



جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iran National Standardization Organization



استاندارد ملی ایران

۱۶۳۴۵

چاپ اول

اردیبهشت ۱۳۹۲

INSO

16345

1st. Edition

May.2013

تنش پذیری سازمانی: سامانه‌های مدیریت
امنیت، آمادگی و استمرار - الزامات به همراه
راهنمای استفاده

**Organizational Resilience: Security,
Preparedness, and Continuity Management
Systems- Requirements with Guidance for
Use**

ICS:03.100.01

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است. تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می شود و پس از دریافت نظرها و پیشنهادهای در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند در کمیته ملی طرح و بررسی و در صورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود. بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان ملی استاندارد (ISO)^۱، کمیسیون ملی الکتروتکنیک (IEC)^۲ و سازمان ملی اندازه شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین المللی بهره گیری می شود.

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای ملی برای محصولات کشور، اجرای استانداردهای صادراتی و درجه بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سامانه های مدیریت کیفیت و مدیریت زیست-محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) و وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط سامانه تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامه تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه ملی یکاها، کالیبراسیون (واسنجی) و وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است

1 - International Organization for Standardization

2 - International Electrotechnical Commission

3 - International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« تنش پذیری سازمانی: سامانه‌های مدیریت امنیت، آمادگی و استمرار – الزامات به‌همراه راهنمای

استفاده »

سمت و/یا نمایندگی

رئیس

رئیس هیأت مدیره، شرکت فناوری اطلاعات بهاران (با مسؤولیت محدود)

عماد افشار، افسانه
(لیسانس مهندسی الکترونیک)

دبیر:

مدیرعامل، شرکت فناوری اطلاعات بهاران

داننده، آزاده
(لیسانس مهندسی کامپیوتر)

اعضا: (اسامی به ترتیب حروف الفبا)

مدیرعامل شرکت پدیدپرداز

آذرکار، علی
(فوق لیسانس مهندسی کامپیوتر نرم‌افزار)

کارشناس ارشد شرکت فن‌آوران اطلاعات بهاران

باقری، بی‌تا
(فوق لیسانس مهندسی صنایع)

کارشناس شرکت فن‌آوران اطلاعات بهاران

باقری، پارسا
(لیسانس مهندسی شیمی)

کارشناس شرکت مدیریت شبکه برق ایران

ذبیح زاده، احسان
(فوق لیسانس مهندسی برق قدرت)

کارشناس

فرهاد شیخ احمد، لیلا
(فوق لیسانس مهندسی کامپیوتر نرم‌افزار)

مشاور مرکز اپای دانشگاه تربیت مدرس

قسمتی، سیمین
(فوق لیسانس فناوری اطلاعات، لیسانس مهندسی الکترونیک)

کارشناس شرکت انرژی سپهر پایدار

کریمخانی، میثم
(لیسانس مهندسی صنایع)

مسؤول کمیسیون تدوین مقررات و استاندارد سازمان نظام صنفی رایانه‌ای استان تهران

لاریجانی، لیلا
(فوق لیسانس مخابرات)

فهرست مندرجات

صفحه	عنوان
ب	آشنایی با سازمان ملی استاندارد ایران
ج	کمیسیون فنی تدوین استاندارد
ز	پیش‌گفتار
ح	۰ مقدمه
ح	۱-۰ کلیات
ح	۲-۰ رویکرد فرآیندی
۱	۱ دامنه کاربرد
۲	۲ مراجع الزامی
۳	۱-۲ مراجع عمومی
۳	۲-۲ کاربست موازی یا یکپارچه تعدادی از سامانه‌های مدیریتی
۳	۳ اصطلاحات و تعاریف
۳	۴ الزامات سامانه مدیریت تنش‌پذیری سازمانی
۳	۱-۴ الزامات عمومی
۵	۱-۱-۴ دامنه سامانه مدیریت تنش‌پذیری سازمانی
۵	۲-۴ خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی
۵	۱-۲-۴ بیانیه خط‌مشی
۶	۲-۲-۴ تعهد مدیریت
۷	۳-۴ طرح‌ریزی
۷	۱-۳-۴ ارزیابی مخاطرات و تحلیل اثرات
۸	۲-۳-۴ الزامات قانونی و سایر الزامات
۸	۳-۳-۴ اهداف سازمانی، اهداف عملکردی و برنامه‌ها
۹	۴-۴ پیاده‌سازی و بهره‌برداری
۹	۱-۴-۴ منابع، نقش‌ها، مسئولیت‌ها و اختیارات
۱۰	۲-۴-۴ صلاحیت، آموزش و آگاهی
۱۱	۳-۴-۴ ارتباطات و هشدار
۱۲	۴-۴-۴ مستندسازی
۱۲	۵-۴-۴ کنترل مستندات
۱۳	۶-۴-۴ کنترل عملیاتی
۱۴	۷-۴-۴ پیش‌گیری، آمادگی و واکنش به رویداد
۱۶	۵-۴ بررسی (ارزش‌یابی)

۱۶	۴-۵-۱ پیش و سنجش
۱۶	۴-۵-۲ ارزیابی انطباق و عملکرد سامانه
۱۶	۴-۵-۲-۱ ارزیابی انطباق
۱۷	۴-۵-۲-۲ تمرین و آزمون
۱۷	۴-۵-۳ عدم انطباق، اقدامات اصلاحی و اقدامات پیش‌گیرانه
۱۸	۴-۵-۴ کنترل سوابق
۱۸	۴-۵-۵ ممیزی داخلی
۱۹	۴-۶ بازنگری مدیریت
۱۹	۴-۶-۱ کلیات
۱۹	۴-۶-۲ ورودی بازنگری
۱۹	۴-۶-۳ خروجی‌های بازنگری
۲۰	۴-۶-۴ نگهداشت
۲۱	پیوست الف (اطلاعاتی) راهنمای استفاده از استاندارد
۲۱	الف-۰ مقدمه
۲۳	الف-۱ الزامات عمومی
۲۵	الف-۲ خط‌مشی مدیریت تنش‌پذیری سازمانی
۲۶	الف-۳ طرح‌ریزی
۲۶	الف-۳-۱ ارزیابی مخاطرات و تحلیل اثرات
۲۹	الف-۳-۲ الزامات قانونی و سایر الزامات
۲۹	الف-۳-۳ اهداف سازمانی، اهداف عملکردی و برنامه‌ها
۳۱	الف-۴ پیاده‌سازی و بهره‌برداری (پیاده‌سازی تاکتیکی)
۳۱	الف-۴-۱ منابع، نقش‌ها، مسئولیت‌ها و اختیارات
۳۲	الف-۴-۲ صلاحیت، آموزش و آگاهی
۳۳	الف-۴-۳ ارتباطات و هشدار
۳۴	الف-۴-۴ مستندسازی
۳۵	الف-۴-۵ کنترل مستندات
۳۶	الف-۴-۶ کنترل عملیاتی
۳۶	الف-۴-۷ پیش‌گیری، آمادگی و واکنش به رویداد
۴۴	الف-۵ بررسی
۴۴	الف-۵-۱ پیش و سنجش
۴۴	الف-۵-۲ ارزیابی انطباق و عملکرد سامانه
۴۴	الف-۵-۲-۱ ارزیابی انطباق
۴۴	الف-۵-۲-۲ تمرین و آزمون

۴۶	الف-۵-۳ عدم انطباق، اقدام اصلاحی و اقدام پیشگیرانه
۴۶	الف-۵-۴ کنترل سوابق
۴۷	الف-۵-۵ ممیزی داخلی
۴۷	الف-۶ بازنگری مدیریت
۴۹	پیوست ب (الزامی) واژگان

پیش‌گفتار

استاندارد « تنش‌پذیری سازمانی: سامانه‌های مدیریت امنیت، آمادگی و استمرار- الزامات همراه با راهنمای استفاده» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان سامانه صنفی رایانه‌ای کشور تهیه و تدوین شده و در دویست و هفتاد و ششمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۱۲/۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مآخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ASIS SPC.1 : 2009 , Organizational Resilience: Security, Preparedness, and Continuity
Management Systems- Requirements with Guidance for Use

این استاندارد سامانه مدیریت در محیط بخش خصوصی، غیرانتفاعی، غیر دولتی و بخش عمومی کاربرد دارد. این استاندارد چارچوب مدیریتی است که برای برنامه‌ریزی عملیاتی و تصمیم‌گیری در شرایطی که پیش‌بینی، پیش‌گیری (در حد امکان)، آمادگی^۱ و واکنش^۲ به رویدادی انقطاعی^۳ (اضطراری^۴، بحرانی و فاجعه) ضرورت دارد، کاربرد دارد. این سامانه مدیریتی ظرفیت‌های سازمان را در زمینه مدیریت رویداد و بقا پس از وقوع آن را ارتقا می‌دهد و تعیین اقدامات مناسب برای کمک به سازمان به منظور حصول اطمینان از بقا پذیری مستمر را در بر می‌گیرد. قطع نظر از سازمان، رهبری آن در مقابل ذی‌نفعان، وظیفه دارد که برای بقای سازمان برنامه‌ریزی کند. این استاندارد معیارهای عام قابل ممیزی را برای ایجاد، رسیدگی، نگهداشت و بهبود سامانه مدیریتی ارائه می‌کند که هدف آن ارتقای ظرفیت‌های پیش‌گیری^۵، آمادگی، تخفیف دادن، واکنش، استمرار^۶ و بازیابی^۷ در برابر رویدادهای انقطاعی است.

این استاندارد به‌گونه‌ای طراحی شده است که بتواند با سامانه‌های مدیریت کیفیت، ایمنی، زیست‌محیطی، امنیت اطلاعات، مخاطرات و سایر سامانه‌های مدیریتی درون یک سازمان یکپارچه شود. بنابراین سامانه مدیریتی که به‌خوبی طراحی شده باشد می‌تواند الزامات همه این استانداردها را تامین نماید. سازمان‌هایی که رویکرد فرآیندی را در سامانه مدیریتی خود (مثلاً بر اساس استاندارد ملی ایران به شماره ۹۰۰۱: سال ۱۳۸۸، استاندارد ملی ایران به شماره ۱۴۰۰۱: سال ۱۳۷۷ و/یا استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷) پذیرفته باشند ممکن است بتوانند از سامانه مدیریتی فعلی خود به‌عنوان مبنایی برای سامانه مدیریت تنش‌پذیری سازمانی، مطابق توصیه‌های استاندارد حاضر، استفاده کنند.

۲-۰ رویکرد فرآیندی

رویکرد سامانه‌های مدیریتی، سازمان‌ها را تشویق می‌کند که نیازمندی‌های سازمانی و ذی‌نفعان را تحلیل نموده و فرآیندهایی را که در موفقیت سازمان سهیم هستند، تعریف کنند. سامانه مدیریتی می‌تواند چارچوبی را برای بهبود مستمر در جهت افزایش احتمال ارتقای امنیت، آمادگی، واکنش، استمرار و تنش‌پذیری فراهم کند. سامانه مدیریتی در سازمان و مشتریان این اعتماد به‌نفس را ایجاد می‌کند که سازمان قادر است محیطی امن و ایمن را برای برآورده ساختن نیازمندی‌های سازمان و ذی‌نفعان فراهم کند.

1 - Preparedness
 2 - Respond
 3 - Disruptive incident
 4 - Emergency
 5 - Prevention
 6 - Continuity
 7 - Recovery

این استاندارد رویکرد فرآیندی را برای ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداشت و بهبود سامانه مدیریتی تنش‌پذیری سازمانی پذیرفته است. سازمان نیاز دارد که فعالیت‌های زیادی را به‌منظور تحقق عملکرد موثر خود شناسایی و مدیریت نماید. هر فعالیتی که برای تبدیل ورودی‌ها به خروجی‌هایش از منابع استفاده می‌کند و مدیریت می‌شود را می‌توان یک فرآیند در نظر گرفت. اغلب، خروجی یک فرآیند مستقیماً، ورودی فرآیند بعدی را تشکیل می‌دهد.

کاربرد سامانه‌ی از فرآیندها در درون یک سازمان، به‌همراه شناسایی و تعامل این فرآیندها و مدیریت آنها، تحت عنوان «رویکرد فرآیندی» شناخته می‌شود.

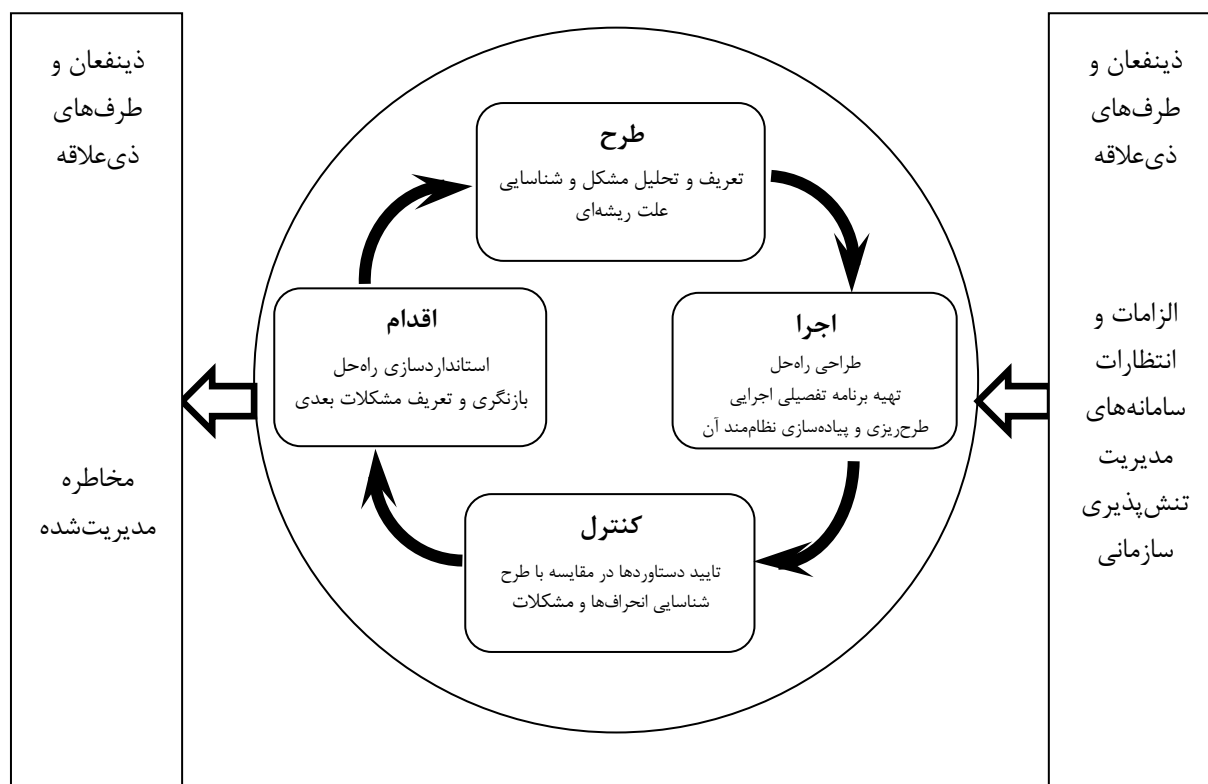
رویکرد فرآیندی برای مدیریت تنش‌پذیری سازمانی که در این استاندارد ارائه شده است، کاربران استاندارد را تشویق می‌کند تا بر اهمیت موارد زیر تاکید کنند:

- الف- درک الزامات سازمان در زمینه مخاطرات، امنیت، آمادگی، واکنش، استمرار و بازیابی؛
- ب- تعیین خط‌مشی و اهداف برای مدیریت مخاطرات؛
- پ- پیاده‌سازی و بهره‌برداری کنترل‌های لازم برای مدیریت مخاطرات سازمان با در نظر گرفتن مأموریت آن؛
- ت- پایش و بازنگری عملکرد و اثربخشی سامانه مدیریت تنش‌پذیری سازمانی؛
- ث- بهبود مستمر بر مبنای سنجش عینی.

این استاندارد مدل طرح- اجرا- کنترل- اقدام (PDCA)^۱ را پذیرفته است و از آن برای ساختاردهی به فرآیندهای سامانه مدیریتی تنش‌پذیری سازمانی استفاده کرده است. مدل PDCA گاهی به‌عنوان مدل ارزیابی- حفاظت- تایید- بهبود (APCI)^۲ نیز مورد ارجاع واقع می‌شود. * نشان می‌دهد که سامانه مدیریت تنش‌پذیری سازمانی چگونه الزامات سامانه مدیریت تنش‌پذیری سازمانی و انتظارات طرف‌های ذی‌علاقه را به عنوان ورودی‌های خود دریافت کرده و از طریق اجرای اقدامات و فرآیندهای ضروری، دستاوردهای مدیریت مخاطرات را که به آن الزامات و انتظارات پاسخ می‌دهد، تولید می‌کند. * همچنین ارتباط بین فرآیندهایی که در بند ۴ معرفی شده‌اند را نشان می‌دهد.

1 - Plan- Do- Check- Act

2 - Assess- Protect- Confirm- Improve



شکل ۱- مدل «طرح-اجرا-کنترل-اقدام»

تعیین خط‌مشی، اهداف، فرآیندها و رویه‌های سامانه مدیریت مرتبط با مدیریت مخاطرات و بهبود امنیت، آمادگی در برابر رویدادها، پاسخ‌گویی، استمرار و بازیابی و همچنین دستیابی به نتایج بر اساس خط‌مشی و اهداف عمومی سازمان.	طرح (ایجاد سامانه مدیریت)
پیاده‌سازی و بهره‌برداری خط‌مشی، کنترل‌ها، فرآیندها و رویه‌های سامانه مدیریت.	اجرا (پیاده‌سازی و بهره‌برداری سامانه مدیریت)
ارزیابی و سنجش عملکرد فرآیند در قیاس با خط‌مشی، اهداف و تجارب عملی سامانه مدیریت و گزارش نتایج به مدیریت به‌منظور بازنگری آن.	کنترل (پایش و بازنگری سامانه مدیریت)
انجام اقدامات اصلاحی و پیش‌گیرانه بر مبنای نتایج ممیزی داخلی سامانه مدیریت و بازنگری مدیریت به‌منظور دستیابی به بهبود مستمر سامانه مدیریت.	اقدام (نگهداشت و بهبود سامانه مدیریت)

انطباق با این استاندارد می‌تواند از طریق فرآیند ممیزی مطابق با روشگان^۱ استاندارد ملی ایران به شماره ۹۰۰۱: سال ۱۳۸۸، استاندارد ملی ایران به شماره ۱۴۰۰۱: سال ۱۳۷۷ و/یا استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷ و مدل تصدیق PDCA شود.

تنش پذیری سازمانی: سامانه‌های مدیریت امنیت، آمادگی و استمرار - الزامات همراه با راهنمای استفاده

۱ دامنه کاربرد

هدف از تدوین این استاندارد، مشخص کردن الزامات سامانه مدیریت تنش پذیری سازمانی است. این سامانه سازمان را در جهت تدوین و پیاده‌سازی خط‌مشی‌ها، اهداف و برنامه‌ها با مدنظر قراردادن الزامات قانونی^۱ و سایر الزاماتی که سازمان نسبت به آن‌ها متعهد است، اطلاعات مرتبط با خطرات و تهدیدهای مهمی که ممکن است بر سازمان (و ذی‌نفعانش) مؤثر باشد و حفاظت از دارایی‌های حیاتی^۲ (فیزیکی، نامشهود، زیست‌محیطی و نیروی انسانی) توانمند می‌سازد. این استاندارد در مورد مخاطرات و/یا اثرات^۳ آن‌ها که توسط سازمان شناسایی شده و سازمان می‌تواند آن‌ها را کنترل نموده، بر آن‌ها تاثیر گذاشته یا آن‌ها را کاهش دهد، کاربرد دارد. در خود این استاندارد معیارهای خاص عملکرد، مشخص نمی‌شود.

این استاندارد در مورد هر سازمانی که نسبت به موارد زیر علاقه‌مند باشد، کاربرد دارد:

- الف- ایجاد، پیاده‌سازی، نگهداشت و بهبود سامانه مدیریت تنش‌پذیری سازمانی؛
- ب- حصول اطمینان از انطباق با خط‌مشی اظهارشده سامانه مدیریت تنش‌پذیری سازمانی؛
- پ- نمایش انطباق با این استاندارد از طرق زیر:
 - ممیزی شخص اول و خوداظهاری؛ یا
 - تایید انطباق توسط طرف‌هایی که علایقی در سازمان دارند (مانند مشتریان)؛ یا
 - تایید خوداظهاری توسط طرف‌های خارج از سازمان؛ یا
 - اخذ گواهینامه برای سامانه مدیریت تنش‌پذیری سازمانی توسط یک سازمان بیرونی.

انتظار می‌رود که همه الزامات این استاندارد در هر نوع سامانه مدیریت تنش‌پذیری سازمانی در نظر گرفته شود. این استاندارد همه عناصر لازم برای یکپارچه‌سازی مدیریت، فناوری، تسهیلات^۴، فرآیندها و افراد با فرهنگ تنش‌پذیری، مدیریت مخاطرات و سامانه مدیریت تنش‌پذیری سازمانی یک سازمان را در اختیار قرار می‌دهد. میزان کاربرد آن‌ها به عواملی مانند آستانه‌های تحمل مخاطرات^۵ و خط‌مشی سازمان؛ ماهیت فعالیت‌های سازمان، محصولات و خدمات و مکان قرار گرفتن سازمان و شرایطی که در آن کار می‌کند بستگی دارد.

1 - Legal
2 - Critical
3 - Impacts
4 - Facilities
5 - Risk Tolerance

این استاندارد الزامات عامی را به عنوان چارچوبی که در مورد همه انواع سازمان‌ها (یا قسمت‌هایی از آن‌ها)، مستقل از اندازه و ماهیت عملیات آن‌ها کاربرد دارد، ارائه می‌دهد. همچنین رهنمودهایی به سازمان‌ها ارائه می‌دهد تا بتوانند معیارهای عملکرد خاص خود را تعیین کنند و سامانه مدیریت تنش‌پذیری سازمانی را متناسب با نیازهای خود و ذی‌نفعانشان متناسب‌سازی و پیاده کنند.

این استاندارد بر تنش‌پذیری به معنی ظرفیت انطباقی یک سازمان در محیط پیچیده و متغیر و همچنین حفاظت از دارایی‌های حیاتی تاکید دارد. کاربرد این استاندارد سازمان را در موقعیتی قرار می‌دهد که در برابر همه انواع عمدی، غیرعمدی و/یا طبیعی رویدادهای انقطاعی، که اگر مدیریت نشود می‌تواند به شرایط اضطراری، بحران^۱ یا فاجعه^۲ منجر شود، آمادگی بیشتر و واکنش سریع‌تر داشته باشد. این استاندارد همه مراحل مدیریت رویداد شامل قبل، در حین و بعد از واقعه مخرب را پوشش می‌دهد.

استاندارد حاضر، سازمان را در حوزه‌های زیر توانمند می‌سازد:

الف- تدوین خط‌مشی پیش‌گیری، آمادگی و واکنش/استمرار/بازیابی؛

ب- تدوین اهداف، رویه‌ها و فرآیندها در جهت دستیابی به تعهدات خط‌مشی؛

پ- حصول اطمینان از صلاحیت، آگاهی و آموزش؛

ت- تعیین سنجش‌هایی برای سنجش عملکرد و نشان دادن دستیابی به موفقیت؛

ث- انجام اقدامات مورد نیاز برای بهبود عملکرد؛

ج- نشان دادن انطباق سامانه با الزامات استاندارد حاضر؛ و

چ- ایجاد و به‌کارگیری فرآیندی برای بهبود مستمر.

