

DIN EN ISO 19650-5

ICS 35.240.67; 91.010.01

Einsprüche bis 2019-09-12

Entwurf

**Organisation von Daten zu Bauwerken –
Informationsmanagement mit BIM –
Teil 5: Spezifikation für Sicherheitsbelange von BIM, der digitalisierten
Bauwerke und des smarten Assetmanagements (ISO/DIS 19650-5:2019);
Deutsche und Englische Fassung prEN ISO 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);
German and English version prEN ISO 19650-5:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-07-12 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nabau@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Bauwesen (NABau), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 74 Seiten

DIN-Normenausschuss Bauwesen (NABau)

Nationales Vorwort

Dieses Dokument (prEN ISO 19650-5:2019) wurde vom Technischen Komitee ISO/TC 59 „Buildings and civil engineering works“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 442 „Building Information Modelling (BIM)“ erarbeitet, dessen Sekretariat von SN (Norwegen) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 005-01-39 AA „BIM — Building Information Modeling (SpA zu ISO/TC 59/SC 13 — CEN/TC 442)“ im DIN-Normenausschuss Bauwesen (NABau).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 19650-1:2018	siehe DIN EN ISO 19650-1:2019-08
ISO 19650-2:2018	siehe DIN EN ISO 19650-2:2019-08
ISO 19650-3:2019	siehe E DIN EN ISO 19650-3:2019-08
ISO 31000:2018	siehe DIN ISO 31000:2018-10
ISO 55000	siehe DIN ISO 55000

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 19650-1:2019-08, *Organisation und Digitalisierung von Informationen zu Bauwerken und Ingenieurleistungen, einschließlich Bauwerksinformationsmodellierung (BIM) — Informationsmanagement mit BIM — Teil 1: Begriffe und Grundsätze (ISO 19650-1:2018); Deutsche Fassung EN ISO 19650-1:2018*

DIN EN ISO 19650-1:2019-08, *Organisation und Digitalisierung von Informationen zu Bauwerken und Ingenieurleistungen, einschließlich Bauwerksinformationsmodellierung (BIM) — Informationsmanagement mit BIM — Teil 2: Planungs-, Bau- und Inbetriebnahmephase (ISO 19650-2.2:2018); Deutsche Fassung EN ISO 19650-2:2018*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

DIN ISO 55000, *Asset Management — Übersicht, Leitlinien und Begriffe*

E DIN EN ISO 19650-3:2019-08, *Organisation von Daten zu Bauwerken — Informationsmanagement mit BIM — Teil 3: Nutzungsphase von baulichen Anlagen*

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

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: parallele Umfrage
Dokumentsprache: D

STD Version 2.9p

Inhalt

	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	9
2 Normative Verweisungen.....	9
3 Begriffe.....	9
4 Ermittlung des Bedarfs an einem sicherheitsbewussten Ansatz mithilfe eines Prozesses zur Bewertung der Sensitivität.....	11
4.1 Bestimmung des Umfangs der Sicherheitsrisiken.....	11
4.2 Ermittlung der Sensibilität der Organisation.....	12
4.3 Ermittlung der Sensibilitäten Dritter.....	13
4.4 Dokumentation des Ergebnisses der Sensibilitätsbewertung.....	13
4.5 Regelmäßige Überprüfung der Sensibilitätsbewertung.....	13
4.6 Bestimmung des Bedarfs eines sicherheitsbewussten Ansatzes.....	14
4.7 Die Organisation(en) muss (müssen) das Ergebnis der Anwendung des Sicherheitseinstufungsprozesses für jede Initiative, jedes Projekt, jedes Asset, jedes Produkt oder jede Dienstleistung, auf die bzw. das es angewendet wurde, dokumentieren, auch wenn kein Bedarf an einem sicherheitsbewussten Ansatz über den Schutz der sensiblen kommerziellen und persönlichen Informationen hinaus ermittelt wurde.....	15
4.8 Sicherheitsbewusster Ansatz erforderlich.....	15
4.9 Kein sicherheitsbewusster Ansatz erforderlich.....	15
5 Entwicklung des sicherheitsbewussten Ansatzes.....	15
5.1 Verwaltung, Rechenschaftspflichten und Zuständigkeiten im Zusammenhang mit dem sicherheitsbewussten Ansatz.....	15
5.2 Beginn der Entwicklung des sicherheitsbewussten Ansatzes.....	17
6 Entwicklung einer Sicherheitsstrategie.....	17
6.1 Allgemeines.....	17
6.2 Bewertung der Sicherheitsrisiken.....	18
6.3 Entwicklung von Maßnahmen zur Minderung von Sicherheitsrisiken.....	18
6.4 Dokumentation der Restrisiken und hinnehmbaren Sicherheitsrisiken.....	19
6.5 Überprüfung der Sicherheitsstrategie.....	19
7 Entwicklung eines Sicherheitsmanagementplans.....	20
7.1 Allgemeines.....	20
7.2 Anforderungen bezüglich der Bereitstellung von Informationen gegenüber Dritten.....	20
7.3 Logistische Sicherheitsanforderungen.....	21
7.4 Verwaltung der Rechenschaftspflichten und Zuständigkeiten in Bezug auf die Sicherheit.....	21
7.5 Überwachung und Prüfung.....	22
7.6 Überprüfung des Sicherheitsmanagementplans.....	22
8 Entwicklung eines Plans zum Management von Sicherheitsverstößen/-vorfällen.....	22
8.1 Allgemeines.....	22
8.2 Feststellung eines Sicherheitsverstößes oder -vorfalls.....	23
8.3 Eindämmung und Wiederherstellung.....	23

8.4	Überprüfung nach einem Sicherheitsverstoß oder -vorfall	24
8.5	Überprüfung des Plans zum Management von Sicherheitsverstößen/-vorfällen	24
9	Zusammenarbeit mit Informationsbereitstellern	25
9.1	Zusammenarbeit außerhalb formaler Informationsbestellungen	25
9.2	In den Dokumenten der Informationsbestellung enthaltene Maßnahmen	25
9.3	Leistungsnachweis nach der Informationsbestellung	26
9.4	Ende der Informationsbestellung	26
10	Einhaltung einschlägiger Vorschriften und Normen	26
Anhang A (informativ) Informationen zum Sicherheitskontext		27
A.1	Verständnis der potentiellen Sicherheitsprobleme	27
A.2	Sicherheitsberatung	28
Anhang B (informativ) Informationen zu Arten der Steuerung der Personal-, der physischen und der technischen Sicherheit und Management der Informationssicherheit		29
B.1	Personalaspekte	29
B.2	Physische Aspekte	30
B.3	Technologische Aspekte	30
B.4	Informationssicherheit	32
Anhang C (informativ) Bewertungen bezüglich der Bereitstellung von Informationen gegenüber Dritten		34
C.1	Informationsbewertung	34
C.2	Rechtliche und gesetzlich vorgeschriebene Prozesse	35
C.3	Öffentlicher Zugang zu Informationen	35
C.4	Öffentliche Präsentationen	35
Anhang D (informativ) Vereinbarungen über die Informationsweitergabe		36
D.1	Vereinbarungen über die Informationsweitergabe	36
Literaturhinweise		38

Europäisches Vorwort

Dieses Dokument (prEN ISO 19650-5:2019) wurde vom Technischen Komitee ISO/TC 59 „Buildings and civil engineering works“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 442 „Building Information Modelling (BIM)“ erarbeitet, dessen Sekretariat von SN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 19650-5:2019 wurde von CEN als prEN ISO 19650-5:2019 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 59, *Bauwesen*, Unterkomitee SC 13, *Organisation und Digitalisierung von Informationen zu Bauwerken und Ingenieurleistungen, einschließlich Bauwerksinformationsmodellierung (BIM)* erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO 19650, veröffentlicht unter dem allgemeinen Titel *Organisation und Digitalisierung von Informationen zu Bauwerken und Ingenieurleistungen, einschließlich Bauwerksinformationsmodellierung (BIM)* ist auf der ISO-Internetseite abrufbar.

