فرآیندهای طراحی، نظارت و اجرای سیستم های فن آوری اطلاعات و ارتباطات

Dr Nasser Modiri

فروردین 1400

فهرست

1 فرایندهای ITSM

ITSMمخفف IT Service Management- به همه فعالیت های درگیر با طراحی، ایجاد، ارائه، مدیریت و پشتیبانی چرخه حیات سرویس های فناوری اطلاعات اشاره می کند. هدف اصلی ITSM تراز کردن فناوری اطلاعات با نیازهای تجارت با تبدیل ITاز تیم آتش نشانی به ارائه دهندگان خدمات داخلی است. سرویس های فناوری اطلاعات (IT Services) ، هر چیز مرتبط با ITکه در محل کار باهاش سر و کار داریم، مثل لپ تاپ و یا نرم افزار هایی که روی لپ تاپ داریم، دستگاه پرینتری ، اینترنت و یا سیستم حضور و غیاب و... ، همه این ها سرویس های فناوری اطلاعات هستند که توسط واحد IT سازمان در اختیار کاربران قرار می گیرد.

با اینکه بسیاری از کارمندان (کاربران شبکه) و یا حتی مدیران سطح بالای سازمان، ITSMرو فقط به صورت خدمات پشتیبانی واحد IT میبینند، در واقعیت مفهموم ITSM بسیار فراتر از این حرف ها است. واحد IT سازمان مسئول مدیریت همه سرویس های فناوری اطلاعات از ابتدا تا انتها است.

در این بخش مروری خـواهیم داشت بر مفاهیم **مدیریت خدمات فناوری اطلاعات(ITSM)** و فـرایند های مـرتبط با آن. در این نـوشته سعی می کنیم به خـواننده کمک کنیم تا اصول مدیریت خدمات IT را درک کنند و همچنین بهترین راه ها برای استراتژی فرایندهای اصول ITSM ، تجزیه و تحلیل معیارها و اجرای بهترین شیوه های آن را ارائه کنیم . علاوه بر این ، به دیگر موضوعات مهم و جالب از جمله آخرین روند و فن آوری در اصول ITSM نیز می پردازیم . این راهنمای ساده و آسان برای همه از مبتدی تا کارشناسان فناوری اطلاعات مناسب است.

مزایای ITSM می توان به دو بخش تقسیم شد:

➢ برخی از مزایای فناوری اطلاعاتITSM :

- این امر در تعیین انتظارات و استانداردهای خدمات کمک می کند.
- به اندازه گیری عملکرد کمک می کند.
- این امر به انجام تجزیه و تحلیل علت ریشه ای از مشکلات کمک می کند.
- افزایش بهره وری
- کمک می کند نقش ها و مسئولیت ها را تعریف کرد
- کاهش شکاف بین تشخیص حوادث و حل انها
- امکان شناسایی و زفع مشکلات تکراری

➢ برخی از مزایای تجاریITSM :

- فناوری اطلاعات می تواند به سرعت نسبت به تغییر و نو آوری در بازار واکنش نشان دهد
- کاهش هزینه ها
- اطمینان می دهد که خدمات همیشه در دسترس کارمندان است

1- تفاوت ITSM و ITIL

خیلی از افراد در تعریف درست تفاوت ITSM و ITIL دچار اشتباه می شوند. در یک تعریف ساده میشود گفت که ITIL یک چارچوب و مجموعه ای از بهروش ها برای اجرای ITSM هست. به عبارت دیگر وقتی در مورد ITSM صحبت می کنیم منظور دقیقا پیاده سازی و مدیریت سرویس های فناوری اطلاعات است، کاری که در عمل توسط تیم IT سازمان انجام میشود. در مقابل ITILمجموعه ای از پیشنهادات و روش های توصیه شده برای همان کارها است. در واقع ITIL به شما توصیه میکند که با چه روش ها و فرآیند هایی امور ITSM را انجام دهید.بنابراین، یک سازمان ممکنه از ITSM استفاده کنه ولی نه بر اساس چارچوب ITIL

1.1 چارچوب‌های پرکاربردITSM

- چارچوبCOBIT : چارچوبی برای توسعه، پیاده‌سازی، نظارت و بهبود قوانین IT و روش‌های مدیریتی است. چارچوب COBITتوسط انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی (ISACA)ارائه شده است.
- **چارچوبMicrosoft Operation Framework** : یک مجموعه شامل 23 سند است که متخصصان IT را طی فرآیندهای تولید، پیاده‌سازی و مدیریت صحیح و مقرون به‌صرفه خدمات IT راهنمایی می‌کند.
- چارچوب Six Sigma (شش سیگما): یک چارچوب مدیریتی است که توسط شرکت Motorola در ۱۵ ژانویه ۱۹۸۷ معرفی گردید. شش سیگما یک طرح بهبود و فرآیند منسجم و نظام مند برای تمرکز بر میزان پیشرفت و ارائه سرویس‌های مناسب و کاهش نقص‌های موجود در محصول و خدمات است.

- استاندارد ISO 20000 : یک استاندارد جهانی است که به توصیف نیازهای سیستم ITSM می‌پردازد. اگرچه این استاندارد توسط موسسه استاندارد انگلستان جهت شبیه‌سازی روش‌های تعیین شده در چارچوب ITIL ارائه شده است، با این حال از سایر چارچوب‌های ITSM همچون Microsoft Operation Framework نیز پشتیبانی می‌کند.
- چارچوب TOGAF : یک چارچوب معماری سازمانی است که توسط موسسه Open Group ارائه گردیده است. این چارچوب یک رویکرد ساختاریافته برای سازمان‌هایی است که قصد پیاده‌سازی و نظارت بر تکنولوژی IT را دارند.
- چارچوب ITIL (کتابخانه زیرساخت فناوری اطلاعات): چارچوب پرکابردی است که به منظور هم راستا کردن IT با نیازهای کسب و کار بهروش‌هایی ارائه می‌کند. ITIL شامل پنج بخش است. این بخش‌ها عبارتند از :استراتژی، طراحی، انتقال، عملیات اجرایی و بهبود مستمر خدمات. توسعه مستمر چارچوب ITIL به شرکت انگلیسی Axelos(یک شرکت سرمایه‌گذاری که توسط دولت انگلستان تاسیس شده) واگذار گردیده است

چارچوب COBIT : چارچوبی برای توسعه، پیاده‌سازی، نظارت و بهبود قوانین IT و روش‌های مدیریتی است. چارچوب COBITتوسط انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی (ISACA)ارائه شده است.

1.1.1 چارچوب COBIT

چارچوب COBIT بعنوان همخوانی یکی از پرکاربردترین چارچوب ها برای تعریف مولفه های پروژه های فن آوری اطلاعات و ارتباطات میباشد. چارچوب COBIT یک مدل فرایند مرجع و یک زبان مشترک را برای همه اشخاص در یک سازمان فراهم می-کند. یک مدل فرایند باعث تقویت مالکیت فرایند شده و منجر به تعریف مسئولیت ها و جوابگویی می‌شود. برای کنترل فناوری اطلاعات به نحوی موثر مهم است که فعالیت‌ها و ریسک‌های موجود در فناوری اطلاعات را که نیازمند مدیریت هستند را درک کنیم.

COBIT از میان این 4 حوزه، 34 فرایند فناوری اطلاعات را که عموما استفاده می‌شوند، شناسایی کرده است. در ادامه هرکدام از این نواحی و فرایندهای مربوط به آنها شرح داده می شود.

طرح ریزی و سازمان دهی

فاز اول: حوزه برنامه‌ریزی و سازماندهی (PO: Plan and Organise)

فرایندهای اصلی این حوزه که توسط COBIT شناسایی شده اند عبارتند از:

- PO1 : تعریف یک طرح استراتژیکی برای فناوری اطلاعات
- PO2 : تعریف معماری اطلاعات
- PO3 : تعیین سمت و سوی فنی و تخصصی
- PO4 : تعریف فرایندها، سازمان فناوری اطلاعات و روابط بین آنها
- PO5 : مدیریت بر سرمایه گذاری‌ها در فناوری اطلاعات
- PO6 : بیان مقاصد و سمت و سوی مدیریت
- PO7 : مدیریت منابع انسانی فناوری اطلاعات
- PO8 : مدیریت کیفیت
- PO9 : ارزیابی و مدیریت ریسک‌های فناوری اطلاعات
- PO10 : مدیریت پروژه‌ها
- دستیابی و پیاده سازی

فازدوم: حوزه اکتساب و پیاده‌سازی (AI: Acquire and Implement)

فرآیندهای اصلی این حوزه که توسط COBIT شناسایی شده‌اند عبارتند از:

- AI1: شناسایی راه‌حل‌های اتوماتیک
- AI2 : تعیین و نگهداری نرم‌افزار کاربردی
- AI3 : تعیین و نگهداری زیر ساخت فنی
- AI4 : فعال‌سازی عملیات و کاربرد
- AI5 : تهیه منابع فناوری اطلاعات
- AI6 : مدیریت تغییرات
- AI7 : معتبر ساختن و مستقر کردن راهکارها و تغییرات
- تحویل و پشتیبانی

فاز سوم: حوزه ارایه و پشتیبانی (DS: Deliver and Support)

فرایندهای اصلی این حوزه که توسط COBIT شناسایی شده اند عبارتند از:

- DS1: تعریف و مدیریت سطوح سرویس دهی
- DS2 : مدیریت سرویس های شخص ثالث
- DS3 : مدیریت کارایی و ظرفیت
- DS4 : تضمین استمرار خدمات
- DS5 : تضمین امنیت سیستم ها
- DS6 : تعیین و تخصیص هزینه ها
- DS7 : آموزش و تعلیم کاربران
- DS8 : مدیریت Service Desk و Incidents
- DS9 : مدیریت پیکربندی
- DS10 : مدیریت مشکلات
- DS11 : مدیریت داد ه ها
- DS12 : مدیریت محیط فیزیکی
- DS13 : مدیریت عملیات
- نظارت و ارزیابی

فاز چهارم: حوزه پایش و ارزیابی (ME: Monitor and Evaluate)

فرایندهای اصلی این حوزه که توسط COBIT شناسایی شده اند عبارتند از:

- ME1: نظارت و ارزیابی کارایی فناوری اطلاعات
- ME2 : نظارت و ارزیابی کنترل داخلی
- ME3 : انطباق با نیازمندی های خارجی
- ME4 : ایجاد حاکمیت فناوری اطلاعات

1.1.2 فرآیندهای اصلی ITSM

- **فرآیند مدیریت رخداد ها (Incident Management)**: یک سازمان را قادر می سازد که پاسخ اولیه در مورد یک رخداد یا درخواست خدمات توسط مشتریان را ضبط کند.

- **فرآیند مدیریت مشکلات (ITIL Problem Management)**: سازمان را قادر می سازد تجزیه و تحلیل علت اصلی یک یا چند حادثه مشابه را انجام دهد.
- **فرآیند مدیریت دارایی ها (Asset Management)**: دید کاملی از کلیه داراییهای فناوری اطلاعات سازمان را نشان می دهد.
- **فرآیند مدیریت تغییرات (Change Management)**: برای انجام تغییرات اساسی در زیرساخت IT ، یک مدل تغییر ارائه می دهد.
- **فرآیند مدیریت پیکربندی (CMDB)**: این فرآیند وظیفه دارد تا اطمینان حاصل کند که دارایی های مورد نیاز برای ارائه سرویس‌ها به دقت کنترل می‌شوند و اطلاعات دقیق و قابل اطمینان در خصوص آن دارایی ها نیز در مواقع نیاز، در دسترس هستند. این اطلاعات شامل جزئیات مربوط به نحوه پیکربندی دارایی و ارتباطات بین دارایی ها است. چنین کاری بسیار ضروری و مهم است و سراسر چرخه حیات سرویس را پوشش می‌دهد.
  - مدیریت دسترسی: به یک سازمان کمک می کند تا قابلیت های سرویس IT خود را بهینه کند.
  - سطح سرویس: در ارائه سطح معینی از تعهد هنگام ارائه خدمات فناوری اطلاعات کمک می کند.
  - مدیریت پروژه: به انجام یک افزودنی جدید در زیرساخت IT به صورت منظم کمک می کند.
  - مدیریت دانش: به سازمان کمک می کند تا یک مخزن راه حل برای موضوعات شناخته شده ایجاد کند.

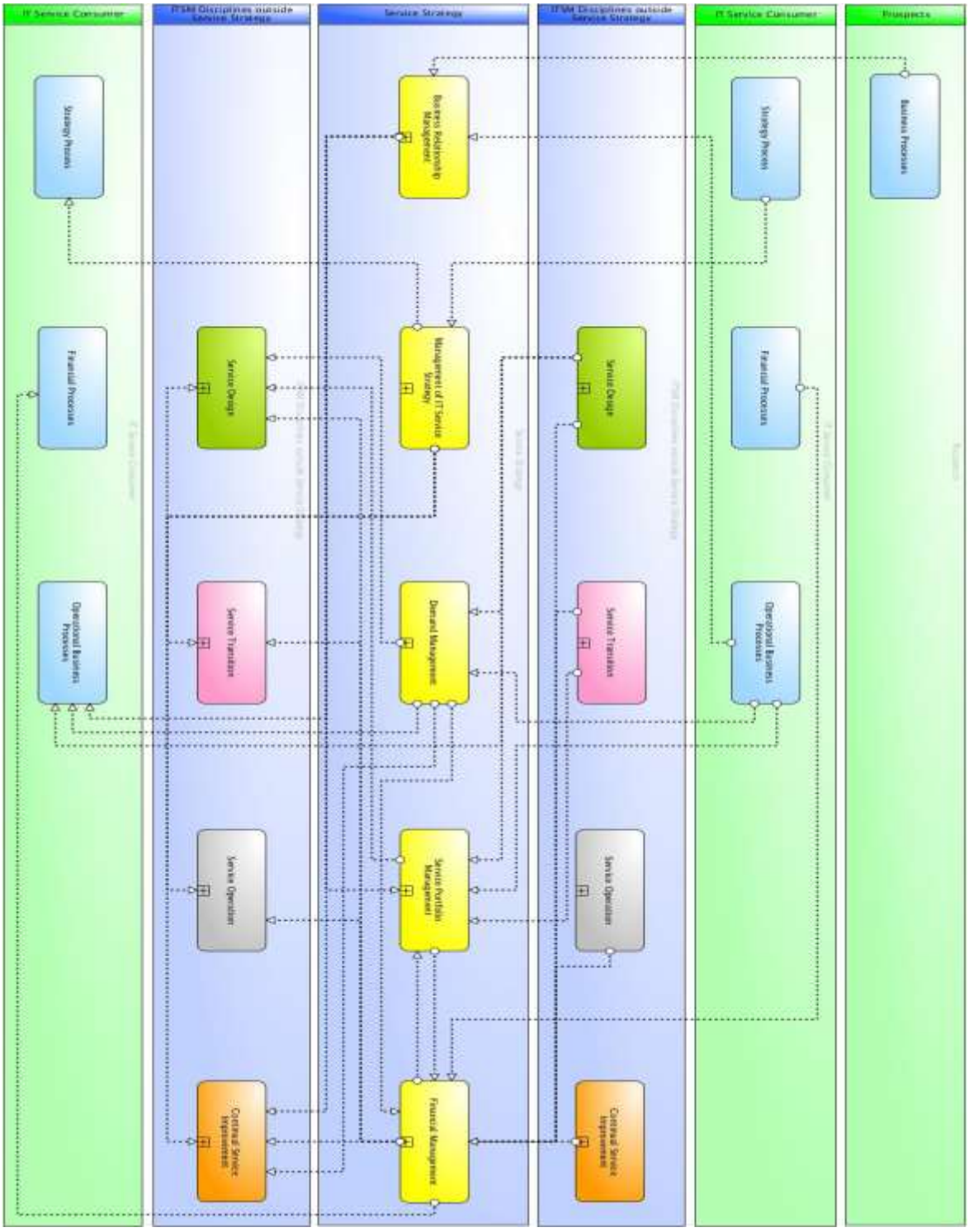
نکته مهم: فرایند های ذکر شده بالا حداقل فرایندهای مطرح شده در خصوص پیاده سازی ITSM می باشند یعنی هر چارچوب یا فریمورکی که برای ITSM راهکار ارائه می دهد باید حداقل موارد مطرح شده در موضوعات بالا را پوشش دهد. لذا با توجه به اینکه ITIL یک استاندارد کامل می باشد و تقریبا در تمام دنیا به عنوان یک استاندارد پذیرفته شده است و علاوه بر پوشش حداقل فرایندهای ITSM شامل بهروش های اضافی دیگر نیز می باشد.

