including the requirements placed on a member of a delivery team at the end of an appointment.

9.2.2 The organization(s) shall detail the allocation of the information security function to the delivery team, including the requirement for security to be retained at accountable levels within the delivery team, with responsibility delegated appropriately, in order that it can be effectively and efficiently managed.

9.2.3 Where appropriate, the provisions shall include the application of the same requirements contained in the appointment documentation for the appointed parties, who are appointed directly to the organization(s), through the layers of sub-appointments.

9.2.4 Where compliance with specific security standards is required (e.g. the provision of specific physical or cyber security measures to a defined standard), these shall be clearly identified in the appointment documentation, along with any expected independent, third-party inspection or verification.

9.2.5 To handle security breaches/incidents caused by a professional advisor, contractor or appointed party, there shall be clear provisions in the appointment documentation for the reporting of the security breach/incident to the organization(s) and for provision of assistance in the investigation and follow up actions.

9.2.6 The measures embedded into the appointment documentation shall include provisions that allow the organization(s) to review security measures and compliance with the relevant security policies and processes at any level in the relevant delivery team.

9.2.7 The organization(s) shall insert a clause within the appointment documentation to enable adjustments in response to changes in the political, legislation or regulatory environment to be implemented.

9.2.8 The organization(s) shall require, upon termination of an appointment, that all relevant information, including that which the appointed party has shared with other members of its delivery team, is delivered, stored securely, disposed or destroyed in compliance with organizational and appointment-related requirements.

9.2.9 Where appropriate, the organization(s) shall require the appointed party to verify that defined procedures for the delivery, disposal or destruction of sensitive information have been completed, and to verify the ongoing security arrangements for sensitive information that is to be retained.

9.2.10 The organization(s) shall require sufficient decommissioning and demobilization processes to be put in place to maintain the security of asset information.

9.3 Post appointment award

9.3.1 The organization(s) shall monitor and enforce all security-related provisions in the appointment documentation relating to its appointed parties in order that they adopt an acceptable security-minded approach to the fulfilment of their appointment-related obligations.

9.3.2 The organization(s) shall work with its delivery team to assist in the understanding of the security requirements and to address any outstanding security issues.

9.4 End of appointment

The organization(s) shall implement appropriate and proportionate measures for checking the compliance of any delivery team with any requirements for the delivery, secure storage, disposal or destruction of sensitive information.

Annex A
(informative)

Information on the security context

A.1 Understanding the potential security issues

Making use of the security advice available, the organization(s) should gain an understanding of:

a) the range of threats that can seek to make use of vulnerabilities to:

   1) compromise the value and longevity of initiatives and projects;

   2) compromise the value, longevity and ongoing use of the organization's assets, products and/or services;

   3) cause harm, damage or distress to, or compromise, an organization's personnel or other users of the asset or services;

   4) disrupt or corrupt information and/or systems;

   5) cause reputational damage; and/or

   6) acquire personal data, intellectual property or commercially sensitive information;

   NOTE 1 Threats include terrorism, hostile actions by countries, commercial espionage, organized crime, activists, lone actors, hackers and malicious insiders.

b) the range of traditional and evolving techniques of hostile reconnaissance to which initiatives, projects, assets, products, services and personal information can be vulnerable;

   NOTE 2 During hostile reconnaissance, the hostile party is looking for information:

   1) it can exploit about security (e.g. physical vulnerabilities or system configuration);

   2) to identify the modus operandi;

   3) about the state of security (i.e. the chances of being detected/the chance of success);

   4) about the pattern-of-life of an individual, group of individuals, or pattern-of-use of an asset.

   NOTE 3 From the perspective of the hostile party, achieving successful attack planning depends on the reliability of this information and the ability to exploit it before preventative measures can be implemented.

c) the potential for components or individual assets or products that will be embedded within a larger asset, product or system to be counterfeit, maliciously or fraudulently sub-standard or contaminated;

d) the potential for, and potential impact of, malicious acts caused by a range of external and insider threats, including malware, hackers or disaffected personnel that can compromise:

   1) intellectual property and/or commercially sensitive information;

   2) personal information;

   3) metadata integrity; or

   4) master referential data integrity.

NOTE 4 The malicious acts can result in loss, disclosure or corruption of, or unauthorised access or unauthorised changes to information.

e) the potential for insecure or poorly maintained systems to expose or permit unauthorized access to sensitive information;

f) the potential for information to be used to conduct pattern-of-life analysis to facilitate malicious or criminal exploitation of habits, routines and preferences;

g) the potential for the aggregation information to:

1) lead to the identification of individuals or groups of individuals;

2) reveal sensitive information about initiatives, projects, assets, products, services, individuals or communities; or

3) reveal information about the configuration of assets, products, components and/or software in a system.