Einleitung

Die bebaute Umgebung unterliegt ständigen Entwicklungen. Es ist damit zu rechnen, dass die Digitalisierung des Ingenieurwesens, einschließlich der Bauwerksinformationsmodellierung (BIM), sowie die zunehmende Anwendung digitaler Technologien in der Planung, Konstruktion, Herstellung, dem Betrieb und dem Management von Assets oder Produkten und in der Bereitstellung von Dienstleistungen in der bebauten Umgebung erhebliche Auswirkungen auf die beteiligten Personen haben wird. Um die Effektivität und Effizienz zu erhöhen, müssen Initiativen und Projekte, im Rahmen derer neue Assets oder Lösungen entwickelt oder bereits vorhandene Assets und Lösungen modifiziert oder verwaltet werden, wahrscheinlich viel stärker auf Kooperation ausgerichtet sein. Eine derartige Zusammenarbeit fordert transparentere, offenere Arbeitsmethoden und, soweit möglich, eine angemessene Weitergabe und Nutzung digitaler Informationen.

Digitale bebaute Umgebungen sind zukünftig herausgefordert, steuerliche, finanzielle und funktionale Ziele sowie Ziele der Nachhaltigkeit und des Wachstums zu erfüllen. Dies hat sehr wahrscheinlich Auswirkungen auf die Prozesse der Beschaffung, der Bereitstellung und des Betriebs, einschließlich einer viel stärkeren Zusammenarbeit zwischen Fachbereichen, wodurch die Verfügbarkeit von Informationen drastisch erhöht wird.

Der Einsatz rechnergestützter Technologien unterstützt bereits neue Arbeitsmethoden, wie die Entwicklung außerhalb des Standorts, die werksbasierte Herstellung und die Automatisierung am Standort. Fortgeschrittene cyber-physische Systeme, die Sensoren (das Cyber- oder Verarbeitungselement) zur Steuerung oder Beeinflussung physischer Teile des Systems einsetzen, sind in der Lage, in Echtzeit zu arbeiten, um Ergebnisse in der realen Welt zu beeinflussen. Es ist davon auszugehen, dass derartige Systeme künftig eingesetzt werden, um durch die Erfassung von Echtzeitinformationen über die Nutzung und den Zustand von Assets eine Steigerung der Energieeffizienz und ein besseres Lebenszyklus-Management von Assets zu erzielen. Sie werden bereits in den Bereichen Transport, Versorgung, Infrastruktur, Gebäude, Herstellung, Gesundheitswesen und Verteidigung verwendet und könnten auch für die Entwicklung intelligenter Gemeinschaften genutzt werden, sofern sie als integrierte cyber-physische Umgebungen interagieren können.

Infolge dieser zunehmenden Nutzung und Abhängigkeit von Informations- und Kommunikationstechnologien müssen die damit verbundenen Sicherheitslücken sowie die sich daraus ergebenden sicherheitstechnischen Auswirkungen auf bebaute Umgebungen, Assets, Produkte, Dienstleistungen, Einzelpersonen oder Gemeinschaften sowie auf alle zugehörigen Informationen betrachtet werden.

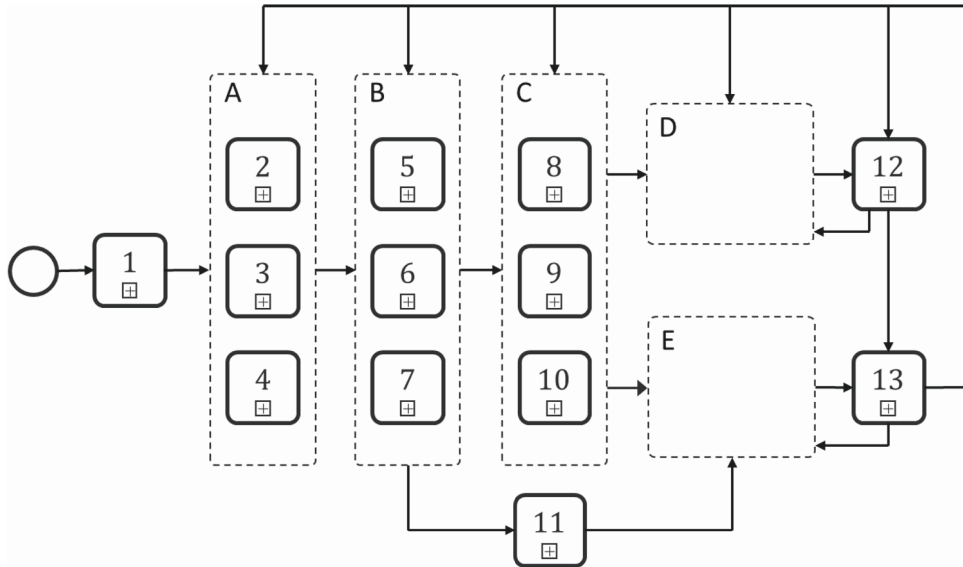
Diese Norm schafft einen Rahmen, um Organisationen dabei zu unterstützen, die zentralen Sicherheitslücken und die Art der Steuerung zu verstehen, die erforderlich ist, um die bestehenden Sicherheitsrisiken auf ein Level zu beschränken, das für alle Beteiligten vertretbar ist. Ihr Zweck liegt nicht darin, die Zusammenarbeit zwischen Organisationen zu unterbinden oder den Nutzen digitaler Techniken im Ingenieurwesen, wie BIM, anderer kooperativer Arbeitsmethoden und digitaler Technologien zu untergraben.

Die in ISO/IEC 27001 enthaltenen Informationssicherheitsanforderungen beziehen sich auf einzelne Organisationen; die Digitalisierung des Ingenieurwesens setzt aber die Weitergabe von Informationen zwischen zahlreichen Organisationen voraus. ISO/IEC 27001 kann deshalb nicht auf diese Organisationen in ihrer Gesamtheit angewendet werden. Diese Norm empfiehlt daher die Einführung eines sicherheitsbewussten, risikobasierten Ansatzes, der sowohl organisationsübergreifend als auch organisationsintern angewendet werden kann. Durch die angemessene und verhältnismäßige Charakteristik des Ansatzes sollte nicht verhindert werden, dass kleine und mittelständische Unternehmen Teil des Bereitstellungsteams sind.

Der sicherheitsbewusste Ansatz kann über den gesamten Lebenszyklus einer Initiative, eines Projekts, eines Assets, eines Produkts oder einer Dienstleistung (egal ob in Planung oder bereits vorhanden) angewendet werden, in dem sensible Informationen erhalten, erstellt, verarbeitet und/oder gespeichert werden.

Bild 1 zeigt, wie dieser sicherheitsbewusste Ansatz mit anderen Strategien, Richtlinien, Plänen und Informationsanforderungen der Organisation für die digitale Bereitstellung, Instandhaltung und den Betrieb von Projekten und Assets mithilfe der BIM abgestimmt werden kann.

