INSO-ISO-IEC-TR
27031
1st. Edition
Identical with
ISO/IEC TR
27031:2011
Aug.2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ایران-ایزو-آی‌ای‌سی-تی آر
۲۷۰۳۱
چاپ اول
شهریور ۱۳۹۲

فناوری اطلاعات- فنون امنیتی –

راهنماهایی برای آمادگی فناوری اطلاعات

و ارتباطات به منظور تداوم کسب و کار

Information technology— Security techniques — Guidelines for information and communication technology readiness for business continuity

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ 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 وکوششی 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 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 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت 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 شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] 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 بین‌المللی بهره‌گیری می‌شود .

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 بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (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 of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات – فنون امنیتی – راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به منظور تداوم کسب و کار»

رئیس:	**سمت و/یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	دبیر تدوین و مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا : (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانیان همت، بهزاد (لیسانس مهندسی برق الکترونیک)	مترجم و کارشناس انتشارات قدیس
سعیدی، عذرا (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
عسگرزاده، مجید (فوق لیسانس مهندسی کامپیوتر)	مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات ، دانشجو دکتری کامپیوتر
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم

	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	
فیاضی، مهدی (لیسانس مهندسی برق الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
معروف، سینا (لیسانس مهندسی کامپیوتر- سخت‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رییس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات ایران
مهدوی اردکانی، علیرضا (فوق لیسانس مدیریت فناوری اطلاعات)	شرکت داده پردازان آبشار
موجبی، محمود (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناصری، علی (دکتری برق مخابرات)	عضو هیأت علمی دانشگاه امام حسین (ع)

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات – فنون امنیتی – راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به منظور تداوم کسب و کار» که پیش‌نویس آن در کمیسیون‌های مربوط به وسیله سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در دویست و سومین اجلاس کمیته‌ی ملی استاندارد رایانه و فراوری داده ها مورخ ۱۳۹۱/۷/۲۴ مورد تصویب قرارگرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهاد 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 تجدید نظر استانداردهای ملی استفاده کرد.

منابع و مآخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC TR 27031:*2011, Information technology— Security techniques — Guidelines for information and communication technology readiness for business continuity*

• مقدمه

در طی سالیان، فناوری اطلاعات و ارتباطات (ICT)[1] به قسمت عمده ای از بسیاری از فعالیت‌های زیر ساخت‌های بحرانی در تمامی قسمت‌های سازمانی چه عمومی، خصوصی داوطلبانه، تبدیل شده است.
رشد سریع اینترنت و دیگر خدمات شبکه الکترونیکی و قابلیت‌های امروزه سامانه‌ها و کاربردها، موجب شده است که سازمان ها بیش از پیش به زیر ساخت‌های ICT قابل اطمینان و امن تکیه زنند.
در ضمن، نیاز به مدیریت تداوم کسب کار (BCM)[2]، شامل پیش‌بینی رخداد، طرح بازیابی بحران و مدیریت و پاسخگویی اضطراری، به وسیله‌ی دامنه خاصی از دانش، تخصص و استانداردهای تدوین و منتشر شده در سال‌های اخیر شامل استاندارد بین المللی BCM که توسط ISO/TC223 تدوین شده، شناسایی و پشتیبانی شده است.

یادآوری- کمیته فنی ISO/TC223 در مرحله‌ی تدوین استاندارد بین المللی مدیریت تداوم کسب وکار مربوط است.(ISO22301)

خرابی در خدمات ICT، از جمله وقوع معضلات امنیتی نظیر نفوذ به سامانه‌ها و آلودگی به بدافزارها، بر تداوم عملیات کسب و کار اثر خواهد گذاشت. بنابراین مدیریت ICT و تداوم مرتبط و سایر جنبه‌های امنیتی، قسمت کلیدی الزامات تداوم کسب وکار را تشکیل می‌دهد. علاوه بر این در بحث‌های کلان، فعالیت‌های کسب و کار بحرانی که نیازمند تداوم کسب وکار هستند، معمولا وابسته به ICT هستند. این وابستگی‌ها به این معناست که اختلال در ICT می‌تواند باعث ایجاد مخاطره‌های راهبردی در شهرت سازمان وتوانایی‌ش در فعالیت گردد.
آمادگی ICT از اجزای ضروری برای بسیاری از سازمان‌ها در پیاده‌سازی مدیریت امنیت اطلاعات و مدیریت تداوم کسب وکار است. به عنوان قسمتی از پیاده‌سازی و اجرای سامانه مدیریت امنیت اطلاعات (ISMS)[3] مشخص شده در(استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷) و متناظر در سامانه مدیریت تداوم کسب وکار (BCMS)[4]، تدوین وپیاده‌سازی طرح آمادگی برای خدمات ICT برای مساعدت برای اطمینان از تداوم کسب وکار مهم است. در نتیجه BCM اثر بخش، به آمادگی ICT اثر بخش، به منظور اطمینان از این‌که اهداف سازمان در زمان‌های وقفه می‌تواند ادامه داشته باشد، وابسته است.
این مورد به خصوص از این جهت مهم است که غالبا در نتیجه وقفه در ICT مواجه با پیچیدگی‌های افزوده غیر قابل تشخیص و یا به دشواری قابل تشخیص هستیم.
به منظور آمادگی ICT سازمان برای تداوم کسب وکار (IRBC)[5] سازمان که فرآیندی نظام یافته را به منظور

---

1 - Information and Communication Technology
2 - Business Continuity Management
3 - Information Security Management System
4 - Business continuity Management System
5 - ICT Readiness for Business Continuity

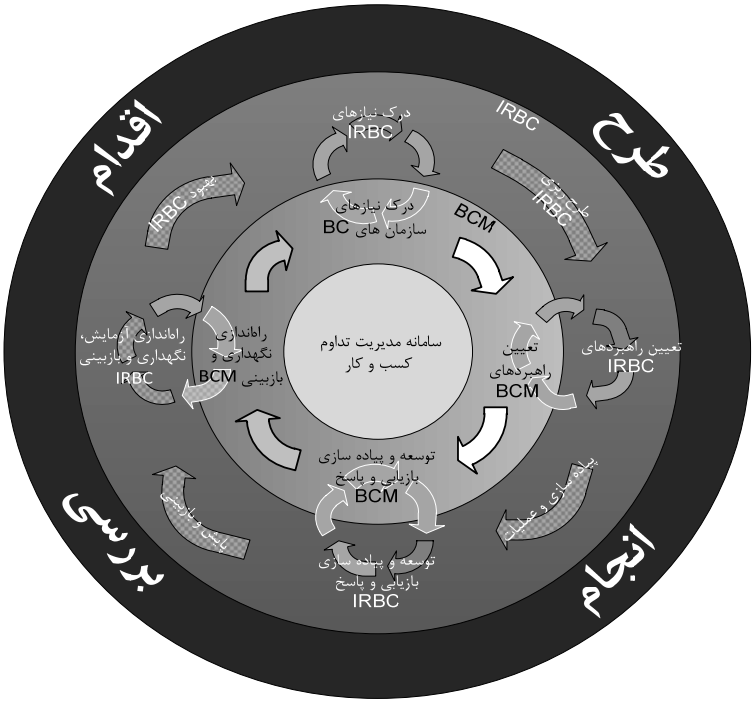
جلوگیری، پیش‌بینی و مدیریت وقفه ICT و رخداد که پتانسیل ایجاد وقفه خدمات ICT را دارد، به انجام رساند. که این می‌تواند با به کارگیری مراحل چرخه ای طرح -اجرا-بررسی- اقدام – (PDCA)[1] به عنوان قسمتیاز سامانه مدیریت در IRBC ICT، بهتر حاصل شود. در این روش IRBC، BCM از طریق اطمینان از این‌که خدمات ICT به طور مقتضی قابل بازگشت هستند و می‌تواند برای سطوح از پیش تعیین شده مطابق با مقیاس زمانی مورد نیاز وتوافق با سازمان بازیابی شوند، پشتیبانی می‌نماید.

جدول۱- چرخه درطرح-اجرا-بررسی-اقدام IRBC

طرح	برقراری خط مشی IRBC، اهداف، مقاصد، فرآیندها وروش‌های اجرایی تداوم کسب وکار مرتبط با مدیریت مخاطره‌ها وبهبود آمادگی ICT به منظور حصول نتایجی مطابق با خط مشی‌ها و اهداف کلان یک سازمان
اجرا	پیاده‌سازی واجرا خط مشی، کنترل‌ها، فرآیندها و روش‌های اجرایی IRBC
بررسی	ارزیابی و در موارد مقتضی سنجش کارایی فرآیند مطابق با خط مشی اهداف وتجارب عملی IRBC و گزارش نتایج به مدیریت به منظور بازنگری
اقدام	انجام اقدامات اصلاحی و پیشگیرانه بر مبنای بازنگری مدیریت به منظور دست‌یابی به بهبود مداوم در IRBC

اگر سازمانی از استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، برای استقرار ISMS و یا استانداردهای مرتبط برای برقراری BCMS استفاده می‌کند، استقرار IRBC ترجیحاً ملاحظات موجود یا فرآیندهای خواسته شده مرتبط با این استانداردها را باید در نظر بگیرد. این ارتباط‌دهی می‌تواند از برقراری IRBC پشتیبانی نماید و همچنین از فرآیندهای دوگانه برای سازمان‌ها جلوگیری نماید. شکل ۱ اثر متقابل IRBC و BCMS را به طور خلاصه بیان می‌نماید.

1 - Plan-Do-Check-Act



شکل ۱: تجمیع IRBC و BCMS

در طرح‌ریزی و پیاده‌سازی IRBC سازمان می‌تواند به ISO/IEC 24762:2008 برای طرح‌ریزی و تحویل خدمات بازیابی بحران ICT مراجعه نماید، صرف نظر از این‌که به هرحال آن خدمات توسط فروشنده برون-سپاری شده یا داخلی در سازمان فراهم شده باشد.

فناوری اطلاعات-فنون امنیتی- راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به منظور تداوم کسب و کار

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، توصیف اصول و مفاهیم آمادگیICT برای تداوم کسب و کار و همچنین ارائه چارچوبی از روش‌ها و فرآیندها به منظور شناسایی و تعیین تمامی جنبه‌ها(مانند معیارهای کارایی، طراحی و پیاده‌سازی) برای بهبود آمادگی ICT سازمان جهت اطمینان از تداوم کسب و کار است. این استاندارد برای هر سازمانی (خصوصی، دولتی، غیر دولتی، بدون در نظر گرفتن اندازه) که در حال توسعه آمادگی ICT خود برای برنامه تداوم کسب وکار (IRBC)، والزامات خدمات ICT آن به خدمات/ زیر ساخت‌ها برای آمادگی پشتیبانی از عملیات کسب و کار در رویدادی از رویدادهای نوظهور و رخدادها و اختلالات مربوطه که می‌توانند روی تداوم‌های (شامل امنیت) بحرانی کسب و کار تأثیر بگذارند، کاربرد دارد. همچنین این استاندارد به سازمان اجازه می‌دهد تا پارامترهای کارایی که به IRBC آن، در شیوه‌ای سازگار و تشخیص داده شده اندازه‌گیری کند.

دامنه کاربرد این استاندارد جهانی، تمامی رخدادها و رویدادها (شامل مسایِل امنیتی مربوطه) را در بر می‌گیرد که می‌تواند اثری در زیرساخت‌ها و سامانه‌های ICT داشته باشد. همچنین این، شیوه‌های ساماندهی رخداد امنیت اطلاعات و مدیریت و خدمات و طرح‌ریزی ICT را تعمیم داده و در بر می‌گیرد.

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 مدرکی 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 :

۲-۱ استاندارد ملی ایران به شماره ۱۸۰۴۴: سال ۱۳۸۹، *فناوری اطلاعات - فنون امنیتی- مدیریت رویداد امنیت اطلاعات*

۲-۲ استاندارد ملی ایران به شماره ۲۷۰۰۰: سال ۱۳۹۰، *فناوری اطلاعات- تکنیک های امنیتی- سیستم های مدیریت امنیت اطلاعات- قسمت بررسی و واژگان*

۲-۳ استاندارد ملی ایران به شماره ۲۷۰۰۱: سال۱۳۸۷، *فناوری اطلاعات- تکنیک های امنیتی- سیستم های مدیریت امنیت اطلاعات- قسمت نیازها*

۲- ۴ استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷، *فناوری اطلاعات-تکنیک های امنیتی- نظام نامه شیوه مدیریت امنیت اطلاعات*

۲-۵ استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۸۸، *فناوری اطلاعات- تکنیک های امنیتی- مدیریت مخاطره امنیت اطلاعات*

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می رود:

۳-۱

پایگاه جایگزین[1]

مکان عملیاتی جایگزین منتخب توسط سازمان تا هنگامی که عملیات کسب و کار عادی را پس از وقوع یک اختلال نمی‌توان با استفاده از محل عادی انجام عملیات انجام داد، مورد استفاده قرار می‌گیرد.

۳-۲

مدیریت تداوم کسب و کار (BCM)

فرآیند مدیریت فراگیری است که تهدیدات بالقوه را برای یک مجموعه شناسایی کرده و پیامدهای آن را برعملیات کسب و کار بررسی کند و یک چارچوب جهت ایجاد امکان‌بازگشت سازمانی با قابلیت پاسخ مؤثر که از منافع سهام‌داران اصلی، اعتبار، نام تجاری و فعالیت‌های ارزش زا حراست می‌کند.

۳-۳

طرح تداوم کسب و کار (BCP)[2]

روال‌های مستند شده که سازمان‌ها را برای پاسخ، بازیابی، ادامه حیات و بازگشت به یک سطح عملیاتی از پیش تعیین شده پس از اختلال، راهنمایی می‌کند.

یاد آوری- به گونه‌ای این شامل منابع، خدمات و فعالیت‌های مورد نیاز برای اطمینان از استمرار کارکردهای بحرانی کسب و کار می‌باشد.

۳-۴

تحلیل اثر کسب و کار (BIA)[3]

فرآیند تحلیل کارکردهای عملیاتی و اثراتی که یک اختلال ممکن است بر آن‌ها داشته باشد.

1 - Alternate Site
2 - Business Continuity Plan
3 - Business Impact Analysis

۵-۳

بحراني

توصیفی کیفی برای نشان دادن اهمیت یک منبع، فرآیند یا کارکرد که باید بطور دائم در دسترس و عملیاتی باشند یا در کوتاه‌ترین زمان پس از وقوع یک رخداد، مواقع ضروری یا فاجعه در دسترس و عملیاتی باشند.

۶-۳

اختلال

رخداد، خواه قابل پیش بینی (مانند طوفان) خواه غیر قابل پیش‌بینی (مانند قطع برق، زلزله، یا حمله به زیرساخت‌ها / سامانه‌های ICT) که روند عادی عملیات در محل سازمان را مختل می‌کند.

۷-۳

بازيابي فاجعه ICT

توانایی عناصر ICT یک سازمان برای پشتیبانی کارکردهای بحرانی کسب وکار برای بازگشت به یک سطح قابل قبول در یک بازه زمانی از پیش تعیین شده پس از اختلال.

۸-۳

طرح بازيابي فاجعه ICT (ICT DRP) [1]

طرح به طور وضوح مستند شده و تعریف شده‌ای که توانایی‌های ICT را وقتی اختلال رخ می‌دهد بازیابی می‌کند.

یادآوری- در بعضی از سازمان‌ها طرح تداوم ICT نام دارد.

۹-۳

حالت خرابی

شیوه ای که توسط آن یک خطا شناسائی می شود

یادآوری- به طور کلی راه وقوع خرابی و پیامد آن روی عملکرد سامانه را توصیف می‌کند.

۱۰-۳

آمادگی ICT براي تداوم کسب و کار (IRBC)

توانمندی یک سازمان برای حمایت عملیات کسب و کار به وسیله پیش گیری، شناسایی و واکنش به اختلال و بازیابی خدمات ICT.

1 - ICT Disaster Recovery Plan

۳-۱۱

کمینه هدف تداوم کسب و کار (MBCO)

کمینه سطح خدمات و/یا محصولات که در طول یک اختلال برای سازمان به منظور رسیدن به اهداف کسب و کار قابل قبول باشد.

۳-۱۲

نقطه بازیابی آرمانی (هدف) (RPO)

زمانی مشخص که اطلاعات بعد از یک اختلال باید به آن زمان بازیابی شود

۳-۱۳

زمان بازیابی آرمانی (هدف) (RTO)

بازه زمان بعد از وقوع اختلال که در آن مدت کمینه سطوح خدمات و/یا محصولات و سامانه‌های پشتیبانی، برنامه‌های کاربردی یا کارکردها باید بازیابی شوند.