NOTE 5 Aggregation risks can arise from:

1) aggregation by accumulation, where the volume of information stored together increases the level of impact that would occur if the information was compromised;

2) aggregation by association, where the association of different types of information, which in themselves have little or no impact when compromised, have a higher level of impact when associated together; or

3) a combination of accumulation and association.

h) the reputation risks arising from the issues listed above.

A.2 Security advice

A.2.1 To assist in the development of the security-minded approach, the organization(s) should use suitable security guidance to gain advice on the security risks that arise through greater availability of information, integration of services and systems, and the increased dependency on technology-based systems.

A.2.2 If the organization(s) is already security-minded, it can have people in post who are suitably qualified and experienced, with a sufficient understanding of governance, physical, technological, personnel and people security and the relationships and interdependencies between them, who can provide complete advice and assistance in understanding the security context. Where this is not the case, external specialist security advice should be sought.

Annex B
(informative)

Information on types of personnel, physical, and technical security controls and management of information security

B.1 Personnel aspects

In developing policies and processes relating to personnel security, organizations should consider including:

a) identification of high-risk functions within the organization(s) and any organizations employed as part of an appointment or providing services;

NOTE Examples of a high-risk function include those which have access to the details of the security strategy, information relating to sensitive assets, or one that fulfils an IT system administration or key information management role.

b) security screening and vetting requirements for any individual(s) in contact with sensitive assets, including information, both in general and specific roles;

c) security competence requirements of individuals in specific roles;

d) induction of all new personnel and organizations providing services to the organization(s) so that they are appropriately briefed on their responsibilities and the required security-minded culture, including:

1) the need to provide and record general security awareness training as part of a project, or ongoing operations, alongside health and safety, project or site familiarization and other similar training;

2) mandatory topics to be covered by these awareness sessions and the required learning outcomes from each;

e) general security awareness and training requirements to develop and promote a security-minded culture, including refresher training;

f) role-based security training requirements to facilitate the adoption and maintenance of a security-minded culture;

g) ongoing security training and awareness requirements;

h) access and permission requirements to information and information models; and

i) demobilization of organization(s) and personnel.

B.2 Physical aspects

In developing policies and processes relating to physical security, the organization(s) should consider including:

a) physical security measures required at the locations where sensitive information is held or remote access to systems within any part of a sensitive asset has been granted;

b) where applicable, physical security measures required at the location of a new or existing built asset;

c) where applicable, protection of neighbouring built assets not otherwise generally visible and/or accessible; and

NOTE Neighbouring built assets are built assets (and the services that supply them) that share a boundary (including beneath it or overhead) with the built asset under consideration, or that are in the neighbourhood of that built asset but physically separated by a public or private street, public or privately-owned open space or similar feature.

d) protective measures required for computing, electronic devices and equipment.

B.3 Technological aspects

B.3.1 In developing policies and processes relating to technological security, the organization(s) should consider including:

a) measures related to the cyber security of systems capturing, processing and storing sensitive information including the requirement for regular vulnerability assessment and penetration testing;

b) the security of interconnections and interactions between such systems;

c) the security around systems controlling physical assets;

d) the permissible interoperability of systems and resilience of each system to failure;

e) configuration management and change control processes and procedures for the systems processing and storing project and asset information and the technical environment hosting them;

f) the secure disposal and/or destruction of information held by organizations no longer involved in the initiative, project, asset, product or service, and/or removal of access to that information; and

g) where information is retained for the period required to comply with legal, regulatory, or organizational requirements, whichever is longer, the measures to be applied regarding the security of that retained information, and the measures to be applied following that period to ensure its secure disposal, destruction and/or removal of access.

B.3.2 Wherever possible, the systems used for capturing, processing and/or storing sensitive information should be secure by default (i.e. full functionality is available without compromising security and that default settings for security will be at their highest level) or the system settings configured to maximize protection of that information.