Die Einführung der in dieser Norm beschriebenen Maßnahmen wird dabei helfen, das Risiko des Verlusts, des Missbrauchs oder der Modifikation sensibler Informationen zu verringern, wodurch die Sicherheit, den Schutz und die Widerstandsfähigkeit von Assets, Produkten, der bebauten Umgebung oder von Dienstleistungen, die im Zusammenhang mit diesen Informationen bereitgestellt werden, beeinträchtigt werden könnte. Diese Maßnahmen dienen auch dem Schutz vor Verlust, Diebstahl oder Offenlegung kommerzieller und persönlicher Informationen sowie geistigen Eigentums. Derartige Vorfälle können dem Ruf einer Organisation ernsthaft schaden, wenn ihr durch entgangene Chancen und die Abzweigung von Ressourcen für Untersuchungen, Lösungen und Medienaktivitäten zusätzlich zur Unterbrechung und Verzögerung alltäglicher Betriebsaktivitäten geschadet wird. Wenn derartige Vorfälle passieren und Informationen öffentlich zugänglich gemacht wurden, ist es darüber hinaus geradezu unmöglich, alle diese Informationen wiederherzustellen bzw. die anhaltende Weitergabe zu verhindern.



Legende

- A Koordinierte und einheitliche Strategien und Richtlinien
- B Koordinierte und einheitliche Pläne
- C Koordinierte und einheitliche Informationsanforderungen
- D Während der Betriebsphase von Assets durchgeführte Aktivitäten (siehe auch ISO 19650-3)
- E Während der Bereitstellungsphase des Assets durchgeführte Aktivitäten (siehe auch ISO 19650-2)
- 1 Organisationsbezogene Pläne und Ziele
- 2 Strategische(r) Asset-Management-Plan/-Richtlinie (siehe ISO 55000)
- 3 Sicherheitsstrategie
- 4 Weitere organisationsbezogene Strategien und Richtlinien
- 5 Asset-Management-Plan (siehe ISO 55000)
- 6 Sicherheitsmanagementplan
- 7 Weitere organisationsbezogene Pläne
- 8 Asset-Informationsanforderungen (AIR)
- 9 Sicherheitsinformationsanforderungen
- 10 Organisationsbezogene Informationsanforderungen (OIR)
- 11 Strategischer Geschäftsfall und strategischer Auftrag
- 12 Betriebliche Nutzung von Assets
- 13 Leistungsmessung und Verbesserungsmaßnahmen

Bild 1 — Einbindung des sicherheitsbewussten Ansatzes in den umfassenderen BIM-Prozess

1 Anwendungsbereich

Diese Norm legt die Grundsätze und Anforderungen eines ausgereiften sicherheitsbewussten Informationsmanagements fest, das als „Bauwerksinformationsmodellierung (BIM) nach der Normenreihe ISO 19650“ beschrieben werden kann, und behandelt das sicherheitsbewusste Management von sensiblen Informationen, die als Teil von oder im Zusammenhang mit einer Initiative, einem Projekt, einem Asset, einem Produkt oder einer Dienstleistung erhalten, erstellt, verarbeitet und gespeichert werden.

Sie geht auf die Schritte ein, die erforderlich sind, um ein angemessenes und verhältnismäßiges Sicherheitsbewusstsein und eine entsprechende Sicherheitskultur für Organisationen zu schaffen und zu erhalten, die Zugriff auf diese Informationen haben, einschließlich der Notwendigkeit, die Einhaltung der Sicherheitsanforderungen zu überwachen und zu prüfen.

Der beschriebene Ansatz kann über den gesamten Lebenszyklus einer Initiative, eines Projekts, eines Assets, eines Produkts oder einer Dienstleistung (egal ob in Planung oder bereits vorhanden) angewendet werden, in dem sensible Informationen erhalten, erstellt, verarbeitet und/oder gespeichert werden.

Diese Norm ist für jede Organisation vorgesehen, die in den Einsatz des digitalen Ingenieurwesens und zugehöriger Technologien für die Erstellung, den Entwurf, die Konstruktion, die Herstellung, den Betrieb, das Management, die Modifizierung, die Verbesserung, den Rückbau und/oder das Recycling von Assets oder Produkten sowie für die Bereitstellung von Dienstleistungen innerhalb der bebauten Umgebung eingebunden ist. Sie wird auch für Organisationen interessant sein, die ihre kommerziellen Informationen, ihre persönlichen Informationen und ihr geistiges Eigentum schützen möchten.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— IEC Electropedia: unter <http://www.electropedia.org/>

— ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1

Asset

Objekt, Sache oder Einheit, das bzw. die für eine Organisation einen potenziellen oder tatsächlichen Wert besitzt

[QUELLE: ISO 55000:2014]

Anmerkung 1 zum Begriff: Ein Asset kann fest, transportierbar oder beweglich sein. Es kann sich dabei um ein einzelnes Objekt einer Anlage, ein Fahrzeug, ein System von miteinander verbundenen Geräten, einen Raum innerhalb einer Struktur, ein Stück Land, einen ganzen Teil der Infrastruktur, ein ganzes Gebäude oder ein Portfolio von Assets im Zusammenhang mit Land oder Wasser handeln. Es kann Informationen sowohl in digitaler als auch in ausgedruckter Form umfassen.

Anmerkung 2 zum Begriff: Der Wert eines Assets kann sich im Laufe seines Lebens ändern und ein Asset kann am Ende seines Lebens immer noch einen bestimmten Wert besitzen. Der Wert kann materiell oder immateriell, finanziell oder nicht finanziell sein.

3.2

beliebter Ort

Ort oder Umgebung, der bzw. die öffentlich zugänglich ist und aufgrund der hohen Besucherdichte oder der Art des Standorts einem höheren Risiko einer Terrorattacke ausgesetzt ist

Anmerkung 1 zum Begriff: Als beliebte Orte gelten: Sportstadien, Arenas, Orte für Festivals und Musikveranstaltungen, Hotels und Restaurants, Kneipen, Clubs, Bars und Casinos, Haupteinkaufsstraßen, Einkaufszentren und Märkte, Besucherattraktionen, Kinos und Theater, Schulen und Universitäten, Krankenhäuser und Kultstätten, Geschäftszentren und Verkehrsknotenpunkte. Dazu können auch Ereignisse und öffentliche Räume wie Parkanlagen und Plätze gehören.

Anmerkung 2 zum Begriff: Ein beliebter Ort muss nicht zwingend zu jeder Zeit gut besucht sein – eine hohe Besucherdichte kann schwanken und vorübergehend auftreten, wie zum Beispiel bei Sportereignissen oder Open-Air-Festivals.

3.3

Metadaten

Daten über Daten oder Datenelemente

3.4

Wissensbedarf

legitime Forderung eines potentiellen Empfängers von Informationen alle in diesen Informationen enthaltenen sensiblen Daten zu kennen, auf sie zuzugreifen oder sie zu besitzen

3.5

Risikoneigung

Höhe und Art eines Risikos, die eine Organisation anstrebt oder zu halten versucht

3.6

Sicherheit

Zustand des relativen Schutzes vor Bedrohung oder Schädigung durch zufällige, unbeabsichtigte Handlungen oder Ereignisse

3.7

Schutz

Zustand des relativen Schutzes vor Bedrohung oder Schädigung durch absichtliche, unerwünschte, feindliche oder böswillige Handlungen

3.8

Sicherheitsverstoß

Verletzung oder Übertretung der Sicherheit

[QUELLE: ISO 14298:2013]

3.9

Sicherheitsvorfall

verdächtige Handlung oder verdächtiger Umstand, die bzw. der die Sicherheit bedroht

