استاندارد ملی ایران
۱۱۳۱۱
چاپ اول
۱۳۹۹

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO
11311
1st. Edition
2021

Identical with
ISO 22301:
2019

امنیت و تاب‌آوری- سیستم‌های مدیریت تداوم کسب و کار- الزامات

Security and resilience- Business continuity management systems- Requirements

ICS: 03.100.01; 03.100.70

استاندارد ملی ایران شمارهٔ ۱۱۳۱۱ (چاپ اول): ۱۳۹۹

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج – ایران

تلفن: ۸-۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.gov.ir

وبگاه: http: //www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No. 2592 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.gov.ir

Website: http: //www.isiri.gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذینفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«امنیت و تاب‌آوری- سیستم‌های مدیریت تداوم کسب و کار- الزامات»

رئیس:	**سمت و/یا محل اشتغال**
سازور، زینب (دکتری مهندسی صنایع)	عضو هیئت علمی- دانشگاه تهران
دبیر:	
وحدانی، محمود (کارشناسی ارشد مهندسی صنایع- صنایع)	اداره کل استاندارد خراسان شمالی
اعضا: (اسامی به ترتیب حروف الفبا)	
امینی، اسماعیل (کارشناسی ارشد مهندسی صنایع)	رئیس گروه سنجش نرخ کیفیت کالاها- سازمان ملی استاندارد ایران
حسنی، مجتبی (کارشناسی علوم اجتماعی)	رئیس گروه طرح و اجرای اداره کل پدافند غیرعامل- استانداری خراسان شمالی
شکرخدایی، فرشید (دکتری مدیریت کسب و کار)	نائب رئیس- انجمن مدیریت کیفیت ایران
کریمی، حسین (دکتری مهندسی صنایع)	عضو هیئت علمی- دانشگاه بجنورد
محقی، حمیدرضا (دکتری مهندسی صنایع)	عضو هیئت علمی- دانشگاه بجنورد
مدرس صادقی، محمد (دکتری مدیریت کسب و کار)	دبیر کارگروه توسعه استانداردهای سیستم‌های مدیریت- انجمن مدیریت کیفیت ایران
نقدی‌پور، الهام (کارشناسی ارشد شیمی کاربردی)	عضو مستقل
ویراستار:	**سمت و/ یا محل اشتغال**
کرمی، زهرا (کارشناسی ارشد مهندسی صنایع)	سازمان ملی استاندارد ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «امنیت و تاب‌آوری- سیستم‌های مدیریت تداوم کسب و کار- الزامات» که پیش‌نویس آن در کمسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی/ منطقه‌ای به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، در دویست و شصت و یکمین اجلاسیه کمیتهٔ ملی استاندارد مدیریت کیفیت مورخ ۱۳۹۹/۱۰/۳۰ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی درزمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین‌شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO 22301: 2019, Security and resilience – Business continuity management systems – Requirements

۰ مقدمه

۰-۱ کلیات

این استاندارد ساختار و الزامات مورد نیاز جهت پیاده سازی و حفظ یک سیستم مدیریت تداوم کسب و کار (BCMS)[1] را مشخص می‌کند که متناسب با میزان و نوع تاثیری که سازمان ممکن است پس از ایجاد اختلال بپذیرد یا نپذیرد، تداوم کسب و کار را ایجاد می‌کند.

نتایج حفظ یک BCMS توسط قوانین و مقررات سازمان، الزامات صنعتی و سازمانی، محصولات و خدمات ارائه شده، فرایندهای به کار گرفته شده، اندازه و ساختار سازمان و الزامات طرف‌های ذینفع آن شکل می‌گیرند.

یک BCMS بر اهمیت موارد زیر تأکید می‌کند:

- درک نیازهای سازمان و ضرورت ایجاد خط‌مشی‌ها و اهداف تداوم کسب و کار؛
- فرایندهای عملیاتی و نگهداری، قابلیت‌ها و ساختارهای واکنشی برای اطمینان از حفظ سازمان در برابر اختلالات؛
- پایش و بررسی عملکرد و اثربخشی BCMS ؛
- بهبود مداوم بر اساس معیارهای کمی و کیفی.

یک BCMS، مانند هر سیستم مدیریتی دیگر، شامل اجزای زیر است:

الف- یک خط‌مشی؛

ب- افراد شایسته با مسئولیت‌های تعریف شده؛

پ- فرآیندهای مدیریتی مرتبط با:

۱- خط‌مشی؛

۲- طرح‌ریزی؛

۳- پیاده‌سازی و اجرا؛

۴- ارزشیابی عملکرد؛

۵- بازنگری مدیریت؛

۶- بهبود مداوم؛

1- Business Continuity Management System

ت- اطلاعات مدونی که از کنترل عملیات پشتیبانی نموده و ارزیابی عملکرد را مقدور سازد.

۰-۲ مزایای یک سیستم مدیریت تداوم کسب و کار

هدف از یک BCMS آمادگی، ایجاد و حفظِ کنترل‌ها و قابلیت‌هایی برای مدیریتِ توانایی کلی یک سازمان جهت ادامه فعالیت در هنگام بروز اختلالات می‌باشد. در دستیابی به این هدف، سازمان:

الف- از دیدگاه تجاری:

۱- از اهداف استراتژیک خود پشتیبانی می‌نماید؛

۲- یک مزیت رقابتی ایجاد می‌نماید؛

۳- شهرت و اعتبار خود را حفظ و افزایش می‌دهد؛

۴- به تاب‌آوری سازمانی کمک می‌نماید؛

ب- از دیدگاه مالی:

۱- آسیب‌پذیری حقوقی و مالی را کاهش می‌دهد؛

۲- هزینه‌های مستقیم و غیر مستقیم اختلالات را کاهش می‌دهد؛

پ- از دیدگاه طرف‌های ذینفع:

۱- از زندگی، دارایی و محیط زیست محافظت می‌نماید؛

۲- انتظارات طرف‌های ذینفع را در نظر می‌گیرد؛

۳- اطمینان خاطری به توانایی سازمان جهت رسیدن به موفقیت ایجاد می‌کند؛

ت- از دیدگاه فرآیندهای داخلی:

۱- توانایی خود جهت اثربخش ماندن در هنگام اختلالات را بهبود می‌بخشد؛

۲- کنترل پیشگویانه از خطرات را به طور کارا و اثربخش به تصویر می‌کشد؛

۳- آسیب پذیری‌های عملیاتی را رفع می‌نماید.

۰-۳ چرخه‌ی «طرح‌ریزی- اجرا- بررسی- اقدام» (PDCA)[1]

این استاندارد جهت پیاده‌سازی، حفظ و بهبود مداومِ اثربخشیِ BCMS در یک سازمان از چرخه‌ی طرح-ریزی (ایجاد)- اجرا (پیاده سازی و بهره‌برداری)- بررسی (نظارت و ارزیابی) و اقدام (حفظ و بهبود) یا PDCA استفاده می‌نماید.

این موضوع از سازگاری این استاندارد با سایر استانداردهای سیستم‌های مدیریت مانند ISO 9001، ISO14001، ISO/IEC 20000-1، ISO/IEC 27001 و ISO 28000 اطمینان ایجاد می‌نماید، بنابراین از پیاده‌سازی و اجرا به صورت سازگار و یکپارچه با سایر سیستم‌های مدیریتی، پشتیبانی می‌کند.

مطابق با چرخه‌ی PDCA ، بندهای ۴ تا ۱۰ این استاندارد موارد زیر را پوشش می‌دهد:

- بند ۴ الزامات ضروری برای ایجاد محیط BCMS جهت به کارگیری در سازمان و همچنین نیازها، الزامات و دامنه را معرفی می کند.

- بند ۵ الزامات مربوط به نقش مدیریت ارشد در BCMS و نحوه بیان انتظارات راهبری به سازمان از طریق بیانیه خط‌مشی را به صورت خلاصه معرفی می‌کند.

- بند ۶ الزامات تعیین اهداف استراتژیک و اصول راهنما برای BCMS را به صورت یک کل توصیف می کند.

- بند ۷ از عملیات BCMS مرتبط با تعیین شایستگی و برقراری ارتباط با طرف‌های ذینفع، در صورت نیاز به صورت مکرر، پشتیبانی می کند و در عین حال اطلاعات مدون مورد نیاز را مستندسازی، کنترل، نگهداری و حفظ می‌کند.

- بند ۸ نیازهای تداوم کسب و کار را تعریف کرده، نحوه‌ی پرداختن به آن‌ها را تعیین می‌کند و روش‌هایی را برای مدیریت سازمان در هنگام ایجاد یک اختلال تکوین می‌نماید.

- بند ۹ به صورت خلاصه الزامات ضروری برای سنجش عملکرد تداوم کسب و کار ، مطابقت BCMS با این استاندارد و اجرای بازنگری مدیریت را بیان می‌کند.

- بند ۱۰ به شناسایی عدم انطباق‌های BCMS و ایجاد بهبود مداوم از طریق اقدامات اصلاحی می‌پردازد.

۰-۴ محتویات این استاندارد

این استاندارد با الزامات ISO برای استانداردهای سیستم مدیریت مطابقت دارد. این الزامات شامل یک ساختار سطح بالا، متن اصلی یکسان و اصطلاحات رایج با تعاریف محوری می‌باشد که جهت بهره‌مندی کاربران از پیاده‌سازی چند استاندارد سیستم مدیریت ISO طراحی شده است.

1- Plan- Do- Check- Act

این استاندارد شامل الزامات خاص سایر سیستم‌های مدیریت نمی‌باشد، اگر چه اجزاء آن می‌توانند با سایر سیستم‌های مدیریت همسو یا یکپارچه شوند.