چالشهای رایج در عموم سازمانها برای پیاده سازی ITSM

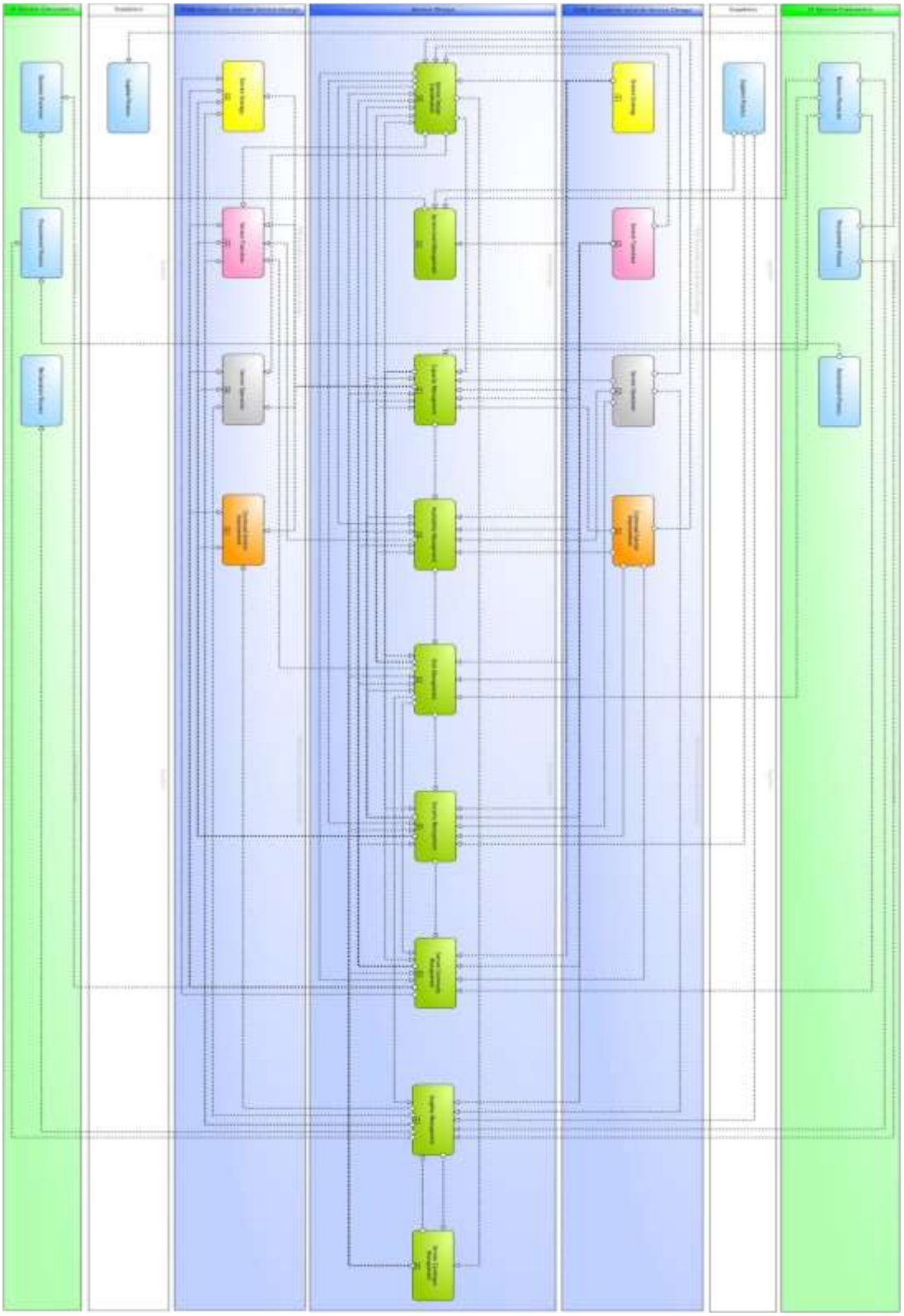
- عدم شفافیت در خدمات قابل ارائه
- عدم همسویی خدمات فناوری اطلاعات با نیازهای کسب و کار
- عدم نظارت و کنترل مناسب برروی تغییرات و در نتیجه ایجاد تبعات جانبی پس از اعمال تغییرات
- نارضایتی عمومی مشتریان و ذینفعان از خدمات پشتیبانی
- بهره‌وری پایین تیمهای پشتیبانی و فنی به دلیل انجام دوباره‌کاریهای متعدد، عدم ثبت دانش و بسیاری موارد دیگر
- عدم شفافیت در توقعات طرفین، ارائه کننده و استفاده کننده خدمات
- عدم مدیریت بهینه منابع سازمانی (تجهیزات، نیروی انسانی، زمان و ...)
- عدم امکان برنامه ریزی اثربخش به دلیل نبود شواهد و مستندات قابل استناد از تجربیات مشابه قبلی
- بروز حوادث تکراری و ایجاد وقفه های مکرر در ارائه خدمات

با توجه به پیشرفت ها و تحولات فناوری اطلاعات(IT)، تاثیرات شگرفی بر کسب و کار گذاشته است. و در بسیاری از سازمان ها، فناوری اطلاعات جزء جدایی ناپذیر کسب و کار به شمار می رود و از یک ابزار پشتیبانی به توانمند ساز خطوط کسب و کار تبدیل شده است. در چنین شرایطی، راهبری و مدیریت کار آمد حوزه فناوری اطلاعات نیازمند به کارگیری استانداردها و چارچوب تجربه شده بین المللی نظیر ITIL می باشد. ماهیت چارچوب ITIL و طراحی آن بر مبنای چرخه حیات سرویس و همچنین فرایند محور بودن آن سبب شده تا پیاده سازی چاچوب، تاثیرات متعددی را بر ساختار و سازمان فناوری اطلاعات، از ابعاد مختلف داشته باشد. موفقیت پیاده سازی چارچوب ITIL در گروه تغییر پارادایم ذهنی و رفتاری مدیران و کارکنان فناوری اطلاعات و سازمان دهی مجدد ساختار سازمانی در چرخه حیات پیاده سازی آن است. هدف این نوشته معرفی چارچوب ITIL و مزایای پیاده سازی چارچوب در سازمان های فناوری اطلاعات و ارتباطات بود.