3.10

sicherheitsbewusst

das Verständnis und die routinemäßige Durchführung entsprechender angemessener Sicherheitsmaßnahmen in jeder Geschäftssituation zur Verhinderung und/oder Unterbrechung feindlicher, böswilliger, betrügerischer und krimineller Verhaltensweisen oder Aktivitäten

3.11

sensible Informationen

Verlust, Missbrauch oder Modifikation von Informationen oder unberechtigter Zugriff auf Informationen mit möglichen Folgen:

- negative Auswirkungen auf die Privatsphäre, das Wohlergehen oder die Sicherheit einer oder mehrerer Einzelpersonen;
- Schaden an geistigem Eigentum oder Betriebsgeheimnissen einer Organisation;
- kommerzieller oder wirtschaftlicher Schaden für eine Organisation oder ein Land und/oder
- Gefährdung der Sicherheit, Innen- und Außenpolitik einer Nation

3.12

Restrisiko

Risiko, das nach der Durchführung von Kontrollmaßnahmen verbleibt

[QUELLE: ISO 16530-1:2017]

3.13

Bedrohung

mögliche Ursache eines Vorfalls, die zu einem Schaden führen kann

3.14

oberste Leitung

Person oder Personengruppe, die eine Organisation auf der obersten Ebene führt und steuert

Anmerkung 1 zum Begriff: Die oberste Leitung ist innerhalb der Organisation in der Lage, Verantwortung zu delegieren und Ressourcen bereitzustellen.

Anmerkung 2 zum Begriff: Im Kontext dieser Norm sollte die Leitung als Funktion und nicht als Handlung verstanden werden.

3.15

Sicherheitslücke

Schwäche, die ausgenutzt werden kann, um Schaden zu verursachen

4 Ermittlung des Bedarfs an einem sicherheitsbewussten Ansatz mithilfe eines Prozesses zur Bewertung der Sensitivität

4.1 Bestimmung des Umfangs der Sicherheitsrisiken

4.1.1 Die oberste Leitung einer Organisation, welche Initiativen, Projekte, Assets, Produkte oder Dienstleistungen erstellt, verwaltet, betreibt, abschafft oder umgestaltet, muss den Umfang der Sicherheits-

risiken bestimmen, die durch die bessere Verfügbarkeit von Informationen, die Integration von Dienstleistungen und Systemen sowie durch die erhöhte Abhängigkeit von technologiebasierten Systemen entstehen.

ANMERKUNG Informationen zu Arten von Sicherheitsrisiken, die berücksichtigt werden sollten, sind in Anhang A enthalten.

4.1.2 Wenn zwei oder mehr Organisationen beteiligt sind an:

- a) der Einleitung eines Projekts zur Entwicklung eines/einer oder mehrerer neuer Assets, Produkte oder Dienstleistungen oder Modifizierung bereits vorhandener Assets, Produkte oder Dienstleistungen,
- b) dem Management, dem Betrieb, der Umgestaltung oder der Abschaffung eines oder mehrerer Assets und/oder
- c) der Bereitstellung einer oder mehrerer Asset-basierter Dienstleistungen,

muss die oberste Leitung dieser Organisationen den Umfang der Sicherheitsrisiken bestimmen, die durch die bessere Verfügbarkeit von Informationen, die Integration von Dienstleistungen und Systemen sowie durch die verstärkte Abhängigkeit von technologiebasierten Systemen entstehen.

ANMERKUNG 1 Eine derartige Zusammenarbeit mehrerer Organisationen kann in einer Stadt/Kommune, im Rahmen eines großen, multifunktionalen Entwicklungsprogramms oder bei der Bereitstellung eines Transportsystems vorkommen.

ANMERKUNG 2 Informationen zu Arten von Sicherheitsrisiken, die berücksichtigt werden sollten, sind in Anhang A enthalten.

4.2 Ermittlung der Sensibilität der Organisation

4.2.1 Unter Berücksichtigung des vorhandenen Umfangs von Sicherheitsrisiken muss (müssen) die in 4.1.1 genannte(n) Organisation(en) ermitteln, ob eine Initiative, ein Projekt, ein Asset, ein Produkt oder eine Dienstleistung und alle zugehörigen Informationen, egal ob in Planung oder bereits vorhanden, ganz oder teilweise als sensibel zu betrachten sind.

4.2.2 Ein bauliches Asset gilt ganz oder teilweise als sensibel, wenn es:

- a) kritische nationale Infrastrukturen, die von der Kommunalverwaltung oder der Landesregierung als solche eingestuft werden, umfasst;
- b) eine Abwehr- oder Vollzugsfunktion, eine nationale Sicherheitsfunktion oder eine diplomatische Funktion erfüllt;
- c) sich um einen wirtschaftlichen Standort handelt, an dem wertvolle Werkstoffe, Zahlungsmittel, Arzneimittel, Chemikalien, Ölchemikalien oder Gase erstellt, verarbeitet, gehandelt oder gelagert werden, oder die Rohstoffe für die Herstellung dieser Werkstoffe bereitgestellt oder produziert werden;
- d) sich um eine Sehenswürdigkeit, einen Standort von nationaler Bedeutung oder einen beliebten Ort handelt;
- e) als Ort für sicherheitsrelevante Veranstaltungen genutzt wird oder dafür vorgesehen ist.

ANMERKUNG Die Tatsache, dass die oben genannten Kriterien auf ein bauliches Asset nicht zutreffen, schließt die Anwendung einer höheren Sicherheitsstufe nicht aus, wenn die Organisation(en) dies wünscht (wünschen).

4.2.3 Ein Asset, ein Produkt oder eine Dienstleistung gilt als sensibel, wenn ein ausreichendes Risiko besteht, dass es bzw. sie verwendet wird oder verwendet werden könnte, um die Integrität, die Sicherheit, den Schutz und/oder die Widerstandsfähigkeit eines Assets, Produkts oder einer Dienstleistung oder seine bzw. ihre Funktionsfähigkeit zu beeinträchtigen.

4.2.4 Ein Asset, ein Produkt oder eine Dienstleistung muss auch dann als sensibel eingestuft werden, wenn es bzw. sie die Sicherheit, den Schutz und/oder die Privatsphäre einzelner Personen oder von Gemeinschaften oder deren persönliche Daten maßgeblich beeinflussen könnte.

4.2.5 Wenn Unsicherheit besteht, ob eine Initiative, ein Projekt, ein Asset, ein Produkt oder eine Dienstleistung als sensibel gilt, muss (müssen) die betreffende(n) Organisation(en) bei Sicherheitsberatern, die über entsprechende Fachkompetenz in den erforderlichen Bereichen verfügen, Rat suchen.

ANMERKUNG Informationen zum Einholen einer geeigneten Sicherheitsberatung sind in Anhang A enthalten.

4.3 Ermittlung der Sensibilitäten Dritter

4.3.1 Im Rahmen der Bewertung einer Initiative, eines Projekts, eines Assets, eines Produkts oder einer Dienstleistung muss auch ermittelt werden, ob der Zugriff auf anderweitig nicht öffentlich zugängliche Informationen über eine andere Organisation, deren Assets, Produkte oder Dienstleistungen, erfolgen wird oder bereits erfolgt ist.

ANMERKUNG Anderweitig nicht öffentlich zugängliche Informationen, die sensibel sein könnten, können beispielsweise im Rahmen von physischen Prüfungen unterirdischer Strukturen, von Infrastrukturnetzen und von Systemen auf privatem Gelände entstehen.

4.3.2 Sofern es aus kommerziellen oder lokal bedingten Gründen nicht untersagt ist, muss (müssen) die Organisation(en) mit der betreffenden Organisation in Kontakt treten, um zu bestimmen, ob ein Teil dieser Informationen sensibel ist, und, sollte dies der Fall sein, welche Maßnahmen für ihre Erfassung, Verarbeitung, Speicherung, Weitergabe und Löschung ergriffen werden müssen.

