وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات

چالش‌های مدیریت تداوم کسب و کار در حوزه زیرساخت ارتباطات و فناوری اطلاعات

عنوان گزارش: چالش‌های مدیریت تداوم کسب و کار در زیرساخت ارتباطات و فناوری اطلاعات
کلمات کلیدی: مدیریت تداوم کسب و کار، زیرساخت های حیاتی، ارتباطات و فناوری اطلاعات، پدافند غیرعامل
تهیه کننده: ابوذر صولت رفیعی
ناظر علمی: نسرین تاج نیشابوری
گروه پژوهشی: فناوری امنیت شبکه
تاریخ انتشار: دی ماه ۱۴۰۲

چکیده

مقوله مدیریت تداوم کسب‌وکار (BCM[1]) نه تنها برای سازمان‌ها و شرکت‌های خصوصی، بلکه برای زیرساخت‌های حیاتی الزامی است. آسیب پذیری‌های مختلف زیرساخت‌های حیاتی در برابر تهدیدات، می‌تواند عواقب جبران‌ناپذیری برای امنیت ملی کشورها داشته باشد. در نتیجه مدیریت تداوم کسب و کار برای زیرساخت‌های حیاتی، به ویژه برای حوزه ارتباطات و فناوری اطلاعات ضروری است. این زیرساخت ستون فقرات بسیاری از زیرساخت‌های حیاتی دیگر مانند انرژی، حمل‌ونقل، بهداشت، امور مالی و حتی دولت است و هر گونه اختلال یا شکست در آن می‌تواند اثرات آبشاری و فاجعه‌باری بر دیگر زیرساخت های حیاتی داشته باشد. مدیریت تداوم کسب و کار در زیرساخت‌های حیاتی نیازمند یک رویکرد جامع و کامل است. همچنین مستلزم هماهنگی و همکاری در سطوح مختلف بین دستگاهی، بین زیرساختی و در سطح ملی است. یکی از مهمترین راه‌های اجرای موفق مدیریت تداوم کسب و کار برای زیرساخت-های حیاتی، توسعه اسناد راهبردی و استانداردها در سطح ملی است، از این رو کشورهای سراسر جهان، هر کدام با مخاطرات، جغرافیا و ساختارهای حاکمیتی منحصربه فرد خود، شیوه‌های متنوع و در عین حال مؤثر مدیریت تداوم کسب و کار را اتخاذ کرده‌اند. پس به طور قطع، طراحی و اجرای مدیریت تداوم کسب و کار در سطح کلان تحت تاثیر ویژگی های منحصر به فرد یک کشور است. این موضوع در کشور ما نیز، در اسناد بالادستی همچون مصوبات و الزامات پدافند غیرعامل در کشور مورد توجه و تاکید قرار گرفته و برای سازمان‌ها به فراخور ماهیت و اهمیت آن‌ها لازم الاجرا است. از طرفی با توجه به بررسی‌های میدانی و اقدامات سازمان‌ها در مدیریت تداوم کسب و کار در زیرساخت‌های حیاتی در کشور و به طور خاص زیرساخت ارتباطات و فناوری اطلاعات (سازمان‌های حوزه زیرساختی)، به نظر می‌رسد این حوزه با مشکلات و چالش های جدی در طراحی و پیاده‌سازی مواجه است. در این گزارش، سعی شده است با توجه به تجربیات حاصل از فعالیت در حوزه مشاوره در زمینه طراحی و پیاده‌سازی مدیریت تداوم کسب و کار در برخی سازمان‌ها، همچنین بررسی و تحلیل اقدامات برخی سازمان‌های زیرساخت‌های حیاتی حوزه فاوا کشور، مهمترین مشکلات و چالش های کلان این حوزه در کشور ارائه گردد.

[1] Business Continuity Management

فهرست مطالب

۱- مقدمه

فرآیندهای کسب وکار در هر سازمان از مهم‌ترین و حیاتی‌ترین فرآیندهایی می‌باشد که بقا و تداوم یک سازمان به آن بستگی دارد. به همین دلیل یکی از دغدغه‌ها و چالش‌های مدیران، بکارگیری سیاست‌ها و مکانیزم‌هایی است که بتوانند تدوام در کسب و کار سازمان را تضمین نمایند. در همین راستا، استانداردها و سیستم‌های مدیریتی و به‌روش‌ها[1] جهت ارتقاء امنیت اطلاعات و در راستای حفظ و اطمینان از تداوم کسب و کار مورد استفاده قرار می‌گیرند. این موضوع در کشور ما و در اسناد بالادست مانند مصوبات و الزامات پدافند غیرعامل در کشور مورد توجه و تاکید قرار گرفته و برای سازمان‌ها به فراخور ماهیت و اهمیت آن‌ها لازم اجرا است. زیرا آسیب پذیری زیرساخت‌های حیاتی در برابر تهدیدات مختلف، می‌تواند عواقب شدیدی برای امنیت ملی کشور داشته باشد. در نتیجه مدیریت تداوم کسب و کار برای زیرساخت‌های حیاتی، به ویژه بخش فاوا ضروری است مدیریت تداوم کسب و کار در زیرساخت‌های حیاتی نیازمند یک رویکرد جامع است که شامل شناسایی ذینفعان مختلف، مانند اپراتورها، ارائه دهندگان خدمات، تامین‌کنندگان، تنظیم کننده‌ها و مسئولین مربوطه می‌شود. همچنین مستلزم هماهنگی و همکاری در سطوح مختلف بین دستگاهی، بین زیرساختی و در سطح ملی است. از مهمترین راه های اجرای موفق مدیریت تداوم کسب وکار برای زیرساخت‌های حیاتی، توسعه اسناد راهبردی و استانداردهای ملی است که:

- نقش ها و مسئولیت‌های بازیگران مربوطه را مشخص می‌نماید.
- معیارها و روش‌های شناسایی و اولویت بندی زیرساخت‌های حیاتی و خدمات آن‌ها را بررسی می‌نماید،
- بهترین شیوه‌ها و دستورالعمل‌ها را برای ارزیابی ریسک و مدیریت ارائه می‌کند.
- و حداقل الزامات و شاخص‌های عملکرد تداوم کسب و کار و مکانیسم‌های نظارت و ارزیابی را تعیین می‌نماید.

از این رو کشورهای سراسر جهان نیز، هر کدام با ریسک‌ها، جغرافیا و ساختارهای حاکمیتی منحصربه فرد خود، شیوه‌های متنوع و در عین حال مؤثر مدیریت تداوم کسب و کار را اتخاذ کرده‌اند. به عنوان مثال، سنگاپور، ایالات متحده، ژاپن، انگلستان، استرالیا، کانادا، سوئیس، نیوزیلند، امارات متحده عربی و عربستان سعودی نگاه ویژه ای به موضوع مدیریت تداوم کسب و کار دارند که زیربنای سیاست‌ها، مقررات و یک دولت انعطاف‌پذیر و تاب آور است.

در این گزارش ضمن اشاره به اقدامات برخی کشورها در حوزه سیاست‌گذاری و تدوین اسناد راهبردی، به چالش‌های کلان این حوزه در کشور اشاره می‌گردد.