این استاندارد شامل الزاماتی است که می‌تواند توسط یک سازمان جهت اجرای BCMS و ارزیابی انطباق آن مورد استفاده قرار گیرد. سازمانی که مایل است انطباق خود با این استاندارد را ثابت کند، می تواند از طریق روش‌های زیر این کار را انجام دهد:

- انجام یک خود ارزیابی و خود اظهاری ؛ یا

- ارزیابی انطباق خود توسط طرف‌های ذینفع سازمان، مانند مشتریان؛ یا

- بررسی انطباق خود اظهاری سازمان توسط یک طرف خارج از سازمان؛ یا

- گواهی کردن/ ثبت کردن BCMS خود، توسط یک سازمان خارجی.

بندهای ۱ تا ۳ این استاندارد، هدف و دامنه کاربرد، مراجع الزامی و اصطلاحات و تعاریف مورد استفاده در این استاندارد را شامل می‌شوند. بندهای ۴ تا ۱۰ شامل الزاماتی است که برای ارزیابی انطباق با این استاندارد بایستی به کار گرفته شوند.

در این استاندارد فعل‌های وجهی با معانی زیر به کار می‌رود. معادل این افعال به زبان انگلیسی در داخل دو کمان پس از افعال فارسی قید شده است

- فعل وجهی «باید» (shall) بیانگر «الزام» است.

- فعل وجهی «بایستی» (should) بیانگر «توصیه» است.

- فعل وجهی «ممکن است» (may) بیانگر «اجازه» است.

- فعل وجهی «می‌تواند» (can) بیانگر «امکان یا توانایی» است.

اطلاعاتی که تحت عنوان «یادآوری» داده شده است برای ارائه راهنمایی در خصوص درک و روشن ساختن الزامات مرتبط می‌باشد.

امنیت و تاب‌آوری- سیستم‌های مدیریت تداوم کسب و کار- الزامات

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزامات جهت پیاده‌سازی، حفظ و بهبود یک سیستم مدیریت به منظور محافظت، کاهش احتمال وقوع، آمادگی، واکنش و بازیابی در هنگام بروز اختلالات می‌باشد.

الزامات مشخص شده در این استاندارد عمومی بوده و قصد بر آن است که برای تمامی سازمانها یا بخش‌های آن صرف نظر از نوع، اندازه و ماهیت آن قابل اعمال باشد. میزان کاربرد این الزامات به محیط عملیاتی و پیچیدگی سازمان بستگی دارد.

این استاندارد قابل اعمال برای تمام انواع و اندازه‌های سازمان‌هایی هستند که:

الف- یک BCMS را پیاده‌سازی نموده، حفظ و بهبود می‌دهند؛

ب- به دنبال حصول اطمینان از انطباق با خط‌مشی تداوم کسب و کار اظهار شده خود می‌باشند؛

پ- نیاز دارند در هنگام بروز یک اختلال بتوانند به ارائه‌ی محصول و خدمات خود در یک سطح پیش تعریف شده‌ی قابل قبول ادامه دهند؛

ت- به دنبال افزایش تاب‌آوری خود از طریق بکارگیری موثر BCMS هستند.

این استاندارد می‌تواند برای ارزیابی توانایی یک سازمان در تأمین نیازها و تعهدات تداوم کسب و کار خود مورد استفاده قرار گیرد.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده‌شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

ISO 22300, Security and resilience - vocabulary.

یادآوری- استاندارد ملی ایران شماره ۱۹۱۸۲: سال ۱۳۹۳، امنیتِ جامِعِگی- واژه‌نامه، با استفاده از استاندارد ISO22300:2012 تدوین شده است.

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف ارائه شده در استاندارد ISO 22300، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

فعالیت

activity

مجموعه‌ای از یک یا چند وظیفه با یک خروجی تعریف شده

[منبع: برگرفته از زیربند ۳-۱، استاندارد ISO 22300: 2018، تغییرات: تعریف جایگزین و مثال حذف شده است.]

۳-۲

ممیزی

audit

فرایندی (۳-۲۶) نظام‌یافته، مستقل و مدون برای بدست آوردن شواهد عینی و ارزیابی آن به صورت عینی برای تعیین میزانی که معیارهای ممیزی برآورده می‌شوند.

یادآوری ۱- یک ممیزی می‌تواند یک ممیزی داخلی (شخص اول) یا یک ممیزی خارجی (شخص دوم یا سوم) باشد و همچنین ممیزی می‌تواند یک ممیزی ترکیبی (ترکیبی از دو یا چند رشته تخصصی) باشد.

یادآوری ۲- یک ممیزی داخلی توسط خود *سازمان* (۳-۲۱) یا توسط یک طرف خارجی و از جانب سازمان انجام می‌گیرد.

یادآوری ۳- «شواهد عینی» و «معیارهای ممیزی» در استاندارد ISO 19011 تعریف شده‌اند.

یادآوری ۴- عناصر اصلی ممیزی شامل تعیین *انطباق* (۳-۷) یک مورد بر طبق یک روش اجرایی می‌باشد که توسط کارکنانی که در خصوص مورد ممیزی شده مسئولیت ندارند، انجام می‌شود.

یادآوری ۵- یک ممیزی داخلی می‌تواند برای یازنگری مدیریت و یا سایر اهداف داخلی انجام شود و می‌تواند مبنایی برای اظهار سازمان در مورد انطباق به وجود آورد. مستقل بودن از طریق نداشتن مسئولیت در مورد *فعالیت* (۳-۱) تحت ممیزی می‌تواند به اثبات برسد. ممیزی‌های خارجی شامل ممیزی‌های شخص دوم و سوم می‌باشد. ممیزی‌های شخص دوم توسط طرف‌هایی که منافعی در سازمان دارند، انجام می‌شود مانند مشتریان یا اشخاص دیگر از جانب آن‌ها. ممیزی‌های شخص سوم توسط سازمان‌های ممیزی‌کننده مستقل بیرونی انجام می‌شود مانند آن‌هایی که ارائه‌دهنده خدمات گواهی‌کردن/ ثبت کردن انطباق یا سازمان‌های دولتی هستند.

یادآوری ۶ – این اصطلاح یکی از اصطلاحات مشترک و تعاریف اصلی از ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد. تعریف اصلی با اضافه کردن یادآوری‌های ۴ و ۵ تغییر یافته است.

۳-۳

تداوم کسب و کار

business continuity

توانایی یک *سازمان* (۳-۲۱) برای تداوم ارائه‌ی *محصولات و خدمات* (۳-۲۷) در هنگام بروز یک اختلال در درون چهارچوب‌های زمانی قابل قبول و در یک ظرفیت از پیش تعریف شده

[منبع: برگرفته از زیربند ۳-۲۴، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین شده است.]

۳-۴

طرح تداوم کسب و کار

business continuity plan

اطلاعات مدونی (۳-۱۱) که یک *سازمان* (۳-۲۱) را جهت واکنش‌دهی به یک *اختلال* (۳-۱۰) و از سرگیری، بازیابی و اعاده‌ی ارائه‌ی *محصولات و خدمات* (۳-۲۷) مطابق با *اهداف* (۳-۲۰) *تداوم کسب و کار* (۳-۳) خود، راهنمایی می‌کند.

[منبع: برگرفته از زیربند ۳-۲۷، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین شده است و یادآوری ۱ حذف شده است.]

۳-۵

تحلیل تأثیر کسب و کار

business impact analysis

فرایند (۳-۲۶) تجزیه و تحلیل *اثرگذاری* (۳-۱۳) یک *اختلال* (۳-۱۰) بر روی *سازمان* (۳-۲۱) در طول زمان

یادآوری- خروجی یک بیانیه و توضیحات توجیهی برای *الزامات* (۳-۲۸) *تداوم کسب و کار* (۳-۳) می‌باشد.

[منبع: برگرفته از زیربند ۳-۲۹، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین شده است و یادآوری ۱ حذف شده است.]

۳-۶

شایستگی

competence

توانایی به‌کارگیری دانش و مهارت‌ها برای بدست آوردن نتایج مورد نظر

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۷

انطباق

conformity

برآورده شدن یک *الزام* (۳-۲۸)

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۸

بهبود مداوم

continual improvement

فعالیتی (۳-۱) تکرار شونده برای ارتقای *عملکرد* (۳-۲۳)

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۹

اقدام اصلاحی

corrective action

اقدامی برای از بین بردن علت (های) یک عدم انطباق (۳-۱۹) و جلوگیری از بروز مجدد آن

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۱۰

اختلال

disruption

یک *رخداد* (۳-۱۴) پیش‌بینی شده یا پیش‌بینی نشده که منجر به یک انحراف برنامه‌ریزی نشده و منفی از ارائه‌ی *محصولات و خدمات* (۳-۲۷) مورد انتظارِ مطابق با *اهداف* (۳-۲۰) *سازمان* (۳-۲۱) می‌شود

[منبع: برگرفته از زیربند ۳-۷۰، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین شده است.]

۳-۱۱

اطلاعات مدون

documented information

اطلاعات و واسط حاوی آن که لازم است توسط *سازمان* (۳-۲۱) کنترل و نگهداری شود.

یادآوری ۱- اطلاعات مدون می‌تواند در هر شکل و واسط و از هر منبعی باشد.

یادآوری ۲- اطلاعات مدون می‌تواند اشاره به موارد زیر داشته باشد:

- *سیستم مدیریت* (۳-۱۶) شامل *فرایندهای* (۳-۲۶) مرتبط؛
- اطلاعات ایجاد شده به منظور فعالیت سازمان (مستندات)؛
- شواهد مربوط به نتایج بدست آمده (سوابق).

یادآوری ۳- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۱۲

اثربخشی

effectiveness

میزانی که فعالیت‌های طرح‌ریزی شده تحقق یافته‌اند و نتایج طرح‌ریزی شده بدست آمده است

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۱۳

اثرگذاری

impact

خروجی یک *اختلال* (۳-۱۰) که *اهداف* (۳-۲۰) را تحت تأثیر قرار می‌دهد

۳-۱۴

رخداد

incident

رویدادی که می‌تواند یک اختلال، خسارت، اضطرار یا بحران باشد یا می‌توانست منجر به آن شود

[منبع: برگرفته از زیربند ۳-۱۱۱، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین شده است.]

