# ISO 31000:2018 Risk management- Guidelines

# مدیریت ریسک- رهنمودها

# فهرست

## مقدمه

این استاندارد برای استفاده کسانی تهیه شده است که با مدیریت ریسک ها، تصمیم‌گیری‌ها، تعیین و تحقق اهداف و بهبود عملکرد در سازمان‌ها ارزش ایجاد کرده و از آن ارزش محافظت می‌کنند.

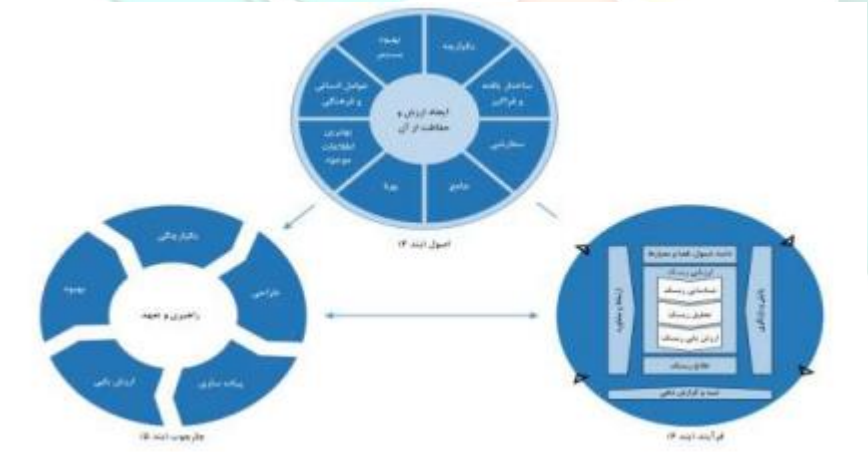
سازمان‌هایی در هر نوع و اندازه، با عوامل و تاثیرات خارجی و داخلی مواجه هستند که احتمال دستیابی آن ها به اهداف خود را نامعلوم می‌سازد.

مدیریت ریسک، فرآیندی تکراری است که در تنظیم راهبرد، دستیابی به اهداف و تصمیم‌گیری آگاهانه، به سازمان‌ها کمک می‌کند.

مدیریت ریسک، قسمتی از حکمرانی[1] و راهبری است و در چگونگی مدیریت یک سازمان در تمامی سطوح، نقشی اساسی داشته و به بهبود سیستم‌های مدیریت کمک می‌کند.

مدیریت ریسک، قسمتی از همه فعالیت های مرتبط با یک سازمان بوده و شامل تعامل با ذی نفعان است. مدیریت ریسک، فضای خارجی و داخلی سازمان، شامل رفتارهای انسانی و عوامل فرهنگی را در نظر می‌گیرد.

مدیریت ریسک، بر اصول، چارچوب و فرآیند ترسیم‌شده در این استاندارد، همان‌طور که در شکل ۱ نشان داده شده است، استوار است. ممکن است این مؤلفه‌ها به صورت کامل یا جزئی در یک سازمان وجود داشته باشد، ولی به منظور مدیریت ریسک کارآمد، مؤثر و پایدار، ممکن است تطبیق یا بهبود آن ها لازم باشد.



شکل ۱ – اصول، چارچوب و فرآیند

۱- Governance

مدیریت ریسک – رهنمودها

## ۱- هدف و دامنه کاربرد

هدف از تدوین این استاندارد، ارائه رهنمودهایی در رابطه با مدیریت ریسکی است که سازمان‌ها با آن مواجـه هستند. این رهنمودها را می‌توان متناسب با هر سازمان و فضای آن، سفارشی‌سازی کرده و به‌کار برد.

این استاندارد، رویکردی مشترک را برای مدیریت هر نوع ریسک بیان کرده و مختص صنعت یا بخش خاصی نیست. این استاندارد، در تمام طول عمر یک سازمان کاربرد داشته و قابلیت آن را دارد تا برای هر فعالیتی از جملـه تصمیم سازی در همه سطوح به‌کار رود.

## ۲-مراجع الزامی

این استاندارد مراجع الزامی ندارد.

## ۳-اصطلاحات و تعاریف [۱]

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

### ۳-۱ ریسک (risk)

تأثیر عدم قطعیت بر اهداف است.

یادآوری -۱ یک تأثیر، انحراف از انتظارات سازمان بوده و می‌تواند مثبت، منفی یا هر دو باشد و می‌تواند به فرصت ها و تهدید ها

پرداخته، آن ها را ایجاد کرده یا منجر شود.

یادآوری -۲ اهداف می‌توانند جنبه‌ها و طبقه بندی های مختلفی داشته و در سطوح مختلفی به‌کار روند.

یادآوری -۳ معمولا ریسک به صورت منابع ریسک (به زیربند ۳-۴ مراجعه شود)، رویدادهای بالقوه (بـه زیربنـد ۳-۵ مراجعـه شـود) ، پیامدها (به زیربند ۳-۶ مراجعه شود) و احتمال (به زیربند ۳-۷ مراجعه شود) آن ها تعریف می‌شود.

### ۳-۲ مدیریت ریسک (risk management)

فعالیت های هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به ریسک (به زیربند ۳-۱ مراجعه شود) است.

---

[۱] اصـطلاحات و تعـاریف بـه‌کـار رفتـه در اسـتانداردهای ISO و IEC در وبگـاه‌هـای www.iso.org/obp و www.electropedia.org/ قابل‌دسترس است.

### ۳-۳ ذی نفع (stakeholder)

شخص یا سازمانی که می‌تواند تأثیر گذاشته، تأثیر پذیرفته، یا خود را در معرض آثار یک تصمیم یـا فعالیـت قرار دهد.

یادآوری- اصطلاح «شخص علاقه‌مند[۱]» را می‌توان به‌عنوان جایگزینی برای «ذی نفع» به‌کار برد.

### ۳-۴ منبع ریسک (risk source)

عنصری که به تنهایی یا به صورت ترکیبی، قابلیت افزایش ریسک (به زیربند ۳-۱ مراجعه شود) را دارد.

### ۳-۵ رویداد (event)

وقوع یا تغییر مجموعه خاصی از وقایع است.

یادآوری -۱ یک رویداد می‌تواند یک یا چند بار به وقوع بپیوندد و می‌تواند دلایل و پیامدهـای (بـه زیربنـد ۳-۶ مراجعـه شـود) مختلفی داشته باشد.