۳-۱۴

امکان‌بازگشت

توانایی یک سازمان برای مقاومت در برابر تأثیرات بوجود آمده توسط یک اختلال.

۳-۱۵

چکانش

رویدادی که باعث شروع یک واکنش در یک سامانه می‌شود.

یادآوری- همچنین رویداد چکانیدن نامیده می‌شود.

۳-۱۶

سابقه حیاتی

سابقه الکترونیکی یا کاغذی که برای حفظ، ادامه یا بازسازی عملیات یک سازمان و حفاظت از حقوق سازمان، کارمندان، مشتریان و ذی‌نفعان ضروری است.

۴ کوته‌نوشت‌ها

IRBC	ICT Readiness for Business Continuity	آمادگی ICT برای تداوم کسب و کار
ISMS	Information Security Management System	سامانه مدیریت امنیت اطلاعات

۵ مرور کلی

۵-۱ نقش IRBC در مدیریت تداوم کسب و کار

مدیریت تداوم کسب و کار (BCM) فرآیندی مدیریتی فراگیر است که پیامدهای بالقوه‌ای را شناسایی می‌کند که تهدید است برای یک تداوم سازمانی از فعالیت‌های کسب و کار و ارائه چارچوبی برای برقراری امکان‌بازگشت و توانایی برای یک پاسخ مؤثر که تأمین اعتبار سازمان از اختلال‌ها است، ارائه می دهد.

به عنوان قسمتی از فرآیند BCM، IRBC همانند یک سامانه مدیریتی عمل می‌کند که به عنوان یک عامل مکمل و پشتیبانی‌کننده BCM یک سازمان و/یا برنامه ISMS آمادگی سازمان را برای موارد زیر افزایش می‌دهد:

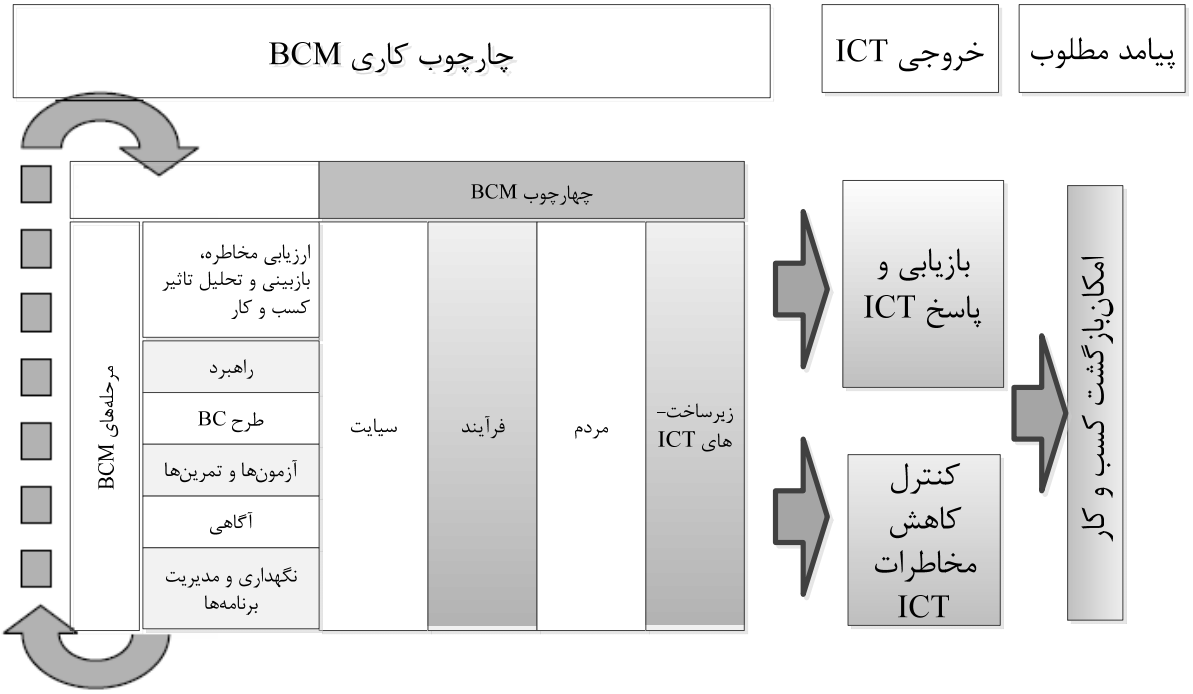
الف) برخورد با تغییر مداوم مخاطره‌ها محیط؛

ب) حصول اطمینان از تداوم عملیات بحرانی کسب و کار و به وسیله خدمات ICT انجام می گردد (پشتیبانی می گردد)؛

پ) آمادگی برخورد قبل از وقوع وقفه در خدمات ICT به محض شناسایی یک یا تعدادی از وقایع مرتبط که به رخدادها تبدیل شده است؛ و

ت) برخورد و بازیابی از خرابی و رخداد/بلای طبیعی؛

شکل۲ خروجی مطلوب ICT را برای پشتیبانی فعالیت‌های مدیریتی تداوم کسب و کار نشان می‌دهد



شکل۲- چارچوب مدیریت تداوم کسب و کار و ارتباطات آن با خروجی ICT و پی آمد مورد انتظار

استاندارد بین المللی BCM به وسیله ISO/TC 223 تهیه و تدوین شده است تا بتواند پیشگیری از حوادث و واکنش و بازیابی از رخدادها را ممکن سازد. فعالیت‌های BCM که شامل آمادگی رخداد، مدیریت تداوم عملیات، طرح بازیابی از بحران (DPR[1]) وکاهش مخاطره‌ها است، بر روی رشد امکان‌بازگشت سازمان تمرکز دارد و آن را برای پاسخ مؤثر به رخدادها و بهبود در درون بازه‌های زمانی از پیش تعیین شده آماده می‌کند.
از این رو یک سازمان اولویت های BCM خود را تنظیم کرده که آن مجموعه فعالیت های IRBC را مشخص می کند. به نوبه خود BCM متکی به IRBC است، به منظور رسیدن به اطمینان از اینکه سازمان می تواند اهداف مستمر خود را در تمام زمان و به خصوص در طول دوره اختلال بررسی کند.

همان طور که در شکل ۳ نشان داده شده است، چنین فعالیت‌های آمادگی برای مقاصد زیر انجام می‌شود :

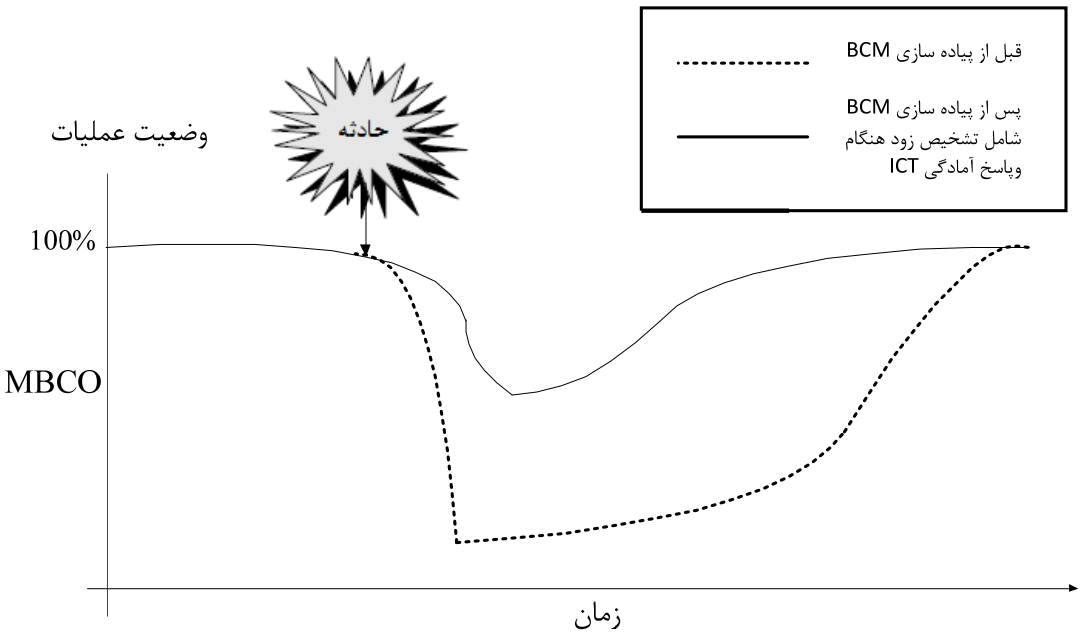
الف) بالا بردن ظرفیت شناسایی بحران و رخداد؛

ب) پیشگیری یک خرابی ناگهانی یا شدید؛

پ) کاهش قابل قبول موارد عملیاتی که در آن ممکن است خرابی غیر قابل مهار باشد؛

ت) کاهش زمان بازیابی؛ و

ث) پایین آوردن میزان اثر پس از وقوع رخداد؛



شکل ۳- مفهوم آمادگی ICT برای تداوم کسب و کار

1 - Disaster Recovery Planning

۲-۵ اصول IRBC

آمادگی ICT برای تداوم کسب و کار (IRBC) در پیرامون عوامل کلیدی و اصولی زیر استوار است

الف) پیشگیری از رخداد: حفاظت خدمات ICT از تهدیدها ازقبیل اشکالات سخت‌افزاری و محیطی، خطاهای عملیاتی، حمله مخرب وبلاهای طبیعی، امری بحرانی به منظور نگهداری سطح‌های مطلوب دسترس‌پذیر سامانه‌ها برای یک سازمان است؛

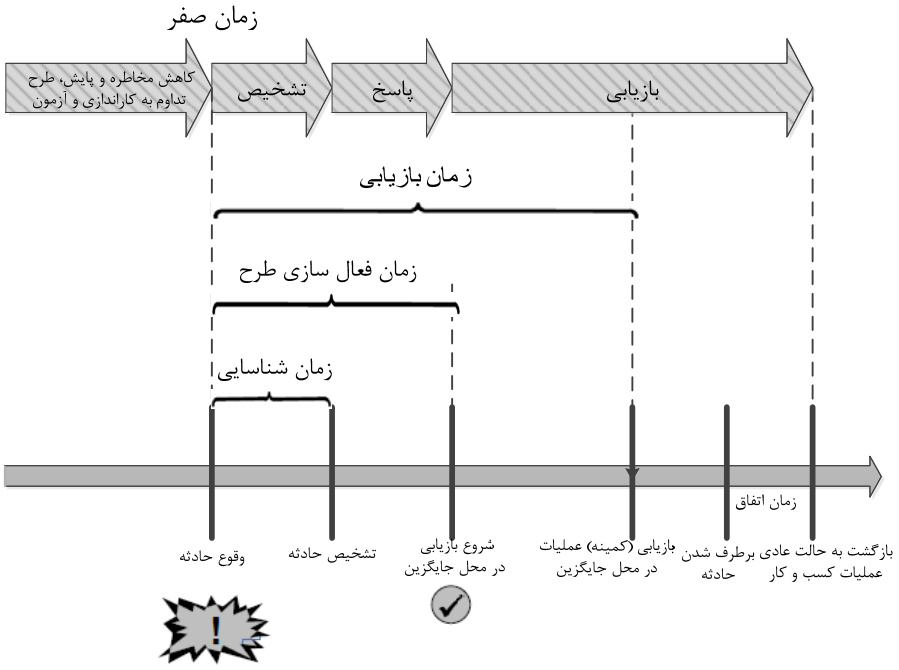
ب) تشخیص رخداد: تشخیص رخداد در کوتاهترین مدت، پیامد خدمات را کمینه و زمان بازیابی را کاهش و کیفیت خدمات حفظ می‌کند؛

پ) پاسخ: پاسخ به یک رخداد به مناسبترین روش، باعث می‌شود تا بازیابی بهتر شود و زمان از کار افتادگی کمینه شود. پاسخ ضعیف می‌تواند منجر به افزایش یک رخداد جزیی به چیزی جدی شود؛

ت) بازیابی: شناسایی و پیاده‌سازی راهبرد بازیابی مناسب سبب حصول اطمینان از سرآغاز دوباره خدمات وحفظ تمامیت داده‌ها می‌شود. درک ویژگی‌های بازیابی اجازه می‌دهد تا خدمات با اولویت بالاتر، ابتدا بازیابی شوند. سپس خدمات با اولویت کمتر اجرا می‌شوند وگاهی اصلا اجرا نمی‌شوند؛ و

ث) رشد و بهبود: درس‌هایی که از اختلالات کوچک و بزرگ آموخته می‌شود باید مستند شود، سپس مورد تحلیل و بازنگری قرار بگیرد. درک این درس‌ها اجازه خواهد داد که سازمان بهتر آماده کنترل و جلوگیری از حوادث اختلالات شود.

شکل۴ چگونگی پشتیبانی و پوشش عنصرهای IRBC مربوط از یک نمونه بازه زمانی بازیابی فاجعه ICT را نشان می‌دهد و به نوبه خود فعالیت‌های تداوم کسب و کار را پشتیبانی می‌کند. اجرای IRBC، سازمان را قادر به پاسخ مؤثر با تهدیدهای جدید و در حال ظهور می‌کند و همچنین قادر به پاسخ و بازیابی از اختلالات خواهد بود.



شکل ۴: اصول IRBC در بازه زمانی بازیابی رخداد عادی ICT

یادآوری- مرحله بازیابی شامل فعالیت‌هایی در زمان بازیابی/ازسرگیری خدمات، عملیات پایدار ICT DR و ترمیم و بازگشت به عملیات عادی می باشد.، برای جزیات بیشتر به شکل الف-۱ از پیوست الف مراجعه شود.

۵-۳ عنصرهاي IRBC

عنصرهای کلیدی IRBC را می توان به صورت زیر خلا صه کرد :

الف) نیروی انسانی : متخصصین با مهارت ودانش مناسب ودرخور سابقه شخصیتی مناسب؛

ب) امکانات : محیط ومکانی که منابع ICT در آن مستقر می‌شوند؛

پ) فناوری :

۱- سخت افزار (شامل رک، خدمت گذار، منابع ذخیره‌سازی و دستگاه‌های نواری و لوازم جانبی)؛

۲- شبکه کامپیوتری(شبکه‌های انتقال داده، خدمات صوتی)، سوییچ‌ها، مسیریاب‌ها؛ و

۳- نرم افزار (شامل سامانه عامل و برنامه‌های کاربردی، پیوندها یا ارتباط میان برنامه‌ها و روال پردازش موازی)؛

ت) داده: داده‌های کاربردی، داده‌های صوتی وانواع دیگرداده؛

ث) فرآیندها : شامل مستند سازی برای توصیف چگونگی برپاسازی منابع ICT و قابل دسترس کردن عملیات مؤثر، بازیابی و نگهداری خدمات ICT؛ و

ج) تأمین کنندگان: اجزای دیگر از خدمات انتها به انتها که در آن ارائه خدمات ICT وابسته به یک ارائه‌دهنده خدمات خارجی یا سازمانی دیگر درون زنجیره تأمین است به عنوان مثال ارائه دهنده داده بازارهای مالی، حامل مخابراتی یا ارائه دهنده خدمات اینترنتی.

۵-۴ خروجي‌ها ومزاياي IRBC

مزایای یک IRBC مؤثر برای یک سازمان به شرح زیر است :

الف) درک و شناسایی مخاطره‌ها برای تداوم خدمات ICT و نقاط ضعف آن؛

ب) شناسایی پیامدهای بالقوه اختلال در خدمات ICT؛

پ) همکاری بین مدیران کسب و کار و فراهم کنندگان خدمات ICT (داخلی یا خارجی) افزایش می یابد؛

ت) نیروهای ICT شایسته را توسعه و تقویت می‌کند. که این کار را به وسیله اعمال طرح‌های تداوم ICT و بررسی ترتیبات IRBC است؛

ث) ارائه تضمین به مدیران ارشد که این تضمین بر سطوح از پیش تعیین شده خدمات ICT و پشتیبانی کافی دریافتی و امکانات ارتباطی در صورت اختلال بستگی دارد؛

ج) ارائه تضمین به مدیران ارشد از درستی حفظ امنیت اطلاعات (محرمانه بودن، یکپارچه بودن و قابل دسترس بودن) و حصول اطمینان از پایبندی به سیاست‌های امنیت اطلاعات؛

چ) برقراری اطمینان کافی در راهبرد تداوم کسب وکار ازطریق برقراری ارتباط میان سرمایه‌گذاری در راه حل‌های IT با نیازهای کسب و کار و حصول اطمینان از این که خدمات ICT در سطح مناسب نسبت به اهمیتشان در سازمان محافظت می‌شوند؛

ح) خدمات ICT مقرون به صرفه بوده و کمتر یا بیشتر سرمایه گذاری نمی‌شوند و این از طریق درک درستی از سطح وابستگی خود بر روی خدمات ICT مربوطه است که خدمات ICT و طبیعت، موقعیت، وابستگی متقابل و استفاده از اجزای خدمات ICT را تشکیل می دهند؛

خ) می‌تواند اعتبار خود را در زمینه احتیاط و کارایی افزایش دهد؛

د) وجود مزیت‌های بالقوه رقابتی از طریق نشان دادن توانایی برای ارائه تداوم کسب وکار وحفظ ارائه محصول و خدمات در زمان اختلال؛ و

ذ) درک و مستندسازی خواسته‌های ذی‌نفعان وارتباط و استفاده آنها از خدمات ICT.