۳-۱۵

طرف ذینفع (اصطلاح ترجیح داده شده)

interested party (preferred term)

ذینفع (اصطلاح پذیرفته شده)

stakeholder (admitted term)

شخص یا سازمانی که می‌تواند بر یک تصمیم یا فعالیت تأثیر گذارد، یا از آن تأثیر پذیرد، یا خود را متأثر از آن بداند

مثال: مشتریان، مالکان، کارکنان، تأمین‌کنندگان، بانکداران، سازمان‌های تنظیم‌کننده‌ی مقررات، اتحادیه‌ها، شرکاء یا جامعه‌ای که می‌تواند شامل رقبا یا گروه‌های مخالفت‌کننده باشد.

یادآوری ۱- یک تصمیم‌گیرنده می‌تواند یک طرف ذینفع باشد.

یادآوری ۲- انجمن‌های تحت تأثیر و جمعیت‌های محلی به عنوان طرف‌های ذینفع در نظر گرفته می‌شوند.

یادآوری ۳- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد. تعریف اصلی با اضافه کردن یک مثال و یادآوری‌های ۱ و ۲ تغییر یافته است.

۳-۱۶

سیستم مدیریت

management system

مجموعه‌ای از اجزای مرتبط به هم یا متعامل یک *سازمان* (۳-۲۱) برای تعیین *خط‌مشی‌ها* (۳-۲۴) و *اهداف* (۳-۲۰) و *فرایندهایی* (۳-۲۶) برای دستیابی به آن اهداف

یادآوری ۱- یک سیستم مدیریت می‌تواند به یک یا چند نظام بپردازد.

یادآوری ۲- اجزای سیستم مدیریت شامل ساختار سازمان، نقش‌ها و مسئولیت‌ها، طرح‌ریزی و عملیات می‌باشد.

یادآوری ۳- دامنه شمول یک سیستم مدیریت می‌تواند کلّ سازمان، حوزه‌های کاری خاص و معینی از سازمان، بخش‌های خاص و معینی از سازمان، یا یک یا چند حوزه کاری در میان یک گروه از سازمان‌ها را شامل گردد.

یادآوری ۴- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۱۷

اندازه‌گیری

measurement

فرایند (۳-۲۶) تعیین یک مقدار

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۱۸

پایش

monitoring

تعیین وضعیت یک سیستم، یک *فرایند* (۳-۲۶) یا یک *فعالیت* (۳-۱)

یادآوری ۱- برای تعیین وضعیت می‌تواند نیاز به بررسی، نظارت، یا مشاهده با دقت باشد.

یادآوری ۲- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۱۹

عدم‌انطباق

nonconformity

برآورده نشدن یک *الزام* (۳-۲۸)

یادآوری ۱- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۲۰

هدف

objective

نتیجه‌ای که قرار است بدست آید

یادآوری ۱- هدف می‌تواند راهبردی، تاکتیکی یا عملیاتی باشد.

یادآوری ۲- اهداف می‌توانند با حوزه‌های مختلفی مرتبط باشند (مانند اهداف مالی، سلامتی و ایمنی، و زیست محیطی) و می‌توانند در سطوح متفاوتی (مانند راهبردی، در سرتاسر سازمان، پروژه، محصول و *فرایند* (۳-۲۶)) به‌کار روند.

یادآوری ۳- هدف می‌تواند به صورت‌های دیگر هم بیان شود، به طور مثال به عنوان نتیجه مورد نظر، مقصود، معیار عملیاتی، به عنوان یک هدف *تداوم کسب و کار* (۳-۳)، یا از طریق استفاده از سایر واژه‌ها با معنای مشابه.

یادآوری ۴- در مضمون *سیستم‌های مدیریت* (۳-۱۶) تداوم کسب و کار، اهداف تداوم کسب و کار برای دستیابی به نتایج خاص، اهداف تداوم کسب و کار همخوان با *خط‌مشی* (۳-۲۴) تداوم کسب و کار توسط *سازمان* (۳-۲۱) تعیین می‌گردد.

یادآوری ۵- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۲۱

سازمان

organization

شخص یا گروهی از کارکنان که برای دستیابی به *اهداف* (۳-۲۰) خود، وظایف خاص خود را همراه با مسئولیت‌ها، اختیارات و روابط دارند

یادآوری ۱- مفهوم سازمان شامل تاجر منفرد، شرکت، گروه مجتمع شرکت‌ها، مؤسسه تجاری، بنگاه کسب و کار، تجارت‌خانه، تشکیلات اقتصادی، نهاد مرجع، شراکت بین بنگاهی، بنیاد خیریه یا مؤسسه، یا بخشی یا ترکیبی از آن‌ها چه به صورت سهامی یا غیر سهامی، اعم از ثبت شده یا نشده یا از بخش عمومی یا خصوصی می‌باشد، اما تنها به این موارد محدود نیست.

یادآوری ۲- برای سازمان‌های با بیش از یک واحد عملیاتی، هر واحد عملیاتی می‌تواند به عنوان یک سازمان تعریف شود.

یادآوری ۳- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد. تعریف اصلی با اضافه کردن یادآوری ۲ تغییر یافته است.

۳-۲۲

برون‌سپاری

outsource

ایجاد ترتیباتی که طبق آن یک *سازمان* (۳-۲۱) بیرونی، بخشی از حوزه‌های کاری یا *فرایندهای* (۳-۲۶) سازمان را انجام می‌دهد

یادآوری ۱- یک سازمان بیرونی، سازمان خارج از دامنه شمول سیستم مدیریت است، هر چند که حوزه کاری یا فرایند برون-سپاری شده در محدوده دامنه‌شمول باشد.

یادآوری ۲- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۲۳

عملکرد

performance

نتیجه قابل اندازه‌گیری

یادآوری ۱- عملکرد می‌تواند به یافته‌های کمی یا به یافته‌های کیفی مربوط باشد.

یادآوری ۲- عملکرد می‌تواند به *فعالیت‌های* (۳-۱) مدیریتی، *فرایندها* (۳-۲۶)، محصولات (شامل خدمات)، سیستم‌ها یا *سازمان‌ها* (۳-۲۱) مربوط باشد.

یادآوری ۳- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۲۴-۳

خط‌مشی

policy

مقاصد و جهت‌گیری یک *سازمان* (۳-۲۱) آن‌گونه که رسماً توسط *مدیریت ارشد* (۳-۳۱) آن بیان شده است

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۲۵-۳

فعالیت اولویت‌بندی شده

prioritized activity

فعالیتی (۳-۱) که به منظور جلوگیری از *اثرگذاری‌های* (۳-۱۳) غیر قابل قبول به کسب و کار در هنگام ایجاد یک *اختلال* (۳-۱۰)، به آن فوریت داده شده است.

[منبع: برگرفته از زیربند ۳-۱۷۶، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین و یادآوری ۱ حذف شده است.]

۲۶-۳

فرایند

process

مجموعه‌ای از *فعالیت‌های* (۳-۱) مرتبط به هم یا متعامل که ورودی‌ها را به خروجی‌ها تبدیل می‌کند

یادآوری- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۲۷-۳

محصول و خدمت

product and service

خروجی یا نتیجه ایجاد شده بوسیله‌ی یک *سازمان* (۳-۲۱) برای *طرف‌های ذینفع* (۳-۱۵)

مثال: اقلام تولیدی، بیمه اتومبیل، پرستاری اجتماعی.

[منبع: برگرفته از زیربند ۳-۱۸۱، استاندارد ISO22300: 2018، تغییرات: واژه‌ی «محصول و خدمت» جایگزین واژه‌ی «محصول یا خدمت» شده و تعریف جایگزین شده است.]

۳-۲۸

الزام

requirement

نیاز یا انتظاری که بیان می‌شود، عموماً، تلویحی یا اجباری است

یادآوری ۱- «عموماً تلویحی» می‌باشد یعنی در عرف یا رویه‌ی عمومی یک *سازمان* (۳-۲۱) و *طرف‌های ذینفع* (۳-۱۵)، نیاز یا انتظار مورد نظر تلویحی است.

یادآوری ۲- الزام مشخص شده، الزامی است که بیان شده باشد برای مثال در *اطلاعات مدون* (۳-۱۱)

یادآوری ۳- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۳-۲۹

منبع

resource

کلیه دارایی‌ها (شامل کارخانه و تجهیزات)، افراد، مهارت‌ها، فناوری، ساختمان‌ها و تدارکات و اطلاعات (اعم از الکترونیک یا غیر الکترونیک) که یک سازمان بایستی برای استفاده در هنگام نیاز در دسترس داشته باشد تا با بکارگیری آن‌ها به اهداف خود نائل شود

[منبع: برگرفته از زیربند ۳-۱۹۳، استاندارد ISO22300: 2018، تغییرات: تعریف جایگزین شده است.]

۳-۳۰

ریسک

risk

تأثیر عدم قطعیت بر *اهداف* (۳-۲۰)

یادآوری ۱- تأثیر عدم قطعیت، انحراف- مثبت یا منفی- از آنچه که مورد انتظار است، می‌باشد.

یادآوری ۲- عدم قطعیت، بیانگر وضعیت کمبود اطلاعات، حتی به صورت جزئی در رابطه با درک یا دانش داشتن در مورد یک رخداد یا تبعات و احتمال وقوع آن است.

یادآوری ۳- ریسک اغلب با اشاره به رخدادهای بالقوه (همانگونه که در استاندارد ISO Guide 73 تعریف شده است) و تبعات رخدادها (همانگونه که در استاندارد ISO Guide 73 تعریف شده است) یا ترکیبی از اینها مشخص می‌گردد.

یادآوری ۴- ریسک اغلب بر حس ترکیبی از تبعات یک رخداد (تغییراتی در شرایط) و احتمال وقوع مربوطه (همانگونه که در استاندارد ISO Guide 73 تعریف شده است) بیان می‌شود.

یادآوری ۵- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد. تعریف با اضافه کردن «بر اهداف» تغییر یافته است تا با استاندارد ISO 31000 همخوانی داشته باشد.