یادآوری -۲ همچنین یک رویداد می‌تواند موردی باشد که انتظار آن می‌رود ولی اتفاق نمی‌افتد یـا مـوردی باشـد کـه انتظـار نمی‌رود ولی اتفاق می‌افتد.

یادآوری -۳ رویداد می‌تواند منبع ریسک باشد.

### ۳-۶ پیامد (consequence)

برونداد یک رویداد (به زیربند ۳-۵ مراجعه شود) که بر اهداف تأثیر می‌گذارد.

یادآوری - ۱ یک پیامد می‌تواند قطعی یا غیرقطعی بوده و به صورت مستقیم یا غیر مستقیم بـر اهـداف، تـأثیر مثبـت یـا منفـی بگذارد.

یادآوری - ۲ پیامدها را می‌توان به صورت کیفی یا کمی بیان کرد.

یادآوری -۳ هر پیامدی می‌تواند از طریق تأثیرات آبشاری[۲] و انباشته[۳] تشدید شود.

### ۳-۷ احتمال (likelihood)

شانس اتفاق افتادن یک مورد است.

---

[۱] Interested party

[۲] Cascading

[۳] Cumulative

یادآوری -۱ در اصطلاح‌شناسی مدیریت ریسک (به زیربند ۳-۲ مراجعه شود)، واژه «احتمال» برای اشاره به شانس اتفاق افتادن موردی به‌کار می‌رود، خواه به طور عینی یا ذهنی، کیفی یا کمی، تعریف، اندازه‌گیری یا تعیین شده و با استفاده از اصطلاحات عمومی و ریاضی (مانند احتمال[۱] یا فراوانی در سراسر دوره زمانی معین) توصیف شده باشد.

یادآوری - ۲ اصطلاح انگلیسی«likelihood»، در برخی زبان‌ها معادل مستقیم ندارد؛ در عوض، اغلب معادل اصطلاح «probability» استفاده می‌شود. با این حال، در زبان انگلیسی«probability» اغلب سرسختانه به‌عنوان یک اصطلاح ریاضی تعبیر می‌شود. بنابراین، در اصطلاح شناسی مدیریت ریسک،«likelihood» با این منظور به‌کار می‌رود که توصیه می‌شود همان تعبیر گسترده مانند اصطلاح «probability» را داشته باشد که در بسیاری از زبان‌ها، غیر از زبان انگلیسی دارد.

### ۳-۸ کنترل (control)

سنجه‌ای که ریسک (به زیربند ۳-۱ مراجعه شود) را حفظ[۲] و یا تعدیل می‌کند.

یادآوری -۱ کنترل‌ها شامل هر فرآیند، خط مشی، وسیله، رویه یا سایر شرایط و/یا اقداماتی هستند که ریسک را حفظ و یا تعدیل می‌کند ولی محدود به آن ها نیست.

یادآوری -۲ کنترل ها ممکن است همیشه اثر تعدیلی مورد انتظار یا مفروض را اعمال نکنند.

## ۴- اصول

مقصود از مدیریت ریسک، ایجاد ارزش و حفاظت از آن است. مدیریت ریسک، عملکرد را بهبود بخشیده، نوآوری را تقویت کرده و از دستیابی به اهداف پشتیبانی می‌کند.

اصول مطرح شده در شکل ۲، راهنمایی را در مورد مشخصه های یک مدیریت ریسک کارآمد و مؤثر ارائه می‌کند که با ارزش آن ارتباط برقرار کرده و منظور و هدف آن را توضیح می‌دهد. این اصول، اساس مدیریت ریسک بوده و توصیه می‌شود در زمان تدوین چارچوب و فرآیند های مدیریت ریسک سازمان، در نظر گرفته شوند. توصیه می‌شود این اصول، سازمان را قادر سازد تا تاثیرات عدم قطعیت بر اهداف سازمان را مدیریت کند.

[۱] Probability

[۲] Maintain


شکل -۲ اصول

مدیریت ریسک کارآمد، به عناصری که در شکل ۲ نشان داده شده نیاز دارد. این عناصر را می‌توان به صورت زیر، بیشتر توضیح داد:

الف- یکپارچه

مدیریت ریسک، بخشی جدایی‌ناپذیر از همه فعالیت های سازمانی است.

ب- ساختار یافته و فراگیر

رویکردی ساختار یافته و فراگیر برای مدیریت ریسک، که به نتایج پایدار و قابل مقایسه کمک می‌کند.

پ- سفارشی

چارچوب و فرآیند مدیریت ریسک، با فضای خارجی و داخلی مرتبط با اهداف سازمان، تنظیم و متناسب می‌شود.

ت- جامع

مشارکت مناسب و به موقع ذی نفعان باعث می‌شود که دانش، دیدگاه‌ها و یافته‌های آن ها در نظر گرفته شده و در نتیجه منجر به بهبود آگاهی و مدیریت ریسک آگاهانه می‌شود.

ث- پویا

با تغییر فضای خارجی و داخلی یک سازمان، ریسک ها ممکن است آشکار شده، تغییر یافته یا محو شوند. مدیریت ریسک، این تغییرات و رویدادها را پیش‌بینی، شناسایی و تایید کرده و به شیوه‌ای مناسب و به موقع پاسخ می‌دهد.

ج- بهترین اطلاعات موجود

ورودی‌های مدیریت ریسک، بر مبنای اطلاعات قدیمی و جاری و همچنین انتظارات سازمان از آینده است. مدیریت ریسک، همه محدودیت‌ها و عدم قطعیت‌های مرتبط با این اطلاعات و انتظارات را به وضوح در نظر می‌گیرد. توصیه می‌شود اطلاعات، به موقع و واضح ارائه شده و در دسترس ذی نفعان مرتبط قرارگیرد.

چ- عوامل انسانی و فرهنگی

فرهنگ و رفتار انسانی، به نحو قابل توجهی بر همه جنبه‌های مدیریت ریسک، در هر سطح و مرحله تأثیر می گذارد.