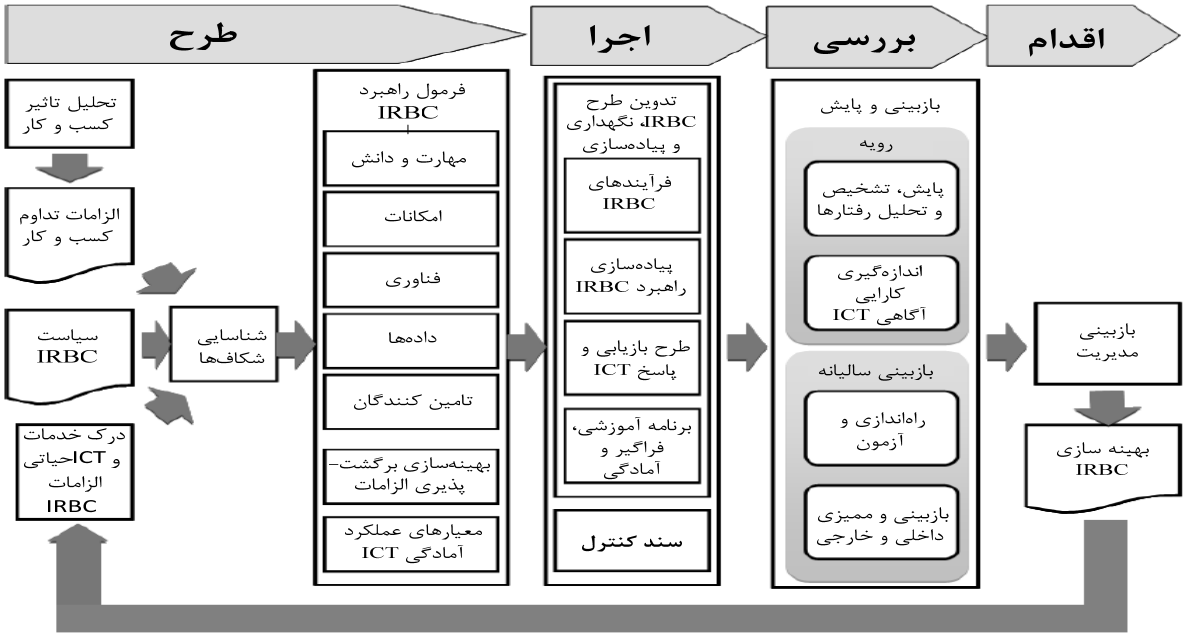
بنابراین IRBC راه قابل قبولی برای تعیین وضعیت خدمات سازمان ICT در پشتیبانی از اهداف تداوم کسب و کار خود در پرداختن به پرسش « آیا ICT ما قادر به عکس العمل است؟» به جای« آیا ICT ما امن است؟ » فراهم می‌کند.

۵-۵ برقراری IRBC

زمانی IRBC بسیار کارآمد و مقرون به صرفه می شود که خدمات ICT طراحی و ساخته شده از آغاز به کار، خود را به عنوان بخشی از راهبرد IRBC که از اهداف تداوم کسب و کار سازمان حمایت می کند. این تضمین می کند که خدمات ICT بهتر ساخت شده ، جهش و درک شود. مقاوم سازی IRBC می تواند پیچیده ، مخرب و گران باشد.

این سازمان باید به توسعه، پیاده‌سازی، نگهداری و تداوم بهبود در یک مجموعه‌ای مستند شده جهت کمک به فرآیندهای پشتیبانی IRBC اهمیت بدهد. این فرآیندها باید اطمینان حاصل کنند که اهداف IRBC به روشنی بیان شده است، درک و ابلاغ شده و تعهد مدیریت ارشد به IRBC نشان داده شده است.

شکل ۵ : به صورت گرافیکی فعالیت‌هارا در مراحل مختلف IRBC نمایش می‌دهد.



شکل ۵ : مراحل در IRBC

۵-۶ استفاده از طرح اجرا بررسی اقدام براي برقراری IRBC

آمادگیICT برای تداوم کسب و کار(IRBC) شامل سازمانی در برقراری فرآیندها به منظور توسعه و افزایش عناصر کلیدی IRBC (مطابق بند ۵-۲) به منظور بهبود ظرفیت برای پاسخ بـه هـر نـوع اخـتلال از جملـه تغییر شرایط مخاطره از طریق استفاده از رویکرد طرح اجرا بررسی اقدام می باشد. شـکل ۵ فعالیـت‌هـا را در مراحل مختلف IRBC به صورت گرافیکی ارائه می‌کند.

۵-۷ مسئولیت مدیریت

۵-۷-۱ راهبری و تعهد مدیریت

برای مؤثر بودن برنامه IRBC باید یک فرایند به طور کامل با فعالیت های مدیریتی سازمان یکپارچه شود ، که از طرف سازمان و مدیریت ارشد رهنمود و ترویج می‌شود. تعدادی از فعالان حرفه‌ای IRBC و کارکنان از سایر مدیریت‌ها و بخش های دیگر ممکن است نیاز باشد تا به حمایت و مدیریت برنامه IRBC بپردازند. میزان منابع مورد نیاز به پشتیبانی چنین برنامه‌ای وابسته به اندازه و پیچیدگی سازمان خواهد بود.

۵-۷-۲ سیاست IRBC

سازمان باید سیاست IRBC را مستند شده داشته باشد. در ابتدا، این مسأله ممکن است نیاز به پالایش و ارتقاء بیشتر به عنوان ورودی یک فرآیند IRBC بلوغ یافته داشته باشد. این سیاست باید به طور منظم بررسی و در راستای نیازهای سازمان به روز شده و باید مطابق با اهداف بلند مرتبه سازمانی BCM باشد.

سیاست IRBC باید سازمان را با اصول مستند شده همگام سازد. برای رسیدن به آنچه تمایل دارد و در برابر آن اثربخشی IRBC بتواند اندازه‌گیری شود، برای این منظور باید این اقدامات را انجام دهد:

الف) برقراری و نشان دادن تعهد مدیریت ارشد به برنامه IRBC؛

ب) شامل یا ارجاع به اهداف IRBC سازمانی؛

پ) تعریف دامنه IRBC از جمله محدودیت‌ها و استثناءها؛

ت) توسط مدیریت ارشد امضا و تایید شود؛

ث) ارتباط برقرار کردن مناسب با ذی‌نفعان داخلی و خارجی؛

ج) شناسایی و ارائه اختیارات مربوطه برای دسترس‌پذیری منابع از قبیل بودجه، پرسنل لازم برای انجام فعالیت‌ها در راستای سیاست IRBC؛ و

چ) در فواصل برنامه‌ریزی شده و هنگامی که تغییرات قابل توجهی مانند تغییر محیطی، تغییرات کسب و کار و ساختار سازمانی رخ داده باشد، بررسی شود؛

۶ طرح‌ریزیIRBC

۶-۱ کلیات

هدف اصلی از مرحله طرح‌ریزی این است که آمادگی مورد نیاز برای سازمان ICT، برقراری شود از جمله:

الف) راهبرد IRBC و طرح IRBC که برای پشتیبانی از کسب و کار و الزامات قانونی، حقوقی و تنظیم مقرراتی مربوط به محدوده تعریف شده و دستیابی به مقاصد و اهداف تداوم کسب و کار سازمانی مورد نیاز است؛ و

ب) معیارهای عملکرد سازمان برای نظارت بر درجه ای از آمادگی ICT سازمان، نیاز به دستیابی به این اهداف و مقاصد مورد نیاز دارد؛

۶-۲ منابع

۶-۲-۱ کلیات

به عنوان قسمتی از اختیارات سیاست،سازمان باید یک معیار برای برنامه IRBC به عنوان قسمتی از تعریف اهداف کلی BCM برقراری و پیاده‌سازی کند و علاوه بر این، منابع مورد نیاز برای برقراری و پیاده‌سازی اقدام و نگهداری برنامه‌های IRBC تعیین و ارائه کند.

نقش‌های IRBC، مسؤولیت‌ها، شایستگی‌ها و اختیارات باید تعریف و مستند شود.

مدیریت ارشد باید این اقدامات را انجام دهد:

الف) انتصاب یا معرفی یک شخص ارشد و با اقتدار و اختیار مناسب به مسئول سیاست IRBC و پیاده‌سازی آن؛ و

ب) تعیین یک یا چند نفر از افراد شایسته، که بدون در نظر گرفتن مسؤولیت‌های دیگر، باید پیاده‌سازی و حفظ سامانه مدیریت IRBC را که در این استاندارد بین المللی توصیف شده بر عهده گیرند؛

۶-۲-۲ شایستگي کارمندان IRBC

سازمان باید اطمینان حاصل کند که تمام پرسنل که به مسئولیت IRBC گمارده شده‌اند شایستگی انجام وظایف الزامی را داشته باشند. برای جزئیات بیشتر به ۷-۲-۱ مراجعه کنید.

۶-۳ تعریف الزامات

۶-۳-۱ کلیات

به عنوان قسمتی از برنامه BCM، سازمان فعالیت خود را با توجه به اولویت خود برای تداوم (به عنوان تجزیه و تحلیل برآورد تأثیر کسب وکار) طبقه‌بندی کرده و کمینه سطحی که در آن کدام فعالیت اولویت دارد که با از سرگیری انجام شود، تعریف می کند. مدیریت ارشد باید با الزامات تداوم کسب وکار سازمان موافقت کند و این شرایط در زمان بازیابی هدف (RTO) و نقطه بازیابی هدف (RPO) برای کمینه هدف تداوم کسب و کار (MBCO) به ازای هر محصول خدمات یا فعالیت منجر خواهد شد. این RTOها از نقطه وقوع اختلال و اجرا شروع می‌شود و تا محصول، خدمات یا فعالیت ادامه دارد.

۶-۳-۲ درک خدمات بحرانی ICT

ممکن است تعدادی از خدمات ICT که بحرانی در نظر گرفته شده‌اند و نیازمند بازیابی باشند. هر یک از این خدمات بحرانی ICT باید زمان بازیابی هدف (RTO) و نقطه بازیابی هدف (RPO) خود را برای حداقل هدف تداوم کسب و کار (MBCO) از خدمات ICT را به صورت مستند داشته باشند.

(این ممکن است شامل جنبه ارائه خدمات ICT همچون میزکمک[1] باشد.) RTO خدمات بحرانی ICT همواره کمتر از RTO تداوم کسب و کار است.(برای جزئیات بیشتر از RTO و RPO به پیوست الف توجه کنید.)

این سازمان باید خدمات بحرانی ICT خود را شناسایی و مستند کند که شامل نام و شرح مختصری است که در سطح کاربری سازمان معنی‌دار است. این درک مشترک بین کسب و کار و کارکنان ICT اطمینان به همراه خواهد داشت، با این‌که ممکن است نام‌های مختلف برای همان خدمات ICT استفاده شده باشد. هر یک از خدمات بحرانی ذکر شده ICT باید محصول و یا خدمات این سازمان که آن را پشتیبانی می‌کند تشخیص دهد و مدیریت ارشد باید موافق با خدمات عادی ICT و الزامات IRBC مرتبط به آن باشد.

برای هر یک از خدمات مهم فناوری اطلاعات و ارتباطات شناسایی شده و پذیرفته شده، تمام اجزای خدمات انتها به انتها ICT باید توضیح داده شده و مستند شوند. پیکربندی عادی هر دو محیط تحویل خدمات ICT و محیط تحویل خدمات تداوم ICT باید مستند شود.

برای هریک از خدمات بحرانی ICT با قابلیت تداوم فعلی (مانند وجود یک نقطه خرابی) از دیدگاه پیشگیرانه برای ارزیابی مخاطره‌های ناشی از اختلال خدمت و یا بررسی تخریب (که می‌تواند به عنوان قسمتی از ارزیابی مخاطره کلی BCM در نظر گرفته شده باشد) باید بازنگری شود. فرصت‌ها نیز باید به منظور بهبود خدماتICT و امکان‌بازگشت مرتب شوند و در نتیجه احتمال وقوع و/یا تأثیر اختلال در خدمت دهی را کاهش‌دهد. همچنین ممکن است فرصت‌های برجسته را تشخیص و قادر به پاسخ سریع به اختلال خدمات ICT باشد. سازمان می‌تواند تصمیم بگیرد که آیا یک مورد کسب و کار برای سرمایه گذاری در فرصت شناسایی شده به منظور بهبود امکان‌بازگشت خدمات وجود دارد. این خدمات ارزیابی مخاطره‌ها (که ممکن است قسمتی از چارچوب کلی مدیریت مخاطره‌ها سازمان را تشکیل دهند) ممکن است به مورد کسب و کارنیز برای افزایش قابلیت بازیابی خدمات ICT توصیه کند.

۶-۳-۳ شناسايي شكاف بين توانايي‌هاي آمادگی ICT و الزامات تداوم كسب و كار

برای هر خدمت بحرانی ICT ترتیبات آمادگی فعلی – مانند پیشگیری، پایش، تشخیص، پاسخ و بازیابی- باید با الزامات تداوم کسب و کار مقایسه شده و هر گونه شکاف باید مستند شود.

مدیریت ارشد باید از هرگونه شکاف بین توانایی‌های بحرانی IRBC و الزامات تداوم کسب و کار آگاه باشد. چنین شکافی ممکن است مخاطره‌ها را نشان دهد و نیاز به امکان‌بازگشت اضافی و منابع بازیابی مانند موارد زیر داشته داشته باشد :

الف) کارکنان، ازجمله تعداد، مهارت‌ها و دانش؛

ب) امکانات برای مکان دادن امکانات ICT، به عنوان مثال اتاق کامپیوتر؛

پ) پشتیبانی از فناوری، نصب آن‌ها، تجهیزات و شبکه‌ها (فناوری)؛

ت) برنامه‌های اطلاعاتی و پایگاه دادگان؛

1 - help desk

ث) امور مالی و یا تخصیص بودجه؛ و
ج) خدمات خارجی و تأمین کنندگان (تدارکات)؛
مدیریت ارشد باید تعاریف خدمات ICT را ثبت کرده و فهرست مستند از خدمات بحرانی ICT و مخاطره‌ها مرتبط با توجه به شکاف‌های شناسایی شده بین قابلیت‌های بحرانی IRBC و الزامات تداوم کسب و کار را تاکید کند. این باید شامل تایید جای مناسب از مخاطره‌ها شناسایی شده باشد. گزینه‌هایی برای مقابله با شکاف‌ها و مخاطره‌ها تعریف شود و سپس باید به وسیله تعیین راهبرد IRBC بررسی شود.

۶-۴ تعیین گزینه‌های راهبردي IRBC

۶-۴-۱ کلیات

راهبردهای IRBC باید رویکرد امکان‌بازگشت مورد نیاز برای پیاده‌سازی را تعریف کند. به طوری که اصول پیشگیری از رخداد، تشخیص، پاسخ، بازیابی و ترمیم در جای خود انجام بشود.
طیف گسترده ای از گزینه‌های راهبردی IRBC باید ارزیابی شوند و راهبرد انتخاب شده باید قادر به پشتیبانی از تداوم کسب و کار مورد نیاز سازمان باشد. این سازمان باید به پیاده‌سازی و منابع مورد نیاز مداوم در هنگام پیشرفت راهبرد، توجه کند. با تأمین کنندگان خارجی هم ممکن است قرار داد ارائه خدمات و مهارت های تخصصی که نقش مهمی در پشتیبانی از راهبرد دارند، بسته شود. راهبرد IRBC باید به اندازه کافی انعطاف پذیری برای تهیه راهبردهای کسب و کار مختلف در بازارهای مختلف داشته باشد.
علاوه بر این، راهبرد باید به محدودیت ها و عوامل داخلی توجه کند، مانند :
الف) بودجه ؛
ب) دسترسی به منابع ؛
پ) هزینه‌های منافع و بالقوه؛
ت) محدودیت‌های فناوری ؛
ث) مخاطره پذیری سازمان ؛
ج) راهبرد IRBC موجود سازمان ؛
چ) تعهدات تنظیمی[1]؛

۶-۴-۲ گزینه‌هاي راهبردي IRBC

سازمان باید طیفی از گزینه‌ها را برای آمادگی در مقابل رخداد برای خدمات بحرانی ICT خود در نظر بگیرد. گزینه‌ها باید برای افزایش حفاظت و امکان‌بازگشت باشند و همچنین بازیابی و برگرداندن ناشی از اختلال ناخواسته، که ممکن است شامل آرایش داخلی باشد، از جمله خدمات ارائه شده به سازمان و خدمات تدارک شده از خارج و توسط یک یا چند طرف سوم ارائه شود. موارد انتخابی باید از اجزای مختلف مورد نیاز برای حصول اطمینان از تداوم و بهبود خدمات بحرانی ICT استفاده کند. IRBC در بسیاری جهات ممکن است به دست آید و باید عناصر IRBC را همانند آن‌چه در قسمت۵-۳ توصیف شده است، تعیین کند.