۳-۳۱

مدیریت ارشد

top management

شخص یا گروهی از کارکنان که یک *سازمان* (۳-۲۱) را در بالاترین سطح هدایت و کنترل می‌کنند

یادآوری ۱- مدیریت ارشد قدرت آن را دارد که در درون سازمان اختیارات را تفویض و *منابع* (۳-۲۹) را تأمین کند.

یادآوری ۲- اگر دامنه شمول *سیستم مدیریت* (۳-۱۶) فقط بخشی از یک سازمان را پوشش دهد، در این صورت اصطلاح «مدیریت ارشد» به آن‌هایی که آن بخش از سازمان را هدایت و کنترل می‌کنند اطلاق می‌شود.

یادآوری ۳- این اصطلاح یکی از اصطلاحات مشترک و از تعاریف اصلی ساختار سطح بالا برای استانداردهای سیستم مدیریت می‌باشد.

۴ محیط کسب و کار سازمان

۴-۱ شناخت سازمان و محیط کسب و کار آن

سازمان باید مسائل برون‌سازمانی و درون سازمانی مرتبط با مقصود خود را که بر توانایی سازمان برای دستیابی به نتیجه (های) مورد نظر از BCSM تأثیر دارد، تعیین نماید.

یادآوری: این مسائل توسط اهداف کلی سازمان، محصولات و خدمات آن و میزان و نوع ریسکی که سازمان ممکن است بپذیرد یا نپذیرد، تحت تأثیر قرار خواهد گرفت.

۴-۲ شناخت نیازها و انتظارات طرف‌های ذینفع

۴-۲-۱ کلیات

سازمان زمانی که BCMS خود را ایجاد می‌کند باید موارد زیر را تعیین کند:

الف- طرف‌های ذینفعی که مرتبط با BCMS می‌باشند؛

ب- الزامات مرتبط با طرف‌های ذینفع که مرتبط با BCMS می‌باشند.

۴-۲-۲ الزامات قانونی و مقرراتی

سازمان باید:

الف- فرایندی را جهت شناسایی، دستیابی و ارزیابی الزامات قانونی و مقرراتی مرتبط با تداوم محصولات، خدمات، فعالیت‌ها و منابع خود ایجاد و برقرار نگه دارد؛

ب- اطمینان حاصل کند که این الزامات قانونی و مقرراتی و سایر الزامات در اجرا و حفظِ BCMS سازمان در نظر گرفته شده‌اند.

پ- این اطلاعات را مدون کرده و به‌روز نگهداری کند.

۴-۳ تعیین دامنه‌کاربرد سیستم مدیریت تداوم کسب و کار

۴-۳-۱ کلیات

سازمان باید محدوده‌ها و قابلیت به‌کارگیری BCMS را برای تعیین دامنه‌کاربرد آن مشخص نماید.

سازمان هنگام تعیین این دامنه‌کاربرد، باید موارد زیر را مورد توجه قرار دهد:

الف- مسائل برون‌سازمانی و درون‌سازمانی اشاره شده در زیر بند ۴-۱؛

ب- الزامات طرف‌های ذینفع اشاره شده در زیر بند ۴-۲؛

پ- مأموریت، اهداف و تعهدات برون‌سازمانی و درون‌سازمانی خود.

دامنه‌کاربرد باید به عنوان اطلاعات مدون در دسترس باشد.

۴-۳-۲ دامنه‌کاربرد سیستم مدیریت تداوم کسب و کار

سازمان باید:

الف- بخش‌هایی از سازمان که تحت BCMS قرار می‌گیرند را با درنظر گرفتن موقعیت (ها)، اندازه، ماهیت و پیچیدگی آن‌ها تعیین نماید؛

ب- محصولات و خدماتی را که تحت BCMS قرار می‌گیرند مشخص نماید.

هنگام تعریف دامنه‌کاربرد، سازمان باید موارد مستثنی را مدون و تشریح نماید. این موارد همانطور که توسط تحلیل اثر کسب و کار یا ارزیابی ریسک و الزامات قانونی و مقرراتی قابل اعمال تعیین می‌شود، نباید توانایی و مسئولیت سازمان برای ایجاد تداوم کسب و کار را تحت تأثیر قرار دهند.

۴-۴ سیستم مدیریت تداوم کسب و کار

سازمان باید یک BCMS را شامل فرایندهای مورد نیاز و تعامل آن‌ها بر طبق الزامات این استاندارد ایجاد و اجرا نماید و آن‌را برقرار نگه دارد و به طور مداوم بهبود بخشد.

۵ راهبری

۵-۱ راهبری و تعهد

مدیریت ارشد باید از طریق انجام موارد زیر راهبری و تعهد خود را در ارتباط با BCMS اثبات نماید:

الف- حصول اطمینان از اینکه خط‌مشی و اهداف تداوم کسب و کار برای BCMS تعیین شده‌اند و با جهت-گیری راهبردی سازمان سازگار می‌باشند؛

ب- حصول اطمینان از یکپارچگی الزامات BCMS در فرایندهای کسب و کار سازمان؛

پ- حصول اطمینان از دردسترس بودن منابع مورد نیاز برای BCMS؛

ت- تفهیم اهمیت تداوم کسب و کار اثربخش و انطباق با الزامات BCMS؛

ث- حصول اطمینان از اینکه نتایج مورد انتظار BCMS حاصل می‌شود؛

ج- هدایت و پشتیبانی از اشخاص برای کمک به اثربخشی BCMS؛

چ- ترویج بهبود مداوم؛

ح- پشتیبانی از سایر اشخاص دارای نقش‌های ذی‌ربط مدیریتی برای اثبات راهبری و تعهد آن‌ها، آنگونه که در حوزه‌های مسئولیت‌شان موضوعیت دارد.

یادآوری: اشاره به اصطلاح «کسب و کار» در این استاندارد را می‌توان در معنای وسیع آن، این‌گونه تفسیر نمود که به معنای محوری بودن این فعالیت‌ها در ارتباط با مقاصد مربوط به موجودیت سازمان باشد.

۵-۲ خط‌مشی

۵-۲-۱ تعیین خط‌مشی تداوم کسب و کار

مدیریت ارشد باید خط‌مشی تداوم و کسب و کار را به نحوی تعیین نماید که:

الف- متناسب با مقصود سازمان باشد؛

ب- چهارچوبی را برای تعیین اهداف تداوم کسب و کار فراهم نماید؛

پ- شامل تعهد در مورد برآورده کردن الزامات قابل اعمال باشد؛

ت- شامل تعهد در مورد بهبود مداوم BCMS باشد.

۵-۲-۲ ابلاغ خط‌مشی تداوم کسب و کار

خط‌مشی تداوم کسب و کار باید:

الف- به عنوان اطلاعات مدون دردسترس باشد؛

ب- در درون سازمان اطلاع‌رسانی شده باشد؛

پ- دردسترس طرف‌های ذینفع، آن‌گونه که مقتضی است، قرار گیرد.

۵-۲-۳ نقش‌ها، مسئولیت‌ها و اختیارات

مدیریت ارشد باید از اینکه مسئولیت‌ها و اختیارات در درون سازمان برای نقش‌های ذی‌ربط تعیین و ابلاغ شده است، اطمینان حاصل کند.

مدیریت ارشد باید مسئولیت‌ها و اختیارات را به منظورهای زیر تعیین نماید:

الف- حصول اطمینان از اینکه BCMS با الزامات این استاندارد انطباق دارد؛

ب-گزارش‌دهی در مورد عملکرد BCMS به مدیریت ارشد.

۶ طرح‌ریزی

۶-۱ اقدامات برای پرداختن به ریسک‌ها و فرصت‌ها

۶-۱-۱تعیین ریسک‌ها و فرصت‌ها

هنگام طرح‌ریزی BCMS، سازمان باید به منظورهای زیر مباحث اشاره شده در زیربند ۴-۱ و الزامات اشاره شده در زیربند ۴-۲ را در نظر بگیرد و ریسک‌ها و فرصت‌هایی را که نیاز است به آن‌ها پرداخته شود، تعیین نماید:

الف- ایجاد اطمینان در مورد اینکه به نتیجه (های) مورد نظر BCMS می‌توان دست یافت؛

ب- پیشگیری یا کاهش تأثیرات نامطلوب؛

پ- دستیابی به بهبود مداوم.

۶-۱-۲ پرداختن به ریسک‌ها و فرصت‌ها

سازمان باید موارد زیر را طرح‌ریزی نماید:

الف- اقدامات مربوط به پرداختن به این ریسک‌ها و فرصت‌ها؛

ب- چگونگی اقدامات:

۱- این اقدامات را در فرایندهای سیستم مدیریت کیفیت تلفیق کند و اجرا نماید (به زیربند ۸-۱ مراجعه شود)؛

۲- اثربخشی این اقدامات را ارزیابی نماید (به زیربند ۹-۱ مراجعه شود)؛

یادآوری: ریسک‌ها و فرصت‌ها در ارتباط با اثربخشی سیستم مدیریت می‌باشند. در زیربند ۸-۲ به ریسک‌های مرتبط با اختلالِ کسب و کار پرداخته شده است.

۶-۲ اهداف تداوم کسب و کار و طرح‌ریزی برای دستیابی به آن‌ها

۶-۲-۱ ایجاد اهداف تداوم کسب و کار

سازمان باید اهداف تداوم کسب و کار را سطوح و بخش‌های کاری مرتبط ایجاد نماید.

اهداف تداوم کسب و کار باید:

الف- همخوان با خط‌مشی تداوم کسب و کار باشد؛

ب- قابل اندازه‌گیری باشد (در صورت عملی بودن)؛

پ- الزامات قابل اعمال، در آن‌ها در نظر گرفته شود (به زیربندهای ۴-۱ و ۴-۲ مراجعه شود)؛

ت- مورد پایش قرار گیرند؛

ث- اطلاع‌رسانی شوند؛

ج- برحسب اقتضا به‌روز رسانی شوند.