B.3.3 As part of the selection process, the software systems used for capturing, processing or storing sensitive information should be assessed on their ability to deliver each of the aspects listed below to a level that is appropriate and proportionate to the sensitivity of that information:

a) confidentiality — controlling, and preventing unauthorized access to, information which can be sensitive or breach privacy, in isolation or in aggregate;

b) availability (including reliability) — ensuring that the information, systems, and associated processes are consistently discoverable, accessible, usable and, where appropriate, disclosable in an appropriate and timely fashion;

NOTE An appointment can specify availability in terms of a percentage (e.g. 99,999 9 % per annum) with a specified maximum time for restoration of a normal service (e.g. 30 minutes) and can vary between assets/products and services.

c) safety — systems and related processes are designed, implemented, operated and maintained so as to prevent the creation of harmful states which can lead to injury or loss of life, or unintentional environmental damage, or damage to assets;

d) resilience — the ability of information, services and systems to transform, renew and recover in a timely way in response to adverse events;

e) possession — systems and associated processes are designed, implemented, operated and maintained so as to prevent unauthorized control, manipulation or interference, and to ensure that information is used only in accordance with the terms of the compliance and the rights and obligations specified in the appointment documentation;

f) authenticity — ensuring that information input to, and output from, systems, the state of the system and any associated processes and information are genuine;

g) utility — ensuring that asset information and systems remain useful over the period access to that information may be required; and

h) integrity — maintaining the completeness, accuracy, consistency, coherence and configuration of information and systems.

B.3.4 Prior to the implementation of any system based on the internet of things or other distributed technologies, the organization(s) should:

a) understand the security architecture of the proposed technologies;

b) determine the extent to which the architecture meets the security requirements of the organization(s);

c) assess any security risks, including the potential impact of a failure of the technology, against the risk appetite of the organization(s) and the benefits which it is anticipated can be gained; and

d) put in place appropriate and proportionate security risk mitigation measures to manage any unacceptable security risks.

B.4 Information security

B.4.1 In developing policies and processes relating to information security, the organization(s) should consider including:

a) the requirements for conducting inspections and surveys that can gather sensitive information not otherwise publicly available;

b) the management and monitoring of the secure storage of, secure access to, and ultimately secure disposal and destruction of information, including information that is retained for a period to comply with legal or other regulatory requirements and with any specific requirements of the organization(s), whichever is longer;

NOTE 1 It is important that access to sensitive information is managed on a need-to-know basis, with organizations and personnel only having access to the sensitive information that is relevant and necessary for the completion of their tasks.

c) the maximum amount of information relating to sensitive assets/products or systems to be contained in databases, information exchanges and, where applicable, information models;

d) the embedding of any requirements relating to any special handling or protection of information which has security sensitivity and has been provided to the organization(s) by a third party;

e) protection against the loss, disclosure, corruption of, or loss of access or unauthorized changes to information, metadata and referential master data; and

NOTE 2 Referential master data comprises a set of permissible values to be used by other data fields in shared information models.

f) monitoring and recording changes to processes and technologies used for information capture, processing, including information synthesis, and storage.

B.4.2 The policies and processes should be applicable across the generic information lifecycle which comprises:

a) capture — the activity associated with the creation and initial storage of a piece of information, including its metadata;

b) acquisition — the purchase or transfer of information from other parties;

c) maintenance — the activities that serve to deliver the information ready for synthesis or usage in a form and manner that is appropriate for these purposes and include: validation and verification; cleansing; reformatting; enrichment; movement; integration from multiple systems; and updating of published information;

d) synthesis — the creation of derived information;

e) usage — the application of information to activities, functions or tasks;

f) archival — the replication or placement of information in an archive where it is stored but where no maintenance, usage or publication occurs;

g) publication — the process of making the information available within or outside an organization; and

h) purging — the removal of every known copy of an individual piece of information from an organization.

Annex C
(informative)

Assessments relating to the provision of information to third parties

C.1 Information assessment

C.1.1 An assessment should include establishing:

a) who will have access to the information that is being shared;

b) whether other parties and stakeholders are to be consulted prior to sharing and/or publishing;

c) the justification for sharing or publishing, in particular:

   1) the objective;

   2) the potential benefits and how they will be captured;

   3) the risks if it is not shared or published;

   4) demonstration that the proposed sharing is proportionate to the objective and the potential benefits; and

   5) whether or not the objective can be achieved, or the benefits delivered, without sharing or publishing it;

d) the authority to share or publish the information, in particular:

   1) whether the organization that will be sharing or publishing it is the information controller and/or has the right, legal authority and power to do so;

   2) whether there are any legal obligations to share or publish (e.g. legislation or a court order); and

   3) whether it was provided in confidence.

e) any information protection issues;

f) the security risks with sharing or publishing and whether or not these risks exceed the risk appetite of the organization(s);

g) appropriate and proportionate security risk mitigation measures to manage any information protection issues or unacceptable security risks;

h) the willingness and capability of the party receiving the information to manage it appropriately; and

i) any residual security risks and remaining information protection issues.

