SNI

Standar Nasional Indonesia

SNI ISO 22301:2014

Keamanan masyarakat — Sistem manajemen kelangsungan usaha – Persyaratan

Societal security – Business continuity management systems — Requirements

(ISO 22301: 2012, IDT)

ICS 03.100.01

Badan Standardisasi Nasional

BSN
Gd. Manggala Wanabakti
Blok IV, Lt. 3,4,7,10.
Telp. +6221-5747043
Fax. +6221-5747045
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Daftar isi

Prakata

Standar Nasional Indonesia (SNI) ISO 22301:2014, *Keamanan masyarakat — Sistem manajemen kelangsungan usaha — Persyaratan*, adalah adopsi identik dari ISO 22301:2012, *Societal security – Business continuity management systems — Requirements*, melalui penerjemahan dua bahasa (*bilingual*). Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya.

Untuk tujuan ini telah dilakukan perubahan editorial berikut:

a) tanda titik telah diganti dengan tanda koma dan sebaliknya untuk penulisan bilangan,

b) beberapa istilah *International Standard* diterjemahkan menjadi standar nasional.

Standar ini dapat diterapkan untuk semua jenis dan ukuran organisasi yang ingin
a) menetapkan, menerapkan, memelihara dan memperbaiki sistem manajemen kelangsungan usahanya,
b) memastikan kesesuaian dengan kebijakan kelangsungan usaha,
c) menunjukkan kesesuaian dengan pihak lain,
d) mendapatkan sertifikasi/registrasi atas sistem manajemen kelangsungan usahanya dari badan sertifikasi pihak ketiga yang terakreditasi, atau
e) memberikan pernyataan telah sesuai dengan standar ini.

Standar ini dapat digunakan untuk menilai kemampuan suatu organisasi dalam memenuhi kewajiban dan kebutuhan kelangsungan usahanya.

Standar ini disusun oleh Panitia Teknis 13-08, Penanggulangan Bencana dan telah dikonsensuskan di Jakarta, pada tanggal 13 Desember 2013 yang dihadiri oleh para pemangku kepentingan terkait yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah.

Beberapa istilah dan definisi tidak secara eksplisit digunakan di dalam batang tubuh standar ini, namun tetap dimasukkan dalam butir 3 standar ini untuk menjaga keidentikan adopsinya terhadap ISO 22301:2012 (E). Beberapa istilah dan definisi tersebut misalnya *maximum acceptable outage (3.25), maximum tolerable period of disruption (3.26), minimum business continuity objective (3.28), recovery point objective (3.44), dan recovery time objective (3.45).*

Selain itu perlu dicatat pula bahwa beberapa istilah telah disesuaikan dengan tujuan penggunaan dalam dokumen ini atau didefinisikan sedikit berbeda dari sumbernya meskipun perbedaannya tidak signifikan dan hanya berbeda karena menggunakan kata-kata lain yang semakna.

Untuk menghindari keraguan maka standar ini disandingkan dengan standar aslinya yaitu ISO 22301:2012 pada kolom sebelah kanan dan pengguna dianjurkan untuk melihat dokumen terkait lain yang menyertai.

ISO 22300:2012, *Societal security -- Terminology* yang dijadikan acuan dalam Pasal 2 Istilah dan definisi telah diadopsi secara identik menjadi SNI ISO 22300:2012, *Keamanan masyarakat – Terminologi.*

0 Pendahuluan

0.1 Umum

Standar ini menetapkan persyaratan untuk mempersiapkan dan mengelola secara efektif suatu Sistem Manajemen Kelangsungan Usaha (SMKU).

SMKU menekankan pentingnya
— memahami kebutuhan organisasi dan perlunya menetapkan kebijakan dan tujuan manajemen kelangsungan usaha,
— menerapkan dan mengoperasikan kendali dan langkah-langkah untuk mengelola segenap kemampuan organisasi dalam pengelolaan insiden yang menggangu,
— memantau dan mengkaji-ulang kinerja dan efektivitas SMKU, dan
— peningkatan terus-menerus berdasarkan pengukuran yang objektif.

Seperti sistem manajemen lainnya, SMKU memiliki komponen utama sebagai berikut:
a) kebijakan;
b) orang dengan tanggung jawab tertentu;
c) proses manajemen yang terkait dengan
   1) kebijakan,
   2) perencanaan,
   3) pelaksanaan dan operasi,
   4) penilaian kinerja,
   5) kaji-ulang manajemen, dan
   6) peningkatan
d) dokumentasi berisi bukti yang dapat diaudit; dan
e) proses manajemen kelangsungan usaha yang relevan bagi organisasi yang bersangkutan.

Kelangsungan usaha berkontribusi positif bagi tercapainya masyarakat yang lebih tangguh. Komunitas yang lebih luas, dan dampak lingkungan organisasi terhadap organisasi, serta organisasi lainnya mungkin perlu dilibatkan dalam proses pemulihan.

0.2 Model "*Plan-Do-Check-Act* (PDCA)"

Standar ini menerapkan model "*Plan-Do-Check-Act*" (PDCA) untuk merencanakan, menetapkan, melaksanakan, mengoperasikan, memantau, mengkaji-ulang, memelihara dan meningkatkan terus-menerus efektivitas SMKU organisasi.

Dengan penerapan model ini terjamin suatu derajat konsistensi dengan standar sistem manajemen lainnya, seperti ISO 9001, *Quality management systems*, ISO 14001, *Environmental management systems*, ISO/IEC 27001, *Information security management systems*, ISO/IEC 20000-1, *Information technology — Service management*, dan ISO 28000, *Specification for security management systems for the supply chain*, sehingga mendukung pelaksanaan dan pengoperasian yang konsisten dan terpadu dengan sistem manajemen terkait.

Gambar 1 memperlihatkan cara SMKU dengan masukan berupa pihak yang berkepentingan dan persyaratan untuk manajemen kelangsungan, melalui tindakan dan proses yang diperlukan, sehingga diperoleh hasil berupa kelangsungan usaha yang terkelola yang memenuhi persyaratan tersebut.

0 Introduction

0.1 General

This standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).

A BCMS emphasizes the importance of
— understanding the organization's needs and the necessity for establishing business continuity management policy and objectives,
— implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents,
— monitoring and reviewing the performance and effectiveness of the BCMS, and
— continual improvement based on objective measurement.

A BCMS, like any other management system, has the following key components:
a) a policy;
b) people with defined responsibilities;
c) management processes relating to
    1) policy,
    2) planning,
    3) implementation and operation,
    4) performance assessment,
    5) management review, and
    6) improvement
d) documentation providing auditable evidence; and
e) any business continuity management processes relevant to the organization.

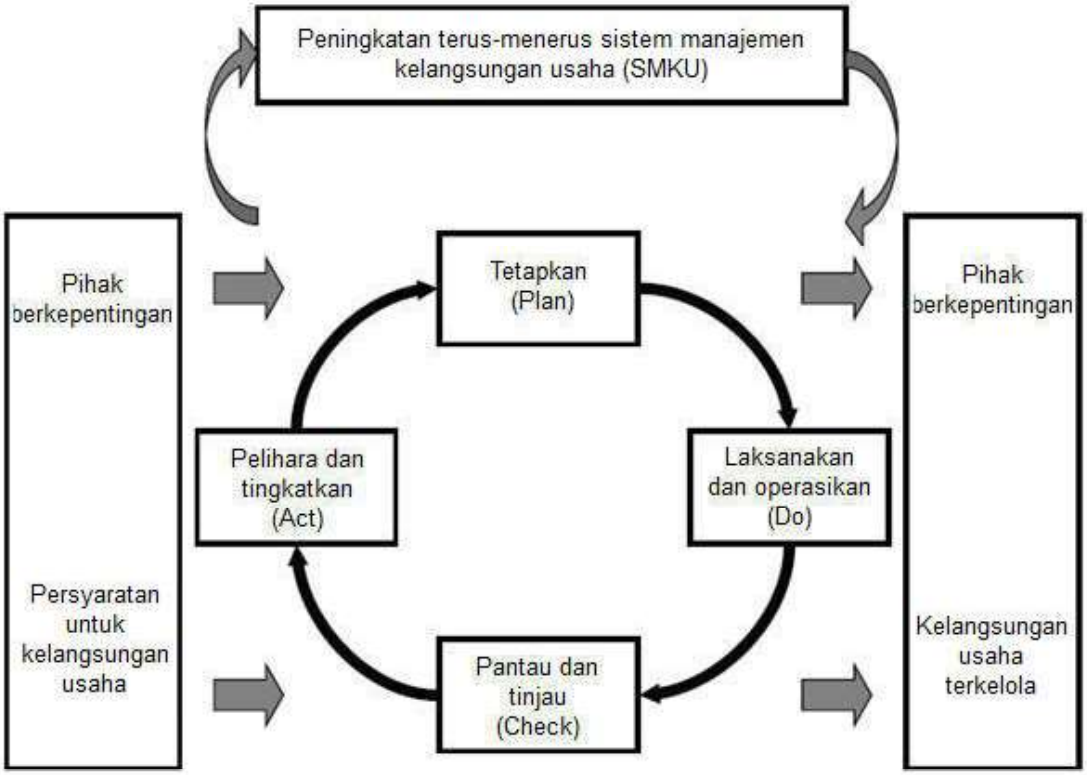
Business continuity contributes to a more resilient society. The wider community and the impact of the organization's environment on the organization and therefore other organizations may need to be involved in the recovery process.

0.2 The Plan-Do-Check-Act (PDCA) model

This standard applies the "Plan-Do-Check-Act" (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards, such as ISO 9001, *Quality management systems*, ISO 14001, *Environmental management systems*, ISO/IEC 27001, *Information security management systems*, ISO/IEC 20000-1, *Information technology — Service management*, and ISO 28000, *Specification for security management systems for the supply chain*, thereby supporting consistent and integrated implementation and operation with related management systems.

Figure 1 illustrates how a BCMS takes as inputs interested parties, requirements for continuity management and, through the necessary actions and processes, produces continuity outcomes (i.e. managed business continuity) that meet those requirements.



Gambar 1 — Model PDCA yang diterapkan pada proses SMKU

Tabel 1 — Penjelasan tentang model PDCA

Plan (Tetapkan)	Tetapkan kebijakan, tujuan, sasaran, kendali, proses dan prosedur kelangsungan usaha yang relevan dengan peningkatan kelangsungan usaha agar dapat memberikan hasil yang sejalan dengan kebijakan dan tujuan organisasi secara keseluruhan.
Do (Laksanakan dan operasikan)	Laksanakan dan operasikan kebijakan, kendali, proses dan prosedur kelangsungan usaha.
Check (Pantau dan kaji-ulang)	Pantau dan kaji-ulang kinerja terhadap kebijakan dan tujuan kelangsungan usaha, laporkan hasilnya kepada manajemen untuk dikaji-ulang, dan tentukan serta berikan wewenang tindakan untuk peningkatan dan peningkatan.
Act **(Pelihara dan tingkatkan)**	Pelihara dan tingkatkan SMKU melalui tindakan korektif, berdasarkan hasil kaji-ulang manajemen dan penilaian kembali lingkup SMKU dan kebijakan serta tujuan kelangsungan usaha.

0.3 Komponen PDCA dalam standar ini

Dalam model *Plan-Do-Check-Act* seperti yang ditunjukkan pada Tabel 1, Butir 4 sampai Butir 10 dalam standar ini mencakup komponen-komponen berikut.

— Pasal 4 adalah komponen dari *Plan*. Di sini disebutkan persyaratan untuk membangun konteks SMKU yang berlaku untuk organisasi, berikut kebutuhan, persyaratan, dan ruang lingkupnya.

— Pasal 5 adalah komponen dari *Plan*. Di sini dirangkum persyaratan khusus untuk peran manajemen puncak dalam SMKU, dan cara kepemimpinan menyampaikan secara jelas ekspektasinya kepada organisasi melalui pernyataan kebijakan.