سازمان باید اطلاعات مدونی از اهداف تداوم کسب و کار را نگهداری نماید

۶-۲-۲ تعیین اهداف تداوم کسب و کار

هنگام طرح‌ریزی چگونگی دستیابی به اهداف تداوم کسب و کار، سازمان باید موارد زیر را تعیین نماید:

الف- چه چیزی انجام خواهد شد؛

ب- چه منابعی مورد نیاز خواهد بود؛

پ- چه کسی مسئول خواهد بود؛

ت- چه زمانی تکمیل خواهد شد؛

ث- نتایج مربوطه چگونه مورد ارزیابی قرار خواهند گرفت.

۶-۳ طرح‌ریزی تغییرات برای سیستم مدیریت تداوم کسب و کار

هرگاه سازمان در مورد تغییر در BCMS تعیین نیاز نماید، از جمله موارد مشخص شده در بند ۱۰، تغییرات باید به صورت طرح‌ریزی شده انجام شود.

الف- مقصود از تغییرات و تبعات بالقوه آن‌ها؛

ب- انسجام BCMS؛

پ- دردسترس بودن منابع؛

ت- تخصیص یا تخصیص مجدد مسئولیت‌ها و اختیارات.

۷ پشتیبانی

۷-۱ منابع

سازمان باید منابعی را که برای ایجاد، اجرا و برقرار نگه‌داشتن BCMS و بهبود مداوم آن مورد نیاز است، تعیین و تأمین نماید.

۷-۲ شایستگی

سازمان باید:

الف- شایستگی لازم را برای اشخاصی که تحت کنترل سازمان کارهایی را انجام می‌دهند که بر عملکرد تداوم کسب و کار آن تأثیر می‌گذارد، تعیین نماید؛

ب- اطمینان حاصل کند که این اشخاص بر مبنای تحصیلات، آموزش، یا تجربه مناسب، شایسته می‌باشند؛

پ- اقداماتی را برای کسب شایستگی لازم، بر حسب امکان، انجام دهد و اثر بخشی اقدامات انجام شده را ارزیابی نماید؛

ت- اطلاعات مدون مناسبی را به عنوان شواهد شایستگی حفظ نماید.

یادآوری: اقدامات قابل انجام می‌تواند برای مثال شامل ارائه آموزش، هدایت‌گری[1] یا انتقال اشخاصی که در حال حاضر در استخدام می‌باشند یا به خدمت گرفتن یا بستن قرارداد با اشخاص شایسته باشد.

۷-۳ آگاهی

اشخاصی که تحت کنترل سازمان کار می‌کنند باید از موارد زیر آگاه باشند:

الف- خط‌مشی تداوم کسب و کار؛

ب- سهم آنان در اثربخشی BCMS، از جمله منافع عملکرد بهبود یافته‌ی تداوم کسب و کار؛

پ- تبعات انطباق نداشتن با الزامات BCMS؛

ت- نقش و مسئولیت خود آن‌ها قبل از اختلال، در هنگام اختلال و بعد از آن.

1- Mentoring

۷-۴ اطلاع‌رسانی

سازمان باید اطلاع‌رسانی‌های درون‌سازمانی و برون‌سازمانی مربوط به BCMS، شامل موارد زیر را تعیین نماید:

الف- در مورد چه چیزی اطلاع‌رسانی انجام شود؛

ب- چه هنگام اطلاع‌رسانی انجام شود؛

پ- به چه کسی اطلاع‌رسانی انجام شود؛

ت- چگونه اطلاع‌رسانی انجام شود؛

ث- چه کسی اطلاع‌رسانی را انجام خواهد داد.

۷-۵ اطلاعات مدون

۷-۵-۱ کلیات

BCMS سازمان باید شامل موارد زیر باشد:

الف- اطلاعات مدونی که توسط این استاندارد الزام شده است؛

ب- اطلاعات مدونی که توسط سازمان برای اثربخشی BCMS ضروری تشخیص داده می‌شود.

یادآوری: گستره‌ی اطلاعات مدون برای BCMS می‌تواند به دلایل زیر از یک سازمان به سازمان دیگر متفاوت باشد:

- اندازه سازمان و نوع فعالیت‌ها، فرایندها، محصولات و خدمات و منابع آن؛

- پیچیدگی فرایندها و تعامل آن‌ها؛

- شایستگی اشخاص.

۷-۵-۲ ایجاد و به‌روز رسانی

هنگام ایجاد و به‌روز رسانی اطلاعات مدون، سازمان باید از مناسب بودن موارد زیر اطمینان حاصل نماید:

الف- شناسایی و توصیف آن‌ها (برای مثال عنوان، تاریخ، مؤلف یا شماره مرجع)؛

ب- قالب اطلاعات (برای مثال زبان، نسخه نرم‌افزاری، تصویر) و واسط آن‌ها (برای مثال کاغذی، الکترونیکی)؛

پ- بازنگری و تأیید مناسب بودن و کفایت آن‌ها.

۷-۵-۳ کنترل اطلاعات مدون

۷-۵-۳-۱ اطلاعات مدون مورد نیاز BCMS و این استاندارد باید برای حصول اطمینان از موارد زیر تحت کنترل قرار گیرد:

الف- در هر جا و در هر زمان که مورد نیاز است، در دسترس و مناسب برای استفاده باشد؛

ب- در حد کفایت حفاظت شود (برای مثال در برابر نقض محرمانگی، استفاده نادرست یا نقض درستی آن-ها).

۷-۵-۳-۲ به منظور تحت کنترل قرار دادن اطلاعات مدون، سازمان باید بر حسب امکان فعالیت‌های زیر را انجام دهد:

الف- توزیع، دسترسی، بازیابی و استفاده از آن‌ها؛

ب- ذخیره‌سازی و محافظت، از جمله محافظت از خوانا بودن آن‌ها؛

پ- کنترل تغییرات آن‌ها؛

ت- حفظ و تعیین تکلیف آن‌ها.

اطلاعات مدون با منشأ خارجی که توسط سازمان برای طرح‌ریزی و اجرای BCMS ضروری تشخیص داده می‌شود باید شناسایی شده و بر حسب اقتضاء تحت کنترل قرار گیرد.

یادآوری: دسترسی، تلویحاً به معنای اجازه مربوط به فقط دیدن اطلاعات مدون یا اجازه و اختیار دیدن اطلاعات مدون می-باشد.

۸ عملیات

۸-۱ طرح‌ریزی و کنترل فرایندهای عملیاتی

سازمان باید فرایندهای مورد نیاز برای برآورده کردن الزامات و انجام اقدامات تعیین شده در بند ۶-۱ را با انجام موارد زیر طرح‌ریزی، اجرا و کنترل نماید:

الف- تعیین معیارهایی برای فرایندها؛

ب- اجرای کنترل فرایندها بر اساس معیارها؛

پ- نگهداری اطلاعات مدون در حد ضرورت به منظور حصول اطمینان از اینکه فرایندها آنگونه که طرح-ریزی شده‌اند، اجرا می‌شوند.

سازمان باید تغییرات طرح‌ریزی شده را تحت کنترل قرار دهد و تبعات تغییرات ناخواسته را بازنگری نماید و به منظور کاهش هر گونه تأثیرات نامطلوب، آن گونه که ضروری است، اقدام نماید.

سازمان باید اطمینان حاصل کند که فرایندهای برون‌سپاری شده تحت کنترل می‌باشند.

۸-۲ تحلیل اثر کسب و کار و ارزیابی ریسک

۸-۲-۱ کلیات

سازمان باید:

الف- فرایندهایی نظام‌مند برای تحلیل تأثیر کسب و کار و ارزیابی ریسک‌های اختلال پیاده‌سازی نموده و برقرار نگه دارد؛

ب- تحلیل تأثیر کسب و کار و ارزیابی ریسک را در فواصل زمانی برنامه‌ریزی شده و همچنین هنگامی که تغییرات قابل توجهی در سازمان یا محیط کسب و کار آن وجود دارد، بازنگری نماید.

یادآوری: سازمان ترتیب انجام تحلیل تأثیر کسب و کار و ارزیابی ریسک را تعیین می‌کند.

۸-۲-۲ تحلیل تأثیر کسب و کار

سازمان باید فرایندهایی را برای تحلیل تأثیرات کسب و کار به منظور تعیین اولویت‌ها و الزامات تداوم کسب و کار، به‌کار گیرد. این فرایندها باید:

الف- انواع تأثیرات و معیارهای مرتبط با محیط کسب و کار سازمان را تعریف نماید؛

ب- فعالیت‌هایی را که از ارائه‌ی محصولات و خدمات پشتیبانی می‌کنند، مشخص نماید؛

پ- از انواع تأثیرات و معیارها برای ارزیابی تأثیرات حاصل از اختلال بر روی این فعالیت‌ها در طول زمان، استفاده نماید؛

ت- چهارچوب زمانی را که در آن تأثیرات توقف انجام فعالیت‌ها برای سازمان غیر قابل پذیرش می‌شود را مشخص نماید؛

یادآوری ۱: این چهارچوب زمانی را می‌توان به عنوان «حداکثر مدت زمان قابل تحمل اختلال (MTPD)[1]» نام برد.

ث- در چهارچوب مشخص شده در قسمت د، چهارچوب‌های زمانی اولویت‌بندی شده‌ای را برای از سرگرفتن فعالیت‌های مختل شده با یک حداقل ظرفیت قابل قبول مشخص شده، تنظیم نماید؛

1- Maximum Tolerable Period of Disruption

یادآوری ۲: این چهارچوب زمانی را می‌توان به عنوان «هدف زمانیِ بازیابی (RTO)[1]» نام برد.

ج- این تحلیل را برای مشخص کردن فعالیت‌های اولویت‌بندی شده استفاده نماید؛

چ- تعیین نماید چه منابعی برای پشتیبانی از این فعالیت‌های اولویت‌بندی شده مورد نیاز است؛

ح- وابستگی‌ها، از جمله شرکا و تأمین‌کنندگان، و وابستگی‌های متقابلِ فعالیت‌های اولویت‌بندی شده را تعیین نماید.