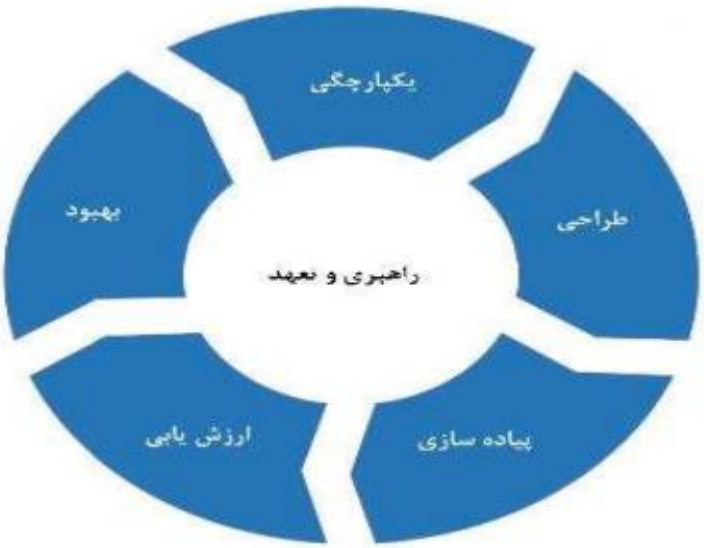
ح- بهبود مستمر

مدیریت ریسک، از طریق یادگیری و تجربه، به طور مستمر بهبود می‌یابد.

# ۵ چارچوب

## ۵-۱ کلیات

مقصود از چارچوب مدیریت ریسک، کمک به سازمان برای یکپارچه سازی مدیریت ریسک در فعالیت ها و کارکردهای مهم است. اثربخشی مدیریت ریسک، به یکپارچگی آن در حکمرانی سازمان، شامل تصمیم سازی، بستگی دارد. تحقق این امر، به پشتیبانی ذی نفعان، به‌خصوص مدیریت ارشد سازمان نیاز دارد. توسعه چارچوب، شامل یکپارچه سازی، طراحی، پیاده سازی، ارزش یابی و بهبود مدیریت ریسک در سرتاسر سازمان است. شکل۳ ،اجزای یک چارچوب را نشان می‌دهد.




شکل -۳ چارچوب

توصیه می‌شود سازمان، رویه‌ها و فرآیند های مدیریت ریسک موجود خود و همه شکاف‌ها را ارزش یابی کـرده و آن شکاف‌ها را درون چارچوب، شناسایی کند.

توصیه می‌شود اجزای چارچوب و نحوه تعامل آن ها با یکدیگر، متناسب با نیازهای سازمان تنظیم شود.

## ۵-۲ راهبری و تعهد

توصیه می‌شود در صورت امکان، مدیریت ارشد و نهادهای نظارتی اطمینان حاصل کنند که مدیریت ریسـک در همه فعالیت های سازمانی، یکپارچه شده و راهبری و تعهد را با انجام موارد زیر اثبات کند:

- سفارشی سازی و پیاده سازی تمام اجزای چارچوب؛
- صدور یک بیانیه یا خط‌مشی که رویکرد، طرح یا نحوه کار[۱] مدیریت ریسک را تعیین کند؛
- اطمینان از اختصاص منابع لازم به مدیریت ریسک؛
- تفویض و تعیین اختیارات، مسئولیت‌ها و وظایف در سطوح مناسب درون سازمان.

انجام امور فوق به سازمان کمک خواهد کرد تا:

- مدیریت ریسک را با اهداف، راهبرد و فرهنگ خود، هم‌راستا سازد؛
- همه وظایف و همچنین تعهدات داوطلبانه خود را شناسایی کرده و به آن ها بپردازد؛
- میزان و نوع ریسکی را که ممکن است به‌عنوان راهنمایی برای توسعه معیارهای ریسک در نظر گرفته شود را تعیین کرده، و از برقراری ارتباط این موارد با سازمان و ذی نفعان آن، اطمینان حاصل کند؛
- ارزش مدیریت ریسک را به سازمان و ذی نفعان آن منتقل کند؛
- پایش نظام مند ریسک ها را ترویج کند؛
- از تناسب میان چارچوب مدیریت ریسک با فضای سازمان، اطمینان حاصل کند.

مدیریت ارشد سازمان پاسخگوی اجرای مـدیریت ریسـک اسـت، در حـالی کـه نهادهـای نظـارتی سـازمان، پاسخگوی نظارت بر مدیریت ریسک هستند. اغلب، انجام موارد زیر از نهادهای نظارتی انتظار می‌رود یا ملـزم به انجام آن ها هستند:

- در زمان تنظیم اهداف سازمان، از در نظر گرفتن ریسک ها به طور کامل اطمینان حاصل کنند؛
- در پیگیری اهداف، ریسک های پیش روی سازمان را شناسایی کنند؛
- از پیاده سازی و بهره برداری مؤثر سیستم‌ها برای مدیریت این‌گونه ریسک ها اطمینان حاصل کنند؛
- از مناسب بودن این ریسک ها در محدوده اهداف سازمان اطمینان حاصل کنند؛
- از ارتباط صحیح اطلاعات مرتبط با این ریسک ها و مدیریت آن ها، اطمینان حاصل کنند.

[۱] Course of action

## ۵-۳ یکپارچگی

یکپارچه سازی مدیریت ریسک، به شناخت ساختارها و فضای سازمانی بستگی دارد. ساختارها، بسته به مقاصد، اهداف و پیچیدگی سازمان، متفاوت هستند. ریسک، در هر قسمت از ساختار سازمان، مدیریت می شود. همه افراد یک سازمان، در قبال مدیریت ریسک مسئولیت دارند.

حکمرانی؛ هدایت سازمان، روابط خارجی و داخلی آن، قوانین، فرآیندها و رویه‌های لازم برای دستیابی به مقاصد سازمان را بر عهده دارد. ساختارهای مدیریت، جهت‌گیری حکمرانی را به سوی راهبرد و اهداف مرتبط مورد نیاز برای دستیابی به سطوح مطلوب عملکرد پایدار و رشد و ترقی بلند مدت، میسر می‌سازد. تعیین مسئولیت پاسخگویی و نقش‌های نظارتی مرتبط با مدیریت ریسک در یک سازمان، قسمت‌های جدایی‌ناپذیر از حکمرانی آن سازمان محسوب می‌شوند.

یکپارچه سازی مدیریت ریسک در یک سازمان، فرآیندی پویا و تکراری محسوب شده و توصیه می‌شود، متناسب با نیازها و فرهنگ سازمان، سفارشی‌سازی شود. بهتر است مدیریت ریسک، قسمتی از مقاصد، حکمرانی، راهبری و تعهد، راهبرد، اهداف و عملکردهای سازمانی بوده و جدا از آن ها نباشد.

## ۵-۴ طراحی

### ۵-۴-۱ شناسایی سازمان و فضای آن

در زمان طراحی چارچوب مدیریت ریسک، توصیه می‌شود سازمان، فضای خارجی و داخلی خود را مورد بررسی قرار داده و شناسایی کند.

بررسی فضای خارجی سازمان، ممکن است شامل موارد زیر باشد ولی به آن ها محدود نمی‌شود:

- عوامل اجتماعی، فرهنگی، سیاسی، قانونی، نظارتی، مالی، فناورانه، اقتصادی و زیست محیطی، اعم از بین‌المللی، ملی، منطقه‌ای یا محلی؛
- محرک ها و گرایش های کلیدی که بر اهداف سازمان تاثیر می‌گذارند،
- روابط، یافته‌ها، ارزش‌ها، نیازها و انتظارات ذی نفعان خارجی؛
- روابط و تعهدات قراردادی؛
- پیچیدگی شبکه ها و وابستگی ها؛

بررسی فضای داخلی سازمان ممکن است شامل موارد زیر باشد ولی به آن ها محدود نمی‌شود:

- چشم‌انداز، ماموریت و ارزش‌ها؛
- حکمرانی، ساختار سازمانی، نقش‌ها و پاسخگویی‌ها؛
- راهبرد، اهداف و خط‌مشی‌ها؛
- فرهنگ سازمان؛

- استانداردها، رهنمودها و مدل‌های اتخاذ شده توسط سازمان؛
- قابلیت هایی که به عنوان منابع و دانش شناخته می‌شوند (برای مثال، سرمایه، زمان، نیروی انسانی، مالکیت معنوی، فرآیندها، سیستم‌ها و فناوری‌ها)؛
- داده ها، سیستم‌های اطلاعاتی و جریان‌های اطلاعات؛
- روابط با ذی نفعان داخلی، با درنظر گرفتن یافته ها و ارزش‌های آن ها؛
- روابط و تعهدات قراردادی؛
- وابستگی‌های متقابل و ارتباطات داخلی.

## ۵-۴-۲ تشریح تعهد به مدیریت ریسک

توصیه می‌شود مدیریت ارشد و نهادهای نظارتی، در صورت امکان، تعهد مستمر خود به مدیریت ریسک را از طریق یک خط‌مشی، یک بیانیه یا اَشکال دیگری که به روشنی، حکایت از اهداف سازمان و تعهد به مدیریت ریسک دارد، اثبات و تشریح کند. توصیه می‌شود این تعهد، شامل موارد زیر بوده ولی به آن ها محدود نشود:

- مقصود سازمان از مدیریت ریسک و ارتباطات با اهداف و سایر خط مشی های سازمان؛
- تقویت نیاز به یکپارچه سازی مدیریت ریسک در فرهنگ کلی سازمان؛
- هدایت یکپارچه سازی مدیریت ریسک در فعالیت های اصلی کسب و کار و تصمیم سازی؛
- اختیارات، مسئولیت ها و پاسخگویی ها؛
- در دسترس قراردادن منابع لازم؛
- شیوه‌ای که از طریق آن به اهداف متناقض رسیدگی می‌شود؛
- اندازه‌گیری و گزارش دهی در شاخص‌های عملکرد سازمان؛
- بازنگری و بهبود.

توصیه می‌شود تعهد مدیریت ریسک، به صورتی که مناسب است، درون سازمان و به ذی نفعان ابلاغ شود.

## ۵-۴-۳ واگذاری نقش‌ها، اختیارات، مسئولیت‌ها و پاسخگویی‌های سازمانی

توصیه می‌شود مدیریت ارشد و نهادهای نظارتی، هر جا که قابل اجرا است، اطمینان حاصل کنند که اختیارات، مسئولیت‌ها و پاسخگویی‌های نقش‌های مرتبط، با درنظر گرفتن مدیریت ریسک، در همه سطوح سازمان، واگذار و ابلاغ شده و توصیه می‌شود:

- تاکید کند که مدیریت ریسک از مسئولیت های اصلی است؛
- افرادی که پاسخگویی و اختیار برای مدیریت ریسک دارند (مالکان ریسک) را شناسایی کند.

### ۵-۴-۴ تخصیص منابع

توصیه می‌شود مدیریت ارشد و نهادهای نظارتی، هر جا که قابل اجرا باشد، از تخصیص منابع مناسب برای مدیریت ریسک، اطمینان حاصل کنند. این منابع می‌تواند، شامل موارد زیر بوده ولی به آن ها محدود نمی‌شود:

- افراد، مهارت ها، تجربه و شایستگی؛
- فرآیند ها، روش‌ها و ابزارهای سازمان که برای مدیریت ریسک به‌کار می‌روند؛
- فرآیند ها و روش‌های اجرایی مستند؛
- سیستم های مدیریت اطلاعات و دانش؛
- نیازهای توسعه و آموزش حرفه‌ای.

توصیه می‌شود سازمان، قابلیت ها و محدودیت های منابع موجود را در نظر بگیرد.

### ۵-۴-۵ برقراری ارتباط و مشاوره

توصیه می‌شود سازمان، به منظور حمایت از این چارچوب و تسهیل استفاده مؤثر از مدیریت ریسک، رویکردی مصوب در رابطه با ارتباط و مشاوره برقرار سازد. ارتباط، شامل به اشتراک‌گذاشتن اطلاعات با جامعه هدف است. مشاوره نیز شامل شرکت‌کنندگانی است که انتظارات خود را در تصمیم‌گیری ها و شکل آن یا سایر فعالیت‌ها بازخورد می‌دهند. توصیه می‌شود روش‌های ارتباط و مشاوره و محتوا، در جایی که مرتبط است، منعکس‌کننده انتظارات ذی نفعان باشد.

توصیه می‌شود ارتباط و مشاوره، به موقع انجام شود و اطمینان دهد که اطلاعات مرتبط، به طور مناسب، جمع‌آوری، تطبیق[۱]، ترکیب[۲] و به اشتراک گذاشته شده و بازخورد ارائه می‌شود و بهبود ها صورت می‌گیرد.

## ۵-۵ پیاده سازی

توصیه می‌شود سازمان، چارچوب مدیریت ریسک را با استفاده از موارد زیر پیاده سازی کند:

- توسعه طرحی مناسب شامل زمان و منابع؛
- شناسایی این‌که انواع مختلف تصمیم ها در سرتاسر سازمان، کجا، چه وقت و چگونه و توسط چه کسی گرفته می‌شوند؛
- تغییر فرآیند های تصمیم سازی قابل اجرا در مواقع لزوم؛
- اطمینان از این‌که ترتیبات سازمان در خصوص مدیریت ریسک، به طور واضح، شناسایی و اعمال شده است.

---

[۱] Collated

[۲] Synthesised

پیاده سازی موفق چارچوب مدیریت ریسک، نیازمند مشارکت و آگاهی ذی نفعان است. این امر، سازمان‌ها را قادر می‌سازد تا به طور صریح، عدم قطعیت را در تصمیم سازی درنظر گیرند، همچنین اطمینان حاصل کنند که هر عدم قطعیت جدید یا بعدی را، همان‌طورکه هست، می‌توان در نظر گرفت.

چارچوب مدیریت ریسکی که به طور مناسب طراحی و پیاده سازی شده باشد، تضمین خواهد کرد که فرآیند مدیریت ریسک، قسمتی از همه فعالیت های سرتاسر سازمان، شامل تصمیم سازی و تغییراتی در فضاهای خارجی و داخلی است که به قدر کفایت، گرفته خواهد شد.

## ۵-۶ ارزش یابی

به منظور ارزش یابی اثر بخشی چارچوب مدیریت ریسک، توصیه می‌شود سازمان:

- به صورت دوره‌ای، عملکرد چارچوب مدیریت ریسک را در برابر مقصود، طرح های اجرایی، شاخص‌ها و رفتار مورد انتظار خود، اندازه‌گیری کند؛
- تعیین کند که آیا چارچوب مدیریت ریسک برای پشتیبانی از سازمان در دستیابی به این اهداف مناسب است یا خیر.

## ۵-۷ بهبود

### ۵-۷-۱ تطبیق دادن

توصیه می‌شود سازمان، به طور مستمر چارچوب مدیریت ریسک را پایش کرده و آن را با تغییرات خارجی و داخلی تطبیق دهد. با انجام این کار، سازمان می‌تواند ارزش خود را بهبود دهد.

### ۵-۷-۲ بهبود مستمر

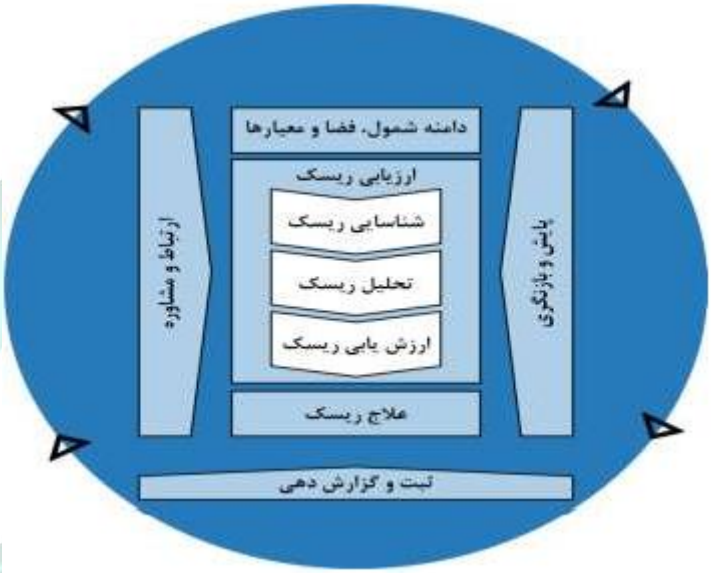
توصیه می‌شود سازمان، به طور مستمر، شایستگی، کفایت و اثربخشی چارچوب مدیریت ریسک و نحوه یکپارچه سازی فرآیند مدیریت ریسک را بهبود بخشد.

با شناسایی شکاف ها یا فرصت های بهبود مرتبط، توصیه می‌شود سازمان، طرح ها و وظایف را توسعه داده و آن ها را به افرادی که در پیاده سازی، پاسخگو هستند واگذار کند. توصیه می‌شود این بهبود ها، به محض اجرا، به پیشرفت مدیریت ریسک کمک کند.

# ۶-فرآیند

## ۶-۱ کلیات

فرآیند مدیریت ریسک، شامل به کارگیری منظم خط مشی‌ها، روش‌های اجرایی و اقداماتی برای فعالیت های ارتباط و مشاوره، برقراری فضا و ارزیابی، علاج [۱]، پایش، بازنگری، ثبت و گزارش ریسک است. ایـن فرآینـد در شکل ۴ نشان داده شده است.




شکل -۴ فرآیند

توصیه می‌شود فرآیند مدیریت ریسک جزئی جدایی‌ناپذیر از مـدیریت و تصمیم سازی بـوده و در سـاختار، عملیات و فرآیند های سازمان، یکپارچه شود. فرآیند مدیریت ریسک می‌تواند در سطوح راهبـردی، عملیـاتی، برنامه‌ریزی یا پروژه، به‌کار گرفته شود.

کاربرد های زیادی از فرآیند مدیریت ریسک می‌تواند در یک سازمان وجود داشـته و به منظور دسـتیابی بـه اهداف و مناسب‌کردن فضای خارجی و داخلی که درآن به کارگرفته می‌شود، سفارشی‌سازی شود.

توصیه می‌شود ماهیت پویا و متغیر رفتار و فرهنگ انسانی، در سرتاسر فرآیند مدیریت ریسک، در نظر گرفته شود.

گرچه فرآیند مدیریت ریسک اغلب به صورت ترتیبی ارائه می‌شود، ولی در عمل، تکراری است.

[۱] Treating

## ۶-۲ ارتباط و مشاوره

مقصود از ارتباط و مشاوره، کمک به ذی نفعان مرتبط در شناسایی ریسک است، که بر اساس آن، تصمیم‌گیری می‌شود و دلایل لزوم اقدامات خاص است. ارتباط، به دنبال ارتقاء آگاهی و شناسایی ریسک است حال آن‌که مشاوره، شامل دستیابی به بازخورد و اطلاعات لازم برای پشتیبانی از تصمیم سازی است.

توصیه می‌شود هماهنگی نزدیک میان این دو، با در نظر گرفتن محرمانه بودن و یکپارچگی اطلاعات و همچنین رعایت حریم خصوصی افراد، تبادل اطلاعات واقعی، به موقع، مرتبط، درست و قابل شناسایی را تسهیل کند.

توصیه می‌شود ارتباط و مشاوره با ذی نفعان مناسب خارجی و داخلی، در سرتاسر همه مراحل فرآیند مدیریت ریسک انجام شود.

ارتباط و مشاوره، به منظور دستیابی به اهداف زیر انجام می‌شود:

- گرد هم آوردن حوزه های تخصصی مختلف برای هر مرحله از فرآیند مدیریت ریسک؛
- حصول اطمینان از در نظر گرفتن مناسب دیدگاه‌های مختلف در زمان تعریف معیارهای ریسک و ارزش یابی ریسک ها؛
- تامین اطلاعات کافی، به منظور تسهیل نظارت بر ریسک و تصمیم سازی؛
- ایجاد حس فراگیر بودن و مالکیت در میان افرادی که تحت تأثیر ریسک هستند.

## ۶-۳ دامنه شمول، فضا و معیارها

### ۶-۳-۱ کلیات

مقصود از تعیین دامنه شمول، فضا و معیارها، سفارشی‌سازی فرآیند مدیریت ریسک، توانایی ارزیابی موثر ریسک و علاج مناسب ریسک است. دامنه شمول، فضا و معیارها، شامل تعریف دامنه شمول فرآیند و شناسایی فضای خارجی و داخلی است.

### ۶-۳-۲ تعریف دامنه شمول

توصیه می‌شود سازمان، دامنه شمول فعالیت های مدیریت ریسک خود را تعریف کند. از آن‌جا که فرآیند مدیریت ریسک ممکن است در سطوح مختلفی (مانند سطوح راهبردی، عملیاتی، برنامه‌ریزی، پروژه یا سایر فعالیت‌ها) به‌کار رود، واضح بودن اهداف مورد نظر مربوطه و هم‌ترازی آن ها با اهداف سازمانی دامنه شمول مورد نظر، مهم است.

در زمان طرح‌ریزی رویکرد، ملاحظات شامل موارد زیر است:

- اهداف و تصمیماتی که باید اتخاذ شوند؛
- بروندادهایی که انتظار می‌رود از مراحل مختلف فرآیند به‌دست آید؛
- زمان، مکان، موارد شمول و خارج از شمول خاص؛

- ابزارها و تکنیک های مناسب ارزیابی ریسک؛
- منابع مورد نیاز، مسئولیت‌ها و سوابقی که باید نگه‌داری شود؛
- روابط با سایر پروژه‌ها، فرآیندها و فعالیت‌ها.

## ۶-۳-۳ فضای خارجی و داخلی

فضای خارجی و داخلی، محیطی است که سازمان در آن به دنبال تعریف و دستیابی به اهداف خود است. توصیه می‌شود فضای فرآیند مدیریت ریسک، بر مبنای شناسایی محیط خارجی و داخلی که سازمان در آن فعالیت می‌کند، برقرار شود و بهتر است منعکس‌کننده محیط خاص فعالیتی باشد که فرآیند مدیریت ریسک قرار است بر آن اعمال شود.

شناسایی این فضا به دلایل زیر اهمیت دارد:

- مدیریت ریسک در محدوده اهداف و فعالیت های سازمان انجام شود؛
- عوامل سازمانی می‌توانند یک منبع ریسک باشند؛
- هدف و دامنه شمول فرآیند مدیریت ریسک ممکن است به طور کلی، به اهداف سازمان وابسته باشد.

توصیه می‌شود سازمان، فضای خارجی و داخلی فرآیند مدیریت ریسک را با در نظر گرفتن عواملی که در زیربند ۵-۴-۱ به آن ها اشاره شد، برقرار کند.

## ۶-۳-۴ تعریف معیارهای ریسک

توصیه می‌شود سازمان، میزان و نوع ریسکی که ممکن است در ارتباط با اهداف خود با آن ها روبرو شود یا نشود را مشخص کرده و همچنین معیارهایی را به منظور ارزش یابی اهمیت ریسک و پشتیبانی از فرآیند های تصمیم سازی، تعریف کند. بهتر است معیارهای ریسک، با چارچوب مدیریت ریسک هم‌راستا بوده و با هدف و دامنه شمول خاص فعالیت مورد نظر، سفارشی‌سازی شده باشد. توصیه می‌شود معیارهای ریسک، منعکس کننده ارزش‌ها، اهداف و منابع سازمان بوده و با خط مشی‌ها و بیانیه های مدیریت ریسک، سازگار باشد. بهتر است این معیارها، با در نظر گرفتن تعهدات سازمان و دیدگاه‌های ذی نفعان تعریف شود.

در حالی که توصیه می‌شود معیارهای ریسک، در ابتدای فرآیند ارزیابی ریسک، تعریف شود، با این حال، این معیارها پویا بوده و در صورت لزوم، بهتر است به طور مستمر مورد بازنگری و اصلاح قرار گیرد.

به منظور تنظیم معیارهای ریسک، توصیه می‌شود موارد زیر در نظر گرفته شود:

- ماهیت و نوع عدم قطعیت هایی که می‌تواند بر بروندادها و اهداف (محسوس و نامحسوس) اثر گذارند؛
- چگونگی تعریف و اندازه‌گیری پیامد ها (مثبت و منفی) و احتمال؛
- عوامل مرتبط با زمان؛
- ثبات در استفاده از اندازه‌گیری‌ها؛
- چگونگی تعیین سطح ریسک؛

- چگونگی در نظر گرفتن ترکیبات و توالی‌های چندین ریسک؛
- ظرفیت سازمان.

## ۶-۴ ارزیابی ریسک

### ۶-۴-۱ کلیات

ارزیابی ریسک به معنای فرآیند کلی شناسایی، تحلیل و ارزش یابی ریسک است. توصیه می‌شود ارزیابی ریسک، به طور منظم، تکرارشونده و مشارکتی، با در نظر گرفتن دانش و دیدگاه‌های ذی نفعان اجرا شود. بهتر است این امر، با استفاده از بهترین اطلاعات دردسترس و در صورت لزوم، با تحقیقات بیشتر صورت گیرد.

### ۶-۴-۲ شناسایی ریسک

مقصود از شناسایی ریسک، یافتن، تشخیص و توصیف ریسک هایی است که ممکن است سازمان را در دستیابی به اهداف خود یاری رسانده یا مانع آن شوند. اطلاعات مرتبط، مناسب و به روز، در شناسایی ریسک ها، مهم است.

سازمان می‌تواند به منظور شناسایی عدم قطعیت هایی که ممکن است بر یک یا چند هدف تأثیر بگذارند، از گستره وسیعی از تکنیک ها استفاده کند. توصیه می‌شود عوامل زیر و رابطه میان آن ها، در شناسایی ریسک، مد نظر قرار گیرد:

- منابع محسوس و نامحسوس ریسک؛
- علل و رویدادها؛
- تهدید ها و فرصت ها؛
- آسیب‌پذیری ها و قابلیت ها؛
- تغییرات در فضای خارجی و داخلی؛
- شاخص های ریسک های نو ظهور؛
- ماهیت و ارزش دارایی ها و منابع؛
- پیامد ها و تأثیر آن ها بر اهداف؛
- محدودیت های دانش و قابلیت اتکا به اطلاعات؛
- عوامل مرتبط با زمان؛
- گرایش ها[1]، فرضیات و عقاید افراد دخیل.