پیوست الف راهنمایی‌هایی برای طرح‌ریزی، پیاده‌سازی، آزمایش، نگهداشت و بهبود سامانه مدیریت تنش‌پذیری سازمانی ارائه می‌دهد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدارکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است. استفاده از مراجع زیر برای این استاندارد الزامی است:

1 - crisis
2 - disaster

۱-۲ مراجع عمومی

2-1-1 ISO Guide 73:2002, Risk management- Vocabulary- Guidelines for use in standards

۲-۲ کاربرد موازی یا یکپارچه تعدادی از سامانه‌های مدیریتی

۱-۲-۲ استاندارد ملی ایران به شماره ۹۰۰۱: سال ۱۳۸۸، سامانه‌های مدیریت کیفیت - الزامات

۲-۲-۲ استاندارد ملی ایران به شماره ۱۴۰۰۱: سال ۱۳۷۷، سیستم‌های مدیریت زیست محیطی - مشخصات همراه با راهنمای استفاده

۳-۲-۲ استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - سامانه‌های مدیریت امنیت اطلاعات - الزامات

۴-۲-۲ استاندارد ملی ایران به شماره ۲۸۰۰۰: سال ۱۳۸۷، سامانه‌های مدیریت امنیت زنجیره تامین مشخصات

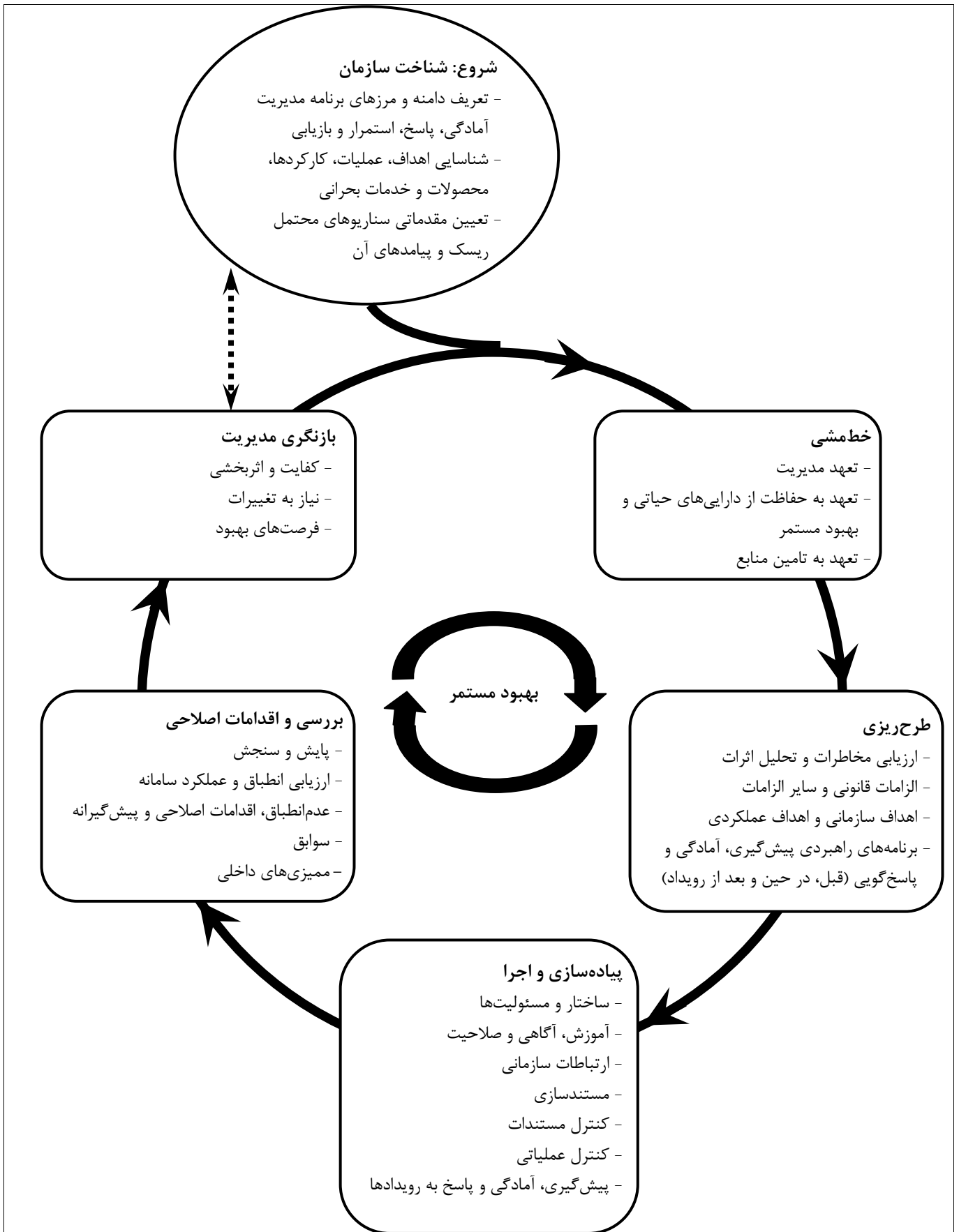
۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف تعیین شده در پیوست ب به کار می‌رود.

۴ الزامات سامانه مدیریت تنش‌پذیری سازمانی

۱-۴ الزامات عمومی

سازمان باید سامانه مدیریت تنش‌پذیری سازمانی (امنیت، آمادگی و استمرار) را مطابق با الزامات این استاندارد ایجاد، مستند، پیاده‌سازی، نگهداری نموده و در مورد بهبود مستمر آن اقدام نماید و نحوه پاسخ‌گویی به این الزامات را تعیین کند.



شکل ۲- نمودار جریان سامانه مدیریت تنش‌پذیری سازمانی

۴-۱-۱ دامنه سامانه مدیریت تنش پذیری سازمانی

سازمان باید دامنه سامانه مدیریت تنش پذیری سازمانی را تعریف و مستند کند.

در تعریف دامنه، سازمان باید:

الف- مرزهای^۱ سازمان را که در دامنه برنامه تنش پذیری سازمانی قرار می‌گیرد، تعریف کند (همه سازمان یا یک یا چند قسمت از آن).

ب- الزامات سامانه مدیریت تنش پذیری سازمانی را با در نظر گرفتن مأموریت، اهداف، تعهدات اجباری داخلی و بیرونی (شامل موارد مرتبط با ذی‌نفعان) و مسئولیت‌های قانونی پایه‌ریزی کند.

پ- اهداف عملیاتی، دارایی‌ها^۲، کارکردها، خدمات و محصولات حیاتی را در نظر بگیرد.

ت- سناریوهای مخاطرات را مبتنی بر وقایع بالقوه داخلی و بیرونی که می‌توانند بر عملیات و کارکردهای حیاتی سازمان در حوزه اثرات بالقوه آنها تاثیر داشته باشد، تعیین کند.

ث- دامنه سامانه مدیریت تنش پذیری سازمانی را بر حسب و متناسب با اندازه، ماهیت و پیچیدگی سازمان، از منظر بهبود مستمر تعریف کند.

سازمان باید دامنه را سازگار با حفاظت و مراقبت از یکپارچگی سازمان و ارتباطات آن با ذی‌نفعان، شامل تعاملات با تامین‌کنندگان کلیدی، شرکای برون‌سپاری و سایر ذی‌نفعان (مثلا شرکا و تامین‌کنندگان زنجیره تامین سازمان، مشتریان، سهام‌داران، جامعه‌ای که در آن کار می‌کند و غیره) تعریف کند.

بیانیه کاربست پذیری^۳ باید وزن راهبردی مدیریت امنیت، آمادگی، مدیریت شرایط اضطراری، مدیریت فاجعه، مدیریت بحران و مدیریت استمرار کسب‌وکار را در طراحی سامانه مدیریتی، مبتنی بر ارزیابی مخاطرات و تحلیل اثرات آن، تعریف کند.

۴-۲ خط‌مشی سامانه مدیریت تنش پذیری سازمانی

مدیریت ارشد باید خط‌مشی سامانه مدیریت تنش پذیری سازمانی را تعریف و مستند کرده و منابع آن را فراهم کند. خط‌مشی سامانه مدیریت تنش پذیری سازمانی باید حاوی تعهد به حفاظت از دارایی‌های انسانی، زیست‌محیطی و فیزیکی؛ و همچنین پیش‌بینی و آمادگی برای وقایع بازدارنده^۴ بالقوه؛ و نیز استمرار عملیات و کسب‌وکار باشد.

۴-۲-۱ بیانیه خط‌مشی

بیانیه خط‌مشی سازمان باید اطمینان حاصل کند که در دامنه تعریف‌شده سامانه مدیریت تنش‌پذیری سازمانی، موارد زیر رعایت شده است:

1 - Boundaries
2 - Assets
3 - Statement of Applicability
4 - Adverse

- الف- با ماهیت و اندازه تهدیدها، خطرات^۱ و مخاطرات و آثار (پیامدها) آنها بر فعالیتها، کارکردها، محصولات و خدمات (شامل ذی‌نفعان و محیط زیست) سازمان تناسب دارد.
- ب- شامل تعهد در برابر ایمنی حیات کارکنان و جامعه، به‌عنوان اولین اولویت، است.
- پ- شامل تعهد به بهبود مستمر است.
- ت- شامل تعهد به ارتقای پایداری و تنش‌پذیری سازمانی است.
- ث- شامل تعهد به پیش‌گیری، کاهش و تخفیف^۲ مخاطرات است.
- ج- شامل تعهد به انطباق با الزامات قانونی مرتبط و سایر الزاماتی که سازمان در برابر آنها تعهد دارد است.
- چ- چارچوبی را برای تعیین و بازنگری اهداف سازمانی و اهداف عملکردی سامانه مدیریت تنش‌پذیری سازمانی فراهم می‌کند.
- ح- خط‌مشی مستند، پیاده‌سازی و نگهداری می‌شود.
- خ- به محدودیت‌ها و موارد خارج از شمول ارجاع می‌دهد.
- د- آستانه‌های تحمل‌پذیری مخاطرات را در ارتباط با دامنه سامانه مدیریت تعیین و مستند می‌کند.
- ذ- به اطلاع همه افرادی که برای سازمان یا به نمایندگی از سازمان کار می‌کنند رسانده می‌شود.
- ر- در دسترس ذی‌نفعان مرتبط قرار دارد.

یادآوری- سازمان ممکن است نسخه غیرمحرمانه خط‌مشی خود را که حاوی اطلاعات حساس امنیتی نیست در اختیار عموم قرار دهد.

- ز- فرد مشخصی را به‌عنوان مالک^۳ خط‌مشی و/یا نقطه تماس مسئول معرفی می‌کند.
- ژ- در مقاطع برنامه‌ریزی شده و همچنین مقاطعی که تغییرات اساسی رخ می‌دهد بازنگری می‌شود.
- س- توسط مدیریت ارشد امضا شده و مرتبط بودن خط‌مشی سالانه مورد بازنگری قرار می‌گیرد و سوابق آن مستند می‌شود.

۲-۲-۴ تعهد مدیریت

- مدیریت باید شواهدی مبنی بر تعهد خود در برابر ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداشت و بهبود سامانه مدیریت تنش‌پذیری سازمانی را از طرق زیر ارائه نماید:
- الف- تدوین خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی؛
- ب- حصول اطمینان از اینکه اهداف و طرح‌های سامانه مدیریت تنش‌پذیری سازمانی تدوین شده است؛
- پ- تعیین نقش‌ها، مسئولیت‌ها و صلاحیت‌های^۴ مدیریت تنش‌پذیری سازمانی؛

1 - Hazards
2 - Mitigation
3 - Owner
4 - Competency

- ت- تعیین فرد یا افرادی به‌عنوان مسئول سامانه مدیریت تنش‌پذیری سازمانی با اختیارات و صلاحیت‌های مناسب که در برابر پیاده‌سازی و نگهداشت سامانه مدیریت پاسخ‌گو باشد؛
- ث- اطلاع‌رسانی به سازمان در مورد اهمیت دستیابی به اهداف مدیریت تنش‌پذیری سازمانی و انطباق با خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی، مسئولیت‌های آن در برابر قانون و نیاز به بهبود مستمر؛
- ج- تامین منابع کافی برای ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداشت و بهبود سامانه مدیریت تنش‌پذیری سازمانی؛
- چ- تصمیم‌گیری در مورد معیارهای پذیرش مخاطرات و سطوح قابل قبول مخاطره؛
- ح- حصول اطمینان از اینکه ممیزی‌های داخلی سامانه مدیریت تنش‌پذیری سازمانی انجام می‌شود؛
- خ- انجام بازنگری‌های مدیریتی سامانه مدیریت تنش‌پذیری سازمانی؛ و
- د- نمایش تعهد خود به بهبود مستمر.

۳-۴ طرح‌ریزی

۱-۳-۴ ارزیابی مخاطرات و تحلیل اثرات

- سازمان باید فرآیند رسمی و مستند ارزیابی را برای موارد زیر تدوین، پیاده‌سازی و نگهداری کند:
- الف- هدایت نظام‌مند شناسایی و تعیین ارزش دارایی‌ها به‌منظور شناسایی موضوعات حیاتی شامل فعالیت‌ها، کارکردها، خدمات، محصولات، شراکت‌ها^۱، زنجیره‌های تامین، ارتباط با ذی‌نفعان و آثار بالقوه مرتبط با رویدادهای انقطاعی براساس سناریوهای مخاطرات؛
- ب- شناسایی خطرات و تهدیدهای عمدی، غیرعمدی و طبیعی که به صورت بالقوه ممکن است اثر مستقیم یا غیرمستقیم بر عملیات، کارکردها، دارایی‌های انسانی، نامشهود و فیزیکی، محیط زیست و ذی‌نفعان سازمان داشته باشد؛
- پ- تحلیل نظام‌مند مخاطرات، آسیب‌پذیری^۲، بحرانی‌بودن و آثار (پیامدها) آنها؛
- ت- تحلیل و اولویت‌بندی نظام‌مند کنترل‌ها و شیوه‌های برخورد با مخاطرات و هزینه‌های مرتبط؛ و
- ث- تعیین مخاطراتی که تاثیر مهمی بر فعالیت‌ها، کارکردها، خدمات، محصولات، ارتباط با ذی‌نفعان و محیط زیست دارند (مخاطرات مهم و اثرات مهم).

سازمان باید:

- الف- اطلاعات فوق را مستند کرده و آنها را به‌شکل مقتضی به‌روز و محرمانه نگهدارد؛
- ب- متناسب با تغییرات در سازمان یا تغییراتی که در محیط عملیاتی سازمان، رویه‌ها، کارکردها، خدمات، شراکت‌ها و زنجیره‌های تامین آن رخ می‌دهد مخاطرات و تاثیرات آن را بازرزیابی نماید؛
- پ- اهداف و اولویت‌های مرتبط با زمان بازرزیابی را تعیین کند؛

1 - Partnerships
2 - Vulnerability

ت- فواید و هزینه‌های مستقیم و غیرمستقیم گزینه‌های کاهش مخاطره و ارتقای پایداری^۱ و تنش‌پذیری را ارزیابی نماید؛

ث- نسبت به لحاظ نمودن مخاطرات و اثرات مهم در ایجاد، پیاده‌سازی و بهره‌برداری سامانه مدیریت تنش‌پذیری سازمانی اطمینان حاصل کند.

۴-۳-۲ الزامات قانونی و سایر الزامات

سازمان باید برای موارد زیر رویه‌هایی را تدوین و نگهداری کند:

الف- شناسایی الزامات قانونی، مقرراتی و سایر الزاماتی که سازمان در برابر آنها متعهد است و با خطرات، تهدیدها و مخاطرات سازمان که در ارتباط با تسهیلات، فعالیت‌ها، کارکردها، محصولات، خدمات، زنجیره تامین، محیط زیست و ذی‌نفعان سازمان است، مرتبط است.

ب- تعیین اینکه این الزامات چگونه برای خطرات، تهدیدها، مخاطرات و آثار بالقوه آنها به کار می‌رود.

سازمان باید این اطلاعات را مستند کرده و آنها را به‌روز نگهدارد.

سازمان باید اطمینان حاصل کند که الزامات قانونی، مقرراتی و غیره که در برابر آنها متعهد است در ایجاد، پیاده‌سازی و نگهداشت سامانه مدیریت تنش‌پذیری سازمانی لحاظ شده است.

۴-۳-۳ اهداف سازمانی، اهداف عملکردی و برنامه‌ها

سازمان باید اهداف سازمانی و اهداف عملکردی را برای اجتناب، پیش‌گیری، بازداشتن^۲، تخفیف دادن، واکنش نشان دادن و بازیابی از رویدادهای انقطاعی، به‌شکل مستند، تدوین و نگهداری کند. اهداف سازمانی و اهداف عملکردی مدون همچنین باید انتظارات مرتبط با سایر روابط سازمانی بیرون از حدود سازمان (مانند تامین‌کنندگان) را که برای انجام ماموریت و کارکردهای عملیاتی سازمان حیاتی هستند، تعیین نمایند.

اهداف سازمانی و اهداف عملکردی باید به‌صورت کیفی و / یا کمی قابل سنجش بوده، با خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی سازگار باشند و شامل تعهد به موارد زیر باشند:

الف- پیش‌گیری، کاهش و تخفیف مخاطرات؛

ب- ارتقای تنش‌پذیری؛

پ- الزامات استمرار مالی، عملیاتی و کسب‌وکار (شامل استمرار نیروی کار)؛

ت- انطباق با الزامات قانونی و سایر الزامات؛

ث- بهبود مستمر.

1 - Sustainability

2 - Deter

سازمان باید هنگام تعیین و بازنگری اهداف سازمانی و اهداف عملکردی، الزامات قانونی، مقرراتی و غیره، مخاطرات مهم و اثرات مهم، گزینه‌های فناورانه، الزامات مالی، عملیاتی و کسب‌وکار و دیدگاه‌های ذی‌نفعان و سایر طرف‌های ذی‌علاقه خود را در نظر بگیرد.

سازمان باید یک یا چند برنامه راهبردی را برای دستیابی به اهداف سازمانی و اهداف عملکردی خود تدوین نماید. این برنامه‌ها باید شامل موارد زیر باشند:

الف- تعیین مسئولیت و منابع لازم برای دستیابی به اهداف سازمانی و اهداف عملکردی در واحدهای وظیفه‌ای و سطوح مرتبط سازمان؛

ب- در نظر گرفتن فعالیت‌ها، کارکردها، الزامات قانونی یا مقرراتی، تعهدات قراردادی، نیازهای ذی‌نفعان، توافق‌نامه‌های دوجانبه کمک و محیط زیست؛ و

پ- راه‌ها و محدوده‌های زمانی که در قالب آن‌ها باید به برنامه‌ها دست یافت.

سازمان باید یک یا چند برنامه راهبردی را برای موارد زیر تدوین نماید:

الف- پیش‌گیری و بازداشتن- اجتناب، حذف، بازداشتن یا پیش‌گیری از احتمال وقوع رویداد انقطاعی و پیامدهای آن شامل جابجایی^۱ دارایی انسانی یا فیزیکی که در معرض مخاطره قرار دارد.

ب- تخفیف- کمینه کردن تاثیر یک رویداد انقطاعی.

پ- واکنش در شرایط اضطراری- واکنش اولیه به رویداد انقطاعی شامل حفاظت از افراد و اموال از آسیب آنی. واکنش اولیه توسط مدیریت ممکن است بخشی از واکنش اولیه سازمان باشد.

ت- استمرار- فرآیندها، کنترل‌ها و منابعی که باید برای حصول اطمینان از اینکه سازمان در دستیابی به اهداف عملیاتی حیاتی خود استمرار دارد، در دسترس باشند.

ث- بازیابی- فرآیندها، منابع و ظرفیت‌های سازمان در محدوده زمانی تعیین شده در اهداف، بازسازی^۲ می‌شوند تا سازمان به الزامات عملیاتی جاری خود دست بیابد.

سازمان باید برنامه‌های راهبردی خود را ارزیابی کرده تا تعیین کند که آیا این اقدامات، مخاطره‌های جدیدی را ایجاد کرده‌اند یا خیر.

۴-۴ پیاده‌سازی و بهره‌برداری

۱-۴-۴ منابع، نقش‌ها، مسئولیت‌ها و اختیارات

مدیریت باید در مورد در دسترس بودن منابع ضروری برای پیاده‌سازی و کنترل سامانه مدیریت تنش‌پذیری سازمانی اطمینان حاصل کند. منابع شامل منابع انسانی و مهارت‌های خاص، تجهیزات، زیرساخت‌های داخلی، فناوری، اطلاعات، هوشمندی^۳ و منابع مالی است.

1- Removal

2 - re-established

3 - Intelligence

نقش‌ها، مسئولیت‌ها و اختیارات باید به‌منظور تسهیل سامانه مدیریت اثربخش تنش‌پذیری سازمانی، تعریف و مستند شده و اطلاع‌رسانی شود.

مدیریت ارشد سازمان باید نماینده(گان) مدیریت ویژه‌ای را تعیین کند که مستقل از سایر مسئولیت‌ها، نقش‌ها، مسئولیت‌ها و اختیار تعریف‌شده‌ای برای موارد زیر داشته باشد:

الف- حصول اطمینان از اینکه سامانه مدیریت تنش‌پذیری سازمانی بر اساس الزامات این استاندارد ایجاد، اطلاع‌رسانی، پیاده‌سازی و نگهداری می‌شود؛

ب- گزارش‌دهی عملکرد سامانه مدیریت تنش‌پذیری سازمانی به مدیریت ارشد به‌منظور بازنگری آن و به‌عنوان مبنایی برای بهبود.

سازمان باید:

الف- تیم مدیریت تنش‌پذیری سازمانی را با اختیارات مناسب تشکیل دهد تا بر آمادگی در برابر رویدادها، واکنش به رویدادها و بازیابی از رویدادها نظارت کند؛

ب- ظرفیت‌ها و رویه‌های لجستیکی لازم برای یافتن، تدارک، ذخیره، توزیع، نگهداشت، آزمایش و حسابداری خدمات، کارکنان، منابع، مواد و تسهیلات تولیدی یا اهدایی را به‌منظور پشتیبانی از سامانه مدیریت تنش‌پذیری سازمانی ایجاد نماید؛

پ- اهداف مدیریت منابع را برای زمان‌های واکنش، کارکنان، تجهیزات، آموزش‌ها، تسهیلات، منابع مالی، بیمه، کنترل تعهدات^۱، دانش تخصصی، مواد و بازه‌های زمانی که به آنها نیاز است، چه از منابع داخلی سازمان و چه از منابع شرکای سازمان، تعیین نماید؛

ت- رویه‌هایی برای مساعدت ذی‌نفعان، ارتباطات، پیمان‌های راهبردی^۲ و کمک دوجانبه تدوین نماید.

سازمان باید رویه‌های مالی و اداری را برای پشتیبانی از برنامه مدیریت تنش‌پذیری سازمانی قبل، در حین و پس از رویداد تدوین نماید. این رویه‌ها باید موارد زیر را رعایت کنند:

الف- حصول اطمینان از اینکه تصمیمات مالی می‌تواند تسریع شود؛

ب- با سطوح اختیارات و اصول حسابداری تعریف‌شده انطباق داشته باشند.

۴-۴-۲ صلاحیت، آموزش و آگاهی^۳

سازمان باید اطمینان حاصل کند که هر فردی که کاری را انجام می‌دهد که به‌طور بالقوه می‌تواند از خطرات، تهدیدها و مخاطرات مهم پیش‌گیری نموده یا آن را موجب شود یا به آن واکنش نشان دهد یا آن را تخفیف دهد یا از آن تاثیر بپذیرد، دارای صلاحیت است (بر مبنای تحصیلات، آموزش یا تجربه مناسب) و باید سوابق آن را حفظ کند.

1 - liability control

2 - strategic alliances

3 - Awareness

سازمان باید نیازهای آموزشی مرتبط با مدیریت خطرات، تهدیدها و مخاطرات خود و همچنین سامانه مدیریت تنش‌پذیری خود را شناسایی نماید. سازمان باید برای برآوردن این نیازها، آموزش‌ها را تامین نموده یا اقدامات دیگری را انجام داده و سوابق آن را حفظ نماید.

سازمان باید برای حصول اطمینان از اینکه کارکنانی که برای سازمان یا به نمایندگی از سازمان کار می‌کنند در موارد زیر آگاهی دارند، رویه‌هایی را تدوین، پیاده‌سازی و نگهداری کند:

الف- خطرات، تهدیدها و مخاطرات مهم و آثار مرتبط واقعی یا بالقوه که با کار آنها مرتبط است و منافع حاصل از عملکرد شخصی بهبودیافته؛

ب- رویه‌های پیش‌گیری، بازداشتن، تخفیف دادن، حفاظت فردی، تخلیه^۱، واکنش، استمرار و بازیابی از رویداد؛

پ- اهمیت انطباق با خط‌مشی و رویه‌های مدیریت تنش‌پذیری سازمانی و الزامات سامانه مدیریت تنش‌پذیری سازمانی؛

ت- نقش‌ها و مسئولیت‌های کارکنان در دستیابی به انطباق با الزامات سامانه مدیریت تنش‌پذیری سازمانی؛

ث- پیامدهای بالقوه عدول از رویه‌های مشخص شده؛

ج- منافع حاصل از عملکرد شخصی بهبودیافته.

سازمان باید فرهنگ مدیریت تنش‌پذیری را ایجاد کرده، ارتقا داده و درونی سازد تا:

الف- اطمینان حاصل کند که فرهنگ مدیریت تنش‌پذیری بخشی از ارزش‌های محوری سازمان و همچنین حاکمیت سازمان^۲ است؛

ب- ذی‌نفعان را نسبت به خط‌مشی مدیریت تنش‌پذیری و نقش آنها در برنامه‌ها آگاه سازد.

۴-۴-۳ ارتباطات و هشدار^۳

سازمان باید با در نظر داشتن خطرات، تهدیدها و مخاطرات خود و همچنین سامانه مدیریت تنش‌پذیری، رویه‌هایی را برای موارد زیر ایجاد، پیاده‌سازی و نگهداری کند:

الف- مستندسازی، ثبت سوابق و اطلاع‌رسانی تغییرات در مستندات، طرح‌ها، رویه‌ها، سامانه مدیریتی و نتایج ارزیابی‌ها و بازنگری‌ها؛

ب- ارتباطات داخلی بین سطوح و کارکردهای مختلف سازمان؛

پ- ارتباطات بیرونی با شرکا و سایر ذی‌نفعان؛

ت- دریافت، مستندسازی و پاسخ به ارتباطات برقرارشده از طرف ذی‌نفعان بیرونی سازمان؛

ث- انطباق و یکپارچه‌سازی با سامانه ملی یا منطقه‌ای مشاوره مخاطرات یا تهدیدها یا سامانه‌های مشابه آن در کاربردهای طرح‌ریزی و عملیاتی؛

1 - Evacuation

2 - Organization governance

3 - Warning

- ج- هشدار به ذی‌نفعانی که قابلیت بالقوه تاثیرپذیری از رویداد انقطاعی واقعی یا قریب‌الوقوع را دارند؛
- چ- حصول اطمینان از وجود ابزارهای ارتباطی در شرایط وقوع بحران و توقف عملیات؛
- ح- تسهیل ارتباط ساخت‌یافته با مسئولین واکنش در شرایط اضطراری؛
- خ- حصول اطمینان از تعامل درونی سازمان‌ها و کارکنان متعددی که مسئول واکنش هستند؛
- د- ثبت اطلاعات مهم در مورد رویداد، اقدامات انجام شده و تصمیمات اخذ شده؛ و
- ذ- بهره‌برداری از تسهیلات ارتباطی.

سازمان باید بر اساس ایمنی حیات^۱ به‌عنوان اولین اولویت و همچنین مشورت با ذی‌نفعان، در مورد اطلاع‌رسانی بیرونی مخاطرات مهم خود و تاثیرات آنها، تصمیم‌گیری نموده و تصمیم خود را مستند کند. اگر تصمیم، اطلاع‌رسانی باشد سازمان باید روش‌هایی را برای ارتباط بیرونی، آماده‌باش^۲ و هشدار (شامل استفاده از رسانه‌ها) ایجاد و پیاده‌سازی نماید.

سامانه‌های ارتباطی مدیریت تنش‌پذیری سازمانی باید به طور منظم مورد آزمون قرار گیرد.

۴-۴-۴ مستندسازی

- مستندات سامانه مدیریت تنش‌پذیری سازمانی باید شامل موارد زیر باشد:
- الف- خط‌مشی، اهداف سازمانی و اهداف عملکردی مدیریت تنش‌پذیری سازمانی؛
 - ب- توصیف دامنه‌ی سامانه مدیریت تنش‌پذیری سازمانی؛
 - پ- توصیف عناصر اصلی سامانه مدیریت تنش‌پذیری سازمانی و یکپارچگی آنها با مستندات مرتبط؛
 - ت- مستندات شامل سوابقی که بر اساس استاندارد حاضر، الزامی است؛
 - ث- مستندات شامل سوابقی که سازمان آنها را برای حصول اطمینان از طرح‌ریزی، اجرا و کنترل اثربخش فرآیندهای مرتبط با مخاطرات مهم، ضروری تشخیص داده است.

۵-۴-۴ کنترل مستندات

مستندات موردنیاز سامانه مدیریت تنش‌پذیری سازمانی و همچنین استاندارد حاضر، باید تحت کنترل باشند. سوابق نوع خاصی از مستندات هستند و باید بر اساس الزامات تعیین شده در بند ۴-۵-۴ تحت کنترل قرار گیرند.

- سازمان باید رویه‌ای (یا رویه‌هایی) را برای موارد زیر تدوین، پیاده‌سازی و نگهداری کند:
- الف- تایید کفایت مستندات پیش از انتشار آنها؛
 - ب- بازنگری، به‌روزرسانی و تایید مجدد مستندات بر اساس ضرورت؛
 - پ- حصول اطمینان از اینکه تغییرات و وضعیت نسخه جاری مستندات شناسایی می‌شود؛

1 - Life safety
2 - Alerts

ت- حصول اطمینان از این که نسخه‌های مرتبط از مستندات کاربردی در نقاط استفاده در دسترس قرار دارد؛

ث- تعیین پارامترهای مرتبط با نگهداری و آرشیو مستندات؛

ج- حصول اطمینان از اینکه نسخه‌های اصلی و آرشیو شده مستندات، داده‌ها و اطلاعات قابل شناسایی و خوانا هستند؛

چ- حصول اطمینان از اینکه مستندات با منشاء خارجی که توسط سازمان برای طرح‌ریزی و اجرای سامانه مدیریت تنش‌پذیری سازمانی ضروری تشخیص داده شده‌اند، شناسایی شده و توزیع آنها تحت کنترل قرار دارد؛

ح- شناسایی همه مستندات تاریخ گذشته، که سازمان نگهداری آنها را ضروری تشخیص داده است به‌عنوان نسخ منسوخ؛ و

خ- حصول اطمینان از یکپارچگی مستندات از طریق کسب اطمینان در مورد اینکه از دسترسی غیرمجاز حفاظت شده‌اند، به‌طور امن پشتیبان‌گیری شده‌اند، فقط در دسترس کارکنان مجاز قرار دارند و در مقابل آسیب، دستکاری^۱ و از بین رفتن محافظت می‌شوند.

۴-۴-۶ کنترل عملیاتی

سازمان باید از طرق زیر، عملیات مرتبط با مخاطرات مهم شناسایی شده که با خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی، ارزیابی مخاطرات، تحلیل اثرات، اهداف سازمانی و اهداف عملکردی سازگاری دارند، را شناسایی و طرح‌ریزی نماید تا از طرق زیر اطمینان حاصل نماید که این عملیات تحت شرایط مشخص شده اجرا می‌شوند:

الف- تدوین، پیاده‌سازی و نگهداری رویه‌هایی مرتبط با خطرات، تهدیدها و مخاطرات شناسایی شده برای فعالیت‌ها، کارکردها، محصولات و خدمات سازمان و همچنین اطلاع‌رسانی در مورد رویه‌های کاربردی و الزامات مرتبط به تامین‌کنندگان (شامل پیمانکاران)؛

ب- تدوین، پیاده‌سازی و نگهداری رویه‌های مکتوب برای کنترل وضعیت در شرایطی که نبود آنها موجب انحراف از خط‌مشی، اهداف سازمانی و اهداف عملکردی مدیریت تنش‌پذیری سازمانی می‌شود؛ و

پ- تصریح معیارهای عملیاتی در رویه‌های مستندشده.

رویه‌های کنترل عملیاتی باید به قابلیت اطمینان و تنش‌پذیری، ایمنی و سلامت افراد و حفاظت از اموال و محیط زیست که تحت تاثیر رویداد انقطاعی قرار می‌گیرند، بپردازند.

1 - Deterioration

۷-۴-۴ پیش‌گیری، آمادگی و واکنش به رویداد

سازمان باید رویه‌هایی را برای شناسایی رویدادهای انقطاعی بالقوه که می‌توانند بر سازمان، فعالیت‌هایش، کارکردهایش، خدماتش، ذی‌نفعانش و محیط زیست تاثیر داشته باشند، تدوین، پیاده‌سازی و نگهداری کند. رویه‌ها باید چگونگی پیش‌گیری، آمادگی و واکنش سازمان به رویدادها را مستند کنند. سازمان باید در برابر رویدادهای انقطاعی واقعی آماده بوده و به آن‌ها واکنش نشان دهد تا پیامدهای مضر آنها را پیش‌گیری کرده یا کاهش دهد.

هنگام تدوین، پیاده‌سازی و نگهداری رویه یا رویه‌هایی برای آمادگی و واکنش سریع به یک رویداد انقطاعی، سازمان بهتر است اقدامات زیر را در نظر داشته باشد:

الف- حفاظت از ایمنی حیات؛

ب- حفاظت از دارایی‌ها؛

پ- پیش‌گیری از گسترش دامنه رویداد انقطاعی؛

ت- کاهش طول توقف عملیات؛

ث- بازگرداندن استمرار عملیات حیاتی^۱؛

ج- بازیابی عملیات معمول (شامل ارزشیابی بهبودها)؛

چ- حفاظت از وجهه^۲ و خوشنامی^۳ سازمان (شامل پوشش رسانه‌ای و ارتباط با ذی‌نفعان).

تدوین رویه‌هایی برای پیش‌گیری، آمادگی و واکنش به رویداد که برای نیازهای خاص سازمان مناسب باشد، از مسئولیت‌های سازمان است. بهتر است سازمان هنگام تدوین رویه‌ها، نیازهایش را با توجه به موارد زیر مد نظر قرار دهد:

الف- ماهیت خطرات میدانی^۴ (مثلا موارد قابل اشتعال و سمی، مخازن نگهداری و گازهای تحت فشار) و اقداماتی که باید در هنگام بروز رویداد انقطاعی یا انتشارهای اتفاقی انجام شود؛

ب- ماهیت خطرات موضعی، در همسایگی یا سایر خطرات بیرونی که تاثیر بالقوه بر سازمان دارد؛

پ- محتمل‌ترین نوع و اندازه‌ی رویداد انقطاعی؛

ت- مناسب‌ترین روش تخفیف و واکنش اضطراری به رویداد انقطاعی برای اجتناب از تبدیل آن به بحران یا فاجعه؛

ث- رویه‌های برای پیش‌گیری از تخریب محیط زیست؛

ج- رویه‌های فرماندهی و کنترل، و ساختار از پیش‌تعریف شده‌ی سلسله مراتب فرماندهی^۵ برای مرکز (مراکز) عملیات اضطراری و/یا سایت کاری جایگزین؛

1 - Critical operational continuity

2 - Image

3 - Reputation

4 - Onsite hazards

5 - Command

- چ- رویه‌ها و اختیارات برای اعلام وضعیت اضطراری، آغاز رویه‌های اضطراری، فعال نمودن طرح‌ها و اقدامات، ارزیابی آسیب و اتخاذ تصمیمات مالی؛
- ح- طرح‌های ارتباطات داخلی و بیرونی شامل مطلع نمودن مقامات و ذی‌نفعان مرتبط؛
- خ- رویه‌هایی برای به خدمت گرفتن و/یا ارائه خدمات درمانی؛
- د- اقدامات لازم برای کمینه کردن تلفات^۱ انسانی و تخریب فیزیکی و زیست‌محیطی؛
- ذ- اقدامات لازم برای تامین امنیت اطلاعات حیاتی، سامانه‌های اطلاعاتی، تسهیلات و افراد؛
- ر- اقداماتی که برای تخفیف و واکنش در برابر انواع مختلف رویداد(های) انقطاعی یا وضعیت(های) اضطراری باید انجام شوند؛
- ز- نیاز به فرآیند یا فرآیندهایی برای ارزیابی پس از وقوع به‌منظور تعیین و پیاده‌سازی اقدامات اصلاحی و پیش‌گیرانه؛
- ژ- آزمایش دوره‌ای رویه‌ها و فرآیندهای مدیریت رویدادها و شرایط اضطراری و واکنش در برابر آن‌ها؛
- س- آموزش کارکنان مسئول واکنش به رویدادها و شرایط اضطراری؛
- ش- فهرستی از کارکنان کلیدی و موسسات کمک‌رسان شامل جزئیات تماس (مثلا سازمان آتش‌نشانی، مرکز فوریت‌های پزشکی، ضابطان قضایی، مراکز خدمات پاک‌سازی مواد خطرناک)؛
- ص- مسیرهای تخلیه و نقاط تجمع شامل فهرست کارکنان و جزئیات تماس؛
- ض- احتمال تاثیرگذاری رویداد انقطاعی یا وضعیت اضطراری بر زیرساخت‌های حیاتی (مانند: برق آب، مخابرات، حمل‌ونقل) یا تاثیرپذیری از آنها
- ع- امکان استفاده از مساعدت دوجانبه سازمان‌های همسایه؛
- غ- رویه‌ها و اقدامات لازم برای بازیابی هر فعالیت حیاتی در چارچوب بازه زمانی هدف‌گذاری شده‌ی سازمان و منابعی که برای بازیابی مورد نیاز است.
- سازمان باید به‌صورت دوره‌ای رویه‌های پیش‌گیری، آمادگی و واکنش خود را، بخصوص پس از وقوع حوادث یا رویدادهایی که می‌تواند گسترش یافته و به شرایط اضطراری، بحران یا فاجعه تبدیل شود، بازنگری و در صورت نیاز اصلاح نماید.
- سازمان باید اطمینان یابد که هر فردی که اقدامات پیش‌گیری، آمادگی و واکنش را از جانب آن، انجام می‌دهد دارای صلاحیت کافی مبتنی بر تحصیلات، آموزش‌ها یا تجارب مرتبط است و سوابق آن را نگهداری نماید.
- سازمان باید این اطلاعات را مستند نموده و آنها را در فواصل زمانی منظم یا هنگام بروز تغییرات، به‌روزرسانی نماید.

1 - Casualties

۵-۴ بررسی^۱ (ارزش‌یابی)^۲

سازمان باید طرح‌ها، رویه‌ها و ظرفیت‌های مدیریت تنش‌پذیری سازمانی را از طریق ارزیابی، آزمون، گزارش‌های پس از وقوع رویداد، آموخته‌ها^۳، ارزیابی‌های عملکرد و تمرین‌ها^۴ به صورت دوره‌ای، ارزش‌یابی نماید. تغییرات مهم در این عوامل بهتر است فوراً در رویه‌ها منعکس شود.

سازمان باید سوابق مربوط به نتایج ارزش‌یابی‌های دوره‌ای را نگهداری کند.

۱-۵-۴ پایش^۵ و سنجش^۶

سازمان باید سنجه‌های عملکرد و رویه‌هایی را برای پایش و سنجش منظم مشخصه‌هایی^۷ از عملیات خود که تاثیر قابل توجهی بر عملکرد سازمان (شامل مشارکت‌ها و ارتباطات زنجیره تامین) دارند، تدوین، پیاده‌سازی و نگهداری کند. رویه‌ها باید شامل مستندسازی اطلاعات لازم برای پایش عملکرد و کنترل‌های عملیاتی مقتضی باشند و با اهداف سازمانی و اهداف عملکردی مدیریت تنش‌پذیری سازمانی انطباق داشته باشند.

سازمان باید عملکرد سامانه‌هایی که از دارایی‌های حفاظت می‌کند و همچنین سامانه‌های ارتباطی و اطلاعاتی خود را ارزیابی و مستند کند.

۲-۵-۴ ارزیابی انطباق و عملکرد سامانه

۱-۲-۵-۴ ارزیابی انطباق

سازمان باید متناسب با تعهداتش در حوزه انطباق، رویه‌هایی را برای ارزیابی دوره‌ای انطباق با الزامات قانونی و مقرراتی تدوین، پیاده‌سازی و نگهداری کند.

سازمان باید انطباق با سایر الزاماتی که در برابر آنها متعهد است، از جمله الگوهای موفق صنعت^۸ را ارزیابی نماید. سازمان ممکن است مایل باشد این ارزیابی را با ارزیابی انطباق با قوانین و مقرراتی که در بالا اشاره شد، ترکیب کند یا آنها را در رویه‌هایی مجزا پوشش دهد.

سازمان باید سوابق نتایج ارزیابی‌های دوره‌ای را نگهداری کند.

۲-۲-۵-۴ تمرین و آزمون

سازمان باید مناسب بودن و کارایی سامانه مدیریت تنش‌پذیری سازمانی، برنامه‌ها، فرآیندها و رویه‌های خود (شامل مشارکت‌ها و ارتباطات زنجیره تامین) را مورد آزمون قرار داده و ارزش‌یابی نماید.

-
- 1 - Checking
 - 2 - Evaluation
 - 3 - Lessons learned
 - 4 - Exercises
 - 5 - Monitoring
 - 6 - Measurement
 - 7 - Characteristics
 - 8 - Industry best practices

سازمان باید سامانه مدیریت تنش‌پذیری سازمانی خود را از طریق تمرین‌ها و آزمایش‌هایی، صحت‌گذاری نماید به طوری که این تمرین‌ها و آزمایش‌ها:

الف- با دامنه سامانه مدیریت تنش‌پذیری سازمانی و اهداف سازمان سازگار باشد؛
ب- بر مبنای سناریوهای واقع‌بینانه‌ای انجام شود که به خوبی طرح‌ریزی شده و اهداف و مقاصد آن‌ها به روشنی تعریف شده باشد؛

پ- ریسک اختلال در عملیات و ظرفیت بالقوه ایجاد مخاطره در عملیات و دارایی‌ها را کمینه کند؛
ت- گزارش رسمی پس از تمرین را تولید کند به طوری که شامل دستاوردها، توصیه‌ها و ترتیباتی برای پیاده‌سازی بهبودها در زمان‌های مقرر باشد؛

ث- با هدف ترویج بهبود مستمر، بازنگری شود؛ و
ج- در فواصل زمانی برنامه‌ریزی شده و بعضی مواقع در زمان‌های غیرمنظم که توسط مدیریت سازمان تعیین شده است و همچنین هنگامی که تغییرات مهمی در سازمان و محیط عملیاتی آن رخ می‌دهد، انجام شود.

۴-۵-۳ عدم انطباق، اقدامات اصلاحی و اقدامات پیش‌گیرانه

سازمان باید رویه‌هایی را برای پرداختن به عدم انطباق‌های واقعی و بالقوه و همچنین تعیین اقدامات اصلاحی و پیش‌گیرانه تدوین، پیاده‌سازی و نگهداری کند. این رویه‌ها باید الزاماتی را برای موارد زیر تعریف کنند:

الف- شناسایی و اصلاح عدم انطباق‌ها و انجام اقداماتی برای تخفیف اثرات آن‌ها؛
ب- بررسی عدم انطباق‌ها، تعیین علل آنها و انجام اقداماتی که از وقوع مجدد آنها جلوگیری می‌کند؛
پ- ارزیابی نیاز به اقداماتی که از عدم انطباق‌ها پیش‌گیری کند و پیاده‌سازی اقدامات مناسبی که برای اجتناب از وقوع مجدد آنها طراحی شده است؛
ت- ثبت نتایج اقدامات اصلاحی و پیش‌گیرانه انجام شده؛
ث- بازنگری اثربخشی اقدامات اصلاحی و پیش‌گیرانه انجام شده.

اقدامات تعیین شده باید با تاثیرات مشکلات بالقوه متناسب باشند و به سرعت انجام شوند.
سازمان باید مخاطرات تغییر یافته را شناسایی کرده و الزامات اقدام پیش‌گیرانه را، با تمرکز بر مخاطراتی که تغییر زیادی یافته‌اند، شناسایی نماید.

اولویت اقدامات پیش‌گیرانه باید بر مبنای نتایج ارزیابی مخاطرات و تحلیل اثرات تعیین شود.
سازمان باید تغییرات ضروری را در مستندات سامانه مدیریت تنش‌پذیری سازمانی اعمال کند.

۴-۵-۴ کنترل سوابق

سازمان باید سوابقی را برای نشان دادن انطباق با الزامات سامانه مدیریت تنش‌پذیری سازمانی و همچنین انطباق با این استاندارد و نتایجی که به آنها دست یافته است، ایجاد و نگهداری کند.

سازمان باید رویه‌هایی را برای حفاظت از یکپارچگی سوابق که موضوعات دسترسی، شناسایی، ذخیره، حفاظت، بازیابی، نگهداری و امحاء آنها را پوشش دهد، تدوین، پیاده‌سازی و نگهداری کند. سوابق باید شفاف، قابل شناسایی و قابل ردیابی باشند و این ویژگی‌ها را در چرخه حیات خود حفظ نمایند.

۴-۵-۵ ممیزی داخلی

سازمان باید ممیزی داخلی سامانه مدیریت تنش‌پذیری سازمانی را در فواصل برنامه‌ریزی شده و همچنین در بعضی مواقع به صورت غیر دوره‌ای (که توسط مدیریت سازمان تعیین شده است) انجام دهد تا مشخص شود که آیا اهداف کنترلی، کنترل‌ها، فرآیندها و رویه‌های سامانه تنش‌پذیری سازمانی ویژگی‌های زیر را دارد یا خیر:

- الف- با الزامات این استاندارد و قوانین و مقررات مرتبط انطباق دارد؛
- ب- با الزامات مدیریت مخاطرات سازمان انطباق دارد؛
- پ- به صورت اثربخش پیاده‌سازی و نگهداری می‌شود؛
- ت- مطابق انتظار اجرا می‌شود.

برنامه ممیزی باید با در نظر گرفتن وضعیت و اهمیت فرآیندها و حوزه‌هایی که باید ممیزی شوند و همچنین نتایج ممیزی‌های قبلی طرح‌ریزی شود. معیارها، دامنه، تواتر و روش‌های ممیزی باید تعریف شود. انتخاب ممیزان و انجام ممیزی‌ها باید عینیت و بی‌طرفی فرآیند ممیزی را تضمین کند. ممیزان نباید کارهای خود را ممیزی کنند.

مسئولیت‌ها و الزامات طرح‌ریزی و اجرای ممیزی‌ها و همچنین گزارش‌دهی نتایج و نگهداری سوابق (به بند ۴-۵-۴ مراجعه شود) باید در رویه مکتوبی تعریف شود.

مدیریتی که مسئول حوزه مورد ممیزی است باید مطمئن شود که اقدامات لازم برای حذف عدم‌انطباق‌های شناسایی شده و دلایل آنها بدون فوت وقت انجام می‌شود. فعالیت‌های پیگیری رفع عدم‌انطباق‌ها باید شامل تصدیق اقدامات انجام شده و گزارش‌دهی نتایج تصدیق باشند.

۴-۶ بازنگری مدیریت^۱

۴-۶-۱ کلیات

مدیریت باید به منظور حصول اطمینان از استمرار مناسب بودن، کفایت و اثربخشی سامانه مدیریت تنش‌پذیری سازمانی، این سامانه را در فواصل برنامه‌ریزی شده مورد بازنگری قرار دهد. این بازنگری باید شامل ارزیابی فرصت‌های بهبود و نیاز به تغییراتی در سامانه تنش‌پذیری سازمانی از جمله خط‌مشی و اهداف سامانه باشد. نتایج بازنگری باید به طور شفاف مستند شده و سوابق آن نگهداری شود (به بند ۴-۵-۴ مراجعه شود).

1 - Management review

۲-۶-۴ ورودی بازنگری

ورودی‌های بازنگری مدیریت باید شامل موارد زیر باشد:

- الف- نتایج ممیزی‌ها و بازنگری‌های سامانه مدیریت تنش‌پذیری سازمانی؛
- ب- بازخورد طرف‌های ذی‌علاقه؛
- پ- فنون، محصولات یا رویه‌هایی که می‌تواند برای بهبود عملکرد و اثربخشی سامانه مدیریت تنش‌پذیری سازمانی در سازمان استفاده شود؛
- ت- وضعیت اقدامات اصلاحی و پیش‌گیرانه؛
- ث- نتایج تمرین‌ها و آزمون‌ها؛
- ج- آسیب‌پذیری‌ها یا تهدیدهایی که در ارزیابی قبلی مخاطرات در حد کفایت به آنها پرداخته نشده است؛
- چ- نتایج سنجش اثربخشی؛
- ح- پیگیری‌های انجام شده از بازنگری‌های قبلی مدیریت؛
- خ- هر تغییری که می‌تواند بر سامانه مدیریت تنش‌پذیری سازمانی تاثیر داشته باشد؛
- د- کفایت خط‌مشی و اهداف؛ و
- ذ- توصیه‌های بهبود.

۳-۶-۴ خروجی‌های بازنگری

خروجی بازنگری مدیریت باید شامل تصمیمات و اقدامات مرتبط با موارد زیر باشد:

- الف- بهبود اثربخشی سامانه مدیریت تنش‌پذیری سازمانی؛
- ب- به‌روزروری طرح‌های ارزیابی مخاطرات، تحلیل اثرات، آمادگی و واکنش به رویدادها؛
- پ- در صورت نیاز، اعمال اصلاحات در رویه‌ها و کنترل‌هایی که بر مخاطرات تاثیرگذار هستند به منظور واکنش به رخدادهای داخلی یا بیرونی که ممکن است بر سامانه مدیریت تنش‌پذیری سازمانی تاثیر داشته باشد، شامل تغییر در موارد زیر:
 - الزامات کسب‌وکار و عملیات؛
 - الزامات امنیتی و کاهش مخاطرات؛
 - فرآیندهای وضعیت عملیاتی که بر الزامات عملیاتی موجود تاثیر می‌گذارد؛
 - الزامات قانونی و مقرراتی؛
 - تعهدات قراردادی؛ و
 - سطوح مخاطره و یا معیارهای پذیرش مخاطره.
- ت- منابع مورد نیاز؛ و
- ث- بهبود در زمینه چگونگی سنجش اثربخشی کنترل‌ها.

۴-۶-۴ نگهداشت^۱

مدیریت ارشد باید برنامه‌ای برای نگهداشت سامانه مدیریت تنش‌پذیری سازمانی تعریف و مستند کند تا اطمینان کسب کند که هر تغییر داخلی یا بیرونی که بر سازمان تاثیرگذار است، در ارتباط با سامانه مدیریت تنش‌پذیری سازمانی بازنگری می‌شود. این برنامه باید فعالیت‌های حیاتی جدیدی که لازم است در برنامه نگهداشت سامانه مدیریت تنش‌پذیری سازمانی گنجانده شود، را شناسایی کند.

۵-۶-۴ بهبود مستمر

سازمان باید مرتباً اثربخشی سامانه مدیریت تنش‌پذیری سازمانی را از طریق به‌کارگیری خط‌مشی، اهداف، نتایج ممیزی، تحلیل وقایع پایش شده، اقدامات اصلاحی و پیش‌گیرانه و بازنگری مدیریت بهبود بخشد.

1 - Maintenance

پیوست الف (اطلاعاتی) راهنمای استفاده از استاندارد

یادآوری - مطالب ارائه شده در این پیوست تنها جنبه اطلاعاتی داشته و به منظور کمک به درک الزامات ذکر شده در بند ۴ این استاندارد آورده شده است. این مطالب، با وجودی که به الزامات ذکر شده در بند ۴ می‌پردازد و کاملاً با آن سازگار است اما به هیچ عنوان چیزی به آنها اضافه یا از آنها کم نمی‌کند یا به هیچ طریقی آنها را تغییر نمی‌دهد.

الف-۰ مقدمه

فجایع طبیعی، حوادث زیست‌محیطی، وقایع نامطلوب فناوری و بحران‌های انسان‌ساخت به طور تاریخی نشان می‌دهد که رویدادهای انقطاعی می‌تواند رخ دهد و بر بخش عمومی و خصوصی به طور یکسان تاثیر بگذارد. این چالش فراتر از اکثر طرح‌های واکنش به شرایط اضطراری یا فعالیت‌های مدیریت فجایعی است که قبلاً به کار گرفته شده است. اکنون سازمان‌ها باید درگیر فرآیند جامع و نظام‌مند پیش‌گیری، آمادگی، تخفیف دادن، واکنش، استمرار و بازیابی شوند. دیگر تهیه طرح واکنش که سناریوهای فاجعه یا شرایط اضطراری را پیش‌بینی می‌کنند، کافی نیست. تهدیدهای امروز ایجاب می‌کند که فرآیندی جاری، پویا و تعاملی برای حصول اطمینان از استمرار فعالیت‌های محوری سازمان، قبل، در حین و بخصوص پس از وقوع یک بحران عمده وجود داشته باشد.

این استاندارد برای همه سازمان‌ها در انواع و اندازه‌های مختلف، عناصر مورد نیاز را برای دستیابی و نشان دادن کاهش پیش‌گیرانه مخاطرات و عملکرد تنش‌پذیری سازمانی مرتبط با تسهیلات فیزیکی، خدمات، فعالیت‌ها، محصولات، زنجیره‌های تامین و استمرار عملیاتی (کسب‌وکار) آنها ارائه می‌کند. این امر با در نظر داشتن موارد زیر انجام می‌شود:

الف- افزایش مخاطرات و تهدیدهای امنیتی؛

ب- قوانین و مقررات سخت‌گیرانه‌تر؛

پ- واقعیات کسب‌وکار رقابتی‌تر؛

ت- افزایش وابستگی‌ها در جامعه (در سطح سازمانی، کارکردی، یا حقوقی)؛

ث- بالا بردن آگاهی در مورد نیاز به طرح‌ریزی مکفی برای واکنش به شرایط اضطراری و اقدامات جبرانی؛

ج- ملاحظات مرتبط با طرف‌های ذی‌علاقه و تاثیرپذیر؛ و

چ- نیاز به تضمین استمرار عملیاتی و تنش‌پذیری.

رویداد انقطاعی که به شکل مناسبی مدیریت نشود، می‌تواند به سرعت به یک موقعیت اضطراری، بحران یا حتی فاجعه تبدیل شود. آمادگی در برابر یک رویداد قبل از وقوع آن، می‌تواند تاثیرات آن را کمینه کند. رویداد انقطاعی مدیریت نشده علاوه بر خرابی‌های فیزیکی و زیست‌محیطی مهم، جراحت و تلفات جانی، می‌تواند وجهه، خوشنامی و نشان تجاری یک سازمان را نیز مخدوش کند. این استاندارد چارچوبی را برای

کمک به سازمان‌ها در مدیریت موفقیت‌آمیز یک رویداد انقطاعی از طریق تدوین راهبرد و برنامه اجرایی در جهت محافظت از منافع خود و ذی‌نفعانشان ارائه می‌کند.

طرح‌ریزی و آمادگی پیش‌گیرانه در برابر توقف‌ها و رویدادهای بالقوه، تاثیر و طول مدت توقف [عملیات] را کاهش خواهد داد. فرآیند مدیریتی کل‌نگر می‌تواند به کمینه کردن و اجتناب از تعلیق خدمات و عملیات حیاتی کمک کند و در نتیجه امکان برگشت به خدمات و عملیات معمول را در اسرع وقت فراهم می‌کند.

این استاندارد راهنمایی‌ها یا توصیه‌هایی را برای سازمان‌ها در بخش‌های خصوصی، غیرانتفاعی و عمومی ارائه می‌کند تا الگوهای موفق را در جهت کمک و گسترش اقدام در موارد زیر، شناسایی کرده و تعریف کنند:

الف- فراهم آوردن چشم‌اندازی مبتنی بر دیدگاه مدیریت ارشد و رهبری برای راهبردهایی در جهت حفاظت از دارایی‌ها و تضمین تنش‌پذیری سازمان؛

ب- شناسایی و ارزیابی دارایی‌ها، خدمات و کارکردها به منظور تعیین بخش‌هایی از عملیات و کسب‌وکار که برای موفقیت کوتاه‌مدت و درازمدت سازمان حیاتی هستند؛

پ- شناسایی خطرات و تهدیدهای بالقوه و ارزیابی مخاطرات و اثرات؛

ت- تخفیف اثرات طیف وسیعی از خطرات و تهدیدها شامل بلایای طبیعی، حوادث فناورانه و زیست‌محیطی و فجایع انسان‌ساخت (تروریسم و جنایت)؛

ث- درک نقش‌ها و مسئولیت‌های مورد نیاز برای حفاظت از دارایی‌ها و تنش‌پذیری بیشتر؛

ج- مدیریت منابع لازم برای آمادگی و واکنش به رویدادها و شرایط اضطراری؛

چ- ایجاد پیمان‌های راهبردی^۱ و توافق‌نامه‌های کمک دو جانبه^۲؛

ح- تدوین و نگهداری طرح‌های آمادگی و واکنش به رویدادها و شرایط اضطراری و رویه‌های اجرایی مرتبط؛

خ- تعیین و اجرای آموزش‌ها و تمرین‌هایی برای پشتیبانی و ارزیابی آمادگی برای شرایط اضطراری/رویدادها، طرح‌های واکنش به رویدادها و شرایط اضطراری و رویه‌های عملیاتی؛

د- حصول اطمینان از آگاهی کارکنان، مشتریان، تامین‌کنندگان و سایر ذی‌نفعان مرتبط در مورد ترتیبات آمادگی و واکنش به رویدادها و شرایط اضطراری و برخورداری از اعتماد به نفس در کاربرد آنها؛

ذ- تدوین رویه‌های ارتباطات داخلی و بیرونی شامل پاسخ به درخواست رسانه‌ها و جامعه برای [دریافت] اطلاعات؛

ر- تعیین سنجه‌های سنجش و نشان دادن موفقیت؛

ز- مستندسازی منابع، زیرساخت‌ها، کارها و مسئولیت‌های کلیدی مورد نیاز برای پشتیبانی از کارکردهای حیاتی عملیات؛ و

ژ- تدوین فرآیندهایی که تضمین کند همگام با تغییر مخاطرات و محیط عملیاتی، اطلاعات به‌روز و مرتبط نگهداشته می‌شود.

1 - Strategic alliances

2 - Mutual aids

حفاظت سازمان از دارایی‌های فیزیکی، مجازی^۱ و انسانی موضوع درستی است. موفقیت سامانه مدیریت به تعهد همه سطوح و واحدها در سازمان، بخصوص مدیریت ارشد سازمان، بستگی دارد. تصمیم‌گیران باید آماده باشند تا بودجه و منابع ضروری را به این امر تخصیص دهند. لازم است ساختار اداری مناسبی برای پرداختن اثربخش به پیش‌گیری، تخفیف و مدیریت ایجاد شود. این امر تضمین می‌کند که همه افراد درگیر درک می‌کنند که چه کسی تصمیم می‌گیرد، تصمیمات چگونه اجرا می‌شوند و نقش‌ها و مسئولیت‌های مشارکت‌کنندگان چیست. بهتر است کارکنانی که برای مدیریت رویداد انتخاب می‌شوند، این نقش‌ها را به‌عنوان بخشی از وظایف معمول خود انجام دهند، و نباید انتظار داشت که این کارها به صورت داوطلبانه انجام شود. مستقل از نوع سازمان (انتفاعی، غیرانتفاعی، مذهبی، غیردولتی) رهبری آن در قبال ذی‌نفعان وظیفه دارد که برای حفظ و بقای سازمان برنامه‌ریزی کند.

الف-۱ الزامات عمومی

هدف پیاده‌سازی سامانه مدیریت تنش‌پذیری سازمانی مبتنی بر استاندارد حاضر، دستیابی به عملکرد بهبود یافته در زمینه‌ی امنیت، آمادگی، واکنش، استمرار و بازیابی است. بنابراین این استاندارد بر این اصل استوار است که سازمان به‌صورت دوره‌ای سامانه مدیریت تنش‌پذیری سازمانی خود را بازنگری و ارزیابی خواهد کرد تا فرصت‌های بهبود را شناسایی کرده و آنها را اجرا کند. نرخ، دامنه و بازه زمانی این فرآیند بهبود مستمر توسط سازمان و تحت تاثیر شرایط اقتصادی و سایر عوامل تعیین می‌شود. بهبودهای سامانه مدیریت تنش‌پذیری سازمانی به بهبودهای بیشتر در عملکرد امنیت، آمادگی، واکنش، استمرار و بازیابی و همچنین تنش‌پذیری سازمان منجر خواهد شد. این استاندارد از سازمان می‌خواهد تا:

الف- خط‌مشی مناسبی را برای سامانه مدیریت تنش‌پذیری سازمانی تدوین کند؛

ب- خطرات و تهدیدهای مرتبط با فعالیت‌ها، کارکردها، محصولات و خدمات قبلی، حال و آینده سازمان را به‌منظور تعیین مخاطرات، پیامدها و اثرات مهم آنها شناسایی کند؛

پ- الزامات قانونی و سایر الزامات مرتبط را که سازمان در برابر آنها متعهد است، شناسایی کند؛

ت- اولویت‌ها را شناسایی کرده و اهداف سازمانی و اهداف عملکردی مناسب سامانه مدیریت تنش‌پذیری سازمانی را تعیین کند؛

ث- ساختار و برنامه‌ای برای پیاده‌سازی خط‌مشی و دستیابی به اهداف سازمانی و برآوردن اهداف عملکردی ایجاد کند؛

ج- طرح‌ریزی، کنترل، پایش، اقدامات اصلاحی و پیش‌گیرانه و فعالیت‌های ممیزی و بازنگری را تسهیل کند تا در مورد انطباق با خط‌مشی و مناسب بودن سامانه مدیریت تنش‌پذیری سازمانی اطمینان حاصل کند؛

چ- ظرفیت لازم برای انطباق با محیط متغیر را داشته‌باشد.

سازمانی که فاقد سامانه مدیریت تنش‌پذیری سازمانی است بهتر است موقعیت کنونی خود را با توجه با دارایی‌های حیاتی و سناریوهای محتمل مخاطره از طریق انجام یک بازنگری مشخص کند. بهتر است هدف

1 - Virtual

این بازنگری در نظر گرفتن همه خطرات و تهدیدهای سازمان و مخاطرات و تاثیرات مرتبط آنها بر دارایی‌های حیاتی، به‌عنوان مبنایی برای استقرار سامانه مدیریت تنش‌پذیری سازمانی باشد.

این بازنگری بهتر است چهار حوزه کلیدی زیر را پوشش دهد:

الف- شناسایی مخاطرات شامل موارد مرتبط با شرایط عادی عملیات، شرایط غیرعادی عملیات شامل روشن کردن^۱ و خاموش کردن^۲ و شرایط اضطراری و حوادث.

ب- شناسایی الزامات قانونی مرتبط و سایر الزاماتی که سازمان در برابر آنها متعهد است.

پ- تمرین کارها و رویه‌های موجود مدیریت مخاطرات شامل فعالیت‌های مرتبط با تدارکات و عقد قرارداد.

ت- ارزیابی شرایط اضطراری و حوادث قبلی.

در همه موارد، بهتر است عملیات و کارکردهای عادی و غیرعادی درون سازمان، ارتباطش با ذی‌نفعان ذیربط و شرایط بالقوه اضطراری و منجر به توقف در نظر گرفته شود. ابزارها و روش‌های انجام بازنگری، متناسب با ماهیت فعالیت‌ها، می‌تواند شامل فهرست‌های کنترلی (چک‌لیست‌ها)، انجام مصاحبه، بازرسی و سنجش مستقیم یا نتایج ممیزی‌ها و بازنگری‌های پیشین باشد.

سازمان در مورد تعریف مرزهای خود آزادی و انعطاف‌پذیری دارد و می‌تواند انتخاب کند که این استاندارد را در همه سازمان یا در یک واحد عملیاتی خاص پیاده کند. سازمان بهتر است دامنه سامانه مدیریت تنش‌پذیری سازمانی خود را تعریف و مستند کند.

تعیین دامنه به‌منظور شفاف‌سازی مرزهای سازمان که قرار است سامانه مدیریت تنش‌پذیری سازمانی در آن اعمال شود، صورت می‌گیرد، بخصوص هنگامی که سازمان، بخشی از یک سازمان بزرگتر در یک مکان مشخص است. با تعریف دامنه، کلیه فعالیت‌ها، محصولات و خدمات سازمان در دامنه مورد نظر باید در سامانه مدیریت تنش‌پذیری سازمانی در نظر گرفته شوند. در تعیین دامنه، اعتبار سامانه مدیریت تنش‌پذیری سازمانی به انتخاب مرزهای سازمانی بستگی دارد. بهتر است هنگامی که بخشی از سازمان خارج از دامنه سامانه مدیریت تنش‌پذیری سازمانی قرار می‌گیرد سازمان بتواند دلایل این خارج بودن را تشریح کند.

اگر این استاندارد برای یک واحد عملیاتی خاص پیاده شود، خط‌مشی‌ها و رویه‌های تدوین شده در سایر قسمت‌های سازمان می‌تواند برای تامین الزامات این استاندارد مورد استفاده قرار گیرد، به شرط آن که برای واحد عملیاتی مورد نظر تناسب داشته باشد.

مدیریت تنش‌پذیری سازمانی با موضوعات و اقدامات قبل، در حین و بعد از رویداد انقطاعی سروکار دارد. بنابراین این استاندارد پیش‌گیری، اجتناب^۳، بازداشتن، آمادگی، تخفیف، واکنش، استمرار و بازیابی را شامل می‌شود. محیط مخاطرات و همچنین واقعیت‌های عملیاتی یا کسب‌وکار، وزن راهبردی متفاوتی را برای هر

1 - start up
2 - shut down
3 - Avoidance

یک این عناصر قایل هستند ولی برای هیچیک از آنها نباید وزن صفر را در نظر گرفت. بیانیه کاربست‌پذیری باید بر مبنای ارزیابی مخاطرات و تحلیل اثرات، وزن راهبردی مدیریت امنیت، آمادگی، مدیریت شرایط اضطراری، مدیریت فجایع، مدیریت بحران و مدیریت استمرار کسب‌وکار را در تدوین سامانه مدیریت تنش‌پذیری سازمانی براساس ارزیابی مخاطرات و تحلیل اثرات، روشن بیان کند (به بند ۴-۳-۱ مراجعه شود).

الف-۲ خط‌مشی مدیریت تنش‌پذیری سازمانی

خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی، نیروی پیشران^۱ پیاده‌سازی و بهبود سامانه مدیریت تنش‌پذیری سازمانی است که می‌تواند پایداری و تنش‌پذیری [سازمان] را حفظ کرده و آن را گسترش دهد. بنابراین بهتر است خط‌مشی، بیانگر تعهد مدیریت ارشد در موارد زیر باشد:

الف- انطباق با الزامات قانونی و سایر الزامات مرتبط؛

ب- پیش‌گیری، آمادگی و تخفیف رویدادهای انقطاعی؛

پ- بهبود مستمر.

خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی مبنایی را شکل می‌دهد که بر اساس آن سازمان اهداف سازمانی و اهداف عملکردی خود را تعیین می‌کند. بهتر است خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی به‌اندازه کافی شفاف باشد تا بتواند توسط طرف‌های ذی‌علاقه داخلی و بیرونی درک شود و به‌صورت دوره‌ای بازنگری و اصلاح شود تا شرایط و اطلاعات در حال تغییر را منعکس کند. بهتر است حوزه کاربرد آن (یعنی دامنه) به‌روشنی قابل شناسایی باشد و ماهیت^۲ یگانه، اندازه و تاثیر مخاطرات فعالیت‌ها، وظایف، محصولات و خدمات سازمان را منعکس سازد.

بهتر است خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی به اطلاع همه افرادی که برای سازمان (یا به‌نماینده‌گی از سازمان) کار می‌کنند، از جمله پیمانکارانی که در تاسیسات سازمان کار می‌کنند، رسانده شود. ارتباط با پیمانکاران می‌تواند به‌شکل متفاوتی در بیانیه خط‌مشی بیان شود، مثلاً در قالب قواعد، راهنماها و رویه‌ها و در نتیجه ممکن است تنها بخش‌های مرتبطی از خط‌مشی را دربرگیرد. بهتر است مدیریت ارشد خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی را، با در نظر گرفتن خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی نهاد بالادستی که سازمان مورد نظر بخشی از آن است و پس از تصویب آن نهاد، تعریف و مستند کند.

ضروری است که مدیریت ارشد سازمان منابع لازم را تامین نموده و مسئولیت ایجاد، نگهداشت، آزمون و پیاده‌سازی سامانه جامع مدیریت تنش‌پذیری سازمانی را به‌عهده بگیرد و از آن حمایت کند. این امر تضمین می‌کند که مدیریت و کارکنان در همه سطوح سازمان درک می‌کنند که سامانه مدیریت تنش‌پذیری سازمانی اولویت حیاتی مدیریت ارشد سازمان است. این موضوع نیز دارای اهمیت یکسانی است که مدیریت ارشد

1 - Driver

2 - Nature

رویکرد «از بالا به پایین» را در سامانه مدیریت تنش‌پذیری سازمانی به کار گیرد تا از این طریق، مدیریت در همه سطوح سازمان، پاسخ‌گویی و مسئولیت خود را در برابر اثربخشی و کارایی نگهداشت طرح‌ها، به‌عنوان بخشی از اولویت‌های کلی حاکمیت [سازمان]، درک کند.

بہتر است تیمی برای طرح‌ریزی سامانه مدیریت تنش‌پذیری سازمانی، شامل سرپرستان ارشد همه واحدهای کارکردی سازمان و گروه‌های پشتیبان، شکل بگیرد تا از این طریق پذیرش گسترده سامانه مدیریت تنش‌پذیری سازمانی تضمین شود.

الف-۳ طرح‌ریزی

الف-۳-۱ ارزیابی مخاطرات و تحلیل اثرات

بند ۴-۳-۱ استاندارد، فرآیندی را برای سازمان به‌منظور شناسایی خطرات، تهدیدها، مخاطرات و تاثیرات آن ارائه نموده است تا از این طریق موارد مهم آنها تعیین شده و در اولویت سامانه مدیریت تنش‌پذیری سازمان قرار گیرد.

بہتر است فعالیت‌ها، کارکردها، تعهدات^۱ و فرآیندهای حیاتی شناسایی و مستند شود. به‌عنوان مثال می‌توان از خرید، ساخت، زنجیره تامین، فروش، توزیع، حساب‌های دریافتی، حساب‌های پرداختی، حقوق و دستمزد، فناوری اطلاعات و تحقیق و توسعه نام برد. پس از شناسایی فرآیندها و کارکردهای حیاتی، می‌توان با استفاده از معیارهای ارزیابی، هر یک از آنها را تحلیل نمود. سازمان‌ها ممکن است دسته‌هایی از فعالیت‌ها، محصولات و خدمات را برای شناسایی حیاتی بودن، مخاطرات و اثرات آن‌ها انتخاب کنند.

بہتر است سازمان ارزیابی جامع مخاطرات و تحلیل اثرات را در داخل دامنه سامانه مدیریت تنش‌پذیری سازمانی و با در نظر داشتن ورودی‌ها و خروجی‌ها (مورد انتظار و ناخواسته) و در ارتباط با موضوعات زیر انجام دهد:

الف- فعالیت‌ها، محصولات و خدمات فعلی و مرتبط قبلی؛

ب- فعالیت‌ها، کارکردها، محصولات و خدمات جدید یا در دست تغییر یا برنامه‌ریزی شده؛

پ- ارتباط با ذی‌نفعان؛

ت- تعاملات با محیط‌زیست و جامعه؛

ث- زیرساخت‌های حیاتی.

بہتر است این فرآیند، شرایط عملیاتی عادی و غیرعادی، شرایط روشن و خاموش کردن و همچنین موقعیت‌های اضطراری و انقطاعی قابل پیش‌بینی منطقی را به‌منظور تعیین زمان بازیابی هدف و پاسخ‌گویی به زمان بازیابی در نظر بگیرد.

رویکردها و متدولوژی‌های متعددی برای ارزیابی مخاطرات و تحلیل اثرات وجود دارد که ترتیب گام‌های اقتباس‌شده تحلیل را مشخص می‌کند. صرف نظر از متدولوژی، بہتر است سازمان فرآیند ارزیابی رسمی و

1 - Obligations

مکتوبی برای شناسایی تهدیدها و خطرات و تحلیل مخاطرات، آسیب‌پذیری، حیاتی‌بودن، پیامدها و تاثیرات داشته باشد.

بهبتر است در ارزیابی مخاطرات و تحلیل اثرات نکات زیر مد نظر قرار گیرد:

الف- توجه به میزان حیاتی بودن فعالیت‌ها، کارکردها، محصولات و خدمات سازمان و مخاطرات مرتبط با آنها و قابلیت بالقوه آنها در تاثیر مستقیم یا غیرمستقیم بر عملیات، کارکنان، اموال، دارایی‌ها، جبران خدمت، وجهه و خوشنامی، سود، اعتبار مالی و/یا محیط سازمان.

ب- استفاده از روشگان کمی یا کیفی مستند برای تخمین احتمال وقوع مخاطرات بالقوه شناسایی شده و شدت تاثیر آنها در صورت تحقق.

پ- قراردادن معیارهای منطقی^۱ به‌عنوان مبنای کار. این امر از طریق توجه کافی به کلیه مخاطرات بالقوه‌ای که در مورد عملیات، شناسایی شده است، صورت می‌گیرد.

ت- در نظر گرفتن وابستگی به دیگران و وابستگی آنها به سازمان، از جمله وابستگی‌ها و تعهدات به زیرساخت‌های حیاتی و زنجیره تامین.

ث- در نظر گرفتن یکپارچگی داده‌ها و ارتباطات راه‌دور و امنیت سایبر.

ج- ارزیابی پیامدهای تعهدات قانونی و سایر تعهداتی که بر فعالیت‌های سازمان حاکم است.

چ- در نظر گرفتن مخاطرات مرتبط با ذی‌نفعان، پیمانکاران، تامین‌کنندگان و سایر طرف‌های موثر.

ح- تحلیل اطلاعات مخاطرات و انتخاب آن دسته از مخاطراتی که ممکن است پیامدهای قابل توجهی داشته‌باشند و/یا آن دسته از مخاطراتی که تعیین اهمیت پیامدهای آنها دشوار است.

خ- تحلیل و ارزیابی سطح تنش‌پذیری در برابر هر خطر یا تهدید و هر دارایی حیاتی.

د- ارزیابی مخاطرات و تاثیراتی که قابل کنترل و تاثیرپذیری هستند (البته در تمامی شرایط، این سازمان است که درجه کنترل و راهبردهای خود را برای پذیرش، اجتناب، مدیریت، کمینه کردن، انتقال و/یا

برخورد با مخاطرات تعیین می‌کند.)

ممکن است در بعضی مکان‌ها زیرساخت‌های حیاتی، دارایی‌های اجتماعی و میراث فرهنگی عنصر مهمی از محیط پیرامونی که سازمان در آن فعالیت دارد، باشد و در نتیجه باید در درک تاثیرات آن بر محیط، در نظر گرفته شوند.

از آنجایی که سازمان ممکن است مخاطرات و تاثیرات متعددی داشته باشد، بهتر است معیارها و روشگان برای تشخیص آنهايي که مهم در نظر گرفته خواهند شد تدوین و مستند کند. روش‌های متعددی برای تعیین مخاطرات مهم و تاثیرات آنها وجود دارد. البته هر روشی که استفاده شود بهتر است نتایج یکنواختی تولید کند و شامل ایجاد و کاربرد معیارهای ارزیابی، مانند موارد مرتبط با حیاتی بودن هر فعالیت و کارکرد سازمان، موضوعات قانونی و ملاحظات ذی‌نفعان داخلی و بیرونی باشد. بهتر است سازمان تاثیر توقف‌ها بر

1 - Reasonable

عملیات خود را تحلیل کرده و عملیات حیاتی خود را که بالاترین اولویت را در بازگشتن به حالت عادی دارد شناسایی کند تا بتواند مقادیر هدف مربوط به زمان بازیابی را تعیین نماید.

بهتر است سازمان‌ها هنگام ارزیابی تاثیرات موارد زیر را در نظر بگیرند:

- الف- هزینه نیروی انسانی: صدمات فیزیکی و روانی به کارکنان، مشتریان، تامین‌کنندگان و سایر ذی‌نفعان.
- ب- هزینه مالی: جایگزینی تجهیزات و اموال، زمان کار نکردن^۱، هزینه اضافه‌کاری، افت ارزش ناشی از موجودی انبار، فروش/کسب‌وکار از دست رفته، دعاوی، پرداخت‌ها/جریمه‌های قانونی و غیره.
- پ- هزینه وجهه شرکت: خوشنامی، شهرت در جامعه^۲، فشار منفی^۳، از دست دادن مشتریان و غیره.
- ت- زیان‌های اقتصادی به جامعه‌ای که سازمان در آن کار می‌کند: تاثیر غیرمستقیم بر اقتصاد منطقه‌ای، کاهش حجم خالص اقتصاد منطقه، کاهش میزان مالیات اخذ شده در منطقه و غیره.
- ث- تاثیرات زیست‌محیطی: پایین آمدن کیفیت محیط زیست یا به‌خطر افتادن گونه‌ها^۴.

بهتر است حداکثر مدت زمان قابل قبول برای خارج از خدمت بودن و زمان هدف بازیابی با رعایت موارد زیر تعیین شود:

- الف- تا قبل از اینکه تاثیرات به سطح غیرقابل قبول برسند، فرآیندها چه مدتی می‌توانند غیرعملیاتی باشند.
- ب- زودترین زمان بازگرداندن فرآیندها به حالت عادی چه مقداری است (فرآیندی با کوتاه‌ترین زمان مجاز برای خارج از خدمت بودن، اولین فرآیندی است که به حالت عادی باز می‌گردد).
- پ- مقادیر هدف مختلف زمان‌های بازیابی برای مقاطع مختلف سال (پایان سال، اعلام درآمد مشمول مالیات و غیره)
- ت- شناسایی و مستندسازی رویه‌های جایگزین برای پیمان راهبردی، کمک دوجانبه، راه‌حل‌های موقت غیرخودکار^۵، هشدار/اخطار و غیره.
- ث- ارزیابی هزینه‌های مربوط به رویه‌های جایگزین در مقایسه با حالت انتظار بازگرداندن سامانه به حالت عادی.

بهتر است سازمان هنگام تولید اطلاعات مرتبط با مخاطرات و تاثیرات مهم، نیاز به نگهداری از اطلاعات را برای مقاصد تاریخچه‌ای و همچنین استفاده از آنها در طراحی و پیاده‌سازی سامانه مدیریت تنش‌پذیری سازمانی در نظر بگیرد.

بهتر است محل فعالیت‌ها، زمان و هزینه انجام تحلیل و همچنین در دسترس بودن داده‌های قابل اطمینان در فرآیند شناسایی و ارزیابی مخاطرات و تاثیرات در نظر گرفته شود. اطلاعاتی که قبلاً برای طرح‌ریزی کسب‌وکار، مقررات یا سایر مقاصد تهیه شده است ممکن است در این فرآیند استفاده شود.

1 - downtime
2 - standing in the community
3 - negative press
4 - Species
5 - Manual workaround

انتظار نمی‌رود فرآیند شناسایی و ارزیابی مخاطرات و تاثیرات، تعهدات قانونی سازمان را افزایش یا تغییر دهد.

الف-۳-۲ الزامات قانونی و سایر الزامات

سازمان نیاز دارد که الزامات قانونی که در مورد فعالیت‌ها و کارکردهایش اعمال می‌شود را شناسایی کند. الزامات قانونی می‌تواند شامل موارد زیر باشد:

الف- الزامات قانونی ملی و بین‌المللی؛

ب- الزامات قانونی ایالتی، استانی یا بخشی؛

پ- الزامات قانونی محلی.

مثال‌هایی از سایر الزاماتی که سازمان ممکن است نسبت به آنها متعهد باشد عبارت است از:

الف- توافق‌نامه با مقامات محلی؛

ب- توافق‌نامه با مشتریان؛

پ- رهنمودهای غیر مقرراتی (مثلا فرمان‌دهی یکپارچه/ سامانه فرمان‌دهی رویداد)؛

ت- اصول یا آیین‌کار^۱ داوطلبانه؛

ث- تعهدات برچسب‌گذاری داوطلبانه و مراقبت از محصول؛

ج- الزامات انجمن‌های تجاری؛

چ- توافق‌نامه با گروه‌های اجتماعی و سازمان‌های غیردولتی؛

ح- تعهدات اجتماعی سازمان یا نهاد بالادست آن (سازمان مادر)؛ و/یا

خ- الزامات بنگاهی یا شرکتی.

تعیین نحوه تاثیرگذاری الزامات قانونی و سایر الزامات بر ارزیابی مخاطرات سازمان، در فرآیند شناسایی این الزامات انجام می‌شود. بنابراین ممکن است نیازی نباشد که رویه جداگانه یا اضافه‌ای برای تعیین این موارد وجود داشته باشد.

الف-۳-۳ اهداف سازمانی، اهداف عملکردی و برنامه‌ها

بهتر است اهداف سازمانی و اهداف عملکردی در صورت امکان مشخص و قابل سنجش باشد و جنبه‌های کوتاه‌مدت و درازمدت را پوشش دهد. بهتر است برنامه‌ها، ابزارهای راهبردی را برای دستیابی به اهداف سازمانی و اهداف عملکردی تعریف کنند.

بهتر است اهداف سازمانی، اهداف عملکردی و برنامه‌ها مبتنی بر ارزیابی مخاطرات و تحلیل تاثیرات باشد.

بهتر است سازمان هنگام در نظر گرفتن گزینه‌های فناوری خود، به‌کارگیری بهترین فناوری‌های در دسترس را که از نظر اقتصادی مناسب و مقرون به‌صرفه است و مناسب تشخیص داده شده است، در نظر بگیرد.

1 - Code of practice

اشاره به الزامات مالی سازمان به این معنی نیست که سازمان‌ها مجبورند از متدولوژی‌های حسابداری هزینه‌ها استفاده کنند، هرچند سازمان ممکن است تصمیم بگیرد که هزینه‌های مستقیم، غیرمستقیم و پنهان^۱ را لحاظ کند.

تدوین و استفاده از یک یا چند برنامه برای پیاده‌سازی موفقیت‌آمیز سامانه مدیریت تنش‌پذیری سازمانی اهمیت دارد. بهتر است هر برنامه نحوه دستیابی سازمان به اهداف سازمانی و اهداف عملکردی شامل زمان‌بندی، منابع مورد نیاز و کارکنان مسئول پیاده‌سازی برنامه را توصیف کند. این برنامه ممکن است به اجزایی تقسیم شود تا به عناصر خاصی از عملیات سازمان پردازد.

در صورت امکان و عملی بودن بهتر است برنامه همه مراحل فعالیت‌ها و کارکردهای سازمان که مرتبط با طرح‌ریزی، طراحی، احداث، راه‌اندازی آزمایشی، بهره‌برداری، گسترش، تولید، بازاریابی، امحاء ضایعات و از رده خارج کردن^۲ است را در نظر بگیرد. تدوین برنامه ممکن است برای فعالیت‌ها، محصولات و خدمات فعلی و جدید انجام شود.

بهتر است برنامه‌های پیش‌گیری، آمادگی و تخفیف، جابجایی افراد و اموالی که در معرض مخاطره قرار دارند؛ مکان‌یابی مجدد، گسترش^۳ و پیش‌بینی سامانه‌ها یا تجهیزات حفاظت؛ امنیت اطلاعات، داده‌ها، مستندات و حفاظت سایبر؛ ایجاد رویه‌هایی برای ارتباطات و هشدار تهدید یا خطر؛ افزونگی^۴ یا تکرار کارکنان کلیدی، سامانه‌ها، تجهیزات، اطلاعات، عملیات، یا مواد حیاتی شامل مواردی که از سازمان‌های مشارکت‌کننده تامین می‌شود، را در نظر بگیرند.

بهتر است سازمان واکنش به رویداد و بازیابی آن را طرح‌ریزی کند که در آن فعالیت‌های محوری^۵، تعهدات قراردادی، ضروریات مرتبط با کارکنان و جوامع مجاور، استمرار عملیاتی و بازسازی محیط زیست را در نظر بگیرد. سازمان‌ها در مدیریت بحران رویکردهای متفاوتی دارند. مستقل از رویکرد، سه گام عمومی و مرتبط با یکدیگر در مدیریت واکنش وجود دارد که در صورت وقوع رویداد انقطاعی، نیازمند طرح‌ریزی و پیاده‌سازی پیش‌دستانه است:

الف- واکنش به شرایط اضطراری: اولین واکنش به یک رویداد انقطاعی معمولاً حفاظت از افراد و اموال در برابر صدمات فوری است. واکنش اولیه توسط مدیریت، ممکن است بخشی از اولین اقدام سازمان را تشکیل دهد.

ب- استمرار: برای حصول اطمینان از اینکه سازمان همچنان به اهداف عملیاتی حیاتی خود دست می‌یابد، فرآیندها، کنترل‌ها و منابع در دسترس قرار می‌گیرد.

1 - Hidden
2 - Decommissioning
3 - retrofitting
4 - Redundancy
5 - Core

پ- بازیابی: فرآیندها، منابع و ظرفیت‌های سازمان برای دستیابی سازمان به الزامات عملیاتی جاری مجدداً استقرار می‌یابند. این امر اغلب شامل معرفی بهبودهای قابل توجه سازمانی است که حتی به گستره‌ی تمرکز مجدد بر اهداف راهبردی یا عملیاتی نیز می‌رسد.

الف-۴ پیاده‌سازی و بهره‌برداری (پیاده‌سازی تاکتیکی)

الف-۴-۱ منابع، نقش‌ها، مسئولیت‌ها و اختیارات

پیاده‌سازی موفقیت‌آمیز سامانه مدیریت تنش‌پذیری سازمانی نیازمند تعهد همه افرادی است که برای سازمان یا به‌نماینده‌گی از سازمان کار می‌کنند. بنابراین بهتر است نقش‌ها و مسئولیت‌ها فقط محدود به کارکرد مدیریت مخاطرات در نظر گرفته نشود و می‌تواند سایر حوزه‌های سازمان مانند مدیریت عملیات یا مدیریت کارکنان را علاوه بر مدیریت مخاطرات، امنیت، آمادگی، استمرار و واکنش در بر بگیرد.

بهتر است این تعهد از بالاترین سطح مدیریت آغاز شود. بر این اساس، مدیریت ارشد خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی را برقرار می‌کند و اطمینان حاصل می‌کند که سامانه مدیریت تنش‌پذیری سازمانی پیاده می‌شود. به‌عنوان قسمتی از این تعهد، مدیریت ارشد نماینده ویژه مدیریت را با مسئولیت‌ها و اختیارات تعریف شده برای پیاده‌سازی سامانه مدیریت تنش‌پذیری سازمانی تعیین می‌کند. در سازمان‌های بزرگ یا پیچیده ممکن است بیش از یک نفر به‌عنوان نماینده مدیریت تعیین شود. در بنگاه‌های کوچک یا متوسط، ممکن است یک نفر این کار را انجام دهد.

لازم است که ساختار اداری مناسبی برای پرداختن موثر به مدیریت بحران هنگام وقوع یک رویداد انقطاعی وجود داشته باشد. تعاریف روشنی باید برای ساختار مدیریتی، اختیارات تصمیم‌گیری‌ها و مسئولیت پیاده‌سازی وجود داشته باشد. بهتر است سازمان تیم مدیریت بحران داشته باشد تا واکنش به رویداد یا واقعه را رهبری کند. بهتر است این تیم متشکل از کارکردهایی چون منابع انسانی، فناوری اطلاعات، تسهیلات، امنیت، حقوقی، ارتباطات و روابط عمومی، تولید، انبار و سایر کارکردهای حیاتی پشتیبان کسب‌وکار باشد که همگی زیر نظر مدیریت ارشد یا نمایندگان وی هدایت شوند.

تیم مدیریت بحران می‌تواند با در نظر گرفتن عواملی مانند اندازه و نوع سازمان، تعداد کارکنان، محل و غیره با تعداد لازم از تیم‌های واکنش پشتیبانی شود. بهتر است تیم‌های واکنش طرح‌های واکنش برای پرداختن به جنبه‌های متنوع بحران‌های بالقوه، مانند ارزیابی خسارت، برپاسازی سایت^۱، حقوق و دستمزد، منابع انسانی، فناوری اطلاعات و پشتیبانی‌های اداری، تدوین کنند. بهتر است طرح‌های پاسخ‌گویی با سامانه مدیریت تنش‌پذیری سازمانی سازگار بوده و قسمتی از آن باشند. بهتر است افراد برای عضویت در تیم‌های پاسخ‌گویی بر اساس مهارت‌ها، سطح تعهد و میزان علاقه جذب شوند.

مدیریت باید اطمینان حاصل کند که منابع مناسب برای تضمین ایجاد، پیاده‌سازی و نگهداری سامانه مدیریت تنش‌پذیری سازمانی، تامین شده است. این موضوع نیز اهمیت دارد که نقش‌ها و مسئولیت‌های

1 - site restoration

کلیدی سامانه مدیریت تنش‌پذیری سازمانی به‌خوبی تعریف شده و به اطلاع تمام افرادی که برای سازمان یا به‌نمایندگی از سازمان کار می‌کنند، رسانده شده است.

بهتر است نقش‌ها، مسئولیت‌ها و اختیارات تعریف و مستند شود و برای هماهنگی با ذی‌نفعان بیرونی به اطلاع آنان رسانده شود. این امر شامل تعاملات با پیمانکاران، شرکا، سازمان‌های درگیر در زنجیره تامین، مقامات دولتی (عمومی) و موسسات مالی است.

الف-۴-۲ صلاحیت، آموزش و آگاهی

بهتر است سازمان آگاهی، دانش، ادراک^۱ و مهارت‌های لازم برای همه افرادی که مسئولیت و اختیاراتی برای انجام کارهایی از طرف سازمان را دارند شناسایی کند. این استاندارد چنین می‌گوید:

الف- اهمیت انطباق با خطمشی و رویه‌های سامانه مدیریت تنش‌پذیری سازمانی و الزامات آن؛

ب- خطرات، تهدیدها و مخاطرات مهم و تاثیرات بالفعل یا بالقوه آنها در ارتباط با کار آنها و منافع حاصل از عملکرد فردی بهبودیافته؛

پ- نقش‌ها و مسئولیت‌های مورد نیاز برای دستیابی به انطباق با الزامات سامانه مدیریت تنش‌پذیری سازمانی؛

ت- رویه‌هایی برای پیش‌گیری، بازداشتن، تخفیف دادن، حفاظت از خود، تخلیه، واکنش و بازیابی؛

ث- پیامدهای بالقوه عدول از رویه‌های مشخص شده.

بهتر است برنامه‌های آگاه‌سازی و آموزش برای ذی‌نفعان داخلی و بیرونی سازمان که ممکن است تحت تاثیر رویداد انقطاعی قرار گیرند تهیه شود.

آگاهی، دانش، ادراک و صلاحیت می‌تواند از طریق مهارت‌آموزی، آموزش یا تجربه کاری به‌دست آید یا بهبود یابد.

بهتر است سازمان از پیمانکارانی که از طرف او کار می‌کنند بخواهد که نشان دهد کارکنان او از صلاحیت و/یا آموزش‌های لازم برخوردارند.

بهتر است مدیریت سطح تجربه، صلاحیت و آموزش لازم برای حصول اطمینان از وجود ظرفیت لازم در کارکنان، بخصوص آنهایی که وظایف تخصصی مدیریت تنش‌پذیری سازمانی را انجام می‌دهند، را تعیین کند.

بهتر است همه کارکنان برای انجام مسئولیت‌های فردی خود هنگام وقوع رویداد انقطاعی یا بحران آموزش‌های لازم را دیده باشند. بهتر است آنها همچنین در مورد عناصر کلیدی سامانه مدیریت تنش‌پذیری سازمانی و همچنین طرح‌های واکنش که به طور مستقیم بر آنها تاثیر دارد، توجیه شوند. چنین آموزشی می‌تواند شامل رویه‌هایی برای اقدامات مرتبط با تخفیف، تخلیه، استقرار در پناهگاه^۲، فرآیندهای کنترل

1 - Understanding

2 - Shelter-in-place

اعتبار هنگام ورود برای کارکنان، چیدمان در سایت‌های کاری جایگزین و پاسخ به درخواست‌های رسانه‌ها توسط سازمان باشد.

بهتر است تیم‌های مدیریت بحران و واکنش آموزش‌های لازم مرتبط با مسئولیت‌ها و وظایف خود را که شامل تعامل با اولین پاسخ‌دهندگان و ذی‌نفعان نیز می‌شود، ببینند. فهرست‌های کنترلی اقدامات و اطلاعات حیاتی که باید جمع‌آوری شوند، ابزارهای با ارزشی در فرآیندهای تعلیم و واکنش هستند. بهتر است تیم‌ها در فواصل زمانی منظم (کمینه سالی یک بار) و اعضای جدید هنگام ملحق شدن به تیم، آموزش ببینند. همچنین بهتر است این تیم‌ها در مورد پیش‌گیری از رویدادهایی که می‌توانند به بحران تبدیل شوند نیز آموزش ببینند.

توصیه می‌شود که هر منبع بیرون از سازمان که ممکن است در واکنش دخیل باشد، مانند آتش‌نشانی، پلیس، بهداشت عمومی و فروشندگان شخص ثالث، با بخش‌های مرتبط طرح‌های واکنش آشنا باشد.

الف-۴-۳ ارتباطات و هشدار

ارتباطات داخلی برای حصول اطمینان در مورد پیاده‌سازی اثربخش سامانه مدیریت تنش‌پذیری سازمانی اهمیت دارد. روش‌های ارتباطات داخلی می‌تواند شامل جلسات منظم گروه‌های کاری، خبرنامه‌ها، تابلوهای اعلانات و سایت‌های اینترانت باشد.

بهتر است سازمان‌ها ارتباط با موسسات خدمات عمومی، سازمان‌ها و مقام‌های مسئول در زمینه‌ی اطلاعات حساس، هشدارها، پیش‌گیری، واکنش و بازیابی مرتبط با وقفه‌های بالقوه‌ی شناسایی شده در ارزیابی مخاطرات را شناسایی و برقرار کنند. بهتر است ترتیبات لازم برای اطلاع‌رسانی و هشدار در درون و بیرون سازمان برای شرایط عادی و غیرعادی پیش‌بینی شود.

بهتر است سازمان‌ها رویه‌ای برای دریافت، مستندسازی و پاسخ به ارتباطات ذی‌نفعان و طرف‌های ذی‌علاقه داشته باشند. این رویه می‌تواند شامل گفتگو با طرف‌های ذی‌علاقه و در نظر گرفتن ملاحظات ایشان باشد. در برخی موقعیت‌ها پاسخ به ملاحظات طرف‌های ذی‌علاقه ممکن است شامل اطلاعات درباره‌ی مخاطرات و تاثیرات مرتبط با کارکردها و عملیات سازمان باشد. همچنین بهتر است این رویه‌ها به برقراری ارتباط لازم با سازمان‌های خدمات عمومی در ارتباط با طرح‌ریزی شرایط اضطراری و سایر موضوعات مرتبط پردازند.

سازمان ممکن است بخواهد ارتباطات خود را با در نظر گرفتن تصمیمات اخذ شده برای گروه‌های هدف مرتبط، پیغام‌ها و موضوعات مناسب و رسانه منتخب طرح‌ریزی کند. بهتر است سازمان‌ها هنگام در نظر گرفتن ارتباطات بیرونی در مورد خطرات، تهدیدها، مخاطرات، تاثیرات و رویه‌های کنترلی، دیدگاه‌ها و اطلاعات مورد نیاز تمامی ذی‌نفعان را مد نظر قرار دهند. اگر سازمانی بخواهد در مورد خطرات، تهدیدها، مخاطرات، تاثیرات و رویه‌های کنترلی خود به بیرون از سازمان اطلاع‌رسانی کند، بهتر است برای این کار رویه‌ای داشته باشد. این رویه می‌تواند بر اساس عوامل مختلفی شامل نوع اطلاعاتی که باید ارائه شود، گروه هدف و تک تک شرایط سازمان تغییر کند. روش‌های ارتباطات بیرونی می‌تواند شامل گزارش‌های سالیانه، خبرنامه‌ها، تارنماها، هشدارها و جلسات عمومی باشد.

ارتباطات مؤثر یکی از مهم‌ترین اجزاء مدیریت بحران است. بهتر است ذی‌نفعان داخلی و بیرونی به‌منظور انتقال اطلاعات آماده‌باش، هشدار، بحران و اطلاعات واکنش سازمانی شناسایی شوند. به‌منظور فراهم آوردن بهترین ارتباطات و پیام‌های مناسب برای گروه‌های مختلف، می‌توان مخاطبین را دسته‌بندی نمود. از این طریق پیام‌های مخصوص یک گروه می‌تواند منتشر شود.

طرح‌ریزی از قبل در ارتباطات بسیار حساس است. می‌توان از قبل پیش‌نویس الگوهای پیام‌ها، دست‌نوشته‌ها و بیانیه‌ها را برای تهدیدهای شناسایی شده در ارزیابی مخاطرات تهیه نمود. بهتر است رویه‌هایی برای حصول اطمینان از این که ارتباطات می‌تواند با یک اعلام کوتاه به‌سرعت انجام شود وجود داشته باشد، بخصوص زمانی که از منابعی مانند اینترانت، سایت‌های اینترنتی و خطوط تلفن ویژه^۱ استفاده می‌شود.

بهتر است سازمان فرد مشخصی را به‌عنوان سخنگو معرفی کند (با در نظر گرفتن یک نفر برای جانشینی) که ارتباطات بحران را با رسانه‌ها و دیگران مدیریت و منتشر کند. بهتر است این فرد قبل از بروز بحران آموزش‌های لازم را در مورد ارتباط با رسانه‌ها ببیند. بهتر است همه اطلاعات از یک منبع واحد عبور کند تا اطمینان حاصل شود که پیام‌ها با یکدیگر همخوانی دارند. بهتر است بر این نکته تاکید شود که کارکنان باید به‌سرعت مطلع شوند که تماس‌های رسانه‌ها را به چه سمتی هدایت کنند و این که فقط سخنگوهای مجاز سازمان می‌توانند با رسانه‌ها ارتباط داشته باشند. در بعضی موقعیت‌ها ممکن است وجود یک سخنگوی آموزش‌دیده حاضر در سایت نیز، ضروری باشد.

الف-۴-۴ مستندسازی

بهتر است سطح جزئیات مستندسازی برای توصیف سامانه مدیریت تنش‌پذیری سازمانی و نحوه کارکردن قسمت‌های آن با یکدیگر کفایت داشته باشد و برای دستیابی به اطلاعات تفصیلی بیشتر در مورد اجرای قسمت‌های مشخصی از سامانه مدیریت تنش‌پذیری سازمانی راهنمایی لازم را ارائه دهد. این مستندسازی می‌تواند با مستندسازی سایر سامانه‌های پیاده شده توسط سازمان یکپارچه باشد. لزومی ندارد که مستندات در قالب یک نظام‌نامه باشد.

گستره مستندسازی سامانه تنش‌پذیری سازمان می‌تواند در سازمان‌های مختلف، تحت تاثیر عوامل زیر، متفاوت باشد:

- الف- اندازه و نوع سازمان و فعالیت‌ها، محصولات و خدمات آن؛
- ب- پیچیدگی فرآیندها و تعاملات آنها؛
- پ- صلاحیت کارکنان.

مثال‌هایی از مستندات عبارت است از:

- الف- بیانیه‌های خط‌مشی، اهداف سازمانی و اهداف عملکردی؛

1- Toll-free Hotlines

ب- اطلاعات در مورد مخاطرات و تاثیرات مهم؛

پ- رویه‌ها؛

ت- اطلاعات فرآیندها؛

ث- نمودارهای سازمانی؛

ج- استانداردهای داخلی و بیرونی؛

چ- طرح‌های واکنش در سایت، تخفیف، شرایط اضطراری و بحران؛ و

ح- سوابق.

بهتر است هرگونه تصمیم‌گیری در مورد مستند کردن یک رویه بر مبنای موضوعاتی از قبیل موارد زیر صورت گیرد:

الف- پیامدهای مستند نکردن از جمله پیامدهای مرتبط با دارایی‌های انسانی و فیزیکی و محیط زیست.

ب- نیاز به نشان دادن انطباق با الزامات قانونی و سایر الزاماتی که سازمان در برابر آنها متعهد است.

پ- ضرورت حصول اطمینان از این که فعالیتی به شکل یکنواخت انجام می‌شود.

ت- مزایای مستندسازی که می‌تواند شامل موارد زیر باشد:

- سهولت در پیاده‌سازی از طریق ارتباطات و آموزش.

- سهولت در نگهداشت و تجدیدنظر (اصلاح).

- مخاطره کمتر در مورد ابهام و انحراف.

- قابلیت نمایش و شفافیت.

ث- الزامات استاندارد حاضر.

مستنداتی که از ابتدا برای مقاصد غیر از سامانه مدیریت تنش‌پذیری سازمانی ایجاد شده‌اند می‌توانند به‌عنوان بخشی از این سامانه استفاده شوند و در این حالت لازم است در سامانه به آنها ارجاع داده شود.

الف-۴-۵ کنترل مستندات

هدف بند ۴-۴-۵ این استاندارد حصول اطمینان از این موضوع است که سازمان مستندات خود را به‌روشی که برای پیاده‌سازی سامانه مدیریت تنش‌پذیری سازمانی کفایت می‌کند، ایجاد و نگهداری می‌کند. اما در هر صورت بهتر است تمرکز سازمان بر پیاده‌سازی موثر سامانه مدیریت تنش‌پذیری سازمانی و همچنین بر عملکرد امنیت، آمادگی، واکنش، استمرار و بازیابی باشد، نه بر سامانه پیچیده کنترل مستندات.

بهتر است سازمان‌ها از یکپارچگی مستندات خود اطمینان حاصل کنند. این کار از طریق حصول اطمینان از غیرقابل دستکاری بودن^۱، تهیه نسخه پشتیبان به طریق امن، قابل دسترسی فقط توسط افراد مجاز و حفاظت در برابر آسیب، زوال و از دست رفتن مستندات انجام می‌شود.

1 - Tamperproof

الف-۴-۶ کنترل عملیاتی

بهتر است سازمان آن دسته از عملیات خود را که با مخاطرات مهم شناسایی شده مرتبط است ارزیابی نموده و اطمینان حاصل نماید که آنها به شکلی اجرا می‌شوند که تأثیرات مخرب مرتبط با آنها، در راستای تامین الزامات خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی و برآوردن اهداف سازمانی و اهداف عملکردی آن، تحت کنترل قرار دارد یا کاهش می‌یابد. بهتر است این امر همه بخش‌های عملیات از جمله فعالیت‌های نگهداشت را نیز پوشش دهد.

از آنجایی که این بخش از سامانه مدیریت تنش‌پذیری سازمانی نحوه وارد کردن الزامات سامانه در عملیات روزمره را هدایت می‌کند، نیازمند استفاده از رویه (های) مکتوبی برای کنترل شرایط است. نبود رویه‌های مکتوب می‌تواند به انحراف از خط‌مشی سامانه مدیریت تنش‌پذیری سازمانی و اهداف سازمانی و اهداف عملکردی آن منجر شود.

بهتر است برای کمینه کردن احتمال وقوع یک رویداد انقطاعی، این رویه‌ها به شکل مقتضی شامل کنترل‌هایی برای طراحی، نصب، بهره‌برداری، نوسازی^۱ و اعمال تغییرات روی تجهیزات و ابزاری که مخاطره‌آمیز هستند باشند. هنگامی که ترتیبات موجود اصلاح می‌شود یا ترتیبات جدیدی معرفی می‌شود که می‌تواند بر عملیات و فعالیت‌ها تأثیر بگذارد، بهتر است سازمان قبل از پیاده‌سازی آنها، کمینه کردن تهدیدها و مخاطرات مرتبط با آنها را در نظر بگیرد.

الف-۴-۷ پیش‌گیری، آمادگی و واکنش به رویداد

مسئولیت هر سازمانی است که رویه‌هایی برای پیش‌گیری، آمادگی و واکنش به رویداد، که با نیازهای خاص سازمان تناسب داشته باشد را تدوین کند. توصیه می‌شود سازمان‌ها در تدوین این رویه‌ها ملاحظات زیر را در نظر بگیرند:

الف- بهتر است رویداد انقطاعی بالقوه، شناسایی و درک شده و به آن پرداخته شود تا به این ترتیب بتوان از آن اجتناب یا پیش‌گیری نمود. ارزیابی مخاطرات می‌تواند برای شناسایی مشخصات رویدادهای انقطاعی بالقوه، شامل علائم پیش‌آگهی^۲ و هشدار، استفاده شود.

۱- بهتر است مدیریت مخاطرات، فرآیندی نظام‌مند و کل‌نگر باشد که بر مبنای ارزیابی رسمی مخاطرات برای شناسایی، سنجش، کمی کردن و ارزشیابی مخاطرات به منظور یافتن راه‌حل بهینه شکل گرفته است.

۲- گزینه‌های برخورد با مخاطرات می‌تواند شامل راهبردهای اجتناب، حذف، کاهش، پراکندگی، انتقال و پذیرش باشد. اجتناب و حذف می‌تواند شامل گریز^۳ از فعالیت‌هایی که منجر به ایجاد

1 - Refurbishment

2 - Precursors

3 - Evade

مخاطره می‌شود یا حذف منبع مخاطره باشد. کاهش، مخاطره یا شدت زیان را کم می‌کند. پراکندگی، دارایی‌ها و/یا از دست دادن بالقوه ظرفیت را توزیع می‌کند. انتقال، به معنی شراکت مخاطره با طرف یا طرف‌های دیگر است. پذیرش، تصمیم مبتنی بر آگاهی در مورد قبول یک مخاطره خاص است.

ب- پیش‌گیری می‌تواند شامل گام‌های پیش‌بینانه برای هماهنگی با سازمان‌های اطلاعاتی، انتظامی^۱ و خدمات عمومی؛ ایجاد توافق‌نامه‌های تسهیم اطلاعات؛ حفاظت فیزیکی از دارایی‌های کلیدی؛ کنترل دسترسی‌ها؛ برنامه‌های آگاه‌سازی و آموزش آمادگی؛ سامانه‌های آماده‌باش و هشدار؛ و اقداماتی برای کاهش تهدیدها باشد.

پ- بهتر است فرهنگ سازمانی، برنامه‌های عملیاتی و اهداف مدیریتی، افراد را تشویق کنند تا خود را شخصا در برابر پیش‌گیری، اجتناب، بازداشتن و کشف^۲ مسئول بدانند.

ت- بازداشتن و کشف می‌تواند [وقوع] فعالیت یا اقدام مخربی را که بر ضد سازمان انجام می‌شود، دشوار کند یا تاثیر آن را، اگر نه کاملا، به میزان قابل توجهی محدود کند. استفاده از راهبردهای پیش‌گیرانه، کاشفانه و بازدارنده می‌تواند در حالت‌های زیر اتفاق افتد:

۱- در سطح معماری: موانع طبیعی یا انسان‌ساخت، زیرساخت‌های جابجاشده یا مجددا طراحی شده.

۲- در سطح اجرایی: حذف مواد خطرناک، بازطراحی سامانه‌ها و عملیات، ترتیب کشیک مسئولین امنیت، برنامه‌های آگاه‌سازی کارکنان، نظارت شمارشگر^۳ و اطلاعات آنها برای اجتناب، جانمایی مجدد سامانه‌ها، عملیات، زیرساخت‌ها و کارکنان.

۳- در سطح فناوری: مواد و فرآیندهای جایگزین، شبکه‌های مخابراتی و اطلاعاتی متعامل، کشف نفوذ^۴، کنترل دسترسی‌ها، نظارت ضبط‌شده، بازدید از بسته‌ها و چمدان‌ها و کنترل سامانه‌ها.

ث- طرح‌ریزی حفاظت فیزیکی شامل حفاظت از زمین‌های پیرامونی، ساختمان‌های پیرامونی، حفاظت از فضای داخلی و حفاظت از محتوا است. دفاع از محیط بیرونی آغاز می‌شود.

۱- طرح‌ریزی حفاظت فیزیکی شامل وظایف کشف، تاخیر^۵ و واکنش است.

۲- اقدامات حفاظت فیزیکی بهتر است طوری طراحی شود که امکان کشف در دورترین نقطه ممکن نسبت به هدف فراهم شود. تاخیرها در نقاط نزدیک‌تر به هدف طراحی می‌شود.

۳- طراحی سامانه امنیتی بهتر است ارتباط کشف بیرونی یا داخلی را با ارزیابی و واکنش برقرار کند.

۴- اقدامات حفاظت فیزیکی می‌تواند شامل پیش‌گیری از جرم از طریق طراحی محیطی، موانع فیزیکی و مستحکم‌سازی سایت، کنترل‌های فیزیکی ورود و دسترسی، سامانه روشنایی امنیتی،

1 - Law enforcement
2 - Detection
3 - Counter Surveillance
4 - Intrusion Detection
5 - Delay

سامانه‌ها و هشدارهای کشف نفوذ، تلویزیون‌های مداربسته، کارکنان حراست و خط‌مشی‌ها و رویه‌های امنیتی باشد.

ج- بهتر است راهبردهای تخفیف مقرون به صرفه برای پیش‌گیری یا کاهش تاثیرات بحران‌های بالقوه به خدمت گرفته شود.

- ۱- بهتر است راهبرد تخفیف، اقدامات فوری، میان‌مدت و درازمدت را در نظر بگیرد.
- ۲- بهتر است منابع مختلفی که در فرآیند تخفیف دادن مشارکت دارند شناسایی شوند. بهتر است این منابع، شامل کارکنان کلیدی و نقش‌ها و مسئولیت‌های آنها، تسهیلات، فناوری و تجهیزات، در طرح مستند شوند و به بخشی از کار روزمره تبدیل شوند.
- ۳- بهتر است سامانه‌ها و منابع، به‌عنوان بخشی از راهبردهای مقابله، مدام پایش شوند. چنین پایش‌هایی می‌تواند مشابه کار ساده مدیریت موجودی باشد.
- ۴- بهتر است منابعی که سازمان را در مقابله با بحران پشتیبانی می‌کنند به‌طور مرتب پایش شوند تا اطمینان حاصل شود که در دسترس هستند و می‌توانند مطابق آنچه برای هنگام بحران طراحی شده است، عمل کنند. مثال‌هایی از چنین سامانه‌ها و منابع، بدون آن که محدود به موارد زیر باشد، عبارت است از: تجهیزات شرایط اضطراری، سامانه‌های هشدار و اطفای حریق، منابع و فروشندگان محلی، سایت‌های کاری جایگزین، نقشه‌ها و طرح‌های طبقات، نسخ پشتیبان سامانه، انبار خارج از سایت.

چ- بهتر است سازمان رویه‌هایی را برای تشخیص زمان وقوع خطرهای خاصی که نیازمند سطحی از واکنش است ایجاد کند. یک برنامه قوی برای خط‌مشی‌ها و رویه‌های کشف و اجتناب این فرآیند را پشتیبانی می‌کند.

- ۱- دپارتمان‌ها یا واحدهای خاص به طریقی شکل گرفته‌اند تا علائم هشدار یک بحران قریب‌الوقوع را مشاهده کنند. بهتر است کارکنانی که در این دپارتمان‌ها یا واحدها کار می‌کنند به‌طور مناسبی آموزش‌های لازم را ببینند. بهتر است مسئولیت گزارش‌دهی یک بحران بالقوه (شامل سازوکارهای اعلان) به اطلاع همه کارکنان رسانده شود. هنگامی که ساختار مکتوب گزارش‌دهی وجود داشته باشد و به آنچه کارکنان گزارش می‌دهند، توجه شود، بدنه عمومی کارکنان می‌تواند منبع عالی برای اطلاعات پیش‌بینانه باشد.

ح- به محض تشخیص یک رویداد انقطاعی بالقوه، بهتر است فوراً به یک سرپرست، عضوی از مدیریت یا فرد دیگری که در زمینه اعلان و مدیریت بحران مسئولیت دارد گزارش شود.

- ۱- بهتر است معیار خاصی برای اعلان، تعیین شده و مستند شود و همه کارکنان از آن تبعیت کنند (زمان‌بندی و ترتیب اعلان‌ها به‌طور شفاف مستند شود). لازمه فعال شدن واقعی فرآیند واکنش، برآوردن شرایط بسیار خاصی است.

۲- هنگامی که شرایط یا پارامترهای خاص یک بحران بالقوه حادث می‌شود، بهتر است افراد حائز شرایط به فهرست محرمانه‌ی به‌روزشده‌ای از افراد و سازمان‌هایی که باید با آنها تماس گرفته شود دسترسی داشته باشند.

۳- اعلان‌ها در هنگام بروز بحران بهتر است به‌موقع و شفاف باشد و بهتر است از رویه‌های و فناوری‌های مختلفی استفاده شود (باید به این موضوع که دستگاه‌هایی که استفاده می‌شوند، محاسن و محدودیت‌هایی دارند، توجه کرد).

۴- در بعضی از انواع بحران، خود سامانه‌های اعلان، از طریق مشکلات ظرفیتی یا آسیب زیرساخت‌ها، تحت تاثیر فاجعه قرار می‌گیرند. بنابراین اهمیت دارد که افزونگی برای سامانه اعلان و راه‌های مختلفی برای تماس با افراد و سازمان‌های فهرست‌شده در نظر گرفته شود.

خ- بهتر است *ارزیابی مشکل* (فرآیندی برای تصمیم‌گیری که ماهیت موضوعی که باید به آن پرداخته شود را تعیین می‌کند) و *ارزیابی شدت* (فرآیندی که شدت بحران و هزینه‌های مرتبط با آن را در درازمدت تعیین می‌کند) در آغاز بحران انجام شود. عواملی که باید در نظر گرفته شود عبارت است از: اندازه مشکل، پتانسیل‌های آن برای گسترش و تاثیر احتمالی وضعیت.

د- بهتر است وضعیتی که قرار گرفتن در آن، به اعلام شرایط اضطراری یا بحران منجر می‌شود، به‌روشنی تعریف شده، مستند شود و با پارامترهای خیلی خاص و کنترل شده تطبیق داشته باشد. بهتر است همچنین مسئولیت اعلام یک بحران نیز به‌روشنی تعریف شده و [به فرد مشخصی] تخصیص داده شود. اولین و دومین جانشین فرد مسئول بهتر است معرفی شود. فعالیت‌هایی که اعلام شرایط اضطراری یا بحران، آنها را فعال می‌کند به‌شرح زیر و نه محدود به آن هستند:

۱- اعلان‌های دیگر؛

۲- تخلیه، پناه‌گیری یا جابجایی؛

۳- پروتکل ایمنی؛

۴- فعال‌سازی سایت واکنش و سایت جایگزین؛

۵- تشکیل تیم؛

۶- تکالیف کارکنان و دسترسی به آنها؛

۷- فعال‌سازی قرارداد شرایط اضطراری؛

۸- تغییرات عملیاتی.

ذ- بهتر است برنامه‌های آمادگی و واکنش حول سناریوی «بدترین حالت ممکن»، با درک این موضوع که اندازه پاسخ‌گویی می‌تواند در انطباق با بحران واقعی متناسب شود، تدوین شود.

ر- افراد مهم‌ترین جنبه طرح آمادگی و واکنش هستند. نحوه مدیریت نیروی انسانی سازمان بر موفقیت یا شکست مدیریت رویداد تاثیر می‌گذارد.

۱- بهتر است سامانه‌ای تمهید شود که توسط آن بتوان بلافاصله پس از شروع بحران روی کمک همه کارکنان حساب کرد. این سامانه می‌تواند شامل طیف متنوعی از سامانه‌ها از درخت ساده‌ای از تماس‌های تلفنی گرفته تا سایت تفصیلی تماس با پیمانکاران بیرونی باشد. بهتر است اطلاع تماس دقیق و به‌روز همه کارکنان نگهداری شود. بهتر است پیش‌بینی‌های لازم برای درگیر کردن بخش‌های مرتبط با خدمات مسافرتی سازمان برای کمک به جابجایی کارکنان در سفرهای کاری صورت بگیرد.

۲- بهتر است ترتیبات لازم برای اعلان صدمات و تلفات به بستگان درجه اول [قربانیان] پیش‌بینی شود. در صورت امکان، بهتر است اعلان توسط یکی از مدیران ارشد (توسط خود وی) انجام شود. آموزش‌های لازم بهتر است تامین شود.

۳- بهتر است سازمان در شرایط تلفات و صدمات جدی، برنامه‌ای برای ارتباط با خانواده‌ها داشته باشد. بهتر است نماینده‌ای که برای تماس با خانواده‌ها انتخاب می‌شود غیر از کسی باشد که اعلان را انجام می‌دهد. این نماینده در نقش اولین نقطه تماس بین خانواده و سازمان عمل می‌کند. آموزش‌های جامع برای این نماینده از ضروریات است.

۴- بهتر است در صورت نیاز مشاوره در مورد بحران پیش‌بینی شود. در بسیاری از موارد این مشاوره فراتر از صلاحیت و تجربه برنامه همیاری کارکنان سازمان است (در صورت در دسترس بودن). بهتر است قبل از وضعیت بحران، منابع قابل اطمینان دیگری برای مشاوره شناسایی شود.

۵- بحران ممکن است تبعات مالی بیش از توان سازمان، کارکنانش و خانواده‌های آنان و سایر ذی‌نفعان داشته باشد. بهتر است این موضوع به‌عنوان بخش مهمی از برنامه آمادگی و واکنش در نظر گرفته شود. این امر می‌تواند شامل پشتیبانی مالی از خانواده قربانیان نیز باشد. علاوه بر آن ممکن است موضوعات مالیاتی مطرح باشد که بهتر است پیشاپیش به آن توجه شده و شفاف شود.

۶- بهتر است سامانه حقوق و دستمزد در طول بحران عملیاتی باقی بماند.

ز- تصمیمات لجستیکی^۱ که قبل‌تر اتخاذ می‌شود می‌تواند بر موفقیت یا شکست یک طرح خوب آمادگی و واکنش موثر باشد. موارد زیر از جمله آنها است:

۱- بهتر است مرکز اولیه مدیریت بحران از قبل شناسایی شود. این مرکز، اولین سایتی است که توسط تیم مدیریت بحران و تیم‌های واکنش برای هدایت و سرپرستی فعالیت‌های مدیریت بحران استفاده می‌شود. بهتر است این سایت، منبع برق بدون وقفه (UPS)^۲، رایانه ضروری، امکانات مخابراتی، سامانه گرمایش و تهویه هوا و سایر سامانه‌های پشتیبان را داشته باشد. علاوه بر آن، کالاهای اضطراری بهتر است شناسایی شده و در سایت ذخیره شود.

1 - Logistic

2 - Uninterruptable Power System

۲- در صورتیکه تخصیص یک مرکز خاص مقدور نباشد، بهتر است از وجود مکان معینی که این تیم‌ها بتوانند برای هدایت و سرپرستی فعالیت‌های مدیریت بحران از آن استفاده کنند اطمینان حاصل شود. بهتر است اقدامات مربوط به کنترل دسترسی‌ها پیاده شده و دسترسی به این سایت برای اعضای تیم به صورت ۲۴×۷ فراهم شود.

۳- بهتر است مرکز ثانویه‌ای برای مدیریت بحران شناسایی شود تا اگر مرکز اولیه تحت تاثیر بحران قرار گرفت، بتوان از آن استفاده نمود.

۴- بهتر است سازمان، ایجاد مراکز فرماندهی مجازی برای دسترسی غیرمتمرکز (توزیع شده) به اطلاعات و همچنین دسترسی به ذی‌نفعانی که در نقاط دور و پراکنده قرار دارند را در نظر داشته باشد.

۵- بهتر است سازمان سایت‌های کاری^۱ جایگزین برای ازسرگیری و بازیابی کسب‌وکار شناسایی کند. در صورت نبود سایر تسهیلات شرکت و/یا مناسب نبودن آنها، دسترسی به سایت‌های جایگزین می‌تواند از طریق تامین‌کنندگان مناسب فراهم شود. بهتر است طرح‌ریزی مرتبط با شناسایی و در دسترس بودن سایت‌های کاری جایگزین، در مراحل اولیه فرآیند طرح‌ریزی آمادگی و واکنش انجام شود. بهتر است سایت‌های کاری جایگزین دسترسی کافی به منابع لازم برای ازسرگیری کسب‌وکار را که در تحلیل تاثیرات شناسایی شده‌اند فراهم آورد.

۶- انبار خارج از سایت، راهبرد ارزش‌مندی برای تخفیف است که واکنش سریع به بحران و ازسرگیری یا بازیابی سریع کسب‌وکار را امکان‌پذیر می‌سازد. بهتر است موقعیت انبار خارج از سایت، فاصله مناسبی از تسهیلات اولیه داشته باشد تا احتمال قرار گرفتن تحت تاثیر همان وقایع مشابه وجود نداشته باشد. اقلامی که باید برای انبار خارج از سایت در نظر گرفته شود شامل سوابق حیاتی و مهمی (کاغذی و غیره) است که برای عملیات کسب‌وکار حیاتی است. بهتر است در طرح، رویه‌هایی برای حصول اطمینان از تحویل به موقع اقلام ضروری در انبار خارج از سایت به مرکز مدیریت بحران یا سایت‌های کاری جایگزین پیش‌بینی شود.

ژ- به محض اینکه تیم مدیریت بحران فعال شد، بهتر است میزان خسارت ارزیابی شود. ارزیابی خسارت می‌تواند توسط خود تیم مدیریت بحران یا تیم ویژه ارزیابی خسارت انجام شود. بهتر است مسئولیت مستندسازی همه اتفاقات و پاسخ‌های مرتبط با رویداد، از جمله هزینه‌های مالی، تعیین شود.

۱- در شرایطی که اموال سازمان دچار خسارت فیزیکی شده است، تیم مدیریت بحران یا تیم ویژه ارزیابی خسارت بهتر است به سایت منتقل شوند. این تیم پس از اخذ مجوز ورود به سایت از مقامات ایمنی عمومی، ارزیابی اولیه‌ای از میزان خسارت وارده و مدت زمان احتمالی که تسهیلات قابل استفاده نیستند به عمل می‌آورد.