۸-۲-۳ ارزیابی ریسک

سازمان باید یک فرایند ارزیابی ریسک را پیاده‌سازی نموده و برقرار نگه دارد.

یادآوری : در استاندارد ISO 31000 به این فرایند ارزیابی ریسک پرداخته شده است.

سازمان باید:

الف- ریسک‌های اختلال برای فعالیت‌های اولویت‌بندی شده‌ی سازمان و منابع مورد نیاز آن‌ها را مشخص نماید؛

ب- ریسک‌های مشخص شده را تحلیل و ارزیابی نماید؛

پ- مشخص نماید کدام ریسک‌ها نیاز به برطرف نمودن دارد.

یادآوری : ریسک‌ها در این زیربند مربوط به اختلال در فعالیت‌های کسب و کار می‌باشند. ریسک‌ها و فرصت‌های مربوط به اثربخشی سیستم مدیریت در زیر بند ۶-۱ پرداخته شده است.

۸-۳ استراتژی‌ها و راه‌حل‌های تداوم کسب و کار

۸-۳-۱ کلیات

بر اساس نتایج حاصل از تحلیل تأثیر کسب و کار و ارزیابی ریسک، سازمان باید استراتژی‌های تداوم کسب و کار را که گزینه‌هایی را برای قبل از بروز اختلال، در هنگام بروز اختلال و پس از آن در نظر می‌گیرند، مشخص کرده و انتخاب نماید. استراتژی‌های تداوم کسب و کار باید از یک یا چند راه حل تشکیل شده باشند.

۸-۳-۲ مشخص کردن استراتژی‌ها و راه‌حل‌ها

مشخص کردن استراتژی‌ها و راه‌حل‌ها باید بر اساس میزانی باشد که آن‌ها:

1- Recovery Time Objective

الف- الزامات تداوم و احیاء فعالیت‌های اولویت‌بندی شده در چهارچوب زمانی مشخص شده و ظرفیت مورد توافق را برآورده می‌نمایند؛

ب- فعالیت‌های اولویت‌بندی شده سازمان را محافظت می‌کنند؛

پ- احتمال اختلال را کاهش می‌دهند؛

ت- مدت زمان اختلال را کوتاه می‌کنند؛

ث- تأثیر اختلال بر خدمات و محصولات سازمان را محدود می‌کنند؛

ج- دردسترس بودن منابع کافی را فراهم می‌نمایند.

۸-۳-۳ انتخاب استراتژی‌ها و راه‌حل‌ها

انتخاب استراتژی‌ها و راه‌حل‌ها باید براساس میزانی باشد که آن‌ها:

الف- الزامات تداوم و احیاء فعالیت‌های اولویت‌بندی شده در چهارچوب زمانی مشخص شده و ظرفیت مورد توافق را برآورده می‌نمایند؛

ب- میزان و نوع ریسکی را که سازمان ممکن است بپذیرد یا نپذیرد، در نظر می‌گیرند؛

پ- هزینه‌ها و منافع مربوطه را در نظر می‌گیرند.

۸-۳-۴ الزامات منابع

سازمان باید الزاماتِ منابع برای پیاده‌سازی راه‌حل‌های تداوم کسب و کار انتخاب شده را تعیین کند. انواع منابع درنظر گرفته شده باید شامل موارد زیر باشد اما به این موارد محدود نمی‌شود:

الف- افراد؛

ب- اطلاعات و داده‌ها؛

پ- زیرساخت‌های فیزیکی مانند ساختمان‌ها، محل‌های کار یا سایر تسهیلات و تأسیسات مربوطه؛

ت- تجهیزات و مواد مصرفی؛

ث- سیستم‌های فناوری اطلاعات و ارتباطات (ICT)[1]؛

ج- حمل و نقل و تدارکات؛

چ- مالی؛

1- Information and Communication Technology

ح- شرکاء و عرضه‌کنندگان.

۸-۳-۵ پیاده‌سازی راه‌حل‌ها

سازمان باید راه‌حل‌های انتخاب شده جهت تداوم کسب و کار را پیاده‌سازی و نگهداری نماید تا در صورت لزوم فعال شوند.

۸-۴ طرح‌ها و روش‌های اجرایی تداوم کسب و کار

۸-۴-۱ کلیات

سازمان باید ساختار واکنشی را که از توانایی هشدار به موقع و اطلاع‌رسانی به طرف‌های ذینفع مربوطه برخوردار است، پیاده‌سازی نموده و برقرار نگه دارد. این ساختار باید طرح‌ها و روش‌های اجرایی را برای مدیریت سازمان در هنگام بروز اختلال فراهم آورد. این طرح‌ها و روش‌های اجرایی باید زمانیکه فعال کردن راه‌حل‌های تداوم کسب و کار مورد نیاز باشد، به‌کار گرفته شوند.

یادآوری : انواع مختلفی از روش‌های اجرایی که شامل برنامه‌های تداوم کسب و کار می‌باشد، وجود دارد.

سازمان باید بر اساس نتایج راه‌حل‌ها و استراتژی‌های انتخاب شده، طرح‌ها و روش‌های اجرایی تداوم کسب و کار را مشخص کرده و مدون نماید.

روش‌های اجرایی باید:

الف- با توجه به اقدامات فوری که باید در هنگام اختلال انجام شوند، واضح باشند؛

ب- برای واکنش به تغییر شرایط داخلی و خارجی حاصل از یک اختلال، انعطاف پذیر باشد؛

پ- بر تأثیر رخدادهایی که به طور بالقوه منجر به اختلال می‌شوند، تمرکز نمایند؛

ت- در به حداقل رسانیدن تأثیر اختلال، از طریق پیاده‌سازی راه‌حل‌های مناسب، مؤثر باشند؛

ث- نقش‌ها و مسئولیت‌هایی را برای انجام وظایف مذکور در آن‌ها تخصیص دهند.

۸-۴-۲ ساختار واکنشی

۸-۴-۲-۱ سازمان باید ساختاری را که یک یا چند تیم مسئول برای واکنش به اختلالات را مشخص می‌کند، پیاده‌سازی نموده و برقرار نگه دارد.

۸-۴-۲-۲ نقش‌ها و مسئولیت‌های هر تیم و روابط بین تیم‌ها باید به طور شفاف بیان گردد.

۸-۴-۲-۳ در مجموع، تیم‌ها باید شایستگی جهت موارد زیر را داشته باشند:

الف- ارزیابی ماهیت و اندازه‌ی یک اختلال و اثرگذاری بالقوه آن؛

ب- ارزیابی اثرگذاری اختلال در مقابل آستانه‌های از پیش تعریف شده که شروع یک واکنش رسمی را توجیه می‌کند؛

پ- فعال نمودن یک واکنش تداوم کسب و کار مناسب؛

ت- طرح‌ریزی اقداماتی که لازم است برعهده گرفته شوند؛

ث- تعیین اولویت‌ها (با در نظر گرفتن امنیت جانی به عنوان اولویت اول)؛

ج- پایش کردن اثرات اختلال و واکنشِ سازمان؛

چ- فعال نمودن راه‌حل‌های تداوم کسب و کار؛

ح- ارتباط با طرف‌های ذینفع مرتبط، مسئولان و واسط‌ها.

۸-۴-۲-۴ برای هر تیم باید موارد زیر وجود داشته باشند:

الف- کارکنان مشخص شده و افراد جایگزین آن‌ها با مسئولیت، اختیارات و شایستگی لازم برای انجام نقش تعیین شده؛

ب- روش‌های اجرایی مدون شده برای هدایت اقدامات آن‌ها (به زیربند ۸-۴-۴ مراجعه شود) از جمله اقدامات برای فعال‌سازی، اجرا، هماهنگی و برقراری ارتباط جهت واکنش به اختلال.

۸-۴-۳ هشداردهی و اطلاع‌رسانی

۸-۴-۳-۱ سازمان باید روش‌های اجرایی را جهت انجام موارد زیر، مدون نموده و برقرار نگه دارد:

الف- اطلاع‌رسانی درون‌سازمانی و برون‌سازمانی با طرف‌های ذینفع مرتبط، شامل اینکه چه چیزی، چه زمانی، به چه کسی و چگونه اطلاع‌رسانی انجام شود؛

یادآوری : سازمان می‌تواند روش‌های اجرایی را برای اینکه چگونه و تحت چه شرایطی سازمان با کارکنان و تماس‌های فوریتی آن‌ها اطلاع‌رسانی انجام دهد، مدون کرده و برقرار نگه دارد.

ب- دریافت، مدون کردن و واکنش به اطلاع‌رسانی‌های طرف‌های ذینفع، شامل هر سیستم مشورتی ملی یا منطقه‌ای یا معادل آن؛

پ- حصول اطمینان از در دسترس بودن وسایل اطلاع‌رسانی در هنگام اختلال؛

ت- تسهیل ارتباط سازمانی با گروه‌های امداد فوریتی؛

ث- تهیه جزئیاتی از واکنش رسانه‌ای سازمان پس از یک رخداد، از جمله استراتژی اطلاع‌رسانی؛

ج- ثبت جزئیات اختلال، اقدامات انجام شده و تصمیمات اخذ شده.

۸-۴-۳-۲ در صورت امکان، موارد زیر نیز باید در نظر گرفته شده و پیاده‌سازی شود:

الف- آماده‌باش دادن (اعلام خطر کردن) به طرف‌های ذینفعی که به صورت بالقوه در معرض یک اختلال واقعی یا قریب‌الوقوع قرار دارند؛

ب- حصول اطمینان از همکاری و ارتباط مناسب بین سازمان‌های مختلف امدادی.

روش‌های اجرایی هشداردهی و اطلاع‌رسانی سازمان باید، به عنوان بخشی از برنامه‌های مانور سازمان که در زیربند ۸-۵ تشریح شده است، تمرین گردند.