1 - regulatory

۶-۴-۲-۱ مهارت‌ها و دانش

سازمان باید راهبردهای مناسب جهت حفظ کردن مهارت‌های اصلی و دانش ICT را مشخص نماید. این امر ممکن است فراتر از کارکنان، به پیمانکاران متخصص و ذی‌نفعان دیگر که دارای مهارت‌ها و دانش گسترده ICT هستند برسد.

راهبرد برای حفظ یا ارائه آن مهارت‌ها ممکن است شامل موارد زیر باشد :

الف) مستندسازی به روشی که در آن خدمات بحرانی ICT انجام می‌شود؛

ب) آموزش مهارت چندگانه کارکنان و پیمانکاران ICT به منظور افزایش فزاینده مهارت؛

پ) جداسازی مهارت‌های اصلی برای کاهش شدت مخاطره (این ممکن است مستلزم جدایی فیزیکی کارکنان با مهارت‌های اصلی شود و یا تضمین این که بیش از یک نفر دارای مهارت‌های اصلی لازم باشد)؛

ت) نگهداری و مدیریت دانش؛

۶-۴-۲-۲ تسهیلات

با توجه به مخاطره‌های شناسایی شده، سازمان باید راهبردی را برای کاهش تأثیر در دسترس نبودن امکانات طبیعی ICT تدبیر کند.

این ممکن است شامل یک یا چند مورد از موارد زیر باشد :

الف) تسهیلات (مکان) جایگزین در درون سازمان، از جمله جا به جایی فعالیت‌های دیگر؛

ب) امکانات جایگزین ارائه شده توسط سازمان‌های دیگر؛

پ) امکانات جایگزین ارائه شده توسط متخصصان شخص ثالث؛

ت) کار از خانه و یا در قسمت‌های از راه دور دیگر ؛

ث) دیگر امکانات کاری مناسب مورد توافق؛

ج) استفاده از نیروی کار جایگزین در پایگاه تاسیس شده؛ و

چ) امکانات جایگزین که می‌تواند به پایگاه مختل شده برای ارائه جایگزینی مستقیم برخی از دارایی‌های فیزیکی درگیر حمل و استفاده گردد؛

راهبردها برای امکانات ICT، می‌تواند بسیار قابل توجه باشد و طیف وسیعی از گزینه‌ها ممکن است در دسترس باشد. انواع مختلف رخداد یا تهدید ممکن است نیاز به پیاده‌سازی راهبردهای مختلف (انتخاب و رویکرد ترکیبی) دارند که با توجه به اندازه سازمان،وسعت فعالیت، مکان، فناوری، بودجه و ... آن سازمان نسبت داده می‌شود.

با در نظر گرفتن استفاده از محل‌های جایگزین موارد زیر را باید مورد توجه قرار داد :

الف) امنیت پایگاه؛

ب) دسترسی[1] کارمندان؛

1 - access

پ) نزدیکی به امکانات موجود؛ و
ت) دسترس‌پذیری[1]؛

۶-۴-۲-۳ فناوری

خدمات ICT که فعالیت‌های بحرانی کسب و کار به آن وابسته است، باید پیش از ازسرگیری فعالیت‌های وابسته به کسب و کار بحرانی خود در دسترس باشد. بنابراین راه حل‌های مورد نیاز این است که اطمینان از در دسترس بودن برنامه‌های کاربردی در زمانبندی خاص حاصل شود،به عنوان مثال RTOها قسمتی از BIA حساب می‌شود. زیرساخت های فناوری و نرم افزارهای کاربردی باید در طی بازه‌های زمانی خواسته شده توسط سازمان به عنوان یک هدف قرار داده شود.

فناوری‌هایی که ازخدمات بحرانی ICT پشتیبانی می‌کنند به طور مرتب نیاز به تنظیمات پیچیده برای اطمینان از تداوم دارند بنابراین موارد زیر باید درهنگام انتخاب راهبرد IRBC در نظر گرفته شود :

الف) RTOها و RPOها برای خدمات ICT بحرانی هستند، که از فعالیت‌های بحرانی شناسایی شده توسط برنامه BCM پشتیبانی می کنند؛
ب) محل و فاصله بین پایگاه‌های فناوری؛
پ) تعداد پایگاه‌های فناوری؛
ت) دسترسی از راه دور به سامانه؛
ث) الزامات خنک کننده؛
ج) الزامات برقی؛
چ)استفاده از پایگاه‌های بدون کارمند (تاریک) در مقابل پایگاه‌های دارای کارمند؛
ح)اتصالات و مسیرهای افزونه مخابراتی؛
خ) ماهیت برگشت‌پذیری[2] (آیا مداخله دستی جهت فعال سازی تدارک ICT جایگزین مورد نیاز است یا این‌که باید به صورت خودکار اتفاق بیافتد.)؛
د) سطح اتوماسیون مورد نیاز؛
ذ) سطح منسوخ شدن تکنولوژی؛ و
ر) اتصال به ارائه دهنده خدمات برون سپاری شده و سایر پیوندهای خارجی؛

۶-۴-۲-۴ داده‌ها

علاوه بر این فعالیت های بحرانی کسب و کار ممکن است به داده های بروز یا نزدیک به آن بستگی داشته باشد. تداوم راه حل ها باید به منظور پاسخگویی به نقطه بازیابی هدف (RPO) هریک از فعالیت های بحرانی کسب و کار سازمان به صورتی که آن ها مربوط به فعالیت های بحرانی کسب و کار است طراحی شود.

1 - availability
2 - failback

گزینه‌های IRBC منتخب باید محرمانگی، یکپارچگی ودسترس پذیری داده‌های مهم که فعالیت‌های بحرانی (استاندارد ملی ایران به شماره ۲۷۰۰۱: سال۱۳۸۷و استاندارد ملی ایران به شماره ۲۷۰۰۲: سال۱۳۸۷) را پشتیبانی می‌کند، تضمین نماید.

ذخیره سازی داده‌ها و راهبردهایIRBC باید الزامات تداوم کسب و کار سازمان را برآورده کند و باید موارد زیر را مورد ملاحظه قرار دهد:

الف) الزامات RPO؛

ب) چگونگی ذخیره سازی امن داده ها مانند دیسک، نوار یا رسانه های نوری؛ سازو کارهای تهیه پشتیبان و ترمیم مناسب باید در جای خود باشند تا اطمینان حاصل شود که داده‌ها امن هستند و در یک محیط ایمن قرار دارند؛

پ) جایی‌که در آن اطلاعات ذخیره، حمل و یا منتقل می‌شود، فاصله زمانی، مکان، پیوندهای شبکه و غیره (درون سازمانی، برون سازمانی یا طرف سوم) و بازه‌های مورد انتظار برای بازیابی رسانه‌های پشتیبان؛ و

ت) بازیابی بازه‌های زمانی، بر حسب حجم داده‌ها چگونگی ذخیره آن‌ها و پیچیدگی فرآیند بازگرداندن فنی همراه با الزامات کاربر خدمات و نیازهای تداوم سازمانی ؛

درک درست استفاده «انتها به انتها» از داده‌ها در سراسر سازمان بحرانی است. این شامل تغذیه اطلاعات طرف های سوم و تغذیه اطلاعاتی از جانب آن ها می‌شود.

باید به خاطر سپرده شود که ماهیت، جریان و حجم داده ها در داخل سازمان بسیار متفاوت خواهد بود.

۶-۴-۲-۵ فرآیندها

در انتخاب راهبرد IRBC، سازمان باید فرآیندهای ضروری شامل ضروریات در پیشگیری، تشخیص، پاسخ به رخداد و بازیابی مقابله با فاجعه را برای اطمینان از کارا بودن این راهبرد در نظر بگیرد. سازمان همچنین باید عوامل ضروری برای پیاده سازی مؤثر آن دسته از فرآیندهای منحصر به فرد مانند مجموعه مهارت‌های کلیدی، داده‌های بحرانی، فناوری‌های توانمند ساز کلیدی، یا تجهیزات/امکانات بحرانی را شناسایی کند.

۶-۴-۲-۶ تأمین کنندگان

سازمان باید حامیان خارجی که ارائه خدمات ICT را پشتیبانی می کنند و گام‌های مناسب برای اطمینان از این تجهیزات بحرانی و خدمات را می‌تواند برای تأمین کنندگان خود فراهم کند، طی زمان بندی از پیش تعیین شده و مورد توافق، شناسایی و مستند کند. وابستگی‌هایی ممکن است در مورد سخت افزار، نرم افزار، ارتباطات، برنامه‌های کاربردی، خدمات میزبانی طرف سوم، خدمات شهری و مسائل زیست محیطی، از جمله تهویه مطبوع، پایش محیط زیست و سامانه ضد حریق وجود داشته باشند.

رهنمودها برای این خدمات ممکن است شامل موارد زیر باشند :

الف) ذخیره سازی تجهیزات اضافی و کپی نرم افزار در محل دیگری؛

ب) توافق با تأمین کنندگان برای تحویل تجهیزات جایگزینی در زمان کوتاه؛

پ) تعمیر سریع و/یا تعویض قطعات معیوب در صورت خرابی تجهیزات؛
ت) تامین دوگانه تاسیسات از قبیل برق و مخابرات؛
ث) تجهیزات مولد فوریت؛ و
ج) شناسایی تأمین کنندگان جایگزین/جانشین؛

سازمان باید الزامات مدیریت تداوم کسب و کار و ICT را در قراردادهای خود با شرکا و ارائه کنندگان خدمات در بر گیرد. برنامه قرارداد باید شامل اشاره به تعهدات هر یک از طرفین، توافق سطح خدمات، پاسخ به رخدادها عمده، تخصیص هزینه، تعداد دفعات تغییر و اقدامات اصلاحی باشد.

۶-۵ تأیید نهایی[1]

گزینه‌های راهبردی IRBC انتخاب شده باید باتوجه به توصیه‌هایی برای تصمیم گیری بر اساس مخاطره پذیری و هزینه مخاطره‌ها به مدیریت ارشد ارائه شود.
باید به اطلاع مدیریت ارشد برسد که چنانچه گزینه‌های راهبردی IRBC انتخاب شده قادر به پاسخگویی به الزامات تداوم کسب و کار نباشند، در این حالت مدیریت ارشد نسبت به ظرفیت موجود مطلع می گردد.
مدیریت ارشد باید راهبردهای IRBC را از گزینه‌های ارائه شده انتخاب کند، گزینه‌های مستند را تصویب و تایید کند تا گزینه‌هایی که به درستی انجام شده‌اند تایید و پشتیبانی خود را از شرایط کلی تداوم کسب و کار اعلام کنند.

گزینه‌های راهبردی IRBC انتخاب شده باید :
الف) برای مخاطرات محتمل و اثرات اختلال مهیا شود؛
ب) راهبردهای تداوم کسب و کار انتخاب شده توسط سازمان یکپارچه شود؛
پ) مناسب جهت برآورده سازی اهداف کلی سازمان در دامنه مخاطره پذیری آن باشد.

۶-۶ بهبود قابلیت IRBC

۶-۶-۱ افزایش امکان‌بازگشت

سازمان باید راهبردهای سطح بالا IRBC را در برگیرد و منبعی برای بهبود خاص قابلیت های IRBC که مورد نیاز برای تحقق نیازهای IRBC شناسایی شده است، برنامه‌ریزی کند. چنین بهبودی ممکن است از طریق اقدامات پیشگیرانه و اصلاحی به دست آید (به بندهای ۹-۲ و ۹-۳ مراجعه شود) و نیز دیگر فرآیندهای خاص یا روش‌هایی است که پاسخ‌های مربوط به BIA سازمان و مخاطره پذیری آن را در بر خواهد داشت.
اطلاعات چنین فرآیندهایی و یا روش‌هایی را می توان در پیوست ب و ت یافت.

1 - Sign Off

۶-۷ معیارهاي عملکرد آمادگی ICT

۶-۷-۱ شناسايي معيارهاي عملکرد

در هر محیط ICT، بالقوه رویدادهای تهدید کننده زیادی وجود دارد – مانند خرابی سخت افزار، نفوذ امنیتی و غیره- و سازمان باید قادر به پایش بر تهدیدات باشد و درک کند آیا سامانه IRBC قادر است به اندازه کافی با آن‌ها مقابله کند.

بنابراین سازمان باید معیارهای عملکرد جهت سنجش اثر بخشی آمادگی ICT خود را تعریف کند. چنین معیارهایی برای تعیین کیفیت مورد نظر از پاسخ به یک اختلال، در هر دو زمینه‌ی اثر بخشی و کارایی می‌تواند مورد استفاده قرارگیرد.

معیارهای عملکرد برای IRBC را باید بر اساس الزامات IRBC و همچنین اهداف کلی BCM از نظر پاسخ به رخداد و الزامات تداوم کسب و کار در نظر گرفت (به بند ۸-۳-۱ مراجعه شود).

۷ پیاده‌سازی و عملیات

۷-۱ کلیات

راهبردهای IRBC تنها باید پس از تایید مدیریت ارشد اجرا شود.در این نقطه، مرحله پیاده‌سازی آغاز می‌شود.این بند توصیه‌هایی را برای پیاده سازی راهبردهای IRBC انتخابی سازمان در راستای ساختار سازمانی فراهم می‌کند. طرح‌ها و روش‌های مورد نیاز برای پشتیبانی پیاده‌سازی ارائه می کند.

سازمان باید منابع (به بند ۷-۲ مراجعه شود)، روش‌های اجرایی وعملیات IRBC مدیریت کند، و نیز برنامه‌های آموزشی و آگاهی سازی را پیاده سازی نماید. پیاده‌سازی باید به عنوان یک پروژه از طریق فرآیند کنترل تغییر رسمی سازمان و کنترل مدیریت پروژه BCM به منظورحصول اطمینان از اینکه به طور کامل به رویت مدیریت می رسد و به او گزارش می شود، کنترل شود.

مرجع باید در طول اجرای اجزای تشخیص رخداد، پاسخ و بازیابی رخداد به استانداردهای بین المللی مربوطه زیر توجه داشته باشد

از جمله موارد زیر :

الف)استاندارد ISO / IEC18043، برای انتخاب و بهره برداری ازسامانه‌های تشخیص نفوذ؛

ب)استاندارد ISO / IEC18044،برای رویه پاسخ رخداد؛ و

پ)استاندارد ISO / IEC24762،برای خدمات بازیابی رخداد؛

یادآوری- ISO / IEC18044 ، تجدید نظر شده و به عنوان ISO / IEC 27035 ، مجدد شماره گذاری شده است.

۷-۲ پیاده‌سازی عناصر راهبرد IRBC

۷-۲-۱ آگاهي، مهارت‌ها ودانش

آگاهی عمومی از آمادگی عناصر خدمات ICT - نیروی انسانی، امکانات، فناوری، داده‌ها، فرآیندها، و تأمین کنندگان و همچنین اجزای بحرانی آن‌ها- یک عنصر تعیین کننده در تضمین پشتیبانی مورد نیاز برای حاکمیت تداوم کسب و کار و سامانه‌های مدیریت از جمله آمادگی ICT است.