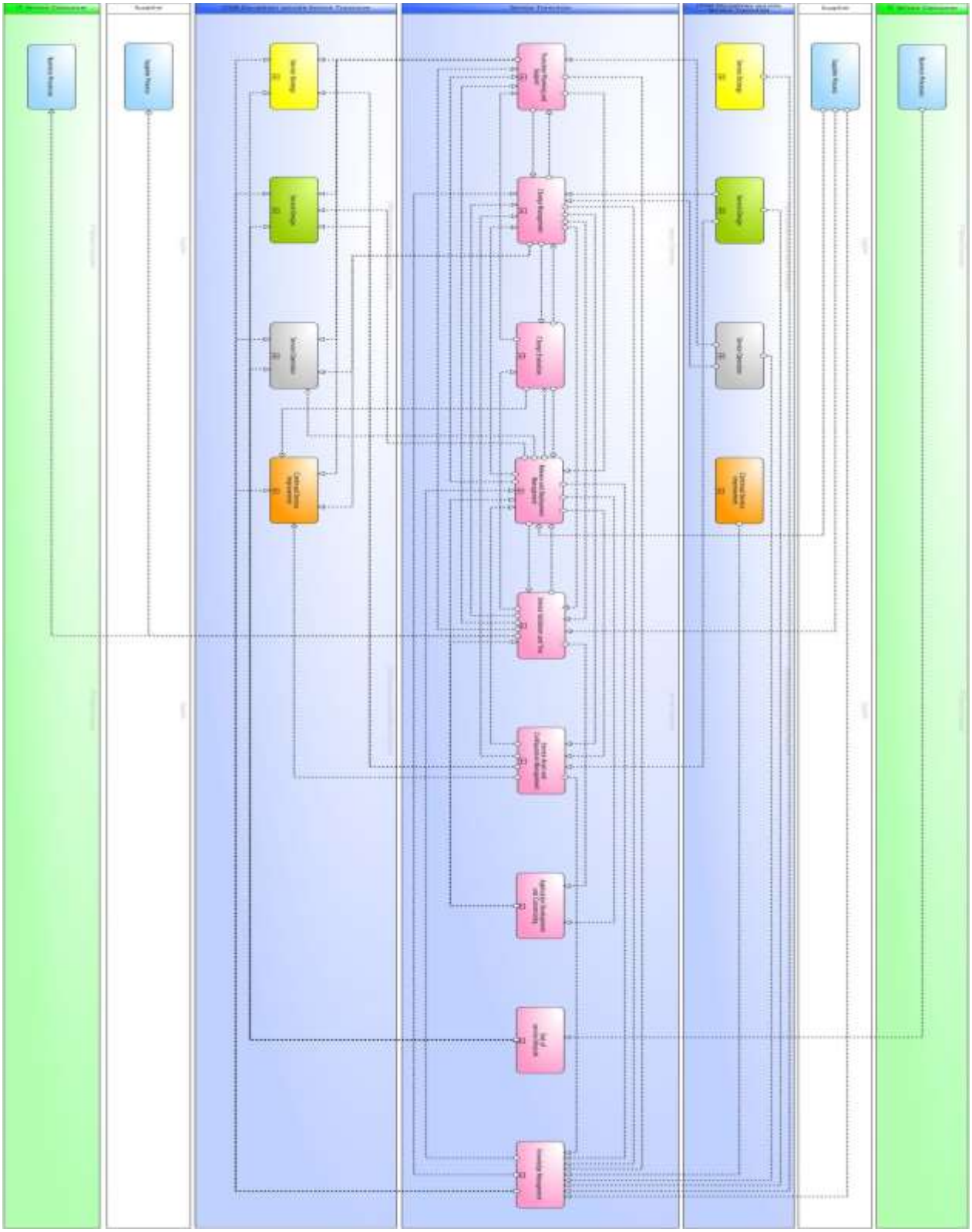
Service Strategy



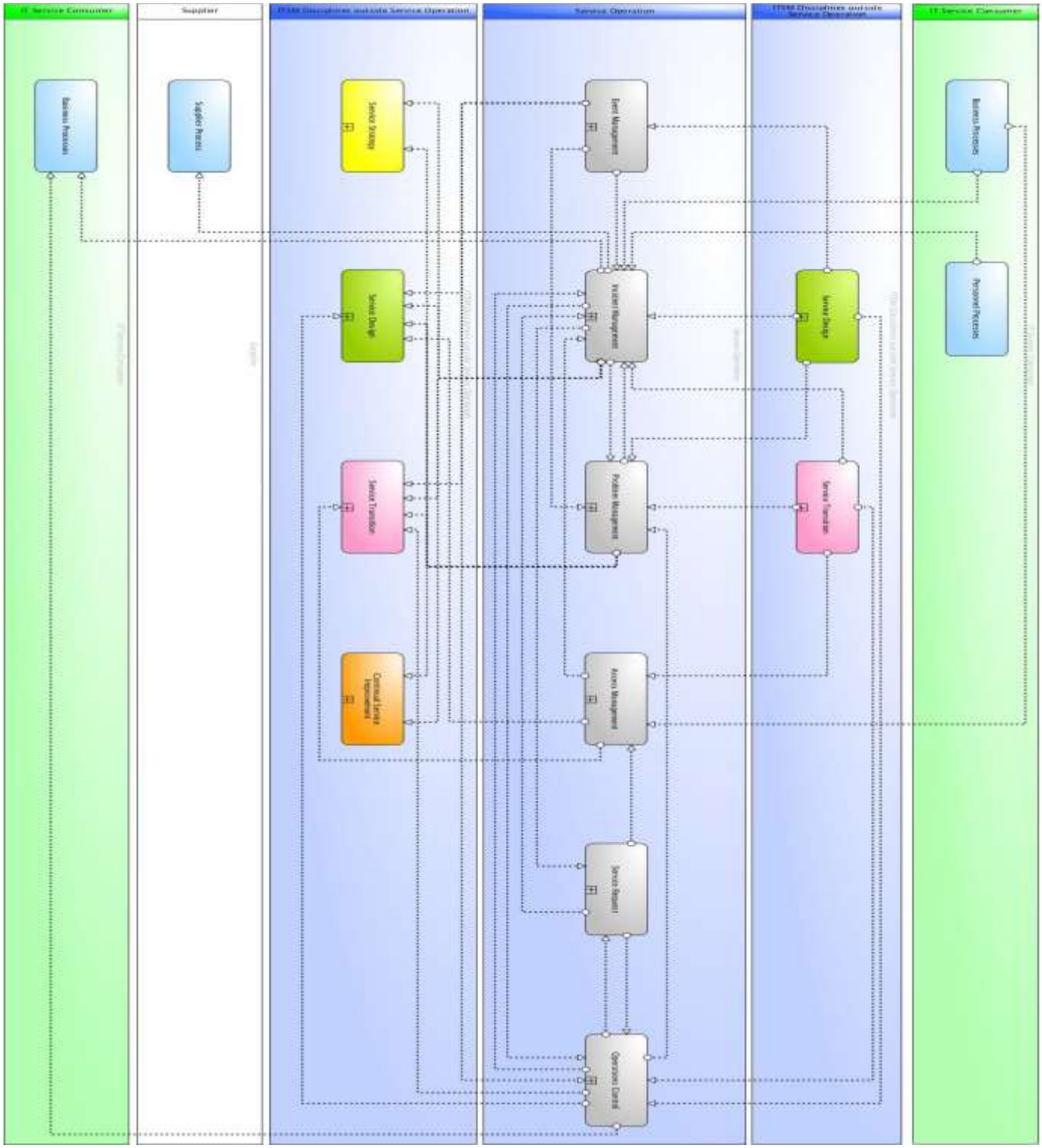
Service Design



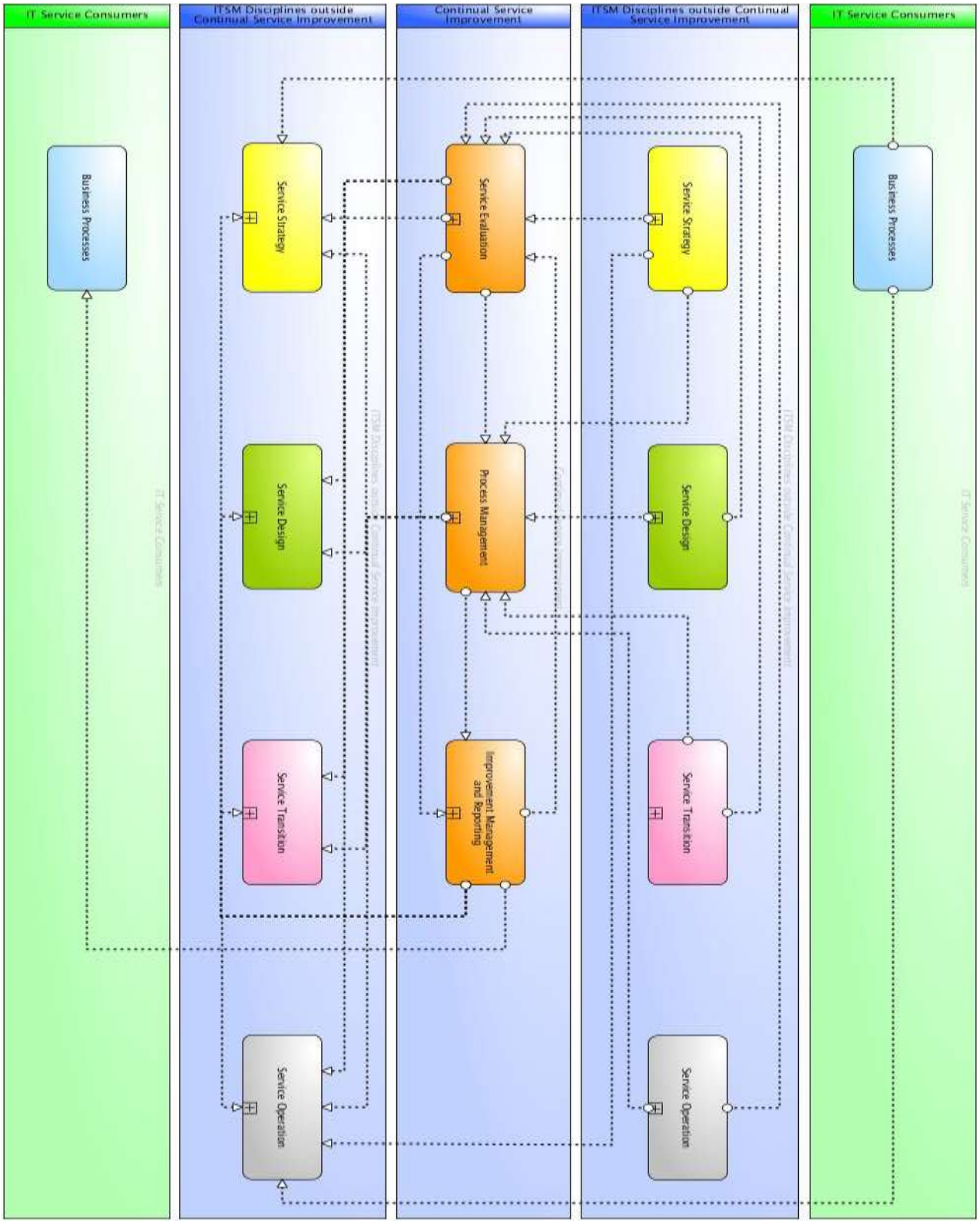
Service Transition



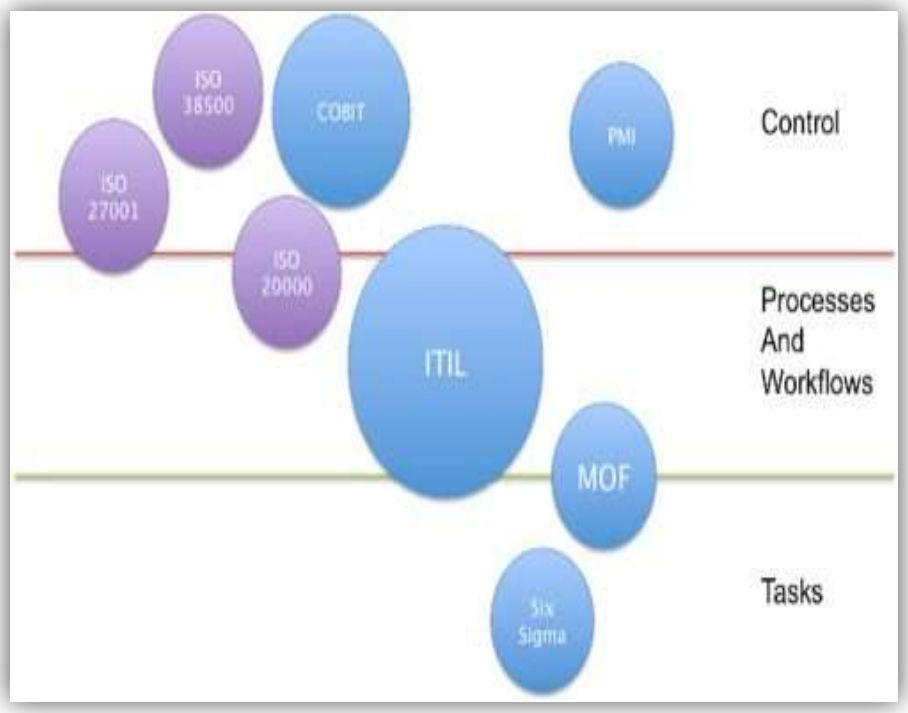
Service Operation



Service Continual Service Improvement



2 چرخه عمر(ITIL (Lifecycle



هسته ITIL نسخه 3 داری پنج نقطه مرکزی است که باهم چرخه عمر سرویس ITIL را تشکیل می دهند.

- Service Strategy - استراتژی سرویس
- Service Design - طراحی سرویس
- Service Transition - انتقال سرویس
- Service Operation - عملیات سرویس
- Continual Service Improvement -بهبود مداوم سرویس

هر مرحله در این چرخه حیات سرویس، کلیه مراحل دیگر را پشتیبانی میکند ITIL .کلیه قابلیت های مورد نیاز یک سازمان را مشخص نمیکند، اما برای هر سازمان فناوری اطلاعاتی که بخواهد در خصوص نقشه راه خود تصمیم گیری کند، راهنمایی های لازم و کاربردی در رابطه با تدوین استراتژی و نیز سرویس ها ارائه میدهد. بعلاوه ITIL مکمل به روش های (Best Practices) صنایع دیگر نیز میباشد. برای مثال، سازمانی که در خصوص مدیریت پروژه های خود به یک راهنما نیاز دارد، میتواند به روش های مدیریت پروژه را با اصول و مبانی چارچوب ITILتکمیل کند.

2.1 مزایای استفاده از ITIL

- ✓ چارچوب مبتنی بر بهترین تجارب و کارکردها
- ✓ دیدگاه فرایند گرا در مقابل دیدگاه وظیفه گرا
- ✓ اجتناب از بروکراسی در فرآیندها
- ✓ امکان پیاده‌سازی فرآیندها به‌صورت تدریجی
- ✓ تمرکز بر رضایت مشتریان خدمات
- ✓ افزایش پایایی و توان عملیاتی خدمات
- ✓ بهینه‌سازی استفاده از منابع، مالی، نیروی انسانی، دانش فنی و ...
- ✓ بهبود کیفیت در برنامه‌ریزی‌ها، فرهنگ استفاده از خدمات و برقراری نظم در امور
- ✓ مستقل از سکوهای عملیاتی
- ✓ کاهش هزینه‌ها و ریسک روبه‌رو شدن با نیازهایی که تا به حال شناسایی نشده‌اند
- ✓ وجود استانداردهای معتبر برای ارائه‌دهندگان خدمات IT
- ✓ توانایی تولید بیشتر و استفاده بهتر از مهارت‌ها و تجارب

2.2 فرایندهای ITIL

فرایندها مجموعه ساختارهای فعالیتی هستند که برای دستیابی به یک هدف خاص طراحی شده اند. که عبارتند از:

1) Service Strategy – استراتژی سرویس
2) Service Design –طراحی سرویس
3) Service Transition – انتقال سرویس
4) Service Operation – عملیات سرویس
5) Continual Service Improvement – بهبود مدام سرویس

فرایندها چهار ویژگی اصلی دارند:

1) آنها ورودی ها را به خروجی تبدیل می کنند
2) آنها نتایج را به مشتری یا ذینفع خاص تحویل می دهند
3) آنها قابل اندازه گیری هستند
4) آنها توسط حوادث خاص برانگیخته می شوند

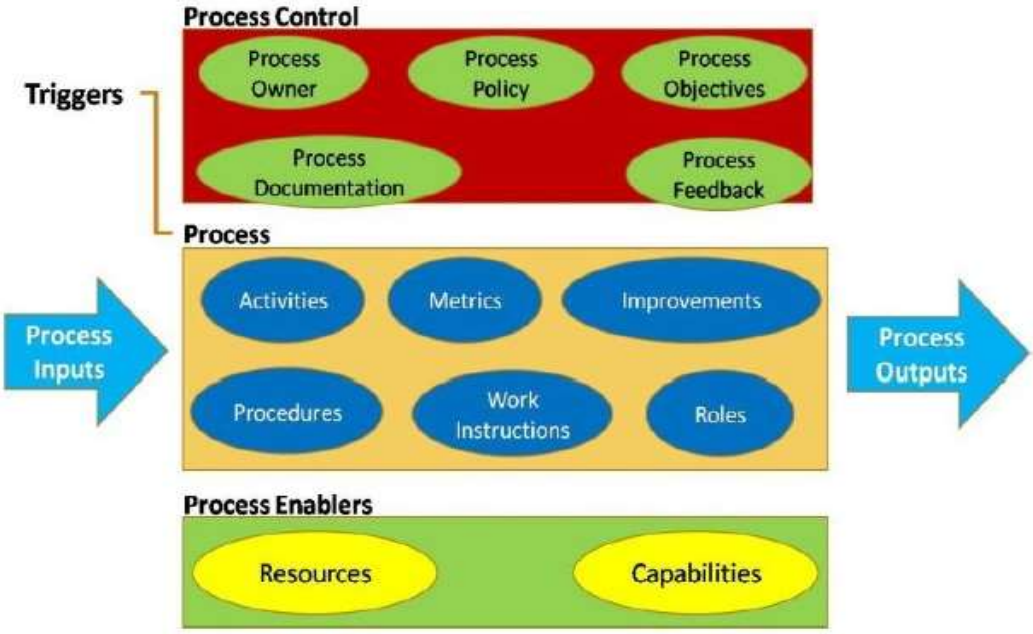
ITIL به تعدادی از فرآیندهای خاص مرتبط با هر مرحله از چرخه عمر می پردازد ، همچنین فرآیندهای مربوط به ساختار کلی آنها را که در مدل سه لایه زیر نشان داده شده است ، مورد بحث قرار می دهد.

- Process Control: مانند سیاستهای فرآیند ، مالکیت ، مستندات ، برنامه های بررسی و غیره.
- The Process itself: شامل مراحل فرآیند ، مراحل ، دستورالعمل کار ، نقش ها ، محرک ها ، معیارها ، ورودی ها و خروجی ها می باشد.
- Process Enablers: فعال کننده های پردازش مانند منابع و قابلیت های مورد نیاز برای پشتیبانی از فرایند.

2.2.1 استراتژی سرویس(Service Strategy)

این مرحله اساس ITSM را تشکیل می دهد. این شامل تعریف خدماتی است که سازمان ارائه می دهد و یا برای پیشبرد اهداف به کار می گیرد. استراتژی سرویس(خدمات) در مرکز (هسته) چرخه حیات ITIL v3قرار گرفته اما نمی تواند به تنهایی و بدون سایر بخش های ساختار IT ایجاد شود. این بخش دربرگیرنده یک framework(زیربنا) برای ایجاد تجربیات موفق(best practices)در اثر توسعه بلند مدت استراتژی سرویس است. این بخش شامل موضوعات مختلفی مانند:

- **مدیریت سبد خدمات:** مدیریت سبد خدمات ابزاری است که می‌توان از طریق آن سرمایه گذاری در بخش منابع را بصورت پویا و شفاف مدیریت نمود. هدف SPMآن است که همگام با مدیریت ریسک و هزینه ها، ارزش ایجاد شده برای کسب و کار را نیز بیشینه کند
- **مدیریت مالی برای سرویس‌های فناوری اطلاعات:** تضمین می‌دهد که ما سرمایه‌های بخش ITرا ردیابی و شناسایی کرده و برای سرویس‌های ارائه شده صرف کنیم.
- **مدیریت تقاضا:** مدیریت تقاضای ITILبه کسب و کارها کمک می‌کند تا تقاضای مشتریان برای سرویس‌ها را درک و پیش بینی کنند
- **مدیریت روابط تجاری:** مدیریت روابط تجاری در ITILبسیار شبیه به مدیریت سبد خدمات و مدیریت استراتژی، کار می‌کند. این به خدمات فناوری اطلاعات در اطلاع رسانی و پیاده سازی استراتژی و انتخاب خدمات کمک می‌کند.
- **مدیریت استراتژی برای سرویس‌های فناوری اطلاعات:** مدیریت استراتژی برای سرویس‌های فناوری اطلاعات در تلاش است تا مدیریت سرویس ITرا به یک دارایی استراتژیک برای سازمان تبدیل کند. همگام سازی فناوری اطلاعات با کسب و



کار به تنهایی کافی نیست. فناوری اطلاعات باید با کسب و کار یکپارچه نیز بشود.

استراتژی سرویس هر سازمان بایستی بر اساس یک باور بنیادین پایه‌ریزی شود: مشتری محصولات را نمی‌خرد بلکه رضایت مندی از برطرف شدن نیازهای خاصش را می‌خرد .برای موفقیت در این جهت مشتریان بایستی ارزش‌هایی که انتظار دریافتشان را دارند در نتیجه عملکرد صحیح و بر مبنای طراحی و ارائه بهینه سرویسها برایشان ملموس باشد. همچنین پیدا کردن درک عمیقی از نیازهای مشتریان، اینکه این نیازها چه هستند و اینکه چه موقع و به چه دلیل به‌وجود می‌آیند و بدست دادن درک شفاف و روشنی از اینکه چه کسانی مشتری بالقوه سرویس هستند، از مقاصد استراتژی سرویس است.

هدف

استراتژی خدمت هر ارائه‌دهنده خدمتی می‌بایست بر اساس این اصل بنیادین باشد که مشتریانشان محصول خریداری نمی‌نمایند، آن‌ها رضایتمندی آن نیازهای مخصوص را خریداری می‌نمایند؛ بنابراین ارزش کافی خدمات ارائه‌شده (در قالب نتایج مورد انتظار مشتری) می‌بایست توسط مشتری درک شود تا موفقیت حاصل شود.

دستیابی به درک عمیق نیازهای مشتری، آن این نظر که چه چیزی نیاز دارد و چه زمانی و چرا بدان نیازمند است، نیازمند درک درست این موضوع است که مشتری بالقوه یا موجود ارائه‌دهنده خدمت کیست. این موضوع به‌نوبه خود نیازمند این است که ارائه‌دهنده سرویس اطلاعات وسیع‌تری از بازار بالقوه و جاری که در آن فعالیت می‌کند و یا قصد انجام فعالیت در آن را دارد، درک کند.

استراتژی خدمت نمی‌تواند مجزا از استراتژی و فرهنگ‌سازمانی که ارائه‌دهنده خدمت در آن قرار دارد شکل‌گرفته و یا دوام یابد. ارائه‌دهنده خدمت در یک سازمان ممکن است منحصراً برای ارائه خدمت به یک واحد خاص از کسب‌وکار، ارائه خدمت به چندین واحد کسب‌وکار و یا ممکن است به‌عنوان یک ارائه‌دهنده خدمت خارج سازمانی به چندین کسب‌وکار خارجی خدمت‌رسانی نماید. استراتژی پذیرفته‌شده می‌بایست ارزش کافی برای مشتریان و تمامی ذینفعان خدمت تأمین نماید. درواقع باید اهداف استراتژیک ارائه‌دهنده خدمت را پوشش دهند.

قطع‌نظر از زمینه‌ای که ارائه‌دهنده خدمت در آن فعالیت می‌کند، می‌بایست استراتژی خدمتش بر اساس شناخت روشنی از وجود رقابت باشد، آگاهی از هر جنبه‌ای که انتخاب می‌کند و یک دیدگاه کلی از اینکه چگونه یک ارائه‌دهنده خدمت، خود را متفاوت از رقبا جلوه دهد. تمامی ارائه‌دهندگان خدمت نیاز به استراتژی خدمت دارند.

ازاین‌روست که مبحث استراتژی خدمت در مرکز چرخه عمر ITIL V3 قرارگرفته است. استراتژی خدمت شروع به راهنمایی تمامی ارائه‌دهندگان خدمات فناوری اطلاعات و مشتریانشان می‌نماید تا به آن‌ها در انجام کار و رشد بلندمدت به‌وسیله ساخت یک استراتژی واضح کمک نماید. به‌عنوان‌مثال فهم و درک دقیق:

- خدماتی که باید ارائه دهند.
- کسی که خدمات می‌بایست به او ارائه شود.
- چگونه می‌بایست بازارهای داخلی و خارجی را برای خدماتشان توسعه دهند؟
- رقابت بالقوه و جاری در این بازارها و اهدافی که ارزش کار انجام‌شده توسط شما یا چگونگی انجام آن توسط شما را متمایز سازد.
- چگونه مشتریان با توجه به استفاده از انواع مختلف ارائه‌دهندگان خدمت تصمیمات خدمت سپاری را اتخاذ خواهند نمود؟
- چگونه دید و کنترل بر ایجاد ارزش از طریق مدیریت مالی ایجاد خواهد شد؟
- چگونه موارد کسب‌وکار قوی برای ایمن‌سازی سرمایه‌گذاری استراتژیک در دارایی‌های خدمت و امکانات مدیریت خدمت ایجاد خواهد شد؟

مفاهیم کلیدی

مبحث استراتژی خدمت چند مفهوم کلیدی ITIL را تعریف می‌کند.

چهار P استراتژی

- چشم‌انداز :(Perspective) تصور و راه مشخص.
- جایگاه :(Position) مبنا و اساسی که ارائه‌دهنده در آن رقابت خواهد کرد.
- برنامه :(Plan) ارائه‌دهنده چگونگی دست‌یابی به تصورات خود.
- الگو :(Pattern) راه بنیادین انجام کارها- الگوهای مشخص در تصمیم‌ها و اقدامات در طول زمان

رقابت و بازار

- هر ارائه‌دهنده خدمتی تحت نیروهای رقابتی قرار دارد.
- تمامی ارائه‌دهندگان خدمت و مشتریان در یک و یا بیش از یک بازار داخلی یا خارجی فعالیت می‌کنند. ارائه‌دهنده خدمت می‌بایست برای دستیابی به درک بهتر (نسبت به رقبایش) از پویایی بازار، مشتریانی که در آن بازار حضور دارند، ترکیب عوامل اصلی موفقیت مختص آن بازار، تلاش نماید.

ارزش خدمت

ارزش خدمت در قالب نتایج کسب‌وکار درک شده توسط مشتری تعریف‌شده و در قالب ترکیب دو مؤلفه زیر بیان می‌شود:

- تسهیل خدمت: آنچه مشتری در قالب پشتیبانی از نتایج و یا حذف محدودیت‌ها دریافت می‌نماید.
- وارانتی خدمت: چگونگی ارائه خدمت و انطباق آن برای استفاده، ازلحاظ قابلیت دسترسی، ظرفیت، استمرار و ایمنی.

ارزش خدمت همچنین شامل مجموعه مفاهیمی از خدمات مانند دارایی‌ها، شبکه‌های ارزش، ایجاد ارزش و حفظ ارزش است.

انواع ارائه‌کنندگان خدمت

- نوع ۱: منحصراً در یک سازمان قرار دادن به‌منظور ارائه خدمت به یک واحد کسب‌وکار خاص.
- نوع ۲: در همان سازمان به چندین واحد کسب‌وکار خدمت‌رسانی می‌نماید.
- نوع ۳: به‌عنوان یک ارائه‌دهنده خدمت خارجی عمل کرده و به چندین مشتری خارجی خدمت‌رسانی می‌کند.

مدیریت خدمت به‌عنوان یک دارایی استراتژیک

استفاده از ITIL برای انتقال قابلیت‌های مدیریت خدمت به دارایی‌های استراتژیک با استفاده از اصولی برای شایستگی‌های محوری عملکرد مشخص، مزایای پایدار و افزایش پتانسیل ارائه‌دهندگان خدمت از طریق:

- امکاناتش: توانایی ارائه‌دهنده (ازنظر مدیریت، سازمان، فرایندها، دانش و نفرات) برای هماهنگی، کنترل و گسترش منابع.
- منابعش: هدایت ورودی‌ها برای تولید خدمات، به‌عنوان‌مثال مالی، سرمایه، زیرساخت، برنامه‌های کاربردی، اطلاعات و نفرات.

عوامل اصلی موفقیت(CSFs)

تعریف، سنجش و بازنگری‌های دوره‌ای CSF ها برای تعیین دارایی‌های خدمت نیازمند پیاده‌سازی موفق استراتژی خدمت مطلوب است.

حسابداری خدمت‌گرا

استفاده از مدیریت مالی به‌منظور درک خدمات ازنظر مصرف و تأمین و دستیابی به ترجمانی بین سیستم‌های مالی و مدیریت خدمت.

مدل‌های تأمین خدمت

دسته‌بندی و تحلیل مدل‌های متنوعی که ممکن است توسط مشتریان انتخاب‌شده و یا توسط ارائه‌دهندگان خدمت به‌منظور مأخذ و ارائه خدمات استفاده می‌شود و مدیریت مالی اثرات مدل‌های درون‌مرزی، برون‌مرزی یا همسایگی:

- خدمت مدیریت‌شده: جایی که یک واحد کسب‌وکار نیازمند به یک خدمت کامل، ارائه آن خدمت را برای خودش پایه‌گذاری می‌کند.
- خدمت اشتراک گذارده شده: ارائه خدمات چندگانه به یک واحد کسب‌وکار یا بیشتر از طریق زیرساخت یا منابع مشترک.
- کاربردپذیری: خدمات بر اساس مقدار نیاز هر مشتری، توالی زمانی و ساعت موردنیاز مشتری ارائه می‌شود.

طراحی و توسعه سازمان

دستیابی به یک شکل و ساختار روبه‌پیشرفت برای سازمان ارائه‌دهنده خدمت که استراتژی خدمت را توانمند سازد. ملاحظاتی شامل:

- مراتب توسعه سازمانی: ارائه خدمات از طریق شبکه، هدایت، تفویض، هماهنگی یا همکاری بستگی به وضعیت تکاملی سازمان دارد.
- استراتژی سپارش: تصمیم‌گیری آگاهانه روی سپارش خدمت ازنظر خدمات داخلی، خدمات به‌اشتراک‌گذارده‌شده، برون‌سپاری کامل خدمات، کنسرسیوم اولیه یا برون‌سپاری گزینشی.
- تجزیه‌وتحلیل خدمت: استفاده از تکنولوژی به‌منظور کمک به درک کارایی یک خدمت از طریق تحلیل.
- واسط خدمت: مکانیسمی که کاربران و دیگر فرایندها از طریق آن با هر خدمت تعامل می‌کنند.
- مدیریت مخاطره: نقشه‌برداری و مدیریت مجموعه مخاطراتی که یک سبد خدمت را تحت تأثیر قرار می‌دهند.

فعالیت‌ها و فرایندهای کلیدی

علاوه بر ایجادکنندگان استراتژی، استراتژی خدمت فرایندهای کلیدی زیر را نیز شامل می‌شود.

مدیریت مالی

مدیریت مالی وظایف و فرایندهایی که مسئولیت مدیریت بودجه‌بندی، حسابداری و تأمین نیازمندی‌های ارائه‌دهنده خدمت فناوری اطلاعات را به عهده دارند را پوشش می‌دهد. مدیریت مالی کسب‌وکار و فناوری اطلاعات را – ازلحاظ مالی – با تعریفی از ارزش خدمات فناوری اطلاعات، ارزش دارایی‌های زمینه‌ساز تأمین خدمات و تعریف پیش‌بینی عملیاتی مجهز می‌کند.

مسئولیت‌ها و فعالیت‌های مدیریت مالی فناوری اطلاعات منحصراً در حوزه حسابداری و مالی فناوری اطلاعات قرار ندارد. بسیاری از قسمت‌های سازمان برای ایجاد و استفاده از اطلاعات مالی در حال تأمل هستند؟ گردآوری، به‌اشتراک‌گذاری و حفظ اطلاعات مالی که قسمت‌ها نیاز دارند، امکان انتشار اطلاعات به‌منظور تغذیه فعالیت‌ها و تصمیمات حیاتی.

مدیریت سبد خدمتSPM

SPMشامل مدیریت کنشی و آینده‌ساز (proactive management) سرمایه‌گذاری در کل چرخه عمر خدمت می‌شود، به‌طورکلی شامل خدمات، طراحی و انتقال برنامه‌ریزی‌شده، همچنین خدمات زنده‌ای (live services) که در کاتالوگ‌های خدمت (live services) متنوع درج شده و خدمات از رده خارج شده.(Retired services)

SPMیک فرآیند مداوم است که شامل موارد زیر است:

- تعریف: سیاهه خدمات، تضمین موارد کسب‌وکار و اعتبار داده‌های سبد.
- تحلیل: حداکثر کردن ارزش سبد، تنظیم و اولویت‌بندی و متعادل نمودن عرضه و تقاضا.
- تأیید: نهایی‌سازی سبد پیشنهادی، تصویب منابع و خدمات.
- رسمیت: مکتوب نمودن تصمیمات، تخصیص منابع و رسمی کردن خدمات.

مدیریت تقاضا

مدیریت تقاضا یکی از زمینه‌های بحرانی مدیریت خدمت است. تقاضایی که به‌صورت ضعیف مدیریت شده است، به علت عدم اطمینان در تقاضا، منبع مخاطره‌ای برای ارائه‌دهندگان خدمت است. ظرفیت مازاد بدون اینکه ارزشی (که پایه‌ای برای بازیابی هزینه است) ایجاد کرده باشد، باعث تولید هزینه می‌شود.

هدف از مدیریت تقاضا درک و فهم تقاضای خدمت مشتری و تدارک ظرفیت‌ها برای انجام آن است. در سطح استراتژیک می‌تواند شامل تحلیل فعالیت‌های انجام‌شده در حوزه الگوهای فعالیت کسب‌وکار و مشخصات کاربر باشد. در سطح تاکتیکی می‌تواند شامل ارائه قیمت‌های متغیر به‌منظور ترغیب مشتریان به استفاده آن خدمات فناوری اطلاعات در زمان‌های شلوغی کمتر باشد.

بسته سطح خدمت (SLP) سطح تسهیلات و وارانتی بسته خدمت را تعریف نموده و به‌منظور رفع نیازهای الگوی فعالیت کسب‌وکار طراحی شده است.

نقش‌های کلیدی و مسئولیت‌ها

مبحث استراتژی خدمت برخی نقش‌ها و مسئولیت‌های خاص در ارتباط با انجام استراتژی خدمت موفق را تعریف می‌نماید؛ شامل:

مدیر ارتباط کسب‌وکار(BRM)

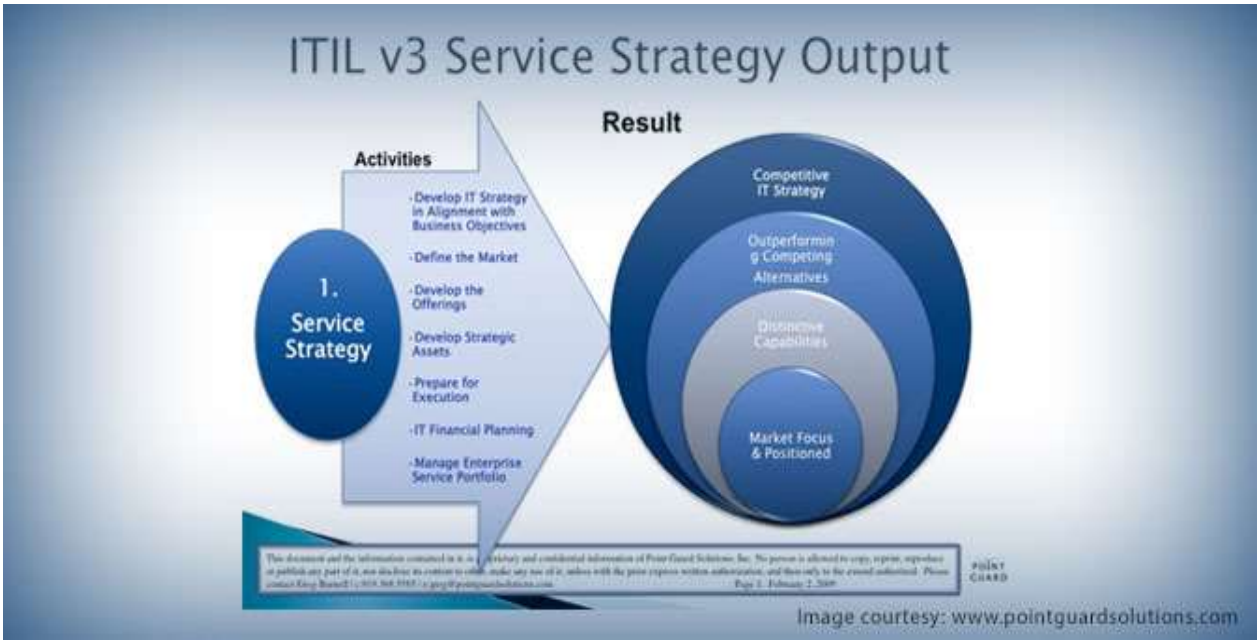
مدیران ارتباط کسب‌وکار، ارتباط قوی درزمینه‌ی کسب‌وکار به‌منظور درک کسب‌وکار و محصولات مشتریان با آن‌ها برقرار می‌کنند. مدیران ارتباط کسب‌وکار به نمایندگی از مشتری به‌منظور تبادل‌نظر برای دستیابی به ظرفیت تولید با مدیران تولید ارتباطی تنگاتنگ دارند.

مدیر تولید(PM)

مدیران تولید مسئولیت توسعه و مدیریت خدمات را در سراسر چرخه عمر به عهده می‌گیرند و مسئولیت ظرفیت تولیدی، برنامه‌ریزی خدمت و خدمات، راهکارها و بسته‌هایی که در کاتالوگ‌های خدمت ارائه‌شده‌اند را به عهده دارند.

مدیر ارشد سپارش(CSO)

مدیر ارشد سپارش قهرمان استراتژی سپارش در سازمان است، مسئول رهبری و هدایت اداره سپارش و توسعه استراتژی خدمت در ارتباط نزدیک با.CIO



2.2.2 استراتژی طراحی سرویس(Service Design)

Service Designشامل اصول طراحی سرویس‌ها و فرآیندها بوده و یک رویکرد طراحی جامع جهت کمک به سازمان‌ها برای ارائه بهتر سرویس‌ها فراهم می‌کند.

هدف اصلی این مرحله، برنامه ریزی و طراحی خدمات فناوری اطلاعاتی است که سازمان برای رفع نیازهای تجاری ارائه می دهد

پنج مشخصه کلیدی service designعبارتند از:

- طراحی راه حل سرویس
- مدیریت ابزارها و سیستم‌های اطلاعاتی
- تکنولوژی
- فرآیندها
- معیارها و مقیاس‌های ارزیابی

طراحی سرویس شامل زیر فرایند های ذیل می باشد.

Service Catalog Management – مدیریت کاتالوگ خدمات: تضمین می‌کند که یک سرویس کاتالوگ دقیق و بروز برای همه افرادی که امکان مشاهده آن را دارند، در دسترس است.

- **Service Level Management – مدیریت سطح خدمات:** فرآیند مدیریت سطح سرویس (SLM) بر جستجو و درک نیازمندی ها تمرکز دارد
- **Availability Management – مدیریت در دسترس بودن:** از مناسب بودن زیرساخت، ابزارها، نقش‌ها و غیره برای اهداف توافق شده، اطمینان حاصل می‌کند
- **Capacity Management – مدیریت ظرفیت**: در ITILتضمین می کند که ظرفیت کافی در همه زمان ها برای برآورده ساختن نیازهای توافق شده کسب و کار به شیوه ای مقرون به صرفه در دسترس است

- **Service Continuity Management – مدیریت استمرار خدمات:** بر پشتیبانی از استمرار کلی کسب و کار تمرکز دارد. ما ITSCMرا به عنوان فرآیندی درنظر می‌گیریم که وظیفه آن مدیریت ریسک هایی است که بطور جدی بر روی سرویس‌های ITتاثیر می‌گذارد.
- **IT Security Management – مدیریت امنیت فناوری اطلاعات:** همراستا کردن ITبا امنیت کسب و کار و اطمینان از مدیریت مؤثر امنیت اطلاعات در همه فعالیت‌های مدیریت سرویس و سرویس.
- **Supplier Management- مدیریت تامین کننده:** با اشخاص ثالث مانند تامین کنندگان، به منظور مذاکره در خصوص قراردادهای مربوط به محصولات یا سرویس‌ها همکاری می‌کندSupplier management ، پیروی از شرایط قرارداد و رسیدگی به هرگونه نقض در آن را کنترل و نظارت می‌کند Supplier management .تمدید قرارداد، مذاکره مجدد در خصوص آن و اتمام قراردادها را تعیین می‌کند.

طراحی سرویس، مرحله ای است که در سرتا سر چرخه حیات سرویس وجود دارد و نقش مهمی در فرآیند تغییرات تجاری بازی می کند. طراحی درخور و خلاقانه سرویس های IT شامل بر معماری، فرآیندها، خط مشی و مستندسازی برای فراهم نمودن نیازهای تجاری حال و آینده کسب و کار.

هدف

طراحی خدمت یک مرحله از کل چرخه عمر خدمت و یک عامل مهم در فرایند تغییر کسب‌وکار است. نقش طراحی خدمت در فرایند تغییر کسب‌وکار را می‌توان به شکل زیر تعریف کرد:

طراحی مناسب و نوآورانه خدمات فناوری اطلاعات، شامل معماری‌ها، فرایندها، سیاستها و مستندات، به‌منظور رفع نیازهای توافق شده جاری و آینده کسب‌وکار.

آرمان‌های اصلی و اهداف طراحی خدمت:

- طراحی خدمات به‌منظور رسیدن به نتایج توافق شده کسب‌وکار
- طراحی فرایندهایی برای پشتیبانی چرخه عمر خدمت
- شناسایی و مدیریت مخاطرات
- طراحی زیرساخت‌ها، محیط، برنامه‌های کاربردی و منابع داده اطلاعات و قابلیت فناوری اطلاعات به‌صورت ایمن و منعطف
- طراحی معیارها و روش‌های اندازه‌گیری
- تولید و نگهداری برنامه‌ها، فرایندها، سیاست‌ها، استانداردها، معماری‌ها، چارچوب‌ها و مدارک به‌منظور پشتیبانی کردن راهکارهای فناوری اطلاعات کیفی
- توسعه مهارت‌ها و قابلیت در فناوری اطلاعات
- کمک به بهبود کلی در کیفیت خدمت فناوری اطلاعات

مسئولیت‌های کلیدی

طراحی خدمت با مجموعه‌ای از نیازمندی‌های کسب‌وکار آغاز و با توسعه یک راهکار خدمت پایان می‌یابد که به‌منظور دستیابی به نتایج و نیازمندی‌های کسب‌وکار و ارائه بسته طراحی خدمت (SOP) برای تحویل به مرحله انتقال خدمت، طراحی شده است.

پنج زمینه منحصربه‌فرد طراحی خدمت:

- راهکارهای خدمت تغییریافته یا جدید
- ابزارها و سیستم‌های مدیریت خدمت بخصوص سبد خدمت
- معماری‌های تکنولوژی و سیستم‌های مدیریت
- فرایندها، نقش‌ها و قابلیت‌ها

در طراحی خدمت می‌بایست یک روش جامع به‌منظور تضمین ثبات و یکپارچگی در تمامی فعالیت‌ها و فرآیندهای فناوری اطلاعات، ارائه کسب‌وکار انتها به انتها مرتبط با عملکرد و کیفیت، به تأیید برسد. طراحی خدمت خوب به اثربخشی و کارایی در استفاده از چهار P طراحی بستگی دارد:

- افراد :(People) افراد، مهارت‌ها و صلاحیت‌ها در تدارک خدمات فناوری اطلاعات گنجانده می‌شود.

- محصولات :(Products) تکنولوژی و سیستم‌های مدیریتی در تحویل خدمات فناوری اطلاعات استفاده می‌شود.
- فرایندها :(Processes) فرایندها، نقش‌ها و فعالیت‌ها در تدارک خدمات فناوری اطلاعات گنجانده می‌شود.
- همکاران :(Partners) فروشندگان، سازندگان و تأمین‌کنندگان تدارک خدمت فناوری اطلاعات را همکاری و پشتیبانی می‌کنند.

بسته طراحی خدمت(SDP)

تمام جوانب یک خدمت فناوری اطلاعات و نیازمندی‌های آن طی هر مرحله از چرخه عمرش تعریف می‌شود SOP .برای هر خدمت جدید، دارای تغییر اصلی یا از رده خارج شده فناوری اطلاعات ایجاد می‌شود.

فعالیت‌ها و فرایندهای کلیدی

مدیریت کاتالوگ خدمتSCM

کاتالوگ خدمت منبع مرکزی اطلاعات در مورد خدمات فناوری اطلاعات تحویل‌شده به کسب‌وکار به‌وسیله سازمان ارائه دهنده تعبیه می‌کند. تضمین اینکه حوزه‌های کسب‌وکار می‌توانند یک تصویر دقیق و مداوم آن خدمات فناوری اطلاعات در دسترس، جزئیات و وضعیت آن‌ها را ببینند.

هدف از مدیریت کاتالوگ خدمت، ارائه یک منبع اطلاعات منفرد و مداوم در مورد تمامی خدمات توافق شده است و تضمین اینکه خدمت مذکور به‌طور وسیعی برای کسانی که دسترسی آن‌ها به آن تأیید شده است قابل‌دسترس است.

اطلاعات کلیدی فرایند SCM در کاتالوگ خدمت قرار دارد. ورودی اصلی این اطلاعات از سبد خدمت و کسب‌وکار از طریق فرایندهای مدیریت ارتباط کسب‌وکار یا مدیریت سطح خدمت حاصل می‌شود.

مدیریت سطح خدمتSLM

SLMاهداف خدمات فناوری اطلاعات مناسب را با کسب‌وکار تبادل‌نظر، توافق و مستند می‌کند و سپس گزارش‌هایی در خصوص مقایسه خدمات تحویل‌شده با سطح خدمت توافق شده تهیه و کنترلی می‌نماید.

هدف از فرایند SLM تضمین این موضوع است که تمام خدمات عملیاتی و کارایی آن‌ها با یک شیوه حرفه‌ای و پایدار در کل سازمان فناوری اطلاعات اندازه‌گیری شده و خدمات و گزارش‌های تولیدشده نیازهای مشتریان و کسب‌وکار پوشش داده است.

اطلاعات اصلی تهیه‌شده توسط فرایند SLM شامل توافقنامه سطح خدمت(SLA) ، توافقنامه سطح عملیاتی OLA دیگر توافقنامه‌های پشتیبانی، همچنین تولید برنامه بهبود خدمت (SIP) و برنامه کیفیت خدمت است.

مدیریت ظرفیت

مدیریت ظرفیت شامل مدیریت ظرفیت کسب‌وکار، خدمات و مؤلفه‌ها در طی چرخه عمر خدمت است. یک عامل کلیدی موفقیت در مدیریت ظرفیت، اطمینان از توجه به آن در مرحله طراحی است.

هدف مدیریت ظرفیت ارائه یک نقطه توجه و مدیریت برای تمامی مسائل مرتبط با عملکرد و ظرفیت، در ارتباط با منابع و خدمات و تطبیق دادن ظرفیت فناوری اطلاعات با تقاضاهای توافق شده کسب‌وکار است.

سیستم اطلاعاتی مدیریت ظرفیت (CMIS) اساس موفقیت فرایند مدیریت ظرفیت است. اطلاعات موجود در CMIS به‌وسیله زیر فرایندهای مدیریت ظرفیت برای تهیه و تدارک گزارش‌های فنی و مدیریتی از جمله برنامه ظرفیت ذخیره و تحلیل می‌شوند.

مدیریت دسترس‌پذیری

هدف از مدیریت دسترس‌پذیری ارائه یک نقطه توجه و مدیریت برای تمامی مسائل، مرتبط با دسترس‌پذیری، در ارتباط با خدمات، مؤلفه‌ها و منابع، تضمین این موضوع که اهداف دسترس‌پذیری در تمامی زمینه‌ها به‌دست‌آمده و اندازه‌گیری شده است و اینکه از اهداف با نیازمندی‌های توافق شده جاری و آینده کسب‌وکار از طریق روشی مقرون‌به‌صرفه تطبیق داده شده و یا فراتر رفته است.

مدیریت دسترس‌پذیری می‌بایست در دو سطح پیوسته اتفاق بیفتد و به بهینه‌سازی مستمر برسد و به‌طور کنشی دسترس‌پذیری خدمات فناوری اطلاعات و سازمان پشتیبانی آن را بهبود بخشد. دو جنبه کلیدی مطرح است:

- فعالیت‌های واکنشی: نظارت، اندازه‌گیری، تحلیل و مدیریت اتفاق‌ها، رویدادها و مشکلات ناشی از عدم دسترس پذیری خدمت.
- فعالیت‌های کنشی: برنامه‌ریزی، طراحی، پیشنهاد و بهبود کنشی (پیشبینانه) دسترس‌پذیری.

فعالیت‌های مدیریت دسترس‌پذیری می‌بایست قابلیت دسترسی، قابلیت اطمینان، نگهداشت‌پذیری و خدمت پذیری در هر دو سطح خدمت و اجزاء مدنظر قرار دهد به‌خصوص فعالیت‌هایی که وظایف حیاتی کسب‌وکار (VBFs) را پشتیبانی می‌کند.

فرایند مدیریت دسترس‌پذیری می‌بایست بر اساس یک سیستم اطلاعاتی باشد (AMIS) که شامل تمامی اندازه‌گیری‌ها و اطلاعات موردنیاز برای ارائه اطلاعات مناسب به کسب‌وکار در قالب سطوح خدمت است AMIS .همچنین در تولید برنامه دسترس‌پذیری نقش دارد.

مدیریت مستمر خدمات فناوری اطلاعات(ITSCM)

همان‌گونه که تکنولوژی جزء اصلی بسیاری از فرایندهای کسب‌وکار است، فناوری اطلاعات مستمر و با دسترس‌پذیری بالا برای حیات کسب‌وکار مهم است. این مهم با تعریف اقدامات کاهش مخاطره و گزینه‌های بازیابی قابل‌دستیابی است. نگهداشت مداوم قابلیت‌های بازیابی ضروری است به شرطی که کارا باقی بماند.

هدف از ITSCM نگهداشت قابلیت‌های بازیابی مستمر در خدمات فناوری اطلاعات به‌منظور تطبیق نیازها، احتیاجات و محدوده کسب‌وکار توافق شده است.

ITSCMیک سری از اقدامات در طول چرخه عمر است به‌منظور تضمین اینکه، برای یک‌بار برنامه‌های بازیابی و استمرار توسعه‌یافته باشند، برنامه‌های مذکور با برنامه‌های استمرار کسب‌وکار و اولویت‌های کسب‌وکار منطبق نگه داشته می‌شوند.

مدیریت امنیت اطلاعات(ISM)

ISMمی‌بایست در چارچوب کل ساختار حاکمیت شرکت مورد توجه قرار گیرد. حاکمیت شرکت مجموعه‌ای از مسئولیت‌ها و شیوه‌هاست که توسط مدیریت ارشد و هیئت‌مدیره با هدف ارائه هدایت استراتژیک، تضمین دستیابی به اهداف، اثبات مدیریت مناسب مخاطرات و تأیید استفاده اثربخش آن منابع یکپارچه به کار گرفته می‌شود.

هدف فرایند ISM تطبیق امنیت فناوری اطلاعات با امنیت کسب‌وکار است و تضمین این موضوع که امنیت اطلاعات در تمامی خدمت و فعالیت‌های مدیریت خدمت به‌صورت اثربخشی مدیریت شده است. به طوری که:

- اطلاعات در زمان موردنیاز در دسترس و قابل‌استفاده هستند (دسترس‌پذیری.(
- اطلاعات تنها برای کسی که اجازه دانستن آن را دارد قابل‌مشاهده و آشکار شده است (محرمانگی.(
- اطلاعات به‌صورت کامل و دقیق در برابر اصلاح غیرمجاز حفاظت شده است (یکپارچگی.(
- تراکنش‌های کسب‌وکار، همچنین تبادل اطلاعات می‌تواند تأیید اعتبار شود (صحت و عدم انکار(

ISMمی‌بایست یک سیاست کلی را همراه با مجموعه‌ای از کنترل‌های پشتیبانی در یک سیستم اطلاعات مدیریت امنیت (SMIS) یکپارچه که با سیاست‌ها و استراتژی‌های کسب‌وکار مطابقت داده شده است، حفظ و اجرا نماید.

مدیریت تأمین‌کننده

فرایند مدیریت تأمین‌کننده تضمین‌کننده این موضوع است که تأمین‌کنندگان و خدمات ارائه‌شده توسط آن‌ها به‌منظور پشتیبانی اهداف خدمت فناوری اطلاعات و انتظارات کسب‌وکار مدیریت می‌شوند.

هدف از فرایند مدیریت تأمین‌کننده کسب ارزش در قالب پول از تأمین‌کنندگان و تضمین اینکه تأمین‌کنندگان در راستای اهداف مندرج در قراردادها و توافقنامه‌ها با رعایت تمامی مفاد و شرایط اقدام کنند.

پایگاه داده قرارداد و تأمین‌کننده(SCD) یک منبع حیاتی اطلاعات در مورد تأمین‌کنندگان و قراردادها است و می‌بایست شامل تمامی اطلاعات لازم برای مدیریت تأمین‌کنندگان، قراردادها و خدمات مربوطه باشد.

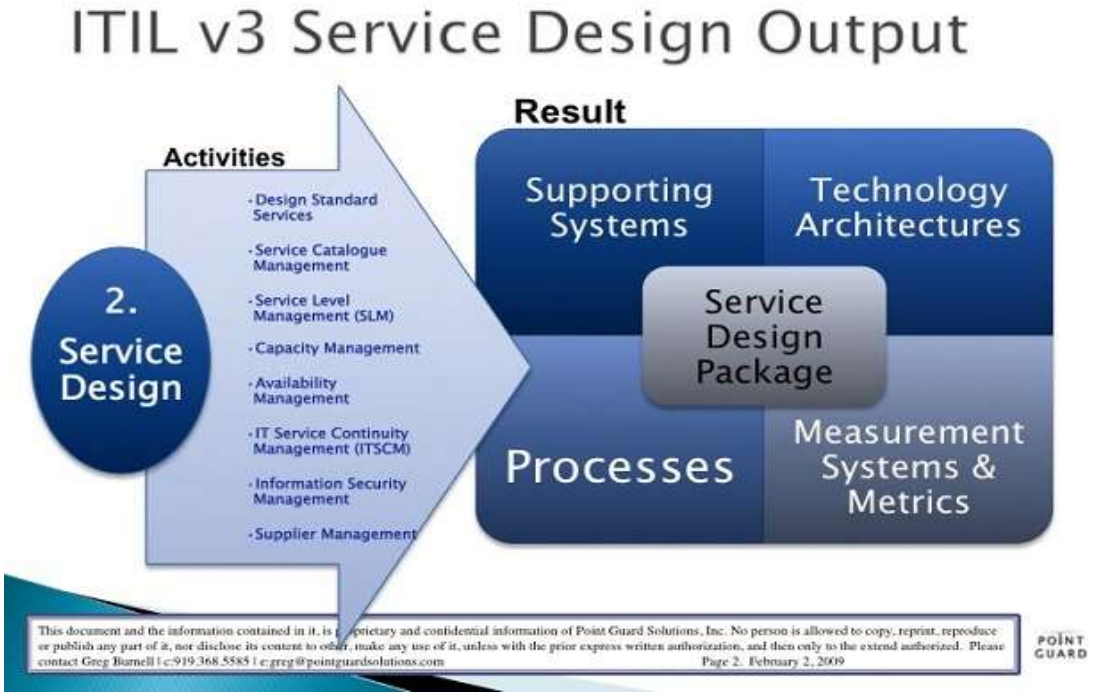
فعالیت‌های کلیدی مرحله طراحی خدمت

- جمع‌آوری، تحلیل و مهندسی نیازمندی‌های کسب‌وکار و تضمین اینکه به‌وضوح مستند شده‌اند.
- طراحی و توسعه راهکارها، تکنولوژی، فرایندها، اطلاعات و اندازه‌گیری‌های خدمت مناسب.
- تولید و بازنگری تمامی طرح‌های فرایندها و مدارک مربوط به طراحی خدمت.
- تعامل با دیگر نقش‌ها و فعالیت‌های برنامه‌ریزی و طراحی.
- تولید و حفظ مدارک طراحی و سیاست‌ها.
- مدیریت مخاطره تمامی فرایندهای طراحی و خدمات.
- تطبیق با تمامی شرکت و سیاست‌ها و استراتژی‌های فناوری اطلاعات.

مسئولیت‌ها و نقش‌های کلیدی

نقش‌های کلیدی فعالیت‌ها و فرایندهای طراحی خدمت به شرح زیر هستند:

- مدیر طراحی خدمت: مسئولیت هماهنگی و استفاده از طرح‌های راهکار کیفی برای خدمات و فرایندها.
- معمار / طراح فناوری اطلاعات: مسئول هماهنگی و طراحی تکنولوژی‌ها، معماری‌ها، استراتژی‌ها، طرح‌ها و برنامه‌های موردنیاز.
- مدیر کاتالوگ خدمت: مسئول تولید و نگهداری یک کاتالوگ خدمت دقیق.
- مدیر سطح خدمت: مسئول تضمین اینکه سطوح کیفی خدمت، موردتوافق قرارگرفته و به دست آمده است.



- مدیر دسترس‌پذیری: مسئول تضمین اینکه تمامی خدمات به اهداف قابل‌دسترس توافق شده آن‌ها دست یافته اند.
- مدیر استمرار خدمت فناوری اطلاعات: مسئول تضمین اینکه کلیه خدمات مطابق با نیازها، احتیاجات و محدوده‌های توافق شده کسب‌وکار قابل بازیابی هستند.
- مدیر ظرفیت: مسئول تضمین این موضوع که ظرفیت فناوری اطلاعات با تقاضاها توافق شده جاری و آینده کسب‌وکار مطابقت داشته باشد
- مدیر امنیت: مسئول تضمین اینکه امنیت فناوری اطلاعات با مخاطرات، ضربات و نیازمندی‌های سیاست امنیت توافق شده کسب‌وکار مطابقت داشته باشد.
- مدیر تأمین‌کننده: مسئول تضمین اینکه ارزش پولی کسب‌شده از تمامی تأمین‌کنندگان و قراردادها و آنچه قراردادها و توافقنامه‌ها را پایه‌ریزی کرده‌اند با نیازمندی‌های کسب‌وکار مطابقت داشته باشد.

2.2.3 استراتژی انتقال سرویس(Service Transition)

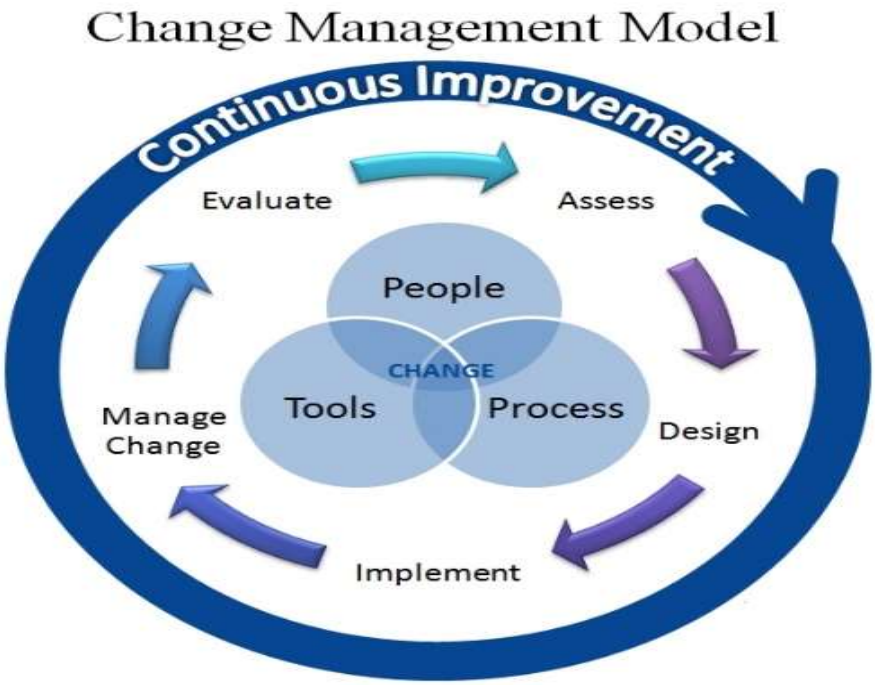
ITIL service transition به برنامه ریزی و مدیریت تغییر حالت یک سرویس در چرخه حیاتش کمک می‌کند .مدیریت ریسک برای خدمات جدید، تغییر یافته و یا قدیمی، از محیط محصول محافظت می‌کند. این به کسب و کارها کمک می‌کند تا برای خود و مشتریانشان ارزش ایجاد کنند.

هیچ تغییری بدون ریسک نخواهد بود. در حقیقت، تغییر می‌تواند ریسک بیشتری ایجاد کند. در هنگام انتقال سرویس، بر روی برنامه ریزی ارتباطات جهت آگاهی و هماهنگ سازی، تمرکز کنید. یکی از بزرگترین چالش‌ها در انتقال سرویس، تغییر رفتار مردم جهت انطباق آنها با سرویس جدید یا سرویس متفاوت است. از نظر روانشناسی مردم نیاز دارند که نسبت به تغییرات خود و محیط اطرافشان احساس امنیت و راحتی کنند.

استراتژی انتقال سرویس شامل زیر فرایندهای ذیل می باشد:

- **Managing changes to the "BAU" environment – مدیریت تغییرات در محیط های تجارت**

  مرسوم: فرآیندی است که برای درک و به حداقل رساندن ریسک‌ها در هنگام تغییر فناوری اطلاعات طراحی شده است
- **Service Asset and Configuration Management- مدیریت دارایی و پیکر بندی:** سرویس‌های IT معمولا از یک مجموعه component های مجزا تشکیل شده اند، مانند سرورها، نرم افزار و میان افزار و اطلاعات پیکربندی مخصوص به خود. مدیریت پیکربندی و دارایی در ITIL یا به اختصار SACM در مورد برنامه ریزی دقیق و مدیریت روابط و ویژگی های تمام این اجزاء (components) در سراسر هریک از سرویس‌های زیرساخت شما می‌باشد.
- **Transition Planning and Support- برنامه ریزی و پشتیبانی انتقال:** در هر زمان، پروژه های متعددی از مرحله انتقال سرویس در چرخه حیات می‌گذرد .مسئولیت هماهنگی فعالیت های انتقال سرویس برای همه این پروژه ها بر عهده برنامه ریزی و پشتیبانی انتقال است.
- **Release and Deployment Management- مدیریت توسعه و نسخه:** برنامه ریزی، زمانبندی و کنترل تهیه،



تست و استقرار نسخه ها و ارائه قابلیت‌های جدید مورد نیاز توسط کسب و کار ضمن حفظ یکپارچگی سرویس‌های موجود.

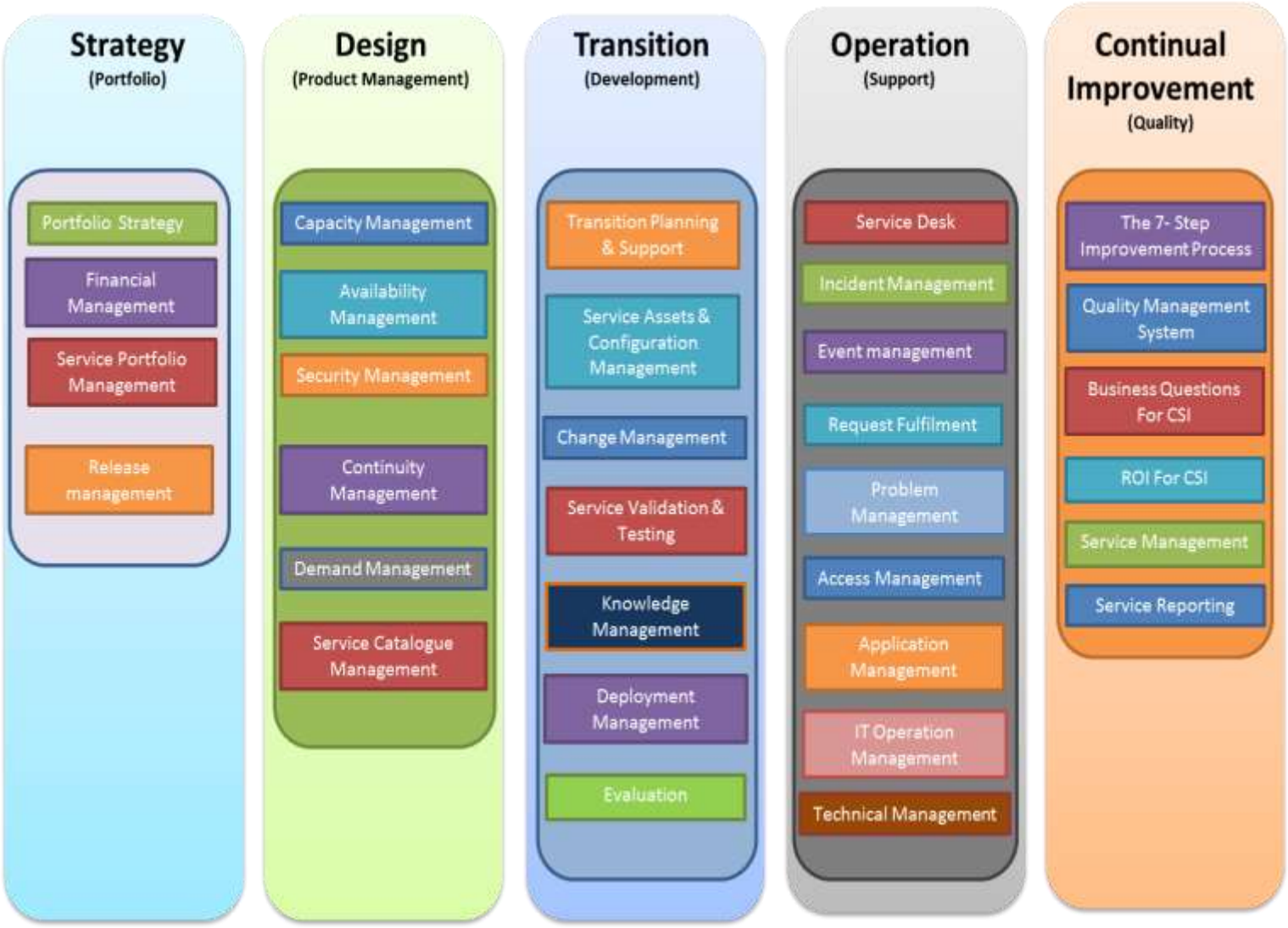
- **Change Management- مدیریت تغییرات:** تغییرات را قبل از آنکه به مرحله بعدی از چرخه حیات خود وارد شوند، مورد تجزیه و تحلیل قرار می‌دهد.
- **Service Validation and Testing- اعتبارسنجی و آزمایش خدمات:** عمل تست می‌تواند در هر نقطه از چرخه حیات سرویس انجام شود، اما عموما در طول مرحله انتقال سرویس صورت می‌گیرد. فرآیند اعتبارسنجی و تست سرویس در زمان تست سرویس‌های تغییریافته یا سرویس‌های جدید، برنامه ریزی و اجرا و گزارش می‌شود. جهت پشتیبانی از تصمیمی که در خصوص رفتن به مرحله بعدی گرفته شده، نتایج تست به فرآیند ارزیابی تغییر انتقال داده می‌شود.
- **Evaluation- ارزیابی:** تغییرات را قبل از آنکه به مرحله بعدی از چرخه حیات خود وارد شوند، مورد تجزیه و تحلیل قرار می‌دهد. چرخه حیات یک سرویس شامل چندین نقطه تصمیم گیری است که باید در آنجا در خصوص رفتن یا نرفتن به مرحله بعدی تصمیم گیری شود
- **Knowledge Management- مدیریت دانش:** مدیریت دانش، مسئولیت نگهداری سیستم مدیریت دانش سرویس (SKMS)را بر عهده دارد، این سیستم کل دانش موجود در سازمان مدیریت سرویس را نشان می‌دهد .برای ارائه موفق سرویس، دانش باید جمع آوری و سازماندهی شده و در دسترس کلیه افرادی که به دانستن آن نیاز دارند، قرار گیرد SKMS . دربرگیرنده کلیه داده های ذخیره شده دیگری است که توسط مدیریت سرویس مورد استفاده قرار می‌گیرد.

هدف

نقش انتقال خدمت، تحویل خدمت موردنیاز کسب‌وکار به کاربرد عملیاتی است. انتقال خدمت این کار را از طریق دریافت بسته طراحی خدمت از مرحله طراحی خدمت و تحویل تمامی عناصر موردنیاز برای انجام و پشتیبانی خدمت مستمر به مرحله عملیاتی به انجام می‌رساند. چنانچه شرایط، مفروضات یا نیازمندی‌های کسب‌وکار در خلال طراحی تغییر نماید آنگاه ممکن است نیازمند تغییراتی در حین مرحله انتقال خدمت به‌منظور تحویل خدمت موردنیاز باشیم.

انتقال خدمت روی پیاده‌سازی تمام جنبه‌های خدمت و نه‌فقط برنامه‌های کاربردی و چگونگی استفاده از آن‌ها در شرایط نرمال تمرکز دارد. این موضوع مستلزم تضمین این نکته است که خدمت بتواند در شرایط بد و غیرطبیعی قابل پیش‌بینی عمل کند و در برابر خرابی و خطاهای موجود پشتیبانی ارائه نماید. این موضوع مستلزم شناخت کافی از موارد زیر است:

- ارزش کسب‌وکار بالقوه و کسی که ارزش به او تحویل‌شده و یا توسط او مورد قضاوت قرار می‌گیرد.
- شناسایی تمام ذینفعان در بین تأمین‌کننده، مشتری و دیگر زمینه‌ها
- برنامه‌های کاربردی و انطباقی طراحی خدمت، شامل چیدمان تغییرات طراحی که در خلال انتقال نیاز به آن احساس شده است.



مسئولیت‌های کلیدی

انتقال خدمت به‌وسیله مسئولیت‌های پایه‌ریزی شده‌ای که استفاده کارا و اثربخش از خدمات جدیداً تغییریافته را تسهیل می‌کند، پشتیبانی می‌شود.
مسئولیت‌های کلیدی شامل:

- فهم تمامی خدمات، تسهیلات و ضمانت‌نامه‌ها به‌منظور انتقال اثربخش یک خدمت که برای دانستن ماهیت و هدفش ازلحاظ نتایج و یا محدودیت‌های رفع شده کسب‌وکار (تسهیلات) و تضمین این موضوع که خدمات عمومی تحویل داده خواهد شد (ضمانت‌نامه‌ها.)
- ایجاد یک سیاست رسمی و چارچوب معمول برای پیاده‌سازی تمامی تغییرات موردنیاز، انسجام و جامعیت تضمین می‌کنند که خدمات، ذینفعان، دیگر فرصت‌ها نادیده گرفته نشده و بنابراین باعث شکست خدمت نشده است.
- پشتیبانی از تبادل دانش، پشتیبان تصمیم‌گیری و استفاده مجدد از فرایندها، سیستم‌ها و عوامل دیگر، انتقال خدمت اثربخش با مشارکت تمام قسمت‌های مربوطه ارائه می‌شود، تضمین دانش مناسب در دسترس است و کاری که به انجام رسیده قابل‌استفاده مجدد در شرایط مشابه آینده است.
- پیش‌بینی و مدیریت دوره اصلاحات به‌صورت فعال بوده (پیشبینانه) و تعیین احتیاجات محتمل دوره اصلاحات، هنگامی‌که عواملی از یک خدمت نیازمند تنظیم باشند، به‌صورت منطقی انجام و به‌صورت کامل مستندسازی خواهد شد.
- اطمینان از مشارکت انتقال خدمت و نیازمندی‌های انتقال خدمت در چرخه عمر خدمت.

فعالیت‌ها و فرایندهای کلیدی

در مجموعه فرایندهای انتقال خدمت، برخی از فرایندهای مهم در انتقال خدمت در تمامی فرایندهای چرخه عمر هستند، نقش ورودی و ملاحظات کنترلی و دیده‌بانی در کل مراحل چرخه عمر دارند و در آن‌ها تأثیرگذارند. مجموع فرایندهای چرخه عمر عبارت‌اند:

- مدیریت تغییر
- دارایی خدمت و مدیریت پیکربندی
- مدیریت دانش

فرایندهایی که روی انتقال خدمت تمرکز دارند ولی منحصر به این مرحله نیستند عبارت‌اند از:

- برنامه‌ریزی و پشتیبانی انتقال
- مدیریت توسعه و نسخه
- تست و تأیید اعتبار خدمت
- ارزیابی

مدیریت تغییر

مدیریت تغییر تضمین‌کننده این موضوع است که تغییرات طی یک روش کنترل‌شده ذخیره، ارزیابی، مجوزدار، اولویت‌بندی، برنامه‌ریزی، آزمون، پیاده‌سازی، مستند و بازبینی شده باشد.

هدف از فرایند مدیریت تغییر تضمین این موضوع است که روش‌های استانداردشده برای اعمال سریع و کارای تمام تغییرات استفاده شده است، تمامی این تغییرات در سیستم مدیریت پیکربندی ضبط شده است و کلیه مخاطرات کسب‌وکار بهینه‌شده‌اند.

فرایند تمامی تغییرات خدمت را نشان می‌دهد.

تغییر خدمت اضافه کردن، تغییر یا حذف یک خدمت یا جزء خدمت مجاز، برنامه‌ریزی شده یا پشتیبانی شده و مستندات مربوطه است.

بنابراین مدیریت تغییر مربوط به تمام چرخه عمر است و برای تمامی سطوح مدیریت خدمت (استراتژیکی، تاکتیکی و عملیاتی) به کار برده می‌شود.

شکل ۴ -محدوده مدیریت تغییر و نسخه خدمات

مدیریت تغییر، کاهش در خطاهای خدمات جدید یا تغییریافته و پیاده‌سازی دقیق‌تر و سریع‌تر تغییرات را در پی دارد. مدیریت تغییر باعث می‌شود سرمایه‌ها و منابع محدود روی تغییراتی که بیشترین سود را برای کسب‌وکار دارند، تمرکز داده شوند.

مدیریت پیکربندی و دارایی خدمت(SACM)

SACMبه‌وسیله ارائه اطلاعات دقیق و کنترل تمامی دارایی‌ها و ارتباط آن‌ها که زیرساخت یک سازمان را تشکیل می‌دهد، کسب‌وکار را پشتیبانی می‌کند.

هدف از SACM شناسایی، کنترل و حسابداری دارایی‌های خدمت و بخش‌های پیکربندی (CI) حفاظت و تضمین یکپارچگی آن در چرخه عمر خدمت است.

حوزه SACM همچنین به دارایی‌های فناوری اطلاعات و ارائه‌دهندگان داخلی و خارجی که دارایی‌های مشترک نیازمند به کنترل دارند تعمیم داده شده است.

برای خدمات فناوری اطلاعات و زیرساخت‌های بزرگ و پیچیده SACM نیازمند استفاده از سیستم پشتیبانی است که به‌عنوان سیستم مدیریت پیکربندی (CMS)شناخته می‌شود.

مدیریت دانش

هدف از مدیریت دانش تضمین این موضوع است که فرد درست با دانش درست، در زمان درست خدمات موردنیاز کسب‌وکار را تحویل و پشتیبانی می‌نماید؛ که خود باعث موارد زیر است:

- خدمات کاراتر با کیفیتی بهبودیافته
- فهم واضح و متداول از ارزش خدمت ارائه‌شده
- اطلاعات مرتبط که همیشه در دسترس باشد

در قلب مدیریت دانش ساختار (داده – اطلاعات – دانش – خرد) قرار دارد که داده‌های خام – غیرقابل‌استفاده – را به دارایی‌های باارزش تبدیل می‌کند. این موضوع با سیستم مدیریت دانش خدمت، نگهداری اطلاعات و دانش و خرد حاصل از داده‌های پیکربندی و دارایی تبیین می‌شود.

برنامه‌ریزی و پشتیبانی انتقال

هدف برنامه‌ریزی و پشتیبانی انتقال عبارت‌اند از:

- برنامه‌ریزی و هماهنگی منابع به‌منظور تضمین اینکه نیازمندی‌های استراتژی خدمت که در طراحی خدمت گنجانده شده است به نحو اثربخشی در عملیات خدمت قابل تشخیص باشد.
- شناسایی، مدیریت و کنترل مخاطرات خرابی و اختلال در فعالیت‌های انتقال

برنامه‌ریزی و پشتیبانی انتقال اثربخش می‌تواند توانایی یک ارائه‌دهنده خدمت را به‌منظور مدیریت حجم زیادی از تغییر و نسخه‌ها بر پایه مشتری به‌طور قابل‌توجهی بهبود بخشد.

مدیریت توسعه و نسخه

هدف از فرایند مدیریت توسعه و نسخه، جمع‌آوری و جاگذاری تمام جنبه‌های خدمات به‌منظور تولید و ایجاد استفاده اثربخش آن خدمات جدید یا تغییریافته است.

توسعه و نسخه اثربخش، ارزش قابل‌توجهی از کسب‌وکار را با انجام تغییرات با سرعت، خطر و هزینه بهینه و ارائه یک پیاده‌سازی سازگار، مناسب و قابل ممیزی از خدمات کسب‌وکار قابل‌استفاده و مفید، موجب خواهد شد.

مدیریت توسعه و نسخه کل مراحل جمع‌آوری و پیاده‌سازی خدمات جدیداً تغییریافته را به‌منظور استفاده عملیاتی، از برنامه‌ریزی نسخه تا پشتیبانی از حیات اولیه، پوشش می‌دهد.

اعتبارسنجی و آزمون خدمت

آزمون موفق به فهم کلی نگرانه خدمت بستگی دارد – چگونگی استفاده آن و روشی که ساخته شده است. تمامی خدمات – داخلی یا خریداری‌شده – نیاز به آزمون مناسب دارند، تأمین اعتبارسنجی موردنیاز کسب‌وکار ممکن است از محدوده کاملی از شرایط مورد انتظار تا حد مخاطره کسب‌وکار توافق شده، قابل‌دستیابی باشد.

هدف کلیدی از آزمون و اعتبارسنجی خدمت ارائه نمونه قابل‌مشاهده‌ای از این موضوع است که خدمت جدیداً تغییریافته از نیازمندی‌های کسب‌وکار، شامل SLAهای توافق شده، پشتیبانی می‌کند.

خدمات آشکارا و واضح در برابر تسهیلات و ضمانت‌نامه‌ها که در بسته طراحی خدمت به‌تفصیل بیان شده، شامل آزمون عملکرد، دسترس‌پذیری، استمرار، امنیت، قابلیت استفاده و رگرسیون کسب‌وکار مورد آزمایش قرار می‌گیرد.

ارزیابی

اطمینان از مفید بودن خدمت برای کسب‌وکار برای انتقال خدمت موفق، مهم است و این موضوع به اطمینان از استمرار خدمت به‌وسیله ایجاد تکنیک‌های سنجش و معیارهای مناسب، تعمیم می‌یابد.

ارزیابی به ورودی انتقال خدمت توجه دارد، به موارد مرتبط به موارد ذیل می‌پردازد:

طراحی خدمت و خود روش انتقال و تناسب خدمت جدید یا تغییریافته با عملیات و محیط‌های کسب‌وکار واقعی مورد انتظار و پیش رو

فعالیت‌های عملیاتی مرحله انتقال خدمت

انتقال خدمت همچنین روی برخی از فعالیت‌های عملیاتی تمرکز دارد. این فعالیت‌ها کاربرد گسترده‌تری از انتقال خدمت داشته و به شرح زیر هستند:

- مدیریت ارتباطات و توافقات انجام‌شده در مدیریت خدمت فناوری اطلاعات
- مدیریت تغییر سازمانی و ذینفعان
- مدیریت ذینفعان
- سازمان انتقال خدمت و نقش‌های کلیدی

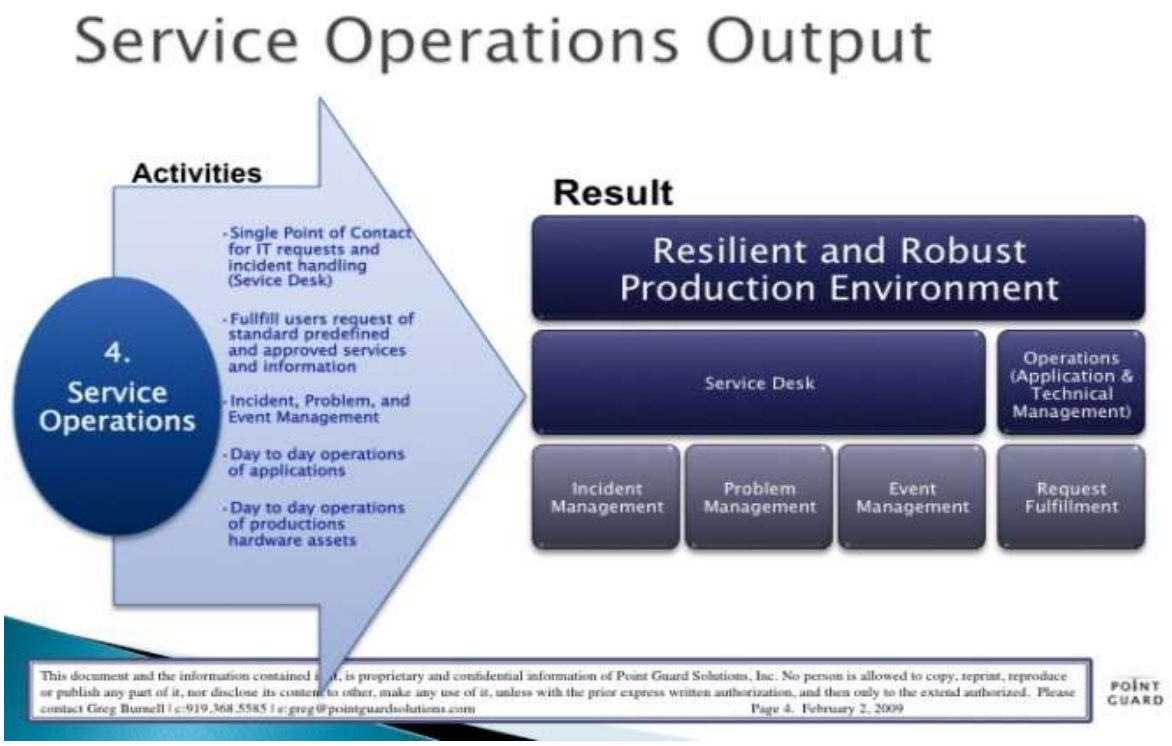
مسئولیت‌ها و نقش‌های کلیدی

افراد ارائه‌دهنده انتقال خدمت در یک سازمان می‌بایست برای انجام کارا و اثربخش کارها سازمان‌دهی شوند، گزینه‌های متنوعی برای ارائه این کار وجود دارد. قابل پیش‌بینی نیست که یک سازمان نوعی گروه جداگانه از افراد را برای ایفای این نقش در نظر بگیرد و یا در مقابل، روندی از تجربه و مهارت‌ها مورداستفاده قرار دهد – بدین معنی که افراد در مراحل مختلف چرخه عمر مشارکت نم

2.2.4 استراتژی عملیات سرویس(Service Operation)

Service operationشامل فعالیت ها، فرایندها و زیرساخت های روزمره است که مسئولیت تأمین ارزش برای کسب و کار را از طریق تکنولوژی بر عهده دارد.

ما در استراتژی سرویس(Service Strategy) ، طراحی سرویس(Service Design) ، انتقال سرویس (Service Transition)و بهبود مستمر سرویس (Continual Service Improvement)ارزش ایجاد می‌کنیم. اما هیچ سرویسی مصرف نشده و هیچ فعالیت تجاری در این زمینه تجربه نشده است. از آنجا که کاربران می‌توانند در طول اجرای سرویس به سرویس دسترسی داشته باشند، به همین علت ما به سطوح بالای پشتیبانی نیاز خواهیم داشت تا بتوانیم مصرف سرویس را در بالاترین سطح حفظ نماییم. هیچ یک از مشتریان نمی‌خواهند برای سرویسی که در حد نیاز کارایی ندارد یا برای استفاده در دسترس نیست، هزینه پرداخت کنند.



استراتژی عملیات سرویس شامل زیر فرایندهای ذیل الذکر می باشد

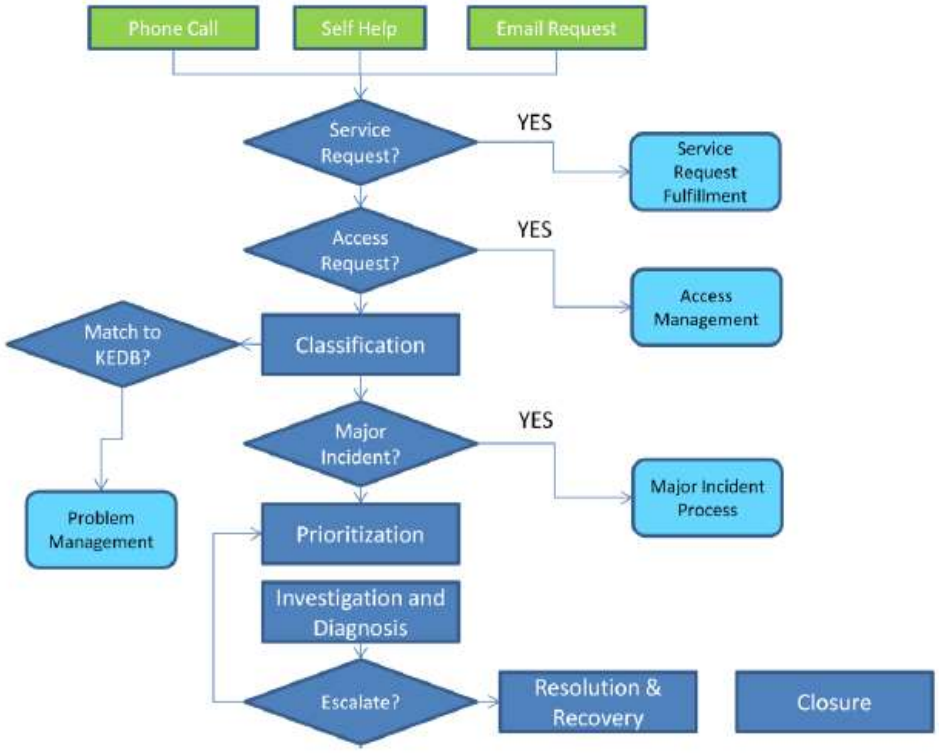
- **Incident Management – مدیریت رخداد:** مدیریت رخداد مربوط به ترمیم سریع خدمات و به حداقل رساندن تأثیر بر تجارت است. در بیشتر موارد اما نه در همه موارد ، روند مدیریت رخداد متعلق به **Service Desk** است. بر اساس توصیه های ITIL ، فرآیند مدیریت رخداد مراحل زیر را در بر می‌گیرد:

1) شناسایی رخداد
2) ثبت رخداد

3) دسته بندی رخداد
4) اولویت بندی رخداد
5) پاسخ رخداد(تشخیص اولیه- ارجاع رخداد به سطوح بالاتر-تحقیق و تشخیص-اجرا و بازیابی- بستن رخداد)

- **Problem Management – مدیریت مشکل:** مدیریت مسئله مربوط به شناسایی و تصحیح نقص ها یا خطاهای موجود در محیطی است که باعث بروز حوادث می شوند. مدیریت مسئله به کاهش و جلوگیری از بروز حوادث کمک می کند. مدیریت مسئله بطور گسترده به دو فرایند اصلی تقسیم می شود 1- مدیریت مشکل واکنشی 2- مدیریت مشکل فعال
- **Event Management – مدیریت رویداد:** مدیریت رویداد مربوط به تشخیص وقایع در زیرساخت ها و انتخاب اقدامات واکنشی مناسب است. با تسهیل در تشخیص زود هنگام رخداد، مدیریت رویداد به کاهش تعداد رخدادی که کاربران را تحت تأثیر قرار می دهد کمک می کند و می تواند عملکرد فرآیند مدیریت رخداد را به میزان قابل توجهی بهبود بخشد. رویدادها ممکن است یکی از سه نوع اساسی باشند:

❖ اطلاع رسانی(Informational) - هیچ عملی لازم نیست. اطلاعات رویداد برای مرجع احتمالی آینده ثبت می شود.
❖ هشدار(Warning) - یک مورد زیرساختی به یک آستانه از پیش تعریف شده عملکرد یا ظرفیت نزدیک می شود که می تواند باعث حادثه شود یا نیاز به مداخله دارد.



Integration Between Service Operation Processes

❖ ception استثناء - یک مورد زیرساخت از آستانه فراتر رفته است یا دیگر در پارامترهای تعریف شده کار نمی کند. مداخله لازم است

- **Service Request – درخواست خدمات**: درخواست یک کاربر برای اطلاعات، مشاوره، تغییر استاندارد یا دسترسی به یک سرویس.
- **Access Management- مدیریت دسترسی:** مدیریت دسترسی با مدیریت امنیت اطلاعات همکاری کرده تا از این طریق اطمینان حاصل کند که قوانین دسترسی در سیاست‌های امنیتی اطلاعات، اجرا می‌شود. درخواست‌های دسترسی ممکن است با عنوان درخواست‌های سرویس ایجاد شده و توسط میز خدمات اداره شوند و یا ممکن است به منظور اجرا، به یک گروه امنیتی هدایت شوند
- **Service Desk – سرویس خدمات:** میز خدمات تنها یک نقطه تماس بین کاربران و سازمان فناوری اطلاعات را فراهم می کند. خدمات سرویس حوادث ورودی ، درخواست خدمات ، تغییر درخواست ها و غیره را پردازش می کند. معمولاً (اما نه همیشه) فرآیند مدیریت Incident را مالک و اجرا می کند. میز خدمات همچنین به عنوان مرکز ارتباطات داخلی در ارائه دهنده خدمات IT فعالیت می کند.

هدف

هدف از انجام خدمت ارائه سطوح توافق شده خدمت به کاربران و مشتریان و مدیریت برنامه‌های کاربردی، تکنولوژی و زیرساختی است که ارائه خدمات را پشتیبانی کند.

تنها در خلال این مرحله از چرخه عمر است که خدمات به‌طور واقعی ارزش را به کسب‌وکار منتقل می‌کنند و این مسئولیت افراد درگیر در انجام خدمت است که از انتقال این ارزش اطمینان حاصل نمایند.