۸-۴-۴ طرح‌های تداوم کسب و کار

۸-۴-۴-۱ سازمان باید طرح‌ها و روش‌های اجرایی تداوم کسب و کار را مدون نموده و برقرار نگه دارد. طرح‌های تداوم کسب و کار باید رهنمودها و اطلاعاتی را فراهم آورند تا به تیم‌ها جهت واکنش به یک اختلال کمک نماید و با واکنش‌دهی و بازیابی به سازمان کمک کند.

۸-۴-۴-۲ در مجموع، طرح تداوم کسب و کار باید حاوی موارد زیر باشد:

الف- جزئیاتی از اقداماتی که تیم‌ها انجام خواهند داد تا:

۱- فعالیت‌های اولویت‌بندی شده را در چهارچوب زمانی از پیش تعیین شده، استمرار دهند یا بازیابی نمایند؛

۲- تأثیر اختلال و واکنشِ سازمان به آن را پایش نمایند؛

ب- ارجاع به آستانه (ها) و فرایندهای از پیش تعریف شده برای فعال نمودن واکنش به اختلال؛

پ- روش‌های اجرایی که امکان ارائه‌ی محصولات و خدمات در ظرفیت مورد توافق را فراهم آورند؛

ت- جزئیاتی برای مدیریت پیامدهای فوری یک اختلال، با تبعیت از موارد مربوطه زیر:

۱- رفاه افراد؛

۲- جلوگیری از خسارت بیشتر و از دسترس خارج شدن فعالیت‌های اولویت‌بندی شده؛

۳- اثرگذاری بر محیط زیست.

۸-۴-۴-۳ هر طرح باید شامل موارد زیر شود:

الف- مقصود، دامنه‌شمول و اهداف؛

ب- نقش‌ها و مسئولیت‌های تیمی که طرح را پیاده‌سازی می‌کند؛

پ- اقدامات لازم برای پیاده‌سازی راه‌حل‌ها؛

ت- اطلاعات پشتیبانی مورد نیاز برای فعال نمودن (از جمله معیارهای فعال‌سازی)، اجرا، هماهنگی و برقراری ارتباطِ فعالیت‌های تیم؛

ث- وابستگی‌های متقابل داخلی و خارجی؛

ج- الزامات منابع؛

چ- الزامات گزارش‌دهی؛

ح- فرایندی برای اعلام وضعیت عادی.

هر طرح باید در زمان و مکانی که مورد نیاز است در دسترس و قابل استفاده باشد.

۸-۴-۵ بازیابی

سازمان باید برای بازیابی و اعاده‌ی فعالیت‌های کسب و کار خود از اقدامات موقت اخذ شده در طی اختلال و پس از آن، فرایندهای مدونی داشته باشد.

۸-۵ برنامه‌ی تمرین

سازمان باید برای صحه‌گذاری اثربخشی استراتژی‌ها و راه‌حل‌های تداوم کسب و کار خود در طول زمان، یک برنامه‌ی تمرینی و آزمایشی را پیاده‌سازی نموده و برقرار نگه دارد.

سازمان باید تمرینات و آزمایشاتی را انجام دهد که:

الف- با اهداف تداوم کسب و کار خود همخوان باشد؛

ب- براساس سناریوهای مناسبی باشند که با مقاصد و اهداف از پیش تعریف شده و شفاف طرح‌ریزی شده‌اند؛

پ- کارگروهی، شایستگی، اعتماد به نفس و دانش افرادی که نقشی در رابطه با اختلالات دارند را توسعه دهد؛

ت- با گذشت زمان، راه‌حل‌ها و استراتژی‌های تداوم کسب و کار را صحه‌گذاری نماید؛

ث- گزارش‌های رسمی پس از تمرین را تهیه نماید که حاوی نتایج، توصیه‌ها و اقدامات لازم برای ایجاد بهبود باشد؛

ج- در زمینه‌ی ارتقاء بهبود مداوم بازنگری می‌شوند؛

چ- در فواصل زمانی برنامه‌ریزی شده و زمانی که تغییرات قابل توجهی در سازمان یا محیط کسب و کار آن وجود دارد، اجرا شوند.

سازمان برای اجرای تغییرات و بهبودها باید بر اساس نتایج مانوورها و آزمایش‌های خود عمل نماید.

۸-۶ ارزشیابی مدون‌سازی و قابلیت‌های تداوم کسب و کار

سازمان باید:

الف- شایستگی، کفایت و اثربخشیِ تحلیل اثر کسب و کار، استراتژی‌های ارزیابی ریسک، راه‌حل‌ها، طرح‌ها و روش‌های اجرایی را ارزیابی نماید؛

ب- ارزیابی‌هایی را از طریق بازنگری‌ها، تجزیه و تحلیل، تمرین‌ها، آزمایشات، گزارشات پس از رویداد و ارزیابی‌های عملکرد انجام دهد.

پ- ارزیابی‌هایی را از قابلیت‌های تداوم کسب و کار در شرکاء و تأمین‌کنندگان مربوطه انجام دهد؛

ت- مطابقت با الزامات قانونی و مقرراتی قابل اعمال، بهترین الگوهای صنعت، و انطباق با خط‌مشی‌ها و اهداف تداوم کسب و کار خود را ارزیابی نماید؛

ث- مستندسازی و روش‌های اجرایی را به شیوه‌ای زمان‌مند به‌روز رسانی نماید.

این ارزیابی‌ها باید در فواصل زمانی برنامه‌ریزی شده، پس از یک رویداد یا فعال‌سازی و زمانیکه تغییرات قابل توجهی رخ می‌دهد، اجرا شوند.

۹ ارزشیابی عملکرد

۹-۱ پایش، اندازه‌گیری، تحلیل و ارزشیابی

سازمان باید موارد زیر را تعیین نماید:

الف- چه چیزهایی نیاز است مورد پایش و اندازه‌گیری قرار گیرند؛

ب- در صورت امکان، روش‌هایی برای پایش، اندازه‌گیری، تحلیل و ارزیابی، برای حصول اطمینان از اعتبار نتایج؛

پ- چه زمان و توسط چه کسی باید پایش و اندازه‌گیری انجام شود؛

ت- چه زمان و توسط چه کسی باید نتایج حاصل از پایش و اندازه‌گیری مورد تحلیل و ارزیابی قرار گیرد.

سازمان باید اطلاعات مدون مناسبی را به عنوان شواهد مربوط به نتایج حفظ نماید.

۹-۲ ممیزی داخلی

۹-۲-۱ کلیات

سازمان باید ممیزی‌های داخلی را در فواصل زمانی طرح‌ریزی شده به اجرا درآورد تا اطلاعاتی را در این مورد فراهم کند که آیا BCMS:

الف- با موارد زیر انطباق دارد:

۱- الزامات خود سازمان در مورد BCMS آن؛

۲- الزامات این استاندارد؛

ب- به نحو اثربخش اجرا و نگهداری می‌شود.

۹-۲-۲ برنامه (های) ممیزی

سازمان باید:

الف- برنامه (های) ممیزی شامل دفعات، شیوه‌ها، مسئولیت‌ها، الزامات طرح‌ریزی و گزارش‌دهی را که در آن-(ها) اهمیت فرایندهای مربوطه و نیز نتایج ممیزی‌های قبلی باید در نظر گرفته شوند، طرح‌ریزی، ایجاد و اجرا نماید و برقرار نگه دارد؛

ب- معیارهای ممیزی و دامنه‌شمول هر ممیزی را تعیین نماید؛

پ- ممیزان را به نحوی انتخاب کند و ممیزی‌ها را به نحوی انجام دهد تا از عینیت داشتن[1] و بی‌طرفی فرایند ممیزی اطمینان حاصل شود؛

ت- اطلاعات مدون را به عنوان شواهد اجرای برنامه (های) ممیزی و نتایج ممیزی حفظ نماید؛

ث- اطمینان حاصل کند که هر اقدام اصلاحی لازم بدون تأخیر بی‌مورد، برای رفع عدم انطباق شناسایی شده و علل آن‌ها انجام شده است؛

1- Objectivity

ج- اطمینان حاصل کند که پی‌گیری اقدامات ممیزی از جمله تصدیق اقدامات و گزارش نتایج تصدیق انجام شده‌است.

۹-۳ بازنگری مدیریت

۹-۳-۱ کلیات

مدیریت ارشد باید BCMS سازمان را در فواصل زمانی طرح‌ریزی شده مورد بازنگری قرار دهد تا از تداوم مناسب بودن، کفایت و اثربخشی آن اطمینان حاصل کند.

۹-۳-۲ دروندادهای بازنگری مدیریت

بازنگری مدیریت باید موارد زیر را در نظر بگیرید:

الف- وضعیت اقدامات تصمیم‌گیری‌شده در بازنگری‌های قبلی مدیریت؛

ب- تغییرات در مسائل درون‌سازمانی و برون‌سازمانی مرتبط با BCMS؛

پ- اطلاعات در مورد عملکرد BCMS از جمله شامل رَوَندها در موارد زیر:

۱- عدم‌انطباق‌ها و اقدامات اصلاحی؛

۲- پایش و اندازه‌گیری نتایج ارزیابی؛

۳- نتایج ممیزی؛

ت- بازخورد از طرف‌های ذینفع؛

ث- نیاز به تغییرات در BCMS ازجمله خط‌مشی و اهداف؛

ج- روش‌های اجرایی و منابعی که در سازمان می‌تواند برای بهبود عملکرد و اثربخشی BCMS می‌تواند استفاده شود؛

چ- اطلاعاتی از تحلیل تأثیر کسب و کار و ارزیابی ریسک؛

ح- خروجیِ ارزیابیِ اسناد و قابلیت‌های تداوم کسب و کار (به زیربند ۸-۶ مراجعه شود)؛

خ- ریسک‌ها یا مسائلی که در ارزیابی‌های ریسک گذشته در حد کفایت به آن پرداخته نشده‌اند؛

د-درس‌های آموخته شده و اقدامات انجام شده در شبه‌حادثه‌ها[1] و اختلالات؛

ذ-فرصت‌های بهبود مداوم.