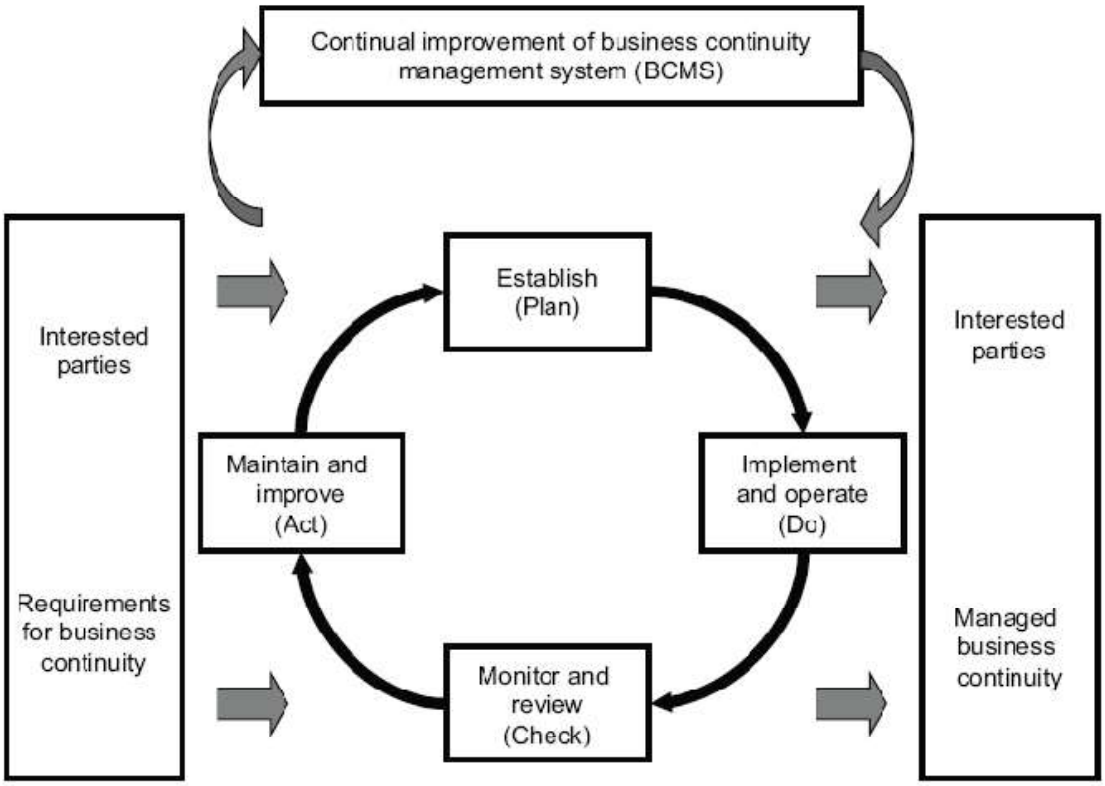


Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model

Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

0.3 Components of PDCA in this standard

In the Plan-Do-Check-Act model as shown in Table 1, Clause 4 through Clause 10 in this standard cover the following components.

— Clause 4 is a component of Plan. It introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements, and scope.

— Clause 5 is a component of Plan. It summarizes the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement.

— Pasal 6 adalah komponen dari *Plan*. Di sini dijelaskan persyaratan yang berkaitan dengan penetapan tujuan strategis dan prinsip-prinsip panduan untuk SMKU secara keseluruhan. Isi dari Butir 6 tidak sama dengan penetapan peluang penanganan risiko yang berasal dari penilaian risiko, serta berbeda dari tujuan pemulihan yang berasal dari analisis dampak usaha (ADU).

CATATAN Persyaratan analisis dampak usaha dan proses penilaian risiko usaha diuraikan secara rinci dalam Butir 8.

— Pasal 7 adalah komponen dari *Plan*. Butir ini mendukung operasi SMKU karena terkait dengan penetapan kompetensi dan komunikasi dengan pihak yang berkepentingan berdasarkan kebutuhan, sambil tetap mendokumentasikan, mengendalikan, memelihara dan menjaga dokumen yang diperlukan.
— Pasal 8 adalah komponen dari *Do*. Di sini didefinisikan persyaratan kelangsungan usaha, ditentukan cara untuk memenuhinya dan dikembangkan prosedur untuk mengelola insiden yang bersifat mengganggu.
— Pasal 9 adalah komponen dari *Check*. Butir ini merangkum persyaratan yang diperlukan untuk mengukur kinerja manajemen kelangsungan usaha (SMKU) sesuai dengan standar ini dan sesuai dengan ekspektasi manajemen, serta mencari umpan balik dari manajemen mengenai ekspektasi ini.
— Pasal 10 adalah komponen dari *Act*. Butir ini mengidentifikasi dan menangani ketidaksesuaian SMKU melalui tindakan korektif.

— Clause 6 is a component of Plan. It describes requirements as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The content of Clause 6 differs from establishing risk treatment opportunities stemming from risk assessment, as well as business impact analysis (BIA) derived recovery objectives.

NOTE The business impact analysis and risk assessment process requirements are detailed in Clause 8.

— Clause 7 is a component of Plan. It supports BCMS operations as they relate to establishing competence and communication on a recurring /as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documentation.
— Clause 8 is a component of Do. It defines business continuity requirements, determines how to address them and develops the procedures to manage a disruptive incident.
— Clause 9 is a component of Check. It summarizes requirements necessary to measure business continuity management performance, BCMS compliance with this standard and management's expectations, and seeks feedback from management regarding expectations.
— Clause 10 is a component of Act. It identifies and acts on BCMS non-conformance through corrective action.

Keamanan masyarakat —Sistem manajemen kelangsungan usaha — Persyaratan

1 Ruang lingkup

Standar ini menetapkan persyaratan untuk merencanakan, menetapkan, menerapkan, mengoperasikan, memantau, mengkaji-ulang, memelihara dan meningkatkan sistem manajemen terdokumentasi untuk melindungi, mengurangi kemungkinan terjadinya, bersiap-siaga, menangani, dan memulihkan diri dari insiden jika terjadi.

Persyaratan yang ditetapkan dalam standar ini bersifat umum dan dimaksudkan untuk dapat diterapkan pada semua organisasi, atau bagiannya, terlepas dari jenis, ukuran dan sifat organisasi. Tingkat penerapan persyaratan ini tergantung pada lingkungan dan kompleksitas operasi organisasi.

Standar ini tidak dimaksudkan untuk menyeragamkan struktur Sistem Manajemen Kelangsungan Usaha (SMKU), melainkan agar organisasi dapat merancang sebuah SMKU yang sesuai dengan kebutuhan dan memenuhi persyaratan pihak berkepentingan. Kebutuhan ini ditentukan oleh persyaratan hukum, peraturan, organisasi dan industri, produk dan jasa, proses yang digunakan, ukuran dan struktur organisasi, dan persyaratan dari pihak berkepentingan.

Standar ini dapat diterapkan untuk semua jenis dan ukuran organisasi yang ingin
a) menetapkan, menerapkan, memelihara dan memperbaiki SMKU,
b) memastikan kesesuaian dengan kebijakan kelangsungan usaha,
c) menunjukkan kesesuaian dengan pihak lain,
d) mendapatkan sertifikasi/registrasi atas SMKU-nya dari badan sertifikasi pihak ketiga yang terakreditasi, atau
e) memberikan pernyataan telah sesuai dengan standar ini.

Standar ini dapat digunakan untuk menilai kemampuan suatu organisasi dalam memenuhi kewajiban dan kebutuhan kelangsungan usahanya.

2 Acuan normatif

Standar ini tidak menggunakan acuan normatif.

3 Istilah dan definisi

Untuk tujuan penggunaan dalam dokumen ini, berlaku istilah dan definisi sebagai berikut.

Societal Security – Buisness continuity management systems – Requirements

1 Scope

This standard for business continuity management specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

The requirements specified in this standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

It is not the intent of this standard to imply uniformity in the structure of a Business Continuity Management System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its interested parties' requirements. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its interested parties.

This standard is applicable to all types and sizes of organizations that wish to
a) establish, implement, maintain and improve a BCMS,
b) ensure conformity with stated business continuity policy,
c) demonstrate conformity to others,
d) seek certification/registration of its BCMS by an accredited third party certification body, or
e) make a self-determination and self-declaration of conformity with this standard.

This standard can be used to assess an organization's ability to meet its own continuity needs and obligations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application.

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

There are no normative references

3 Terms and definitions

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

3.1
aktivitas
proses atau serangkaian proses yang dilakukan oleh sebuah organisasi (atau atas namanya) yang menghasilkan atau mendukung satu atau beberapa produk dan jasa

CONTOH Proses tersebut misalnya rekening, *call center*, TI (teknologi informasi), manufaktur, distribusi.

3.2
audit
proses sistematis, mandiri dan terdokumentasi untuk memperoleh bukti audit dan mengevaluasinya secara objektif untuk menentukan sejauh mana kriteria audit terpenuhi

CATATAN 1 Audit dapat berupa audit internal (pihak pertama) atau audit eksternal (pihak kedua atau pihak ketiga), dan dapat berupa audit gabungan (menggabungkan dua disiplin atau lebih).

CATATAN 2 "Bukti Audit" dan "kriteria audit" didefinisikan dalam ISO 19011.

3.3
kelangsungan usaha
kemampuan organisasi untuk melanjutkan pengiriman produk atau pemberian layanan yang layak setelah adanya insiden yang mengganggu

[SUMBER: ISO 22300]

3.4
manajemen kelangsungan usaha
proses manajemen menyeluruh
- untuk mengidentifikasi ancaman potensial terhadap organisasi dan dampak dari ancaman tersebut jika terwujud terhadap operasi usaha
- serta menyediakan kerangka kerja bagi pembentukan ketahanan organisasi agar mampu memberikan respon efektif untuk menjaga kepentingan para pemangku kepentingan utama, reputasi, kegiatan yang menghasilkan citra dan nilai

3.5
Sistem Manajemen Kelangsungan Usaha (SMKU)
bagian dari sistem manajemen yang membentuk, mengimplementasikan, mengoperasikan, memantau, mengkaji-ulang, memelihara dan meningkatkan kelangsungan usaha

CATATAN Sistem manajemen mencakup struktur organisasi, kebijakan, kegiatan perencanaan, tanggung jawab, prosedur, proses dan sumber daya.

3.6
rencana kelangsungan usaha
prosedur terdokumentasi yang memandu organisasi untuk merespon, memulihkan, melanjutkan, dan mengembalikan organisasi ke tingkat awal operasi setelah terjadi gangguan

CATATAN Biasanya rencana ini mencakup sumber daya, layanan dan kegiatan yang dibutuhkan untuk menjamin kelangsungan fungsi usaha yang vital.

3.7
program kelangsungan usaha
proses manajemen dan tata kelola terus-menerus yang didukung oleh manajemen puncak dan sumber daya yang tepat untuk menerapkan dan memelihara manajemen kelangsungan usaha

3.1
activity
process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services

EXAMPLE Such processes include accounts, call centre, IT, manufacture, distribution.

3.2
audit
systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

NOTE 1 An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

NOTE 2 "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.3
business continuity
capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident

[SOURCE: ISO 22300]

3.4
business continuity management
holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

3.5
business continuity management system
BCMS
part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity

NOTE The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.

3.6
business continuity plan
documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

NOTE Typically this covers resources, services and activities required to ensure the continuity of critical business functions.

3.7
business continuity programme
ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management

3.8
analisis dampak usaha
proses menganalisis aktivitas dan efek dari suatu gangguan usaha terhadap aktivitas tersebut

[SUMBER: ISO 22300, disesuaikan]

3.9
kompetensi
kemampuan dalam menerapkan pengetahuan dan keterampilan untuk mencapai hasil yang diinginkan

3.10
kesesuaian
terpenuhinya suatu persyaratan

[SUMBER: ISO 22300]

3.11
peningkatan terus-menerus
kegiatan berulang untuk meningkatkan kinerja

[SUMBER: ISO 22300, disesuaikan]

3.12
koreksi
tindakan untuk menghilangkan ketidaksesuaian

[SUMBER: ISO 22300]

3.13
tindakan korektif
tindakan untuk menghilangkan penyebab ketidaksesuaian dan mencegah terulang kembali

CATATAN Dalam hal hasil yang tidak diinginkan lainnya, diperlukan tindakan untuk meminimalkan atau menghilangkan penyebab dan untuk mengurangi dampak atau mencegah terulang kembali. Tindakan tersebut berada di luar konsep "tindakan korektif" dalam pengertian definisi ini.

[SUMBER: ISO 22300]

3.14
dokumen
informasi dan media pendukungnya

CATATAN 1 Medianya dapat berupa kertas, disket komputer magnetik, elektronik atau optik, foto atau sampel master, atau kombinasi dari semuanya.

CATATAN 2 Sekumpulan dokumen, misalnya spesifikasi dan rekaman, sering kali disebut "dokumentasi".

3.15
informasi terdokumentasi
informasi yang harus dikendalikan dan dikelola oleh organisasi dan termasuk media penyimpannya

CATATAN 1 Informasi terdokumentasi bisa dalam format dan media apapun dari sumber manapun.

3.8
business impact analysis
process of analyzing actitivites and the effect that a business disruption might have upon them

[SOURCE: ISO 22300]

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
conformity
fulfilment of a requirement

[SOURCE: ISO 22300]

3.11
continual improvement
recurring activity to enhance performance

[SOURCE: ISO 22300]

3.12
correction
action to eliminate a detected nonconformity

[SOURCE: ISO 22300]

3.13
corrective action
action to eliminate the cause of a nonconformity and to prevent recurrence

NOTE In the case of other undesirable outcomes, action is necessary to minimize or eliminate causes and to reduce impact or prevent recurrence. Such actions fall outside the concept of “corrective action” in the sense of this definition.

[SOURCE: ISO 22300]

3.14
document
information and its supporting medium

NOTE 1 The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or a combination thereof.

NOTE 2 A set of documents, for example specifications and records, is frequently called “documentation”.

3.15
documented information
information required to be controlled and maintained by an organization and the medium on which it is contained

NOTE 1 Documented information can be in any format and media from any source.

CATATAN 2 Informasi terdokumentasi dapat berarti
— sistem manajemen, termasuk proses yang terkait;
— informasi yang dibuat untuk dioperasikan oleh organisasi (dokumentasi);
— bukti hasil yang dicapai (rekaman).