سازمان باید:

الف) افزایش، بهبود و حفظ آگاهی از طریق آموزش مداوم و برنامه اطلاعاتی برای کارکنان مربوطه و برقراری یک فرآیند برای ارزیابی اثر بخشی آگاهی رسانی؛
ب) اطمینان حاصل کند که کارکنان از چگونگی مشارکت در دستیابی به اهداف IRBC مطلع هستند؛

سازمان باید اطمینان حاصل کند که تمام پرسنل که به مسئولیت های مدیریت IRBC گمارده شده‌اند شایستگی انجام وظایف الزامی از طریق زیر را داشته باشند :
الف) تعیین صلاحیت‌های لازم برای پرسنل؛
ب) تجزیه و تحلیل نیازهای آموزشی برای پرسنل؛
پ) ارائه آموزش؛
ت) اطمینان از صلاحیت لازم حاصل شده است شده است؛ و
ث) حفظ سوابق تحصیلاتی، آموزش، مهارت، تجارب و شرایط لازم؛

۷-۲-۲ امکانات

سامانه بازیابی و داده‌های بحرانی ICT باید، در صورت امکان، به صورت فیزیکی از قسمت عملیاتی جدا باشد تا از تحت تاثیر قرار گرفتن توسط همان رخداد جلوگیری شود.
در هنگام پیاده سازی راهبرد، مکان در همه محیط ICT باید مورد ملاحظه قرار گیرد. برای مثال در صورت در دسترس بودن، آموزش و یا توسعه سامانه‌های ICT باید به صورت منطقی از سامانه‌های تولید جدا باشد، تا امکان موقعیتی برای آن‌ها فراهم شود که بتوانند در زمان بروز فاجعه پیکره بندی مجدد شوند تا به سرعت بتوان خدمات تولید را فعال نمود.
ویژگی های کلی مقیاس پذیری، قابلیت مدیریت، قابلیت پشتیبانی، عملکرد و هزینه فنون مختلف پیاده سازی باید مورد بررسی قرار گیرد تا فنون مناسب برای راهبردهای انتخاب شده شناسایی شود که از اهداف و مقاصد کلی تداوم کسب و کار پشتیبانی کند.

۷-۲-۳ فناوري

راهبردهای فناوریICT شامل یک یا تعدادی از پیاده‌سازی ها و مقررات زیر می باشد که باید پیاده سازی شود.
الف) آماده به کار داغ، که در آن زیر ساخت‌هایICT در دو قسمت تکرار شود؛
ب) حالت آماده باش گرم، جایی که در یک قسمت ثانویه که در آن بخشی از زیر ساخت‌هایICT آماده باشد در آن بازیابی صورت گیرد؛
پ) حالت آماده باش سرد، جایی کـه در آن از ابتـدا زیـر سـاخت‌هـا در یـک مکـان جـایگزین سـاخته و یـا پیکربندی شده است؛
ت) مقررات حمل ونقل که تحت آن ارائه دهندگان خدمات خارجی، سخت افزار مورد نیاز را عرضه می کنند؛ و
ث) مقرراتی مرکب از راهبردهای قبلی : رویکرد «انتخاب و ترکیب» .

۷-۲-۴ داده‌ها

مقررات دسترس پذیری به داده‌ها باید در راستای الزامات شناسایی شده در راهبردهای مدیریت IRBC باشد و شامل موارد زیر باشد:

الف) فضای اضافی برای ذخیره‌سازی داده‌ها در قالبی که دسترس پذیری به آن دربازه‌های زمانی شناسایی شده در برنامه تداوم کسب و کار را تضمین کند؛

ب) مکان‌های جایگزین برای ذخیره سازی داده‌ها، که ممکن است فیزیکی و یا مجازی باشند،امنیت را فراهم و محرمانگی داده‌ها را حفظ می‌کند؛ بنابراین روش های اجرایی دسترسی متناسب باید تعیین شود و در صورتی که توافقی با طرف سوم برای ذخیره سازی آن اطلاعات باشد مالک اطلاعات باید مطمئن شود که کنترل های متناسب تعیین شوند.

۷-۲-۵ فرآیندها

فرآیندهای IRBC باید به صورت واضح و با جزئیات کافی برای قادر ساختن کارمندان شایسته به اجرای آن‌ها، مستند شوند (برخی از این فرآیندها ممکن است متفاوت با عملیات روزانه باشد).

روش‌های IRBC ممکن است وابسته به موقعیتی باشد که آشکار می‌کند، و در عمل ممکن است نیاز به سازگار شدن در هنگام بروز بحران داشته باشد (مانند درصد خسارت یا آسیب) که اولویت‌های عملیاتی سازمان و مطالبات ذی‌نفعان اقتباس می‌شود.

۷-۲-۶ تأمین کنندگان

سازمان باید اطمینان حاصل کند که تأمین کنندگان بحرانی قادر به پشتیبانی از قابلیت‌های خدمت IRBC مورد نیاز توسط سازمان هستند. این شامل خود مستند و تست تداوم کسب و کار و طرح‌های IRBC با ظرفیت برای پشتیبانی از فعالیت‌های همزمان رخداد و یا طرح بازیابی توسط مشتریان می‌شود. سازمان باید یک فرایند برای ارزیابی از ظرفیت و توانایی تأمین کنندگان قبل از به کارگیری خدمات خود داشته باشد، همچنین به طور مداوم توانایی پایش و بازنگری تأمین کنندگان پس از مشغولیت را داشته باشد. برآوردن الزامات/ شیوه‌های خوب در تعیین قابلیت‌های تأمین کنندگان، مفهوم مفیدی از استانداردهای مرتبط است مانند اتخاذ ISO/IEC 24762 بهترین شیوه توسط تأمین کنندگان میزبانی/مدیریت فرآیند متناوب، ارائه و تسهیلات بازیابی خدمات فاجعه ICT می باشد.

۷-۳ پاسخ به رخدادها

برای پاسخ به هر رخداد ICT باید موارد زیر وجود داشته باشد:

الف) تایید ماهیت و وسعت رخداد؛

ب) در نظر گرفتن کنترل وضعیت؛

پ) محتویات رخداد؛ و

ت) ارتباط با ذی‌نفعان؛

پاسخ رخداد باید یک اقدام مناسب در IRBC را آغاز کند. این پاسخ باید با پاسخ کلی رخداد BCM یکپارچه شود و ممکن است فراخوانی یک رخداد تیم مدیریت یا در یک سازمان کوچک، یک شخص مستقل با مسئولیت برای رخداد و مدیریت تداوم کسب و کار باشد.

یک سازمان بزرگتر ممکن است یک رویکرد محکم را استفاده کند و ممکن است برای تمرکز روی توابع مختلف، تیم‌های مختلفی را ایجاد کند. در داخل ICT، ممکن است این به عهده قسمت‌های فنی و یا خدمات مرتبط باشد.

اشخاص مسئول برای مدیریت رخداد باید طرحی برای فعال سازی، عملیات، هماهنگی و ارتباط پاسخ به رخداد را داشته باشند.

۷-۴ اسناد طرح IRBC

۷-۴-۱ کلیات

این سازمان باید مستنداتی (طرح‌هایی) برای مدیریت اختلال بالقوه و در نتیجه امکان تداوم خدمات ICT و بازیابی فعالیت‌های بحرانی را داشته باشد.

برنامه‌های مدیریت رخداد ICT سازمان، تداوم کسب و کار و بازیابی فنی ممکن است در توالی سریع و یا به طور هم زمان فعال شود.

سازمان ممکن است اسناد طرح خاصی را برای بازیابی و یا از سرگیری خدمات ICT برای بازگشت به حالت «عادی» (طرح‌های بازیابی) گسترش دهد. با این حال، ممکن است تعریف آنچه تا زمان پس از رخداد «عادی» به نظر می‌رسد امکان‌پذیر نباشد، بنابراین ممکن است پیاده‌سازی فوری طرح‌های بازیابی امکان‌پذیر نباشد. بنابراین سازمان باید اطمینان حاصل کند که مقدمات تداوم، قادر به انجام عملیات گسترده پشتیبانی از تداوم کسب و کار گسترده تر، دادن زمان برای توسعه برنامه‌های بازیابی («بازگشت به حالت عادی») است.

۷-۴-۲ محتویات اسناد طرح

یک سازمان کوچک ممکن است یک سند برنامه واحد داشته باشد که تمامی فعالیت‌های بازیابی خدمات ICT از کل عملیات خود را دربربگیرد. یک سازمان بسیار بزرگ ممکن است بسیاری از اسناد طرح داشته باشد، که هر یک در جزئیات بازیابی یک عنصر خاص مشخصات خدمات ICT خود را مشخص کند.

پاسخ ICT و طرح‌های بازیابی باید مختصر و در دسترس کسانی با مسئولیت‌های تعریف شده در طرح باشد.

طرح‌ها باید شامل موارد زیر باشند:

الف) هدف و دامنه

هدف و دامنه هر طرح خاص باید تعریف شده باشد، مورد توافق مدیریت ارشد و درک توسط کسانی که این طرح را مطالبه می کنند باشد. هرگونه رابطه با طرح‌ها یا اسناد مربوطه دیگر در داخل سازمان، به ویژه به طرح‌هایBC، باید به وضوح اشاره شده و روش به دست آوردن و دسترسی به این طرح توصیف شده باشد.

هر مدیریت رخداد و پاسخ ICT و طرح بازیابی باید مجموعه‌ای از اهداف زیر را اولویت بندی کند :

۱ خدمات بحرانی ICT بازیابی شوند؛

۲ بازه‌های زمانیکه در آن بازیابی شوند؛

۳ بازیابی سطح مورد نیاز برای هر یک از فعالیت‌های بحرانی خدمات ICT؛ و
۴ موقعیتی که در آن هر طرح می تواند فراخوانی شود.

طرح ها نیز ممکن است شامل جای مناسب، روش ها و چک لیست هایی باشد که بعد از رخداد از فرایند بازبینی پشتیبانی کند.

ب) نقش‌ها و مسئولیت‌ها

نقش‌ها و مسئولیت‌های افراد و تیم‌های مجاز (هم در تصمیم گیری و هم در اجرا) در طول و پس از رخداد باید به صورت واضح مستند شوند.

پ) فراخوانی طرح

یادآوری- : همواره زمان از دست رفته در طی یک پاسخ را نمی‌توان دوباره به دست آورد. تقریبا همیشه بهتر است که برای شروع یک پاسخ ICT و سپس برای مهار وقوع هرگونه رخداد ای در مراحل اولیه و جلوگیری از تشدید، فرصت بحران از دست نرود.

بنابراین سازمان‌ها نیاز به استفاده از تشدید مدیریت رخداد و فراخوانی پروتکل‌های موجود در طرح مدیریت رخداد تداوم کسب و کار گسترده خود به شکل پایه ای برای مدیریت بالقوه مرتبط با ICT دارند.

روشی که توسط آن پاسخ ICT و طرح بازیابی فراخوانی می‌شود باید به وضوح مستند گردد.

این فرآیند باید برای طرح‌های مربوطه و یا قسمت‌های آن برای مطالبه در کوتاه ترین زمان ممکن، خواه در بیش از یک رویداد بالقوه مخرب و یا بلافاصله پس از وقوع یک رویداد تصویب داده باشد.

طرح باید یک توصیف روشن و دقیق باشد از :

۱ - چگونگی تجهیز فرد یا تیم اختصاص داده شده؛
۲ - نقاط قرار ملاقات فوری؛
۳ - مکان جلسه بعدی تیم و جزئیات مکان هرجلسه متناوب (در یک سازمان بزرگتر این مکان جلسه ممکن است به صورت مرکز فرمان اشاره شود)؛ و
۴ - شرایطی که تحت آن سازمان می پندارد پاسخ IRBC لازم نیست (به عنوان مثال خطا و قطع جزیی برای خدمات بحرانی ICT ممکن است اتفاق بیافتد اما توسط مرکز و مقدمات پشتیبانی و موافقت نامه‌ها مدیریت می‌شود).

سازمان باید فرآیند واضحی را برای نگهداری تیم پاسخ ICT درست بعد از اتمام بحران و باز گرداندن کسب و کار به حالت معمول مستند کند.

ت) پاسخ ICT و طرح بازیابی اسناد صاحب و نگهدارنده

مدیریت باید کسی را برای پاسخ ICT و طرح بازیابی اسناد نامزد کند که برگزاری آن پاسخ گو برای بررسی منظم و به روز کردن اسناد باشد.

نسخه ای از سامانه کنترلی باید به کار گرفته شود و تغییرات به صورت رسمی به تمام اشخاص ذینفع با تداوم توزیع سابقه سند یک طرح نگهداری شده، اطلاع داده شود.

ث) اطلاعات تماس

یادآوری- : سوابق تماس ممکن است شامل « ساعات خارج از خدمت » اطلاعات تماس باشد. با این حال که در آن طرح مرجعی از جمله اطلاعات خصوصی، احترام به حریم خصوصی اطلاعات است که باید توجه بیشتری شود.

مناسب است که در آن، هر طرح مستند شده باید شامل یا ارائه‌ای از یک مرجع برای اطلاعات تماس ضروری برای تمام ذی‌نفعان کلیدی باشد.

۷-۴-۳ مستندات طرح بازیابی و پاسخ ICT

مستندات طرح بازیابی و پاسخ ICT باید؛

الف) انعطاف پذیر، امکان پذیر و مرتبط باشد؛

ب) از لحاظ خوانایی و درک، آسان باشد؛ و

پ) پایه ای برای مدیریت مسایل جدی که توسط سازمان برای شایستگی پاسخ IRBC پنداشته می‌شود ارائه کند (معمولا پس از روی دادن یک اختلال قابل توجه).

اسناد باید چهارچوب فراگیری در حدودی که طرح‌های بازیابی سازماندهی شده زیر را پوشش دهد تعریف کند :

الف) راهبرد کلی؛

ب) خدمات بحرانی (همراه با RTO/PTO)؛

پ) بازه‌های زمانی برای بازیابی؛ و

ت) تیم‌های بازیابی و مسئولیتشان.

طرح‌ها باید مستند شوند به طوری که پرسنل شایسته بتوانند از آن در وقوع یک رخداد استفاده کنند. آن‌ها باید شامل موارد زیر باشند:

الف) هدف: شرح کوتاه از اهداف طرح

ب) دامنه: پوشش با اشاره به نتایج BIA[1]، به شرح زیر است :

۱) حساسیت خدمات: شرح خدمات مربوطه و شناسایی حساسیت های آن؛

۲) فناوری: مروری بر فناوری اصلی است که پشتیبانی خدمات را انجام می‌دهد، از جمله محل قرار گرفتن فناوری؛

۳) سازمان: مروری بر سازمان (ادارات، افراد حیاتی و روش‌ها) که فناوری را مدیریت می‌کند؛ و

1 - Business Impact Analysis

۴) اسناد: بررسی اجمالی از اسناد اصلی برای فناوری از جمله (قسمت‌های خالی) مکان‌هایی که در آن قرار می گیرند.

پ) الزامات در دسترس: نیازهای اساسا تجاری برای دسترسی به خدمات و فن‌آوری مربوط به آن

ت) الزامات امنیت اطلاعات: الزامات برای امنیت اطلاعات خدمات، سامانه ها و داده‌ها، که شامل محرمانه بودن، یکپارچگی و الزامات در دسترسی می‌باشد.

ث) روش‌های بازیابی فناوری: شرح روش هایی که برای بازیابی خدمات ICT دنبال می شود، که شامل موارد زیر می‌باشد:

۱) مجموعه فعالیت‌ها، مانند پشتیبانی میزکار و بازسازی اطلاعات تماس؛

۲) فهرستی از فعالیت‌های بازیابی شبکه، سامانه ها، برنامه‌های کاربردی، پایگاه داده و غیره، به سطح توافق شده در مکان جایگزین، باتوجه به محیط تغییر یافته (به عنوان مثال این می‌تواند در ظرفیت خطوط، ارتباط سامانه با سامانه و غیره تأثیر بگذارد.)؛

۳) لیستی از فعالیت‌ها برای بازسازی قابلیت‌های اساسی مانند امنیت، مسیریابی و ورود به سامانه؛

۴) هماهنگی در درون برنامه‌های کاربردی و یا بین برنامه‌های کاربردی، هماهنگ سازی داده‌ها، و روش‌های خود کار کردن بالقوه برای تحت کنترل داشتن اطلاعات پس افتاده؛

۵) فرآیند مورد نیاز برای بازسازی خدمات ICT و تبدیل آن‌ها برای کاربران خود به عمل در حالت بازیابی؛

۶) روش پشتیبان گیری؛ و

۷) کجا و چگونه نیروی انسانی می‌تواند اطلاعات بیشتر و دستور العمل‌ها و غیره را دریافت کند مانند شماره‌های ضروری ؛و مراحل بازگشت به حالت عادی.

ج) پیوست‌ها :

۱) موجودی سامانه‌های اطلاعاتی، برنامه‌های کاربردی و پایگاه داده‌ها؛

۲) بررسی کلی زیر ساخت‌های شبکه و اسامی خدمت‌گذار؛

۳) موجودی سخت افزار و نرم افزار سامانه؛ و

۴) قراردادها و موافقت نامه سطح خدمات.

چ) تأمین کنندگان کلیدی ICT

۱) کسب وکار به عنوان تأمین کنندگان معمول؛ و

۲) تأمین کنندگان خدمات بازیابی.