---

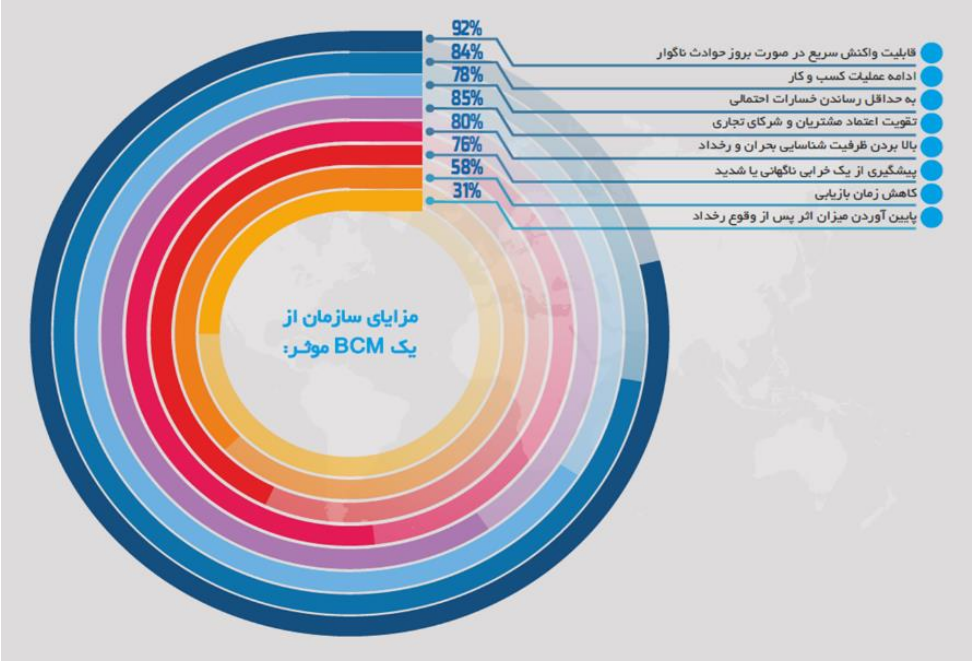
[1] Best prctice

۲-مدیریت تداوم کسب و کار

مدیریت تداوم کسب وکار به سازمان‌ها کمک می‌کند تا برای اختلالات احتمالی مانند بلایای طبیعی، حملات سایبری یا بیماری‌های همه‌گیر آماده شوند و در برابر خطرات بالقوه انعطاف‌پذیری ایجاد کنند. این موضوع شامل شناسایی عملکردهای حیاتی کسب و کار، ارزیابی ریسک‌ها، توسعه استراتژی‌ها و آزمایش برنامه‌ها برای اطمینان از تداوم و انعطاف‌پذیری است. با پیاده‌سازی آن، کسب‌وکارها می‌توانند به سرعت به رویدادهای پیش‌بینی‌نشده پاسخ دهند، از دارایی‌های خود محافظت کنند و عملیات خود را در زمان بحران حفظ کنند.

برخی از مدیران ارشد ممکن است به BCM اهمیت کافی ندهند، زیرا فکر می‌کنند بسیار پرهزینه، وقت گیر یا غیرضروری است. آنها ممکن است تصور کنند که بعید است کسب و کارشان با یک اختلال بزرگ مواجه شود. آنها همچنین ممکن است مزایای فوری و واضح BCM را نبینند، زیرا این یک استراتژی بلند مدت و فعال است که نیاز به آزمایش و به روز رسانی منظم دارد.

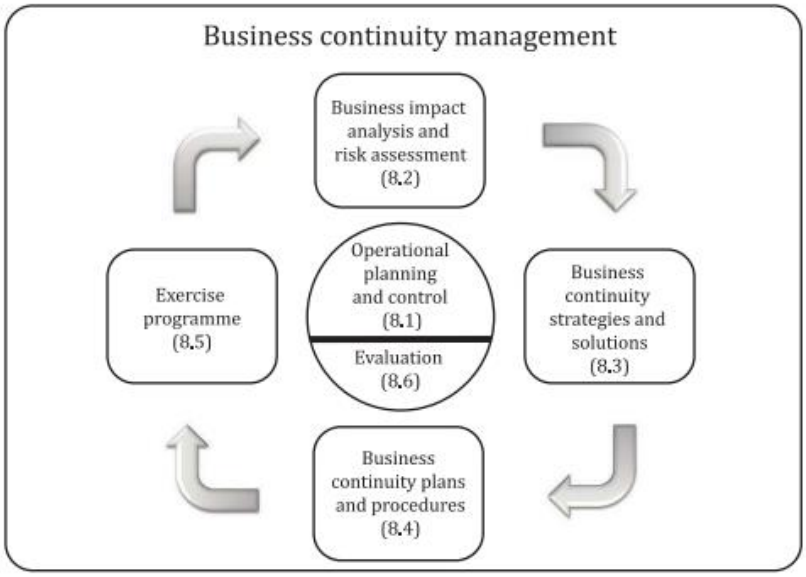
با این حال، این نگرش اشتباه و مخاطره آمیز است، زیرا سازمان را در معرض تهدیدات مختلفی قرار می‌دهد که می‌تواند به شهرت، درآمد و بقای آن آسیب برساند. BCM می تواند مزایای بسیاری برای سازمان داشته باشدکه در شکل شماره ۱ به خلاصه‌ای از مهمترین آن‌ها اشاره شده است.



شکل (۱) : برخی مزایای BCM برای سازمان‌ها

۲-۱- عناصر کلیدی مدیریت تداوم کسب و کار

در استاندارد ISO 22313 با عنوان امنیت و انعطاف پذیری – سیستم‌های مدیریت تداوم کسب و کار - راهنمای استفاده از ISO 22301 منتشر شده در سال ۲۰۲۰ عناصر اساسی مدیریت تداوم کسب و کار را مطابق شکل زیر تشریح می کند:



شکل (۲) : عناصر کلیدی مدیریت تداوم کسب و کار

الف) برنامه ریزی و کنترل عملیاتی (۸,۱): با رهبری مدیریت ارشد، برنامه‌ریزی و کنترل عملیاتی مؤثر شکل گرفته و هسته مدیریت تداوم کسب و کار را تشکیل می‌دهد.

ب) تحلیل تأثیر کسب و کار و ارزیابی ریسک (۸,۲): با ارزیابی تأثیر اختلالات در تحویل محصول/خدمت و درک خطرات مرتبط و نتایج حاصله، برنامه ریزی از سرگیری ارائه خدمات و محصولات فراهم می گردد.

ج) راهبردها و راه‌حل‌های تداوم کسب و کار (۸,۳): شناسایی و ارزیابی استراتژی‌ها به کاهش خطرات و کاهش اختلالات کمک می کند و به از سرگیری فعالیت‌ها در قالب زمانبندی مشخص کمک می‌نماید.

د) برنامه‌ها و رویه‌های تداوم کسب و کار (۸,۴): ایجاد ساختارهای واکنش، سیستم‌های هشدار و طرح های بازیابی، مدیریت موثر اختلالات را امکان پذیر می کند و اطمینان حاصل می کند که الزامات تداوم کسب و کار برآورده شده است.

ه) برنامه تمرین (۸,۵): تمرینات منظم، اثربخشی راه‌حل‌ها، طرح ها و رویه ها را تأیید می کند، آگاهی پرسنل را ارتقا می‌دهد، برنامه‌های به روز را حفظ می کند و تداوم کلی کسب و کار را افزایش می‌دهد.

و) ارزیابی مستندات و قابلیت های تداوم کسب و کار (۸,۶): ارزیابی مستمر، اثربخشی مدیریت تداوم کسب و کار را در دستیابی به اهداف سازمان تضمین می کند.