[1] Biases

فارغ از این‌که منابع ریسک، تحت کنترل سازمان باشد یـا نباشـد، توصـیه مـی‌شـود سـازمان، ریسک ها را شناسایی کند. بهتر است ملاحظاتی در نظر گرفته شود که ممکن است بیش از یک نوع برونداد، حاصل شود.که این امر خود می‌تواند به انواع پیامدهای محسوس یا نامحسوس منجر شود.

## ۶-۴-۳ تحلیل ریسک

مقصود از تحلیل ریسک، شناسایی ماهیت ریسک و مشخصه‌های آن، شامل سطح ریسک، در جـای مناسـب است. تحلیل ریسک، شامل در نظر گرفتن دقیق عدم قطعیت‌ها، منابع ریسک، پیامـدها، احتمـال، رویـدادها، سناریوها، کنترل‌ها و میزان اثربخشی آن ها است. یک رویداد می‌تواند علل و پیامدهای متعددی داشـته و بـر اهداف متعددی اثر گذارد.

تحلیل ریسک می‌تواند بسته به مقصود آن، در دسترس بودن و اعتبار اطلاعات و منابع در دسترس، با درجات مختلفی از جزئیات و پیچیدگی انجام شود. بسته به شرایط و کاربرد مورد نظر، تکنیک های تحلیـل ریسـک می‌تواند کیفی، کمی یا ترکیبی از آن ها باشد. توصیه می‌شود در تحلیل ریسک، عوامل زیر در نظر گرفته شود:

- احتمال رویدادها و پیامدها؛
- ماهیت و بزرگی پیامدها؛
- پیچیدگی و اتصال[۱]؛
- عوامل مرتبط با زمان و بی‌ثباتی‌ها[۲]؛
- اثربخشی کنترل‌های موجود؛
- سطوح حساسیت و اطمینان.

تحلیل ریسک ممکن است تحت تأثیر هرگونه اختلاف نظرها، گرایش ها، یافته ها و قضـاوت هـا قـرار گیـرد. تاثیرات دیگر، کیفیت اطلاعات مورد استفاده، فرضیات و ممنوعیت‌ها و همه محدودیت‌های تکنیک ها و نحوه اجرای آن ها است. توصیه می‌شود این تاثیرات، درنظر گرفته شده، مستند شده و به تصمیم سازان ابلاغ شود. برآورد کمی رویدادهای با عدم قطعیت بالا می‌تواند دشوار باشد. این امر می‌تواند در زمان تحلیل رویدادهایی با پیامدهای شدید، مشکل‌ساز باشد. در چنین مواردی، به‌کار بردن ترکیبـی از تکنیک ها، بیـنش بهتـری را فراهم می‌آورد.

تحلیل ریسک، اطلاعات ورودی لازم برای ارزش یابی ریسک و تصمیم سازی درباره نیاز به علاج ریسک و چگونگی آن و همچنین مناسب‌ترین راهبرد و روش‌های علاج ریسک را فراهم می‌کند. نتایج به‌دست آمده، بینش لازم برای تصمیم ها را در جایی که انتخاب ها انجام می‌شود و گزینه‌های دخیل در انواع و سطوح مختلف ریسک، تامین می‌کند.

---

[۱] Connectivity

[۲] Volatility

## ۶-۴-۴ ارزش یابی ریسک

مقصود از ارزش یابی ریسک، پشتیبانی از تصمیم ها است. ارزش یابی ریسک شامل مقایسه نتایج تحلیل ریسک با معیارهای ایجاد شده ریسک است. این مقایسه برای تعیین این است که در چه مکانی نیاز به اقـدام اضـافی است. این امر می‌تواند به تصمیم‌گیری برای موارد زیر منجر شود:

- کار بیشتری انجام نشود؛
- گزینه‌های علاج ریسک در نظرگرفته شود؛
- به منظور درک بهتر ریسک، تحلیل بیشتری انجام شود؛
- کنترل‌های موجود حفظ شود؛
- اهداف، تجدید نظر شوند.

توصیه می‌شود تصمیم ها، فضای وسیع‌تر و پیامدهای حقیقی و استنباط‌شده در رابطه با ذی نفعان خـارجی و داخلی را در نظر داشته باشد.

توصیه می‌شود برونداد ارزش یابی ریسک، در سطوح مناسب سازمان، ثبت، ابلاغ و سپس تایید شود.

## ۶-۵ علاج ریسک

### ۶-۵-۱ کلیات

مقصود از علاج ریسک، انتخاب و پیاده سازی گزینه‌هایی به منظور مقابله با ریسک است. علاج ریسک، شامل فرآیندی تکراری شامل موارد زیر است:

- فرمول بندی و انتخاب گزینه‌های علاج ریسک؛
- طرح ریزی و پیاده سازی علاج ریسک؛
- ارزیابی اثربخشی علاج ریسک؛
- تصمیم‌گیری در خصوص قابل قبول بودن ریسک باقی مانده؛
- علاج بیشتر ریسک در صورت قابل قبول نبودن ریسک باقی مانده؛

### ۶-۵-۲ انتخاب گزینه های علاج ریسک

انتخاب مناسب‌ترین گزینه(های) علاج ریسک شامل ایجاد تعادل میان مزایای بالقوهٔ حاصل‌شده مربـوط بـه دستیابی به اهداف در مقابل هزینه‌ها، تلاش یا معایب ناشی از پیاده سازی آن است.

گزینه‌های علاج ریسک، الزاما به طور متقابل، انحصاری یا مناسب همه شرایط نبوده و ممکن است شامل یک یا چند مورد از موارد زیر باشند:

- جلوگیری از ریسک، با تصمیم‌گیری در مورد عدم شروع یا ادامه فعالیتی که باعث افزایش ریسک می‌شود؛
- از بین بردن یا افزایش ریسک، به منظور دستیابی به یک فرصت؛
- حذف منبع ریسک؛
- تغییر احتمال؛
- تغییر پیامد ها؛
- به اشتراک‌گذاری ریسک (به‌عنوان مثال از طریق قراردادها، خرید بیمه)؛
- حفظ ریسک، با تصمیم آگاهانه.