C.1.2 Where potential personal information security breaches/incidents or security risks not tolerable to the organization(s) are identified, sharing or publication should be prohibited until appropriate and proportionate measures are implemented to remove the sensitivity or reduce the associated risks to a level that is tolerable to the organization(s).

C.2 Regulatory and statutory processes

C.2.1 The security management plan should detail the approach to the supply and exchange of information with third parties when complying with regulatory and statutory processes**.**

C.2.2 The security management plan should require that sensitive information be suitably separated and protected. This may include redaction or removal of sensitive information regarding sensitive features, specific uses of areas within a built asset and uses of protective measures. It may also include providing unstructured information in formats such as hard copy, images or non-interactive PDF formats, rather than giving access to, for example, interactive information models.

C.2.3 Where sensitive information cannot be excluded from a submission, the organization(s) should liaise with the third party, prior to the submission of information, to agree what appropriate protection measures can be put in place. Where the third party is subject to the provisions of public access or transparency legislation, these measures shall be sufficient to manage the risk to a level that is tolerable to the organization(s).

C.3 Public access to information

The security management plan should detail the approach to protect sensitive information that shall be taken where a request for information is received by an organization that is subject to the provisions of public access or transparency legislation. This should consider the impact of potential issues arising from aggregation.

C.4 Public presentations

The security management plan should set out the requirements for approving any material relating to the initiative, project, asset, product or service that is going to be discussed or displayed at public events, placed in locations accessible to members of the public or other third parties, or made publicly available on websites, in technical or academic publications or marketing material.

Annex D
(informative)

Information sharing agreements

D.1.1 An information sharing agreement, or equivalent, available to all relevant parties, should be put in place prior to the sharing of sensitive information, and where applicable, information models that can be used to cause harm to an initiative, project, asset, product, service, individual or group/community.

D.1.2 The agreement should detail, as a minimum:

a) the purpose(s) of the sharing;

b) the potential recipients, or types of recipient, and the circumstances in which they have access;

c) the type of information to be shared;

d) the quality of the information to be shared, in particular its authenticity, coverage, accuracy, relevance and usability;

e) the requirements in relation to:

   1) information protection, where relevant;

   2) permitted and prohibited rights of use of information;

   3) the cascade of obligations contained in the information sharing agreement through the layers of permitted sub appointments; and

   4) obligations, consistent with the requirements of the security breach/incident management plan, to notify the information owner and/or information controller in the event of any potential or known security breach or incident;

f) user management;

g) information maintenance, including responding to notification of requests for erasure or correction;

h) information security requirements;

i) the arrangements for retention and/or purging of shared information;

j) procedures for dealing with information subjects' rights, including access requests, queries and complaints, as well as transfer between organizations, territories and jurisdictions;

k) monitoring and auditing of the implementation of the information sharing agreement; and

l) sanctions for failure to comply with the information sharing agreement and/or a security breach/incident by an individual member of staff.

NOTE Getting appropriate legal advice will be part of drawing up a robust information sharing agreement.

D.1.3 In the event of an actual or potential security breach/incident, or if there is evidence that information is not being managed and handled in accordance with the information sharing agreement, the organization(s) should either:

a) suspend the information sharing agreement and information sharing until the event or concerns have been investigated and any remedial measures have been agreed and implemented; or

NOTE Under these circumstances, it will be important that the investigation and implementation of mitigation measures are conducted without unnecessary delay.

b) terminate the information sharing agreement and information sharing and, where appropriate, require purging of the shared information if the matter cannot be satisfactorily remedied.

D.1.4 Information sharing agreements should be reviewed at the frequency defined in the security management plan, to establish the effectiveness of the sharing and to confirm that:

a) there is still a legitimate purpose for the continued sharing of information with each recipient, and where there is not, that access has been withdrawn;

b) the information quality and maintenance are to the agreed standards; and

c) the information security arrangements remain appropriate and proportionate, and that any security breaches or incidents have been satisfactorily resolved.

Bibliography

[1] ISO 14298:2013, *Graphic technology — Management of security printing processes*

[2] ISO 16530-1:2017, *Petroleum and natural gas industries — Well integrity — Part 1: Life cycle governance*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO 19650-1, *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*

[5] ISO 22300:2018, *Security and resilience — Vocabulary*

[6] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[7] ISO 31000, *Risk management — Guidelines*

[8] ISO 55000:2014, *Asset management — Overview, principles and terminology*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than one device provided that it is accessible by the sole named user only and that only one copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than one copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright and Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member.**

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK