پردیس بین الملل

مهندسی فناوری اطلاعات

پایان‌نامه کارشناسی ارشد

طرح مقابله با مخاطرات فناوری اطلاعات در صنایع کشتی سازی

از

مصطفی رحمانپور

استاد راهنما

دکتر رضا ابراهیمی آتانی

خرداد ماه ۱۳۹۰


بسم الله الرحمن الرحيم

مهندسی فناوری اطلاعات (تجارت الکترونیک)

طرح مقابله با مخاطرات فناوری اطلاعات در صنایع کشتی سازی

از

مصطفی رحمانپور

استاد راهنما

دکتر رضا ابراهیمی آتانی

استاد مشاور

دکتر شهریار محمدی

خرداد ماه ۱۳۹۰

فهرست مطالب

فهرست جداول

فهرست اشکال

فهرست علائم اختصاری

International Organization for Standardization (ISO)	سازمان بین المللی برای استاندارد سازی
National Institute of Standards and Technology (NIST)	موسسه ملی استانداردها و فناوری
Information Security Management System (ISMS)	سیستم مدیریت امنیت اطلاعات
Allowable Outage Time (AOT)	زمان مجاز قطعی
Business impact analysis (BIA)	تحلیل صدمات شغلی
Business Continuity Plan (BCP)	طرح تداوم کسب وکار
Business Recovery Plan (BRP)	طرح بازیابی کسب وکار
Chief Information Officer (CIO)	مدیر ارشد اطلاعات
Continuity Of Operations Plan (COOP)	طرح تداوم عملیات
Contingency Plan (CP)	طرح مقابله با مخاطرات
Information Technology Contingency Plan (ITCP)	طرح مقابله با مخاطرات فناوری اطلاعات
Line of succession (LOS)	تعیین جانشین
Mean Time between Failures (MTF)	زمان میانگین بین دوخرابی
Occupant Evacuation Plan (OEP)	طرح تخلیه اضطراری پرسنل
Points of contact (POC)	نقطه تماس
Recovery time objective (RTO)	حداکثر زمان قابل قبول قبل از عدم دسترسی به سیستم
Recovery point objective (RPO)	نقطه بازیابی داده ها برای تداوم پردازش
Service level agreement (SLA)	توافقنامه خدماتدهی

چکیده

طرح مقابله با مخاطرات فناوری اطلاعات در صنایع کشتی سازی

مصطفی رحمن پور

در عصر حاضر یافتن مکانی که تولید یا کسب و کار در آن انجام می شود بدون وابستگی به سیستم های فناوری اطلاعات شاید دوراز ذهن به نظر برسد به طور مثال سیستم های یکپارچه تولیدی- صنعتی ترکیبی ساخت یافته از اجزای متعدد سخت افزاری و نرم افزاری است که برای ارتباط و تبادل اطلاعات با یکدیگر از بستری مانند شبکه استفاده می نمایند. چنین سیستم هایی با وجود داشتن مزایای زیاد دارای معایبی نیز هستند. شاید بزرگترین عیب این سیستم ها تامین امنیت و یکپارچگی آنها در برابر مخاطرات فناوری اطلاعات و تبعات ناشی از اختلال در آنهاست. برای برطرف کردن این نقیصه طرح های سازمانی متفاوتی در حوزه های مختلف مانند امنیت، ایمنی، شرایط اضطراری، .... معرفی گردیده است که جامع ترین این طرح ها، طرح مقابله با بحران های فناوری اطلاعات یا ITCP است. یکی از صنایع مادر و مهم در هر کشور که پیشرفت آن نشان دهنده رشد و بالندگی کشور در فناوری های سطح بالا می باشد صنایع کشتی سازی است. فرآیند ساخت کشتی، فناوری های مرتبط و دانش کسب شده از آن، حاصل تلاش تیمهای مختلف و فعالیت گروهی بخشهای زیادی از یک صنعت کشتی سازی می باشد. ناگفته پیداست که بستر ارتباطی این فعالیتها و تیمها عمدتا زیرساختهای نرم افزاری و سخت افزاری موجود در حوزه فناوری اطلاعات می باشد و آسیب دیدن این زیرساختها می تواند فرایند جریان کار را مختل کرده و ضررهای سنگینی به سیستم تحمیل نماید. بنابراین برای اطمینان از تداوم جریان کار در هنگام بروز حملات و حوادث مرتبط با فناوری اطلاعات تهیه و اجرای ITCP اجتناب ناپذیر به نظرمی رسد. دراین پایان نامه الزامات، شرایط، روند تدوین ITCPو نمونه ای از آن برای یک صنعت تشریح شده است که می توان به عنوان الگویی برای سایر محیط های تجاری، صنعتی و اداری استفاده نمود.

واژه‌های کلیدی: مقابله با بحرانهای فناوری اطلاعات، کشتی سازی، امنیت

Abstract

Information Technology Contingency Plan in Shipbuilding
Mostafa Rahmanpour

An IT system is identified by defining boundaries around a set of processes, communications, storage, and related resources. Today there are many integrated systems with complicated software and hardware components that communicate together by network infrastructure. There are advantages and of course disadvantages to this type of systems maybe the biggest disadvantage of them is protecting confidentiality and integrity from information technology threats. For resolving this problem organizations has different plan in different scopes related to vision and mission such as Business Continuity Plan, Continuity of operations plan, incident response plan and etc but the best plan is information technology contingency plan that defined by National Institute of Standards and Technology (NIST).
IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. In recent years shipbuilding has been thrived in our country. Shipbuilding processes are hi-tech and complicated. Role of information technology in shipbuilding is very important therefore protecting all require infrastructure to building ships and related knowledge and intellectual properties is require.

Keywords: Information Technology Contingency Plan, Shipbuilding, Security.

فصل ۱

مقدمه

امروزه صنعت و فناوری اطلاعات آن چنان در هم تنیده شده اند که تولیدات صنعتی در بسیاری از صنایع بدون بهره گیری از سیستم های پیشرفته غیر ممکن یا در صورت امکان فاقد توجیه اقتصادی می باشد. یافتن راهی بهتر برای تولید، همواره عاملی مهم درایجاد وتوسعه اتوماسیون صنعتی بود که تنها محدود به فرایند های تولیدی نمی شد. در کشور ما نیز خود را به صورت سیستم هایی مانند پرداخت حقوق و دستمزد در بخش های اداری، مالی و پشتیبانی ظهور و بروز داد. با ورود فناوری اطلاعات به صنایع، دستگاه های رایانه ای جایگزین ابزارهای سنتی و دستی شدند سپس با توسعه سیستم های نرم افزاری و سخت افزاری و جایگزینی تدریجی فعالیتهای دستی در بخشهای اداری، فنی و تولیدی، فناوری اطلاعات به تدریج فراگیر شد. اما افزایش تعداد سیستم ها به صورت جزیره ای و عدم تبادل اطلاعات میان آنها باعث شد تا دریافت خروجی از یک سیستم برای تامین ورودی های سیستم دیگر به مشکلی بزرگ تبدیل شود. در این میان صنایع بزرگ به فکر رایانه ای کردن فراگیر و سیستماتیک فرایندهای تولیدی شدند. چنین سیستم هایی با استفاده از بانک های اطلاعاتی مشترک، نرم افزارها و سخت افزارهای پیشرفته به فعالیت هایی چون طراحی، ساخت، مهندسی، تست، تعمیرات و مونتاژ به کمک رایانه می پردازند.

از طرف دیگر مهمترین جنبه هر فرایند شغلی، نیروی انسانی است. آنها نیازمند دسترسی به منابع و اطلاعات هستند. آنها نیازبه برقراری ارتباط با یکدیگر دارند. آنها نیازبه ابزارهایی برای بهبود عملکرد خویش می باشند. آنها زمانی که راه را به اشتباه می روند نیازمند پشتیبانی هستند. آنها نیازمند نظارتند. محرمانگی نیز یکی از نیازمندیهای اصلی نیروی انسانی است. این نیازمندیها فاکتورهایی در فعالیت های شغلی می باشد که ما را به سوی امنیت رهنمون می سازند .

اطلاعات یکی از بخشهای مهم هر فرآیند شغلی است. آن را می توان عنصر اولیه سازنده، یکی از اجزای میانی و حتی بخشی از محصول نهایی محسوب کرد. امنیت اطلاعات یکی از نیازمندیهای اصلی برای هر شغلی است که باید به نحو مطلوب مدیریت شود. مدیریت صحیح امنیت اطلاعات می تواند از دست دادن اطلاعات و از کار افتادگی تجهیزات و سرویس جلوگیری کند[۱].

اگرچه رسیدن به امنیت کامل غیر ممکن است، عدم وجود آن می تواند هزینه های گزافی را به سازمان تحمیل کند. میزان امنیت مورد نیاز هر سازمان منحصر به فرد می باشد و بستگی به چشم انداز و ماموریت آن سازمان دارد [۲].

امنیت را می توان در دو طیف بررسی کرد یکی دزدی اطلاعات و دیگری تخریب آن. بعضی از سازمان ها نگران تخریب داده ها هستند و نگرانی از بابت دزدی اطلاعات ندارند و برخی دیگر نیازمند حفاظت از سرمایه های فکری خود هستند زیرا تمام سرمایه آنهاست. سایر سازمان ها در حد وسط قراردارند و می خواهند از هر دو طیف مراقبت کنند.

شاید روزی نباشد که خبری در مورد حوادث امنیتی مانند از بین رفتن وب سایت ها، هک شدن سرور ها، نشت اطلاعات وازبین رفتن تجهیزات فناوری اطلاعات در گوشه و کنار جهان به گوش نرسد. سازمان ها نیاز دارند تا منابع بیشتری را صرف

حفاظت از سرمایه های اطلاعاتی خود کنند و امنیت اطلاعات یکی از دغدغه های اصلی دولت ها و مشاغل است. برای رسیدن به این منظور تعدادی از دولتها و سازمانها معیار ها، استانداردها و قوانینی را وضع کرده اند. از این میان سازمان های ISO و NIST پیشرو می باشند. ISO یک سازمان بین المللی غیر دولتی می باشد که مهمترین استانداردهای امنیت آن عبارتند از[۳]:

- ISO/IEC 27002:2005

این استاندارد آیین نامه مدیریت امنیت اطلاعات است و شامل یک راهنمای پایه و عملیاتی برای جاری سازی استانداردهای امنیت سازمانی و کاربردهای مدیریتی موثر می باشد.

- ISO/IEC 27001:2005

استاندارد نیازمندیهای سیستم مدیریت امنیت اطلاعات که به برپایی، پیاده سازی، عملیاتی کردن، نظارت، بازبینی، نگهداری و بهبود مستندات ISMS می پردازد.

- ISO/IEC 15408

استاندارد ارزیابی شرایط برای امنیت فناوری اطلاعات که به ارزیابی، اعتبار سنجی و تصدیق امنیت سیستم های فناوری اطلاعات می پردازد.

- ISO/IEC 13335

استاندارد مدیریت امنیت فناوری اطلاعات که شامل مفاهیم و مدل امنیت، مدیریت و طراحی امنیت، تکنیک های مدیریت امنیت، انتخاب حفاظ های امنیتی برای سیستم های فناوری اطلاعات می شود.

- ISO/IEC 24762:2008

این استاندارد راهنمایی برای بازیابی سرویس های مرتبط با فناوری ارتباطات و اطلاعات پس از وقوع بلایا فراهم می آورد.

NIST موسسه ای وابسته به وزارت بازرگانی ایالات متحده امریکا می باشد که مسئولیت جاری سازی فنی، فیزیکی، اجرایی و مدیریتی استانداردهای امنیت اطلاعات را برعهده دارد. برخی از استانداردهای آن عبارتند از:

- NIST 800-27 (اصول مهندسی برای امنیت فناوری اطلاعات)
- NIST 800-30(راهنمای مدیریت ریسک برای سیستم های فناوری اطلاعات)
- NIST 800-33(مدل های فنی برای امنیت فناوری اطلاعات)
- NIST 800-34(راهنمای مقابله با مخاطرات فناوری اطلاعات)
- NIST 800-36(راهنما برای انتخاب محصولات امنیت فناوری اطلاعات)

- NIST 800-84(راهنمای برنامه های تست، آموزش و تمرین برای طرح های فناوری اطلاعات)
- NIST 800-100(کتابچه امنیت اطلاعات : راهنمای مدیران)
- NIST 800-115(راهنمای فنی برای تست و ارزیابی امنیت اطلاعات)

سازمان ها نیازبه طرح های مناسبی دارندتاخودرابرای پاسخگویی، تداوم، بازیابی وازسرگیری فرایندهای شغلی وسیستمهای فناوری اطلاعات درهنگام وقوع اختلالات آماده کنند.هرطرح هدف وبرنامه خاصی دارد. حال اشاره ای کوتاه به طرح های موجود در این حوزه می کنیم[۴]:

۱- BCP (Business Continuity Plan): مخاطب یکBCP استمرارعملیات شغلی وسیستم های فناوری اطلاعات درحین و بعد از اختلال سیستم است.

۲- BRP (Business Recovery Plan): استمرار رویه هایی ازفرآیندهای شغلی رادر یک محل دیگرمستند می کند. برخلاف یکBCP هدف BRP استمرارفرآیندهای شغلی درحین اختلال نیست.

۳- DRP (Disaster Recovery Plan): به یک طرح مبتنی برفناوری اطلاعات که برای بازیابی عملیات سیستم موردنظر، برنامه یا وسیله رایانه ای دریک محل دیگرپس ازوقوع یک فاجعه طراحی شده است، اشاره دارد.

۴- ITCP (Information Technology Contingency Plan): رویه هایی برای بازیابی واستمرار یک سیستم فناوری اطلاعات فراهم می آورد. دامنه این طرح گسترده ترازDRP است به این علت که شامل رویه هایی برای بازیابی یک سیستم می شود که درنتیجه اختلالات کوچک بوجود آمده و ضرورتا"نیازی به جابجایی به یک محل دیگر را ندارد.

۵- CIRP (Cyber Incident Response Plan): رویه هایی برای توانمندساختن پرسنل بخش امنیت برای تشخیص، کاهش وبازیابی حملات برضدسیستمهای فناوری اطلاعات ایجادمی کند.

۶- OEP (Occupant Emergency Plan): دستورالعمل هایی برای کارکنان ایجاد می کندتادرشرایط اضطراری باعمل به آن ایمنی وسلامت پرسنل، محیط یا اموال حفظ شود.

با توجه به نو پا بودن صنعت کشتی سازی در کشور و وابسته بودن آن به سیستم های فناوری اطلاعات و اهمیت حفاظت از این سیستم ها در برابر تهدیدات مرتبط با فناوری اطلاعات و عدم توجه صنایع و سازمان ها به این مساله و همچنین وجود استانداردهای بین المللی در این مورد، موضوع این پایان نامه طرح مقابله با بحران های فناوری اطلاعات در صنعت کشتی سازی انتخاب گردید تا ضمن بررسی و پیاده سازی آن در یک صنعت، علاوه برنحوه پیاده سازی این طرح، توجه سایر صنایع و سازمان ها را به خود معطوف سازد تا علاج حادثه قبل از وقوع کنند.

فصل۲

آشنایی با

ITCP(Information Technology Contingency Plan)

۳ – ۱ – مقدمه

سیستم های فناوری اطلاعات به وسیله مرزهایی در اطراف فرایندها، ارتباطات،رسانه های ذخیره سازی و منابع مرتبط قابل شناسایی است. نیازی نیست همه اجزای یک سیستم اطلاعاتی به طور فیزیکی به یکدیگر مرتبط باشند مانند گروهی از رایانه ها ی مجزا در یک سازمان یا گروهی از رایانه ها که در خانه های کارمندان قرار دارند و از طریق یک سیستم ارتباطی مشخص بایکدیگر متصلند یا گروهی از رایانه های همراه که در اختیار کارمندانی قراردارند که جهت انجام کارهای روزانه خود نیاز به جابجایی دارند و یا یک سیستم با پیکربندی خاص که در مکانهایی با محیط یکسان و کنترلهای فیزیکی نصب گردیده است [۵].

سیستم های فناوری اطلاعات به وسیله طیفی از اختلالات آسیب پذیر است. محدوده ای از حد اختلالات ملایم مانند قطع برق یا مشکل هارد تا حدشدید مانند نابودی تجهیزات، آتش سوزی و سایر بلایای طبیعی و حتی حملات تروریستی.

شاید بتوان تعدادی از این آسیبها را تاحد ممکن به حداقل رساندیا با به کارگیری راه حل های مدیریتی، فنی و عملیاتی تقلیل داد، اما کاهش همه ریسکها بطور کامل غیر ممکن است. در بسیاری از موارد منابع بحرانی تحت تاثیر عوامل خارج از کنترل سازمان مانند نیروی برق و خطوط ارتباطی قراردارد.

فرایند ساخت کشتی، فناوری های مرتبط و دانش کسب شده از آن، حاصل تلاش تیمهای مختلف و فعالیت گروهی بخشهای زیادی از یک صنعت کشتی سازی می باشد. ناگفته پیداست که بستر ارتباطی این فعالیتها و تیمها عمدتا زیرساختهای نرم افزاری و سخت افزاری موجود در حوزه فناوری اطلاعات می باشد و آسیب دیدن آنها می تواند جریان کار را مختل کرده و ضررهای سنگینی به صنعت تحمیل نماید.

ITCP(Information Technology Contingency Plan) یک طرح مقابله با حوادث احتمالی یا یک استراتژی بازیابی برای سیستمهای فناوری اطلاعات، عملیات و داده ها قبل، در حین و بعد از بروز آسیب دیدگی می باشد.

۳ – ۲ – اهداف پیاده سازی طرح ITCP

۱- آمادگی برای رویارویی با چالشهای ناشی از تهدیدات شناخته شده فناوری اطلاعات در تحلیل صدمات شغلی.

۲- اطمینان از تداوم کارایی عملیات سازمانی در طول موقعیت های اضطراری در سیستم های فناوری اطلاعات.

۳- حفاظت از تجهیزات و سرمایه های فناوری اطلاعات.

۴- کاهش یا تقلیل انقطاع عملیات.

۵- کاهش آسیب های فناوری اطلاعات و از دست دادن اطلاعات.

۶- برگشت سریع و منظم به حالت اولیه پس از وقوع بحرانهای فناوری اطلاعات[۶].

۳-۳- مخاطبین طرح

مخاطبین ITCP افراد ذیل می باشند :

۱- مدیران که مسئول بازبینی عملیات و فرایند های سازمانی مبتنی بر فناوری اطلاعات هستند.

۲- سرپرستان سیستم که مسئول نگهداری روزانه سیستم های فناوری اطلاعات هستند.

۳- افسران امنیتی سیستم های اطلاعاتی و کارمندانی که مسئول توسعه، پیاده سازی و نگهداری فعالیتهای امنیتی فناوری اطلاعات هستند.

۴- مهندسان و معماران سیستم ها که مسئول طراحی، پیاده سازی یا تغییر سیستم های اطلاعاتی هستند.

۵- کاربرانی که بوسیله ابزارهای فناوری اطلاعات به انجام کارهای روزانه خود می پردازند.

۳-۴- نتیجه طرح

نتیجه اجرای طرح ITCP کتابچه ای می باشد که کارکنان درگیر در صنایع متناسب با سطح دسترسی از مفاد آن اگاه شده و هرکس نقش خود را در فرایند مقابله با حملات و درنتیجه حفظ، پشتیبانی و بازیابی اطلاعات حساس، سرویسها، نرم افزارها، بانکهای اطلاعاتی و ... می داند و به آن طبق دستورالعملهای موجود عمل می نماید.

۳-۵- جایگاه مدیریت ریسک در ITCP

مدیریت ریسک شامل طیف گسترده ای ازفعالیت ها برای تشخیص، کنترل وکاهش ریسکها برای یک سیستم فناوری اطلاعات می شود. مدیریت ریسک بایداحتمال آسیب را باپیاده سازی کنترل های امنیتی کاهش دهد تا از سیستم برضدتهدیدات محیطی، انسانی وطبیعی حفاظت شود .مدیریت ریسک همچنین باید شامل فعالیت هایی برای کاهش یامحدودکردن ریسک

های ناشی از اختلالات موقت سیستم باشد. این معیارها پایه وشالوده شکل گیری ITCP است زیرا به پیش بینی احتمال وقوع حوادث و اقدامات پس ازآن می پردازد[۷].

۳ – ۶ – گام های طرح

اولین گام درفرآیند ITCP تدوین یک خط مشی توسط مدیر ارشدیا افسر ارشد اطلاعاتی می باشدکه اهداف ،دامنه کاربرد، مسئولیت ها و نقشها راپوشش می دهد. این سیاست ها باید شامل رویه هایی باشد که نیازمندی های آموزشی، پشتیبان گیری های مداوم، تمرین، تست ونگهداری طرح راشامل شود.

تحلیل صدمات شغلی (BIA) که دومین مرحله ازفرآیند ITCP می باشد. درواقع مرکزمشخص کردن استراتژی های بازیابی برای اطمینان از دسترسی می باشد. BIA مشخص کننده نیازمندی های سیستم، روابط داخلی آن، اولویت ها و فرآیند های مربوطه می باشد. BIA باورودی هایی مانند صاحبان سیستم،کاربران نهایی، ذینفعان داخلی وخارجی تغذیه می شود. باید منابع بحرانی برای انجام ماموریت سیستم های فناوری اطلاعات مشخص شود. رخدادهای احتمالی که باعث غیرقابل دسترس بودن این منابع می شود نیز باید مشخص گردد. بنابراین منابع مورد نیاز و اولویت بندی بازیابی پایه ایجاد راه حل های مقابله با بحران خواهد بود.

مشخص کردن نوع سایت جایگزین (Alternate site) برای استراتژی بازیابی نیز از BIA منتج می شود.انتخاب سایت جایگزین بایدازلحاظ هزینه بهینه باشد و نیازمندی های سیستم های اطلاعاتی راتامین کند. هرچنداگر سیستم اجازه چند روز قطعی رامی دهد انتخاب Cold site گزینه بهتری خواهدبود. دامنه تهدیدات احتمالی مشخص کننده فاصله سایت جایگزین از سایت اصلی است. هماهنگ کننده ITCP باید از تکنیک های تحلیل ریسک برای مشخص کردن منطقه جغرافیایی، نیازمندیهای دسترسی، نیازمندیهای امنیتی، شرایط محیطی و فاکتورهای هزینه استفاده نماید[۸].

رویه های گزارش دهی نیز باید درITCP ذکر گردد. هماهنگ کننده طرح باید مشخص کند که اگر اختلالی در یک سیستم فناوری اطلاعات اتفاق بیافتد چه کسی کار گزارش دهی را انجام دهد و با چه کسانی باید تماس گرفت. افرادی که باید به آنها گزارش داد معمولا صاحبان سیستم، کاربران و ذینفعان داخلی و خارجی می باشند. طراحی درخت تماس به ترتیب و نحوه تماس گیری ها کمک می کند.

فاز بازسازی، که فاز استمرار نیز نامیده می شود، بعد از فاز بازیابی اجرا می شود فاز بازیابی رویه هایی را اجرا می کند که سیستم های فناوری اطلاعات را به شرایط عادی برگرداند. اگر استفاده از سایت اصلی به علت شدت صدمات وارده امکانپذیر نباشد باید به سیستم یا سایت جدید نقل مکان نمود.

تست به ارزیابی امکان پذیر بودن رویه های طرح، در دسترس بودن تیم بازیابی برای اجرای طرح و تشخیص عیوب آن کمک می کند.برای کارا بودن طرح، تست باید حداقل سالی یکبار یا پس از انجام تغییرات در سیستم های فناوری اطلاعات و فرایند های پشتیبانی شغلی انجام پذیرد. هر بخش از ITCP باید به صورت جداگانه تست شود و پس از آن اثر بخشی تمام رویه های بازیابی به صورت یکپارچه مورد آزمایش قرار گیرد. زمانبندی آزمایش و تمرین باید در خط و مشی ذکر گردد.

به روز رسانی طرح جهت موفقیت آن ضروری می باشد. با بررسی معمولا در هنگام تغییر سیستم ها یا فرایند ها انجام می پذیرد یا به صورت سالیانه. عیوبی که در آزمایش طرح پدیدار می گردد باید در نگهداری طرح مورد بازبینی قرار گیرد. بعضی از عناصر طرح مانند لیست تماسها دائما تغییر می کند.

نشریه ویژه شماره 800-34 موسسه NIST با نام Contingency Planning Guide for Information Technology (IT) Systems دستورالعمل ها، توصیه ها و ملاحظاتی برای ITCP های دولتی فراهم می کند. طرح به ابزارهای کوتاه مدت برای بازیابی سرویس های IT در طول شرایط اضطرار و تخریب اشاره دارد. ابزارهای کوتاه مدت ممکن است شامل نقل مکان عملیات و سیستم های IT به سایت جایگزین، بازیابی عملیات IT با استفاده از تجهیزات جایگزین یا راه اندازی عملیات IT با استفاده از روش های دستی باشد.

سیستم های IT به وسیله تعدادزیادی از عوامل مخرب آسیب پذیرند از طیف ملایم (مانند قطع برق و خطای هارد دیسک) تا طیف شدید (مانند تخریب تجهیزات و آتش سوزی) که ناشی از بلایای طبیعی یا حملات تروریستی است. بسیاری از این آسیب ها را می توان به حداقل رساند یا بااستفاده از راه حل های مدیریتی، فنی و عملیاتی که بخشی از مدیریت ریسک است، تقلیل داد اما تقلیل همه ریسک ها به طور کامل غیر ممکن است. در تعدادی از موارد، منابع بحرانی تحت تاثیر عواملی خارج از کنترل سازمان قراردارند مانند جریان برق و ارتباطات مخابراتی. بنابراین طراحی، اجرا و تست طرح برای کاهش ریسک دردسترس نبودن سیستم و سرویس ضروریست. برای اینکه یک طرح موفق باشد، باید از موارد ذیل اطمینان حاصل شود[۵]:

۱. درک فرایندهای ITCP و جایگاه آن در بین سایر فرایندهای سازمانی .
۲. جاری سازی و آزمایش مجدد سیاست ها و فرایندهای طرح و اعمال آن به عناصر چرخه طرح شامل طراحی مقدماتی، تحلیل صدمات شغلی، انتخاب سایت جایگزین و استراتژی های بازیابی .

۳. جاری سازی و آزمایش سیاست های طرح با نگهداری، آموزش و تمرین .

دراین سند توصیه هایی برای هفت پلاتفرم زیر که دراکثر سیستم های فناوری اطلاعات متداول می باشد، ذکر و متعاقبا استراتژی ها و تکنیک های معمول برای این سیستم ها جهت کمک به تدوین طرح (عمدتا در بخش کنترل های بازدارنده)گرداوری شده است.

- رایانه های شخصی و سیستم های همراه
- سرورها
- وب سایت ها
- شبکه های محلی(LAN)
- شبکه های گسترده(WAN)
- سیستم های توزیع شده
- سیستم های Mainframe

دراین سند هفت مرحله فرایند طرح که یک سازمان برای جاری سازی و نگهداری موفق سیستم های IT خود نیاز دارد، توضیح داده است:

۱- جاری سازی خط مشی: یک بیانیه قراردادی سازمانی که برای جاری سازی موثر طرح لازم است.
۲- اجرای BIA : به تشخیص و اولویت بندی سیستم ها و اجزای بحرانی IT کمک می کند.
۳- شناسایی کنترل های بازدارنده: ابزارهایی برای کاهش اثرات خرابی سیستم که دردسترس بودن آن را افزایش و هزینه های چرخه عمر طرح را کاهش می دهد.
۴- تهیه استراتژی بازیابی: برای اطمینان از بازیابی سریع و موثر سیستم پس از وقوع خرابی تهیه می گردد.
۵- جاری سازی ITCP: شامل راهنمای جزئیات و رویه هایی برای بازگرداندن سیستم آسیب دیده به وضعیت عادی است.
۶- تست، آموزش و تمرین. با تست ایرادات طرح نمایان می گردد و آموزش، پرسنل را برای فعال سازی طرح آماده می کند.
۷- نگهداری: سندی پویا و فعال است که به طور منظم با تغییرات سیستم، بازبینی و به روزرسانی گردد.