نکته بسیار مهم که در چالش‌ها به آن اشاره خواهد شد این است که طبق استاندارد ISO 22313، و دیگر استانداردها، مدل‌ها، چارچوب‌ها و به‌روش‌ها مسئله توالی عناصر مدیریت تداوم کسب و کار برای اثربخشی بسیار مهم و حیاتی است. مراحل تحلیل تأثیر کسب و کار و ارزیابی ریسک، بنیادی هستند، زیرا درک جامعی از اختلالات بالقوه و پیامدهای آن بر فعالیت‌های سازمانی ارائه می‌دهند. بدون تجزیه و تحلیل کامل این جنبه‌ها، تدوین راه‌حل‌های تداوم کسب‌وکار به حدس و گمان تبدیل می‌شود و کاملاً شکست خورده است. تحلیل تأثیر کسب و کار، اولویت بندی‌ها فعالیت ها را مشخص کرده و سازمان‌ها را قادر می‌سازد تا تلاش خود را بر روی فعالیت‌های حیاتی سازمان متمرکز نمایند. ارزیابی ریسک، به نوبه خود شناسایی و ارزیابی استراتژی‌های کاهش اختلالات را تعیین می‌نماید. ***تلاش برای توسعه طرح‌ها و رویه‌های تداوم کسب و کار مانند طرح تداوم کسب و کار، طرح بازیابی بلایا و ... بدون طی نمودن مراحل تجزیه و تحلیل تاثیر کسب و کار و ارزیابی ریسک، قابلیت اطمینان و ارتباط چنین برنامه‌هایی را بسیار کم و عملاً مدیریت تداوم کسب و کار رابا شکست مواجه می‌نماید.***

۲-۲- رویکردهای مدیریت تداوم کسب و کار

رویکردهای مختلفی در مدیریت تداوم کسب و کار وجود دارد که منعکس کننده‌ی نیازها و دیدگاه‌های مختلف سازمان‌های مختلف است. برخی از رویکردهای رایج در این زمینه عبارتند از:

- **رویکرد مبتنی بر استانداردها:** در این رویکرد از دستورالعمل‌ها و بهترین شیوه‌های استانداردها و چارچوب‌های تعیین شده مانند ISO 22313،ISO 22301 ، BS 25999، NFPA 1600 و NIST SP 800-34 استفاده می شود. این رویکرد انطباق، سازگاری و اعتبار برنامه BCM را تضمین می کند.

- **رویکرد مبتنی بر ریسک:** این رویکرد بر شناسایی و اولویت بندی حیاتی‌ترین ریسک‌ها و تهدیدهایی که ممکن است عملیات و اهداف سازمان را مختل کنند، تمرکز دارد. این رویکرد تخصیص منابع و فعالیت ها را با توجه به سطح ریسک و تأثیر هر سناریو امکان پذیر می کند.

- **رویکرد کسب و کار محور:** این رویکرد برنامه BCM را با اهداف استراتژیک، ارزش ها و فرهنگ سازمان هماهنگ می‌کند. این رویکرد شامل مشارکت و تعهد مدیریت ارشد و ذینفعان و همچنین ادغام BCM با سایر عملکردها و فرآیندهای تجاری است.

این رویکردها متقابلاً منحصر به فرد نیستند، بلکه مکمل و وابسته به یکدیگر هستند. یک برنامه جامع و مؤثر BCM باید همه آنها را در نظر گرفته و نیازها و اولویت های آنها را متعادل کند.

۳- اقدامات کشورها در حوزه مدیریت تداوم کسب وکار

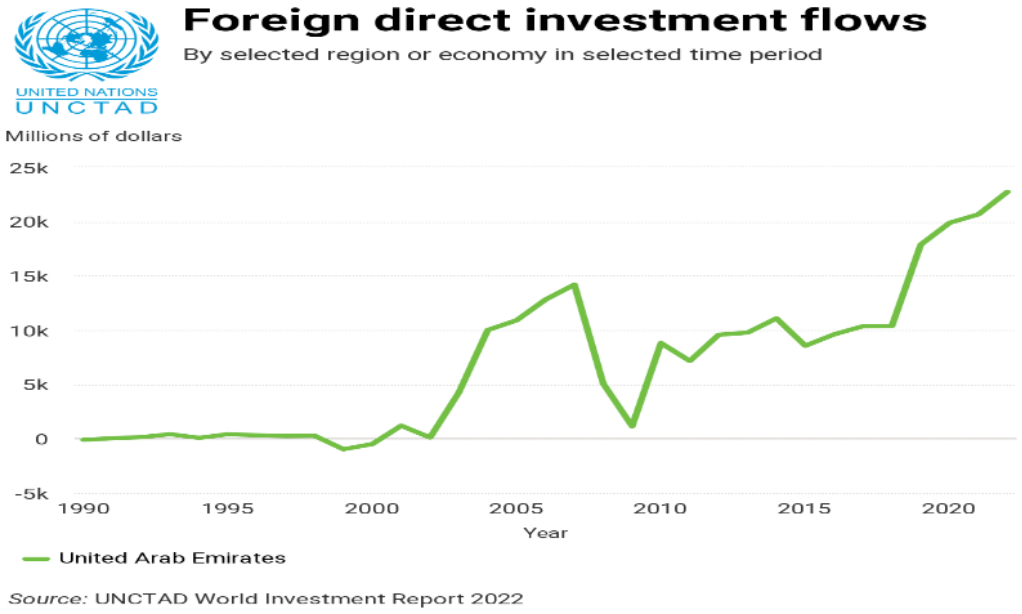
کشورهای مانند ایالات متحده، ژاپن، انگلستان، استرالیا، کانادا، سوئیس، نیوزیلند و سنگاپور که در این گزارش مورد بررسی قرار گرفته‌اند، در خصوص موضوع مدیریت تداوم کسب و کار اقدامات زیادی انجام داده و آن را زیربنای سیاست‌ها و مقررات در کشور خود قرارداده‌اند. آن‌ها معتقدند علاوه بر کاهش آسیب‌پذیری، افزایش اطمینان از تداوم فعالیت‌های ضروری، بازدارندگی، تسهیل مدیریت بحران، افزایش پایداری و مصون‌سازی ; داشتن یک سیاست روشن و مدیریت تداوم کسب و کار قوی (BCM) در سطح کلان عامل مهمی در جذب سرمایه گذاری مستقیم خارجی (FDI)[۱] است. جذب سرمایه گذاری مستقیم خارجی مقوله‌ی مهم در اقتصاد مقاومتی است که باید به آن توجه داشت زیرا اساس اقتصاد مقاومتی این است که کشورها را در قبال فشارها و شوک‌های اقتصادی که از سوی کشورهای دیگر وارد می‌شود، مصون می‌دارد یعنی کشور ضمن تکیه بر توانایی های داخلی به دنبال جذب سرمایه گذاری خارجی نیز باشد. سرمایه گذاران هنگام تصمیم گیری برای سرمایه گذاری به دنبال ثبات و بازگشت سریعتر سرمایه هستند. یک خط مشی BCM که به خوبی تعریف شده باشد این اطمینان را فراهم می‌کند که محیط کسب و کار می تواند در برابر اختلالات مقاومت کند، تداوم را تضمین کند و در نتیجه ریسک سرمایه گذاری را کاهش دهد. این موضوع نشان دهنده تعهد کشور به حفظ یک محیط تجاری باثبات، حتی در مواجهه با حوادث یا بحران های پیش بینی نشده است. این تعهد به نوبه خود می‌تواند اعتماد سرمایه گذاران را افزایش دهد و کشور را به مقصد جذاب تری برای سرمایه گذاری مستقیم خارجی تبدیل کند. بنابراین، کشورهایی مانند امارات تاکید زیادی بر امنیت و تداوم تجارت دارند تا امنیت و ثبات اقتصاد به سرعت در حال رشد خود را تضمین کنند. موقعیت استراتژیک این کشور در خاورمیانه و همچنین موقعیت آن به عنوان یک مرکز تجاری جهانی، امنیت و تداوم کسب و کار را در اولویت‌های اساسی قرار می‌دهد. امارات مقررات و استانداردهای مربوط به تداوم کسب و کار و بازیابی بلایا و حوادث طبیعی را سفارشی سازی نموده و اجرا کرده است. این روند از سال ۲۰۰۹ آغاز شده است و در بالاترین سطح و بصورت ملی به اجرا در آمده است.