3.16
efektivitas
ukuran terealisasinya kegiatan dan tercapainya hasil yang direncanakan

[SUMBER: ISO 22300]

3.17
kejadian
berlangsungnya atau terjadinya perubahan serangkaian keadaan tertentu

CATATAN 1 Suatu kejadian dapat terdiri dari satu kejadian atau lebih, dan dapat diakibatkan oleh beberapa sebab.

CATATAN 2 Suatu kejadian dapat terdiri atas hal yang tidak terjadi.

CATATAN 3 Kejadian kadang-kadang dapat disebut sebagai "insiden" atau "kecelakaan".

CATATAN 4 Suatu kejadian tanpa konsekuensi juga dapat disebut sebagai "nyaris", "insiden", "hampir kena" atau "luput".

[SUMBER: ISO/IEC Guide 73]

3.18
latihan
proses untuk melatih, menilai, mempraktikkan, dan meningkatkan kinerja dalam sebuah organisasi

CATATAN 1 Latihan dapat digunakan untuk memvalidasi kebijakan, rencana, prosedur, pelatihan, peralatan, dan perjanjian antar-organisasi; mengklarifikasi dan melatih personel dalam peran dan tanggung jawab; meningkatkan koordinasi dan komunikasi antar-organisasi, mengidentifikasi kesenjangan sumber daya, meningkatkan kinerja individu dan mengidentifikasi peluang untuk peningkatan, dan kesempatan yang terkontrol untuk berlatih improvisasi.

CATATAN 2 Ujian adalah jenis latihan yang unik dan khusus, yang menggabungkan harapan elemen lulus atau gagal dalam sasaran atau tujuan dari latihan yang sedang direncanakan.

[SUMBER: ISO 22300, disesuaikan]

3.19
insiden
situasi yang bisa berupa (atau dapat menjurus pada) gangguan, kerugian, keadaan darurat, atau krisis

[SUMBER: ISO 22300]

3.20
infrastruktur
sistem fasilitas, peralatan dan layanan yang diperlukan untuk operasi organisasi

NOTE 2 Documented information can refer to
— the management system, including related processes;
— information created in order for the organization to operate (documentation);
— evidence of results achieved (records).

3.16
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 22300]

3.17
event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

NOTE 4 An event without consequences may also be referred to as a “near miss”, “incident”, “near hit”, “close call”.

[SOURCE: ISO/IEC Guide 73]

3.18
exercise
process to train for, assess, practice, and improve performance in an organization

NOTE 1 Exercises can be used for: validating policies, plans, procedures, training, equipment, and inter-organizational agreements; clarifying and training personnel in roles and responsibilities; improving inter-organizational coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement, and controlled opportunity to practice improvisation.

NOTE 2 A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

[SOURCE: ISO 22300]

3.19
incident
situation that might be, or could lead to, a disruption, loss, emergency or crisis

[SOURCE: ISO 22300]

3.20
infrastructure
system of facilities, equipment and services needed for the operation of an organization

3.21
pihak berkepentingan
pemangku kepentingan
orang atau organisasi yang dapat mempengaruhi, dipengaruhi oleh, atau menganggap diri mereka dipengaruhi oleh keputusan atau kegiatan

CATATAN Dalam hal ini bisa juga seseorang atau sekelompok orang yang memiliki kepentingan dalam keputusan atau aktivitas organisasi.

3.22
audit internal
audit yang dilakukan oleh, atau atas nama, organisasi itu sendiri untuk kaji ulang manajemen dan tujuan internal lainnya, dan yang mungkin membentuk dasar bagi organisasi untuk swa-deklarasi kesesuaian

CATATAN Dalam banyak kasus, terutama di organisasi kecil, kemandirian dapat ditunjukkan dengan kebebasan dari tanggung jawab atas kegiatan yang sedang diaudit.

3.23
permohonan pemberlakuan kelangsungan usaha
tindakan penyampaian pernyataan bahwa pengaturan kelangsungan usaha organisasi perlu diberlakukan untuk melanjutkan pengiriman produk atau jasa utama

3.24
sistem manajemen
perangkat unsur organisasi yang saling terkait atau berinteraksi untuk menetapkan kebijakan dan tujuan, dan proses untuk mencapai tujuan tersebut

CATATAN 1 Satu sistem manajemen dapat menangani satu atau beberapa disiplin.

CATATAN 2 Unsur-unsur sistem meliputi struktur organisasi, peran dan tanggung jawab, perencanaan, operasi, dll.

CATATAN 3 Lingkup sistem manajemen dapat mencakup seluruh organisasi, fungsi organisasi tertentu, bagian organisasi tertentu, atau satu atau beberapa fungsi lintas organisasi.

3.25
***outage* maksimum yang dapat diterima**
OMD
jangka waktu yang dibutuhkan untuk tidak dapat diterimanya dampak buruk yang mungkin timbul akibat dari tidak menyediakan produk/layanan atau melakukan suatu kegiatan

CATATAN Lihat juga toleransi waktu gangguan maksimum.

3.26
toleransi waktu gangguan maksimum
TWGM
jangka waktu yang dibutuhkan untuk tidak dapat diterimanya dampak buruk yang mungkin timbul akibat dari tidak menyediakan produk/layanan atau melakukan suatu kegiatan

CATATAN Lihat juga *outage* maksimum yang dapat diterima (3.25).

3.27
pengukuran
proses untuk menentukan suatu nilai

3.21
interested party
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE This can be an individual or group that has an interest in any decision or activity of an organization.

3.22
internal audit
audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's self-declaration of conformity

NOTE In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

3.23
invocation
act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key products or services

3.24
management system
set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives

NOTE 1 A management system can address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

NOTE 3 The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.25
maximum acceptable outage
MAO
time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

NOTE See also maximum tolerable period of disruption.

3.26
maximum tolerable period of disruption
MTPD
time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

NOTE See also maximum acceptable outage.

3.27
measurement
process to determine a value

3.28
tujuan kelangsungan usaha minimum
TKUM
tingkat minimum layanan dan/atau produk agar dicapai tujuan usaha organisasi selama berlangsungnya gangguan

3.29
pemantauan
menentukan status sistem, proses atau kegiatan

CATATAN Untuk menentukan status mungkin dibutuhkan pemeriksaan, pengawasan atau pengamatan secara cermat.

3.30
kesepakatan saling bantu
kesepahaman yang diatur sebelumnya antara dua atau lebih pihak untuk saling memberi bantuan

[SUMBER: ISO 22300]

3.31
ketidaksesuaian
tidak terpenuhinya suatu persyaratan

[SUMBER: ISO 22300]

3.32
tujuan
hasil yang ingin dicapai

CATATAN 1 Tujuan dapat bersifat strategis, taktis atau operasional.

CATATAN 2 Tujuan dapat berhubungan dengan disiplin ilmu yang berbeda (seperti sasaran keuangan, kesehatan dan keselamatan, serta sasaran lingkungan) dan dapat diterapkan pada tingkat yang berbeda pula (seperti tingkat strategis, lingkup-organisasi, proyek, produk, dan proses).

CATATAN 3 Tujuan dapat dinyatakan dengan cara lain, misalnya sebagai hasil yang diinginkan, maksud, kriteria operasional, sebagai tujuan keamanan masyarakat atau dengan penggunaan kata-kata lain dengan arti yang sama (misalnya tujuan, sasaran, atau target).

CATATAN 4 Dalam konteks standar sistem manajemen keamanan masyarakat, tujuan keamanan masyarakat ditetapkan oleh organisasi, konsisten dengan kebijakan keamanan masyarakat, untuk mencapai hasil tertentu.

3.33
organisasi
orang atau sekelompok orang yang memiliki fungsi sendiri dengan tanggung jawab, wewenang dan hubungan untuk mencapai tujuannya

CATATAN 1 Konsep organisasi mencakup, namun tidak terbatas pada perusahaan, korporasi, firma, perusahaan, otoritas, kemitraan, pedagang-tunggal, yayasan amal atau lembaga, atau bagian atau kombinasi dari semuanya, baik berkelompok atau tidak, pemerintah atau swasta.

CATATAN 2 Untuk organisasi dengan lebih dari satu unit operasi, satu unit dapat dianggap sebagai sebuah organisasi.

3.28
minimum business continuity objective
MBCO
minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption

3.29
monitoring
determining the status of a system, a process or an activity

NOTE To determine the status there may be a need to check, supervise or critically observe.

3.30
mutual aid agreement
pre-arranged understanding between two or more entities to render assistance to each other

[SOURCE: ISO 22300]

3.31
nonconformity
non-fulfillment of a requirement

[SOURCE: ISO 22300]

3.32
objective
result to be achieved

NOTE 1 An objective can be strategic, tactical or operational.

NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a societal security objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 In the context of societal security management systems standards, societal security objectives are set by the organization, consistent with the societal security policy, to achieve specific results.

3.33
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE 1 The concept of organization includes, but is not limited to company, corporation, firm, enterprise, authority, partnership, sole-trader, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

NOTE 2 For organizations with more than one operating unit, a single unit may be defined as an organization.

3.34
alih-daya
melakukan pengaturan sedemikian supaya suatu organisasi eksternal melakukan sebagian fungsi atau proses dari organisasi

CATATAN Sebuah organisasi eksternal berada di luar lingkup sistem manajemen, meskipun fungsi atau proses yang dialih-dayakan masuk dalam lingkup

3.35
kinerja
hasil yang terukur

CATATAN 1 Kinerja dapat terkait baik dengan temuan kuantitatif atau kualitatif.

CATATAN 2 Kinerja dapat terkait dengan pengelolaan kegiatan, proses, produk (termasuk jasa), sistem, atau organisasi.

3.36
evaluasi kinerja
proses penentuan hasil yang terukur

3.37
personel
orang yang bekerja untuk dan dalam kendali organisasi

CATATAN Personel mencakup, namun tidak terbatas pada, karyawan, staf paruh-waktu, dan staf tetap.

3.38
kebijakan
maksud dan arah organisasi yang dinyatakan secara resmi oleh manajemen puncak

3.39
prosedur
cara tertentu untuk melaksanakan kegiatan atau proses

3.40
proses
perangkat kegiatan saling terkait atau berinteraksi yang mengubah input menjadi output

3.41
produk dan layanan
hasil bermanfaat yang diberikan oleh organisasi kepada pelanggan, penerima layanan, dan pihak berkepentingan, misalnya barang manufaktur, asuransi mobil dan perawatan masyarakat

3.42
kegiatan prioritas
kegiatan yang harus diberikan prioritas setelah terjadinya insiden untuk mengurangi dampak

CATATAN Istilah umum yang digunakan untuk menggambarkan aktivitas dalam kelompok ini antara lain: kritis, esensial, vital, mendesak, dan penting.

[SUMBER: ISO 22300]

3.34
outsource, verb
make an arrangement where an external organization performs part of an organization's function or process

NOTE An external organization is outside the scope of the management system, although the outsourced function or process is within the scope.

3.35
performance
measurable result

NOTE 1 Performance can relate either to quantitative or qualitative findings.

NOTE 2 Performance can relate to the management of activities, processes, products (including services), systems, or organizations.

3.36
performance evaluation
process of determining measurable results

3.37
personnel
people working for and under the control of the organization

NOTE The concept of personnel includes, but is not limited to employees, part-time staff, and agency staff.

3.38
policy
intentions and direction of an organization as formally expressed by its top management

3.39
procedure
specified way to carry out an activity or a process

3.40
process
set of interrelated or interacting activities which transforms inputs into outputs

3.41
products and services
beneficial outcomes provided by an organization to its customers, recipients and interested parties, e.g. manufactured items, car insurance and community nursing

3.42
prioritized activities
activities to which priority must be given following an incident in order to mitigate impacts

NOTE Terms in common use to describe activities within this group include: critical, essential, vital, urgent, and key.

[SOURCE: ISO 22300]

3.43
catatan
pernyataan tentang hasil yang dicapai atau bukti dari kegiatan yang dilakukan

3.44
tujuan titik pemulihan
TTP
posisi tempat informasi yang harus digunakan kembali agar kegiatan dapat dilanjutkan

CATATAN Bisa juga disebut sebagai "kehilangan data maksimum.

3.45
tujuan waktu pemulihan
TWP
periode waktu setelah insiden ketika
— produk atau layanan harus dilanjutkan, atau
— kegiatan harus dilanjutkan, atau
— sumber daya harus dipulihkan

CATATAN Untuk produk, jasa dan kegiatan, tujuan waktu pemulihan harus lebih singkat dari MAO (3.25) atau MTPD (3.26).

3.46
persyaratan
kebutuhan atau ekspektasi yang dinyatakan, tersirat secara umum atau sebagai kewajiban

CATATAN 1 "Tersirat secara umum" berarti bahwa secara umum organisasi dan pihak berkepentingan menyampaikan secara tersirat kebutuhan atau ekspektasi tersebut.

CATATAN 2 Persyaratan tertentu berarti persyaratan yang dinyatakan, misalnya dalam informasi terdokumentasi.

3.47
sumber daya
semua aset, orang, keterampilan, informasi, teknologi (termasuk pabrik dan peralatan), bangunan, dan perlengkapan dan informasi (baik elektronik atau bukan) yang harus dimiliki dan tersedia untuk digunakan bila diperlukan oleh organisasi dalam beroperasi dan memenuhi tujuannya

3.48
risiko
efek ketidakpastian terhadap tujuan

CATATAN 1 Efek adalah penyimpangan dari prospek yang diharapkan — bisa bersifat positif atau negatif.

CATATAN 2 Tujuan dapat memiliki aspek yang berbeda (seperti sasaran keuangan, kesehatan dan keselamatan, serta lingkungan) dan dapat diterapkan pada tingkat yang berbeda (misalnya tingkat strategis, organisasi, proyek, produk, dan proses). Tujuan dapat dinyatakan dengan cara lain, misalnya sebagai hasil yang diinginkan, maksud, kriteria operasional, sebagai tujuan kelangsungan usaha atau dengan penggunaan kata-kata lain yang semakna (misalnya tujuan, sasaran, atau target).

CATATAN 3 Risiko sering dikaitkan dengan peristiwa yang kemungkinan besar terjadi (Guide 73, 3.5.1.3) dan konsekuensinya (Guide 73, 3.6.1.3), atau kombinasi keduanya.

CATATAN 4 Risiko sering dinyatakan dalam bentuk kombinasi antara konsekuensi suatu kejadian (termasuk perubahan lingkungan) dan kemungkinan peristiwa yang terkait (Guide 73, 3.6.1.1).

3.43
record
statement of results achieved or evidence of activities performed

3.44
recovery point objective
RPO
point to which information used by an activity must be restore to enable the activity to operate on resumption

NOTE Can also be referred to as “maximum data loss”.

3.45
recovery time objective
RTO
period of time following an incident within which
— product or service must be resumed, or
— activity must be resumed, or
— resources must be recovered

NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

3.46
requirement
need or expectation that is stated, generally implied or obligatory

NOTE 1 “Generally implied” means that it is a custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

NOTE 2 A specified requirement is one that is stated, for example in documented information.

3.47
resources
all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective

3.48
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a business continuity objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 3 Risk is often characterize by reference to potential events (Guide 73, 3.5.1.3) and consequences (Guide 73, 3.6.1.3), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (Guide 73, 3.6.1.1) of occurrence.

CATATAN 5 Ketidakpastian adalah tingkat ketidakcukupan informasi, pemahaman atau pengetahuan tentang peristiwa, konsekuensinya, atau kemungkinannya

CATATAN 6 Dalam konteks standar sistem manajemen kelangsungan usaha, tujuan kelangsungan usaha ditetapkan oleh organisasi, konsisten dengan kebijakan kelangsungan usaha, untuk mencapai hasil tertentu. Ketika menerapkan istilah risiko dan komponen manajemen risiko, hal ini harus dikaitkan dengan tujuan organisasi yang meliputi, namun tidak terbatas pada, tujuan kelangsungan usaha sebagaimana ditentukan dalam butir 6.2.

[SUMBER: ISO/IEC Guide 73]

3.49
***risk appetite* (kesanggupan menanggung risiko)**
besaran dan jenis risiko yang diperkirakan sanggup ditanggung organisasi

3.50
penilaian risiko
keseluruhan proses identifikasi, analisis dan evaluasi risiko

[SUMBER: ISO Guide 73, disesuaikan]

3.51
manajemen risiko
kegiatan terkoordinasi yang terkait dengan risiko untuk mengarahkan dan mengendalikan organisasi

[SUMBER: ISO Guide 73]

3.52
pengujian
prosedur evaluasi; alat untuk menentukan keberadaan, kualitas, atau kebenaran sesuatu

CATATAN 1 Pengujian dapat disebut juga sebagai "percobaan".

CATATAN 2 Pengujian sering diterapkan untuk rencana pendukung.

[SUMBER: ISO 22300, disesuaikan]

3.53
manajemen puncak
orang atau sekelompok orang yang mengarahkan dan mengendalikan organisasi pada tingkat tertinggi

CATATAN 1 Manajemen puncak memiliki kekuasaan untuk mendelegasikan wewenang dan menyediakan sumber daya dalam organisasi.

CATATAN 2 Jika lingkup sistem manajemen hanya mencakup bagian dari organisasi maka manajemen puncak adalah orang-orang yang mengarahkan dan mengendalikan bagian dari organisasi tersebut.

3.54
verifikasi
konfirmasi, melalui penyediaan bukti, bahwa persyaratan yang ditentukan telah terpenuhi

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood

NOTE 6 In the context of business continuity management system standards, business continuity objectives are set by the organization, consistent with the business continuity policy, to achieve specific results. When applying the term risk and components of risk management, this should be related to the objectives of the organization that include, but are notlimited to the business continuity objectives as specified in 6.2.

[SOURCE: ISO/IEC Guide 73]

3.49
risk appetite
amount and type of risk that an organization is willing to pursue or retain

3.50
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO Guide 73]

3.51
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO Guide 73]

3.52
testing
procedure for evaluation; a means of determining the presence, quality, or veracity of something

NOTE 1 Testing may be referred to a “trial”.

NOTE 2 Testing is often applied to supporting plans.

[SOURCE: ISO 22300]

3.53
top management
person or group of people who directs and controls an organization at the highest level

NOTE 1 Top management has the power to delegate authority and provide resources within the organization.

NOTE 2 If the scope of the management system covers only part of an organization then top management refers to those who direct and control that part of the organization.

3.54
verification
confirmation, through the provision of evidence, that specified requirements have been fulfilled

3.55
lingkungan kerja
seperangkat kondisi pada saat pekerjaan sedang dilakukan

CATATAN Kondisi mencakup faktor fisik, sosial, psikologis dan lingkungan (seperti temperatur, sistem pengakuan, ergonomik dan suasana kerja).

[SUMBER: ISO 22300, disesuaikan]

4 Konteks organisasi

4.1 Pemahaman organisasi dan konteksnya

Organisasi harus menetapkan isu eksternal dan internal yang relevan dengan tujuan organisasi dan yang mempengaruhi kemampuannya untuk mencapai hasil yang diharapkan dari SMKU nya.

Isu-isu ini harus diperhitungkan ketika menetapkan, menerapkan dan memelihara SMKU organisasi.
Organisasi harus mengidentifikasi dan mendokumentasikan hal berikut ini:
a) kegiatan, fungsi, layanan, produk, kemitraan, rantai pasokan, hubungan dengan pihak berkepentingan, dan dampak potensial terkait dengan insiden mengganggu;
b) hubungan antara kebijakan kelangsungan usaha dan tujuan organisasi dan kebijakan lainnya, termasuk strategi manajemen risiko secara keseluruhan, dan
c) risiko yang dapat ditangani oleh organisasi

Dalam penetapan konteks, organisasi harus
1) menyatakan secara jelas tujuannya, termasuk tujuan yang terkait dengan kelangsungan usaha,
2) menentukan faktor eksternal dan internal penyebab ketidakpastian yang menimbulkan risiko,
3) menetapkan kriteria risiko dengan mempertimbangkan risiko yang dapat ditangani, dan
4) mendefinisikan tujuan dari SMKU.

4.2 Memahami kebutuhan dan ekspektasi pihak berkepentingan

4.2.1 Umum

Ketika membangun SMKU, organisasi harus menetapkan
a) pihak berkepentingan yang relevan dengan SMKU, dan
b) persyaratan dari pihak berkepentingan ini (yaitu kebutuhan dan ekspektasi mereka, baik yang dinyatakan, tersirat maupun sebagai kewajiban).

4.2.2 Persyaratan peraturan dan perundang-undangan

Organisasi harus menetapkan, menerapkan dan memelihara prosedur untuk mengidentifikasi, mengakses, dan menilai persyaratan hukum dan peraturan yang berlaku yang diikuti organisasi yang terkait dengan keberlanjutan operasi, produk dan jasa, serta minat dari pihak berkepentingan yang relevan.

3.55
work environment
set of conditions under which work is performed

NOTE Conditions include physical, social, psychological and environmental factors (such as temperature, recognition schemes, ergonomics and atmospheric composition.

[SOURCE: ISO 22300]

NOTE Terms in common use to describe activities within this group include: critical, essential, vital, urgent and key.

4 Context of the organization

4.1 Understanding of the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its BCMS.

These issues shall be taken into account when establishing, implementing and maintaining the organization's BCMS.

The organization shall identify and document the following:
a) the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident;
b) links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy; and
c) the organization's risk appetite.

In establishing the context, the organization shall
1) articulate its objectives, including those concerned with business continuity,
2) define the external and internal factors that create the uncertainty that gives rise to risk,
3) set risk criteria taking into account the risk appetite, and
4) define the purpose of the BCMS.

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

When establishing its BCMS, the organization shall determine
a) the interested parties that are relevant to the BCMS, and
b) the requirements of these interested parties (i.e. their needs and expectations whether stated, generally implied or obligatory).

4.2.2 Legal and regulatory requirements

The organization shall establish, implement and maintain a procedure(s) to identify, have access to, and assess the applicable legal and regulatory requirements to which the organization subscribes related to the continuity of its operations, products and services, as well as the interests of relevant interested parties.

Organisasi harus memastikan bahwa persyaratan hukum, peraturan dan persyaratan lainnya yang berlaku bagi organisasi diperhitungkan dalam membangun, melaksanakan dan memelihara SMKU nya

Organisasi harus mendokumentasikan informasi ini dan menjaga agar selalu mutakhir. Hal baru atau variasi terhadap persyaratan hukum, peraturan dan persyaratan lainnya harus dikomunikasikan kepada karyawan yang terkena dampak dan pihak lain yang berkepentingan.

4.3 Menentukan lingkup sistem manajemen

4.3.1 Umum

Organisasi harus menentukan batas-batas penerapan SMKU dalam rangka menentukan lingkupnya.

Ketika menentukan lingkup ini, organisasi harus mempertimbangkan
a) isu-isu eksternal dan internal seperti dimaksud dalam butir 4.1, dan
b) persyaratan sebagaimana dimaksud dalam butir 4.2.

Lingkup ini harus tersedia sebagai informasi terdokumentasi.

4.3.2 Lingkup SMKU

Organisasi harus
a) menetapkan bagian organisasi yang akan dimasukkan dalam SMKU,
b) menetapkan persyaratan SMKU, mempertimbangkan misi, tujuan, kewajiban internal dan eksternal organisasi (termasuk yang terkait dengan pihak yang berkepentingan), dan tanggung jawab hukum dan peraturan,
c) mengidentifikasi produk dan jasa dan semua kegiatan yang terkait dalam lingkup SMKU,
d) memperhitungkan kebutuhan dan minat pihak yang berkepentingan, seperti kebutuhan, ekspektasi dan kepentingan (yang sesuai) dari pelanggan, investor, pemegang saham, rantai pasokan, masukan dari masyarakat dan/atau komunitas, dan
e) menentukan lingkup SMKU sesuai dengan sifat, ukuran dan kompleksitas organisasi.

Ketika mendefinisikan lingkup, organisasi harus mendokumentasikan dan menjelaskan pengecualian; setiap pengecualian tersebut tidak boleh mempengaruhi kemampuan dan tanggung jawab organisasi untuk memberikan kelangsungan usaha dan operasional yang memenuhi persyaratan SMKU, sebagaimana ditentukan oleh analisis dampak usaha atau penilaian risiko dan persyaratan hukum atau peraturan yang berlaku.

4.4 Sistem manajemen kelangsungan usaha

Organisasi harus menetapkan, menerapkan, memelihara dan terus-menerus meningkatkan SMKU, termasuk proses-proses yang diperlukan dan interaksinya, sesuai dengan persyaratan standar ini.

5 Kepemimpinan

5.1 Kepemimpinan dan komitmen

Manajemen puncak dan peran manajemen lainnya yang relevan di seluruh organisasi harus menunjukkan kepemimpinan terkait dengan SMKU.

The organization shall ensure that these applicable legal, regulatory and other requirements to which the organization subscribes are taken into account in establishing, implementing and maintaining its BCMS.

The organization shall document this information and keep it up-to-date. New or variations to legal, regulatory and other requirements shall be communicated to affected employees and other interested parties

4.3 Determining the scope of the management system

4.3.1 General

The organization shall determine the boundaries and applicability of the BCMS to establish its scope

When determining this scope, the organization shall consider
a) the external and internal issues referred to in 4.1, and
b) the requirements referred to in 4.2.

The scope shall be available as documented information.

4.3.2 Scope of the BCMS

The organization shall
a) establish the parts of the organization to be included in the BCMS,
b) establish BCMS requirements, considering the organization's mission, goals, internal and external obligations (including those related to interested parties), and legal and regulatory responsibilities,
c) identify products and services and all related activities within the scope of the BCMS,
d) take into account interested parties' needs and interests, such as customers, investors, shareholders, the supply chain, public and/or community input and needs, expectations and interests (as appropriate), and
e) define the scope of the BCMS in terms of and appropriate to the size, nature and complexity of the organization.

When defining the scope, the organization shall document and explain exclusions; any such exclusions shall not affect the organization's ability and responsibility to provide continuity of business and operations that meet the BCMS requirements, as determined by business impact analysis or risk assessment and applicable legal or regulatory requirements.

4.4 Business continuity management system

The organization shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of this standard.

5 Leadership

5.1 Leadership and commitment

Persons in top management and other relevant management roles throughout the organization shall demonstrate leadership with respect to the BCMS.