4.4 Dokumentation des Ergebnisses der Sensibilitätsbewertung

Die Organisation(en) muss (müssen) das Ergebnis jedes Sensibilitätsbewertungsprozesses aufzeichnen und aufbewahren, selbst wenn keine Sensibilität festgestellt wurde, und anerkennen, dass das Ergebnis selbst sensibel sein kann.

4.5 Regelmäßige Überprüfung der Sensibilitätsbewertung

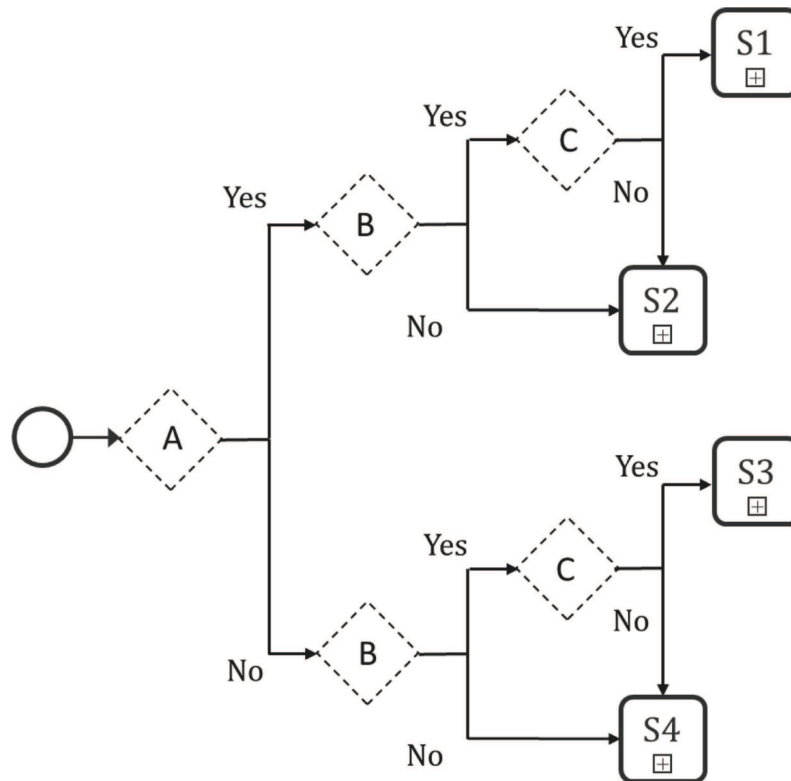
4.5.1 Die Organisation(en) muss (müssen) einen geeigneten Mechanismus für die Durchführung regelmäßiger Überprüfungen vorsehen, bei denen geprüft wird, ob Änderungen an der Sensibilität einer Initiative, eines Projekts, eines Assets, eines Produkts oder einer Dienstleistung, ob aus politischen, ökonomischen, sozialen, technologischen, rechtlichen oder umweltbedingten Gründen, festgestellt werden können.

4.5.2 Eine Überprüfung muss auch durchgeführt werden, wenn sich die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung wesentlich geändert hat, einschließlich hinsichtlich:

- a) des Eigentumsverhältnisses, der Nutzung oder Belegung eines baulichen Assets;
- b) der im Management eines baulichen Assets oder der Herstellung eines Assets oder Produkts verwendeten Prozesse oder Systeme;
- c) der erfassten, verarbeiteten und/oder gespeicherten Informationen;
- d) der bereitgestellten Dienstleistung oder
- e) des Sicherheitskontexts.

4.6 Bestimmung des Bedarfs eines sicherheitsbewussten Ansatzes

Die Organisation(en) muss (müssen) mithilfe des Prozesses zur Einstufung der Sicherheit in Bild 2 bestimmen, ob in Bezug auf die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung ein sicherheitsbewusster Ansatz erforderlich ist.



Legende

- A Gelten die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung sowie die dazugehörigen Informationen, egal ob in Planung oder bereits vorhanden, ganz oder teilweise als sensibel?
- B Erfolgt der Zugriff auf anderweitig nicht öffentlich zugängliche Informationen über eine andere Organisation, deren Assets, Produkte oder Dienstleistungen, oder ist er bereits erfolgt?
- C Gelten die Informationen über eine andere Organisation, ihre Assets, Produkte oder Dienstleistungen, als sensibel?
- S1 Die sensiblen Informationen bezüglich der Initiative, des Projekts, des Assets, des Produkts oder der Dienstleistung sowie die sensiblen Informationen Dritter sind durch Anwendung der Abschnitte 5 bis 10 dieser Norm zu schützen.
- S2 Die sensiblen Informationen bezüglich der Initiative, des Projekts, des Assets, des Produkts oder der Dienstleistung sind durch Anwendung der Abschnitte 5 bis 10 dieser Norm zu schützen.
- S3 Die sensiblen Informationen Dritter sind durch Anwendung der Abschnitte 5 bis 10 dieser Norm zu schützen. Alle sensiblen kommerziellen und persönlichen Informationen sind zu schützen.

Bild 2 — Prozess zur Einstufung der Sicherheit

4.7 Die Organisation(en) muss (müssen) das Ergebnis der Anwendung des Sicherheits-einstufungsprozesses für jede Initiative, jedes Projekt, jedes Asset, jedes Produkt oder jede Dienstleistung, auf die bzw. das es angewendet wurde, dokumentieren, auch wenn kein Bedarf an einem sicherheitsbewussten Ansatz über den Schutz der sensiblen kommerziellen und persönlichen Informationen hinaus ermittelt wurde.

4.8 Sicherheitsbewusster Ansatz erforderlich

4.8.1 Wenn eine Initiative, ein Projekt, ein Asset, ein Produkt oder eine Dienstleistung:

- a) teilweise oder ganz als sensibel eingestuft wurde und/oder
- b) Informationen Dritter enthält, die als sensibel eingestuft wurden,

muss die oberste Leitung der Organisation(en) unter Berücksichtigung der Anforderungen dieser Norm einen angemessenen und verhältnismäßigen sicherheitsbewussten Ansatz entwickeln und implementieren.

4.8.2 Wenn mehr als eine Organisation an der Erstellung, dem Management, dem Betrieb, der Abschaffung oder der Umgestaltung einer Initiative, eines Projekts, eines Assets, eines Produkts oder einer Dienstleistung beteiligt ist, müssen diese unter Berücksichtigung der Anforderungen dieser Norm einen gemeinschaftlichen, angemessenen und verhältnismäßigen sicherheitsbewussten Ansatz entwickeln und implementieren.

4.9 Kein sicherheitsbewusster Ansatz erforderlich

Wenn eine Initiative, ein Projekt, ein Asset, ein Produkt oder eine Dienstleistung als nicht sensibel gilt und keinen Zugriff auf sensible Informationen Dritter hat, muss (müssen) die Organisation(en) abwägen, ob ein Geschäftsnutzen aus der Anwendung eines sicherheitsbewussten Ansatzes gezogen werden kann.

ANMERKUNG 1 Es ist für jede Organisation sinnvoll, entsprechende Schritte zur Minimierung von Bedrohungen durch Betrug und andere kriminelle Aktivitäten sowie durch Sicherheitsvorfälle im Internet vorzunehmen.

ANMERKUNG 2 Es ist sehr wahrscheinlich, dass grundlegende Sicherheitsmaßnahmen bezüglich persönlicher und kommerzieller Informationen in den Bedingungen der Informationsbestellung gefordert werden.