۷-۵ آگاهي، صلاحيت وبرنامه‌های آموزشي

برنامه باید هماهنگ اجرا شود تا اطمینان حاصل شود که فرآیندهای در محل به طور منظم برای ترویج آگاهی کلیIRBC، هستند، همچنین سنجش و افزایش صلاحیت تمام پرسنل مربوطه کلیدی به اجرای موفقیت آمیز IRBC (به بند ۷-۲-۱ مرا جعه شود).

۷-۶ کنترل سند

۷-۶-۱ کنترل سوابقIRBC

کنترل باید بر اساس سوابق IRBC به منظور زیر بنا شوند:

الف) اطمینان حاصل شودکه آن‌ها خوانا، به آسانی قابل شناسایی و بازیابی باقی می‌مانند؛ و

ب) برای ذخیره سازی آن‌ها، حفاظت و بازیابی ر اتأمین کند.

۷-۶-۲ کنترل اسناد IRBC

کنترل باید بیش از اسناد IRBC پیاده شوند تا اطمینان حاصل شود که :

الف) مدارک قبلی با کیفیت مورد تایید قرار گیرند؛

ب) مدراک در صورت لزوم بازبینی و به روز شده و دوباره تایید شوند؛

ب) تغییرات و تجدید نظر وضعیت نسخه فعلی مدارک شناسایی شوند؛

پ) نسخه‌های مربوط به مدارک قابل اجرا در لحظات مورد نیاز برای استفاده، در دسترس باشند؛

ت) مدارک با منشا خارجی شناسایی شده و توزیع آن‌ها کنترل شوند؛ و

ث) استفاده ناخواسته از مدارک منسوخ منع شود و همچنین مدارک مناسب، در صورتی که از هر منظوری حفظ شوند شناسایی شود.

۸ پایش و بازنگری

۸-۱ نگهداری IRBC

۸-۱-۱ کلیات

با تغییر، مخاطره می آید، نه تنها مخاطره خرابی، بلکه مخاطره بی ثباتی سیاست‌ها و راهبردهای موجود. بنابراین راهبرد IRBC باید انعطاف پذیر و سازگار باشد.

هر گونه تغییر درخدمات ICT که ممکن است در قابلیت IRBC تأثیر بگذارد باید تنها پس از تغییر سنجش شده و مورد خطاب قرار گرفته پیامدهای تداوم کسب و کار پیاده شود.

برای اطمینان از این‌که راهبردها و طرح‌هایIRBC برای سازمان مناسب باقی می ماند باید:

الف) مدیریت ارشد باید اطمینان پیدا کند که راهبردهایIRBC همچنان از الزامات سازمان BCM پشتیبانی می‌کند؛

ب) تغییر فرآیند مدیریت باید شامل همه قسمت‌های مسئول با راهبردهایIRBC باشد، هم در طراحی و هم در پیاده‌سازی آن؛

پ) فرآیند توسعه برای خدمات جدید ICT باید شامل تایید نهایی باشد که امکان‌بازگشت آن حتی توسط ساده ترین ارتقاء و یا بهبود به مخاطره نیافتد؛
ت) سعی و کوشش به دلیل فعالیت‌های ادغام و اکتساب باید شامل یک سنجش با امکان‌بازگشت باشد؛ و
ث) حذف مؤلفه‌های ICT باید در سامانه مدیریت IRBC مرتبط منعکس شده باشد.

۸-۱-۲ پایش، تشخیص و تحلیل تهدیدات

این سازمان باید فرآیندی را برای پایش و تشخیص پیدایش ناگهانی تهدیدات امنیتیICT به صورت پیوسته اما نامحدود برقرار کند که شامل زمینه‌های زیر باشد:
الف) حفظ کارکنان، مهارت‌ها و دانش؛
ب) مدیریت امکانات و تجهیزات خانه ICT (به عنوان مثال از طریق پایش بر تعداد و ماهیت رخدادها امنیتی/ آسیب پذیری‌های مربوط به اتاق کامپیوتر)؛
پ) تغییرات در پشتیبانی از فناوری، ابزارالات، تجهیزات و شبکه؛
ت) تغییرات در اطلاعات برنامه‌های کاربردی و پایگاه داده‌ها؛
ث) امور مالی و یا تخصیص بودجه؛ و
ج) اثر بخشی خدمات و تأمین کنندگان خارجی (منابع).

۸-۱-۳ آزمون و به کاراندازی[1]

۸-۱-۳-۱ کلیات

سازمان نباید تنها بازیابی خدمات ICT، بلکه باید حفاظت و امکان‌بازگشت عناصر آن را به کار ببرد به منظور تعیین این‌که:
الف) آیا خدمات می‌تواند بدون در نظر گرفتن شدت رخداد محافظت شود، نگهداری و / یا بازیابی بیابد؟؛
ب) آیا ترتیب مدیریت IRBC می‌تواند تأثیر به کسب و کار را به کمینه برساند؟؛ و
پ) آیا روش‌ها برای بازگشت به کسب و کار به طور معمول معتبر هستند؟.

۸-۱-۳-۲ آزمون و به کاراندازی برنامه

در اکثر مواقع مجموعه کاملی از عناصر و فرآیندهایIRBC از جمله بازیابی ICT نمی‌تواند در یک آزمون و به کاراندازی اثبات شوند. بنابراین به کاراندازی تدریجی ممکن است برای ساخت شبیه سازی کامل یک رخداد واقعی مناسب باشد. این برنامه باید شامل سطوح مختلف به کاراندازی از آشنا کردن تا امکان‌بازگشت اتاق کامپیوتر باشد، همان طور که در شکل ۵، تعریف شد و باید تمام جنبه‌های ارائه خدمات انتها به انتها ICT را مد نظر قرار دهد. مخاطرات موجود مرتبط با آزمون و به کاراندازی و هچنین فعالیت‌هایی از این قبیل نباید سازمان را به یک سطح غیر قابل قبول از مخاطره ببرد. برنامه آزمون و به کاراندازی باید میزان و چگونگی مخاطرات موجود را به صورت کامل تشریح کند. مدیریت ارشدی که آزمون را تایید کند باید برنامه

1 - exercise

را بدست آورده و یک توضیح واضح از مخاطرات مرتبط مستند کند. اهداف برنامه آزمون و به کاراندازی باید به طور کامل با گستره اهداف و دامنه مدیریت تداوم کسب و کار همسو بوده و مکملی برای برنامه‌های به کاراندازی گسترده‌تر سازمان باشد.
هر آزمون و به کاراندازی باید هر دوی اهداف کسب و کار (حتی جایی که کسب و کار مستقیم وجود نداشته باشد) و اهداف فنی را برای آزمون و یا اعتبار دادن به یک عنصر خاص از راهبرد IRBC تعریف کند. به کاراندازی تک تک عناصر در حالت جدا از سطح ترکیب اجزاء، مکملی برای به کاراندازی تمام سامانه است و باید به صورت قسمتی از آزمون جاری و برنامه به کاراندازی نگهداری شود.
برنامه به کاراندازی و آزمون، باید فراوانی، دامنه و قالب هر به کاراندازی را تعریف کند.

موارد زیر نمونه‌های سطح بالا از دامنه به کاراندازی هستند :
الف) **بازیابی داده ها:** بازیابی یک فایل یا پایگاه داده به دنبال بروز اختلال؛
ب) بازیابی از یک خدمت‌گذار (از جمله بازسازی کامل)؛
پ) بازسازی یک برنامه کاربردی (این شاید شامل چندین خدمت‌گذار، زیر برنامه‌های کاربردی و زیرساخت‌ها باشد)؛
ت) شکست[1] خدمات میزبانی بر روی سکوهای[2] با دسترسی بالا (برای مثال، خوشه بندی: شبیه سازی از دست دادن هیچ عضوی از یک خوشه – به پیوست ب مراجعه شود)؛
ث) بازیابی داده از نوار (بازیابی فایل مجرد یا مجموعه فایل‌ها از نوارهای ذخیره سازی خالی)؛
ج) آزمایش شبکه‌ها؛ و
چ) آزمایش شکست زیر ساخت‌های ارتباطی.

به کاراندازی به طور کلی باید به صورت مرحله ای انجام و ارتباط تمام اجزای امتحان قابل بررسی باشد و در پایان با کاربر ارتباط متقابل داشته باشد.

۸-۱-۳-۳ دامنه به کار انداختن

به کاراندازی باید انجام دهد:
الف) اعتماد سازمان را از این‌که راهبردهای امکان‌بازگشت و بازیابی تمام الزامات کسب و کار را بر آورده می‌کند، بالا ببرد؛
ب) نشان می‌دهد که خدمات بحرانی ICT می‌توانند در سطح خدمات مورد توافق یا اهداف بازیابی، بدون در نظر گفتن رخداد، حفظ و بازیابی داده شوند؛

1 - failover
2 - platform

پ) نشان می‌دهد که خدمات بحرانی ICT می‌توانند در صورت وقوع رخداد در محل بازیابی به حالتی قبل از وقوع رخداد برگردند؛

ت) فراهم کردن فرصت برای کارکنان تا آنها با فرآیند بازیابی آشنا شوند؛

ث) آموزش کارکنان و حصول اطمینان از این‌که آن‌ها دانش کافی از طرح‌ها و روش‌های IRBC دارند؛

ج) بررسیIRBC که هماهنگ با زیرساخت‌های ICT و زیرساخت‌های عمومی باقی مانده است؛

چ) هر گونه پیشرفت که برای راهبردهایIRBC، معماری یا بازیابی فرایندها مورد نیاز است را شناسایی کند؛ و

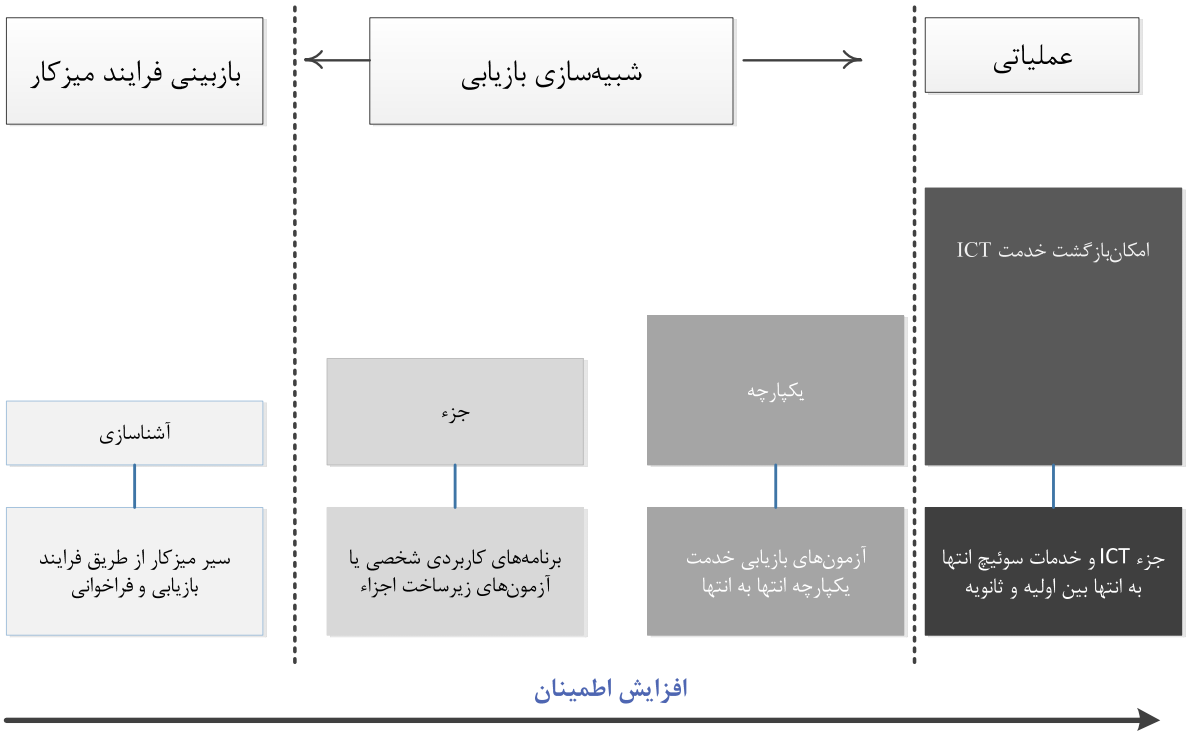
ح) ارائه شواهد برای مقاصد ممیزی و نشان دادن صلاحیت خدمات سازمان ICT.

تمرین را باید برای کل محیط ICT و تمام اجزایی که خدمات انتها به انتها از طریق اتاق کامپیوتر برای کامپیوتر کاربر و یا هر کانال ارائه خدمات دیگر ارائه می کنند بکار برد.

۸-۱-۳-۴ عناصر بازیابی خدمات

سازمان باید تمام عناصر بازیابی خدمات ICT را با توجه به اندازه‌ی آن، پیچیدگی آن و اهداف مدیریت تداوم کسب و کار، مورد آزمایش قرار دهد. به کاراندازی نباید صرفا برروی خدمات بازیابی و از سرگیری تمرکز داشته باشد بلکه باید ظرفیت پاسخ به مشکلات و سامانه پایش و هشدار مدیریتی را در به کاراندازی دخیل کند.

سازمان باید با به کاراندازی در سطح جزئیات از طریق آزمایش کامل سامانه مبتنی بر موقعیت به سطح بالایی از اعتماد به نفس و امکان‌بازگشت برسد.



شکل ۶ : پیشرفت به کاراندازی برنامه و تمرین

عناصر زیر باید اعمال شوند :

الف) اتاق کامپیوتر، مانند امنیت فیزیکی، سامانه تشخیص آتش سوزی ونشت آب، فرآیند تخلیه ؛ گرمایش، تهویه و تهویه سرمایش،پایش بر محیط زیست، و پروتکل‌های هشدار و خدمات برق؛

ب) زیرساخت‌ها، ازجمله امکان‌بازگشت کلی اتصال به شبکه، تنوع شبکه و امنیت شبکه، از جمله حفاظت ضد ویروس و پیشگیری از نفوذ و تشخیص؛

پ) سخت افزار، از جمله خدمت دهنده‌ها، تجهیزات ارتباطات راه دور، ارایه‌های ذخیره سازی و رسانه‌های جدا شدنی؛

ت) نرم افزار؛

ث) داده‌ها؛

ج) خدمات؛ و

چ) نقش و پاسخ تأمین کنندگان.

۸-۱-۳-۵ برنامه‌ریزی به کارانداختن

برای حصول اطمینان که به کاراندازی سبب رخداد نمی‌شود و یا تضعیف توانایی خدمات اتفاق نمی‌افتد، به کاراندازی باید به دقت برنامه‌ریزی شود تا مخاطره وقوع رخداد به صورت یک نتیجه مستقیم به کاراندازی به کمینه برسد.

مدیریت مخاطره باید با سطح به کاراندازی در حال انجام مناسب باشد (یعنی عناصر بازیابی خدمات) که این ممکن است شامل :

الف) اطمینان حاصل کردن که همه داده‌ها سریعا قبل از به کارانداختن پشتیبان گرفته می‌شود؛

ب) هدایت و انجام به کاراندازی در محیط‌های ایزوله شده.؛ و

پ) زمان‌بندی به کاراندازی «ساعات خارج از خدمت » یا در طول زمان‌های سکون[1] در چرخه کسب و کار (زمان با ترافیک کاری کم) با علم کاربران نهایی زمان بندی می شود.

به کاراندازی‌ها باید واقع بینانه، به دقت برنامه‌ریزی شده و همراه توافق با سهامداران باشد، به طوری که کمینه مخاطره اختلال در فرآیندهای کسب و کار وجود داشته باشد. با این حال، آن‌ها نباید، در طی رخداد، انجام شوند.

مقیاس و پیچیدگی به کاراندازی‌ها باید برای بازیابی اهداف سازمان مناسب باشد.

هر به کاراندازی باید یک«مرجع» داشته باشد، از طرف سازمان پذیرفته و در پیشبرد به کاراندازی توسط حامی تایید شود.

که ممکن است شامل موارد زیر باشد :

الف) توصیف؛

ب) اهداف؛

پ) دامنه (مقصود و انتظارات)؛

ت) پیش فرض‌ها؛

ث) محدودیت؛

ج) مخاطرات؛

چ) معیارهای موفقیت؛

ح) منابع؛

خ) نقش‌ها و مسؤولیت‌ها؛

د) برنامه / خطزمانی سطح بالا (مشخص)؛

ذ) به کاراندازی گرفتن داده(ذخیره سازی اطلاعات قالب)؛

1 - quiet times

ر) ثبت به کاراندازی / رخداد (که در زمان های متوالی اتفاق می افتند)؛

ل)گزارش گیری؛ و

م) اعمال پس از به کاراندازی (پیگیری و گزارش).