CONTOH Kepemimpinan dan komitmen ini dapat ditunjukkan dengan memotivasi dan memberdayakan orang-orang untuk berkontribusi pada efektivitas SMKU.

5.2 Komitmen manajemen

Manajemen puncak harus menunjukkan kepemimipinan dan komitmennya terkait dengan SMKU dengan cara

— memastikan ditetapkannya kebijakan dan tujuan untuk sistem manajemen kelangsungan usaha yang kompatibel dengan arah strategis organisasi,
— memastikan adanya integrasi persyaratan sistem manajemen kelangsungan usaha ke dalam proses usaha organisasi,
— memastikan tersedianya sumber daya yang diperlukan untuk sistem manajemen kelangsungan usaha,
— mengkomunikasikan pentingnya manajemen kelangsungan usaha yang efektif dan sesuai dengan persyaratan SMKU,
— memastikan bahwa SMKU mencapai hasil-hasil yang dimaksudkan,
— mengarahkan dan mendorong personel untuk berkontribusi terhadap efektivitas SMKU,
— mendorong peningkatan terus-menerus, dan
— mendukung peran manajemen lain yang relevan untuk menunjukkan kepemimpinan dan komitmen mereka sesuai dengan bidang tanggung jawab mereka.

CATATAN 1 Istilah "usaha" dalam standar ini dimaksudkan agar ditafsirkan secara luas sebagai semua kegiatan inti untuk menjaga eksistensi organisasi.

Manajemen puncak harus memberi bukti komitmennya terhadap pembentukan, pelaksanaan, pengoperasian, pemantauan, kaji-ulang, pemeliharaan, dan peningkatan SMKU dengan
— menetapkan kebijakan kelangsungan usaha,
— memastikan ditetapkannya tujuan dan rencana SMKU,
— menetapkan peran, tanggung jawab, dan kompetensi untuk manajemen kelangsungan usaha, dan
— menunjuk satu atau beberapa personel yang bertanggung jawab atas SMKU dengan otoritas dan kompetensi yang tepat untuk bertanggung jawab atas pelaksanaan dan pemeliharaan SMKU.

CATATAN 2 Manajemen dapat memegang tanggung jawab lain dalam organisasi.

Manajemen puncak harus memastikan bahwa tanggung jawab dan wewenang untuk peran yang relevan ditugaskan dan dikomunikasikan dalam organisasi dengan cara
— mendefinisikan kriteria untuk menerima risiko dan tingkat risiko yang dapat diterima,
— terlibat aktif dalam pelatihan dan pengujian,
— memastikan bahwa audit internal SMKU dilakukan,
— melakukan kaji-ulang manajemen SMKU, dan
— menunjukkan komitmennya terhadap peningkatan terus-menerus.

5.3 Kebijakan

Manajemen puncak harus menetapkan kebijakan kelangsungan usaha yang
a) sesuai dengan tujuan organisasi,
b) menyediakan kerangka untuk menentukan tujuan kelangsungan usaha,
c) berisi komitmen untuk memenuhi persyaratan yang berlaku,
d) berisi komitmen untuk peningkatan SMKU secara terus-menerus.

EXAMPLE This leadership and commitment can be shown by motivating and empowering persons to contribute to the effectiveness of the BCMS.

5.2 Management commitment

Top management shall demonstrate leadership and commitment with respect to the BCMS by

— ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization,
— ensuring the integration of the business continuity management system requirements into the organization's business processes,
— ensuring that the resources needed for the business continuity management system are available,
— communicating the importance of effective business continuity management and conforming to the BCMS requirements,
— ensuring that the BCMS achieves its intended outcome(s),
— directing and supporting persons to contribute to the effectiveness of the BCMS,
— promoting continual improvement, and
— supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

NOTE 1 Reference to "business" in this standard is intended to be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

Top management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the BCMS by

— establishing a business continuity policy,
— ensuring that BCMS objectives and plans are established,
— establishing roles, responsibilities, and competencies for business continuity management, and
— appointing one or more persons to be responsible for the BCMS with the appropriate authority and competencies to be accountable for the implementation and maintenance of the BCMS.

NOTE 2 These persons can hold other responsibilities within the organization.

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization by

— defining the criteria for accepting risks and the acceptable levels of risk,
— actively engaging in exercising and testing,
— ensuring that internal audits of the BCMS are conducted,
— conducting management reviews of the BCMS, and
— demonstrating its commitment to continual improvement.

5.3 Policy

Top management shall establish a business continuity policy that

a) is appropriate to the purpose of the organization,
b) provides a framework for setting business continuity objectives,
c) includes a commitment to satisfy applicable requirements,
d) includes a commitment to continual improvement of the BCMS.

Kebijakan SMKU harus
— tersedia berupa informasi terdokumentasi,
— dikomunikasikan di internal organisasi,
— tersedia jika dibutuhkan oleh pihak yang berkepentingan,
— dikaji-ulang pada interval tertentu dan ketika terjadi perubahan yang signifikan, untuk memelihara kesesuaiannya.

Organisasi harus memelihara dokumentasi informasi mengenai kebijakan kelangsungan usaha.

5.4 Peran, tanggung jawab dan wewenang organisasi

Manajemen puncak harus memastikan bahwa tanggung jawab dan wewenang untuk peran yang relevan telah diberikan dan dikomunikasikan di internal organisasi.
Manajemen puncak harus menetapkan tanggung jawab dan kewenangan untuk
a) menjamin bahwa sistem manajemen sesuai dengan persyaratan standar ini, dan
b) melaporkan kinerja SMKU kepada manajemen puncak.

6 Perencanaan

6.1 Tindakan untuk menanggapi risiko dan peluang

Ketika merencanakan SMKU, organisasi harus mempertimbangkan hal-hal sebagaimana dimaksud dalam butir 4.1 dan persyaratan sebagaimana dimaksud dalam butir 4.2 dan menentukan risiko serta peluang yang perlu ditanggapi untuk
a) memastikan bahwa sistem manajemen dapat mencapai hasil yang dimaksudkan,
b) mencegah, atau mengurangi efek yang tidak diinginkan,
c) mencapai peningkatan terus-menerus.

Organisasi harus
a) merencanakan tindakan-tindakan untuk menanggapi risiko dan peluang tersebut,
b) merencanakan cara untuk
   1) mengintegrasikan dan menerapkan tindakan-tindakan tersebut ke dalam proses SMKU (lihat butir 8.1),
   2) mengevaluasi efektivitas tindakan-tindakan tersebut (lihat butir 9.1).

6.2 Tujuan kelangsungan usaha dan rencana untuk mencapainya

Manajemen puncak harus memastikan bahwa tujuan kelangsungan usaha ditetapkan dan dikomunikasikan kepada fungsi dan tingkat yang relevan dalam organisasi.
Tujuan kelangsungan usaha harus
a) konsisten dengan kebijakan kelangsungan usaha,
b) mempertimbangkan tingkat minimum produk dan layanan yang dapat diterima bagi organisasi untuk mencapai tujuannya,
c) dapat diukur,
d) mempertimbangkan persyaratan yang berlaku, dan
e) dipantau dan diperbarui selayaknya.

Organisasi harus menyimpan informasi terdokumentasi mengenai tujuan kelangsungan usaha.

The BCMS policy shall
- be available as documented information,
- be communicated within the organization,
- be available to interested parties, as appropriate,
- be reviewed for continuing suitability at defined intervals and when significant changes occur.

The organization shall retain documented information on the business continuity policy

5.4 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.
Top management shall assign the responsibility and authority for
a) ensuring that the management system conforms to the requirements of this standard, and
b) reporting on the performance of the BCMS to top management.

The organization shall plan
a) actions to address these risks and opportunities,
b) how to
   1) integrate and implement the actions into its BCMS processes (see 8.1),
   2) evaluate the effectiveness of these actions (see 9.1).

6 Planning

6.1 Actions to address risks and opportunities

When planning for the BCMS, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to
— ensure the management system can achieve its intended outcome(s),
— prevent, or reduce, undesired effects,
— achieve continual improvement.

The organization shall plan
a) actions to address these risks and opportunities,
b) how to
   1) integrate and implement the actions into its BCMS processes (see 8.1),
   2) evaluate the effectiveness of these actions (see 9.1).

6.2 Business continuity objectives and plans to achieve them

Top management shall ensure that business continuity objectives are established and communicated for relevant functions and levels within the organization.
The business continuity objectives shall
a) be consistent with the business continuity policy,
b) take account of the minimum level of products and services that is acceptable to the organization to achieve its objectives,
c) be measurable,
d) take into account applicable requirements, and
e) be monitored and updated as appropriate.

The organization shall retain documented information on the business continuity objectives.

Untuk mencapai tujuan kelangsungan usahanya, organisasi harus menetapkan
— siapa yang akan bertanggung jawab,
— apa yang akan dilakukan,
— sumber daya apa yang akan dibutuhkan,
— kapan akan selesai, dan
— bagaimana hasilnya akan dievaluasi.

7 Dukungan

7.1 Sumber daya

Organisasi harus menetapkan dan menyediakan sumber daya yang dibutuhkan untuk penetapan, penerapan, pemeliharaan, dan peningkatan SMKU secara terus-menerus.

7.2 Kompetensi

Organisasi harus
a) menentukan kompetensi orang yang melakukan pekerjaan di bawah kendali organisasi yang mempengaruhi kinerja,
b) menjamin bahwa orang-orang ini kompeten berdasarkan pendidikan, pelatihan, dan pengalaman,
c) jika mungkin, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil, dan
d) mendokumentasikan dan menyimpan informasi yang tepat sebagai bukti kompetensi..

CATATAN Tindakan yang dapat dilakukan meliputi misalnya penyediaan pelatihan, mentoring, atau penugasan kembali karyawan, atau menyewa atau mengontrak orang yang kompeten.

7.3 Kesadaran

Orang yang melakukan pekerjaan di bawah kendali organisasi harus sadar akan
a) kebijakan kelangsungan usaha,
b) kontribusi mereka terhadap efektivitas SMKU, termasuk manfaat dari kinerja manajemen kelangsungan usaha yang meningkat,
c) implikasi dari ketidaksesuaian dengan persyaratan SMKU, dan
d) peran mereka sendiri selama berlangsungnya insiden yang mengganggu.

7.4 Komunikasi

Organisasi harus menentukan kebutuhan akan komunikasi internal dan eksternal yang relevan dengan SMKU, yang mencakup
a) apa yang harus dikomunikasikan,
b) kapan dikomunikasikan, dan
c) kepada siapa akan dikomunikasikan.

Organisasi harus menetapkan, menerapkan, dan memelihara prosedur untuk
— komunikasi internal di antara pihak yang berkepentingan dan karyawan dalam organisasi,
— komunikasi eksternal dengan pelanggan, entitas mitra, masyarakat setempat, dan pihak lain yang berkepentingan, termasuk media,
— menerima, mendokumentasikan, dan menanggapi komunikasi dari pihak yang berkepentingan,
— mengadaptasikan dan mengintegrasikan sistem peringatan dini nasional atau regional, atau yang setara, ke dalam perencanaan dan penggunaan operasional, jika sesuai,
— menjamin tersedianya sarana komunikasi selama insiden mengganggu,

To achieve its business continuity objectives, the organization shall determine
— who will be responsible,
— what will be done,
— what resources will be required,
— when it will be completed, and
— how the results will be evaluated.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS.

7.2 Competence

The organization shall
a) determine the necessary competence of person(s) doing work under its control that affects its performance,
b) ensure these persons are competent on the basis of appropriate education, training, and experience,
c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken, and
d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization’s control shall be aware of
a) the business continuity policy,
b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity management performance,
c) the implications of not conforming with the BCMS requirements, and
d) their own role during disruptive incidents.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the BCMS including
a) on what it will communicate,
b) when to communicate,
c) with whom to communicate.

The organization shall establish, implement, and maintain procedure(s) for
— internal communication amongst interested parties and employees within the organization,
— external communication with customers, partner entities, local community, and other interested parties, including the media,
— receiving, documenting, and responding to communication from interested parties,
— adapting and integrating a national or regional threat advisory system, or equivalent, into planning and operational use, if appropriate,
— ensuring availability of the means of communication during a disruptive incident,

— memfasilitasi komunikasi terstruktur dengan pihak yang berwenang dan menjamin interoperabilitas beberapa organisasi penanganan insiden dan beberapa personel, bila sesuai, dan
— pengoperasian dan pengujian kemampuan komunikasi yang dimaksudkan untuk digunakan selama terganggunya komunikasi normal.

CATATAN Persyaratan lebih lanjut mengenai komunikasi dalam menanggapi insiden disebutkan dalam butir 8.4.3.

7.5 Informasi terdokumentasi

7.5.1 Umum

SMKU organisasi harus mencakup
a) informasi terdokumentasi yang disyaratkan oleh standar ini, dan
b) informasi terdokumentasi yang ditentukan organisasi karena dianggap perlu untuk efektivitas SMKU.

CATATAN Batasan informasi yang didokumentasikan untuk suatu SMKU pada setiap organisasi dapat berbeda, tergantung pada
— ukuran organisasi dan jenis kegiatan, proses, produk dan layanannya,
— kerumitan proses dan interaksinya, dan
— kompetensi personelnya.

7.5.2 Pembuatan dan pemutakhiran

Ketika membuat atau memutakhirkan informasi terdokumentasi, organisasi harus memastikan secara benar
a) identifikasi dan uraian (misalnya judul, tanggal, penulis atau nomor rujukan),
b) format (misalnya bahasa, versi perangkat lunak, grafik) dan media (misalnya kertas, elektronik), dan kaji-ulang serta persetujuan atas kecocokan dan kecukupan.

7.5.3 Pengendalian informasi terdokumentasi

Informasi terdokumentasi yang dipersyaratkan oleh SMKU dan standar ini harus dikendalikan agar
a) selalu tersedia dan cocok digunakan di mana saja dan setiap kali diperlukan,
b) terlindung dengan baik (misalnya terhadap hilangnya kerahasiaan, pemakaian yang tidak semestinya, atau hilangnya keutuhan).

Untuk pengendalian tersebut, organisasi harus menangani aktivitas berikut ini (sesuai dengan keperluan):
— distribusi, akses, pengambilan dan pemakaian,
— penyimpanan dan pemeliharaan, termasuk pemeliharaan agar mudah dibaca,
— pengendalian atas perubahan (misalnya pengendalian atas versinya),
— penyimpanan dan pengaturan tempat,
— pengambilan dan pemakaian,
— pemeliharaan kemudahan untuk dibaca, dan
— pencegahan dari pemakaian informasi usang tanpa sengaja.

Informasi terdokumentasi yang berasal dari sumber eksternal yang ditetapkan oleh organisasi untuk keperluan perencanaan dan operasi SMKU harus diidentifikasi dan dikendalikan.

— facilitating structured communication with appropriate authorities and ensuring the interoperability of multiple responding organizations and personnel, where appropriate, and
— operating and testing of communications capabilities intended for use during disruption of normal communications.

NOTE Further requirements for communication in response to an incident are specified in 8.4.3.

7.5 Documented information

7.5.1 General

The organization's BCMS shall include
a) documented information required by this standard, and
b) documented information determined by the organization as being necessary for the effectiveness of the BCMS.

NOTE The extent of documented information for a BCMS can differ from one organization to another due to
— the size of organization and its type of activities, processes, products and services,
— the complexity of processes and their interactions, and
— the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information, the organization shall ensure appropriate
a) identification and description (e.g. a title, date, author or reference number),
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic), and review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the BCMS and by this standard shall be controlled to ensure
a) it is available and suitable for use, where and when it is needed,
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable
— distribution, access, retrieval and use,
— storage and preservation, including preservation of legibility,
— control of changes (e.g. version control),
— retention and disposition,
— retrieval and use,
— preservation of legibility (i.e. clear enough to read), and
— prevention of the unintended use of obsolete information.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the BCMS shall be identified, as appropriate, and controlled.

Ketika menetapkan kendali atas informasi terdokumentasi, organisasi harus memastikan adanya proteksi yang memadai atas informasi tersebut (misalnya proteksi terhadap kemungkinan kompromi, modifikasi atau penghilangan secara ilegal.

CATATAN Akses menyiratkan keputusan mengenai izin untuk melihat informasi terdokumentasi saja, atau izin dan wewenang untuk melihat dan mengubah informasi terdokumentasi, dll.

8 Operasi

8.1 Perencanaan dan pengendalian operasional

Organisasi harus merencanakan, melaksanakan dan mengendalikan proses-proses yang diperlukan untuk memenuhi persyaratan, dan untuk melaksanakan tindakan menurut ketentuan dalam butir 6.1, dengan

a) menetapkan kriteria untuk proses-proses tersebut,
b) menerapkan pengendalian proses-proses sesuai dengan kriteria tersebut, dan
c) memelihara informasi terdokumentasi sebatas diperlukan untuk meyakinkan bahwa proses telah dilakukan seperti yang direncanakan.

Organisasi harus mengendalikan perubahan yang direncanakan dan mengkaji-ulang konsekuensi dari perubahan yang tidak disengaja, mengambil tindakan seperlunya untuk mengurangi efek merugikan.

Organisasi harus memastikan terkendalinya proses-proses yang dialih-dayakan.

8.2 Analisis dampak usaha dan penilaian risiko

8.2.1 Umum

Organisasi harus menetapkan, menerapkan dan memelihara proses formal dan terdokumentasi untuk analisis dampak usaha dan penilaian risiko yang

a) menetapkan konteks penilaian, mendefinisikan kriteria dan mengevaluasi dampak potensial dari insiden yang mengganggu,
b) mempertimbangkan persyaratan hukum dan lainnya yang harus diikuti organisasi,
c) meliputi analisis sistematis, prioritisasi penanganan risiko, dan biaya terkait,
d) mendefinisikan output yang dibutuhkan dari analisis dampak usaha dan penilaian risiko, dan
e) menetapkan persyaratan agar informasi ini tetap mutakhir dan rahasia.

CATATAN Ada berbagai metodologi untuk analisis dampak usaha dan penilaian risiko yang akan menentukan urutan pelaksanaannya.

8.2.2 Analisis dampak usaha

Organisasi harus menetapkan, menerapkan, dan memelihara proses evaluasi formal dan terdokumentasi untuk menentukan prioritas, tujuan, dan sasaran kelangsungan dan pemulihan. Proses ini harus mencakup penilaian dampak dari terganggunya kegiatan yang mendukung produk dan layanan organisasi.

Analisis dampak usaha harus mencakup hal-hal berikut:

a) identifikasi kegiatan yang mendukung penyediaan produk dan layanan;
b) penilaian dampak selama tidak melakukan kegiatan-kegiatan tersebut;
c) penetapan kerangka waktu prioritas untuk melanjutkan kegiatan ini pada tingkat minimum yang ditetapkan, mempertimbangkan waktu ketika dampak dari tidak melanjutkan kegiatan ini akan menjadi tidak dapat diterima, dan
d) identifikasi ketergantungan dan sumber daya yang mendukung untuk kegiatan ini, termasuk pemasok, mitra alih-daya dan pihak berkepentingan lain yang relevan.

When establishing control of documented information, the organization shall ensure that there is adequate protection for the documented information (e.g. protection against compromise, unauthorized modification or deletion).

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by
a) establishing criteria for the processes,
b) implementing control of the processes in accordance with the criteria, and
c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled.

8.2 Business impact analysis and risk assessment

8.2.1 General
The organization shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that
a) establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident,
b) takes into account legal and other requirements to which the organization subscribes,
c) includes systematic analysis, prioritization of risk treatments, and their related costs,
d) defines the required output from the business impact analysis and risk assessment, and
e) specifies the requirements for this information to be kept up-to-date and confidential.

NOTE There are various methodologies for business impact analysis and risk assessment which will determine the order in which these will be conducted.

8.2.2 Business impact analysis

The organization shall establish, implement, and maintain a formal and documented evaluation process for determining continuity and recovery priorities, objectives and targets. This process shall include assessing the impacts of disrupting activities that support the organization’s products and services.

The business impact analysis shall include the following:
a) identifying activities that support the provision of products and services;
b) assessing the impacts over time of not performing these activities;
c) setting prioritized timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable; and
d) identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties.

8.2.3 Penilaian risiko

Organisasi harus menetapkan, menerapkan, dan memelihara proses penilaian risiko formal terdokumentasi yang secara sistematis mengidentifikasi, menganalisis, dan mengevaluasi risiko dari insiden yang mengganggu organisasi.

CATATAN Proses ini bisa dibuat sesuai dengan ISO 31000.

Organisasi harus
a) mengidentifikasi risiko gangguan terhadap kegiatan prioritas organisasi dan proses, sistem, informasi, orang, aset, *outsourcing* mitra dan sumber daya lain yang mendukung mereka,
b) menganalisis risiko secara sistematis,
c) mengevaluasi risiko gangguan terkait mana yang memerlukan penanganan, dan
d) mengidentifikasi perlakuan sepadan dengan tujuan kelangsungan usaha dan sesuai dengan risiko yang dapat ditangani organisasi.

CATATAN Organisasi harus menyadari bahwa kewajiban keuangan atau pemerintah tertentu memerlukan komunikasi risiko pada berbagai tingkat rinci. Selain itu, kebutuhan masyarakat tertentu juga dapat menjamin berbagi informasi ini pada tingkat rinci yang sesuai.

8.3 Strategi kelangsungan usaha

8.3.1 Penentuan dan pemilihan

Penentuan dan pemilihan strategi harus didasarkan pada hasil dari analisis dampak usaha dan penilaian risiko.
Organisasi harus menetapkan strategi kelangsungan usaha yang tepat untuk
a) melindungi kegiatan prioritas,
b) menstabilkan, meneruskan, memulai kembali dan memulihkan kegiatan prioritas dan ketergantungannya dan sumber daya pendukung, serta
c) memitigasi, menangani, dan mengelola dampak.

Penentuan strategi harus meliputi persetujuan kerangka waktu prioritas untuk dimulainya kembali kegiatan.

Organisasi harus mengevaluasi kemampuan kelangsungan usaha pemasok.

8.3.2 Menetapkan persyaratan sumber daya

Organisasi harus menetapkan persyaratan sumber daya untuk melaksanakan strategi yang dipilih. Jenis-jenis sumber daya yang ditinjau harus meliputi tetapi tidak terbatas pada
a) orang,
b) informasi dan data,
c) bangunan, lingkungan kerja dan utilitas terkait,
d) fasilitas, peralatan dan bahan habis pakai,
e) sistem teknologi informasi dan komunikasi,
f) transportasi,
g) keuangan, dan
h) mitra dan pemasok.

8.2.3 Risk assessment

The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyses, and evaluates the risk of disruptive incidents to the organization.

NOTE This process could be made in accordance with ISO 31000.

The organization shall
a) identify risks of disruption to the organization's prioritized activities and the processes, systems, information, people, assets, outsource partners and other resources that support them,
b) systematically analyse risk,
c) evaluate which disruption related risks require treatment, and
d) identify treatments commensurate with business continuity objectives and in accordance with the organization's risk appetite.

NOTE The organization must be aware that certain financial or governmental obligations require the communication of these risks at varying levels of detail. In addition, certain societal needs can also warrant sharing of this information at an appropriate level of detail.

8.3 Business continuity strategy

8.3.1 Determination and selection

Determination and selection of strategy shall be based on the outputs from the business impact analysis and risk assessment.

The organization shall determine an appropriate business continuity strategy for
a) protecting prioritized activities,
b) stabilizing, continuing, resuming and recovering prioritized activities and their dependencies and supporting resources, and
c) mitigating, responding to and managing impacts.

The determination of strategy shall include approving prioritized time frames for the resumption of activities.

The organization shall conduct evaluations of the business continuity capabilities of suppliers.

8.3.2 Establishing resource requirements

The organization shall determine the resource requirements to implement the selected strategies. The types of resources considered shall include but not be limited to
a) people,
b) information and data,
c) buildings, work environment and associated utilities,
d) facilities, equipment and consumables,
e) information and communication technology (ICT) systems
f) transportation
g) finance, and
h) partners and suppliers.

8.3.3 Perlindungan dan mitigasi

Untuk risiko teridentifikasi yang memerlukan penanganan, organisasi harus mempertimbangkan langkah-langkah proaktif yang
a) mengurangi kemungkinan gangguan,
b) memperpendek periode gangguan, dan
c) membatasi dampak gangguan pada produk dan jasa utama organisasi.

Organisasi harus memilih dan menerapkan penanganan risiko yang tepat sesuai dengan *risk appetite* organisasi.

8.4 Menetapkan dan menerapkan prosedur kelangsungan usaha

8.4.1 Umum

Organisasi harus menetapkan, menerapkan, dan memelihara prosedur kelangsungan usaha untuk mengelola insiden mengganggu dan melanjutkan kegiatannya didasarkan pada tujuan pemulihan teridentifikasi dalam analisis dampak usaha.

Organisasi harus mendokumentasikan prosedur (termasuk pengaturan yang diperlukan) untuk menjamin kelangsungan kegiatan dan pengelolaan insiden mengganggu.

Prosedur tersebut harus
a) menetapkan protokol komunikasi internal dan eksternal yang sesuai,
b) spesifik mengenai langkah-langkah yang harus segera diambil pada saat gangguan,
c) fleksibel dalam menanggapi ancaman tak terduga dan kondisi internal dan eksternal yang berubah,
d) fokus pada dampak dari kejadian yang berpotensi mengganggu operasional,
e) dikembangkan berdasarkan asumsi-asumsi dan analisis saling ketergantungan, dan
f) efektif dalam meminimalkan konsekuensi melalui pelaksanaan strategi mitigasi yang tepat.

8.4.2 Struktur penanganan insiden

Organisasi harus menetapkan, mendokumentasikan, dan menerapkan prosedur dan struktur manajemen untuk menangani insiden mengganggu menggunakan personel dengan wewenang, tanggung jawab, dan kompetensi yang diperlukan untuk mengelola insiden.