بر اساس گزارش سالانه UNCTAD[۲] در خصوص سرمایه گذاری در سطح جهان در سال ۲۰۲۳، امارات متحده عربی به بالاترین میزان سرمایه گذاری مستقیم خارجی در تاریخ خود در سال ۲۰۲۲ دست یافته و در جذب سرمایه مستقیم خارجی در رتبه نخست منطقه خاور میانه و شمال آفریقا و رتبه سوم جهان در سال جاری قرار گرفت که نتیجه آن جذب ۲۳ میلیارد دلار در سال ۲۰۲۲ بود.

---

[۱] Foreign Direct Investment

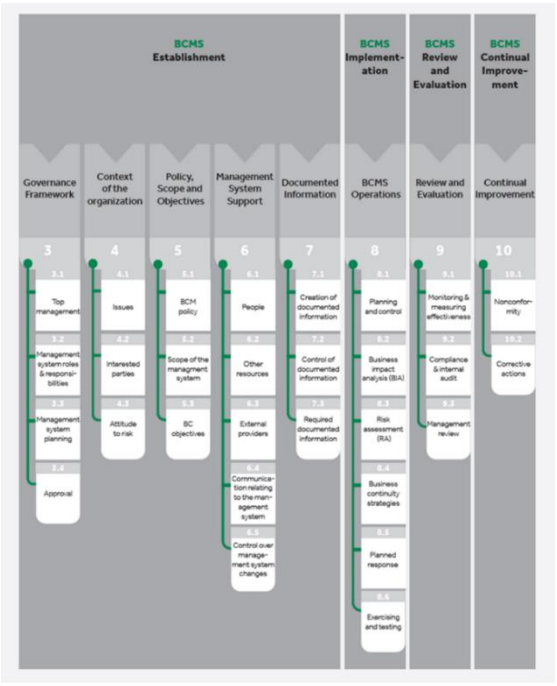
[۲] United Nations Conference on Trade and Development

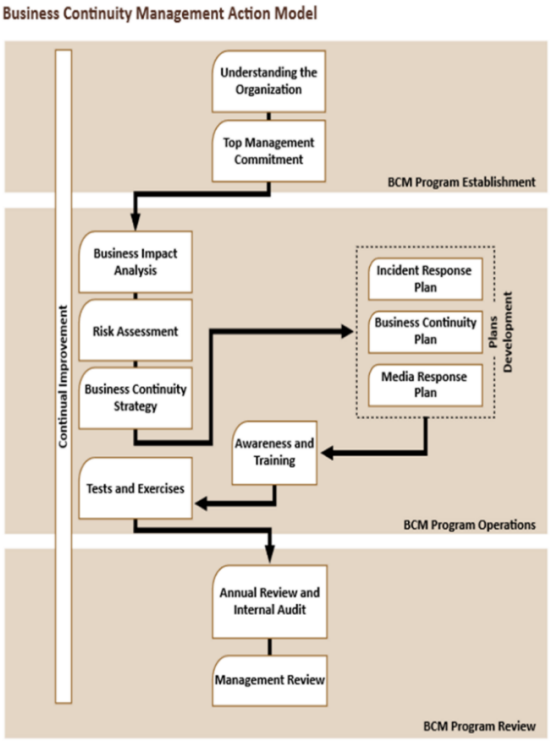


شکل(۳): جریان سرمایه گذاری مستقیم خارجی در کشور امارات

این کشور با کمک موسسه استاندارد ایزو و دیگر نهادهای تحقیقاتی بین المللی و نهادهای تحقیقاتی داخل کشور خود نسبت به تدوین استاندارد ملی و سند راهبردی اقدام نموده است. نکات بسیار مهمی از مطالعه این سند و بررسی تفاوت نسخه‌های ۲۰۱۵ و ۲۰۲۱ آن قابل بهره‌برداری است. در شکل شماره ۴ ساختار سطح بالایی از مدل اجرائی ارائه شده در این اسناد مقایسه شده است.

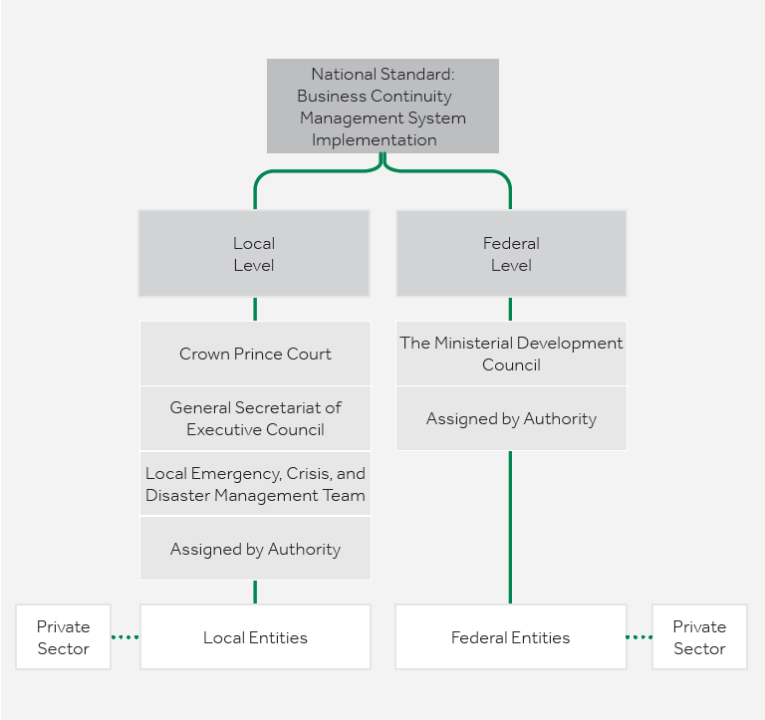
یکی از نکات بسیار مهم در مقایسه این دو سند *مبحث چارچوب های حکمرانی است* که در سال ۲۰۲۱ به این ساختار اضافه شده است. به این موضوع مهم در نقشه راه مدیریت تداوم کسب و کار در کشور عربستان سعودی نیز اشاره شده است. آغازگر این نقشه راه موضوع حکمرانی مدیریت تداوم کسب وکار است که در ادامه به اختصار به این موضوع پرداخته می‌شود.





شکل (۴) ساختار سطح بالا از مدل اجرائی ارائه شده در سال۲۰۱۵ و ۲۰۲۱

همچنین در سندهای مذکور نقش‌ها و مسئولیت‌ها به درستی تعیین گردیده است. لازم به ذکر است که امارات متحده عربی از سطوح قدرت در سطوح فدرال و محلی و چندین بخش دولتی و خصوصی تشکیل شده است. شکل ۵ سلسله مراتب زیرسطح اختیارات را برای نهادهای فدرال و محلی این کشور نشان می‌دهد:



شکل (۵) سلسله مراتب برای نهادهای فدرال و محلی

همچنین عربستان سعودی گام های مهمی برای ایجاد یک سیاست روشن و مدیریت مستمر تداوم کسب و کار (BCM) در سطح کلان برداشته است. با توجه به نیاز ۲۴×۷ در دسترس بودن عملیات تجاری توسط مؤسسات مالی در پادشاهی عربستان سعودی، بانک مرکزی این کشور با ایجاد SAMA[۱] از منظر حاکمیتی، چارچوب مدیریت تداوم کسب و کار (BCM) را برای سازمان های عضو ایجاد کرده است که قابلیت انعطاف پذیری سازمانی را برای اطمینان از تداوم و در دسترس بودن آنها افزایش می‌دهد. در این چارچوب که در سندی ملی، توسط دولت منتشر شده الزامات مدیریت تداوم کسب و کار بر اساس استانداردهای بین المللی، مانند ISO 22301، ISO 27001 و بهترین تجربه‌ها و دستورالعمل‌های این حوزه تدوین شده است. همچنین در سند مذکور نقشه راهی ارائه شده که در شکل شماره ۶ نمایش داده شده است. نکته مهم و قابل توجه این است که بر اساس این سند(ملی) وزارتخانه‌ها و شرکت‌های این کشور نسبت به تدوین طرح‌ها و برنامه‌های مخصوص حوزه کسب و کار خود اقدام نموده‌اند. از جمله آن وزارتخانه‌ها و شرکت‌ها که حوزه های مختلف از صنایع تا مالی و ... را پوشش می‌دهد میتوان به حوزه ICT کشور عربستان سعودی اشاره نمود که وزارتخانه متولی این حوزه خود سندی راهبردی برای حوزه ICT بر اساس سند ملی تدوین نموده است .این روند در کشور امارات و دیگر کشورهایی که دارای اسناد راهبردی ملی در حوزه مدیریت تداوم کسب و کار هستند وجود دارد.

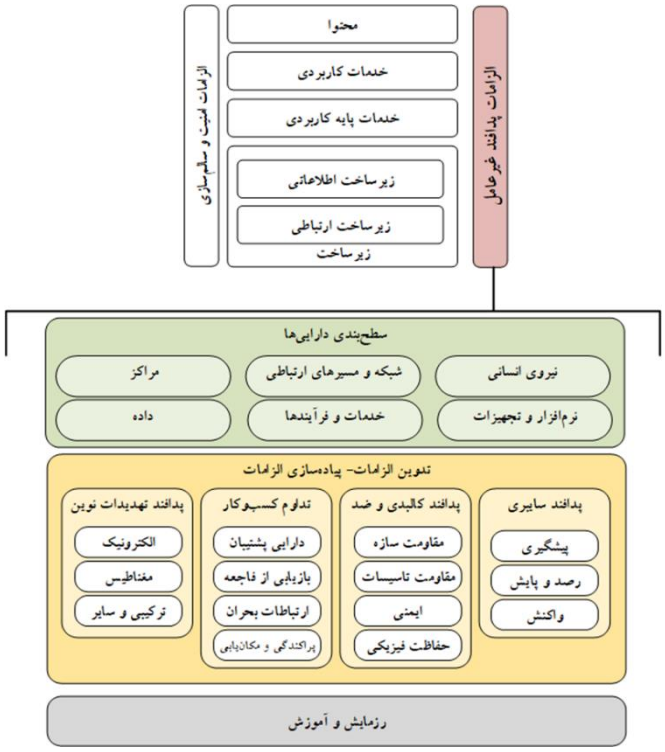
[۱] SAUDI ARABIAN MONETARY AUTHORITY

شکل (۶) نقشه راه مدیریت تداوم کسب وکار در کشور عربستان سعودی

۴-نظام پدافندغیرعامل حوزه ارتباطات و فناوری اطلاعات کشور

همانگونه که در مقدمه این گزارش اشاره شد موضوع تداوم کسب و کار در کشور ما و در اسناد بالادست مانند مصوبات و الزامات پدافند غیرعامل در کشور مورد توجه و تاکید قرار گرفته و برای سازمان‌ها به فراخور ماهیت و اهمیت آن‌ها لازم الاجرا است. لذا هدف از این سند نظام پدافندغیرعامل حوزه فاوای کشور، راهبری و هماهنگی مجموعه سیاست گذاری‌ها، برنامه‌ریزی، اقدامات اجرایی و کنترل و نظارت پدافند غیرعامل در حوزه ارتباطات و فناوری اطلاعات کشور است. به نحوی که موجب، کاهش آسیب‌پذیری، افزایش اطمینان از تداوم فعالیت‌های ضروری، بازدارندگی، تسهیل مدیریت بحران و افزایش پایداری و مصون‌سازی در حوزه زیرساخت و خدمات ارتباطات و فناوری اطلاعات کشور گردد.

در سند پدافند غیرعامل به عنوان یکی از لایه‌های عمودی سند معماری شبکه ملی اطلاعات (مدل مفهومی فضای مجازی کشور در سند طرح کلان و معماری شبکه ملی اطلاعات) به چهار زیر لایه سطح‌بندی دارایی‌ها، تدوین و تبیین الزامات، پیاده‌سازی الزامات، رزمایش و آموزش تقسیم گردیده است.



شکل(۷) معماری الزامات پدافند غیر عامل

لایه تدوین الزامات به ۴ بخش و ۱۴ سر فصل مختلف نگاشت گردیده که بر اساس سطح‌بندی صورت گرفته الزامات باید به صورت شفاف برای تمام سرفصل‌های لایه پیاده‌سازی الزامات تدوین و تبیین گردد.

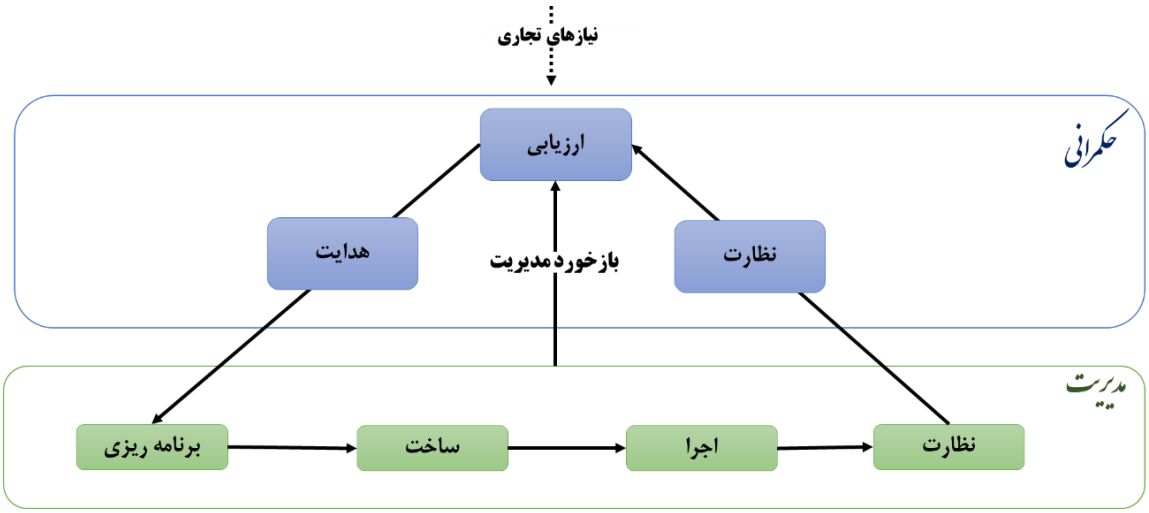
لایه پیاده‌سازی الزامات نیز به ۴ بخش و ۱۴ سر فصل مختلف نگاشت گردیده که بر اساس سطح‌بندی صورت گرفته و الزامات تعیین شده بر بلوک‌های افقی معماری پدافندغیرعامل اعمال می‌گردند. کلیه مجموعه‌ها پس از تعیین سطح دارایی‌های خود و مقایسه وضع موجود با الزامات تعیین‌شده برای سطح مورد نظر، مجموعه اقداماتی را برای دستیابی به استاندارد مطلوب برنامه‌ریزی و اجرا می‌نمایند.