توجیه فرآیند علاج ریسک، از ملاحظات اقتصادی به‌تنهایی، فراتر بوده و توصیه می‌شود همه وظایف، تعهدات داوطلبانه و عقاید ذی نفعان سازمان را در نظر گیرد. توصیه می‌شود انتخاب گزینه‌های علاج ریسک، مطابق با اهداف سازمان، معیارهای ریسک و منابع موجود انجام گیرد. در زمان انتخاب گزینه‌های علاج ریسک، توصیه می‌شود سازمان، ارزش‌ها، یافته ها و مشارکت بالقوه ذی نفعان و مناسب‌ترین راه ها برای تعامل و مشاوره با ایشان را مد نظر قرار دهد. علیرغم تاثیرگذاری برابر، برخی از گزینه‌های علاج ریسک ممکن است برای برخی ذی نفعان، نسبت به سایر ذی نفعان، بیشتر قابل قبول باشد.

علاج‌های ریسک، حتی اگر با دقت، طراحی و اجرا شوند، ممکن است بروندادهای مورد انتظار را ارائه نداده و می‌تواند پیامدهای ناخواسته‌ای به دنبال داشته باشد. به منظور حصول اطمینان از این‌که اَشکال مختلف علاج ریسک، مؤثر واقع شده و مؤثر باقی بمانند، باید پایش و بازنگری، به‌عنوان بخشی جدایی‌ناپذیر از این فرآیند باشد.

علاج ریسک نیز می‌تواند منجر به معرفی ریسک های جدیدی شود که نیاز به مدیریت دارند. اگر هیچ گزینه در دسترسی، برای علاج ریسک وجود نداشته باشد یا اگر گزینه‌های علاج ریسک، به اندازه کافی، ریسک را اصلاح نکنند، توصیه می‌شود ریسک، ثبت شده و مورد بازنگری مداوم قرار گیرد.

توصیه می‌شود تصمیم سازان و سایر ذی نفعان، نسبت به ماهیت و ابعاد ریسک باقیمانده، پس از علاج ریسک، آگاه باشند. بهتر است این ریسک باقیمانده، مستند شده و مورد پایش، بازنگری و در جای مناسب، علاج بیشتر قرار گیرد.

## ۳-۵-۶ آماده سازی و پیاده سازی طرح های علاج ریسک

مقصود از طرح های علاج ریسک، این است که مشخص شود گزینه‌های منتخب علاج ریسک، بهتر است چگونه اجرا گردند تا این تمهیدات، توسط افراد دخیل، درک شده و پیشرفت به موازات طرح، قابل پایش باشد. توصیه می‌شود طرح علاج ریسک، به روشنی، ترتیبی که بهتر است علاج ریسک اجرا شود را مشخص کند.

توصیه می‌شود طرح های علاج، با مشورت با ذی نفعان شایسته، در طرح‌ها و فرآیند های مدیریتی سازمان، یکپارچه شود.

توصیه می‌شود اطلاعات ارائه شده در طرح علاج ریسک، شامل موارد زیر باشد:

- توضیح منطقی برای انتخاب گزینه های علاج ریسک، شامل مزایای قابل دستیابی مورد انتظار؛
- کسانی که در تصویب و اجرای طرح، پاسخگو و مسئول هستند؛

- اقدامات پیشنهادی؛
- منابع مورد نیاز شامل موارد احتمالی[1]؛
- اندازه‌گیری های عملکرد؛
- محدودیت ها؛
- گزارش‌دهی و پایش مورد نیاز؛
- زمان مورد انتظار برای اجرا و تکمیل اقدامات.

## ۶-۶ پایش و بازنگری

مقصود از پایش و بازنگری، حصول اطمینان و بهبود کیفیت و اثربخشی طراحی، پیاده سازی و برونـدادهـای فرآیند است. توصیه می‌شود پایش مداوم و بازنگری دوره‌ای فرآیند مدیریت ریسک و بروندادهای آن، قسمت طرح‌ریزی شده فرآیند مدیریت ریسک، با مسئولیت‌های تعریف شده واضح باشد.

توصیه می‌شود پایش و بازنگری، در تمام مراحل فرآیند انجـام شـود. پـایش و بـازنگری شـامل طـرح‌ریـزی، جمع‌آوری و تحلیل اطلاعات، ثبت نتایج و ارائه بازخورد است. توصیه می‌شود نتایج پایش و بازنگری، در سرتا سر فعالیت های مـرتبط بـا مـدیریت عملکـرد، انـدازه‌گیـری و گزارش‌دهی سازمان، گنجانده شود.

## ۶-۷ ثبت و گزارش دهی

توصیه می‌شود فرآیند مدیریت ریسک و بروندادهای آن از طریق ساز وکارهای مناسب، ثبت و گـزارش شـود. ثبت و گزارش دهی با اهداف زیر صورت می‌گیرد:

- ابلاغ فعالیت های مدیریت ریسک و بروندادهای آن در سرتا سر سازمان؛
- تامین اطلاعات به منظور تصمیم سازی؛
- بهبود فعالیت های مدیریت ریسک؛
- کمک به تعامل بهتر با ذی نفعان، شامل افراد مسئول و پاسخگوی فعالیت های مدیریت ریسک.

توصیه می‌شود تصمیم های مربوط به تهیه، نگه داری و رسیدگی به اطلاعات مستند شده، متناسب با مواردی نظیر کاربرد، حساسیت اطلاعاتی و فضای خارجی و داخلی و نه محدود به این موارد، در نظر گرفته شوند.گزارش‌دهی، قسمتی جدایی‌ناپذیر از حکمرانی سازمان بوده و توصیه می‌شود کیفیت گفتگـو بـا ذی نفعان را بالا برده و از مدیریت ارشد و نهادهای نظارتی در رویارویی با مسئولیت‌هایشان، پشتیبانی کنـد. عـواملی کـه توصیه می‌شود هنگام گزارش‌دهی در نظر گرفته شود شامل موارد زیر بوده ولی به آن ها محدود نمی‌شود:

- تنوع ذی نفعان و نیازها و الزامات اطلاعاتی مخصوص ایشان؛

[1] Contingencies

- هزینه، توالی و بهنگام بودن[1] گزارش‌دهی؛
- روش گزارش‌دهی؛
- مرتبط بودن اطلاعات، با اهداف و تصمیم سازی سازمانی.

[1] Timeliness