ANMERKUNG 3 Solange die Organisation(en) keine höhere Sicherheitsstufe einführen möchte(n), besteht nach aktueller Bewertung keine Notwendigkeit, die Anforderungen aus den Abschnitten 5 bis 10 dieser Norm auf die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung anzuwenden.

5 Entwicklung des sicherheitsbewussten Ansatzes

5.1 Verwaltung, Rechenschaftspflichten und Zuständigkeiten im Zusammenhang mit dem sicherheitsbewussten Ansatz

5.1.1 Wenn eine Organisation einen sicherheitsbewussten Ansatz entwickelt, muss die oberste Leitung festlegen, wer auf oberster Leitungsebene für die Einführung des sicherheitsbewussten Ansatzes verantwortlich ist.

5.1.2 Wenn zwei oder mehr Organisationen einen gemeinschaftlichen sicherheitsbewussten Ansatz entwickeln, muss die oberste Leitung jeder Organisation einen formalen Mechanismus festlegen für:

- a) den Aufbau der erforderlichen Verwaltungsstruktur, wobei sichergestellt werden muss, dass diese rechtmäßig gebildet ist und dass die Verbindung zwischen dieser Struktur und den betreffenden Organisationen formal dokumentiert und vereinbart ist;

- b) die Einigung auf eine oder mehrere Parteien, die die Entwicklung des Ansatzes anleiten, und, wenn diese Leitungsfunktion über mehrere Organisationen verteilt ist, die Sicherstellung, dass Rechenschaftspflichten und Zuständigkeiten klar sind;
- c) die Ernennung derjenigen Personen, die für die Einführung des sicherheitsbewussten Ansatzes verantwortlich sind und

ANMERKUNG Die ernannten Personen sind zur Rechtsausübung und zur Erfüllung der Pflichten ihrer jeweiligen Organisation bestimmt.

- d) zur Überprüfung und gegebenenfalls zur Änderung der Verwaltungsstruktur und der Ernennungen.

ANMERKUNG Ein gemeinschaftlich vereinbarter sicherheitsbewusster Ansatz sollte widerstandsfähiger als der Ansatz einer allein arbeitenden Organisation sein.

Die Organisation(en), die einen sicherheitsbewussten Ansatz implementiert bzw. implementieren, müssen einzelne Personen festgelegt werden, die verantwortlich sind für:

- a) die Bereitstellung einer ganzheitlichen Betrachtung der Sicherheitsbedrohungen und Sicherheitslücken, die sich aus der Anwendung und der Abhängigkeit von Informations- und Kommunikationstechnologien ergeben, die für die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung relevant sind;
- b) das Angebot von Beratung und Anleitung im Umgang mit den resultierenden Sicherheitsrisiken;
- c) die Leitung der Entwicklung einer Sicherheitsstrategie oder, wenn die Organisation bereits eine Sicherheitsstrategie hat, die Verwaltung der Einbettung dieser zusätzlichen Sicherheitsrisiken sowie Maßnahmen zur Risikominderung (siehe Abschnitt 6);
- d) die Leitung der Entwicklung eines Sicherheitsmanagementplans und Unterstützung bei dessen Implementierung oder, wenn die Organisation bereits über einen Sicherheitsmanagementplan verfügt, die Verwaltung der Einbettung der relevanten Richtlinien und Prozesse in diesen Plan (siehe Abschnitt 7);
- e) die Unterstützung der Einbettung der erforderlichen Sicherheitsanforderungen in alle Dokumente der Beschaffung und Informationsbestellung;
- f) die Vermittlung einer sicherheitsbewussten Kultur, damit alle Mitarbeiter ihre Verantwortung in Bezug auf die Sicherheit verstehen und sich entsprechend verhalten;
- g) die Einweisung der betroffenen Parteien in die entsprechenden Aspekte der Sicherheitsrichtlinien und -prozesse;
- h) die Beratung hinsichtlich des Bedarfs an einer Überprüfung und einer Prüfung der relevanten Sicherheitsdokumente, -richtlinien und -prozesse sowie deren Durchführung;
- i) die Beratung hinsichtlich des Bedarfs an dem Testen der relevanten Sicherheitsmaßnahmen und gegebenenfalls dessen Durchführung oder Beauftragung; und
- j) gegebenenfalls die Konsultation geeigneter Sicherheitsberater, die über entsprechende Fachkompetenz in den erforderlichen Bereichen verfügen, um zusätzliche Unterstützung zu bieten.

5.1.3 Es müssen klare Regeln für die Berichterstattung zwischen den einzelnen Personen, die die in 5.1.3 aufgeführten Aufgaben erfüllen, und der Person, die innerhalb der Organisation für die Sicherheit verantwortlich ist, gelten.

ANMERKUNG Diese Funktion kann von einer ausreichend qualifizierten und erfahrenen Person übernommen werden, die sich innerhalb der Organisation selbst um die Sicherheit und andere Belange kümmert oder für diese verantwortlich ist, oder durch einen geeigneten Fachexperten ausgefüllt werden, der von der Organisation dafür angestellt ist.

5.1.4 Es muss akzeptabel sein, bestimmte Sicherheitsaufgaben oder -pflichten auf einer täglichen Basis durchzuführen (z.B. die Personalsicherheit von der Personalabteilung, die Internetsicherheit vom IT-Manager und die Sicherheit von Assets oder die physische Sicherheit vom Asset-Manager oder Gebäudemanager). Die ernannte(n) Person(en) muss (müssen) aber für die operative Effizienz der einzelnen Sicherheitsaspekte verantwortlich bleiben.

5.2 Beginn der Entwicklung des sicherheitsbewussten Ansatzes

5.2.1 Bei einer Initiative, einem Projekt, einem Asset, einem Produkt oder einer Dienstleistung in Planung muss der sicherheitsbewusste Ansatz in der frühestmöglichen Planungsphase entwickelt werden.

ANMERKUNG Informationen zur Entwicklung, die der Öffentlichkeit zur Verfügung gestellt werden, können von Beginn des Designprozesses an für eine feindliche Auskundschaftung von Interesse sein.

5.2.2 Wenn sich ein Projekt auf die Bereitstellungsphase eines Assets, in der die BIM eingesetzt wird, bezieht, muss der sicherheitsbewusste Ansatz zusammen mit den in ISO 19650-2:2018 beschriebenen Anforderungen entwickelt werden.

5.2.3 Wenn eine Initiative, ein Projekt, ein Asset, ein Produkt oder eine Dienstleistung bereits vorhanden ist, muss der sicherheitsbewusste Ansatz so schnell wie praktisch umsetzbar entwickelt werden, wobei der Umfang der bereits öffentlich zugänglichen Informationen zu berücksichtigen ist.

5.2.4 Wenn sich die Aktivität auf die Betriebsphase eines Assets, in der die BIM eingesetzt wird, bezieht, muss der sicherheitsbewusste Ansatz zusammen mit den in ISO 19650-3:2019 beschriebenen Anforderungen entwickelt werden.

6 Entwicklung einer Sicherheitsstrategie

6.1 Allgemeines

6.1.1 Die Organisation(en) muss (müssen) eine Sicherheitsstrategie entwickeln und aufrechterhalten, die Folgendes einschließen muss:

- a) die Bewertung der spezifischen Sicherheitsrisiken, denen die Organisation(en) durch die bessere Verfügbarkeit von Informationen, die Integration von Dienstleistungen und Systemen sowie durch die erhöhte Abhängigkeit von technologiebasierten Systemen ausgesetzt ist (sind), (siehe 6.2);
- b) die möglichen Maßnahmen zur Minderung dieser Sicherheitsrisiken und die zu implementierenden Maßnahmen (siehe 6.3);
- c) eine Zusammenfassung der hinnehmbaren Sicherheitsrisiken und der hinnehmbaren Restrisiken (siehe 6.4); und
- d) die Mechanismen zur Überprüfung und Aktualisierung der Sicherheitsstrategie (siehe 6.5).