۵- چالش های کلان مدیریت تداوم کسب و کار در سازمان‌های حوزه زیرساخت حیاتی فاوا

۵-۱- حکمرانی در حوزه تداوم کسب و کار

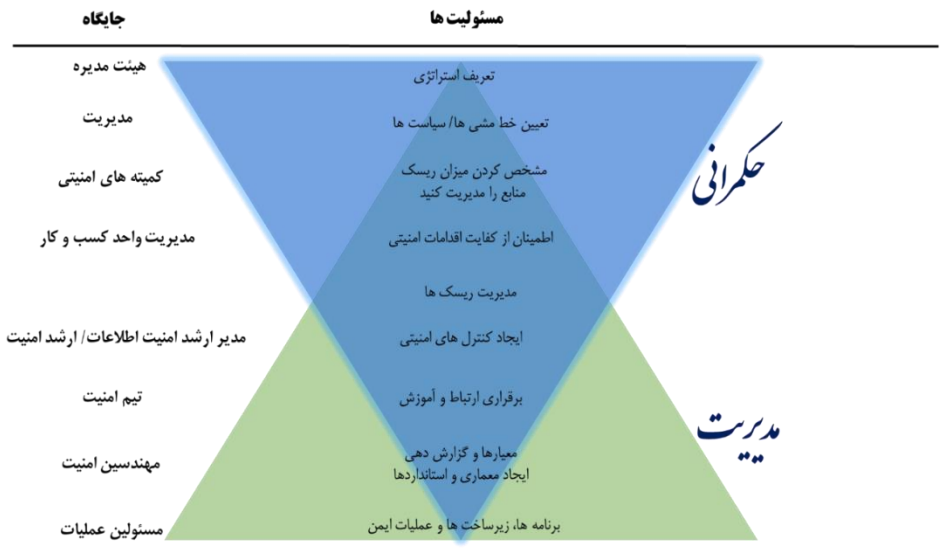
هنگامی که در مورد حکمرانی در تداوم کسب و کار صحبت می‌شود، اغلب آن را با مدیریت یا مدیریت عملیاتی اشتباه می‌گیرند. تفاوت بین مدیریت تداوم کسب و کار و حاکمیت تداوم کسب و کار چندان واضح نیست. برای ساده سازی، مدیریت شامل اجرا و نظارت بر برنامه امنیتی است در حالی که حاکمیت جهت گیری های استراتژیک را فراهم می‌کند و اجرای صحیح آن را تضمین می‌کند. شکل شماره ۸ نشان میدهد که حکمرانی براساس چارچوب CobIT 5 شامل فعالیت هایی مانند ارزیابی ، هدایت و نظارت است. بخش مدیریت نیز شامل فعالیت های مربوط به برنامه تداوم

کسب و کار مانند برنامه ریزی، ساخت، اجرا و نظارت است. بازخورد مدیریت به حاکمیت یکی از نکات کلیدی در این فرآیند است. در واقع این مدیر ارشد است که باید اجرای برنامه و گزارش دادن به نهادهای حاکمیتی را تضمین کند. مدیر ارشد همچنین مسئول ارتباطات دو طرفه با توجه به جهت‌های استراتژیک (یا جهت‌های تجاری جدید مؤثر بر تداوم کسب و کار) و همچنین گزارش شاخص‌های عملیاتی است.



شکل (۸) تمایز بین حاکمیت مدیریت تداوم کسب و کار

همچنین توزیع مسئولیت ها بین حاکمیت و مدیریت نیز در شکل زیر نشان داده شده است.



شکل(۹) توزیع مسئولیت ها بین حاکمیت و مدیریت

نتیجه آنکه موضوع حکمرانی در مدیریت تداوم کسب و کار، موضوعی با اهمیت است که با توجه به تحلیل نتایج و خروجی پیاده سازی مدیریت تداوم کسب و کار در بسیاری از شرکت ها و سازمان‌ها در دنیا مورد توجه قرار گرفته که می‌توان این موضوع مهم را در مقایسه چارچوب‌ها و مدل‌های ارائه شده در یک دهه اخیر مشاهده نمود. از طرفی با

توجه به بررسی و تحلیل اقدامات در سازمان‌های زیرساختی حوزه فاوا در کشور و آنچه در عمل اجرا می‌شود این موضوع به عنوان یک چالش و نکته‌ای که می‌تواند مورد توجه ویژه و بازنگری قرار گیرد مطرح می‌شود.

به نظر می‌رسد داشتن سند راهبردی مدیریت تداوم کسب و کار در سطح ملی برای هر کشوری از جمله کشور ایران حیاتی است. این سند معمولاً رویکرد کشور را برای تضمین تداوم خدمات و عملیات حیاتی در طول یک اختلال یا بحران ترسیم می‌کند. در نظر گرفتن شرایط منحصربه فرد ژئوپلیتیک، اقتصادی و اجتماعی و فرهنگی کشور هنگام طراحی و اجرای استراتژی‌های BCM مهم است. علاوه بر این، با توجه به نقش حیاتی بخش‌های خاص در اقتصاد ایران، مانند حوزه ارتباطات و فناوری اطلاعات، نفت و گاز و ... داشتن استراتژی‌های BCM قوی برای سازمان‌های مرتبط با این بخش‌ها بسیار مهم است. در حالی که داشتن یک سند استراتژیک برای BCM در سطح ملی مهم است، اطمینان از اینکه این سند متناسب با نیازها و شرایط خاص کشور تنظیم شده است، به همان اندازه ضروری است. لذا درتدوین یک سند استراتژیک ملی برای BCM، از جمله یک سند خاص برای حوزه ارتباطات و فناوری اطلاعات، توجه به موضوع حکمرانی، تعیین نقش‌ها، مسئولیت‌ها و وظایف برای مدیریت ریسک‌ها، ایجاد انعطاف‌پذیری و تضمین تداوم خدمات حیاتی در سطح ملی بسیار مهم است. همان اقدامی که کشورهایی چون امارات و عربستان از سال‌های قبل آغاز نموده و از نتایج آن اکنون بهره‌مند می‌گردند.

۵-۲- نگرشی جامع و مانع در مدیریت تداوم کسب و کار

سازمان‌ها به ویژه سازمان‌هایی که در حوزه زیرساخت‌های حیاتی فعالیت و نظارت می‌کنند، شاید نیاز به رویکردی جامع و فراتر به BCM نسبت به طرح های تداوم کسب و کار[۱](BCP) و طرح های بازیابی بلایا [۲](DRP)داشته باشند. همچنین توسعه و اجرای طرح‌های تخصصی مختلف متناسب با ماهیت منحصر به فرد سازمان‌های زیرساخت حیاتی، ضروری است . این استراتژی کل نگر یک پاسخ قوی و موثر به طیفی از اختلالات، از بلایای طبیعی گرفته تا تهدیدات سایبری را تضمین می‌کند و در نتیجه انعطاف پذیری خدمات و عملیات ضروری را تقویت می‌کند. این توضیح به ماهیت چند وجهی BCM می پردازد و بر اهمیت برنامه‌ریزی متنوع برای سازمان‌های زیرساخت حیاتی تأکید می‌کند. این موضوع ممکن است شامل طرح‌هایی مانند، طرح تداوم عملیات [۳]COOP, طرح ارتباطات حادثه (بحران) [۴]CCP, طرح حفاظت از زیرساخت های حیاتی [۵]CIP, طرح واکنش به حوادث سایبری[۶]CIRP, طرح بازیابی بلایا DRP, طرح اضطراری

---

[۱] Business Continuity Plan

[۲] Disaster Recovery Plan

[۳] Continuity of Operations Plan

[۴] Crisis Communications Plan

[۵] Critical Infrastructure Protection

[۶] Cyber Incident Response Plan

سیستم اطلاعاتی[۱]ISCP و طرح اضطراری ساکنین[۲]OEP باشد که هر کدام برای رسیدگی به جنبه‌های خاصی از انعطاف‌پذیری طراحی شده‌اند. باید توجه داشت که ماهیت خدمات ارائه شده توسط سازمان های زیرساخت حیاتی به طور قابل توجهی متفاوت است.لذا تطبیق برنامه‌ها با ماهیت خاص عملیات تضمین می‌کند که عملکردهای حیاتی محافظت می‌شوند و اینگونه اقدامات بازیابی با چالش‌های منحصربه‌فرد ایجاد شده توسط هر بخش همسو می‌شوند.