برنامه‌ریزی یک به کاراندازی باید سازمان را قادر به دستیابی به معیارهای موفقیت شناسایی شده کند.

۸-۱-۳-۶ مدیریت به کاراندازی

ساختار فرماندهی روشن باید با توجه به نقش‌ها و مسئولیت‌ها، به کاراندازی را به افراد مناسب اختصاص دهد.
ساختار فرماندهی به کاراندازی ممکن است شامل موارد زیر باشد :

الف) فرمانده به کاراندازی (همراه(ها) با کنترل کلی آزمون و تمرین)؛

ب) ارتباطات به کاراندازی ؛

پ) تایید کند که کارکنان به اندازه کافی برای انجام به کاراندازی با ایمنی در دسترس باشند؛

ت) ناظران کافی و یا تسهیل کننده به منظور ذخیره اقدامات به کاراندازی و حفظ مسائل ثبتی؛

ث) معیارهای کلیدی به کاراندازی ؛

ج) حدود پایانی پروتکل به کاراندازی ؛ و

چ) قوانین توقف اضطراری به کاراندازی.

به کاراندازی باید از طریق فرمان به کاراندازی اجرا شود تا اطمینان حاصل شود که :

الف) اهداف و حدود پایانی کلیدی را برآورده کند؛

ب) تمام مواد به کاراندازی و فعالیتها دارای سطوح مناسب محرمانه باشند؛

پ) هر گونه مخاطرات جاری، پایش و کاهش بیابد؛

ت) بازدید کنندگان /ناظران تائید صلاحیت شوند؛

ث) اقدامات به کاراندازی باید به شیوه ای سازگار ذخیره شود؛ و

ج) تمام شرکت‌کنندگان باید نظرشان را در مورد به کاراندازی بیان کنند.

۸-۱-۳-۷ بازنگری، گزارش و پیگیری

در پایان به کاراندازی ، باید یافته‌های به کاراندازی بلافاصله مورد بازنگری و پیگیری قرار گیرند. این امر باید شامل موارد زیر باشد:

الف) جمع آوری نتایج و یافته‌ها؛

ب) تجزیه و تحلیل نتایج و یافته‌ها دربرابر اهداف به کاراندازی و معیارهای موفقیت؛

پ) شناسایی شکاف‌ها؛

ت) انتصاب نقاط عمل با خط زمانی تعریف شده؛

ث) ایجاد یک گزارش به کاراندازی برای ملاحظه رسمی توسط حامی به کاراندازی ؛ و

ج) تحکیم و پیگیری گزارش عملیات به کاراندازی.

۸-۲ ممیزی داخلي IRBC

طرح‌های ممیزی داخلی IRBC باید معیارهای ممیزی، دامنه، روش و فراوانی را تعریف و مستند کند (برای مثال ممیز داخلی IRBC انجام شده در سال).

طرح ممیزی باید تضمین کند که فقط ممیزان داخلی واجد شرایط برای ممیزی منصوب می شوند. انتخاب ممیزان و اجرای ممیزی باید بی طرفی و عینیت فرآیند ممیزی را تضمین کند. ممیزان داخلی انجام ممیزی IRBC باید صلاحیت انجام کار و وظایف خود را داشته باشند. برای مثال، ممیزان باید در دوره‌های آموزشی ممیز مربوطه به طوری که به مهارت و دانش لازم دست پیدا کنند برای انجام ممیزی شرکت کنند. روشی باید برای حصول اطمینان از این که کمبودهای شناسایی شده در ممیزی داخلی IRBC جبران شوند، ایجاد شود.

طرح ممیزی باید شامل همکاران و طرف‌های خارجی نیز بشود. به عنوان مثال عوامل فروش بیرونی باید توانایی خود را برای پشتیبانی از راهبردهای IRBC و طرح‌های سازمان در طول عملیات روزانه و پاسخ به بازیابی رخدادهای ممیزی اعلام کنند.

ممیزی داخلی زمانی که تغییرات بسزایی در خدمات بحرانی ICT، الزامات تداوم کسب و کار (به صورتی که مربوط به اهداف IRBC باشد) و یا الزامات IRBC به وجود می‌اید؛ باید انجام شود.

نتایج حاصل از ممیزی داخلی IRBC باید ثبت و گزارش شود. مدیریت باید نتایج ممیزی داخلی IRBC و وضعیت پیگیری اقدامات اصلاحی را مورد بازنگری قرار دهد.

۸-۳ بازنگري مدیریت

۸-۳-۱ کلیات

مدیریت ارشد باید اطمینان حاصل کند از این که سامانه مدیریت IRBC در فواصل طراحی شده، بازنگری شده است. این بازنگری ممکن است ورودی ممیزهای داخلی یا خارجی یا خود ارزیابی باشد. بازنگری باید شامل ارزیابی فرصت‌ها برای بهبود و نیاز به تغییر در مدیریت IRBC، از جمله سیاست‌ها و اهداف IRBC باشد.

علاوه بر این، مدیریت ارشد باید به صورت سالانه الزامات IRBC مورد تایید را بازنگری کند که شامل تعاریف خدمات ICT، فهرست مستند شده خدمات بحرانی ICT و مخاطرات مرتبط با توجه به شکاف شناسایی شده بین قابلیت آمادگی بحرانی ICT و الزامات تداوم کسب و کار می باشد.

نتایج بازنگری باید به صورت واضح مستند شود و سوابق باید نگهداری شوند.

۸-۳-۲ ورودي بازنگري

ورودی برای بازنگری مدیریت باید دارای اطلاعات زیر باشد:

الف) سطح خدمات داخلی؛

ب) توانایی ارائه دهندگان خدمات خارجی برای حفظ سطح مناسب خدمات؛

پ) نتایج حاصل از ممیزی‌های مربوطه؛

ت) گرفتن بازخورد طرف‌های علاقه‌مند ازجمله نظرات مستقل؛

ث) وضعیت اقدامات پیشگیرانه و اصلاحی؛

ج) سطح مخاطره باقی مانده و مخاطره قابل قبول؛

چ) پیگیری اقدامات بازنگری و توصیه‌های مدیریت قبلی؛

ح) درس‌های آموخته شده از آزمون و به کاراندازی ، رخدادها و برنامه آموزش و آگاهی دهنده؛ و

خ) عمل و راهنمایی‌های خوب در حال ظهور.

۸-۳-۳ خروجي بازنگري

خروجی باید توسط مدیریت ارشد تأیید شود و شامل موارد زیر باشد :

الف) تغییر دامنه سامانه مدیریت IRBC؛

ب) بهبود اثر بخشی سامانه مدیریت IRBC؛

پ) تجدید نظر الزامات IRBC، ازجمله تعاریف خدمات ICT، فهرست مستند از خدمات بحرانی ICT و مخاطرات همراه با شکاف شناخته شده بین قابلیت‌های بحرانی آمادگی ICT و الزامات تداوم کسب و کار؛

ت) اصلاح در راهبرد IRBC و روش‌ها در صورت لزوم به منظور پاسخ به وقایع داخلی و/یا خارجی که می‌تواند بر خدمات ICT تأثیر بگذارد، این تغییرها عبارتند از:

۱) الزامات کسب و کار؛

۲) الزامات امکان‌بازگشت ؛ و

۳) سطح مخاطره و / یا سطح پذیرش مخاطره.

ث) نیازهای اساسی(منابع مورد نیاز)؛ و

ج) بودجه و الزامات بودجه.

۸-۴ اندازه‌گیري معیارهاي عملکرد آمادگیICT

۸-۴-۱ پایش و اندازه‌گیري آمادگیICT

سازمان باید آمادگی ICT خود را از طریق اجرای فرآیند اندازه‌گیری از معیارهای عملکرد تعریف شده آمادگی ICT پایش و اندازه‌گیری کند (به بند ۶-۷ مراجعه کنید)

۸-۴-۲ معیارهاي کمي و کیفي عملکرد

معیارهای عملکرد برای IRBC می‌تواند کمی و یا کیفی باشند.

معیارهای کمی ممکن است شامل موارد زیر باشد :

الف) بیش از یک دوره زمانی داده شده، و تعدادی از رخدادها که قبل از اختلال تشخیص داده نشده‌اند (این می‌تواند نشانه ای از تکامل طرزکارهای تشخیص و هشدار رفتاری ارائه کند)؛

ب) زمان تشخیص رخدادها؛

پ) تعدادی از رخدادها که نمی‌توان به طور مؤثر کاهش اثر داد؛

ت) در دسترس بودن منابع داده برای نشان دادن فوریت رخدادها از طریق روند پایش رویدادها؛ و

ث) زمان برای واکنش و پاسخ به رخدادهای نوظهور شناسایی شده.

معیارهای کیفی، داخلی هستند و به منظور تعیین عملکرد IRBC استفاده می‌شوند اما معمولا نیاز به منابع کمتر در فرآیند اندازه‌گیری دارند (که ممکن است برای یک سازمان در اندازه‌های کوچک یا متوسط مناسب باشد و این‌که مشروط به محدودیت منابع است).

این ممکن است شامل تعیین بهره‌وری از فرآیندهای مورد استفاده در برنامه‌ریزی ، تهیه و اجرای فعالیت‌های IRBC باشد و می‌تواند اندازه‌گیری شود از طریق:

الف) نظر سنجی با استفاده از پرسش‌نامه ساختار یافته یا بدون ساختار؛

ب) بازخورد از شرکت کنندگان و ذی‌نفعان؛

پ) انجام کارگاه‌های آموزشی بازخوردی؛ و

ت) دیگر دیدارهای گروهی متمرکز.

۹ بهبود IRBC

۹-۱ بهبود مداوم

سازمان باید به طور مداوم IRBC را از طریق بکار بردن اقدامات پیشگیرانه و اصلاحی بهبود دهد که برای اثرات بالقوه تعیین شده توسط آنالیز تأثیر سازمان کسب و کار (BIA) و مخاطره پذیری آن مناسب هستند.

۹-۲ اقدامات اصلاحي

سازمان باید اقداماتی به منظور تصحیح هر خرابی[1] واقعی خدمات ICT و عناصر IRBC انجام دهد. روش مستند برای اقدامات اصلاحی باید الزامات زیر را تعریف کند :

الف) شناسایی خرابی‌ها؛

ب) تعیین علل خرابی‌ها؛

پ) ارزیابی احتیاجات برای فعالیت‌هایی که از وقوع ناخشنودی‌ها جلوگیری می‌کند؛

ت) تعیین و پیاده سازی اقدامات اصلاحی مورد نیاز؛

ث) ثبت نتایج عمل گرفته شده؛ و

1 - failure

ج) بازبینی اقدامات اصلاحی گرفته شده.

۹-۳ اقدامات پیش گیرنده

این سازمان باید نقاط ضعف بالقوه عناصر IRBC را شناسایی و یک روش مستند برقراری کند برای :

الف) شناسایی خرابی‌های بالقوه؛
ب) شناسایی علل خرابی؛
پ) تعیین و پیاده سازی اقدامات پیش گیرانه مورد نیاز؛ و
ت)ثبت و بازبینی نتایج عمل گرفته شده.

پیوست الف
(اطلاعاتی)
IRBC و نقاط عطف در طول اختلال

شکل الف-۱ نشان می‌دهد که چطور عناصر IRBC در طول یک اختلال مهم نقاط عطف کلیدی را پشتیبانی می کنند. رخدادها و نقاط عطف در طول یک خط زمانی با شروع در زمان صفر[1] وقتی که در خدمات ICT اختلال / رخداد رخ دهد اتفاق می افتد. به عنوان نمونه سناریو رخدادی می‌باشد که شخصی حمله به سامانه تشخیص نفوذ (به صورت معمول «هک» نامیده می‌شود) در سامانه‌های بحرانی سازمان ICT را هدف قرار دهد.

نقطه بازیابی هدف (RPO) به میزان داده ای که به دلیل اختلال از دست رفته و غیر قابل دسترس است، بستگی دارد.

درخط زمان به عنوان مقدار زمان بین آخرین نسخه پشتیبان صحیح تهیه شده و هنگامی که رویداد اختلال رخ می‌دهد نشان داده می شود. RPO به صورت متغیر نسبت به راهبرد بازیابی خدمات ICT به خصوص در ترتیب پشتیبان گیری به کار گرفته می‌شود.

در حالت زمانی صفر، سامانه بحرانی ICT توسط هکرها مورد حمله قرار گرفته و خدمات از کار افتاده است. اولین اقدام بعد از وقوع اختلال در خدمات ICT تشخیص مستقیم رخداد امنیتی است (یعنی وقوع نفوذ) و یا تشخیص غیر مستقیم از بین رفتن خدمات (یا تخریب) که زمان سپری شده قبل از آگاه سازی خواهد بود، به عنوان مثال در برخی نمونه‌ها ممکن است آگاه سازی یک کاربر از طریق یک تماس با مرکز IT انجام گیرد.

زمان در مدتی که اختلال خدمات ICT شناسایی، تحلیل و ابلاغ می‌شود و تصمیمی مبتنی بر فراخوانی IRBC اتخاذ می‌شود، به آرامی سپری می‌شود. این ممکن است از شروع اختلال در خدمات ICT تا زمانی که یک تصمیم یک بار ارتباط و تصمیم گیری در مورد در نظر گرفتن زمان برای فراخوانی IRBC گرفته شود چندین ساعت زمان بگیرد. تصمیم فراخوانی ممکن است به در نظر گرفتن دقت در برخی از موقعیت‌ها نیاز داشته باشد برای مثال جاییی که خدمات به صورت کامل از بین نرفته باشند یا احتمال زیادی برای بازیابی خدمات وجود داشته باشد چون فراخوانی IRBC اغلب بر روی عملیات کسب و کار عادی اثر می گذارد.

به محض فراخوانی، بازیابی خدمات ICT می‌تواند شروع شود. این را می توان به زیرساخت‌های (شبکه، سخت افزار، سامانه عامل، نرم افزار پشتیبان و غیره) و بازیابی قسمت برنامه‌های کاربردی (پایگاه داده، برنامه‌های کاربردی،فرآیندهای دسته ای، واسطها و غیره) تقسیم کرد.

(برای اطلاعات بیشتر به ISO/IEC 24762 مراجعه کنید)

1 - Time Zero

به محض این که خدمات ICT بازیابی شد و آزمایش سامانه توسط کارمند ICT انجام شد، میتوان خدمات را به صورت آزمایشی قبل از این‌که به صورت کامل در اختیار کارمندان برای استفاده در عملیات تداوم کسب وکار باشد، در دسترس برخی از کاربران مورد تایید قرار بگیرد.

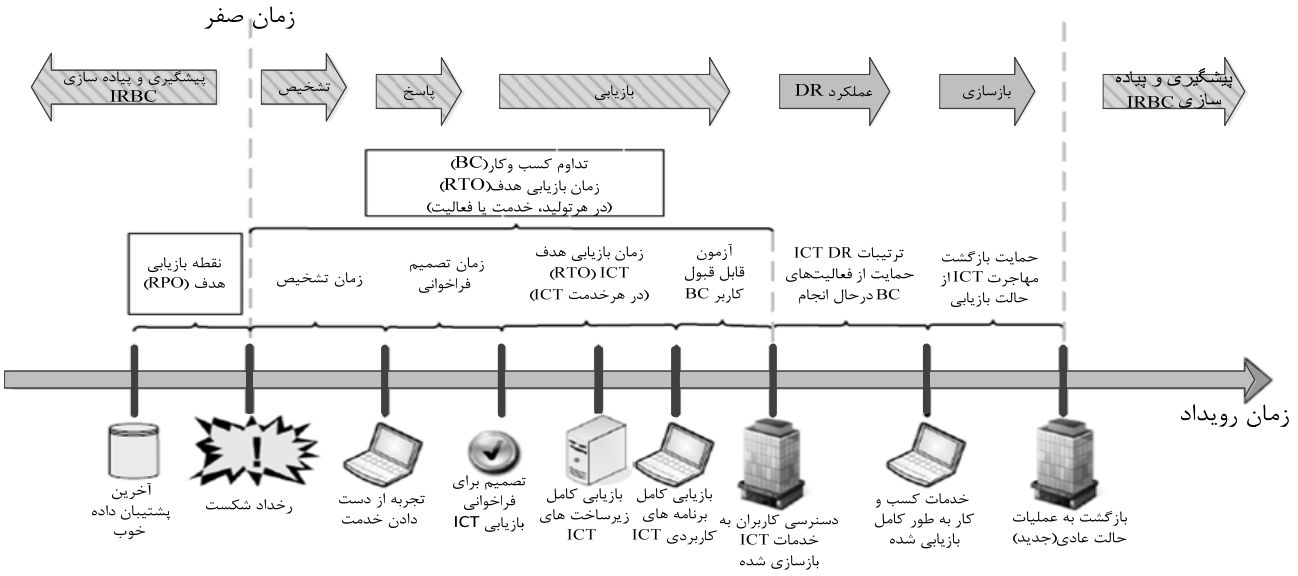
از نظر چشم انداز تداوم کسب و کار برای هر محصولی ، خدماتی و یا فعالیتی، یک زمان بازیابی هدف (RTO) وجود دارد و از زمانی که در آن اختلال رخ می‌دهد و اجرا می‌شود تا زمانی که محصول، خدمات و یا فعالیت‌ها بازیابی یابند در بر میگیرد ولی ممکن است بعضی خدمات ICT برای فعال کردن این و هریک از این خدمات ICT نیاز شوند که می‌توانند تعدادی از سامانه‌های ICT یا برنامه‌های کاربردی را تشکیل دهند.