ANMERKUNG ISO 31000:2018 enthält Grundsätze, ein Rahmenwerk und einen Prozess zum allgemeinen Risikomanagement.

6.1.2 Die Sicherheitsstrategie muss die für die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung relevanten Gesetze und Normen berücksichtigen.

6.1.3 Die Sicherheitsstrategie muss von der obersten Leitung der Organisation(en) unterzeichnet werden.

6.1.4 Der Zugriff auf alle Teile der Sicherheitsstrategie, die sensible Aspekte der Initiative, des Projekts, des Assets, des Produkts oder der Dienstleistung beschreiben oder die die ermittelten Sicherheitsrisiken auflisten, darf nur dann erfolgen, wenn diese Informationen bekannt sein müssen, wobei alle derartigen Informationen hinsichtlich ihrer Erstellung, Weitergabe, Verwendung, Speicherung und Löschung der Risikohöhe entsprechenden Sicherheitsmaßnahmen unterzogen werden müssen.

6.2 Bewertung der Sicherheitsrisiken

6.2.1 Die Organisation(en) muss (müssen) zusätzlich zur Berücksichtigung von Chancen Folgendes bewerten:

- a) die potentiellen Bedrohungen;
- b) die möglichen Sicherheitslücken;
- c) die Art des Schadens, der der Initiative, dem Projekt, dem Asset, dem Produkt oder der Dienstleistung sowie dem Personal, den Bürgern und der Umgebung zugefügt werden könnte und
- d) die Wahrscheinlichkeit, dass eine Sicherheitslücke ausgenutzt wird und diese Auswirkungen hervorruft.

ANMERKUNG 1 Wenn Informationen bereits veröffentlicht wurden, sollte in der Risikobewertung berücksichtigt werden, dass es virtuell unmöglich ist, Informationen, die einmal über das Internet oder anderweitig öffentlich zugänglich gemacht wurden, zu löschen, zu vernichten, zu entfernen oder alle Kopien davon zu sichern.

ANMERKUNG 2 Bei der Bewertung der Sicherheitsrisiken kann es zweckdienlich sein, denselben Risikobewertungsansatz zu verwenden, der an anderer Stelle in der Organisation benutzt wird.

6.2.2 Wo zutreffend, müssen in der Sicherheitsrisikobewertung Sicherheitsrisiken im Zusammenhang mit dem Zugriff auf Information anderer Organisationen berücksichtigt werden, die anderweitig nicht öffentlich zugänglich sind.

6.3 Entwicklung von Maßnahmen zur Minderung von Sicherheitsrisiken

6.3.1 Die Organisation(en) muss (müssen) für jedes Sicherheitsrisiko oder jede erkannte Kombination von Risiken mögliche Minderungsmaßnahmen festlegen und dokumentieren.

6.3.2 Dabei muss (müssen) die Organisation(en) die Steuerungen der Personal-, der physischen und der technischen Sicherheit sowie die Anforderungen im Zusammenhang mit dem Management von Informationen berücksichtigen.

ANMERKUNG 1 Informationen zu den zu berücksichtigenden Arten der Steuerung der Personal-, der physischen und der technischen Sicherheit sowie Faktoren im Management von Informationen sind in Anhang B enthalten.

ANMERKUNG 2 Das Zusammenspiel der Steuerungen Personal-, der physischen und der technischen Sicherheit kann von Betrügern ausgenutzt werden, wenn die Verbindungen zwischen diesen Bereichen nicht untersucht worden sind.

ANMERKUNG 3 Die entwickelten Minderungsmaßnahmen sollten dazu dienen, den kommerziellen, wirtschaftlichen und gesellschaftlichen Wert zu erhalten oder zu schützen.

6.3.4 Bei der Bewertung der einzelnen möglichen Minderungsmaßnahmen muss (müssen) die Organisation(en) Folgendes berücksichtigen:

- a) die Kosten der Minderungsmaßnahmen und ihrer Implementierung;
- b) die Risikoreduzierung, die erreicht werden könnte, und die Höhe der Restrisiken;
- c) die vorhersagbare finanzielle Belastung;

- d) andere Auswirkungen, die die Minderungsmaßnahmen auf das Asset haben können (z. B. Nutzbarkeit, Effizienz und Erscheinungsbild);
- e) das Potential der Maßnahme weitere Sicherheitslücken zu schaffen und
- f) ob die Maßnahme einen anderen Geschäftsnutzen hat.

ANMERKUNG Unter Geschäftsnutzen kann die Reduzierung des Gesamtgeschäftsrisikos und die Sicherstellung der Kenntnis über den Wert von Assets, einschließlich Informationen, verstanden werden.

6.3.3 Die Organisation(en) müssen das Ergebnis der Bewertung verwenden, um zu bestimmen, welche Minderungsmaßnahmen, sofern vorhanden, implementiert werden.

ANMERKUNG Eine verhältnismäßige Minderungsmaßnahme sollte pragmatisch, angemessen und kosteneffizient sein.

6.4 Dokumentation der Restrisiken und hinnehmbaren Sicherheitsrisiken

6.4.1 Im Anschluss an diesen Prozess zur Minderung der Sicherheitsrisiken muss (müssen) die Organisation(en) jegliche Restsicherheitsrisiken identifizieren und aufzeichnen.

6.4.2 Die Organisation(en) muss (müssen) die Prozesse zur Sicherheitsrisikobewertung und zur Minderung der Sicherheitsrisiken für diese Restsicherheitsrisiken so lange fortführen, bis ein Punkt erreicht ist, an dem die Risikoneigung der einzelnen Organisation oder des Organisationsverbunds nicht überschritten wird.

6.4.3 Die Organisation(en) muss (müssen) die hinnehmbaren Sicherheitsrisiken dokumentieren.

6.5 Überprüfung der Sicherheitsstrategie

6.5.1 Die Organisation(en) muss (müssen) einen geeigneten Mechanismus zur Durchführung regelmäßiger Überprüfungen der Sicherheitsstrategie, einschließlich der Effektivität der gegenwärtigen Minderungsmaßnahmen festlegen, um ihre weitere Zweckdienlichkeit festzustellen.

6.5.2 Spontane Überprüfungen müssen durchgeführt werden, sobald politische, wirtschaftliche, soziale, organisatorische, technologische, rechtliche oder umweltbedingte Änderungen auftreten, die die Initiative, das Projekt, das Asset, das Produkt oder die Dienstleistung sowie die zugehörigen Informationen maßgeblich beeinflussen könnten.

6.5.3 Die Überprüfungen müssen mögliche Auswirkungen auf vorhandene Informationsbestellungen berücksichtigen, die durch maßgebliche Änderungen an den Minderungsmaßnahmen voraussichtlich beeinflusst werden, insbesondere wenn es sich dabei um eine Änderung des Umfangs handelt.

6.5.4 Im Anschluss an eine regelmäßige oder spontane Überprüfung muss die Sicherheitsstrategie dahingehend aktualisiert werden, dass alle Änderungen von Bedrohungen, Sicherheitslücken, resultierenden Sicherheitsrisiken und/oder Maßnahmen zur Minderung von Sicherheitsrisiken berücksichtigt werden.