1 - Worksite

۲- برخی از انواع بحران‌ها خسارت فیزیکی آنی برای تسهیلات و سایت سازمان به‌همراه ندارند. این بحران‌ها شامل انواع بحران کسب‌وکار، نیروی انسانی، فناوری اطلاعات و اجتماعی هستند. در این بحران‌ها، تیم ارزیابی احتمالاً خسارت یا تأثیرات را در حین بروز و توسعه‌ی بحران ارزیابی می‌کند.

س- در صورت نیاز، بهتر است سیاست‌های موجود تامین منابع مالی و بیمه بررسی شود و تامین منابع مالی و پوشش بیمه‌ای اضافی، شناسایی و کسب شود.

۱- بهتر است پارامترهای سیاست‌گذاری، از جمله تایید اولیه فروشندگان مرتبط با واکنش توسط کارگزار بیمه از قبل تعیین شود. در صورت امکان، بهتر است میزان منابع مالی که به تضمین استمرار عملیات کمک می‌کند، در فرآیند طرح‌ریزی تعیین شود.

۲- بهتر است منابع نقدی در محلی ذخیره شود که به‌راحتی در دسترس باشد تا از در دسترس بودن آن هنگام بحران اطمینان حاصل شود. همچنین بهتر است مقداری نقدینگی و اعتبار برای نیازهای تعطیلات آخر هفته و ساعات غیراداری در دسترس باشد.

۳- بهتر است همه هزینه‌های مرتبط با بحران در دوره‌های واکنش و بازایی ثبت شود.

۴- بهتر است با کارگزاران بیمه در زودترین زمان ممکن در دوره بحران، مخصوصاً در شرایطی که دامنه بحران زیاد است و رقابت شدیدی برای منابع وجود دارد، تماس گرفته شود. بهتر است همه سیاست‌های بیمه و اطلاعات تماس، در دسترس تیم مدیریت بحران قرار داشته باشد و به‌شکل مقتضی در محلی خارج از سایت بحران نیز نگهداری شود یا پشتیبان‌گیری شود.

ش- حمل و نقل در زمان بحران می‌تواند یک چالش باشد. اگر امکان‌پذیر باشد بهتر است تمهیدات لازم از قبل، پیش‌بینی شود. حوزه‌هایی که حمل و نقل برای آنها حیاتی است به شرح زیر است ولی محدود به این موارد نمی‌شود:

۱- تخلیه کارکنان (مثلاً از یک سایت ویران شده یا از محل یک تسهیل اقماری در منطقه یا کشور دیگری)؛

۲- انتقال به سایت کاری جایگزین؛

۳- انتقال مایحتاج به سایت یا سایت جایگزین؛

۴- انتقال داده‌های حیاتی به سایت کاری؛

۵- انتقال کارکنانی که نیازهای ویژه دارند.

ص- بهتر است توافق‌نامه با فروشندگان یا ارائه‌دهندگان خدمات حیاتی به‌شکل مقتضی تدوین شود و اطلاعات تماس آنها به‌عنوان بخشی از برنامه آمادگی و واکنش نگهداری شود. این اطلاعات می‌تواند شامل شماره تلفن، نام طرف تماس، شماره مشتری، رمز عبور (که به‌خوبی حفاظت می‌شود) و سایر اطلاعاتی است که فردی که با فرآیند آشنایی ندارد بتواند تماس برقرار کند.

۱- در برخی موارد، مناسب خواهد بود اگر از فروشندگان حیاتی بخواهیم برنامه‌ی آمادگی یا واکنش خود و یا خلاصه‌ای از آن را ارائه نمایند تا توانایی آن‌ها در استمرار ارائه‌ی خدمات و کالاهای ضروری، در صورت وقوع یک بحران گسترده، ارزیابی شود. حداقل، بهتر است در مورد نقش فروشنده یا ارائه‌ی دهنده‌ی خدمت و همچنین توافق‌نامه‌های سطح خدمت (SLA)^۱ پیش از وقوع بحران مذاکره شود.

ض- توافق‌نامه همکاری متقابل منابعی را شناسایی می‌کند که در حین بحران می‌توان آنها را به اشتراک گذاشت یا از سازمان‌های دیگر قرض گرفت، همچنین می‌توان از امکان پشتیبانی متقابل نیز استفاده نمود. این توافق‌نامه‌ها باید از منظر حقوقی خوب تنظیم شده و به شکل مناسبی مستند شده باشند و توسط همه طرف‌های درگیر و نمایندگان منابع قابل اتکا به خوبی درک شده باشند و تعهدی به همکاری وجود داشته باشد.

ط- پیمان‌های راهبردی، شرکایی را برای تحویل شناسایی می‌کند که از طریق آن‌ها وابستگی‌های متعاملی با سایر سازمان‌ها برای تولید و تامین محصولات و خدمات و تسهیم مخاطرات پیدا خواهد کرد.

ظ- پس از اینکه میزان خسارت معلوم شد، بهتر است نیازهای مربوط به بازیابی فرآیندها اولویت‌گذاری شده و زمان‌بندی برای ازسرگیری آنها تعیین و مستند شود. بهتر است در اولویت‌گذاری، حیاتی‌بودن بنیادی فرآیندها و عوامل دیگری مانند ارتباط با سایر فرآیندها، زمان‌بندی‌های حیاتی و الزامات مقرراتی، که در تحلیل تاثیرات شناسایی شده‌اند، در نظر گرفته شود. بهتر است تصمیمات مرتبط با اولویت‌گذاری فرآیندها، شامل تاریخ، زمان و دلایل تصمیمات، مستند و نگهداری شود.

ع- پس از این که فرآیندهایی که باید به حالت عادی برگردند، اولویت‌گذاری شدند، می‌توان ازسرگیری کارها را از طریق فرآیندهایی که بر اساس جدول اولویت‌بندی بازیابی شده‌اند، آغاز نمود. ازسرگیری این فرآیندها، بسته به شرایط بحران، می‌تواند در سایت کاری فعلی یا در سایت کاری جایگزین انجام شود. بهتر است مستندات مربوط به این که چه زمانی فرآیندها از سر گرفته شده‌اند، نگهداری شود.

غ- پس از اینکه فرآیندهای حیاتی از سر گرفته شد، می‌توان به از سرگیری سایر فرآیندها پرداخت. بهتر است هر جا که ممکن بود، تصمیمات اخذ شده در مورد اولویت‌گذاری این فرآیندها و همچنین زمان‌بندی از سرگیری واقعی آنها، به تفصیل از قبل مستند شود.

ف- بهتر است سازمان به دنبال آن باشد که سازمان را به «حالت عادی» برگرداند. اگر برگشت به حالت «عادی» قبل از بحران مقدور نبود، بهتر است حالت «عادی جدیدی» تعریف شود. «حالت عادی جدید»، این انتظار را ایجاد می‌کند که سازمان به مرحله قبلی کار بهره‌ورانه برگردد (در حالی که ممکن است تجدیدساختار و تغییراتی در محیط کار رخ داده باشد). بهتر است هریک از گام‌های این فرآیند و تصمیمات اخذ شده به‌دقت مستند شود.

1 - Service Level Agreement

۱- به‌عنوان یک قاعده^۱، در این نقطه است که یک بحران رسماً «خاتمه یافته» اعلام می‌شود. مستندسازی این تصمیم بسیار اهمیت دارد. می‌توان برای تقویت روحیه کارکنان و اعتماد مشتریان از کنفرانس‌های خبری و ارتباط با رسانه‌های عمومی استفاده نمود.

الف-۵ بررسی

الف-۵-۱ پیش و سنجش

داده‌های جمع‌آوری شده از پیش و سنجش می‌تواند برای شناسایی روندها (الگوها) و کسب اطلاعات، تحلیل شود. دانشی که از این اطلاعات به‌دست می‌آید می‌تواند برای پیاده‌سازی اقدامات اصلاحی و پیش‌گیرانه استفاده شود. بهتر است سنجه‌هایی برای سنجش موفقیت سامانه تنش‌پذیری سازمانی تعریف شود. مشخصه‌های کلیدی، خصیصه‌هایی هستند که سازمان برای تعیین نحوه مدیریت مخاطرات و تاثیرات مهم، دستیابی به اهداف سازمانی و اهداف عملکردی، و بهبود عملکرد امنیت، آمادگی، واکنش، استمرار و بازیابی لازم است آنها را در نظر بگیرد.

هنگامی که حصول اطمینان از اعتبار نتایج ضروری است، بهتر است تجهیزات سنجش، در دوره‌های زمانی منظم یا قبل از استفاده، بر اساس استانداردهای سنجش معتبر ملی و بین‌المللی، کالیبره یا تصدیق شوند. بهتر است در مواردی که چنین استانداردهایی وجود ندارد مبنای کالیبراسیون ثبت شده و سوابق آن نگهداری شود.

الف-۵-۲ ارزیابی انطباق و عملکرد سامانه

الف-۵-۲-۱ ارزیابی انطباق

بهتر است سازمان بتواند نشان دهد که دارای انطباق ارزیابی شده با الزامات قانونی شناسایی شده، شامل مجوزها و گواهینامه‌های مرتبط، است.

سازمان بهتر است بتواند نشان دهد که دارای انطباق ارزیابی شده با سایر الزامات شناسایی شده، که نسبت به آنها تعهد دارد، است.

الف-۵-۲-۲ تمرین و آزمون

بهتر است سناریوهای آزمون با استفاده از وقایعی که در ارزیابی مخاطرات و تحلیل تاثیرات شناسایی شده است طراحی شود.

آزمون می‌تواند تیم‌ها و کارکنان واکنش را در انجام وظایفشان اثربخش‌تر کند، نقش‌ها را شفاف کند و ضعف‌های سامانه مدیریت تنش‌پذیری سازمانی، که بهتر است اصلاح شوند، را آشکار کند. تعهد به آزمون به سامانه مدیریت تنش‌پذیری سازمانی اعتبار و اقتدار می‌بخشد.

1 -Rule

بهتر است اولین گام در آزمون، تعیین اهداف و انتظارات باشد. یک هدف حیاتی آزمون این است که تعیین شود آیا یک فرآیند مشخص واکنش به بحران موثر است یا خیر و چگونه می‌توان آن را بهبود بخشید. اهداف دیگر آزمون می‌تواند شامل موارد زیر باشد:

الف- آزمون ظرفیت (مثلا ظرفیت سامانه تلفنی دریافت تماس یا ارسال تماس)؛

ب- کاهش زمان لازم برای انجام یک کار (مثلا استفاده از چند مته برای کاهش زمان پاسخ‌گویی)؛ و

پ- گسترش آگاهی و دانش به عموم جامعه کارکنان در مورد سامانه مدیریت تنش‌پذیری سازمانی.

بهتر است یافته‌های به‌دست آمده از آزمون‌های قبلی و همچنین رویدادهای واقعی تجربه‌شده در چرخه آزمون سامانه مدیریت تنش‌پذیری سازمانی استفاده شود.

بهتر است مسئولیت‌های آزمون سامانه مدیریت تنش‌پذیری سازمانی به افراد مشخصی محول شود. سازمان‌های بزرگ‌تر ممکن است تیم ویژه‌ای را برای آزمون تشکیل دهند. در صورت نیاز می‌توان از تخصص منابع بیرونی (مشاوران، سازمان‌های محلی خدمات اضطراری و غیره) استفاده نمود.

بهتر است برنامه زمان‌بندی برای تعیین تواتر انجام آزمون طرح‌ها و اجزای آن تهیه شود.

بهتر است دامنه آزمون به تدریج و در طول زمان گسترش یابد. توصیه می‌شود آزمون‌ها در شروع نسبتاً ساده باشند و به تدریج و با پیشبرد فرآیند آزمون، پیچیده‌تر شوند. آزمون‌های اولیه می‌توانند شامل چک‌لیست‌ها، تمرین‌های ساده و عناصر کوچک سامانه مدیریت تنش‌پذیری سازمانی باشند. بهتر است با پیشبرد برنامه‌های آزمون، آزمون‌ها پیچیده‌تر شود تا همه سامانه مدیریت تنش‌پذیری، شامل مشارکت بیرونی توسط سازمان‌های عمومی پاسخ‌گو به ایمنی و شرایط اضطراری را در بر بگیرد.

نقش‌های زیادی وجود دارد که مشارکت‌کنندگان در آزمون می‌توانند آنها را انجام دهند. بهتر است همه مشارکت‌کنندگان نقش‌های خود در تمرین را درک کنند و بهتر است تمرین همه شرکت‌کنندگان را درگیر کند. گروه‌های مختلف سازمان و همچنین گروه‌هایی از بخش عمومی می‌توانند در آزمون‌ها شرکت کنند. به‌عنوان بخشی از تمرین، بهتر است شرکت‌کنندگان مجاز باشند در مورد موضوعات و آموخته‌ها بحث و تبادل نظر کنند.

پس از خاتمه، تمرین‌ها و آزمون‌ها باید با حساسیت ارزیابی شوند. بهتر است ارزیابی شامل این موضوعات ولی محدود به آن‌ها نباشد: ارزیابی میزان دستیابی به اهداف و مقاصد آزمون، اثربخشی مشارکت‌ها، آیا سامانه مدیریت تنش‌پذیری سازمانی در شرایط بحران واقعی مطابق انتظار عمل می‌کند. بهتر است آزمون‌های آتی و همچنین سامانه مدیریت تنش‌پذیری سازمانی در صورت نیاز بر اساس نتایج هر آزمون اصلاح شود.

بهتر است طراحی آزمون‌ها نیز ارزیابی شده و به‌شکل مقتضی تغییر کند. بهتر است آزمون‌ها پویا باشند و تغییرات سامانه مدیریت تنش‌پذیری سازمانی، تغییرات کارکنان، رویدادهای واقعی و نتایج تمرینات قبلی را مد نظر قرار دهند.

بهتر است نتایج تمرین‌ها و آزمون‌ها مستند شود.

الف-۵-۳ عدم انطباق، اقدام اصلاحی و اقدام پیشگیرانه

با توجه به ماهیت عدم انطباق، سازمان می‌تواند برای تدوین رویه‌هایی که با الزامات این استاندارد انطباق داشته باشد، برنامه ساده‌ای با کمینه رسمیت یا فعالیت پیچیده‌تر و درازمدت‌تری را در پیش گیرد. بهتر است مستندسازی با سطح اقدامات تناسب داشته باشد.

الف-۵-۴ کنترل سوابق

سوابق سامانه مدیریت می‌تواند شامل موارد زیر باشد ولی محدود به این موارد نیست:

الف- سوابق انطباق؛

ب- سوابق آموزش؛

پ- سوابق پایش فرآیندها؛

ت- سوابق بازرسی، تعمیر و نگهداری و کالیبراسیون^۱؛

ث- سوابق مرتبط پیمانکاران و تامین‌کنندگان؛

ج- گزارش رویدادها؛

چ- سوابق رویدادها و سوابق آزمون‌های آمادگی در برابر شرایط اضطراری؛

ح- نتایج ممیزی؛

خ- نتایج بازنگری مدیریت؛

د- تصمیمات مرتبط با ارتباطات بیرونی؛

ذ- سوابق مربوط به الزامات قانونی مرتبط؛

ر- سوابق مخاطرات و تاثیرات مهم؛

ز- سوابق جلسات مربوط به سامانه‌های مدیریتی؛

ژ- اطلاعات عملکرد امنیت، آمادگی، واکنش، استمرار و بازیابی؛

س- سوابق انطباق با الزامات قانونی؛

ش- ارتباط با ذی‌نفعان و طرف‌های ذی‌علاقه.

بهتر است به اطلاعات محرمانه توجه خاصی شود.

بهتر است سازمان‌ها یکپارچگی سوابق را از طریق عدم امکان دستکاری، پشتیبان‌گیری امن، دسترسی دادن فقط به افراد مجاز، محافظت در برابر آسیب، زوال و از دست رفتن تضمین کنند.

بهتر است سازمان برای تعیین دوره مناسب نگهداری مستندات با شخصیت حقوقی مناسبی در داخل سازمان مشورت کند و فرآیندهایی را برای انجام اثربخش آن، تدوین، پیاده‌سازی و نگهداری کند.

یادآوری- سوابق تنها منبع شواهد برای نشان دادن انطباق با این استاندارد نیستند.

الف-۵-۵ ممیزی داخلی

ممیزی داخلی سامانه مدیریت تنش‌پذیری سازمانی می‌تواند توسط کارکنان داخل سازمان یا افراد خارج از سازمان که توسط سازمان انتخاب شده‌اند و به نمایندگی از سازمان کار می‌کنند، انجام شود. در هر دو حالت، افرادی که ممیزی را انجام می‌دهند باید صلاحیت داشته و در موقعیتی باشند که بتوانند این کار را با رعایت بی‌طرفی و عینیت انجام دهند. در سازمان‌های کوچک‌تر، استقلال ممیزی می‌تواند با انتخاب ممیز به‌شکلی که مسئولیتی در قبال فعالیت‌هایی که ممیزی می‌شود نداشته باشد، نشان داده شود.

یادآوری- اگر یک سازمان بخواهد ممیزی سامانه مدیریت تنش‌پذیری سازمانی خود را با ممیزی امنیت، ایمنی یا زیست‌محیطی هم‌زمان انجام دهد، بهتر است هدف و دامنه هر یک به‌روشنی تعریف شود.

الف-۶ بازنگری مدیریت

بهتر است بازنگری مدیریت همه دامنه سامانه مدیریت تنش‌پذیری سازمانی را پوشش دهد، هرچند به این معنی نیست که همه عناصر سامانه مدیریت تنش‌پذیری سازمانی لازم است در یک نوبت بازنگری شوند بلکه فرآیند بازنگری مدیریت می‌تواند در طول یک دوره زمانی انجام شود.

بهتر است سامانه مدیریت تنش‌پذیری سازمانی به‌طور منظم بازنگری و ارزیابی شود. بهتر است بازنگری‌ها بر اساس زمان‌بندی از پیش تعیین‌شده انجام شود و مستندات بازنگری بر اساس ضرورت نگهداری شود. عوامل زیر می‌توانند انجام بازنگری را ایجاب کنند، در غیر این صورت بهتر است در اولین بازنگری برنامه‌ریزی شده، بررسی شوند:

الف- *ارزیابی مخاطرات و تحلیل تاثیرات:* بهتر است هر بار پس از انجام ارزیابی مخاطرات برای سازمان، سامانه مدیریت تنش‌پذیری سازمانی بازنگری شود. نتایج ارزیابی مخاطرات و تحلیل تاثیرات می‌تواند برای نشان دادن این که آیا سامانه مدیریت تنش‌پذیری سازمانی همچنان کفایت برخورد با مخاطراتی که سازمان با آن مواجه است را دارد یا نه، مورد استفاده قرار گیرد.

ب- *روندهای بخش یا صنعت:* تحولات مهمی که در بخش/صنعت رخ می‌دهند، منجر به آغاز بازنگری سامانه مدیریت تنش‌پذیری سازمانی می‌شوند. از روندهای کلی در بخش/صنعت و در فنون برنامه‌ریزی استمرار کسب‌وکار یا عملیات می‌توان برای مقاصد ترازیابی^۱ استفاده نمود.

پ- *الزامات مقرراتی:* الزامات مقرراتی جدید ممکن است منجر به بازنگری سامانه مدیریت تنش‌پذیری سازمانی شوند.

ت- *رخ دادن وقایع:* بهتر است در ادامه واکنش به یک رویداد انقطاعی، چه برنامه پاسخ‌گویی فعال شده باشد یا نشده باشد، بازنگری انجام شود. اگر برنامه فعال شده باشد، توصیه می‌شود که در بازنگری، تاریخچه برنامه، نحوه کار کردن آن، دلیل فعال شدن برنامه و غیره در نظر گرفته شود. اگر برنامه اجرا نشده باشد، در بازنگری بهتر است بررسی شود که دلیل آن چه بوده و آیا این تصمیم مناسب بوده است.

1 - Benchmarking

ث- نتایج آزمون و تمرین: بهتر است سامانه مدیریت تنش‌پذیری سازمانی به شکل مقتضی بر اساس نتایج آزمون و تمرین، اصلاح شود.

بهتر است تغییرات در مخاطرات، فعالیت‌ها، کارکردها و عملیات سازمان که بر سامانه مدیریت تنش‌پذیری سازمانی اثرگذار است، در بهبود مستمر و نگهداشت سامانه مدیریت تنش‌پذیری سازمانی منعکس شود. موارد زیر مثال‌هایی از رویه‌ها، سامانه‌ها یا فرآیندهایی است که ممکن است بر برنامه تاثیر بگذارد:

الف- تغییرات خط‌مشی؛

ب- تغییرات خطرات و تهدیدها؛

پ- تغییر در سازمان و فرآیندهای کسب‌وکار آن؛

ت- تغییر در مفروضات ارزیابی مخاطرات و تحلیل تاثیرات؛

ث- تغییرات نیروی انسانی (کارکنان و پیمانکاران)؛

ج- تغییر در تامین‌کنندگان و زنجیره تامین؛

چ- تغییر در فرآیند و فناوری؛

ح- تغییر در نرم‌افزارهای سامانه‌ای و کاربردی؛

خ- آموخته‌های حیاتی ناشی از آزمون؛

د- مشکلاتی که هنگام اجرای واقعی برنامه در یک بحران کشف شده است؛

ذ- تغییرات در محیط بیرونی (کسب‌وکارهای جدید در منطقه، جاده‌های جدید یا تغییر در الگوهای ترافیکی و غیره)؛

ر- سایر مواردی که در بازنگری برنامه اشاره شده و در ارزیابی مخاطرات و تحلیل تاثیرات شناسایی شده است.

پیوست ب
(الزامی)
واژگان

ب-۱

زمان خروج از خدمت قابل قبول

حداکثر زمان سپری شده بین توقف و برپاسازی ظرفیت یا قابلیت عملیاتی مورد نیاز.

ب-۲

سایت جایگزین

مکان کاری، غیر از مکان اولیه، که هنگامی که مکان اولیه در دسترس نیست، استفاده می‌شود.

ب-۳

دارایی

هر چیزی که برای سازمان دارای ارزش است.

ب-۴

ممیز

فرد دارای صلاحیتی که ممیزی را هدایت می‌کند.

ب-۵

بهبود مستمر

فرآیند مکرری که سامانه مدیریت تنش‌پذیری سازمان را به‌منظور بهبود عملکرد کلی مدیریت متناسب با خط‌مشی سامانه مدیریت تنش‌پذیری ارتقا می‌دهد.

ب-۶

اقدام اصلاحی

اقدامی که برای حذف علت ریشه‌ای یک عدم انطباق صورت می‌گیرد.

ب-۷

فعالیت حیاتی

هر کارکرد یا فرآیندی که برای ارائه خدمت یا محصول سازمان، ضروری است.

ب-۸

ارزیابی حساسیت

فرآیندی که برای شناسایی و ارزشیابی نظام‌مند دارایی‌های سازمان، مبتنی بر اهمیت مأموریت یا کارکرد آن، افرادی که در معرض مخاطره قرار دارند، یا تاثیر توقف بر استمرار سازمان، طراحی می‌شود.

ب-۹ انطباق

برآورده ساختن یک الزام.

ب-۱۰ پیامد

تبعات یک رویداد.

یادآوری ۱- ممکن است برای یک رویداد بیش از یک پیامد وجود داشته باشد.

یادآوری ۲- پیامدها می‌توانند مثبت یا منفی باشند.

یادآوری ۳- پیامدها می‌توانند به صورت کمی یا کیفی بیان شوند.

ب-۱۱ استمرار

قابلیت راهبردی و تاکتیکی از قبل تاییدشده سازمان برای طرح‌ریزی و واکنش به شرایط، موقعیت‌ها و رویدادها به منظور تداوم عملیات، در سطح قابل قبول از پیش تعریف شده.

یادآوری ۱- استمرار در این استاندارد ملی، اصطلاح عمومی برای استمرار عملیات و کسب‌وکار به منظور حصول اطمینان از توانایی سازمان در تداوم عملیات، خارج از شرایط عادی عملیاتی است. استمرار، نه تنها برای شرکت‌های انتفاعی، بلکه برای سازمان‌ها با هر ماهیتی مانند غیردولتی، عمومی و دولتی کاربرد دارد.

ب-۱۲ راهبرد استمرار

رویکرد یک سازمان که قصد دارد از استمرار و توانایی در بازگشت به حالت عادی خود، هنگام مواجهه با یک رویداد انقطاعی، شرایط اضطراری، بحران یا سایر موارد مهم، اطمینان حاصل کند.

ب-۱۳ بحران

شرایط ناپایداری که در اثر یک رویداد انقطاعی یا تغییر مهم رخ می‌دهد و نیازمند توجه و اقدام فوری برای حفظ حیات، دارایی‌ها، اموال یا محیط زیست است.