هر کدام از این مؤلفه‌های سامانه ICT یا برنامه‌های کاربردی، RTO مجزای خود را به صورت یک زیر مجموعه از RTO خدمات انتها به انتها ICT دارند و باید کمتر از RTO تداوم کسب و کار بوده و با توجه به تشخیص و تصمیم گیری زمان و زمان آزمایش مورد تایید کاربر، باشد (مگر این‌که محصول تداوم کسب و کار، خدمات و یا فعالیت‌ها بتوانند بدون ICT برای یک دوره زمانی پشتیبانی شوند برای مثال استفاده از روش آیین نامه).

بازیابی خدمات ICT به طور معمول عمل برای یک دوره زمانی از اقدامات تداوم کسب و کار را پشتیبانی می‌کند واگر این دوره طولانی باشد آنگاه بازیابی خدمات ICT ممکن است نیاز به تقویت برای پشتیبانی از افزایش حجم فعالیت‌ها، بالا بردن توان بالقوه برای نقطه ای که در آن (زمانی که) محصول، خدمات یا فعالیت‌ها به صورت حجم تراکنش عادی بازیابی می‌شوند داشته باشد.

در نتیجه، در چند نقطه در طول خط زمانی، بازسازی امکان پذیر و مطلوب خواهد بود و عملیات DR به عملیات «عادی» برگشت خواهد یافت. بازگشتن به عملیات طبیعی می‌تواند حالت کلی یا حالت محیطی قبل از اختلال یا یک ترتیب عملیاتی جدید باشد (به ویژه زمانی که رخداد اختلال اجبار تغییر دائمی بر کسب و کار داشته باشد).

با این‌که کارمندان ICT زمان دارند تا به دقت طرح را در طول یک دوره فعالیت طبیعی کم برنامه‌ریزی و بازسازی کنند با این حال این کار آن‌ها یک کار قابل توجه است. پیکان‌های در بالای نمودار نشان می‌دهد که چگونه اصول IRBC ذکر شده در اختلال ISO/IEC 27031 در راستای خط زمانی قرار می‌گیرد.



شکل الف-۱ –IRBC و شاخص کار درطی یک اختلال

پیوست ب

(اطلاعاتی)

سامانه‌های جاسازی شده با دسترسی بالا

در فناوری اطلاعات و ارتباطات، «دسترسی بالا» به سامانه یا مؤلفه‌هایی اطلاق می‌شود که به صورت مداوم قابلیت عملیات برای یک دوره زمانی طولانی را داشته باشند. در دسترس بودن می‌تواند با نسبت «صد درصد عملیاتی» و یا «عدم خرابی» اندازه‌گیری شود. شاید این امر بسیار سخت باشد اما رسیدن به یک استاندارد سخت در دسترس برای یک سامانه یا محصولی که آن را با نام «five 9s» (۹۹.۹۹۹ درصد) می شناسیم در دسترس می باشد.

یک سامانه کامپیوتر و یا شبکه از مولفه‌های بسیاری ساخته شده است که معمولا تمام آن‌ها نیاز به حضور و کارکرد با نظم خاصی در طول عملیات سامانه هستند و وقتی طراحی برای دسترسی بالا، اغلب بر روی فرآیند پشتیبانی و شکست و ذخیره سازی داده ها و دسترسی تمرکز دارد، آنگاه دیگر مؤلفه‌های زیر ساختی از جمله برق و سامانه‌های خنک کننده بسیار اهمیت پیدا می کنند.

به عنوان مثال، در دسترس بودن برق را می توان با چنین اقداماتی تضمین کرد :

الف) استفاده از تغذیه برق بی وقفه (UPS[1])؛

ب) برقراری ظرفیت برق اضطراری؛

پ) منبع دوگانه برق از یک شبکه[2] ؛

تهیه نسخه پشتیبان داده ها و در دسترس قرار دادن را می توان با استفاده از انواع فناوری‌های ذخیره سازی فراهم کرد مانند لوح‌های افزونه (RAID[3])، ذخیره سازی در سطح شبکه (SAN[4]) و غیره.

نیاز به دسترس پذیری برنامه‌های کاربردی نیز در نظر گرفته شود و اغلب از طریق خوشه‌بندی بدست می آید.

چنین فناوری‌هایی فقط می‌تواند در ارئه دسترسی بالا از طریق پیاده‌سازی هم زمان در بیش از یک موقعیت ، واقعا مؤثر باشد. به عنوان یک مثال ساده، فرض کنید که خدمت‌گذار failover در موقعیتی مشابه به صورت اولیه ویا خدمت‌گذار تولید، در صورتی که قسمت را یک اختلال جدی تحت تأثیر قرار دهد سطح لازم از امکان‌بازگشت را ارائه نمی کنند قرار داشته باشند. هر دو خدمت‌گذار توسط همان اختلال تحت تأثیر خواهند بود. خدمت‌گذار failover و دیگر فناوری‌های پشتیبانی واقع را برای بدست آوردن سطح مورد نیاز از دسترسی حدالامکان باید در قسمت دیگری قرار داد.

این کار برای بسیاری از سازمان‌ها در دستیابی به سطوح دسترسی بالا، هزینه و تلاش را شامل می‌شود که می‌تواند دلهره‌آور باشد و در سال‌های اخیر رشد زیادی در استفاده از ارائه دهندگان خدمات طرف ثالث

1 - Uninterruptible Power Supply
2 - grid
3 - Redundant Array of Disks
4 - Storage Area Network

داشته است که قادر به ارائه مهارت، منابع و فناوری‌های انعطاف پذیر در هزینه‌های مقرون به صرفه از طریق ارائه خدمات مدیریتی و یا خدمات ابری[1] می باشند.
با این حال باید به یاد داشت در حالی که در دسترس بودن بالا راه مؤثری برای افزایش امکان‌بازگشت است اما امکان خرابی وجود دارد. بنابراین بسیار حیاتی است که روش و فرآیند DR طراحی و آزمون شده در جای درست بکار گرفته شود

1 - cloud services

پیوست پ

(اطلاعاتی)

سنجش سناریوهای خرابی

پ -۱ کلیات

طیف از فنون بالقوه مدیریت مخاطرات وجود دارد که می‌تواند در سنجش آمادگی ICT برای BC و در توسعه یک چهارچوب مناسب برای ادامه توسعه و افزایش امکان‌بازگشت ICT کمک کند.

استاندارد ISO 31010:2009 « مدیریت مخاطرات– فنون سنجش مخاطرات» در نظر گرفته می‌شود تا به خوبی منعکس کننده تمرین‌های فعلی در انتخاب و استفاده از فنون سنجش مخاطره‌ها باشد. مرجع باید این استاندارد را برای تعیین مناسب ترین فنی که می‌شود در درون سازمان مورد استفاده قرار داد برقرار کند.

سنجش حالت خرابی روشی(سناریو) است که ممکن است در افزایش تأثیر گزاری IRBC مفید باشد و این پیوست اطلاعات بیشتر در مورد این‌که چگونه ممکن است آن پیاده سازی شود را فراهم کند.

پ-۲ روش سنجش

مسائل مربوط به مخاطره ناشناخته ممکن است بین سنجش به عنوان یک نتیجه از تغییرات در داخل و خارج محیط سازمان که ممکن است مانع تداوم کسب و کار و امکان‌بازگشت باشد پدیدار شود. منظور از سناریو سنجش خرابی این است که برای شناسایی شاخص‌های رویداد مناسب و حصول اطمینان که برنامه‌های IRBC، قادر به تشخیص پدیدار شدن چنین مسایل مربوط به مخاطره‌ها می‌باشد و قادر بودن به آماده سازی سازمان برای حصول اطمینان از اقدامات مناسب می‌تواند قبل از وقوع خرابی در نظر گرفته شود.

تعدادی از روش‌های شناسایی خاص برای چنین اهدافی در دسترس هستند که شامل تحلیل تأثیر حالت خرابی (FMEA[1]) و تحلیل تأثیر مؤلفه خرابی (CFIA[2]) می باشند. برای برهان اهداف، این پیوست به بسط روش شناسایی خاص FMEA می پردازد که از طریق یک سازمان باید یک روش مناسب برای چهارچوب و محیط آن انتخاب شود.

تحلیل تأثیر حالت خرابی FMEA، فرآیندی برای شناسای و تحلیل حالت‌های بالقوه خرابی یک سامانه برای طبقه بندی بر اساس شدت و یا تعیین تأثیر خرابی بر سامانه است. در متن این استاندارد، FMEA ممکن است برای تعیین رویداد بحرانی که باید به منظور شناسایی حالت‌های بالقوه تشدید خرابی در یک سامانه سازمان ICT پایش شود بکار برود. این فرآیند بر اساس رسیدن به FMEA می‌باشد که ممکن است برای هر یک از مؤلفه‌های بحرانی خدمات ICT همانطورکه در ۶-۳-۲ توضیح داده شد به کار برده شود.

برای هر یک از مؤلفه‌های بحرانی:

الف) شناسایی حالت بالقوه خرابی ؛

1 - Failure Mode Effect Analysis
2 - Component Failure Impact Analysis

ب) تعیین تأثیر بالقوه برای خدمات ICT یعنی، شدت هر یک از حالات خرابی و پیامدهای هر نتیجه؛
پ) فراوانی وقوع حالت خرابی که سازمان در تجربه قبلی داشته، و نیز سهولت پایش و تشخیص حالت خرابی مشخص می‌کند؛
ت) شاخص(های ارائه) یک سیگنال یا اطلاعات یک قسمت شکست خورده را مشخص می‌کند؛
ث) رویدادهای مستقیم و غیر مستقیم که به یکدیگر مربوط هستند و قصد تغییر حالت هر شاخص را دارند مشخص می‌کند؛
ج) کنترل‌های موجود که از خرابی اجزای بحرانی جلوگیری می کنند، یا می‌توانند وقوع چنین خرابی را تشخیص دهند مشخص می‌کند؛
چ) منابع داده مرتبط و روش‌های مناسب پایش برای شناسایی تغییرات میزان شاخص، رده‌بندی شاخص‌های رویداد با در دسترس قرار دادن روش پایش و آسوده کردن پایش را مشخص می‌کند؛ و
ح) اگر کاهش مخاطره‌ها مناسب و یا کنترل‌های رفع بتوانند برای جلوگیری از وقوع آن، اعمال شوند مشخص می‌کند.

پ-۳ نتایج سنجش

خروجی FMEA شامل لیستی از حالات خرابی بالقوه، اثرات و رویدادهای مرتبط آن است – ممکن است برای تعیین شاخص‌های رویدادی که نیاز به پایش داشته باشد مورد استفاده قرار گیرد.
شناسایی حالات خرابی از طریق فرآیند FMEA را می توان با توجه به شدت سنجش، فراوانی خود رخداد و ساده کردن تششخیص و پایش اولویت بندی کرد.
یک FMEA همچنین دانش اسناد جدید و اقدامات درباره مخاطره‌های ناشی از خرابی برای استفاده در تداوم بهبود است.
اگر FMEA در طول مرحله طراحی با هدف برای جلوگیری از خرابی در آینده استفاده شود، می توان از آن برای کنترل فرآیند قبل و در طول عملیات در حال انجام فرآیند استفاده کرد.
در حالت ایده آل، FMEA در طی اولین مراحل مفهومی طراحی شروع می‌شود و همچنان در طول عمر محصول یا خدمات ادامه پیدا می‌کند.

پیوست ت

(اطلاعاتی)

توسعه معیارهای عملکرد

از آنجایی که عملکرد IRBC برای هر سازمان با سازمان دیگر متفاوت است، هر سازمان باید معیارهای عملکرد IRBC و نگهداری آن‌ها را به عنوان قسمتی از فرآیند تداوم بهبود خود توسعه دهد.

رویکرد اساسی، استفاده از سناریو رخدادهای شناخته شده و رویدادهای مربوط به برقراری خطوط راهنمای پاسخ برای هر دسته بندی از رخدادها و رویدادهای مرتبط با آن به صورت زیر می‌باشد:

الف) به عنوان قسمتی از فرآیندهای ISMS و BCM، رخدادهای شناخته شده و شاخص رویدادهای مهم به صورت ورودی برای گام‌های بعدی استفاده می شوند.

ب) ارائه مجموعه‌ای از رخدادها شناخته شده (مانند نفوذ به کلمات عبور به دلیل خرابی خدمت‌گذار با توجه به ناکافی بودن فضای دیسک سخت).

پ) تعیین وقایعی که منجر به آن رخداد می‌شوند (مانند ناکامی در ورود به سامانه و استفاده از لوح سخت).

ت) تعیین زمان شناسایی مناسب (مانند آستانه رخدادها که باید به مدیر / سامانه، هشدار/ اطلاع رسانی شود).

ث) تعیین زمان پاسخ مناسب (مانند فرصت زمانی که مدیر برای پیشگیری از وقوع رخداد صرف می‌کند).

ج) دسته بندی وقایع به بلوک‌های زمانی پاسخ مطلوب و اقدام بر اساس نوع پاسخ به رخداد؛ وقایع ممکن است با تهدید گروه، گره برنامه های کاربردی، پاسخ گروه اقدامات و یا زمان پاسخ گروه طبقه بندی شوند.

چ) تصحیح ماتریس‌ها و اندازه‌گیری از طریق آزمایش سناریو و مشق / تمرین.

ح) انجام آزمایش برای تعیین این‌که آیا اقدامات برای پاسخ قابل اعمال است و این‌که آیا اهداف قابل دسترس، هستند.

خ) تصحیح دسته بندی‌ها، زمان پاسخ رویداد مورد نظر و اقدامات پاسخ به رویداد مورد نظر. (مانند جست و جوی روش‌های جایگزین برای پایش، شناسایی و اقدام).

د) بهبود به وسیله فراگیری رخدادهای جدید و سناریو خرابی و تکرار فرآیند.

کتاب‌نامه

[**1**] SS 540:2008, Singapore Standard for Business Continuity Management

[**2**] BS 25999-1:2006, *Business continuity management — Part 1: Code of practice*

[**۳**] استاندارد ملی ایران به شماره ۹۰۰۰ : سال ۱۳۸۷، *سیستم های مدیریت کیفیت - مبانی و واژگان*

[**۴**] استاندارد ملی ایران به شماره ۱۸۰۴۳ : سال ۱۳۸۸، *فن آوری اطلاعات - فنون امنیتی - انتخاب - استقرار و عملیات سامانه های تشخیص نفوذ*

[**۵**] استاندارد ملی ایران به شماره ۱-۹۷۹۶ : سال ۱۳۸۶، *فنآوری اطلاعات -مدیریت خدمات - بخش اول : مشخصات*

[**۶**] استاندارد ملی ایران به شماره ۲-۹۷۹۶ : سال ۱۳۸۶، *فن آوری اطلاعات -مدیریت خدمات -قسمت دوم-قواعد کاری*

[7] ISO 22301, *Societal security — Preparedness and continuity management systems — Requirements*2)

[**۸**] استاندارد ملی ایران به شماره ۲۴۷۶۲ : سال ۱۳۸۸، *فن آوری اطلاعات - فنون امنیتی - رهنمودهایی برای سرویس های بازیابی از حادثه در فن آوری ارتباطات و اطلاعات*

[**۹**] استاندارد ملی ایران به شماره ۲۷۰۰۳ : سال ۱۳۸۹، *فناوری اطلاعات - فنون امنیتی - راهنمای اجرای سامانه مدیریت امنیت اطلاعات*

[**۱۰**] استاندارد ملی ایران به شماره ۱۴۰۹۶ : سال ۱۳۸۹، *فناوری اطلاعات -فنون امنیتی-مدیریت امنیت اطلاعات –سنجش*

[**۱۱**] استاندارد ملی ایران به شماره ۱۴۵۶۰ : سال ۱۳۹۱، *مدیریت ریسک - تکنیک های ارزیابی ریسک*