6.5.5 Der Vorgang einer jeden Überprüfung muss dokumentiert werden, und diese Aufzeichnungen müssen als Teil der Sicherheitsstrategie aufbewahrt werden.

6.5.6 Der Zugriff auf alle Teile der Überprüfung, die sensible Aspekte der Initiative, des Projekts, des Assets, des Produkts oder der Dienstleistung beschreiben oder die die ermittelten Sicherheitsrisiken auflisten, darf nur dann erfolgen, wenn diese Informationen bekannt sein müssen, wobei alle derartigen Informationen hinsichtlich ihrer Erstellung, Weitergabe, Verwendung, Speicherung und Löschung der Risikohöhe entsprechenden Sicherheitsmaßnahmen unterzogen werden müssen.

7 Entwicklung eines Sicherheitsmanagementplans

7.1 Allgemeines

7.1.1 Die Organisation(en) muss (müssen) einen Sicherheitsmanagementplan entwickeln, aufrechterhalten und einführen, der die Implementierung der im Rahmen der Sicherheitsstrategie festgelegten Minderungsmaßnahmen auf einheitliche und ganzheitliche Weise ermöglicht.

ANMERKUNG Das Sicherheitsmanagement sollte, sofern zutreffend, auf andere gegenwärtige Sicherheitsmanagementrichtlinien und -pläne der Organisation verweisen.

7.1.2 Der Sicherheitsmanagementplan muss in Bezug auf die Organisation(en) und ihr Bereitstellungsteam Folgendes enthalten:

- a) die Richtlinien, die die sicherheitsbezogenen Geschäftsregeln festlegen, welche von den vereinbarten Minderungsmaßnahmen abgeleitet sind;
- b) die von den Sicherheitsrichtlinien abgeleiteten Prozesse sowie Anleitung hinsichtlich ihrer einheitlichen Implementierung;
- c) die Anforderungen bezüglich der Bereitstellung von Informationen gegenüber Dritten (siehe 7.2);
- d) falls anwendbar, logistische Sicherheitsanforderungen (siehe 7.3);
- e) einen Plan zum Management von Sicherheitsverstößen und -vorfällen (siehe Abschnitt 8);
- f) Einzelheiten zur Rechenschaftspflicht und Zuständigkeit im Hinblick auf die Implementierung der verschiedenen Aspekte des Sicherheitsmanagementplans (siehe 7.4);
- g) Überwachungs- und Prüfungsanforderungen, einschließlich Tests der gegenwärtigen Sicherheitsmaßnahmen (siehe 7.5);
- h) die Mechanismen zur Überprüfung und Aktualisierung des Sicherheitsmanagementplans (siehe 7.6).

ANMERKUNG Alle Lücken oder Auslassungen im Sicherheitsmanagementplan führen zu einer verminderten Effektivität der Sicherheitsstrategie und erhöhen das Risiko eines Sicherheitsverstößes oder -vorfalls.

7.1.3 Der Sicherheitsmanagementplan muss dazu verwendet werden, über die in jegliche Dokumente der Beschaffung oder Informationsbestellung eingegliederten Sicherheitsanforderungen zu informieren.

7.2 Anforderungen bezüglich der Bereitstellung von Informationen gegenüber Dritten

7.2.1 Im Sicherheitsmanagementplan müssen die Anforderungen der Organisation(en) zur Durchführung einer Bewertung vor der vollständigen oder teilweisen Weitergabe und/oder der Veröffentlichung eines neuen, modifizierten oder vorhandenen Informationsmodells festgelegt werden.

7.2.2 In einer derartigen Bewertung müssen folgende Fragen geklärt werden (sofern zutreffend):

- a) die Notwendigkeit der Einhaltung rechtlicher und gesetzlich vorgeschriebener Prozesse;
- b) Anfragen von einer Organisation bezüglich Informationen, die den Bestimmungen des öffentlichen Zugangs oder den Rechtsvorschriften zur Transparenz unterliegen und
- c) der Bedarf an Materialien, die bei öffentlichen oder Fachveranstaltungen, in Marketingunterlagen, in technischen, wissenschaftlichen oder anderen Veröffentlichungen und auf Websites verwendet werden können.

7.2.3 Im Rahmen einer Bewertung muss geprüft werden, soweit dies praktisch umsetzbar ist, ob die Informationen oder Informationsmodelle ganz oder teilweise:

- a) sensible Informationen über eine Initiative, ein Projekt, ein Asset, ein Produkt, eine Dienstleistung, eine Einzelperson oder eine Gruppe/Gemeinschaft enthalten oder deren Ableitung ermöglichen;
- b) bei Zusammenstellung mit vorhandenen weitergegebenen oder veröffentlichten Materialien eine Ableitung von sensiblen Informationen zulassen und
- c) sofern zutreffend, dazu beitragen, Informationen zur Nutzungsstruktur von Assets und/oder zum Lebensrhythmus von Einzelpersonen oder Gruppen/Gemeinschaften zu gewinnen, die sonst nicht öffentlich zugänglich sind.

ANMERKUNG Anleitung zu den von dieser Art von Bewertung abzudeckenden Bereichen ist in Anhang C gegeben.

7.2.4 Wenn sich durch die Bewertung herausstellt, dass einer dieser Umstände zutrifft, muss (müssen) die Organisation(en) für die Weitergabe und/oder die Veröffentlichung dieser Informationen einen angemessenen und verhältnismäßigen risikobasierten Ansatz verwenden.

ANMERKUNG Anhang C gibt Orientierung bei der Auswahl möglicher Maßnahmen zur Reduzierung der Sicherheitsrisiken.

7.2.5 Der Zugriff auf alle Teile der Bewertung, die sensible Informationen enthalten, darf nur dann erfolgen, wenn diese Informationen bekannt sein müssen, wobei die enthaltenen Informationen hinsichtlich ihrer Erstellung, Weitergabe, Verwendung, Speicherung und Löschung entsprechenden Sicherheitsmaßnahmen unterzogen werden müssen.

7.3 Logistische Sicherheitsanforderungen

7.3.1 Wo zutreffend, müssen im Sicherheitsmanagementplan angemessene und verhältnismäßige Sicherheitsmaßnahmen im Zusammenhang mit der Installation sensibler Assets und Systeme festgelegt werden.

ANMERKUNG Im Zuge der Entwicklung dieser Maßnahmen muss unter Umständen eine Beratung durch Fachexperten in Anspruch genommen werden.

7.3.2 Die Organisation(en) muss (müssen) Folgendes berücksichtigen:

- a) den Zeitpunkt der Installation von sensiblen, sicherheitsbezogenen Assets oder Systemen, um den Zugriff auf diese Assets oder Bereiche möglichst auf diejenigen Personen zu begrenzen, die wirklich darauf zugreifen müssen;
- b) die Implementierung angemessener und verhältnismäßiger Sicherheitsmaßnahmen zum Schutz sensibler Assets und Systeme, die aus logistischen Gründen eher ergriffen werden müssen als es im Allgemeinen wünschenswert wäre und
- c) die Durchführung angemessener und verhältnismäßiger Maßnahmen, um den Erfolg von Aktionen zur physischen feindlichen Auskundschaftung zu begrenzen oder zu beeinflussen.

7.4 Verwaltung der Rechenschaftspflichten und Zuständigkeiten in Bezug auf die Sicherheit

Für jede Richtlinie im Managementplan muss die Funktion bzw. müssen die Funktionen festgelegt werden, die für ihre Implementierung, Verwaltung, Überwachung und Überprüfung rechenschaftspflichtig und verantwortlich sind.