.

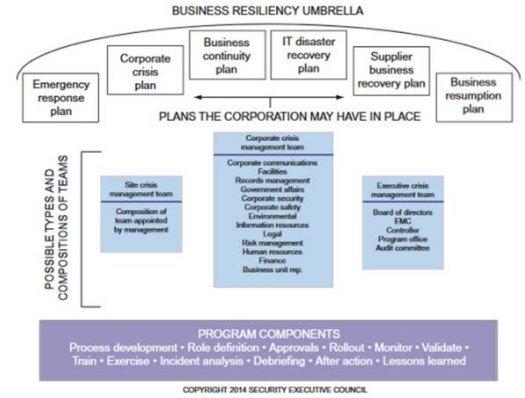


Figure 2.1 The corporate contingency planning umbrella. Copyright 2014 The Security Executive Council. All rights reserved.

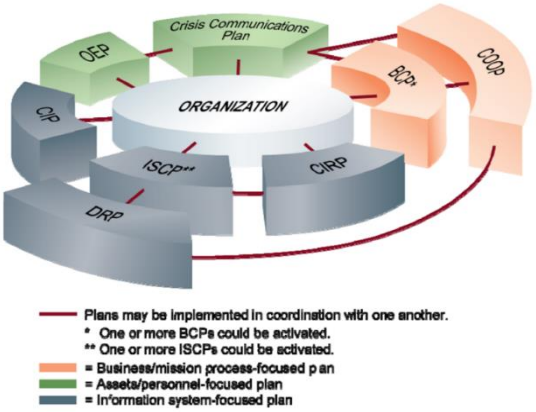


Figure 2-1: Contingency-Related Plan Relationships

شکل (۱۰)روابط طرح ها و برنامه ها (NIST)و چتر تاب‌آوری کسب و کار

از طرفی مانع بودن، نشان‌دهنده اهمیت هماهنگی طرح‌ها و استراتژی‌های مدیریت تداوم کسب و کار با ماهیت خاص سازمان است. ضرورت مانع بودن به این معناست که باید طرح‌ها و استراتژی‌ها با ماهیت دقیق و نیازهای سازمان همخوانی داشته باشند یا ممکن است، یک سازمان با زیرساخت‌های حیاتی فیزیکی، مانند نیروگاه‌ها یا شبکه‌های ارتباطی، نیاز به طرح‌ها و استراتژی‌های خاص‌تری داشته باشد تا در مواجهه با تهدیدات محیطی و فناوری‌های متغیر عملکرد موثری داشته باشد. برنامه‌ریزی جامع و کلان در این زمینه نه تنها باید به تداوم عملیات سازمان اطمینان دهد بلکه باید با ویژگی‌ها و نیازهای خاص هر سازمان هماهنگ باشد. برخی سازمان‌ها ممکن است به دلیل نوع فعالیت یا ساختار خود به طرح‌های مربوط به امنیت فیزیکی نیاز کمتری داشته باشند. در این حالت، هماهنگی با ماهیت سازمان و تطبیق برنامه‌ها با ویژگی‌های خاص عملیات آن امری ضروری است.

۵-۳- تحلیل تأثیر کسب و کار

تحلیل تأثیر کسب و کار در واقع یک گام اساسی و حیاتی در فرآیند مدیریت تداوم کسب و کار (BCM) است. هدف از BIA[۳] شناسایی و ارزیابی تأثیر بالقوه اختلالات بر عملکردها و فرآیندهای تجاری حیاتی سازمان است. تحلیل

---

[۱] Information System Contingency Plan

[۲] Occupant Emergency Plan

[۳] Business Impact Analysis

تأثیر کسب و کار شامل ارزیابی پیامدهای مالی، عملیاتی، اعتباری و نظارتی اختلالات، کمک به اولویت‌بندی تلاش‌های بازیابی و تخصیص مؤثر منابع است.در زمینه زیرساخت های حیاتیکه در آن عملیات بی وقفه خدمات بسیار مهم است، چالش های مرتبط با انجام BIA می تواند قابل توجه باشد. از جمله زیرساخت های حیاتی اغلب شامل عملیات پیچیده و به هم پیوسته هستند. شناسایی و درک وابستگی های متقابل در بین فرآیندها و سیستم‌های مختلف می تواند چالش برانگیز باشد. همچنین سازمان‌های زیرساخت حیاتی، مانند آنهایی که در بخش‌های ارتباطات یا انرژی هستند، معمولاً طیف وسیعی از خدمات را ارائه می کنند. ارزیابی تأثیرات بالقوه کسب و کار در خدمات متنوع نیازمند درک جامعی از اهمیت هر خدمت است. از طرف دیگر این سازمان‌های زیرساخت حیاتی اغلب با سایر سازمان‌ها، تامین کنندگان و ذینفعان در ارتباط هستند. ارزیابی اثرات بالقوه اختلالات در این روابط بسیار مهم است که به دلیل شبکه پیچیده وابستگی ها می تواند چالش برانگیز باشد. همچنین زیرساخت های حیاتی به شدت به منابع خاصی مانند پرسنل ماهر، تجهیزات تخصصی یا فناوری حیاتی متکی است. درک وابستگی به این منابع و ارزیابی تأثیر در دسترس نبودن آنها یکی از جنبه های کلیدی BIA است.

در پایان از آنجایی که پیامدهای اختلال در زیرساخت های حیاتی می تواند شدید باشد و پیامدهایی برای امنیت عمومی، امنیت ملی و اقتصاد داشته باشد، ارزیابی دقیق اثرات کسب و کار از اهمیت بسیار بالایی برخوردار بوده و خود زمینه ساز و آغاز گر طرح‌ها و برنامه‌هایی است که به آن‌ها اشاره شد.

۵-۴- ارزیابی ریسک

ارزیابی ریسک در مدیریت تداوم کسب و کار شامل ارزیابی تهدیدها، آسیب‌پذیری‌ها و اثرات بالقوه برای شناسایی و اولویت‌بندی ریسک‌هایی است که می‌توانند عملیات عادی کسب وکار را مختل کنند. ارزیابی می تواند بر اساس دارایی ها، سناریوها یا هر دو، بسته به اهداف سازمان، استانداردهای صنعتی و ویژگی های خاص زیرساخت حیاتی مورد نظر انجام شود. ***موضوع مهمی که در اغلب سازمان ها. و در تجربیات عملی در اجرای پروژه‌های زیرساختهای حیاتی بعنوان چالشی بزرگ با آن مواجه هستیم.***

در رویکرد مبتنی بر دارایی، تمرکز بر ارزیابی ریسک های مرتبط با دارایی ها یا اجزای خاص درون سازمان است. دارایی‌ها ممکن است شامل دارایی‌های فیزیکی (مانند ساختمان‌ها، تجهیزات)، دارایی‌های اطلاعاتی (مانند داده‌ها، نرم‌افزار)، دارایی‌های انسانی (مانند کارمندان) و موارد دیگر باشد. این رویکرد زمانی مناسب است که علاوه بر محدودیت تعداد دارایی ها، نیاز به اولویت بندی حفاظت از دارایی های خاص به دلیل بحرانی بودن آنها برای عملیات وجود داشته باشد. به عنوان مثال، یک موسسه مالی ممکن است حفاظت از پایگاه های داده مشتریان یا سیستم‌های تراکنش مالی را در اولویت قرار دهد. این همان چیزی است که در سند و نظام نامه پدافند به آن اشاره شده است اما سازمان‌های زیرساخت حیاتی از احصاء آن عاجز هستند و الگو و چارچوب مشخصی برای آن نداشته یا در صورت وجود چارچوب به دلایل مختلف به آن عمل ننموده‌اند یا بطور کامل و صحیح صورت نپذیرفته است.