Struktur respon tersebut harus
a) mengidentifikasi batas dampak yang membenarkan inisiasi respon resmi,
b) menilai sifat dan tingkat insiden mengganggu dan dampak potensialnya,
c) mengaktifkan respon kelangsungan usaha yang tepat,
d) memiliki proses, dan prosedur untuk aktivasi, operasi, koordinasi, dan mengkomunikasikan respon,
e) memiliki sumber daya yang tersedia untuk mendukung proses dan prosedur untuk mengelola insiden mengganggu agar memperkecil dampak, dan
f) berkomunikasi dengan pihak dan otoritas yang berkepentingan, serta media.

Organisasi harus memutuskan, menggunakan keselamatan hidup sebagai prioritas pertama dan konsultasi dengan pihak-pihak berkepentingan yang relevan, baik untuk berkomunikasi eksternal tentang risiko dan dampak signifikan dan mendokumentasikan keputusan. Jika keputusan adalah mengkomunikasikan maka organisasi harus menetapkan dan menerapkan prosedur untuk komunikasi, pewaspadaan dan peringatan eksternal termasuk media yang sesuai.

8.3.3 Protection and mitigation

For identified risks requiring treatment, the organization shall consider proactive measures that
a) reduce the likelihood of disruption,
b) shorten the period of disruption, and
c) limit the impact of disruption on the organization's key products and services.

The organization shall choose and implement appropriate risk treatments in accordance with its risk appetite.

8.4 Establish and implement business continuity procedures

8.4.1 General

The organization shall establish, implement, and maintain business continuity procedures to manage a disruptive incident and continue its activities based on recovery objectives identified in the business impact analysis.

The organization shall document procedures (including necessary arrangements) to ensure continuity of activities and management of a disruptive incident.

The procedures shall
a) establish an appropriate internal and external communications protocol,
b) be specific regarding the immediate steps that are to be taken during a disruption,
c) be flexible to respond to unanticipated threats and changing internal and external conditions,
d) focus on the impact of events that could potentially disrupt operations,
e) be developed based on stated assumptions and an analysis of interdependencies, and
f) be effective in minimizing consequences through implementation of appropriate mitigation strategies.

8.4.2 Incident response structure

The organization shall establish, document, and implement procedures and a management structure to respond to a disruptive incident using personnel with the necessary responsibility, authority and competence to manage an incident.

The response structure shall
a) identify impact thresholds that justify initiation of formal response,
b) assess the nature and extent of a disruptive incident and its potential impact,
c) activate an appropriate business continuity response,
d) have processes, and procedures for the activation, operation, coordination, and communication of the response,
e) have resources available to support the processes and procedures to manage a disruptive incident in order to minimize impact, and
f) communicate with interested parties and authorities, as well as the media.

The organization shall decide, using life safety as the first priority and in consultation with relevant interested parties, whether to communicate externally about its significant risks and impacts and document its decision. If the decision is to communicate then the organization shall establish and implement procedures for this external communication, alerts and warnings including the media as appropriate.

8.4.3 Peringatan dan komunikasi

Organisasi harus menetapkan, menerapkan dan memelihara prosedur untuk
a) mendeteksi suatu insiden,
b) pemantauan insiden secara rutin,
c) komunikasi internal dalam organisasi dan menerima, mendokumentasikan serta menanggapi komunikasi dari pihak berkepentingan,
d) menerima, mendokumentasikan dan menanggapi setiap sistem peringatan dini nasional atau regional atau yang setara,
e) menjamin ketersediaan sarana komunikasi selama insiden,
f) memfasilitasi komunikasi terstruktur dengan responden darurat,
g) mencatat informasi penting tentang insiden, tindakan yang dilakukan dan keputusan yang diambil, dan yang berikut juga harus dipertimbangkan dan dilaksanakan jika berlaku:
   — mengingatkan pihak berkepentingan yang berpotensi terkena dampak insiden yang terjadi atau yang mengancam;
   — menjamin kemampuan antar-operasi dari beberapa organisasi dan personel;
   — pengoperasian fasilitas komunikasi.

Prosedur komunikasi dan peringatan harus dilatihkan secara rutin.

8.4.4 Rencana kelangsungan usaha

Organisasi harus menetapkan prosedur terdokumentasi untuk memberikan respons terhadap insiden mengganggu dan meneruskan atau memulihkan kegiatannya dalam jangka waktu yang telah ditentukan. Prosedur tersebut harus sesuai dengan kebutuhan dari mereka yang akan menggunakannya.

Rencana kelangsungan usaha harus memuat
a) peran dan tanggung jawab khusus untuk orang dan tim yang mempunyai wewenang selama dan setelah insiden,
b) proses untuk mengaktifkan respon,
c) rincian untuk mengelola konsekuensi langsung dari insiden mengganggu dengan memberikan memperhatikan pada
   1) kesejahteraan individu,
   2) opsi strategis, taktis dan operasional untuk menanggapi gangguan, dan
   3) pencegahan kerugian lebih lanjut atau tidak tersedianya kegiatan prioritas;
d) rincian tentang cara dan dalam keadaan apa organisasi akan berkomunikasi dengan karyawan dan keluarga mereka, pihak utama yang berkepentingan dan kontak darurat,
e) cara organisasi akan meneruskan atau memulihkan kegiatan prioritas di dalam jangka waktu yang telah ditentukan,
f) rincian tentang respon media organisasi setelah terjadi insiden, termasuk
   1) strategi komunikasi,
   2) antar antarmuka dengan media
   3) pedoman atau *template* untuk menyusun pernyataan bagi media, dan
   4) juru bicara yang tepat;
g) proses untuk pengakhiran kegiatan setelah insiden berakhir.

Setiap rencana harus menetapkan
— maksud dan ruang lingkup,
— tujuan,
— kriteria dan prosedur aktivasi,
— prosedur pelaksanaan,
— peran, tanggung jawab, dan wewenang,
— persyaratan dan prosedur komunikasi,

8.4.3 Warning and communication

The organization shall establish, implement and maintain procedures for
a) detecting an incident,
b) regular monitoring of an incident,
c) internal communication within the organization and receiving, documenting and responding to communication from interested parties,
d) dreceiving, documenting and responding to any national or regional risk advisory system or equivalent,
e) assuring availability of the means of communication during a disruptive incident,
f) facilitating structured communication with emergency responders,
g) recording of vital information about the incident, actions taken and decisions made, and
h) the following shall also be considered and implemented where applicable:
   — alerting interested parties potentially impacted by an actual or impending disruptive incident;
   — assuring the interoperability of multiple responding organizations and personnel;
   — operation of a communications facility.

The communication and warning procedures shall be regularly exercised.

8.4.4 Business continuity plans

The organization shall establish documented procedures for responding to a disruptive incident and how it will continue or recover its activities within a predetermined timeframe. Such procedures shall address the requirements of those who will use them.

The business continuity plans shall collectively contain
a) defined roles and responsibilities for people and teams having authority during and following an incident,
b) a process for activating the response,
c) details to manage the immediate consequences of a disruptive incident giving due regard to
   1) the welfare of individuals,
   2) strategic, tactical and operational options for responding to the disruption, and
   3) prevention of further loss or unavailability of prioritized activities;
d) details on how and under what circumstances the organization will communicate with employees and their relatives, key interested parties and emergency contacts,
e) how the organization will continue or recover its prioritized activities within predetermined timeframes,
f) details of the organization’s media response following an incident, including
   1) a communications strategy,
   2) preferred interface with the media,
   3) guideline or template for drafting a statement for the media, and
   4) appropriate spokespeople;
g) a process for standing down once the incident is over.

Each plan shall define
— purpose and scope,
— objectives,
— activation criteria and procedures,
— implementation procedures,
— roles, responsibilities, and authorities,
— communication requirements and procedures,

— ketergantungan dan interaksi internal maupun eksternal,
— kebutuhan sumber daya, dan
— aliran informasi dan proses dokumentasi.

8.4.5 Pemulihan

Organisasi harus memiliki prosedur terdokumentasi untuk memulihkan dan mengembalikan kegiatan usaha dari tindakan sementara yang diambil untuk mendukung persyaratan usaha normal setelah insiden.

8.5 Latihan dan pengujian

Organisasi harus melakukan latihan dan pengujian atas prosedur kelangsungan usaha untuk memastikan bahwa prosedur tersebut konsisten dengan tujuan kelangsungan usahanya.

Organisasi harus melakukan latihan dan pengujian yang
a) konsisten dengan ruang lingkup dan tujuan dari SMKU,
b) didasarkan pada skenario yang tepat yang terencana dengan arah dan tujuan yang jelas,
c) secara bersama-sama dari waktu ke waktu memvalidasi seluruh pengaturan kelangsungan usaha, yang melibatkan pihak-pihak berkepentingan yang relevan,
d) meminimalkan risiko gangguan operasi,
e) menghasilkan laporan formal tentang pasca-latihan yang berisi hasil, rekomendasi, dan tindakan untuk melaksanakan peningkatan,
f) ditelaah dalam konteks untuk mempromosikan peningkatan terus-menerus, dan
g) dilakukan pada interval yang direncanakan dan ketika ada perubahan yang signifikan dalam organisasi atau lingkungannya.

9 Evaluasi kinerja

9.1 Pemantauan, pengukuran, analisis dan evaluasi

9.1.1 Umum

Organisasi harus menetapkan
a) hal yang perlu dipantau dan diukur
b) metode untuk pemantauan, pengukuran, analisis dan evaluasi, jika berlaku, untuk memastikan hasil yang benar,
c) jadual waktu pemantauan dan pengukuran, dan
d) jadual waktu analisis dan evaluasi atas hasil pemantauan dan pengukuran.

Organisasi harus menyimpan informasi terdokumentasi sebagai bukti hasil.

Organisasi harus mengevaluasi kinerja dan efektivitas SMKU.

Selain itu, organisasi harus
— mengambil tindakan bila diperlukan untuk mengatasi tren atau hasil yang merugikan sebelum terjadi ketidaksesuaian, dan
— menyimpan informasi terdokumentasi relevan sebagai bukti hasil.

Prosedur untuk memantau kinerja harus menyediakan
— pengaturan metrik kinerja yang sesuai dengan kebutuhan organisasi,
— memantau sejauh mana kebijakan kelangsungan usaha, sasaran dan target organisasi terpenuhi,

— internal and external interdependencies and interactions,
— resource requirements, and
— information flow and documentation processes.

8.4.5 Recovery

The organization shall have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident.

8.5 Exercising and testing

The organization shall exercise and test its business continuity procedures to ensure that they are consistent with its business continuity objectives.

The organization shall conduct exercises and tests that
a) are consistent with the scope and objectives of the BCMS,
b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives,
c) taken together over time validate the whole of its business continuity arrangements, involving relevant interested parties,
d) minimize the risk of disruption of operations,
e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements,
f) are reviewed within the context of promoting continual improvement, and
g) are conducted at planned intervals and when there are significant changes within the organization or to the environment in which it operates.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization shall determine
a) what needs to be monitored and measured,
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results,
c) when the monitoring and measuring shall be performed, and
d) when the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the performance and the effectiveness of the BCMS.

Additionally, the organization shall
— take action when necessary to address adverse trends or results before a nonconformity occurs, and
— retain relevant documented information as evidence of the results.

The procedures for monitoring performance shall provide for
— the setting of performance metrics appropriate to the needs of the organization,
— monitoring the extent to which the organization’s business continuity policy, objectives and targets are met,
— kinerja proses, prosedur dan fungsi yang melindungi kegiatan prioritasnya,

— pemantauan kesesuaian dengan standar ini dan dengan tujuan kelangsungan usaha,
— pemantauan bukti sejarah dari kekurangan kinerja SMKU, dan
— perekaman data dan hasil pemantauan dan pengukuran untuk memfasilitasi tindakan korektif berikutnya.

CATATAN Kinerja yang kurang baik dapat mencakup ketidaksesuaian, nyaris, alarm palsu, dan insiden yang sebenarnya.

9.1.2 Evaluasi prosedur kelangsungan

a) Organisasi harus melakukan evaluasi prosedur dan kemampuan kelangsungan usaha untuk memastikan kesesuaian, kecukupan dan efektivitasnya;
b) Evaluasi ini harus dilakukan melalui kaji-ulang, latihan, pengujian, pelaporan pasca-insiden, dan evaluasi kinerja secara periodik. Perubahan signifikan yang timbul harus tercermin dalam prosedur pada waktu yang tepat;
c) Organisasi harus mengevaluasi secara berkala sesuai dengan persyaratan hukum dan peraturan yang berlaku, praktek industri terbaik, dan kesesuaian dengan kebijakan dan tujuan kelangsungan usaha sendiri; dan
d) Organisasi harus melakukan evaluasi pada interval waktu terencana dan ketika terjadi perubahan yang signifikan.

Ketika insiden yang mengganggu terjadi dan menyebabkan aktivasi prosedur kelangsungan usaha, organisasi harus melakukan kajian pasca insiden dan mencatat hasil-hasilnya.

9.2 Audit Internal

Organisasi harus melakukan audit internal pada interval waktu yang direncanakan untuk mendapat informasi apakah sistem manajemen kelangsungan usahanya telah
a) sesuai dengan
   1) persyaratan organisasi itu sendiri,
   2) persyaratan standar ini, dan
b) diimplementasikan dan dipelihara secara efektif.

