SNI

Standar Nasional Indonesia

SNI ISO 31000:2011

# Manajemen risiko — Prinsip dan pedoman

## *Risk management — Principles and guidelines*

**(ISO 31000:2009, IDT)**

ICS 03.100.01

Badan Standardisasi Nasional

# Daftar isi

## Prakata

Standar Nasional Indonesia (SNI) ISO 31000:2011, dengan judul *Manajemen Risiko – Prinsip dan pedoman,* merupakan adopsi identik dari ISO 31000:2009 (E), *Risk management – Principles and guidelines*, dengan metode terjemahan dua bahasa (*bilingual*). Standar ini sebagai pengganti dari publikasi standar terbitan tahun 2011 yang menggunakan metode republikasi-*reprint*.

Standar ini disusun oleh Komite Teknis 03-10, *Manajemen Risiko*. Standar ini telah dibahas dan disetujui dalam rapat konsensus nasional di Jakarta, pada tanggal 19 Mei 2016. Konsensus ini dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah.

Standar ini merupakan bagian dari seri SNI ISO 31000, *Manajemen risiko,* yang terdiri dari 4 standar yaitu:

- SNI ISO 31000:2011 *Manajemen risiko — Prinsip dan pedoman;*
- SNI ISO Guide 73:2016 *Manajemen risiko — Kosakata;*
- SNI ISO/TR 31004:2016 *Manajemen risiko — Panduan untuk implementasi SNI ISO 31000;*
- SNI ISO/IEC 31010:2016 *Manajemen risiko — Teknik penilaian risiko.*

Dalam Standar ini istilah ”*this International Standard*” diganti menjadi ”*this Standard*”, dan diterjemahkan menjadi “Standar ini”.

Beberapa standar ISO yang dijadikan sebagai referensi dalam Standar ini telah diadopsi menjadi Standar Nasional Indonesia (SNI), yaitu:

1) ISO Guide 73:2009, *Risk management - Vocabulary,* telah diadopsi secara identik menjadi SNI ISO Guide 73:2016, *Manajemen risiko - Kosakata.*

2) ISO 31010:2009, *Risk management – Risk assessment techniques,* telah diadopsi secara identik menjadi SNI ISO 31010:2016, *Manajemen risiko – Teknik penilaian risiko.*

Untuk diketahui oleh pengguna Standar ini bahwa terdapat penulisan yang tidak lengkap pada standar yang di adopsi, ISO 31000:2009, yaitu: pada *Figure-1* dari poin “a s/d k” hanya ditulis secara singkat dan berbeda dengan yang tercantum di batang tubuh standar pada pasal 3 *Principles* poin “a s/d k”; contoh: a) *creates value*, seharusnya tertulis seperti yang tercantum di batang tubuh standar yaitu a) *Risk management creates and protects value.* Oleh karena Standar ini merupakan adopsi identik dengan metode terjemahan maka cara penulisan mengikuti sebagaimana yang tertulis pada standar aslinya.

Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya yaitu ISO 31000:2009 (E) dan/atau dokumen terkait lain yang menyertainya.

# Pendahuluan

Semua jenis dan ukuran organisasi menghadapi faktor dan pengaruh internal dan eksternal yang membuat organisasi tidakpasti apakah dan kapan mereka akan mencapai tujuannya. Efek ketidakpastian ini pada sasaran organisasi adalah "risiko".

Semua kegiatan dari suatu organisasi melibatkan risiko. Organisasi mengelola risiko dengan pengidentifikasian, analisis, dan kemudian pengevaluasian apakah risiko sebaiknya dimodifikasi dengan perlakuan risiko guna memenuhi kriteria risiko organisasi. Sepanjang proses ini, organisasi berkomunikasi dan berkonsultasi dengan para pemangku kepentingan dan memantau serta meninjau suatu risiko beserta pengendalian yang memodifikasi risiko guna memastikan bahwa perlakuan risiko lebih lanjut tidak dibutuhkan. Standar ini menguraikan secara sistematis dan logis dari proses tersebut secara rinci.

Ketika semua organisasi mengelola risiko pada tingkatan tertentu, Standar ini menetapkan sejumlah prinsip yang harus dipenuhi untuk membuat manajemen risiko menjadi efektif. Standar ini merekomendasikan suatu organisasi mengembangkan, mengimplementasikan, dan meningkatkan secara terus-menerus suatu kerangka kerja yang bertujuan untuk mengintegrasikan suatu proses untuk pengelolaan risiko dalam keseluruhan tata kelola, stategi dan perencanaan, manajemen, proses pelaporan, kebijakan, nilai-nilai serta budaya organisasi.

Manajemen risiko dapat diterapkan pada seluruh organisasi, pada banyak wilayah dan tingkatan organisasi, pada setiap waktu, dan juga untuk fungsi, proyek dan kegiatan yang bersifat spesifik.

Meskipun praktik manajemen risiko telah dikembangkan dari waktu ke waktu dan dalam banyak sektor agar memenuhi beragam kebutuhan, suatu adopsi dari proses yang konsisten dalam suatu kerangka kerja yang komprehensif dapat membantu untuk memastikan bahwa risiko dikelola secara efektif, efisien dan koheren lintas organisasi. Suatu pendekatan umum yang digambarkan dalam Standar ini menyediakan prinsip-prinsip dan pedoman untuk pengelolaan segala bentuk risiko secara sistematis, transparan dan kredibel serta didalam setiap ruang lingkup dan konteks.

Setiap sektor spesifik atau aplikasi manajemen risiko yang spesifik membawa serta kebutuhan individual, khalayak, persepsi dan kriteria tersendiri. Oleh karena itu, suatu fitur kunci dari Standar ini adalah pencantuman tentang "penetapan suatu konteks " sebagai kegiatan pada awal suatu proses manajemen risiko umum ini. Penetapan suatu konteks akan menangkap sasaran dari suatu organisasi, suatu lingkungan di mana organisasi tersebut mengejar sasarannya, para pemangku kepentingan organisasi dan keanekaragaman kriteria risiko - semua yang akan membantu dalam mengungkapkan dan menilai sifat serta kompleksitas risiko tersebut.

Hubungan antara prinsip-prinsip untuk pengelolaan risiko, suatu kerangka kerja di mana prinsip tersebut terjadi dan proses manajemen risiko yang digambarkan dalam Standar ini ditunjukkan pada Gambar 1.

Ketika diimplementasikan dan dipelihara sesuai dengan Standar ini, pengelolaan risiko memungkinkan organisasi untuk, misalnya:

- meningkatkan kemungkinan-kejadian dalam pencapaian sasaran;
- mendorong manajemen proaktif;

- menyadari kebutuhan untuk mengidentifikasi dan memperlakukan risiko di keseluruhan organisasi;
- meningkatkan suatu pengidentifikasian peluang dan ancaman;
- mematuhi persyaratan hukum dan peraturan yang relevan serta norma-norma internasional;
- meningkatkan pelaporan wajib dan sukarela;
- meningkatkan tata kelola;
- meningkatkan keyakinan dan kepercayaan pemangku kepentingan;
- menetapkan suatu dasar yang handal untuk pengambilan keputusan dan perencanaan;
- meningkatkan pengendalian;
- mengalokasikan dan menggunakan sumber daya secara efektif untuk perlakuan risiko;
- meningkatkan efektivitas dan efisiensi operasional;
- menguatkan kinerja kesehatan dan keselamatan, serta perlindungan lingkungan;
- meningkatkan pencegahan kerugian dan pengelolaan insiden;
- meminimalkan kerugian;
- meningkatkan pembelajaran organisasi; dan
- meningkatkan ketangguhan organisasi.

Standar ini dimaksudkan untuk memenuhi kebutuhan pemangku kepentingan secara luas, termasuk:

a) mereka yang bertanggung jawab dalam pengembangan kebijakan manajemen risiko dalam organisasi mereka;

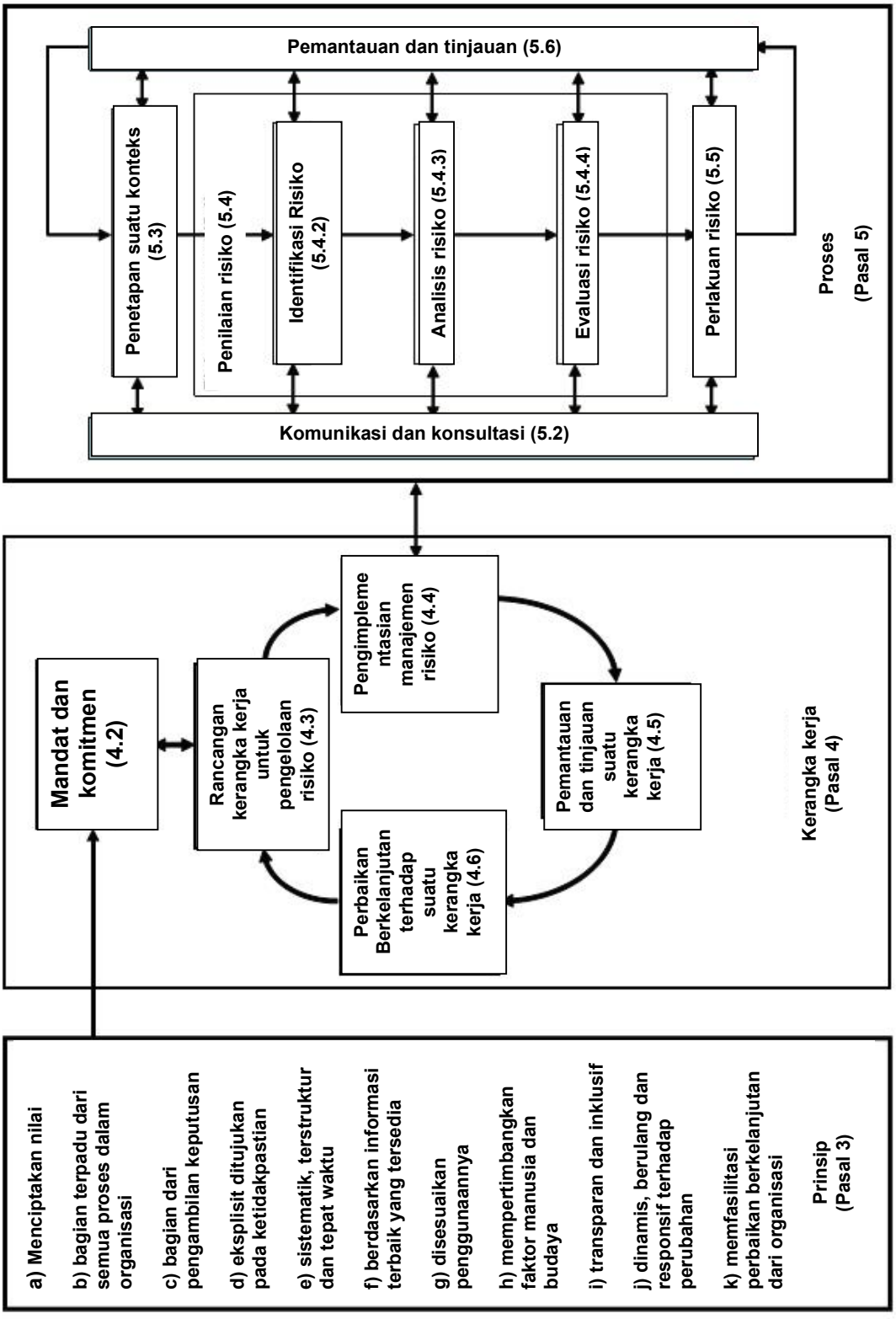
b) mereka yang akuntabel dalam pemastian bahwa risiko dikelola secara efektif dalam organisasi sebagai sebuah kesatuan atau dalam suatu area tertentu, proyek atau kegiatan;

c) mereka yang membutuhkan untuk mengevaluasi efektivitas suatu organisasi dalam pengelolaan risiko, dan

d) pengembang standar, panduan, prosedur dan kode praktik yang, secara keseluruhan atau sebagian, mengatur bagaimana risiko akan dikelola dalam konteks spesifik dokumen ini.

Praktik dan proses manajemen dari banyak organisasi saat ini mencakupi komponen manajemen risiko, dan banyak organisasi telah mengadopsi suatu proses manajemen risiko formal untuk jenis tertentu dari risiko atau keadaan. Dalam kasus tersebut, suatu organisasi dapat memutuskan untuk melakukan suatu tinjauan kritis terhadap praktik dan proses organisasi tersebut saat ini berlandaskan Standar ini.

Dalam Standar ini, ungkapan "manajemen risiko" dan "pengelolaan risiko" keduanya digunakan. Dalam istilah umum, "manajemen risiko" mengacu pada arsitektur (prinsip, kerangka kerja dan proses) dalam pengelolaan risiko secara efektif, sementara "pengelolaan risiko" mengacu pada penerapan arsitektur tersebut untuk risiko tertentu.




**Gambar 1 — Hubungan antara prinsip-prinsip, kerangka kerja dan proses manajemen risiko**

# Manajemen risiko - Prinsip dan pedoman

## 1 Ruang Lingkup

Standar ini menyediakan prinsip dan panduan generik mengenai manajemen risiko.

Standar ini dapat digunakan oleh perusahaan publik, swasta atau organisasi kemasyarakatan, asosiasi, kelompok ataupun individu manapun. Oleh karena itu Standar ini tidak dikhususkan untuk industri atau sektor tertentu.

**CATATAN** Untuk kenyamanan, semua pengguna yang berbeda-beda dari Standar ini secara umum disebut “organisasi”.

Standar ini dapat diterapkan pada sepanjang usia sebuah organisasi dan pada beragam kegiatan termasuk strategi dan keputusan, operasi, proses, fungsi, proyek, produk, layanan dan aset. Standar ini dapat diterapkan pada sebarang jenis risiko, apapun sifatnya, baik yang memiliki konsekuensi positif maupun negatif.

Walaupun Standar ini menyediakan panduan generik, hal ini tidak dimaksudkan untuk mendukung keseragaman manajemen risiko antar organisasi. Rancangan dan pengimplementasian rencana manajemen risiko dan kerangka kerja perlu mempertimbangkan berbagai kebutuhan organisasi tertentu dengan tujuan khususnya, konteks, struktur, operasi, proses, fungsi, proyek, produk, jasa atau aset dan praktik spesifik yang digunakan.

Standar ini dimaksudkan untuk dimanfaatkan bagi penyelarasan proses manajemen risiko pada standar yang telah ada dan yang akan datang. Standar ini menyediakan pendekatan umum guna menunjang standar yang berkaitan dengan risiko spesifik dan atau sektor, serta tidak menggantikan standar-standar tersebut.

Standar ini tidak dimaksudkan untuk tujuan sertifikasi.

## 2 Istilah dan definisi

Dalam dokumen ini, diberlakukan istilah dan definisi berikut .

**2.1**
**risiko**
efek dari ketidakpastian pada sasaran

**CATATAN 1** Efek merupakan penyimpangan dari apa yang diharapkan – positif dan/atau negatif

**CATATAN 2** Sasaran bisa mempunyai berbagai aspek (seperti keuangan, kesehatan dan keselamatan, serta tujuan lingkungan) dan dapat diterapkan pada berbagai tingkatan (seperti strategis, organisasi secara luas, proyek, produk, dan proses)

**CATATAN 3** Risiko sering dinyatakan dengan mengacu pada potensi **kejadian** (2.17) potensial dan **konsekuensi** (2.18), atau kombinasi dari keduanya

**CATATAN 4** Risiko sering dinyatakan dalam kombinasi dari konsekuensi dari suatu kejadian (termasuk perubahan keadaan) dan dikaitkan dengan **kemungkinan-kejadian** (2.19) terjadinya peristiwa tersebut.

**CATATAN 5** Ketidakpastian merupakan keadaan, meskipun hanya sebagian, kekurangan informasi yang berkaitan dengan, pemahaman atau pengetahuan, kejadian, konsekuensinya, atau kemungkinan-kejadian.

[ISO Guide 73:2009, definisi 1.1]

**2.2**
**manajemen risiko**
kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi terkait dengan **risiko** (2.1)

[ISO Guide 73:2009, definisi 2.1]

**2.3**
**kerangka kerja manajemen risiko**
seperangkat komponen yang menyediakan landasan dan pengaturan organisasi untuk perancangan, pelaksanaan, **pemantauan** (2.28), peninjauan dan peningkatan **manajemen risiko** (2.2) secara berkala di seluruh organisasi

**CATATAN 1** Landasan meliputi kebijakan, sasaran, mandat dan komitmen untuk mengelola **risiko** (2.1).

**CATATAN 2** Perangkat organisasi termasuk rencana, hubungan, akuntabilitas, sumber daya, proses dan berbagai kegiatan.

**CATATAN 3** Kerangka kerja manajemen risiko menyatu dalam kebijakan operasional dan praktik organisasi secara keseluruhan.

[ISO Guide 73:2009, definisi 2.1.1]

**2.4**
**kebijakan manajemen risiko**
pernyataan dari keseluruhan maksud dan arah suatu organisasi yang terkait dengan **manajemen risiko** (2.2)

[ISO Guide 73:2009, definisi 2.1.2]

**2.5**
**sikap terhadap risiko**
pendekatan dari suatu organisasi untuk menilai risiko dan akhirnya memutuskan untuk mengejar, mempertahankan, mengambil atau berpaling dari **risiko** (2.1)

[ISO Guide 73:2009, definition 3.7.1.1]

**2.6**
**rencana manajemen risiko**
skema dalam **kerangka kerja manajemen risiko** (2.3) dalam penetapan suatu pendekatan, komponen manajemen dan sumber daya untuk diterapkan pada pengelolaan **risiko** (2.1)

**CATATAN 1** Komponen manajemen biasanya meliputi prosedur, praktik, pembagian tanggung jawab, urutan dan waktu kegiatan.

**CATATAN 2** Rencanaan manajemen risiko dapat diterapkan untuk produk tertentu, proses dan proyek, serta sebagian atau keseluruhan organisasi.

[ISO Guide 73:2009, definisi 2.1.3]

**2.7**
**pemilik risiko**
orang atau entitas dengan akuntabilitas dan wewenang untuk mengelola **risiko** (2.1)

[ISO Guide 73:2009, definition 3.5.1.5]

**2.8**
**proses manajemen risiko**
penerapan sistematis dari kebijakan manajemen, prosedur dan pelaksanaan untuk kegiatan pengkomunikasian, pengkonsultasian, penetapan konteks, dan pengidentifikasian, penganalisaan, pengevaluasian, perlakuan, **pemantauan** (2.28) dan peninjauan **risiko** (2.1)

[ISO Guide 73:2009, definisi 3.1]

**2.9**
**penetapan suatu konteks**
pendefinisian parameter eksternal dan internal yang diperhitungkan pada saat pengelolaan risiko, dan penentuan ruang lingkup serta **kriteria risiko** (2.22) dalam menyusun **kebijakan manajemen risiko** (2.4)

[ISO Guide 73:2009, definisi 3.3.1]

**2.10**
**konteks eksternal**
lingkungan eksternal di mana organisasi berusaha untuk mencapai sasarannya

**CATATAN** Konteks eksternal dapat mencakupi:

- budaya, sosial, politik, hukum, peraturan, keuangan, teknologi, ekonomi, alam dan lingkungan kompetitif, baik internasional, nasional, regional atau lokal;
- pendorong utama dan tren yang memiliki dampak pada sasaran organisasi; dan
- hubungan terkait, persepsi dan nilai-nilai dari **pemangku kepentingan** (2.13) eksternal.

[ISO Guide 73:2009, definisi 3.3.1.1]

**2.11**
**konteks internal**
lingkungan internal di mana organisasi berusaha untuk mencapai sasarannya

**CATATAN** Konteks internal mencakupi:

- tata kelola, struktur organisasi, peran dan akuntabilitas;
- kebijakan, sasaran, dan strategi yang tepat untuk mencapainya;
- kemampuan, pemahaman dalam hal sumber daya dan pengetahuan (misalnya modal, waktu, orang, proses, sistem dan teknologi);
- sistem informasi, arus informasi dan proses membuat keputusan (baik formal maupun informal);
- hubungan terkait, persepsi dan nilai-nilai dari pemangku kepentingan internal.
- budaya organisasi;
- standar, pedoman dan model yang diadopsi oleh organisasi; dan

- bentuk dan cakupan hubungan kontraktual.

[ISO Guide 73:2009, definisi 3.3.1.2]

**2.12**
**komunikasi dan konsultasi**
proses terus menerus serta berulang yang dilakukan oleh organisasi untuk menyediakan, membagi atau memperoleh informasi, dan untuk terlibat dalam dialog dengan **para pemangku kepentingan** (2.13) mengenai pengelolaan **risiko** (2.1)

**CATATAN 1** Informasi dapat berhubungan dengan keberadaan, sifat, bentuk, kemungkinan-kejadian (2.19), signifikansi, evaluasi, akseptabilitas dan perlakuan pengelolaan risiko.

**CATATAN 2** Konsultasi adalah suatu proses dua arah dari komunikasi yang terinformasi antara organisasi dan para pemangku kepentingan pada sebuah isu sebelum membuat keputusan atau menentukan arah pada isu tersebut.
Konsultasi adalah:

- suatu proses yang berdampak terhadap keputusan melalui pengaruh dan ketimbang melalui kekuasaan; dan
- bukan pengambilan keputusan secara bersama, melainkan suatu masukan untuk pengambilan keputusan.

[ISO Guide 73:2009, definisi 3.2.1]

**2.13**
**pemangku kepentingan**
orang atau organisasi yang dapat mempengaruhi, dapat dipengaruhi, atau memiliki persepsi bahwa mereka dapat dipengaruhi oleh suatu keputusan atau kegiatan

**CATATAN** Seorang pembuat keputusan bisa menjadi pemangku kepentingan.

[ISO Guide 73:2009, definisi 3.2.1.1]

**2.14**
**penilaian risiko**
keseluruhan proses dari **identifikasi risiko** (2.15), **analisis risiko** (2.21) serta **evaluasi risiko** (2.24)

[ISO Guide 73:2009, definisi 3.4.1]

**2.15**
**identifikasi risiko**
proses penemuan, pengenalan dan pendeskripsian **risiko** (2.1)

**CATATAN 1** Identifikasi risiko melibatkan pengidentifikasian sumber risiko (2.16), kejadian (2.17), penyebab dan potensi konsekuensi (2.18) mereka.

**CATATAN 2** Identifikasi risiko dapat melibatkan data historis, analisis teoretis, informasi dan pendapat ahli, serta kebutuhan pemangku kepentingan (2.13).

[ISO Guide 73:2009, definisi 3.5.1]

**2.16**
**sumber risiko**
elemen baik dalam bentuk tunggal atau dalam kombinasi, yang memiliki potensi intrinsik menimbulkan **risiko** (2.1)

**CATATAN** Suatu sumber risiko dapat berwujud atau tidak berwujud.

[ISO Guide 73:2009, definisi 3.5.1.2]

**2.17**
**kejadian**
peristiwa atau perubahan dari suatu keadaan tertentu

**CATATAN 1** Suatu kejadian dapat menjadi satu atau lebih peristiwa, dan dapat memiliki beberapa penyebab.

**CATATAN 2** Suatu kejadian dapat terdiri dari sesuatu yang tidak terealisasi.

**CATATAN 3** Suatu kejadian kadang-kadang disebut sebagai "insiden" atau "kecelakaan".

**CATATAN 4** Suatu kejadian tanpa **konsekuensi** (2.18) juga dapat disebut sebagai "nyaris terjadi", "insiden", "nyaris kena" atau "close call".

[ISO Guide 73:2009, definisi 3.5.1.3]

**2.18**
**konsekuensi**
hasil dari **kejadian** (2.17) yang mempengaruhi sasaran

**CATATAN 1** Suatu kejadian dapat menyebabkan berbagai konsekuensi.

**CATATAN 2** Konsekuensi bisa pasti atau tidak pasti serta dapat memiliki efek positif atau negatif pada sasaran.

**CATATAN 3** Konsekuensi dapat dinyatakan secara kualitatif maupun kuantitatif.

**CATATAN 4** Konsekuensi awal dapat memicu efek berantai.

[ISO Guide 73:2009, definisi 3.6.1.3]

**2.19**
**kemungkinan-kejadian**
peluang terealisasinya sesuatu

**CATATAN 1** Dalam terminologi manajemen risiko, kata "kemungkinan-kejadian" digunakan untuk merujuk pada peluang terealisasinya sesuatu, apakah didefinisikan, diukur atau ditentukan secara obyektif atau subyektif, kualitatif maupun kuantitatif, dan dijelaskan menggunakan istilah umum atau matematis (seperti probabilitas atau frekuensi selama periode waktu tertentu).

**CATATAN 2** Istilah Bahasa Inggris "kemungkinan-kejadian (likelihood)" tidak memiliki kesetaraan langsung dalam beberapa bahasa lain; bahkan, sering setara dengan istilah "probabilitas". Namun, dalam bahasa Inggris, "probability (probabilitas)" sering ditafsirkan secara sempit sebagai istilah matematika. Oleh karena itu, dalam terminologi manajemen risiko, "kemungkinan-kejadian" digunakan dengan maksud bahwa memiliki interpretasi yang luas sama dengan istilah "probabilitas" dalam banyak bahasa lain selain bahasa Inggris.

[ISO Guide 73:2009, definisi 3.6.1.1]

**2.20**
**profil risiko**
deskripsi dari sekelompok **risiko** (2.1)

**CATATAN** Sekelompok risiko dapat berisi risiko yang berkaitan dengan keseluruhan organisasi, sebagian dari organisasi, atau sebagaimana yang didefinisikan berbeda tanpa mengubah makna.

[ISO Guide 73:2009, definisi 3.8.2.5]

**2.21**
**analisis risiko**
proses untuk memahami sifat **risiko (**2.1) serta untuk menentukan **tingkat risiko** (2.23)
**CATATAN 1** Analisis risiko memberikan dasar untuk **evaluasi risiko** (2.24) serta keputusan dalam **perlakuan risiko** (2.25)

**CATATAN 2** Analisis risiko mencakupi estimasi risiko.

[ISO Guide 73:2009, definisi 3.6.1]

**2.22**
**kriteria risiko**
rincian acuan yang menjadi dasar untuk evaluasi signifikansi **risiko** (2.1)

**CATATAN 1** Kriteria risiko didasarkan pada sasaran organisasi, serta konteks **eksternal** (2.10) dan **konteks internal** (2.11).

**CATATAN 2** Kriteria risiko dapat diturunkan dari standar, hukum, kebijakan dan persyaratan lainnya.

[ISO Guide 73:2009, definisi 3.3.1.3]

**2.23**
**tingkat risiko**
besarnya **risiko** (2.1) atau kombinasi risiko, dinyatakan dalam kombinasi **konsekuensi** (2.18) dan **kemungkinan-kejadian** (2.19) mereka

[ISO Guide 73:2009, definisi 3.6.1.8]

**2.24**
**evaluasi risiko**
Proses membandingkan hasil **analisis risiko** (2.21) dengan **kriteria risiko** (2.22) untuk menentukan apakah **risiko** (2.1) dan/atau besarannya diterima atau ditoleransi

**CATATAN** Evaluasi risiko membantu dalam keputusan tentang **perlakuan risiko** (2.25).

[ISO Guide 73:2009, definisi 3.7.1]

**2.25**
**perlakuan risiko**
proses untuk memodifikasi **risiko** (2.1)

**CATATAN 1** Perlakuan Risiko dapat melibatkan:

- penghindaran risiko dengan memutuskan untuk tidak memulai atau melanjutkan kegiatan yang menimbulkan risiko;
- pengambilan atau peningkatkan risiko untuk mengejar kesempatan;
- penyingkiran **sumber risiko** (2.16);
- pengubahan **kemungkinan-kejadian** (2.19);
- pengubahan **konsekuensi** (2.18);
- pembagian risiko dengan satu atau berbagai pihak (termasuk kontrak dan pembiayaan risiko); dan
- mempertahankan risiko dengan keputusanyang didasarkan pada informasi yang dianggap cukup.

**CATATAN 2** Perlakuan Risiko yang ditujukan pada konsekuensi negatif kadang-kadang disebut sebagai "mitigasi risiko", "penghilangan risiko", "pencegahan risiko" dan "pengurangan risiko".

**CATATAN 3** Perlakuan Risiko dapat menimbulkan risiko baru atau memodifikasi risiko yang ada.

**2.26**
**pengendalian**
tindakan yang memodifikasi **risiko** (2.1)

**CATATAN 1** Pengendalian mencakupi proses, kebijakan, perangkat, praktik, atau tindakan lain yang memodifikasi risiko.

**CATATAN 2** Pengendalian mungkin tidak selalu menghasilkan efek modifikasi seperti yang diinginkan atau diasumsikan.

[ISO Guide 73:2009, definisi 3.8.1.1]

**2.27**
**risiko residu**
**risiko** (2.1) yang tersisa setelah **perlakuan risiko** (2.25)

**CATATAN 1** Risiko residu dapat termasuk risiko yang tidak teridentifikasi.

**CATATAN 2** Risiko residu dapat dikenal juga sebagai "risiko dipertahankan".

[ISO Guide 73:2009, definisi 3.8.1.6]

**2.28**
**pemantauan**
pemeriksaan, pengawasan, pengobservasian atau penentuan secara kritis yang berkelanjutan terhadap status guna mengidentifikasi perubahan dari tingkat kinerja yang diperlukan atau diharapkan

**CATATAN** Pemantauan dapat diterapkan pada suatu **kerangka kerja manajemen risiko** (2.3), **proses manajemen risiko** (2.8), **risiko** (2.1) atau **pengendalian** (2.26).

[ISO Guide 73:2009, definisi 3.8.2.1]

**2.29**
**tinjauan**
kegiatan yang dilakukan untuk menentukan kesesuaian, kecukupan dan efektivitas dari pokok persoalan guna mencapai sasaran yang ditetapkan

**CATATAN** Tinjauan dapat diterapkan pada suatu **kerangka kerja manajemen risiko** (2.23), **proses manajemen risiko** (2.28), **risiko** (2,1) atau **pengendalian** (2.26).

[ISO Guide 73:2009, definisi 3.8.2.2]

## 3 Prinsip

Agar manajemen risiko efektif, sebuah organisasi pada berbagai tingkatan harus patuh pada prinsip-prinsip berikut.

a) **Manajemen risiko menciptakan dan melindung nilai**

Manajemen risiko berkontribusi pada pencapaian tujuan dan perbaikan kinerja yang dapat didemonstrasikan, dalam misalnya keselamatan dan kesehatan manusia, keamanan, kepatuhan pada hukum dan perundang-undangan, keberterimaan oleh publik, perlindungan lingkungan, mutu produk, manajemen proyek, efisiensi dalam operasi, tata kelola dan reputasi.

b) **Manajemen risiko adalah bagian terpadu dari semua proses dalam organisasi**

Manajemen risiko bukan kegiatan berdiri sendiri yang terpisah dari kegiatan dan proses utama dari sebuah organisasi. Manajemen risiko adalah bagian dari tanggung jawab manajemen dan merupakan bagian terpadu dari semua proses organisasi, termasuk perencanaan strategis dan semua proses manajemen proyek dan proses manajemen perubahan.

c) **Manajemen risiko merupakan bagian dari pengambilan keputusan**

Manajemen risiko membantu para pengambil keputusan untuk membuat pilihan berdasarkan informasi yang dianggap cukup, prioritas tindakan, dan membedakan antar berbagai alternatif tindakan.

d) **Manajemen risiko secara eksplisit ditujukan pada ketidakpastian**

Manajemen risiko secara eksplisit mempertimbangkan ketidakpastian, sifat dari ketidakpastian, dan bagaimana ketidakpastian tersebut disikapi.

e) **Manajemen risiko adalah sistematik, terstruktur dan tepat waktu**

Sebuah pendekatan yang terstruktur, tepat waktu dan sistematik pada manajemen risiko yang berkontribusi terhadap efisiensi dan hasil yang konsisten, dapat diperbandingkan dan andal.

f) **Manajemen risiko berdasarkan informasi terbaik yang tersedia**

Masukan pada proses pengelolaan risiko berdasarkan sumber-sumber informasi seperti data historis, pengalaman, umpan-balik pemangku kepentingan, observasi, prakiraan dan penilaian ahli. Namun, para pembuat keputusan harus memiliki informasi yang cukup bagi dirinya dan harus juga memperhitungkan keterbatasan data atau model yang digunakan atau kemungkinan perbedaan pendapat di antara para ahli.

g) **Manajemen risiko adalah disesuaikan penggunaannya**

Manajemen risiko diselaraskan dengan konteks eksternal dan internal organisasi, serta profil risiko.

h) **Manajemen risiko mempertimbangkan faktor manusia dan budaya**

Manajemen risiko mengakui kapabilitas, persepsi dan intensi dari pihak eksternal dan internal yang dapat memfasilitasi atau menghambat pencapaian sasaran organisasi.

i) **Manajemen risiko adalah transparan dan inklusif**

Keterlibatan yang layak dan tepat waktu dari para pemangku kepentingan, khususnya pengambil keputusan di semua tingkatan organisasi, memastikan bahwa manajemen risiko tetap relevan dan terkini. Keterlibatan juga membolehkan pemangku kepentingan untuk diwakili secara tepat serta guna mendapatkan pandangan mereka untuk dipertimbangkan dalam menentukan kriteria risiko.

j) **Manajemen risiko adalah dinamis, berulang dan responsif terhadap perubahan**

Manajemen risiko peka dan respon secara terus-menerus terhadap perubahan. Pada saat dilakukan pemantauan dan tinjauan risiko, akibat dari terjadinya peristiwa eksternal dan internal, konteks dan pengetahuan berubah maka risiko baru muncul, beberapa berubah dan lainnya menghilang.

k) **Manajemen risiko memfasilitasi perbaikan berkelanjutan dari organisasi**

Organisasi harus mengembangkan dan mengimplementasikan strategi untuk meningkatkan kematangan manajemen risiko bersamaan dengan semua aspek lain dari organisasi mereka.

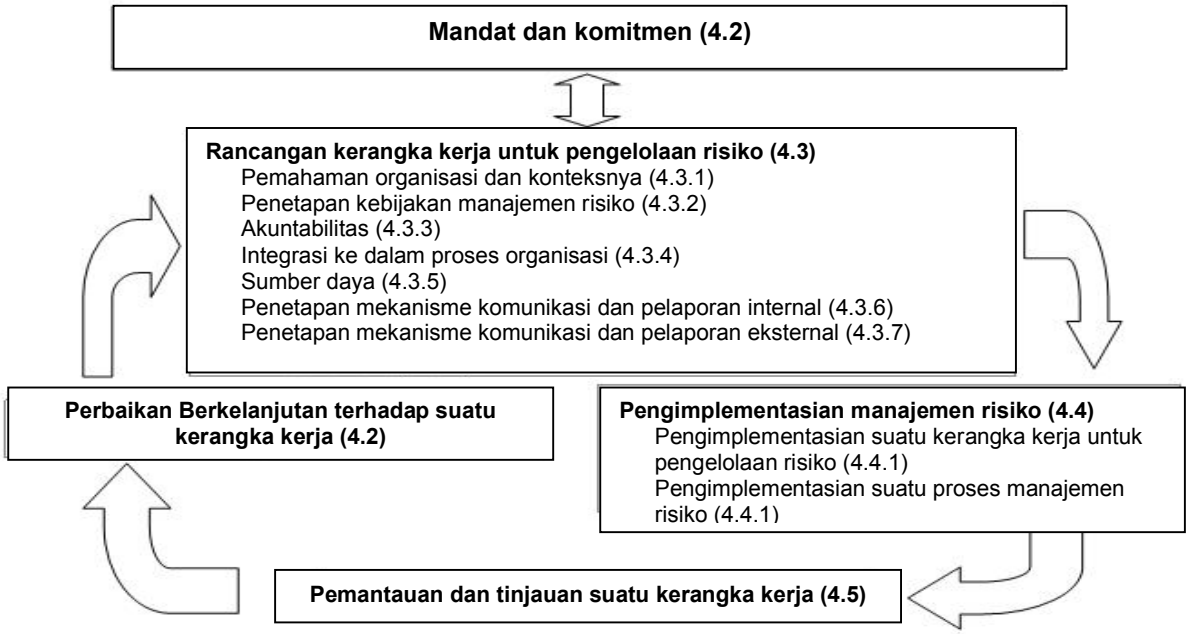
Lampiran A menyediakan saran lebih lanjut bagi organisasi yang ingin mengelola risiko secara lebih efektif.

## 4 Kerangka kerja

### 4.1 Umum

Suksesnya manajemen risiko akan tergantung pada efektifitas kerangka kerja manajemen yang menyediakan dasar dan pengaturan yang akan melekat pada keseluruhan organisasi pada semua tingkatan. Kerangka kerja tersebut membantu dalam pengelolaan risiko secara efektif melalui pengaplikasian dari proses manajemen risiko (lihat pasal 5) pada beragam tingkatan dan dalam konteks khusus organisasi. Kerangka kerja tersebut memastikan bahwa informasi mengenai risiko yang berasal dari proses manajemen risiko dilaporkan secara memadai serta digunakan sebagai dasar pengambilan keputusan dan akuntabilitas pada semua tingkatan organisasi secara relevan.

Pasal ini menguraikan komponen-komponen yang diperlukan dalam kerangka kerja bagi pengelolaan risiko serta bagaimana komponen tersebut saling berkaitan secara berulang, seperti yang tergambarkan pada Gambar 2.




**Gambar 2 - Hubungan antara komponen dari kerangka kerja bagi pengelolaan risiko**

Kerangka kerja ini tidak dimaksudkan untuk menjelaskan sebuah sistem manajemen, namun lebih untuk membantu organisasi untuk mengintegrasikan manajemen risiko ke dalam keseluruhan sistem manajemen. Oleh karena itu, organisasi sebaiknya mengadaptasi komponen-komponen dari kerangka kerja sesuai kebutuhan spesifik organisasi.

Jika di dalam praktik dan proses manajemen organisasi yang sudah ada melibatkan komponen-komponen dari manajemen risiko atau jika organisasi telah mengadopsi suatu proses manajemen risiko formal pada beberapa jenis risiko atau situasi, maka hal ini sebaiknya dinilai dan ditinjau secara kritis terhadap Standar ini, termasuk atribut-atribut yang terdapat dalam Lampiran A, dalam rangka menentukan efektivitas dan kecukupanya.

### 4.2 Mandat dan komitmen

Pengenalan manajemen risiko dan pemastian efektivitasnya yang sedang berjalan membutuhkan komitmen yang kuat dan berkelanjutan dari manajemen organisasi, seperti halnya perencanaan yang strategis dan teliti untuk mendapatkan komitmen di seluruh tingkatan. Dalam hal ini manajemen harus:

- menetapkan dan mengesahkan kebijakan manajemen risiko;
- memastikan bahwa budaya organisasi dan kebijakan manajemen risiko selaras;
- menentukan indikator kinerja manajemen risiko yang selaras dengan indikator kinerja organisasi;
- menyelaraskan sasaran manajemen risiko dengan sasaran dan strategi organisasi;
- memastikan kepatuhan peraturan dan hukum;
- menetapkan akuntabilitas dan tanggung jawab pada tingkat yang layak dalam organisasi;

- memastikan bahwa sumber daya yang diperlukan dialokasikan bagi manajemen risiko;
- mengkomunikasikan manfaat manajemen risiko kepada seluruh pemangku kepentingan; dan
- memastikan bahwa kerangka kerja untuk pengelolaan risiko selalu tetap layak.

### 4.3 Rancangan kerangka kerja untuk pengelolaan risiko

#### 4.3.1 Pemahaman organisasi dan konteksnya

Sebelum memulai rancangan dan implementasi kerangka kerja untuk pengelolaan risiko, adalah penting untuk memahami dan mengevaluasi baik konteks eksternal dan internal organisasi, karena hal ini dapat mempengaruhi rancangan kerangka kerja secara signifikan.

Pengevaluasian konteks eksternal organisasi dapat meliputi, namun tidak terbatas pada :

a) budaya dan sosial, politik, hukum, peraturan, keuangan, teknologi, ekonomi, alam dan lingkungan kompetitif, baik internasional, nasional, regional atau lokal;

b) pendorong utama dan tren yang memiliki dampak pada sasaran organisasi; dan

c) hubungan terkait, persepsi dan nilai-nilai dari pemangku kepentingan eksternal.

Pengevaluasian konteks internal organisasi dapat meliputi hal-hal berikut, tetapi tidak terbatas pada:

- tata kelola, struktur organisasi, peran dan akuntabilitas;
- kebijakan, sasaran, dan strategi yang tepat untuk mencapainya;
- kemampuan, pemahaman dalam hal sumber daya dan pengetahuan (misalnya modal, waktu, orang, proses, sistem dan teknologi);
- sistem informasi, arus informasi dan proses membuat keputusan (baik formal maupun informal);
- hubungan terkait, persepsi dan nilai-nilai dari pemangku kepentingan internal.
- budaya organisasi;
- standar, pedoman dan model yang diadopsi oleh organisasi; dan
- bentuk dan cakupan hubungan kontraktual.

#### 4.3.2 Penetapan kebijakan manajemen risiko

Kebijakan manajemen risiko sebaiknya menyatakan secara jelas sasaran organisasi bagi manajemen risiko, dan komitmen terhadap manajemen risiko serta biasanya membahas hal-hal berikut:

- alasan organisasi untuk mengelola risiko;
- keterkaitan antara sasaran dan kebijakan organisasi dengan kebijakan manajemen risiko;
- akuntabilitas dan tanggung jawab untuk pengelolaan risiko;

- bagaimana cara menangani kepentingan yang bertentangan;
- komitmen untuk menyediakan sumber daya yang diperlukan untuk membantu mereka yang akuntabel dan bertanggung jawab untuk pengelolaan risiko;
- bagaimana cara kinerja manajemen risiko akan diukur dan dilaporkan; serta
- komitmen untuk meninjau dan meningkatkan kerangka kerja dan kebijakan manajemen risiko secara berkala dan dalam merespon suatu peristiwa atau perubahan situasi.

Kebijakan manajemen risiko sebaiknya dikomunikasikan secara layak.

### 4.3.3 Akuntabilitas

Organisasi sebaiknya memastikan tersedianya akuntabilitas, kewenangan, dan kompetensi yang layak untuk pengelolaan risiko, termasuk pengimplementasian dan pemeliharaan proses manajemen risiko serta memastikan kecukupan, efektivitas, dan efisiensi dari setiap pengendalian. Hal ini dapat difasilitasi dengan:

- pengidentifikasian pemilik risiko yang memiliki akuntabilitas dan kewenangan untuk mengelola risiko;
- pengidentifikasian siapa yang akuntabel untuk pengembangan, pengimplementasian, dan pemeliharaan kerangka kerja untuk mengelola risiko;
- pengidentifikasian tanggung jawab lainnya dari personel pada semua tingkatan organisasi untuk proses manajemen risiko;
- penetapan ukuran kinerja dan proses eskalasi pelaporan eksternal dan/atau internal; dan
- pemastian tingkat pengakuan yang layak.

### 4.3.4 Integrasi ke dalam proses organisasi

Manajemen risiko sebaiknya menyatu dalam semua proses dan praktik organisasi dengan cara yang relevan, efektif, dan efisien. Proses manajemen risiko sebaiknya menjadi bagian dan tidak terpisahkan dari proses organisasi. Secara khusus, manajemen risiko sebaiknya menyatu dalam pengembangan kebijakan, perencanaan dan tinjauan bisnis dan strategis, serta proses manajemen perubahan.

Sebaiknya tersedia suatu rencana manajemen risiko secara luas di organisasi untuk memastikan bahwa kebijakan manajemen risiko diimplementasikan dan manajemen risiko tersebut menyatu dalam seluruh praktik dan proses organisasi. Rencana manajemen risiko dapat diintegrasikan ke dalam rencana lainnya dari organisasi, seperti suatu perencanaan strategis.

### 4.3.5 Sumber daya

Organisasi sebaiknya mengalokasikan sumber daya yang layak untuk manajemen risiko.

Pertimbangan sebaiknya diberikan untuk hal berikut ini:

- orang, ketrampilan, pengalaman, dan kompetensi;
- sumber daya yang dibutuhkan untuk setiap tahapan proses manajemen risiko;

- berbagai proses, metode, dan alat bantu organisasi untuk digunakan dalam pengelolaan risiko;
- proses dan prosedur yang terdokumentasi;
- sistem manajemen informasi dan ilmu pengetahuan; dan
- program pelatihan.

### 4.3.6 Penetapan mekanisme komunikasi dan pelaporan internal

Organisasi sebaiknya menetapkan mekanisme komunikasi dan pelaporan internal dalam rangka mendukung dan mendorong akuntabilitas dan kepemilikan risiko. Mekanisme ini sebaiknya dapat memastikan bahwa:

- komponen utama dari kerangka kerja manajemen risiko dan setiap modifikasi yang dilakukan setelahnya, agar dikomunikasikan dengan layak;
- terdapat pelaporan internal yang cukup mengenai efektifitas dan manfaat keluaran pada kerangka kerja manajemen risiko;
- informasi relevan yang diturunkan dari pengaplikasian manajemen risiko tersedia pada tingkatan yang layak dan waktu yang tepat; dan
- terdapat proses konsultasi dengan para pemangku kepentingan internal.

Mekanisme tersebut sebaiknya dengan layak mencakupi berbagai proses untuk mengkonsolidasikan informasi risiko dari berbagai sumber, dan mungkin diperlukan untuk mempertimbangkan sensitivitas dari informasi tersebut.

### 4.3.7 Penetapan mekanisme komunikasi dan pelaporan eksternal

Organisasi sebaiknya mengembangkan dan mengimplementasikan suatu rencana sebagaimana organisasi akan berkomunikasi dengan pemangku kepentingan eksternal. Hal tersebut sebaiknya melibatkan:

- pengikutsertaan pemangku kepentingan eksternal yang tepat dan memastikan pertukaran informasi yang efektif;
- pelaporan ke pihak eksternal dalam memenuhi persyaratan hukum, peraturan, dan kebutuhan tata kelola;
- penyediaan umpan balik dan pelaporan atas komunikasi dan konsultasi;
- pengunaan komunikasi untuk membangun kepercayaan dalam organisasi; dan
- pengkomunikasian dengan para pemangku kepentingan pada peristiwa krisis atau kontijensi.

Mekanisme tersebut sebaiknya mencakupi berbagai proses yang layak untuk mengkonsolidasikan informasi risiko dari berbagai sumber, dan mungkin diperlukan untuk mempertimbangkan sensitivitas dari informasi tersebut.

### 4.4 Pengimplementasian manajemen risiko

#### 4.4.1 Pengimplementasian suatu kerangka kerja untuk pengelolaan risiko

- dalam pengimplementasian kerangka kerja organisasi guna pengelolaan risiko, organisasi tersebut sebaiknya:
- mendefinisikan strategi dan waktu yang tepat untuk pengimplementasian kerangka kerja;
- menerapkan kebijakan dan proses manajemen risiko pada proses organisasi;
- mematuhi ketentuan hukum dan peraturan;
- memastikan bahwa pengambilan keputusan, termasuk pengembangan dan penentuan sasaran, telah diselaraskan dengan manfaat keluaran dari proses manajemen risiko;
- menyelenggarakan informasi dan sesi pelatihan; dan
- berkomunikasi dan berkonsultasi dengan para pemangku kepentingan untuk memastikan bahwa kerangka kerja manajemen risiko tetap layak.

#### 4.4.2 Pengimplementasian suatu proses manajemen risiko

Manajemen risiko sebaiknya diimplementasikan dengan memastikan bahwa proses manajemen risiko yang dijelaskan dalam Pasal 5 diterapkan melalui suatu rencana manajemen risiko disemua tingkatan dan fungsi yang relevan dari organisasi sebagai bagian dari praktik dan proses organisasi.

### 4.5 Pemantauan dan tinjauan suatu kerangka kerja

Dalam rangka memastikan bahwa manajemen risiko berjalan efektif dan terus mendukung kinerja organisasi, organisasi tersebut sebaiknya:

- mengukur kinerja manajemen risiko terhadap berbagai indikator, yang ditinjau secara berkala untuk kelayakannya;
- secara berkala mengukur kemajuan, dan penyimpangan atas rencana manajemen risiko;
- secara berkala dilakukan tinjauan apakah kerangka kerja, kebijakan, dan rencana manajemen risiko masih layak, berdasarkan konteks eksternal dan internal organisasi;
- melaporkan mengenai risiko, kemajuan rencana manajemen risiko, dan sejauh mana kebijakan manajemen risiko diikuti; dan
- melakukan tinjauan efektivitas dari kerangka kerja manajemen risiko.

### 4.6 Perbaikan berkelanjutan terhadap suatu kerangka kerja

Berdasarkan hasil pemantauan dan tinjauan, keputusan sebaiknya dibuat mengenai bagaimana kerangka kerja, kebijakan, dan rencana manajemen risiko dapat ditingkatkan. Keputusan ini sebaiknya menuntun untuk perbaikan pada pengelolaan risiko organisasi serta budaya manajemen risiko organisasi.

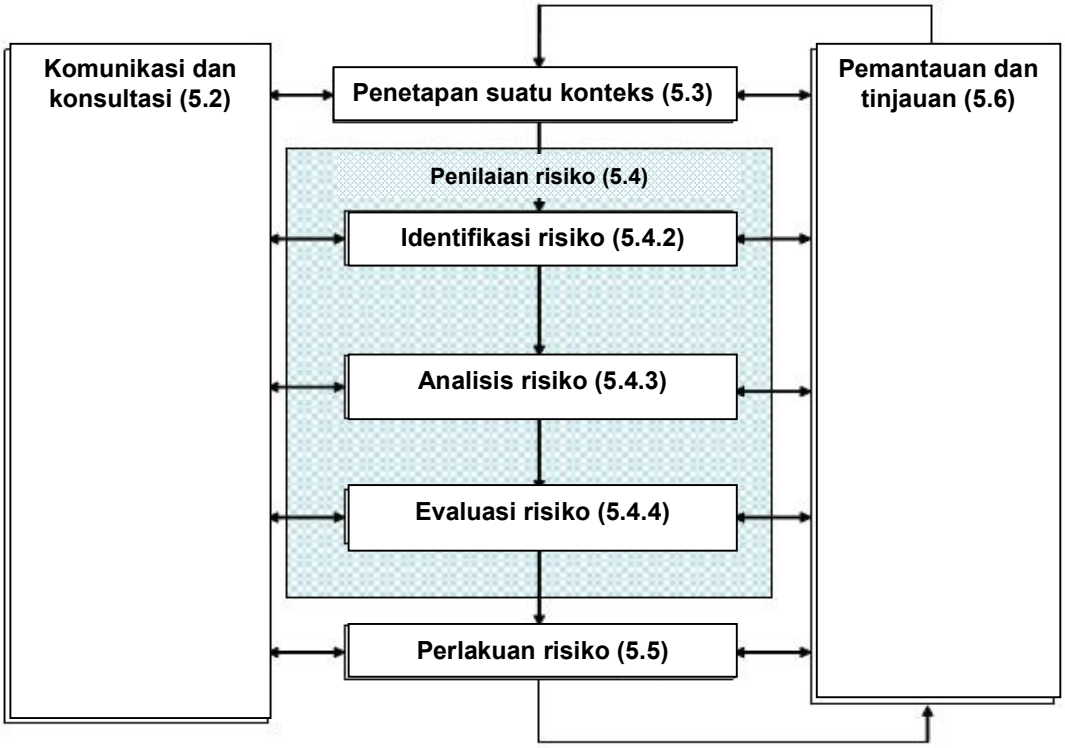
## 5 Proses

### 5.1 Umum

Proses manajemen risiko sebaiknya:

- bagian yang terpadu dari manajemen,
- menyatu dalam budaya dan praktik, dan
- disesuaikan penggunaannya dengan proses bisnis organisasi.

Hal ini terdiri dari kegiatan yang dijelaskan dalam 5.2 sampai dengan 5.6. Proses manajemen risiko ditunjukkan pada Gambar 3.




**Gambar 3 – Proses manajemen risiko**

### 5.2 Komunikasi dan konsultasi

Komunikasi dan konsultasi dengan pemangku kepentingan eksternal dan internal sebaiknya dilaksanakan selama proses manajemen risiko disemua tahapan.

Oleh karena itu, rencana komunikasi dan konsultasi sebaiknya dikembangkan sejak tahap awal. Rencana ini sebaiknya membahas isu yang berkaitan dengan risiko itu sendiri, penyebabnya, konsekuensinya (jika diketahui), dan tindakan yang perlu diambil untuk mengatasinya. Komunikasi dan konsultasi eksternal dan internal yang efektif sebaiknya ada untuk memastikan bahwa pihak yang akuntabel untuk pengimplementasian proses

manajemen risiko, serta para pemangku kepentingan terkait memahami dasar dari keputusan yang dibuat dan alasan mengapa langkah tertentu dibutuhkan.
Suatu pendekatan tim konsultatif dapat:

- membantu menentukan konteks dengan layak;
- memastikan bahwa kepentingan dari pemangku kepentingan dipahami dan dipertimbangkan;
- membantu memastikan bahwa risiko teridentifikasikan secara cukup;
- melibatkan bidang keahlian yang berbeda untuk bersama-sama menganalisis risiko;
- memastikan bahwa pandangan yang berbeda dipertimbangkan dengan layak dalam pendefinisian kriteria risiko dan dalam evaluasi risiko;
- menjamin pengesahan dan dukungan atas suatu rencana perlakuan risiko;
- memperkuat manajemen perubahan yang layak selama proses manajemen risiko; dan
- mengembangkan suatu rencana konsultasi serta komunikasi internal dan eksternal yang tepat.

Komunikasi dan konsultasi dengan para pemangku kepentingan adalah penting karena mereka memberikan penilaian tentang risiko berdasarkan persepsi mereka. Persepsi tersebut dapat beragam karena perbedaaan para pemangku kepentingan dalam hal perhatian, konsep, asumsi, kebutuhan, dan nilai. Persepsi dari pemangku kepentingan sebaiknya diperhitungkan, terekam, dan teridentifikasi dalam proses pengambilan keputusan karena pandangan mereka dapat memiliki dampak signifikan pada suatu keputusan yang dibuat.

Komunikasi dan konsultasi sebaiknya menfasilitasi pertukaran informasi yang benar, relevan, akurat serta dapat dimengeti, dengan memperhitungkan aspek kerahasiaan dan integritas personal.

### 5.3 Penetapan suatu konteks

#### 5.3.1 Umum

Dengan penetapan suatu konteks, organisasi tersebut mengartikulasikan sasarannya, mendefinisikan parameter internal dan eksternal yang diperhitungkan pada saat pengelolaan risiko, serta menetapkan lingkup kerja dan kriteria risiko untuk proses yang masih ada. Meski banyak dari parameter tersebut serupa dengan hal yang dipertimbangkan saat merancang kerangka kerja manajemen risiko (bagian 4.3.1), ketika penetapan suatu konteks pada proses manajemen risiko, parameter-parameter tersebut perlu dipertimbangkan jauh lebih rinci dan khususnya bagaimana parameter tersebut terkait dengan ruang lingkup dari suatu proses manajemen risiko tertentu.

#### 5.3.2 Penetapan suatu konteks eksternal

Konteks eksternal adalah lingkungan eksternal di mana organisasi berusaha untuk mencapai sasarannya.

Memahami suatu konteks eksternal adalah penting untuk memastikan bahwa sasaran dan perhatian dari pemangku kepentingan eksternal dipertimbangkan saat mengembangkan

kriteria risiko. Hal tersebut berdasarkan pada konteks organisasi secara luas, tetapi dengan rincian persyaratan ketentuan hukum dan peraturan yang spesifik, persepsi para pemangku kepentingan serta aspek risiko lainnya yang spesifik pada ruang lingkup dari proses manajemen risiko.

Suatu konteks eksternal dapat mencakupi, tetapi tidak terbatas pada:

- budaya, sosial, politik, hukum, peraturan, keuangan, teknologi, ekonomi, alam dan lingkungan kompetitif, baik internasional, nasional, regional atau lokal;
- pendorong utama dan tren yang memiliki dampak pada sasaran organisasi; dan
- hubungan terkait, persepsi dan nilai-nilai dari pemangku kepentingan eksternal.

### 5.3.3 Penetapan suatu konteks internal

Suatu konteks internal adalah lingkungan internal di mana organisasi berusaha untuk mencapai sasarannya.

Proses manajemen risiko sebaiknya diselaraskan dengan budaya, proses, struktur, dan strategi organisasi. Konteks internal adalah segala sesuatu di dalam organisasi yang dapat mempengaruhi bagaimana cara organisasi akan mengelola risiko. Hal ini sebaiknya ditetapkan karena:

a) manajemen risiko berada di dalam konteks sasaran organisasi;

b) sasaran dan kriteria dari proyek, proses atau kegiatan tertentu sebaiknya dipertimbangkan dalam rangka mencapai sasaran organisasi secara keseluruhan; dan

c) beberapa organisasi gagal untuk mengenali peluang guna mencapai sasaran strategis, sasaran proyek, atau sasaran bisnis, dan hal ini mempengaruhi komitmen, kredibilitas, kepercayaan, dan nilai organisasi yang sedang berjalan.

Adalah penting untuk memahami suatu konteks internal. Hal tersebut mencakupi, tetapi tidak terbatas pada:

- tata kelola, struktur organisasi, peran dan akuntabilitas;
- kebijakan, sasaran, dan strategi yang tepat untuk mencapainya;
- kemampuan, pemahaman dalam hal sumber daya dan pengetahuan (misalnya modal, waktu, orang, proses, sistem dan teknologi);
- hubungan terkait, persepsi dan nilai-nilai dari pemangku kepentingan internal.
- budaya organisasi;
- sistem informasi, arus informasi dan proses membuat keputusan (baik formal maupun informal);
- standar, pedoman dan model yang diadopsi oleh organisasi; dan
- bentuk dan cakupan hubungan kontraktual.

### 5.3.4 Penetapan suatu konteks dari proses manajemen risiko

Sasaran, strategi, ruang lingkup, dan parameter dari kegiatan oganisasi, atau bagian lain dari organisasi di mana proses manajemen risiko diterapkan, sebaiknya ditetapkan. Pengelolaan risiko sebaiknya dilakukan dengan penuh pertimbangan atas kebutuhan guna menjustifikasi penggunaan sumber daya dalam penyelenggaraan manajemen risiko. Sumber daya yang diperlukan, tanggung jawab dan wewenang, serta rekaman yang akan disimpan sebaiknya juga terperinci.

Suatu konteks dari proses manajemen risiko akan beragam sesuai dengan kebutuhan organisasi. Hal ini dapat meliputi, tetapi tidak terbatas pada:

- pendefinisian tujuan dan sasaran dari kegiatan manajemen risiko;
- pendefinisian tanggung jawab untuk dan dalam proses manajemen risiko;
- pendefinisian ruang lingkup, serta kedalaman dan keluasan dari aktivitas manajemen risiko yang akan diselenggarakan, termasuk penyertaan dan pengecualian yang spesifik;
- pendefinisian kegiatan, proses, fungsi, proyek, produk, jasa, atau aset dalam kaitannya dengan lokasi dan waktu;
- pendefinisian hubungan antara proyek, proses, atau aktivitas tertentu dengan proyek, proses, atau aktivitas lain dari organisasi;
- pendefinisian metodologi penilaian risiko;
- pendefinisian cara kinerja dan efektivitas manajemen risiko dievaluasi;
- pengidentifikasian dan penspesifikasian keputusan-keputusan yang sebaiknya diambil; dan
- pengidentifikasian, pelingkupan, ataupun pengerangkaan studi yang diperlukan, cakupan dan sasarannya, serta sumber daya yang diperlukan untuk melakukan studi tersebut.

Perhatian pada hal tersebut dan faktor lain yang relevan sebaiknya membantu meyakinkan bahwa pendekatan manajemen risiko yang digunakan sesuai dengan keadaan, sesuai dengan organisasi dan sesuai dengan risiko yang dapat mempengaruhi pencapaian sasaran organisasi.

### 5.3.5 Pendefinisian kriteria risiko

Organisasi sebaiknya mendefinisikan kriteria risiko yang akan digunakan untuk mengevaluasi signifikansi risiko. Kriteria tersebut sebaiknya merefleksikan nilai, sasaran serta sumber daya organisasi. Beberapa kriteria dapat dikenakan oleh, atau diturunkan dari, persyaratan hukum dan peraturan serta persyaratan lain yang diikuti oleh organisasi. Kriteria risiko sebaiknya konsisten dengan kebijakan manajemen risiko (lihat 4.3.2), didefinisikan pada awal di setiap proses manajemen risiko, dan ditinjau secara berkesinambungan.

- saat pendefinisian kriteria risko, beberapa faktor untuk diperhatikan sebaiknya mencakupi berikut ini:
- sifat dan jenis penyebab dan konsekuensi yang dapat terjadi dan bagaimana hal tersebut akan diukur;

- bagaimana kemungkinan-kejadian akan didefinisikan;
- kerangka waktu dari kemungkinan-kejadian dan/atau konsekuensinya;
- bagaimana tingkat risiko akan ditentukan;
- pandangan dari para pemangku kepentingan;
- tingkat risiko yang dapat diterima atau dapat ditolerir; dan
- apakah kombinasi risiko berganda sebaiknya diperhitungkan, dan jika demikian, bagaimana dan kombinasi mana yang sebaiknya dipertimbangkan.

### 5.4 Penilaian risiko

#### 5.4.1 Umum

Penilaian risiko adalah keseluruhan proses dari identifikasi risiko, analisis risiko serta evaluasi risiko.

**CATATAN** ISO/IEC 31010 menyediakan panduan teknik penilaian risiko

#### 5.4.2 Identifikasi risiko

Organisasi sebaiknya mengidentifikasi sumber risiko, area dampak, kejadian (termasuk perubahan dalam berbagai keadaan) dan penyebabnya, serta potensi konsekuensinya. Tujuan dari tahapan ini adalah menghasilkan suatu daftar risiko yang komprehensif berdasarkan kejadian yang mungkin membuat, memperkuat, mencegah, menurunkan, mempercepat, atau menunda pencapaian sasaran. Adalah penting untuk mengidentifikasi risiko yang terasosiasikan bila tidak mengejar kesempatan. Identifikasi secara komprehensif adalah kritis, karena suatu risiko yang tidak teridentifikasi pada tahapan ini tidak akan dimasukkan pada analisis lebih lanjut.

Identifikasi sebaiknya mencakupi risiko, baik sumber risiko dalam kendali atau di luar kendali organisasi, meskipun sumber risiko tersebut atau penyebabnya mungkin tidak ada bukti. Identifikasi risiko sebaiknya mencakupi pengujian dari efek yang berimbas pada konsekuensi tertentu, termasuk efek-efek kumulatif dan aliran selanjutnya. Identifikasi sebaiknya mempertimbangkan pula konsekuensi secara luas meskipun jika sumber risiko atau penyebab mungkin tidak ada bukti. Dan juga pengidentifikasian apa yang mungkin terjadi, adalah penting untuk mempertimbangkan kemungkinan penyebab dan skenario yang menunjukkan konsekuensi apa yang dapat terjadi. Seluruh konsekuensi dan penyebab signifikan sebaiknya dipertimbangkan.

Organisasi sebaiknya menerapkan alat bantu dan teknik identifikasi risiko yang cocok dengan sasarannya dan kemampuannya, dan guna menghadapi risiko. Informasi yang relevan dan terkini adalah penting dalam identifikasi risiko. Hal ini sebaiknya termasuk latar belakang informasi yang layak jika memungkinkan. Orang dengan pengetahuan yang sesuai sebaiknya dilibatkan dalam pengidentifikasian risiko.

#### 5.4.3 Analisis risiko

Analisis risiko melibatkan pengembangan suatu pemahaman atas risiko. Analisis risiko ini menyediakan suatu masukan dalam evaluasi risiko dan dalam membuat keputusan apakah risiko membutuhkan perlakuan atau tidak, serta keputusan dalam penentuan metodologi dan strategi perlakuan risiko yang paling layak. Analisis risiko juga dapat menyediakan

suatu masukan dalam pengambilan keputusan di mana ada beberapa pilihan harus dibuat dan berbagai opsi yang melibatkan jenis dan tingkatan risiko yang berbeda-beda.

Analisis risiko melibatkan pertimbangan atas penyebab dan sumber risiko, konsekuensi positif dan negatif, serta kemungkinan-kejadian konsekuensi tersebut dapat terjadi. Faktor-faktor yang mempengaruhi konsekuensi dan kemungkinan-kejadian sebaiknya diidentifikasi. Risiko dianalisis dengan menentukan konsekuensi dan kemungkinan-kejadian konsekuensi tersebut, serta atribut lain dari risiko tersebut. Suatu kejadian dapat mempunyai konsekuensi berganda serta dapat mempengaruhi sasaran berganda. Pengendalian yang ada serta efektifitas dan efisiensinya sebaiknya juga diperhitungkan.

Bagaimana cara konsekuensi dan kemungkinan-kejadian dinyatakan dan dikombinasikan untuk menentukan suatu tingkat risiko, sebaiknya mencerminkan jenis risiko, ketersediaan informasi dan tujuan dari keluaran atas penilaian risiko akan digunakan. Semua hal tersebut sebaiknya konsisten dengan kriteria risiko. Adalah penting untuk mempertimbangkan saling ketergantungan antara risiko-risiko satu sama lain dan dengan sumber risikonya.

Keyakinan dalam menentukan tingkat dan sensitivitas risiko untuk prakondisi dan asumsi sebaiknya dipertimbangan dalam analisis, dan secara layak dikomunikasikan secara efektif kepada para pengambil keputusan, dan kepada pemangku kepentingan lainnya. Faktor-faktor seperti keragaman pendapat para ahli, ketidakpastian, ketersediaan, kualitas, kuantitas, serta relevansi informasi yang tersedia, atau keterbatasan pemodelan sebaiknya dinyatakan dan dapat ditonjolkan.

Analisis risiko dapat dilaksanakan dengan tingkat kerincian yang bervariasi, tergantung pada risiko tersebut, tujuan dari analisis, serta informasi, data dan sumber daya yang tersedia. Analisis dapat berbentuk kualitatif, semi kualitatif atau kuantitatif, ataupun kombinasinya, tergantung keadaan.

Konsekuensi dan kemungkinan-kejadiannya dapat ditentukan dengan pemodelan manfaat keluaran atas suatu atau sekumpulan kejadian, atau dengan ekstrapolasi dari studi eksperimen atau dari data yang tersedia. Konsekuensi dapat dinyatakan dalam terminologi suatu dampak nyata dan tidak nyata. Dalam hal-hal tertentu, lebih dari satu nilai numerik atau keterangan dibutuhkan untuk menspesifikasikan konsekuensi dan kemungkinan-kejadiannya untuk waktu, tempat, kelompok atau situasi yang berbeda-beda.

### 5.4.4 Evaluasi risiko

Tujuan dari evaluasi risiko adalah membantu pengambilan keputusan, berdasarkan manfaat keluaran dari analisis risiko, tentang risiko mana yang membutuhkan perlakuan serta prioritas implementasi perlakuan.

Evaluasi risiko melibatkan pembandingan tingkat risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan ketika konteks tersebut dipertimbangkan. Berdasarkan pada perbandingan ini, kebutuhan untuk perlakuan dapat dipertimbangkan.

Keputusan sebaiknya memperhitungkan konteks risiko yang lebih luas dan mencakupi pertimbangan toleransi risiko yang ditanggung oleh para pihak di luar organisasi yang diuntungkan dari risiko. Keputusan sebaiknya dibuat sesuai dengan hukum, peraturan dan ketentuan lainnya.

Dalam keadaan tertentu, evaluasi risiko tersebut dapat mengarah pada suatu keputusan untuk melakukan analisis lebih lanjut. Evaluasi risiko tersebut juga dapat mengarah pada suatu keputusan untuk tidak memperlakukan risiko selain mempertahankan pengendalian

yang ada. Keputusan tersebut akan dipengaruhi oleh sikap risiko dari organisasi serta kriteria risiko yang telah ditetapkan.

### 5.5 Perlakuan risiko

#### 5.5.1 Umum

Perlakuan risiko melibatkan pemilihan satu opsi atau lebih untuk pemodifikasian risiko, dan pengimplementasian opsi tersebut. Begitu diimplementasikan, perlakuan risiko menyediakan atau memodifikasi pengendalian yang sudah ada.

Perlakuan risiko melibatkan suatu siklus proses yang terdiri dari:

- penilaian suatu perlakuan risiko;
- pemutusan apakah tingkat risiko residu dapat ditoleransi;
- jika tidak dapat ditoleransi, perlu dihasilkan suatu perlakuan risiko baru, dan
- penilaian efektifitas dari perlakuan risiko tersebut.

Opsi perlakuan risiko tidak perlu bersifat saling eksklusif atau layak di segala kondisi. Opsi tersebut dapat mencakupi hal berikut:

a) penghindaran suatu risiko dengan memutuskan untuk tidak memulai atau melanjutkan kegiatan yang menimbulkan risiko;

b) pengambilan atau peningkatan suatu risiko untuk mengejar suatu kesempatan;

c) penyingkiran suatu sumber risiko;

d) pengubahan suatu kemungkinan-kejadian;

e) pengubahan suatu konsekuensi;

f) pembagian suatu risiko dengan satu atau berbagai pihak lain (termasuk kontrak dan pembiayaan risiko); dan

g) mempertahankan suatu risiko dengan keputusan yang didasarkan pada informasi yang dianggap cukup.

#### 5.5.2 Pemilihan opsi perlakuan risiko

Pemilihan opsi perlakuan risiko yang paling layak melibatkan penyeimbangan biaya dan upaya implementasi dengan manfaat yang diperoleh yang berkaitan dengan hukum, peraturan, dan persyaratan lainnya, seperti tanggung jawab sosial serta perlindungan terhadap lingkungan alami. Keputusan sebaiknya juga memperhitungkan risiko yang perlakuan risikonya pasti tidak dapat dijustifikasi dengan dasar ekonomis, misalnya risiko tingkat keparahan tinggi (konsekuensi negatif tinggi) tetapi jarang (kemungkinan-kejadian rendah).

Sejumlah opsi perlakuan dapat dipertimbangkan dan diterapkan baik secara individual ataupun kombinasi. Organisasi biasanya memperoleh manfaat dari penerapan suatu kombinasi dari bebagai opsi perlakuan.

Dalam pemilihan opsi perlakuan risiko, suatu organisasi sebaiknya mempertimbangkan nilai-nilai dan persepsi para pemangku kepentingan serta cara yang paling layak untuk berkomunikasi dengan mereka. Ketika opsi perlakuan risiko dapat berdampak pada risiko di tempat lain dalam organisasi atau dengan pemangku kepentingan, mereka sebaiknya diikutsertakan dalam keputusan. Meski sama-sama efektif, beberapa perlakuan risiko dapat lebih diterima oleh para pemangku kepentingan daripada yang lain.

Suatu rencana perlakuan sebaiknya mengidentifikasi secara jelas urutan prioritas dalam hal perlakuan risiko individual sebaiknya diimplementasikan.

Perlakuan risiko itu sendiri dapat menghadirkan risiko. Suatu risiko yang signifikan dapat merupakan suatu kegagalan atau ketidakefektifan dari tindakan perlakuan risiko. Pemantauan perlu menjadi bagian terpadu dari suatu rencana perlakuan risiko untuk memberikan pemastian bahwa suatu tindakan tetap efektif.

Perlakuan risiko juga dapat menghadirkan suatu risiko sekunder yang perlu dinilai, diperlakukan, dipantau dan ditinjau. Risiko sekunder ini sebaiknya tergabung ke dalam suatu rencana perlakuan yang sama seperti risiko awal dan tidak diperlakukan sebagai suatu risiko baru. Kaitan antara dua risiko tersebut sebaiknya teridentifikasi dan terpelihara.

### 5.5.3 Persiapan dan pengimplementasian rencana perlakuan risiko

Tujuan dari rencana perlakuan risiko adalah untuk mendokumentasikan bagaimana opsi perlakuan yang terpilih akan diimplementasikan. Informasi yang tersedia dalam rencana perlakuan sebaiknya mencakupi:

- suatu alasan untuk memilih opsi perlakuan, termasuk manfaat yang diharapkan yang ingin diperoleh;
- pihak yang akuntabel untuk persetujuan suatu rencana dan pihak yang bertanggung jawab untuk pengimplementasian rencana tersebut;
- tindakan yang diusulkan;
- persyaratan sumber daya termasuk kontinjensi;
- pengukuran kinerja dan batasannya;
- persyaratan pelaporan dan pemantauan; serta
- waktu dan jadwal.

Rencana perlakuan sebaiknya terintegrasi dengan proses manajemen dalam organisasi dan didiskusikan dengan para pemangku kepentingan yang sesuai.

Pengambil keputusan dan pemangku kepentingan lainnya sebaiknya menyadari sifat dan tingkat risiko residu setelah perlakuan risiko. Risiko residu tersebut sebaiknya didokumentasikan dan menjadi hal yang perlu pemantauan, tinjauan dan, bila sesuai, perlakuan lebih lanjut.

## 5.6 Pemantauan dan tinjauan

Baik pemantauan maupun tinjauan sebaiknya menjadi suatu bagian yang terencana dalam proses manajemen risiko serta melibatkan pemeriksaan atau surveilen reguler. Hal tersebut dapat secara periodik atau ad hoc.

Tanggung jawab untuk pemantauan dan tinjauan sebaiknya didefinisikan secara jelas.

Proses pemantauan dan tinjauan dalam suatu organisasi sebaiknya mencakup semua aspek dari suatu proses manajemen risiko untuk tujuan dari:

- pemastian bahwa pengendalian efisien dan efektif baik rancangan maupun pelaksanaan;
- pengumpulan informasi lebih lanjut untuk mengembangkan penilaian risiko;
- analisis dan proses pembelajaran dari kejadian (termasuk peristiwa nyaris terjadi), perubahan, tren, keberhasilan dan kegagalannya;
- pendeteksian perubahan dalam konteks eksternal dan internal, termasuk perubahan pada kriteria risiko dan risiko itu sendiri yang dapat memerlukan revisi perlakuan serta prioritas risiko; dan
- pengidentifikasian risiko baru yang muncul.

Perkembangan dalam pengimplementasian rencana perlakuan risiko menyediakan ukuran kinerja. Hasil tersebut dapat digabungkan dalam keseluruhan manajemen kinerja organisasi, pengukuran kinerja organisasi, serta aktifitas pelaporan eksternal dan internal dari kinerja organisasi.

Hasil pemantauan dan tinjauan sebaiknya direkam, dan dilaporkan selayaknya kepada eksternal dan internal, dan sebaiknya juga digunakan sebagai masukan untuk suatu tinjauan terhadap kerangka kerja manajemen risiko (lihat 4.5).

### 5.7 Perekaman suatu proses manajemen risiko

Kegiatan manajemen risiko sebaiknya bisa ditelusuri. Dalam suatu proses manajemen risiko, rekaman menyediakan dasar bagi peningkatan dalam metode dan alat bantu, serta untuk keseluruhan proses.

Keputusan mengenai pembuatan rekaman sebaiknya memperhitungkan:

- kebutuhan organisasi untuk pembelajaran berkesinambungan;
- manfaat dari penggunaan kembali informasi untuk tujuan manajemen;
- biaya dan upaya yang terlibat dalam pembuatan dan pemeliharaan rekaman;
- kebutuhan hukum, peraturan dan operasional untuk rekaman;
- metode akses, kemudahan untuk memperoleh kembali dan media penyimpanan;
- periode retensi; dan
- sensitivitas informasi.

-

# Lampiran A
(informatif)
# Atribut manajemen risiko yang diperkuat

## A.1 Umum

Semua organisasi sebaiknya mengarahkan pada suatu tingkat kinerja yang layak dari kerangka kerja manajemen risikonya sejalan dengan tingkat kritis dari keputusan yang dibuat. Daftar atribut di bawah ini mewakili suatu tingkat kinerja yang tinggi dalam pengelolaan risiko. Untuk membantu organisasi dalam pengukuran kinerja mereka sendiri terhadap kriteria ini, beberapa indikator nyata diberikan untuk setiap atribut.

## A.2 Manfaat keluaran kunci

**A.2.1** Suatu organisasi memiliki pemahaman yang terkini, benar, dan komprehensif atas risikonya.

**A.2.2** Risiko suatu organisasi berada dalam lingkup kriteria risiko organisasi.

## A.3 Atribut-atribut

### A.3.1 Perbaikan terus-menerus

Suatu penekanan ditempatkan pada perbaikan terus-menerus dalam manajemen risiko melalui pengaturan tujuan kinerja organisasi, pengukuran kinerja organisasi, tinjauan kinerja organisasi serta modifikasi selanjutnya atas proses, sistem, sumber daya, kapabilitas dan keterampilan.

Hal ini dapat diindikasikan melalui eksistensi dari tujuan kinerja yang eksplisit baik terhadap kinerja organisasi maupun kinerja manajer secara individu yang diukur. Kinerja suatu organisasi dapat dipublikasikan dan dikomunikasikan. Pada umumnya, tinjauan kinerja terhadap organisasi maupun manajer secara individu akan dilakukan sedikitnya setahun sekali dan kemudian melakukan revisi terhadap proses, serta pengaturan sasaran kinerja yang diperbaharui untuk periode selanjutnya.

Penilaian kinerja manajemen risiko tersebut merupakan bagian terpadu dari sistem penilaian kinerja keseluruhan organisasi serta sistem pengukuran bagi masing-masing departemen dan individu.

### A.3.2 Akuntabilitas penuh atas risiko

Manajemen risiko yang dikuatkan mencakupi tugas perlakuan pengendalian risiko dan tugas perlakuan risiko terhadap akuntabilitas atas risiko yang komprehensif, didefinisikan secara utuh dan diterima sepenuhnya. Individu yang ditunjuk menerima akuntabilitas sepenuhnya, yang ketrampilannya layak, serta memiliki sumber daya yang cukup untuk memeriksa pengendalian, memantau risiko, meningkatkan pengendalian serta komunikasi secara efektif tentang risiko dan pengelolaannya pada pemangku kepentingan eksternal dan internal.

Hal ini dapat diindikasikan oleh seluruh anggota organisasi yang sepenuhnya menyadari risiko, pengendalian serta tugas tersebut di mana mereka akuntabel. Pada umumnya, hal ini akan terekam dalam deskripsi pekerjaan/posisi, basis data atau sistem informasi. Definisi

dari peran, akuntabilitas dan tanggung jawab manajemen risiko sebaiknya menjadi bagian dari keseluruhan program induksi organisasi.

Organisasi memastikan bahwa individu yang akuntabel telah dibekali untuk memenuhi perannya dengan memberikan kepada mereka secara cukup dengan kewenangan, waktu, pelatihan, sumber daya, dan ketrampilan untuk melaksanakan akuntabilitas mereka.

### A.3.3 Aplikasi manajemen risiko dalam setiap pengambilan keputusan

Setiap pengambilan keputusan dalam organisasi, apapun tingkat kepentingan dan signifikansinya, melibatkan pertimbangan eksplisit atas risiko serta aplikasi manajemen risiko pada tingkatan tertentu yang sesuai.

Hal ini dapat ditunjukkan dengan rekaman pertemuan dan rekaman keputusan untuk menunjukkan bahwa diskusi eksplisit mengenai risiko telah dilakukan. Selain itu, rekaman tersebut sebaiknya memungkinkan untuk melihat bahwa semua komponen manajemen risiko yang telah terwakili dalam proses kunci untuk pengambilan keputusan dalam organisasi tersebut, misalnya dalam pengambilan keputusan tentang alokasi modal, mengenai proyek-proyek besar dan mengenai restrukturisasi serta perubahan organisasi. Untuk alasan ini, manajemen risiko yang telah terkomunikasikan dilihat dalam organisasi sebagai penyedia dasar bagi tata kelola yang efektif.

### A.3.4 Komunikasi berkesinambungan

Manajemen risiko yang diperkuat memiliki komunikasi berkesinambungan dengan para pemangku kepentingan eksternal dan internal, termasuk pelaporan yang komprehensif dan rutin mengenai kinerja manajemen risiko, sebagai bagian dari tata kelola yang baik.

Hal ini dapat diindikasikan melalui komunikasi dengan para pemangku kepentingan sebagai komponen terpadu dan komponen yang esensial dari manajemen risiko. Komunikasi dipandang secara tepat sebagai suatu proses dua arah, sedemikian rupa sehingga keputusan tentang tingkat suatu risiko dan kebutuhan dari perlakuan risiko dapat dibuat berdasarkan informasi cukup memadai terhadap kriteria risiko komprehensif dan telah ditetapkan sebelumnya secara memadai.

Pelaporan eksternal dan internal yang komprehensif dan rutin baik mengenai risiko signifikan dan mengenai kinerja manajemen risiko berkontribusi secara substansial pada tata kelola yang efektif dalam organisasi tersebut.

### A.3.5 Integrasi penuh dalam struktur tata kelola suatu organisasi

Manajemen risiko dipandang sebagai pusat dari proses manajemen suatu organisasi, sedemikian rupa sehingga risiko dipertimbangkan dalam konteks efek mengenai ketidakpastian dari sasaran. Struktur dan proses tata kelola didasarkan pada pengelolaan dari risiko. Manajemen risiko yang efektif dipandang oleh para manajer sebagai hal esensial dalam pencapaian suatu sasaran organisasi.

Hal ini diindikasikan melalui bahasa para manajer dan materi tertulis yang penting dalam suatu organisasi melalui penggunaan istilah "ketidakpastian" yang terkait dengan risiko. Atribut ini juga tercermin secara normal dalam pernyataan kebijakan dari organisasi, terutama yang berhubungan dengan manajemen risiko. Pada umumnya, atribut ini akan diverifikasi melalui wawancara dengan para manajer dan melalui bukti tindakan dan bukti pernyataan mereka.

# Risk management — Principles and guidelines

## (ISO 31000:2009)

## Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”.

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of “establishing the context” as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

- increase the likelihood of achieving objectives;
- encourage proactive management;
- be aware of the need to identify and treat risk throughout the organization;
- improve the identification of opportunities and threats;
- comply with relevant legal and regulatory requirements and international norms;

- improve mandatory and voluntary reporting;
- improve governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improve controls;
- effectively allocate and use resources for risk treatment;
- improve operational effectiveness and efficiency;
- enhance health and safety performance, as well as environmental protection;
- improve loss prevention and incident management;
- minimize losses;
- improve organizational learning; and
- improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

a) those responsible for developing risk management policy within their organization;

b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;

c) those who need to evaluate an organization's effectiveness in managing risk; and

d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

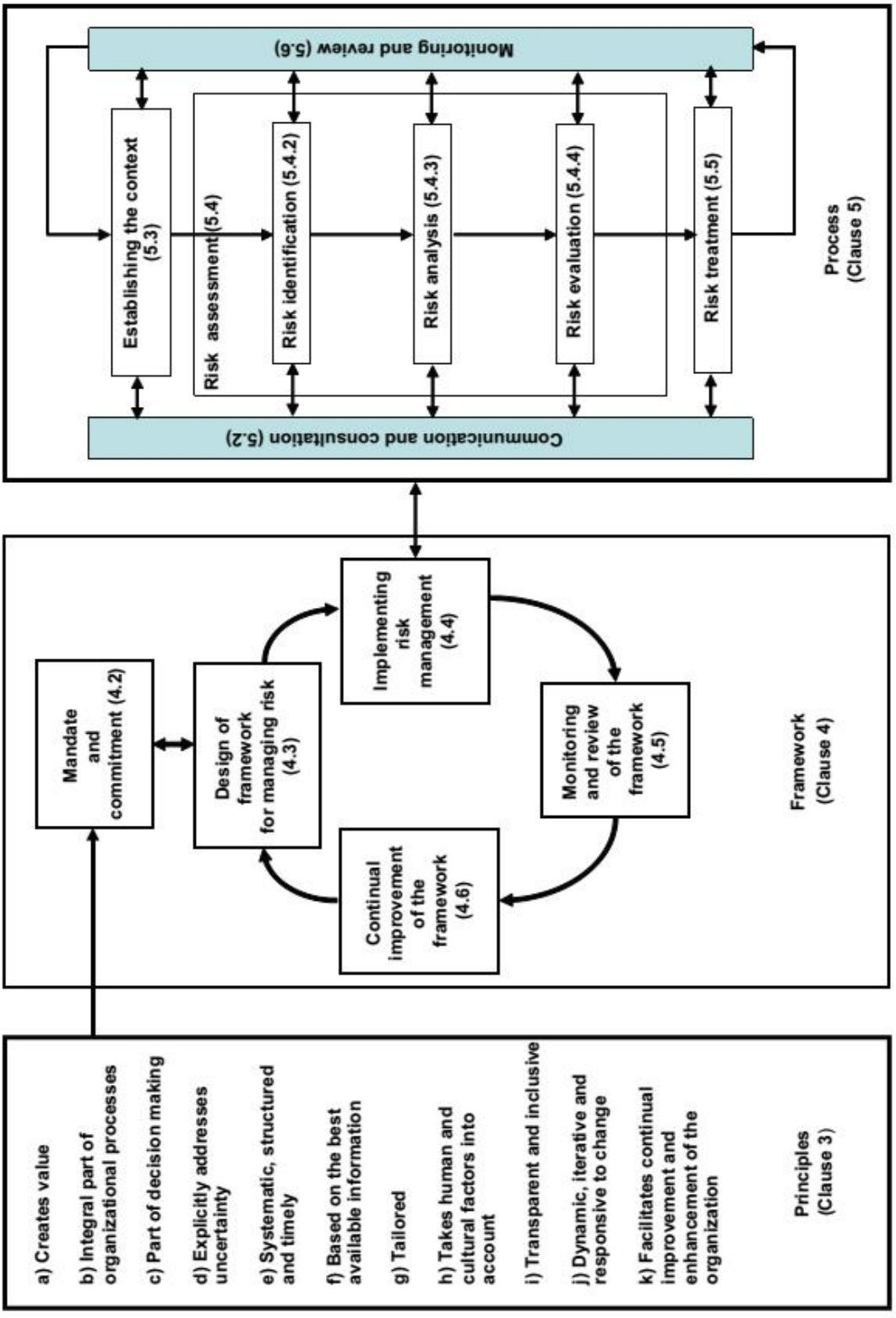



**Figure 1 — Relationships between the risk management principles, framework and process**

# Risk management — Principles and guidelines

## 1 Scope

This International Standard provides principles and generic guidelines on risk management.
This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

**NOTE** For convenience, all the different users of this International Standard are referred to by the general term “organization”.

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

## 2 Terms and definitions

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

**2.1**
**risk**
effect of uncertainty on objectives

**NOTE 1** An effect is a deviation from the expected — positive and/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).

**NOTE 3** Risk is often characterized by reference to potential **events** (2.17) and **consequences** (2.18), 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** (2.19) of occurrence.

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

[ISO Guide 73:2009, definition 1.1]

**2.2**
**risk management**
coordinated activities to direct and control an organization with regard to **risk** (2.1)
[ISO Guide 73:2009, definition 2.1]

**2.3**
**risk management framework**
set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring** (2.28), reviewing and continually improving **risk management** (2.2) throughout the organization

**NOTE 1** The foundations include the policy, objectives, mandate and commitment to manage **risk** (2.1).

**NOTE 2** The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

**NOTE 3** The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

[ISO Guide 73:2009, definition 2.1.1]

**2.4**
**risk management policy**
statement of the overall intentions and direction of an organization related to **risk management** (2.2)

[ISO Guide 73:2009, definition 2.1.2]

**2.5**
**risk attitude**
organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (2.1)

[ISO Guide 73:2009, definition 3.7.1.1]

**2.6**
**risk management plan**
scheme within the **risk management framework** (2.3) specifying the approach, the management components and resources to be applied to the management of **risk** (2.1)

**NOTE 1** Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

**NOTE 2** The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

[ISO Guide 73:2009, definition 2.1.3]

**2.7**
**risk owner**
person or entity with the accountability and authority to manage a **risk** (2.1)

[ISO Guide 73:2009, definition 3.5.1.5]

**2.8**
**risk management process**
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (2.28) and reviewing **risk** (2.1)

[ISO Guide 73:2009, definition 3.1]

**2.9**
**establishing the context**
defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (2.22) for the **risk management policy** (2.4)

[ISO Guide 73:2009, definition 3.3.1]

**2.10**
**external context**
external environment in which the organization seeks to achieve its objectives

**NOTE** External context can include:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

- key drivers and trends having impact on the objectives of the organization; and relationships with, and perceptions and values of external **stakeholders** (2.13).

[ISO Guide 73:2009, definition 3.3.1.1]

**2.11**
**internal context**
internal environment in which the organization seeks to achieve its objectives

**NOTE** Internal context can include:

- governance, organizational structure, roles and accountabilities;

- policies, objectives, and the strategies that are in place to achieve them;

- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

- information systems, information flows and decision-making processes (both formal and informal);

- relationships with, and perceptions and values of, internal stakeholders;

- the organization's culture;

- standards, guidelines and models adopted by the organization; and

- form and extent of contractual relationships.

[ISO Guide 73:2009, definition 3.3.1.2]

**2.12**
**communication and consultation**
continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** (2.13) regarding the management of **risk** (2.1)

**NOTE 1** The information can relate to the existence, nature, form, **likelihood** (2.19), significance, evaluation, acceptability and treatment of the management of risk.

**NOTE 2** Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making.

[ISO Guide 73:2009, definition 3.2.1]

**2.13**
**stakeholder**
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

**NOTE** A decision maker can be a stakeholder.

[ISO Guide 73:2009, definition 3.2.1.1]

**2.14**
**risk assessment**
overall process of **risk identification** (2.15), **risk analysis** (2.21) and **risk evaluation** (2.24)
[ISO Guide 73:2009, definition 3.4.1]

**2.15**
**risk identification**
process of finding, recognizing and describing **risks** (2.1)

**NOTE 1** Risk identification involves the identification of **risk sources** (2.16), **events** (2.17), their causes and their potential **consequences** (2.18).

**NOTE 2** Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s (2.13) needs.

[ISO Guide 73:2009, definition 3.5.1]

**2.16**
**risk source**
element which alone or in combination has the intrinsic potential to give rise to **risk** (2.1)

**NOTE** A risk source can be tangible or intangible.

[ISO Guide 73:2009, definition 3.5.1.2]

**2.17**
**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** (2.18) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

[ISO Guide 73:2009, definition 3.5.1.3]

**2.18**
**consequence**
outcome of an **event** (2.17) affecting objectives

**NOTE 1** An event can lead to a range of consequences.

**NOTE 2** A consequence can be certain or uncertain and can have positive or negative effects on objectives.

**NOTE 3** Consequences can be expressed qualitatively or quantitatively.

**NOTE 4** Initial consequences can escalate through knock-on effects.

[ISO Guide 73:2009, definition 3.6.1.3]

**2.19**
**likelihood**
chance of something happening

**NOTE 1** In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

**NOTE 2** The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[ISO Guide 73:2009, definition 3.6.1.1]

**2.20**
**risk profile**
description of any set of **risks** (2.1)

**NOTE** The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[ISO Guide 73:2009, definition 3.8.2.5]

**2.21**
**risk analysis**
process to comprehend the nature of **risk** (2.1) and to determine the **level of risk** (2.23)

[ISO Guide 73:2009, definisi 3.8.1]

**NOTE 1** Risk analysis provides the basis for **risk evaluation** (2.24) and decisions about **risk treatment** (2.25).

**NOTE 2** Risk analysis includes risk estimation.

[ISO Guide 73:2009, definition 3.6.1]

**2.22**
**risk criteria**
terms of reference against which the significance of a **risk** (2.1) is evaluated

**NOTE 1** Risk criteria are based on organizational objectives, and **external** (2.10) and **internal context** (2.11).

**NOTE 2** Risk criteria can be derived from standards, laws, policies and other requirements.

[ISO Guide 73:2009, definition 3.3.1.3]

**2.23**
**level of risk**
magnitude of a **risk** (2.1) or combination of risks, expressed in terms of the combination of **consequences** (2.18) and their **likelihood** (2.19)

[ISO Guide 73:2009, definition 3.6.1.8]

**2.24**
**risk evaluation**
process of comparing the results of **risk analysis** (2.21) with **risk criteria** (2.22) to determine whether the **risk** (2.1) and/or its magnitude is acceptable or tolerable

**NOTE** Risk evaluation assists in the decision about **risk treatment** (2.25).

[ISO Guide 73:2009, definition 3.7.1]

**2.25**
**risk treatment**
process to modify **risk** (2.1)

**NOTE 1** Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the **risk source** (2.16);
- changing the **likelihood** (2.19);
- changing the **consequences** (2.18);

- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

**NOTE 2** Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

**NOTE 3** Risk treatment can create new risks or modify existing risks.

[ISO Guide 73:2009, definition 3.8.1]

**2.26**
**control**
measure that is modifying **risk** (2.1)

**NOTE 1** Controls include any process, policy, device, practice, or other actions which modify risk.

**NOTE 2** Controls may not always exert the intended or assumed modifying effect.

[ISO Guide 73:2009, definition 3.8.1.1]

**2.27**
**residual risk**
**risk** (2.1) remaining after **risk treatment** (2.25)

**NOTE 1** Residual risk can contain unidentified risk.

**NOTE 2** Residual risk can also be known as “retained risk”.

[ISO Guide 73:2009, definition 3.8.1.6]

**2.28**
**monitoring**
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

**NOTE** Monitoring can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.1]

**2.29**
**review**
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

**NOTE** Review can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.2]

## 3 Principles

For risk management to be effective, an organization should at all levels comply with the principles below.

a) **Risk management creates and protects value**.

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) **Risk management is an integral part of all organizational processes**.

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

c) **Risk management is part of decision making**.

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d) **Risk management explicitly addresses uncertainty**.

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) **Risk management is systematic, structured and timely**.

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) **Risk management is based on the best available information**.

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) **Risk management is tailored**.

Risk management is aligned with the organization's external and internal context and risk profile.

h) **Risk management takes human and cultural factors into account**.

Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

i) **Risk management is transparent and inclusive**.

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) **Risk management is dynamic, iterative and responsive to change**.

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) **Risk management facilitates continual improvement of the organization**.

Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

Annex A provides further advice for organizations wishing to manage risk more effectively.

## 4 Framework

### 4.1 General

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Figure 2.

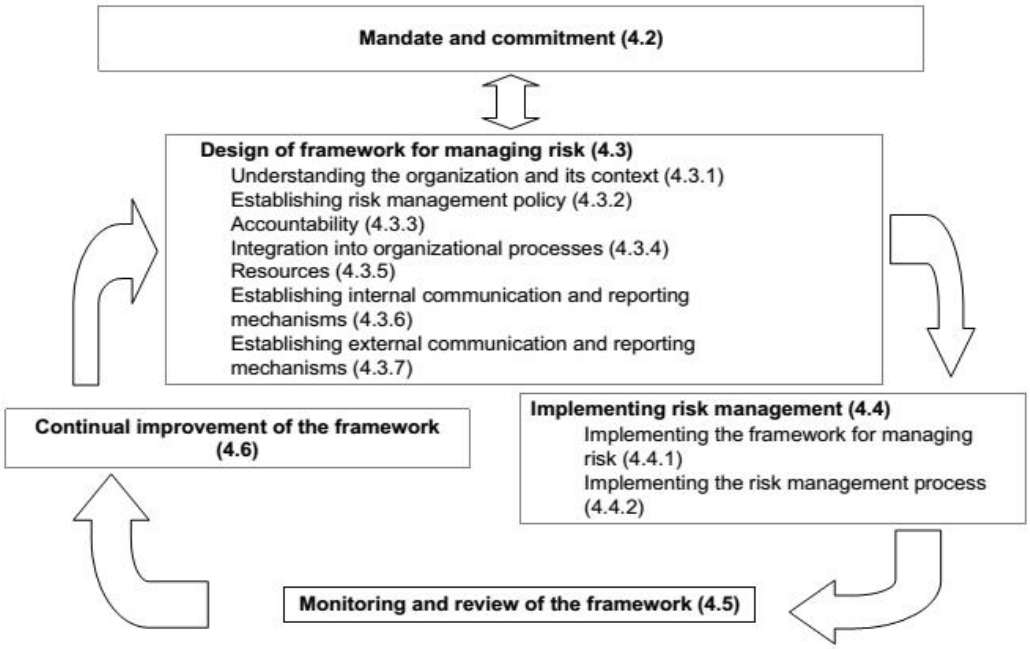



**Figure 2 — Relationship between the components of the framework for managing risk**

This framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against this International Standard, including the attributes contained in Annex A, in order to determine their adequacy and effectiveness.

### 4.2 Mandate and commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels. Management should:

- define and endorse the risk management policy;
- ensure that the organization's culture and risk management policy are aligned;
- determine risk management performance indicators that align with performance indicators of the organization;
- align risk management objectives with the objectives and strategies of the organization;
- ensure legal and regulatory compliance;
- assign accountabilities and responsibilities at appropriate levels within the organization;

- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders; and
- ensure that the framework for managing risk continues to remain appropriate.

### 4.3 Design of framework for managing risk

#### 4.3.1 Understanding of the organization and its context

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organization, since these can significantly influence the design of the framework.

Evaluating the organization's external context may include, but is not limited to:

a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

b) key drivers and trends having impact on the objectives of the organization; and

c) relationships with, and perceptions and values of, external stakeholders.

Evaluating the organization's internal context may include, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organization's culture;
- standards, guidelines and models adopted by the organization; and
- the form and extent of contractual relationships.

#### 4.3.2 Establishing risk management policy

The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:

- the organization's rationale for managing risk;
- links between the organization's objectives and policies and the risk management policy;
- accountabilities and responsibilities for managing risk;
- the way in which conflicting interests are dealt with;
- commitment to make the necessary resources available to assist those accountable and responsible for managing risk;

- the way in which risk management performance will be measured and reported; and
- commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

### 4.3.3 Accountability

The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

- identifying risk owners that have the accountability and authority to manage risks;
- identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
- identifying other responsibilities of people at all levels in the organization for the risk management process;
- establishing performance measurement and external and/or internal reporting and escalation processes; and
- ensuring appropriate levels of recognition.

### 4.3.4 Integration into organizational processes

Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

### 4.3.5 Resources

The organization should allocate appropriate resources for risk management.
Consideration should be given to the following:

- people, skills, experience and competence;
- resources needed for each step of the risk management process;
- the organization's processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programmes.

### 4.3.6 Establishing internal communication and reporting mechanisms

The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:

- key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
- there is adequate internal reporting on the framework, its effectiveness and the outcomes;
- relevant information derived from the application of risk management is available at appropriate levels and times; and
- there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

### 4.3.7 Establishing external communication and reporting mechanisms

The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;
- using communication to build confidence in the organization; and
- communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

## 4.4 Implementing risk management

### 4.4.1 Implementing the framework for managing risk

In implementing the organization's framework for managing risk, the organization should:

- define the appropriate timing and strategy for implementing the framework;
- apply the risk management policy and process to the organizational processes;
- comply with legal and regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;
- hold information and training sessions; and

- communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

### 4.4.2 Implementing the risk management process

Risk management should be implemented by ensuring that the risk management process outlined in Clause 5 is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

### 4.5 Monitoring and review of the framework

In order to ensure that risk management is effective and continues to support organizational performance, the organization should:

- measure risk management performance against indicators, which are periodically reviewed for appropriateness;
- periodically measure progress against, and deviation from, the risk management plan;
- periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;
- report on risk, progress with the risk management plan and how well the risk management policy is being followed; and
- review the effectiveness of the risk management framework.

### 4.6 Continual improvement of the framework

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.

## 5 Process

### 5.1 General

The risk management process should be

- an integral part of management,
- embedded in the culture and practices, and
- tailored to the business processes of the organization.

It comprises the activities described in 5.2 to 5.6. The risk management process is shown in Figure 3.

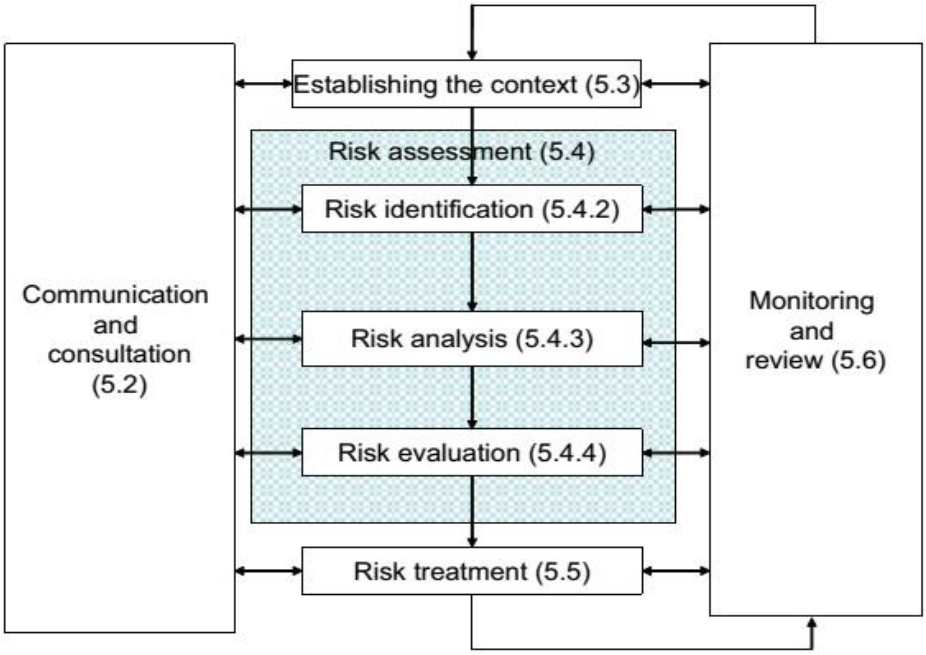



**Figure 3 — Risk management process**

## 5.2 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

- help establish the context appropriately;
- ensure that the interests of stakeholders are understood and considered;
- help ensure that risks are adequately identified;
- bring different areas of expertise together for analyzing risks;
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;
- secure endorsement and support for a treatment plan;

- enhance appropriate change management during the risk management process; and
- develop an appropriate external and internal communication and consultation plan.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision making process.

Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

### 5.3 Establishing the context

#### 5.3.1 General

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

#### 5.3.2 Establishing the external context

The external context is the external environment in which the organization seeks to achieve its objectives.

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, perceptions and values of external stakeholders.

#### 5.3.3 Establishing the internal context

The internal context is the internal environment in which the organization seeks to achieve its objectives.

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It should be established because:

a) risk management takes place in the context of the objectives of the organization;

b) objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole; and

c) some organizations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects ongoing organizational commitment, credibility, trust and value.

It is necessary to understand the internal context. This can include, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of internal stakeholders;
- the organization's culture;
- information systems, information flows and decision making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.

### 5.3.4 Establishing the context of the risk management process

The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

The context of the risk management process will vary according to the needs of an organization. It can involve, but is not limited to:

- defining the goals and objectives of the risk management activities;
- defining responsibilities for and within the risk management process;
- defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;
- defining the activity, process, function, project, product, service or asset in terms of time and location;
- defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;
- defining the risk assessment methodologies;
- defining the way performance and effectiveness is evaluated in the management of risk;

- identifying and specifying the decisions that have to be made; and
- identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the organization and to the risks affecting the achievement of its objectives.

### 5.3.5 Defining risk criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- how likelihood will be defined;
- the timeframe(s) of the likelihood and/or consequence(s);
- how the level of risk is to be determined;
- the views of stakeholders;
- the level at which risk becomes acceptable or tolerable; and
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

## 5.4 Risk assessment

### 5.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

**NOTE** ISO/IEC 31010 provides guidance on risk assessment techniq.

### 5.4.2 Risk identification

The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including

cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

### 5.4.3 Risk analysis

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.

The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling should be stated and can be highlighted.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

### 5.4.4 Risk evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls. This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.

### 5.5 Risk treatment

#### 5.5.1 General

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- assessing a risk treatment;
- deciding whether residual risk levels are tolerable;
- if not tolerable, generating a new risk treatment; and
- assessing the effectiveness of that treatment.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

b) taking or increasing the risk in order to pursue an opportunity;

c) removing the risk source;

d) changing the likelihood;

e) changing the consequences;

f) sharing the risk with another party or parties (including contracts and risk financing); and

g) retaining the risk by informed decision.

#### 5.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks.

A number of treatment options can be considered and applied either individually or in combination. The organization can normally benefit from the adoption of a combination of treatment options.

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.

### 5.5.3 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements; and
- timing and schedule.

Treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

## 5.6 Monitoring and review

Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or *ad hoc*.

Responsibilities for monitoring and review should be clearly defined.

The organization's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

- ensuring that controls are effective and efficient in both design and operation;
- obtaining further information to improve risk assessment;
- analyzing and learning lessons from events (including near-misses), changes, trends, successes and failures;
- detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and
- identifying emerging risks.

Progress in implementing risk treatment plans provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement and external and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework (see 4.5).

### 5.7 Recording the risk management process

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Decisions concerning the creation of records should take into account:

- the organization's needs for continuous learning;
- benefits of re-using information for management purposes;
- costs and efforts involved in creating and maintaining records;
- legal, regulatory and operational needs for records;
- method of access, ease of retrievability and storage media;
- retention period; and
- sensitivity of information.

# Annex A
(informative)
**Attributes of enhanced risk management**

## A.1 General

All organizations should aim at the appropriate level of performance of their risk management framework in line with the criticality of the decisions that are to be made. The list of attributes below represents a high level of performance in managing risk. To assist organizations in measuring their own performance against these criteria, some tangible indicators are given for each attribute.

## A.2 Key outcomes

**A.2.1** The organization has a current, correct and comprehensive understanding of its risks.

**A.2.2** The organization's risks are within its risk criteria.

## A.3 Attributes

### A.3.1 Continual improvement

An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.
This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

### A.3.2 Full accountability for risks

Enhanced risk management includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders.

This can be indicated by all members of an organization being fully aware of the risks, controls and tasks for which they are accountable. Normally, this will be recorded in job/position descriptions, databases or information systems. The definition of risk management roles, accountabilities and responsibilities should be part of all the organization's induction programmes.

### A.3.3 Application of risk management in all decision making

All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.

This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, it should be possible to see that all components of risk management are represented within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes. For these reasons, soundly based risk management is seen within the organization as providing the basis for effective governance.

### A.3.4 Continual communications

Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

This can be indicated by communication with stakeholders as an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.
Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.

### A.3.5 Full integration in the organization's governance structure

Risk management is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives.

This is indicated by managers' language and important written materials in the organization using the term “uncertainty” in connection with risks. This attribute is also normally reflected in the organization's statements of policy, particularly those relating to risk management. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.

## Bibliografi

[1] ISO Guide 73:2009, *Risk management — Vocabulary*

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

## Informasi pendukung terkait perumus standar

**[1] Komtek/SubKomtek perumus SNI**

Komite Teknis 03-10 *Manajemen risiko*

**[2] Susunan keanggotaan Komtek perumus SNI**

Ketua : Antonius Alijoyo

Sekretaris : Hendro Kusumo

Anggota :

1. D.S Priyarsono
2. Hidayat Prabowo
3. Mohammad Mukhlis
4. Roy Ulrich
5. Arif Budiman
6. Nursepdal Verliandry
7. Miryam L. Wijaya
8. Bernado A. Mochtar
9. Ridwan Hendra
10. Charles Reinier Vorst
11. Johan Candra

**[3] Konseptor rancangan SNI**

Gugus kerja Komite Teknis 03-10 *Manajemen risiko*

**[4] Sekretariat pengelola Komtek perumus SNI**

Pusat Perumusan Standar

Kedeputian bidang Penelitian dan Kerjasama Standardisasi

Badan Standardisasi Nasional