در رویکرد مبتنی بر سناریو، تأکید بر ارزیابی ریسک های مربوط به فرآیندهای حیاتی است که از اهداف سازمان پشتیبانی می کند. این رویکرد وابستگی‌های متقابل بین فرآیندهای مختلف را در نظر می گیرد و ارزیابی می کند که چگونه اختلالات می‌توانند بر عملیات کلی کسب‌وکار تأثیر بگذارند و تا زمانی ارزشمند است که درک تداوم سرتاسری فرآیندهای حیاتی کسب و کار مد نظر باشد. به عنوان مثال، در یک سازمان زیرساخت ارتباطی، ارزیابی ممکن است بر روی فرآیندهایی مانند مدیریت شبکه، ارائه خدمات، و پاسخ به حادثه متمرکز شود تا از عملکرد یکپارچه خدمات ارتباطی اطمینان حاصل شود.

در نهایت برخی از سازمان ها با در نظر گرفتن دارایی ها و فرآیندها در ارزیابی ریسک خود، رویکرد ترکیبی را انتخاب می‌کنند. این اقدام اجازه می‌دهد تا درک جامعی از خطرات، با در نظر گرفتن بحرانی بودن دارایی ها و به هم پیوستگی فرآیندها بوجود آید. این رویکرد اغلب برای زیرساخت های حیاتی مانند ارتباطات و فناوری اطلاعات مفید است. برای مثال، یک رویکرد ترکیبی ممکن است شامل ارزیابی ریسک‌های مرتبط با تجهیزات شبکه‌ای خاص (مبتنی بر دارایی های محدود) و در نظر گرفتن اینکه چگونه شکست این دارایی‌ها می‌تواند بر فرآیندهای ارتباطی حیاتی (مبتنی بر سناریو) تأثیر بگذارد، باشد.

انتخاب روش ارزیابی ریسک در زیرساخت های حیاتی باید بر اساس نیازهای خاص سازمان، اهداف و ماهیت زیرساخت باشد. یک رویکرد متفکرانه و خاص، با در نظر گرفتن دارایی‌ها و سناریوها در صورت لزوم، توانایی سازمان را برای شناسایی و کاهش خطرات به طور موثر افزایش می‌دهد. ***اما وقتی صحبت از زیرساخت های حیاتی مانند زیرساخت های ارتباطی و فناوری اطلاعات می‌شود، روش های ارزیابی ریسک باید ویژگی های منحصر به فرد این بخش ها را در نظر بگیرند. برای مثال، فرآیند ارزیابی ریسک برای حفاظت از زیرساخت‌های حیاتی شامل بررسی آسیب‌پذیری‌های زیرساخت، وابستگی‌های متقابل، شکاف‌ها و پیامدهای اختلال در آنها می‌شود.***

ENISA در گزارش چارچوب مدیریت ریسک خود در سال ۲۰۲۲ به مقایسه چارچوب ها و مدل های مطرح ارزیابی ریسک پرداخته و آن‌ها را با هم مقایسه نموده است که در شکل ۱۱ آورده شده است.

شکل (۱۱) مقایسه چارچوب ها و مدل های مطرح ارزیابی ریسک

۶-جمع بندی و پیشنهادات

مدیریت تداوم کسب و کار یک فرآیند حیاتی برای اطمینان از انعطاف پذیری و پایداری سازمان‌های زیرساخت حیاتی است. با این حال، چالش‌ها و مشکلات متعددی وجود دارد که مانع اجرای موثر آن می‌شود همچنین سازمان‌های زیرساخت حیاتی در حوزه فاوا در کشور با چالش های چند وجهی در مدیریت تداوم کسب و کار خود مواجه هستند. ازجمله، حاکمیت نادیده گرفته شده در مدیریت تداوم کسب و کار با فقدان برنامه‌ریزی متوازن در تدوین طرح ها و برنامه‌های مرتبط، نیاز به یک رویکرد جامع و کامل را در مدیریت تداوم کسب و کار طلب می‌کند. همچنین تطبیق برنامه‌ها با تفاوت‌های عملیاتی برای محافظت از عملکردهای حیاتی و اطمینان از همسویی اقدامات بازیابی با چالش‌های منحصر به فرد بسیار مهم است. علاوه بر این، رعایت توالی عناصر BCM، همانطور که توسط استانداردهایی مانند ISO 22313 تاکید شده است، حیاتی است. نادیده گرفتن مراحل اساسی مانند تجزیه و تحلیل تأثیر کسب و کار و ارزیابی ریسک، اثربخشی برنامه‌های تداوم کسب و کار را به خطر می اندازد و بر اهمیت درک جامع از اختلالات احتمالی برای فعالیت‌های سازمانی تأکید می‌کند. درپایان میتوان نتیجه گرفت که پرداختن به این چالش ها نیازمند یک رویکرد استراتژیک و متناسب برای مدیریت تداوم کسب و کار در چشم انداز زیرساخت های حیاتی کشور است.

۷- مراجع

1 ISO/TS 22317:2021:Security and resilienceBusiness continuity management systemsGuidelines for business impact analysis :https://www.iso.org/standard/79000.html

2 ISO 22313:2020: Security and resilience Business continuity management systems Guidance on the use of ISO 22301:https://www.iso.org/standard/75107.html

3 ISO 22301:2019: Security and resilience Business continuity management systems Requirements https://www.iso.org/standard/75106.html

4 ISO 22316:2017:Security and resilience Organizational resilience Principles and attributes https://www.iso.org/standard/50053.html

5 NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems 2010

6 ENISA : INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK Methodology for ssessment of interoperability among risk management frameworks .2022

7 Abu Bakar, Z., Azbiya Yaacob, N., Mohamed Udin, Z., Rajeh Hanaysha, J. and Loon, K-L. (2017), "The Adoption of Business Continuity Management Best Practices Among Malaysian Organizations", Advanced Science Letters, Vol 23 No 9, pp. 8484-8491.

8 Risk Management Framework for Information Systems and Organizations. NIST Special Publication 800-37.2018

9 Hadavi A, Bakhtiari H, Torabi A, (2022), Identifying the main success factors of business continuity management in the petrochemical industry: a factor analysis approach, Vol 10, No 2022

10 Yasaman Maboudian and Kamran Rezaie, Business continuity management in Iran industries - a survey of different sectors, International Journal of Business Continuity and Risk Management, 2014, vol. 5, issue 4, 306-322

11 Fallahi, A., Arzhangi, S. (2011). Business Continuity after the 2003 Bam Earthquake in Iran. In: Kim, Th., et al. Software Engineering, Business Continuity, and Education. ASEA 2011. Communications in Computer and Information Science, vol 257. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27207-3_58

12 S.A. Torabi, H. Rezaei Soufi, Navid Sahebjamnia, A new framework for business impact analysis in business continuity management (with a case study) 2014 Elsevier Ltd. All rights reserved.

نشانی: تهران، انتهای کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات، معاونت پژوهش و توسعه ارتباطات علمی

تلفن: ۰۲۱-۸۸۶۳۰۳۵۵

نمابر: ۰۲۱-۸۸۶۳۰۳۵۶