Organisasi harus
— merencanakan, menetapkan, menerapkan dan memelihara program audit, termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang terlibat dan hasil audit sebelumnya,
— menentukan kriteria audit dan cakupan untuk setiap audit,
— memilih auditor dan melakukan audit untuk menjamin objektivitas dan ketidakberpihakan proses audit,
— memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan, dan
— menyimpan informasi terdokumentasi sebagai bukti hasil.

Program audit, termasuk jadual apapun, harus didasarkan pada hasil penilaian risiko dari kegiatan organisasi dan hasil audit sebelumnya. Prosedur audit harus mencakup ruang lingkup, frekuensi, metodologi dan kompetensi, serta tanggung jawab dan persyaratan untuk melakukan audit dan pelaporan hasil.

Manajemen yang bertanggung jawab atas area yang diaudit harus memastikan bahwa setiap koreksi dan tindakan korektif yang diperlukan dilakukan tanpa ditunda untuk menghilangkan

— performance of the processes, procedures and functions that protect its prioritized activities,
— monitoring compliance with this standard and the business continuity objectives,
— monitoring historical evidence of deficient BCMS' performance, and
— recording data and results of monitoring and measurement to facilitate subsequent corrective actions.

NOTE Deficient performance could include non-conformity, near misses, false alarms, and actual incidents.

9.1.2 Evaluation of business continuity procedures

a) The organization shall conduct evaluations of its business continuity procedures and capabilities in order to ensure their continuing suitability, adequacy and effectiveness;
b) These evaluations shall be undertaken through periodic reviews, exercising, testing, post-incident reporting, and performance evaluations. Significant changes arising shall be reflected in the procedure(s) in a timely manner;
c) The organization shall periodically evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformance with its own business continuity policy and objectives; and
d) The organization shall conduct evaluations at planned intervals and when significant changes occur.

When a disruptive incident occurs and results in the activation of its business continuity procedures, the organization shall undertake a post-incident review and record the results.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the business continuity management system
a) conforms to
   1) the organization's own requirements for its BCMS,
   2) the requirements of this standard, and
b) is effectively implemented and maintained.

The organization shall
— plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits,
— define the audit criteria and scope for each audit,
— select auditors and conduct audits to ensure objectivity and the impartiality of the audit process,
— ensure that the results of the audits are reported to relevant management, and
— retain documented information as evidence of the results.

The audit programme, including any schedule, shall be based on the results of risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected

temuan ketidaksesuaian dan penyebabnya. Kegiatan tindak lanjut harus mencakup verifikasi tindakan yang dilakukan dan pelaporan hasil verifikasi.

9.3 Kaji-ulang manajemen

Manajemen puncak harus mengkaji-ulang SMKU organisasi pada interval waktu terencana untuk memastikan kesesuaian, kecukupan dan efektivitas.

Kaji-ulang manajemen harus mencakup pertimbangan tentang
a) status tindakan dari kaji-ulang manajemen sebelumnya,
b) perubahan dalam isu eksternal dan internal yang relevan dengan sistem manajemen kelangsungan usaha,
c) informasi mengenai kinerja kelangsungan usaha, termasuk kecenderungan pada
    1) ketidaksesuaian dan tindakan korektif,
    2) pemantauan dan hasil evaluasi pengukuran,
    3) hasil audit,
d) kemungkinan untuk peningkatan terus-menerus.

Tinjauan manajemen harus mempertimbangkan kinerja organisasi, termasuk
— tindak lanjut dari kaji-ulang manajemen sebelumnya,
— kebutuhan untuk perubahan SMKU, termasuk kebijakan dan tujuan,
— kesempatan untuk peningkatan,
— hasil audit dan kaji-ulang SMKU, jika perlu termasuk pemasok dan mitra utama,
— teknik, produk atau prosedur, yang dapat digunakan dalam organisasi untuk meningkatkan kinerja dan efektivitas SMKU,
— status tindakan korektif,
— hasil latihan dan pengujian,
— risiko atau masalah yang tidak cukup dibahas dalam penilaian risiko sebelumnya,
— setiap perubahan yang dapat mempengaruhi SMKU, baik di dalam maupun di luar lingkup SMKU,
— kecukupan kebijakan,
— rekomendasi untuk peningkatan,
— pelajaran yang diambil dan tindakan yang timbul dari insiden mengganggu, dan
— praktik dan pedoman yang baik yang timbul.

Output dari kaji-ulang manajemen harus mencakup keputusan yang berkaitan dengan peluang peningkatan terus-menerus dan kemungkinan perlunya perubahan pada SMKU, dan mencakup:
a) variasi lingkup SMKU;
b) peningkatan efektivitas SMKU;
c) pemutakhiran penilaian risiko, analisis dampak usaha, rencana kelangsungan usaha dan prosedur terkait;
d) modifikasi prosedur dan kendali untuk merespon kejadian internal atau eksternal yang dapat berdampak pada SMKU, termasuk perubahan pada
    1. persyaratan usaha dan operasional,
    2. persyaratan pengurangan risiko dan keamanan,
    3. kondisi dan proses operasional,
    4. persyaratan hukum dan peraturan,
    5. kewajiban kontrak,
    6. tingkat risiko dan/atau kriteria untuk menerima risiko,
    7. kebutuhan sumber daya,
    8. pendanaan dan kebutuhan anggaran, dan
e) cara mengukur efektivitas pengendalian.

nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

9.3 Management review

Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of
a) the status of actions from previous management reviews,
b) changes in external and internal issues that are relevant to the business continuity management system,
c) information on the business continuity performance, including trends in
   1) nonconformities and corrective actions,
   2) monitoring and measurement evaluation results,
   3) audit results,
d) opportunity for continual improvement.

Management reviews shall consider the performance of the organization, including
— follow-up actions from previous management reviews,
— the need for changes to the BCMS, including the policy and objectives,
— opportunities for improvement,
— results of BCMS audits and reviews, including those of key suppliers and partners where appropriate,
— techniques, products or procedures, which could be used in the organization to improve the BCMS' performance and effectiveness,
— status of corrective actions,
— results of exercising and testing,
— risks or issues not adequately addressed in any previous risk assessment,
— any changes that could affect the BCMS, whether internal or external to the scope of the BCMS,
— adequacy of policy,
— recommendations for improvement,
— lessons learned and actions arising from disruptive incidents, and
— emerging good practice and guidance.

The output of the the management review shall include decisions related to continual improvement opportunities and the possible need for changes to the BCMS and include the following:
a) variations to the scope of the BCMS;
b) improvement of the effectiveness of the BCMS;
c) update of the risk assessment, business impact analysis, business continuity plans and related procedures;
d) modification of procedures and controls to respond to internal or external events that may impact on the BCMS, including changes to
   1. business and operational requirements,
   2. risk reduction and security requirements,
   3. operational conditions and processes,
   4. legal and regulatory requirements,
   5. contractual obligations,
   6. levels of risk and/or criteria for accepting risks,
   7. resource needs,
   8. funding and budget requirements; and
e) how the effectiveness of controls are measured.

Organisasi harus menyimpan informasi terdokumentasi sebagai bukti hasil dari kaji-ulang manajemen.

Organisasi harus
— mengkomunikasikan hasil kaji-ulang manajemen kepada pihak yang berkepentingan, dan
— mengambil tindakan yang tepat berkaitan dengan hasil tersebut.

10 Peningkatan

10.1 Ketidaksesuaian dan tindakan korektif

Ketika terjadi ketidaksesuaian, organisasi harus
a) mengidentifikasi ketidaksesuaian tersebut, dan
b) merespon terhadap ketidaksesuaian, dan, jika perlu,
    1) mengambil tindakan untuk mengendalikan dan memperbaikinya,
    2) menangani konsekuensinya.
c) mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar tidak terulang atau terjadi di tempat lain, dengan
    1) meninjau ketidaksesuaian,
    2) menentukan penyebab ketidaksesuaian, dan
    3) menentukan apakah ada ketidaksesuaian serupa, atau berpotensi terjadi,
    4) mengevaluasi perlunya tindakan korektif untuk memastikan bahwa ketidaksesuaian tidak terulang atau terjadi di tempat lain,
    5) menentukan dan melaksanakan tindakan korektif yang diperlukan,
    6) meninjau efektivitas tindakan korektif yang diambil dan
    7) melakukan perubahan pada SMKU, jika perlu.
d) mengimplementasikan tindakan yang diperlukan,
e) meninjau efektivitas tindakan korektif yang dilakukan,
f) membuat perubahan pada sistem manajemen kelangsungan usaha, jika perlu.

Tindakan korektif harus sesuai dengan efek dari temuan ketidaksesuaian.
Organisasi harus memelihara informasi terdokumentasi sebagai bukti/data tentang
— sifat ketidaksesuaian dan tindakan korektif berikutnya, dan
— hasil dari tindakan korektif.

10.2 Peningkatan terus-menerus

Organisasi harus terus-menerus meningkatkan kesesuaian, kecukupan atau efektivitas SMKU.

CATATAN Untuk mencapai peningkatan, organisasi dapat menggunakan proses SMKU seperti kepemimpinan, perencanaan dan evaluasi kinerja.

The organization shall retain documented information as evidence of the results of management reviews.

The organization shall
— communicate the results of management review to relevant interested parties, and
— take appropriate action relating to those results.

10 Improvement

10.1 Nonconformity and corrective action

.

When nonconformity occurs, the organization shall
a) identify the nonconformity, and
b) react to the nonconformity, and, as applicable,
   1) take action to control and correct it,
   2) deal with the consequences.
c) evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by
   1) reviewing the nonconformity,
   2) determining the causes of the nonconformity, and
   3) determining if similar nonconformities exist, or could potentially occur,
   4) evaluating the need for corrective action to ensure that nonconformities do not recur or occur elsewhere,
   5) determining and implementing corrective action needed,
   6) reviewing the effectiveness of any corrective action taken, and
   7) making changes to the BCMS, if necessary.
d) implement any action needed,
e) review the effectiveness of any corrective action taken,
f) make changes to the business continuity management system, if necessary

Corrective actions shall be appropriate to the effects of the nonconformities encountered.
The organization shall retain documented information as evidence of
— the nature of the nonconformities and any subsequent actions taken, and
— the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy or effectiveness of the BCMS.

NOTE The organization can use the processes of the BCMS such as leadership, planning and performance evaluation, to achieve improvement.

Bibliografi

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*

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

[4] ISO/IEC 20000-1, *Information Technology — Service Management*

[5] ISO 22300, *societal security – Terminology*

[6] ISO/PAS 22399, *Societal security — Guideline for incident preparedness and operational continuity management*

[7] ISO/IEC 24762, *Information technology — Security techniques — Guidelines for Information and communications technology disaster recovery services*

[8] ISO/IEC 27001, *Information Security Management Systems*

[9] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] ISO 31000, *Risk Management — Principles and Guidelines*

[11] ISO/IEC 31010, *Risk management — Risk assessment techniques*

[12] ISO/IEC Guide 73, *Risk Management – Vocabulary*

[13] BS 25999-1, *Business continuity management — Code of practice*, British Standards Institution (BSI)

[14] BS 25999-2, *Business continuity management — Specification*, British Standards Institution (BSI)

[15] SI 24001, *Security and continuity management systems — Requirements and guidance for use*, Standards Institution of Israel

[16] NFPA 1600, *Standard on disaster/ emergency management and business continuity programs*, National Fire Protection Association (USA)

[17] *Business Continuity Plan Drafting Guideline*, Ministry of Economy, Trade and Industry (Japan), 2005

[18] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[19] ANSI/ASIS SPC.1, *Organizational Resilience: Security, Preparedness, and Continuity Managements Systems – Requirements with Guidance for Use*SS 540: 2008, *Singapore Standard for Business mContinuity Managemen*t

[20] ANSI/ASIS/BSI BCM.01, *Business Continuity Management Systems: Requirements with Guidance for Use*

Bibliography

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*
[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO/IEC 20000-1, *Information Technology — Service Management*
[5] ISO 22300, *societal security – Terminology*

[6] ISO/PAS 22399, *Societal security — Guideline for incident preparedness and operational continuity management*

[7] ISO/IEC 24762, *Information technology — Security techniques — Guidelines for Information and communications technology disaster recovery services*

[8] ISO/IEC 27001, *Information Security Management Systems*

[9] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] ISO 31000, *Risk Management — Principles and Guidelines*

[11] ISO/IEC 31010, *Risk management — Risk assessment techniques*

[12] ISO/IEC Guide 73, *Risk Management – Vocabulary*

[13] BS 25999-1, *Business continuity management — Code of practice*, British Standards Institution (BSI)

[14] BS 25999-2, *Business continuity management — Specification*, British Standards Institution (BSI)

[15] SI 24001, *Security and continuity management systems — Requirements and guidance for use*, Standards Institution of Israel

[16] NFPA 1600, *Standard on disaster/ emergency management and business continuity programs*, National Fire Protection Association (USA)

[17] *Business Continuity Plan Drafting Guideline*, Ministry of Economy, Trade and Industry (Japan), 2005

[18] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[19] ANSI/ASIS SPC.1, *Organizational Resilience: Security, Preparedness, and Continuity Managements Systems – Requirements with Guidance for Use*SS 540: 2008, *Singapore Standard for Business mContinuity Managemen*t

[20] ANSI/ASIS/BSI BCM.01, *Business Continuity Management Systems: Requirements with Guidance for Use*