ب-۱۴ مدیریت بحران

فرآیند کلی‌نگر مدیریتی که آثار بالقوه‌ای را شناسایی می‌کند که سازمان را تهدید می‌کند و چارچوبی را برای ایجاد تنش‌پذیری همراه با قابلیت واکنش موثر فراهم می‌کند که از منافع ذی‌نفعان کلیدی، خوشنامی، برند و

فعالیت‌های ایجاد ارزش مراقبت می‌کند و همچنین قابلیت‌های عملیاتی را به شکل موثر به حالت عادی باز می‌گرداند.

یادآوری ۱- مدیریت بحران همچنین شامل مدیریت آمادگی، واکنش تخفیف‌دهنده، و استمرار یا بازگرداندن به حالت عادی در اثر یک رویداد است. همچنین شامل مدیریت کل برنامه از طریق آموزش، تمرین عملیات و بازنگری به منظور حصول اطمینان از این که طرح‌های آمادگی، واکنش یا استمرار به روز هستند، نیز است.

ب-۱۵

تیم مدیریت بحران

گروهی از افراد که مسئول هدایت توسعه و اجرای طرح‌های واکنش و استمرار عملیات هستند، طرح‌هایی که یک انقطاع عملیاتی یا شرایط اضطراری یا بحرانی را تشریح می‌کند و حین فرآیند بازیابی، قبل و بعد از وقوع انقطاع، هدایت و راهنمایی لازم را فراهم می‌کند.

یادآوری ۱- تیم مدیریت بحران ممکن است شامل افرادی از سازمان و همچنین پاسخ‌دهندگان فوری، ذی‌نفعان و سایر طرف‌های ذیربط باشد.

ب-۱۶

حساسیت

دارای اهمیت بنیادی با در نظر گرفتن اهداف و یا دستاوردها.

ب-۱۷

ظرفیت بالقوه آسیب رساندن

ظرفیت بالقوه مضر یک واقعه، قابل پیش‌بینی یا غیرقابل پیش‌بینی، که بر توانایی سازمان در کارکرد موثر تاثیر می‌گذارد، موجب آسیب‌های حیاتی بر زیرساخت‌ها می‌شود، منجر به خسارت‌های اساسی جانی و مالی برای سازمان یا ذی‌نفعان آن می‌شود، یا موجب تاثیر منفی بر خوشنامی یا یکپارچگی سازمان می‌شود.

ب-۱۸

فاجعه

رویدادی که خسارات یا زیان بزرگی به بار می‌آورد.

ب-۱۹

انقطاع

رویدادی که موجب توقف کسب و کار، کارکرد، عملیات یا فرآیندهای عادی می‌شود که ممکن است قابل پیش‌بینی (مانند طوفان‌ها، ناآرامی‌های سیاسی) یا غیرقابل پیش‌بینی (مانند خاموشی سراسری، حمله تروریستی، مشکلات فناوریانه یا زلزله) باشد.

یادآوری ۱- یک انقطاع می‌تواند در اثر عوامل مثبت یا منفی روی دهد که به توقف در کارکرد، عملیات یا فرآیندهای عادی منجر شود.

ب-۲۰ مدرک

اطلاعات و رسانه پشتیبانی کننده آن.

یادآوری ۱- رسانه می تواند کاغذی، مغناطیسی، دیسک رایانه ای الکترونیکی یا نوری، عکس یا نمونه اصلی یا ترکیبی از آنها باشد.

ب-۲۱ اضطرار

واقعه یا رویداد ناگهانی، فوری یا غیرمترقبه که نیازمند اقدام فوری است.

یادآوری ۱- اضطرار معمولا یک رویداد یا شرایط انقطاعی است که اغلب قابل حدس زدن است یا قابلیت آمادگی در برابر آن وجود دارد اما به ندرت دقیقا قابل پیش بینی است.

ب-۲۲ تمرین ها

ارزشیابی برنامه های سامانه مدیریت تنش پذیری، تمرین نقش های اعضای تیم و کارکنان و آزمون بازیابی و استمرار سامانه های سازمانی (مانند فناوری، سامانه تلفن، موضوعات اداری) به منظور نشان دادن صلاحیت و ظرفیت سامانه مدیریت تنش پذیری.

یادآوری ۱- تمرین ها شامل فعالیت هایی است که به منظور آموزش و آماده سازی اعضای تیم و کارکنان برای واکنش مناسب، با هدف دستیابی به بیشترین سطح عملکرد، انجام می شود.

یادآوری ۲- تمرین می تواند فراخوانی رویه های واکنش و استمرار عملیاتی باشد اما اغلب شبیه سازی یک رویداد اعلام شده یا نشده است که نیازمند واکنش و یا استمرار عملیاتی است و شرکت کنندگان در آن به منظور ارزیابی این که چه مشکلی ممکن است قبل از فراخوانی واقعی رخ دهد، نقشی را بازی می کنند.

ب-۲۳ تخلیه

پراکنده سازی سازمان یافته، مرحله ای و نظارت شده افراد از مناطق خطرناک یا مناطقی که ممکن است خطرناک باشند.

ب-۲۴ حادثه

وقوع یا تغییر مجموعه خاصی از شرایط.

یادآوری ۱- ماهیت، احتمال و پیامدهای یک حادثه نمی تواند کاملا شناخته شده باشد.

یادآوری ۲- یک حادثه می تواند یک یا چند اتفاق باشد و می تواند چندین علت داشته باشد.

یادآوری ۳- احتمال مرتبط با یک حادثه می تواند تعیین شود.

یادآوری ۴- یک حادثه می‌تواند مشتمل بر عدم وقوع یک یا چند موقعیت باشد.

یادآوری ۵- حادثه‌ای با یک پیامد، گاهی رویداد خوانده می‌شود.

ب-۲۵

تسهیلات (زیرساخت)

تاسیسات، ماشین‌آلات، تجهیزات، اموال، ساختمان‌ها، خودروها، سامانه‌های اطلاعاتی، تسهیلات حمل‌ونقل و سایر اقلام زیرساختی یا تاسیساتی و سامانه‌های مرتبط که کارکرد یا خدمت کمی و مشخصی دارند.

ب-۲۶

خطر

منبع احتمالی خطر یا شرایطی (فیزیکی یا عملیاتی) که ظرفیت تولید نوع خاصی از تاثیر مخرب را دارد.

ب-۲۷

اثر

پیامد ارزشیابی شده دستاوردی خاص.

ب-۲۸

تحلیل اثر

فرآیند تحلیل همه کارکردهای عملیاتی و تاثیری که یک توقف عملیاتی ممکن است بر روی آنها داشته باشد.

یادآوری ۱- تحلیل اثر شامل تحلیل اثر کسب‌وکار است که به معنی شناسایی دارایی‌ها، کارکردها، فرآیندها و منابع حیاتی کسب‌وکار و همچنین ارزشیابی خرابی یا خسارت وارده به سازمان در نتیجه یک انقطاع (یا تغییر در محیط کسب‌وکار یا عملیات) است. تحلیل اثر این موارد را شناسایی می‌کند: (۱) چگونه زیان یا تغییر، خود را آشکار می‌سازد؛ (۲) چگونه آن درجه از ظرفیت بالقوه ارجاع کار به سطوح بالاتر ناشی از آسیب یا خسارت...؛ (۳) کمینه خدمات و منابع (انسانی، فیزیکی و مالی) مورد نیاز برای اینکه فرآیندهای کسب‌وکار بتوانند به عملیات خود در سطح قابل قبول ادامه دهند؛ (۴) بازه زمانی که فعالیت‌ها، کارکردها و خدمات سازمان باید بازیابی شوند.

ب-۲۹

رویداد

حادثه‌ای که این ظرفیت را دارد که به خسارت‌های غیرملموس یا فیزیکی انسانی، یا انقطاع در عملیات، خدمات یا کارکردهای یک سازمان، منتهی شود و اگر مدیریت نشود می‌تواند به یک اضطرار، بحران یا فاجعه تبدیل شود.

ب-۳۰

یکپارچگی

خاصیت محافظت از دقت و تمامیت دارایی‌ها.

ب-۳۱ ممیزی داخلی

فرآیند نظام‌مند، مستقل و مستند برای به‌دست آوردن شواهد ممیزی و ارزشیابی عینی آن به‌منظور تعیین میزان برآورده شدن معیارهای ممیزی سامانه مدیریت که توسط سازمان مشخص شده است.

یادآوری ۱- در بسیاری از موارد، بخصوص در مورد سازمان‌های کوچک‌تر، استقلال، از طریق نداشتن مسئولیت در حوزه مورد ممیزی، نشان داده می‌شود.

ب-۳۲ طرح مدیریتی

طرحی شفاف و مستند از اقدامات که معمولاً کارکنان کلیدی، منابع، خدمات و اقدامات مورد نیاز برای پیاده‌سازی فرآیند مدیریت رویداد را پوشش می‌دهد.

ب-۳۳ تخفیف دادن

محدود کردن هر پیامد منفی یک رویداد خاص.

ب-۳۴ توافق‌نامه کمک متقابل

توافق از پیش تنظیم شده میان دو یا چند موجودیت به منظور یاری رساندن به طرفین توافق‌نامه.

ب-۳۵ عدم انطباق

عدم برآورده ساختن یک الزام.

ب-۳۶ هدف

قصد کلی که یک سازمان، دستیابی به آن را برای خود تعیین نموده و با خط‌مشی آن سازگار است.

ب-۳۷ سازمان

گروهی از افراد و تسهیلات با چیدمانی از مسئولیت‌ها، اختیارات و ارتباطات.

یادآوری ۱- یک سازمان می‌تواند یک موجودیت دولتی یا عمومی، شرکت، بنگاه، موسسه، خیریه، انجمن یا قسمتی از آنها یا ترکیبی از آنها باشد.

ب-۳۸ مدیریت تنش‌پذیری سازمان

فعالیت‌ها و کارهای نظام‌مند و هماهنگ‌شده که از طریق آنها سازمان، مخاطرات عملیاتی و تهدیدها و اثرات بالقوه مرتبط با آنها را مدیریت می‌کند.

ب-۳۹

طرح مدیریت تنش‌پذیری سازمان

فرآیند حاکمیتی و مدیریتی جاری که توسط مدیریت ارشد پشتیبانی شده؛ منابع لازم برای آن به‌منظور حصول اطمینان از اینکه گام‌های ضروری برای شناسایی اثرات زیان‌های بالقوه انجام می‌شود، تامین می‌شود؛ راهبردها و طرح‌های عملی بازبایی نگهداری می‌شود؛ از استمرار کارکردها/محصولات/خدمات از طریق تمرین، تکرار، آزمون، آموزش، نگهداشت و تضمین، اطمینان حاصل می‌شود.

ب-۴۰

خط‌مشی

تمایلات و جهت‌گیری‌های کلی یک سازمان که به‌شکل رسمی توسط مدیریت ارشد بیان شده است.

ب-۴۱

آمادگی

فعالیت‌ها، برنامه‌ها و سامانه‌هایی که ممکن است پیش از وقوع یک رویداد، تدوین و پیاده‌سازی شود تا برای پشتیبانی و ارتقاء تخفیف دادن، واکنش و بازبایی شرایط انقطاعی، فاجعه و اضطرارها مورد استفاده قرار گیرد.

ب-۴۲

پیشگیری

اقداماتی که سازمان را قادر می‌سازد تا از وقوع یک انقطاع عملیاتی اجتناب نموده، مانع بروز آن شود یا آثار آن را محدود کند.

ب-۴۳

اقدام پیشگیرانه

اقدامی برای حذف یک عدم انطباق بالقوه.

ب-۴۴

پیشگیری از خطرات و تهدیدها

فرآیندها، کارها، فنون، مواد، محصولات، خدمات یا منابعی که برای اجتناب، کاهش یا کنترل خطرات و تهدیدها و هر نوع مخاطرات مرتبط با آنها که به‌منظور کاهش آثار بالقوه آنها استفاده می‌شود.

ب-۴۵

احتمال

درجه‌ای که یک حادثه ممکن است به وقوع بپیوندد.

یادآوری ۱- مطابق بند ۱-۱ استاندارد ISO 3534-1:1993، تعریف ریاضی احتمال را این طور ارائه کرده است «عدد حقیقی بین ۰ تا ۱ که با یک حادثه تصادفی مرتبط است. احتمال می‌تواند به بسامد درازمدت وقوع حادثه یا میزان باور به وقوع یک حادثه مرتبط باشد. برای درجه بالای باور به وقوع، احتمال نزدیک به ۱ در نظر گرفته می‌شود»

یادآوری ۲- به جای احتمال ممکن است از بسامد برای توصیف مخاطره استفاده شود.

یادآوری ۳- میزان باور به احتمال [وقوع] می‌تواند به صورت رسته یا رده انتخاب شود مانند:

- به ندرت/احتمال کم/محتمل/قطعی

- /باور نکردنی/غیرممکن/دور از ذهن/ممکن/محتمل/اقربالوقوع

ب-۴۶

رویه

راه مشخص برای انجام یک فعالیت.

یادآوری - رویه می‌تواند مکتوب باشد یا نباشد.

ب-۴۷

سابقه

سندی که نتایج به دست آمده را بیان می‌کند یا شواهدی را برای فعالیت‌های انجام شده فراهم می‌کند.

ب-۴۸

زمان بازیابی مورد نظر (RTO)^۱

زمان هدف برای به حالت عادی برگرداندن و بازیابی کارکردها یا منابع که بر اساس زمان قابل قبول خارج از خدمت بودن و سطح قابل قبول عملکرد در هنگام بروز انقطاع عملیاتی تعیین می‌شود

ب-۴۹

مخاطره باقی مانده

مخاطره باقی مانده پس از برطرف کردن مخاطره.

ب-۵۰

تنش پذیری

ظرفیت سازگاری یک سازمان در محیط پیچیده و در حال تغییر.

یادآوری ۱- تنش پذیری، توانایی مقاومت یک سازمان در برابر تاثیر پذیرفتن از یک حادثه یا توانایی سازمان در بازگشت به سطح قابل قبول عملکرد در مدت زمان قابل قبول، پس از تاثیر پذیرفتن از یک حادثه است.

یادآوری ۲- تنش پذیری، قابلیت یک سامانه است در حفظ کارکردها و ساختار خود، هنگام مواجهه با تغییر درونی یا بیرونی و فروپاشی موقر در شرایطی که ضروری است.

1 - Recovery Time Objective

ب-۵۱

منابع

هر دارایی (انسانی، فیزیکی، اطلاعات یا غیرمشهود)، تسهیلات، تجهیزات، مواد، محصولات یا ضایعات که دارای ارزش بالقوه است و می‌تواند مورد استفاده قرار گیرد.

ب-۵۲

طرح واکنش

مجموعه مدون رویه‌ها و اطلاعات که برای استفاده هنگام یک رویداد، تدوین و نگهداری می‌شود.

ب-۵۳

برنامه واکنش

طرح، فرآیندها و منابع لازم برای انجام فعالیت‌ها و خدمات ضروری برای حفظ و نگهداری از جان، مال، عملیات و دارایی‌های حیاتی، انجام می‌شوند.

یادآوری - گام‌های واکنش عموماً شامل تشخیص رویداد، هشدار دادن، ارزیابی، تشریح، اجرای طرح، اطلاع‌رسانی و مدیریت منابع است.

ب-۵۴

تیم واکنش

گروهی از افراد که مسئول تدوین، اجرا، تمرین و نگهداری از طرح واکنش، شامل فرآیندها و رویه‌ها، هستند.

ب-۵۵

مخاطره

تاثیر عدم قطعیت بر اهداف.

یادآوری ۱- اثر به معنی انحراف مثبت یا منفی از انتظارات است.

یادآوری ۲- اهداف می‌توانند جنبه‌های متفاوتی داشته باشند مانند مالی، بهداشت و ایمنی و اهداف زیست‌محیطی و می‌توانند سطوح مختلف داشته باشند مانند راهبردی، در سطح سازمان، پروژه، محصول و فرآیند.

یادآوری ۳- مخاطره اغلب از طریق ارجاع به حوادث و پیامدهای بالقوه یا ترکیبی از آنها و نحوه تاثیرگذاری آنها بر دستیابی به اهداف مشخص می‌شود.

یادآوری ۴- مخاطره اغلب بر حسب ترکیبی از پیامدهای یک حادثه یا تغییر در شرایط، و احتمال وقوع آن بیان می‌شود.

ب-۵۶

پذیرش مخاطره

تصمیم اطلاع‌داده شده در مورد گرفتن یک مخاطره خاص.

یادآوری ۱- پذیرش مخاطره می‌تواند بدون برخورد با مخاطره یا در حین فرآیند برخورد با مخاطره اتفاق بیفتد.

یادآوری ۲- پذیرش مخاطره نیز می‌تواند یک فرآیند باشد.

یادآوری ۳- مخاطره پذیرفته شده باید پایش شده و بازنگری شود.

ب-۵۷

تحلیل مخاطره

فرآیند درک ماهیت مخاطره و تعیین سطح مخاطره.

یادآوری - تحلیل مخاطره، مبنایی برای ارزشیابی مخاطره و تصمیم در مورد برخورد با مخاطره فراهم می‌کند.

ب-۵۸

ارزیابی مخاطره

فرآیند کلی شناسایی مخاطره، تحلیل مخاطره و ارزشیابی مخاطره.

یادآوری - ارزیابی مخاطره دربرگیرنده فرآیند شناسایی تهدیدها و آسیب‌پذیری‌های درونی و بیرونی، شناسایی احتمال و تاثیر حادثه‌ای است که از آن تهدیدها و آسیب‌پذیری‌ها برمی‌خیزد، تعریف کارکردهای حیاتی که برای ادامه عملیات سازمان ضروری هستند، تعریف کنترل‌های لازم برای کاهش در معرض قرار گرفتن، و ارزشیابی هزینه‌های این کنترل‌ها است.

ب-۵۹

اطلاع‌رسانی مخاطره

تبادل یا به اشتراک‌گذاری اطلاعات در مورد مخاطره میان تصمیم‌گیران و سایر ذی‌نفعان.

یادآوری - اطلاعات می‌تواند با وجود، ماهیت، شکل، احتمال، جدیت، قابلیت پذیرش، برخورد یا سایر جنبه‌های مخاطره مرتبط باشد.

ب-۶۰

معیار مخاطره

شرایط مرجع که اهمیت مخاطره با آن ارزیابی می‌شود.

یادآوری - معیار مخاطره می‌تواند شامل هزینه و منفعت مرتبط، الزامات قانونی و مقرراتی، جنبه‌های اقتصادی-اجتماعی و زیست‌محیطی، ملاحظات ذی‌نفعان، اولویت‌ها و سایر ورودی‌های ارزیابی باشد

ب-۶۱

مدیریت مخاطره

فعالیت‌های هماهنگ شده برای هدایت و کنترل یک سازمان با در نظر گرفتن مخاطره.

یادآوری - مدیریت مخاطره عموماً شامل ارزیابی مخاطره، برخورد با مخاطره، پذیرش مخاطره و اطلاع‌رسانی مخاطره است.

ب-۶۲

کاهش مخاطره

اقداماتی که برای کم کردن احتمال یا پیامدهای منفی مخاطره یا هر دوی آنها انجام می‌شود.

ب-۶۳

تحمل مخاطره

آمادگی سازمان در تحمل مخاطره بعد از برخورد با مخاطره به منظور دستیابی به اهداف آن.

ب-۶۴

انتقال مخاطره

به اشتراک‌گذاری بار خسارات یا منافع یا آنچه به دست‌آمده ناشی از مخاطره با طرف دیگر.

یادآوری ۱- الزامات قانونی یا مقرراتی می‌توانند انتقال مخاطره خاصی را محدود، ممنوع یا اجباری کنند.

یادآوری ۲- انتقال مخاطره می‌تواند از طریق بیمه یا سایر تفاهم‌نامه‌ها صورت بگیرد.

یادآوری ۳- انتقال مخاطره می‌تواند مخاطره جدید ایجاد کند یا مخاطره موجود را تغییر دهد.

یادآوری ۴- جابجایی منبع مخاطره، انتقال مخاطره محسوب نمی‌شود.

ب-۶۵

برخورد با مخاطره

فرآیند انتخاب و پیاده‌سازی اقدامات برای تغییر در مخاطره.

یادآوری ۱- اصطلاح «برخورد با مخاطره» گاهی به خود اقدامات نیز اطلاق می‌شود.

یادآوری ۲- اقدامات برخورد با مخاطره می‌تواند شامل اجتناب، بهینه‌سازی، انتقال یا مراقبت از مخاطره باشد.

ب-۶۶

امنیت

شرایط محافظت در برابر خطرهای، تهدیدها، مخاطرات یا خسارت.

یادآوری ۱- در حالت عمومی، امنیت، مفهومی شبیه به ایمنی دارد. تمایز میان این دو، تاکید افزوده بر محافظت در برابر خطری است که منشاء بیرونی دارد.

یادآوری ۲- اصطلاح «امنیت» به معنی این است که چیزی نه تنها [در حال حاضر] امن است بلکه [از گذشته] امن بوده است.

ب-۶۷

جنبه‌های امنیتی

آن مشخصه‌های، عناصر یا خواصی که مخاطره بحران‌ها و فجایع عمدی، غیرعمدی و طبیعی، که باعث توقف در محصولات و خدمات، عملیات، دارایی‌های حیاتی و استمرار سازمان و ذی‌نفعان آن می‌شود یا پیامدهایی برای آنها دارد را کاهش می‌دهد.

ب-۶۸
تمرین شبیه‌سازی

آزمونی که تحت شرایطی که تا حد امکان نزدیک به شرایط واقعی است، انجام می‌شود.

ب-۶۹
منبع

هر چیزی که به تنهایی یا در یک ترکیب، دارای توان ذاتی تبدیل شدن به یک مخاطره را دارد.

ب-۷۰
ذی‌نفع (طرف علاقه‌مند)

فرد یا گروهی که علاقه‌ای در مورد عملکرد یا موفقیت یک سازمان دارد.

یادآوری - این اصطلاح شامل فرد یا گروه دارای علاقه در مورد سازمان، فرآیندهای آن و موفقیت‌هایش است، مانند مشتریان، کارفرمایان، شرکا، کارکنان، مالکان، فروشندگان، جامعه محلی، خط اول پاسخ‌دهندگان، سازمان‌های دولتی و تنظیم‌کنندگان مقررات.

ب-۷۱
زنجیره تامین

مجموعه متصل به هم از منابع و فرآیندها که با سفارش خرید مواد اولیه آغاز می‌شود و به تحویل محصولات و خدمات به کاربر نهایی از طریق حالت‌های مختلف انتقال، گسترش می‌یابد. زنجیره تامین ممکن است شامل تامین‌کنندگان، فروشندگان، سازندگان تسهیلات، تامین‌کنندگان خدمات لجستیک، مراکز توزیع داخلی، توزیع‌کنندگان، فروشندگان عمده و سایر موجودیت‌هایی که به کاربر نهایی ختم می‌شود، باشد.

ب-۷۲
هدف عملیاتی

الزام عملکردیِ تفصیلی کاربردپذیر برای یک سازمان (یا بخشی از آن) که از اهداف سازمان گرفته شده و باید برای دستیابی به آن اهداف، تعیین و برآورده سازی شود.

ب-۷۳
آزمودن

فعالیت‌هایی که برای ارزشیابی اثربخشی یا قابلیت یک طرح مرتبط با هدف یا معیار سنجش مشخصی انجام می‌شود. آزمودن معمولاً شامل تمرین‌هایی است که برای حفظ اثربخشی گروه‌ها و کارکنان در انجام وظایف خود و آشکار ساختن ضعف‌ها در طرح‌های آمادگی و واکنش/استمرار/بازیابی طراحی می‌شود.

ب-۷۴

تهدید

علت بالقوه یک رویداد ناخواسته که ممکن است به آسیب رساندن به جان، دارایی‌ها، سامانه یا سازمان، محیط زیست یا جامعه منجر شود.

ب-۷۵

مدیریت ارشد

مدیران عامل، مدیران و متصدیان یک سازمان که می‌توانند تضمین کنند که سامانه‌های مدیریتی اثربخش (شامل سامانه‌های پایش و کنترل مالی) به منظور حفاظت از دارایی‌ها، کسب ظرفیت و خوشنامی سازمان وجود دارند و برقرار هستند.

ب-۷۶

آسیب‌پذیری

خواص ذاتی چیزی که آن را در معرض مخاطره‌ای قرار می‌دهد که ممکن است پیامدهایی داشته باشد.

ب-۷۷

ارزیابی آسیب‌پذیری

فرآیند شناسایی و کمی کردن آسیب‌پذیری‌ها.