1- Near misses

۹-۳-۳ برونداد‌های بازنگری مدیریت

۹-۳-۳-۱ برونداد‌های بازنگری مدیریت باید شامل تصمیمات و اقدامات مربوط به فرصت‌های بهبود مداوم و هرگونه نیاز به تغییر در BCMS جهت بهبود کارایی و اثربخشی آن، از جمله موارد زیر باشد:

الف- تغییرات در دامنه‌شمول BCMS؛

ب- به‌روز رسانی تحلیل تأثیر کسب و کار، ارزیابی ریسک، استراتژی‌ها و راه‌حل‌های تداوم کسب و کار و طرح‌های تداوم کسب و کار؛

پ- اصلاح روش‌های اجرایی و کنترل‌ها برای واکنش به مباحث درون‌سازمانی و برون‌سازمانی که ممکن است بر BCMS تأثیر بگذارند؛

ت- چگونه اثربخشی کنترل‌ها اندازه‌گیری خواهد شد.

۹-۳-۳-۲ سازمان باید اطلاعات مدونی را به عنوان شواهد مربوط به نتایج بازنگری‌های مدیریت حفظ نماید. سازمان باید:

الف- نتایج بازنگری مدیریت را به طرف‌های ذینفع مرتبط اطلاع‌رسانی نماید؛

ب- اقدامات مناسب مرتبط با آن نتایج را انجام دهد.

۱۰ بهبود

۱۰-۱ عدم‌انطباق و اقدام اصلاحی

۱۰-۱-۱ سازمان باید فرصت‌های بهبود را تعیین کند و اقدامات ضروری برای رسیدن به نتیجه‌های مورد نظر از **BCMS** خود را اجرا نماید.

۱۰-۱-۲ هرگاه عدم‌انطباقی بروز کند، سازمان باید:

الف- در برابر عدم‌انطباق واکنش نشان دهد و برحسب مورد:

۱- برای کنترل و اصلاح آن اقدام نماید؛

۲- به تبعات آن بپردازد؛

ب- به‌منظور اینکه عدم‌انطباق مجدداً بروز نکند یا درجای دیگری بروز نکند، نیاز به اقدام برای حذف علت (های) عدم‌انطباق را از طریق موارد زیر ارزیابی نماید:

۱- بازنگری عدم‌انطباق؛

۲- تعیین علل عدم‌انطباق؛

۳- تعیین اینکه آیا عدم‌انطباق‌های مشابهی وجود دارد، یا به صورت بالقوه می‌تواند بروز کند؛

پ- اجرای هر اقدام مورد نیاز؛

ت- بازنگری اثربخشی هر اقدام اصلاحی انجام شده؛

ث- ایجاد تغییرات در BCMS، در صورت ضرورت.

اقدامات اصلاحی باید متناسب با تأثیرات عدم‌انطباق‌های بروزیافته باشد.

۱۰-۱-۳ سازمان باید اطلاعات مدونی را به عنوان شواهد مربوط به موارد زیر حفظ نماید:

الف- ماهیت عدم‌انطباق‌ها و هر اقدام بعدی انجام شده؛

ب- نتایج اقدامات اصلاحی.

۱۰-۲ بهبود مداوم

سازمان باید به طور مداوم مناسب بودن، کفایت و اثربخشی BCMS را بر اساس معیارهای کمی و کیفی بهبود بخشد.

سازمان باید به‌منظور تعیین اینکه آیا نیازها یا فرصت‌هایی، مرتبط با کسب و کار یا BCMS خود، وجود دارد که باید به عنوان جزئی از بهبود مداوم به آن‌ها پرداخته شود، نتایج تحلیل و ارزیابی و نیز بروندادهای بازنگری مدیریت را در نظر بگیرد.

یادآوری- سازمان می‌تواند فرایندهای BCMS از قبیل راهبری، طرح‌ریزی و ارزیابی عملکرد را جهت نائل شدن به بهبود، به‌کار گیرد.

کتاب‌نامه

[1] ISO 9001, Quality management systems- Requirements

یادآوری ۱: استاندارد ملی ایران- ایزو شمارهٔ ۹۰۰۱: سال ۱۳۹۶، سیستم‌های مدیریت کیفیت، الزامات، با استفاده از استاندارد ISO 9001: 2015 تدوین شده است.

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

یادآوری ۲: استاندارد ملی ایران- ایزو شمارهٔ ۱۴۰۰۱: سال ۱۳۹۷، سیستم‌های مدیریت زیست محیطی- الزامات همراه با راهنمای استفاده ، با استفاده از استاندارد ISO 14001: 2015 تدوین شده است.

[3] ISO 19011, Guidelines for auditing management systems

یادآوری ۳: استاندارد ملی ایران- ایزو شمارهٔ ۱۹۰۱۱: سال ۱۳۹۲، رهنمودهایی برای ممیزی سیستم‌های مدیریت، با استفاده از استاندارد ISO 19011: 2011 تدوین شده است.

[4] ISO/IEC/TS 17021-6, Conformity assessment- Requirements for bodies providing audit and certification of management systems- Part 6: Competence requirements for auditing and certification of business continuity management systems

یادآوری ۴: استاندارد ملی ایران- ایزو- آی ای سی شمارهٔ ۶-۱۷۰۲۱، سال ۱۳۹۴، ارزیابی انطباق- الزامات نهادهای ارائه کننده خدمات ممیزی و گواهی کردن سیستم‌های مدیریت- قسمت ۶: الزامات شایستگی برای ممیزی و گواهی کردن سیستم های مدیریت تداوم کسب و کار، با استفاده از استاندارد ISO/IEC/TC 17021-6: 2۰۱۴ تدوین شده است.

[5] ISO/IEC 20000-1, Information technology- Service management- Part 1: Service management system requirements

یادآوری ۵: استاندارد ملی ایران شمارهٔ ۱-۱۶۳۴۷: سال ۱۳۹۸، فناوری اطلاعات- مدیریت خدمات- قسمت ۱: الزامات سیستم مدیریت خدمات، با استفاده از استاندارد ISO/IEC 20000-1: 2018 تدوین شده است.

[6] ISO 22313, Societal security- Business continuity management systems- Guidance

یادآوری ۶: استاندارد ملی ایران شمارهٔ ۱۹۱۸۳: سال ۱۳۹۳، امنیتِ جامعگی- سیستم‌های مدیریت تداوم کسب و کار- راهنما، با استفاده از استاندارد ISO 22313: 2012 تدوین شده است.

[7] ISO 22316, Security and resilience- Organizational resilience- Principles and attributes

یادآوری ۷: استاندارد ملی ایران شمارهٔ ۲۲۴۲۲: سال ۱۳۹۶، امنیت و انعطاف‌پذیری- انعطاف‌پذیری سازمانی- اصول و ویژگی‌ها، با استفاده از استاندارد ISO 22316: 2017 تدوین شده است.

[8] ISO/TS 22317, Societal security- Business continuity management systems- Guidelines for business impact analysis (BIA)

یادآوری ۸: استاندارد ملی ایران شمارهٔ ۲۱۳۳۸: سال ۱۳۹۵، امنیت اجتماعی- سیستم‌های مدیریت تداوم کسب و کار- رهنمودهایی برای تجزیه و تحلیل اثر کسب و کار (BIA)، با استفاده از استاندارد ISO/TS 22317: 2015 تدوین شده است.

[9] ISO/TS 22318, Societal security- Business continuity management systems- Guidelines for supply chain continuity

یادآوری ۹: استاندارد ملی ایران شمارهٔ ۲۱۶۰۷: سال ۱۳۹۵، امنیت اجتماعی- سیستم‌های مدیریت تداوم کسب و کار- رهنمودهایی برای تداوم زنجیره تأمین، با استفاده از استاندارد ISO/TS 22318: 2015 تدوین شده است.

[10] ISO/TS 22330, Security and resilience- Business continuity management systems- Guidelines for people aspects of business continuity

[11] ISO/TS 22331, Security and resilience- Business continuity management systems- Guidelines for business continuity strategy

[12] ISO/IEC 27001, Information technology- Security techniques- Information security management systems- Requirements

یادآوری ۱۰: استاندارد ملی ایران- ایزو- آی ای سی شمارهٔ ۲۷۰۰۱: سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات، با استفاده از استاندارد ISO/IEC 27001: 2013 تدوین شده است.

[13] ISO/IEC 27031, Information technology- Security techniques- Guidelines for information and communication technology readiness for business continuity

یادآوری ۱۱: استاندارد ملی ایران- ایزو- آی ای سی- تی آر شمارهٔ ۲۷۰۳۱: سال ۱۳۹۱، فناوری اطلاعات، فنون امنیتی، راهنمایی برای آمادگی فناوری اطلاعات و ارتباطات به منظور تداوم کسب و کار، با استفاده از استاندارد ISO/IEC/TR27031: 2011 تدوین شده است.

[14] ISO 28000, Specification for security management systems for the supply chain

یادآوری ۱۲: استاندارد ملی ایران- ایزو شمارهٔ ۲۸۰۰۰: سال ۱۳۸۷، سیستم‌های مدیریت امنیت زنجیره تأمین- مشخصات، با استفاده از استاندارد ISO 28000: 2007 تدوین شده است.

[15] ISO 31000, Risk management- Guidelines

یادآوری ۱۳: استاندارد ملی ایران شمارهٔ ۱۳۲۴۵: سال ۱۳۹۸، مدیریت ریسک- رهنمودها، با استفاده از استاندارد ISO31000: 2018 تدوین شده است.

[16] IEC 31010, Risk management- Risk assessment techniques

یادآوری ۱۴: استاندارد ملی ایران شمارهٔ ۱۴۵۶۰: سال ۱۳۹۱، مدیریت ریسک- تکنیک‌های ارزیابی ریسک، با استفاده از استاندارد ISO/IEC 31010-1: 2009 تدوین شده است.

[17] ISO Guide 73, Risk management- Vocabulary

یادآوری ۱۵: استاندارد ملی ایران شمارهٔ ۱۳۲۴۶: سال ۱۳۸۹، مدیریت ریسک- واژگان، با استفاده از استاندارد ISO Guide73: 2009 تدوین شده است.