برای انجام خدمت بسیار مهم است که تناقض بین اهداف را متعادل نماید:

- دیدگاه فناوری اطلاعات داخلی در برابر دیدگاه کسب‌وکار
- ثبات در برابر پاسخگویی (واکنش(
- کیفیت خدمت در برابر هزینه خدمت
- فعالیت‌های واکنشی در برابر کنشی

برای هریک از این تناقضات، افراد می‌بایست تعادل را حفظ کنند، به‌عنوان‌مثال تمرکز بیش از حد روی یک جنبه از این تناقضات منتج به ارائه ضعیف خدمت باشد.

بسیاری از سازمان‌ها توجه به سلامت عملیاتی خدمات را مفید می‌دانند. سلامت عملیاتی علامت‌های حیاتی که برای اجرای وظایف حیاتی کسب‌وکار شناسایی می‌کند. چنانچه این علامت‌ها در محدوده نرمال باشند سیستم یا خدمت سلامت هستند. این موضوع منجر به کاهش هزینه نظارت شده و افراد را قادر می‌سازد تا روی زمینه‌ای که منجر به موفقیت خدمت می‌شوند، تمرکز کنند.

فعالیت‌ها و فرایندهای کلیدی

فرایند مدیریت رویداد

یک رویداد، تغییر حالتی است که برای مدیریت یک بخش پیکربندی یا خدمت فناوری اطلاعات دارای اهمیت است.

یک رویداد نشان می‌دهد که بعضی چیزها به‌درستی عمل نمی‌کنند و منجر به ثبت یک رخداد شده‌اند.

همچنین ممکن است رویدادها نشان‌دهنده فعالیتی نرمال یا نیاز به مداخله معمول مانند تغییر یک نوار باشد.

مدیریت رویداد بستگی به نظارت دارد اما با آن متفاوت است. مدیریت رویداد ایجاد و تشخیص اعلامیه‌ها است، درحالی‌که نظارت وضعیت اجزاء را حتی زمانی که رویدادی اتفاق نیفتاده است، بررسی می‌کند.

رویدادها ممکن است به‌وسیله یک پیام ارسالی Cl یا یک ابزار مدیریتی نمونه برداری از Cl تشخیص داده شود. پس از اینکه رویداد تشخیص داده شد ممکن است منجر به یک رخداد، مشکل یا تغییر شود یا ممکن است به‌سادگی در حد اطلاعات لازم ذخیره شود.

پاسخ‌دهی به یک رویداد ممکن است اتوماتیک بوده و یا دستی باشد. چنانچه اقدامی لازم باشد سپس یک آغازگر، مانند یک SMS یا یک رخداد ذخیره‌شده اتوماتیک، می‌تواند به افراد پشتیبان هشدار دهد.

فرایند مدیریت رخداد

یک رخداد یک قطعی برنامه‌ریزی نشده برای یک خدمت فناوری اطلاعات یا کاهش در کیفیت خدمت فناوری اطلاعات است. خرابی یک بخش پیکربندی که هنوز خدمت را تحت تأثیر قرار نداده است نیز یک رخداد است.

هدف از مدیریت رخداد بازیابی خدمت نرمال با حداکثر سرعت ممکن و حداقل کردن تأثیر مضر روی عملیات کسب‌وکار است.

رخدادها معمولاً به‌وسیله مدیریت رویداد و یا به‌وسیله تماس کاربران با پیشخوان خدمت مشخص می‌شوند. رخدادها به‌منظور شناسایی فردی که باید روی آن‌ها کار کند و برای تجزیه‌وتحلیل روند گروه‌بندی می‌شوند و طبق ضرورت و تأثیرشان بر کسب‌وکار اولویت‌بندی می‌شوند.

چنانچه رخداد به‌سرعت حل نشود ممکن است تشدید شود. افزایش عملکرد رخداد را به تیم فنی پشتیبانی با مهارت‌های مناسب ارسال می‌کند و افزایش سلسله مراتبی سطوح مناسب مدیریت را به کار می‌گیرد.

بعد از اینکه رخداد موردبررسی و تشخیص داده شد و راه‌حل مورد آزمایش قرار گرفت، پیشخوان خدمت می‌بایست پیش از خاتمه رخداد از رضایت کاربر اطمینان حاصل کند.

یک ابزار مدیریت رخداد برای ضبط و مدیریت اطلاعات رخداد حیاتی است.

فرایند انجام درخواست

یک درخواست خدمت، درخواست یک کاربر است برای اطلاعات، راهنمایی یا برای یک تغییر استاندارد و یا برای دسترسی به یک خدمت فناوری اطلاعات.

هدف از انجام درخواست این است که کاربران را قادر سازد خدمات استاندارد را درخواست و دریافت نمایند؟ این خدمات را تأمین و ارائه نماید؟ اطلاعات خدمات و روش‌های دستیابی به آن‌ها را برای کاربران و مشتریان تهیه نماید؟ اطلاعات عمومی، شکایت‌ها و نظرات را جمع‌آوری نماید.

تمامی درخواست‌ها می‌بایست جمع‌آوری و پیگیری شود. فرایند می‌بایست شامل تاییدات قبل از انجام درخواست باشد.

فرایند مدیریت دسترسی

هدف از فرایند مدیریت دسترسی ارائه اجازه برای کاربران به‌منظور دسترسی به یک خدمت یا گروهی از خدمات، درحالی‌که از دسترسی کاربران فاقد مجوز جلوگیری می‌شود.

مدیریت دسترسی به مدیریت محرمانگی، دسترس‌پذیری و یکپارچگی داده و مالکیت معنوی کمک می‌کند.

مدیریت دسترسی با هویت (اطلاعات منحصربه‌فردی که یک چیز را متمایز می‌کند) و حقوق (تنظیماتی که دسترسی به داده و خدمات را ارائه می‌کند).

فرایند شامل تأیید هویت و حق، اعطای دسترسی به خدمات، ثبت و ردیابی دسترسی و برداشتن یا تعریف حقوق هنگامی‌که وضعیت یا نقش‌ها (ی کاربران) تغییر می‌کند.

فرایند مدیریت مشکل

مشکل یک علت از یک یا چند رخداداست. علت معمولاً در زمان ایجاد سابقه مشکل شناخته‌شده نیست و فرآیند مدیریت مشکل مسئول تحقیقات بیشتر است.

اهداف کلیدی مدیریت مشکل جلوگیری از وقوع رخدادها و مشکلات، حذف تکرار رخدادها و حداقل نمودن اثر رخدادهایی که نمی‌توان مانع آن‌ها شد.

مدیریت مشکل شامل تشخیص علل رخدادها، تعیین راهکار و اطمینان از پیاده‌سازی راهکار است. مدیریت مشکل اطلاعات پیرامون مشکلات و راه حل‌ها و راهکارهای مناسب را حفظ می‌کند.

مشکلات با روشی مشابه رخدادها گروه‌بندی می‌شوند، اما هدف درک علل، مستندسازی راه‌حل‌ها و درخواست تغییر به‌منظور حل دائمی مشکلات است. راه‌حل‌ها در یک پایگاه داده خطای شناخته‌شده مستند می شوند تا کارایی و اثربخشی مدیریت رخداد را بهبود بخشد.

فعالیت‌های معمول انجام خدمت

انجام خدمت شامل تعدادی فعالیت است که جزو پنج فرایند توضیح داده شده قبلی نیست. به شرح زیر:

- کنترل و نظارت: شناسایی وضعیت خدمات و اجزای پیکربندی و اتخاذ اقدام اصلاحی مناسب
- مدیریت کنسول / پل عملیات: یک نقطه هماهنگی مرکزی برای نظارت و مدیریت خدمات
- مدیریت زیرساخت: ذخیره، پایگاه‌های داده، واسط افزار، خدمات دایرکتوری، مرکز داده / ابزار و...

- زمینه‌های عملیاتی فرایندها از دیگر مراحل چرخه عمر: تغییر، پیکربندی، نسخه و توسعه، دسترس پذیری، ظرفیت، دانش، مدیریت استمرار خدمت و ...

وظایف کلیدی

پیشخوان خدمت یک نقطه مرکزی منحصربه‌فرد تماس برای تمام کاربران خدمت ارائه می‌نماید. معمولاً پیشخوان خدمت تمامی رخدادها، درخواست‌های خدمت و درخواست‌های دسترسی را ذخیره و مدیریت می‌کند و یک رابط کاربری برای تمام فرایندهای و فعالیت‌های دیگر انجام خدمت ارائه می‌دهد.

مسئولیت‌های خاص پیشخوان خدمت شامل موارد زیر است:

- ثبت تمامی رخدادها و درخواست‌ها، گروه‌بندی و اولویت‌بندی آن‌ها
- تحقیق و تشخیص اولیه
- مدیریت چرخه عمر رخدادها و درخواست‌ها، افزایش متناسب و حل‌وفصل آن‌ها به‌نحوی‌که رضایت کاربر جلب شود.
- اطلاع‌رسانی به کاربران در خصوص وضعیت خدمات، رخدادها و درخواست‌ها

راه‌های فراوانی برای ساختاردهی و سازمان‌دهی پیشخوان‌های خدمت وجود دارد. شامل:

- پیشخوان خدمت محلی: به‌صورت فیزیکی نزدیک به کاربران است.
- پیشخوان خدمت متمرکز: اجازه می‌دهد افراد کمتری با حجم بیشتری از درخواست‌ها سروکار داشته باشند.
- پیشخوان خدمت مجازی: افراد در مکان‌های مختلف حضور دارند ولی از دید کاربران مانند یک تیم به نظر می‌رسند.
- به دنبال خورشید: پیشخوان‌های خدمت در محدوده‌های زمانی مختلف به‌وسیله انتقال تماس به محل‌های دیگری که در ساعت کاری هستند، پوشش ۲۴ ساعته خدمت ارائه می‌کنند.

وظیفه مدیر فنی

مدیریت فنی شامل تمام افرادی است که تخصص فنی و مدیریتی زیرساخت فناوری اطلاعات ارائه می‌دهند.

مدیریت فنی به برنامه‌ریزی، پیاده‌سازی و حفظ یک زیرساخت فنی باثبات کمک می‌کند و تضمین می‌کند که تخصص‌ها و منابع موردنیاز برای طراحی، ساخت، انتقال، انجام و بهبود خدمات فناوری اطلاعات و تکنولوژی پشتیبانی در دسترس هستند.

فعالیت‌های قابل انجام به‌وسیله مدیریت فنی به شرح زیر است:

- تعریف استانداردهای معماری
- مشارکت در طراحی و ساخت خدمات جدید و شیوه‌های عملیاتی
- کمک به پروژه‌های طراحی خدمت، انتقال خدمت یا بهبود مستمر خدمت.
- کمک به فرایندهای مدیریت خدمت، کمک به تعریف استانداردها و ابزارها و انجام فعالیت‌هایی نظیر ارزیابی درخواست‌های تغییر
- کمک به مدیریت تماس‌ها و تأمین‌کنندگان

مدیریت فنی معمولاً بر اساس زیرساختی که هر تیم پشتیبانی می‌کند سازمان‌دهی می‌شود.

وظیفه مدیریت برنامه‌های کاربردی

مدیریت برنامه‌های کاربردی شامل تمام افرادی است که تخصص فنی و مدیریت برنامه‌های کاربردی ارائه می‌کنند. آنچه آن‌ها ارائه می‌کنند بسیار شبیه نقش مدیریت فنی است اما با تمرکز بیشتر روی نرم‌افزارهای کاربردی به‌جای زیرساخت.

به‌طورمعمول در بسیاری از سازمان‌ها به برنامه‌های کاربردی به‌عنوان خدمات اشاره می‌شود اما برنامه‌های کاربردی فقط مؤلفه مورد نیاز برای ارائه خدمت است. هر برنامه کاربردی ممکن است بیش از یک خدمت را پشتیبانی نماید و هر خدمت ممکن است از بسیاری از برنامه‌های کاربردی استفاده نماید. این موضوع مخصوصاً برای ارائه‌دهندگان خدمت مدرن که خدمات اشتراکی را بر اساس معماری‌های خدمت گرا ایجاد می‌نمایند، صدق می‌کند.

مدیریت برنامه‌های کاربردی همکاری تنگاتنگی با توسعه دارد اما یک وظیفه متمایز با نقش‌های مختلف است. فعالیت‌های انجام‌شده به‌وسیله مدیریت برنامه‌های کاربردی شبیه به موارد توضیح داده شده بالا برای مدیریت فنی است.

مدیریت برنامه‌های کاربردی معمولاً با خطوط (سیاست‌های) کسب‌وکاری که از آن پشتیبانی می‌کند سازمان‌دهی می‌شود.

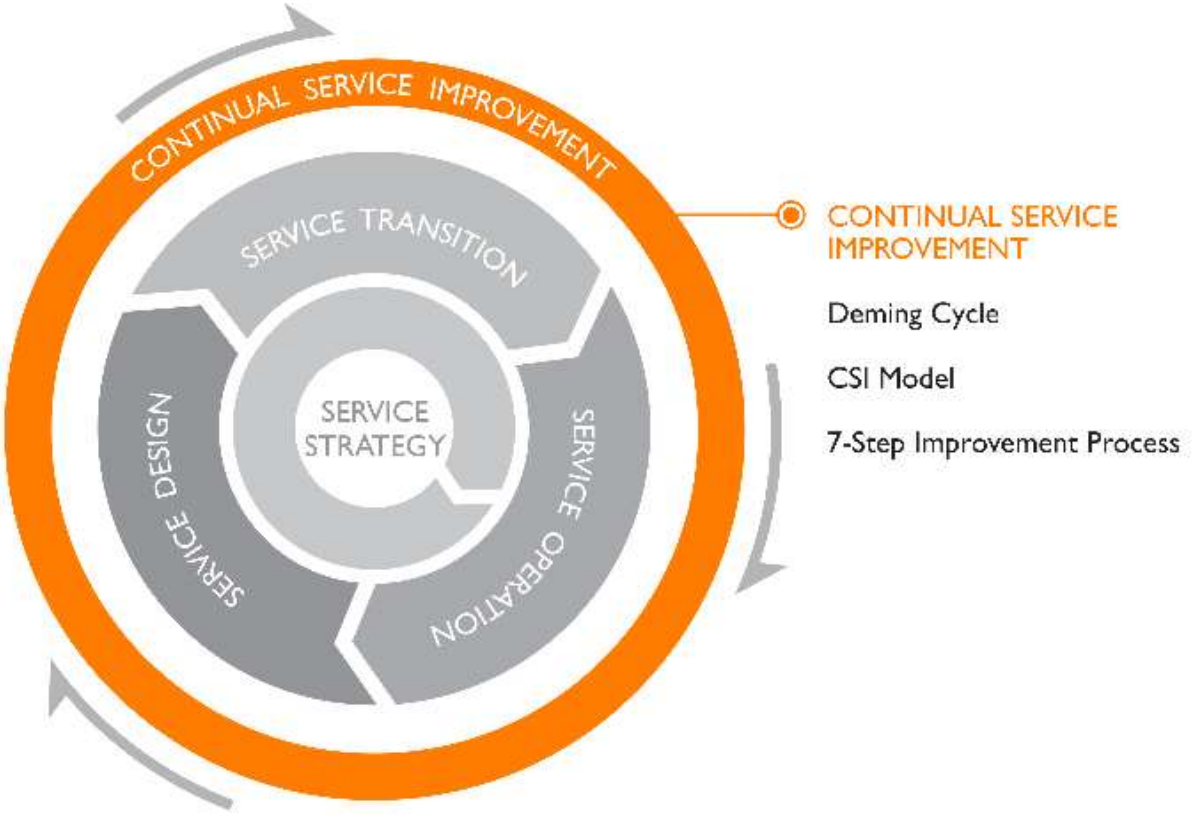
وظیفه مدیریت عملیات فناوری اطلاعات

مدیریت عملیات فناوری اطلاعات مسئول مدیریت و نگهداری زیرساخت مدیریت فناوری اطلاعات موردنیاز (برای تحویل سطح توافق شده فناوری اطلاعات به کسب‌وکار) است و شامل دو وظیفه زیر است:

- کنترل عملیات فناوری اطلاعات معمولاً به‌وسیله گروهی از اپراتورها که فعالیت‌های عملیاتی روتین را انجام می‌دهند، اداره می‌شود. آن‌ها کنترل و نظارت متمرکز، معمولاً از یک پل عملیاتی یا مرکز عملیات، فراهم می‌کنند.
- مدیریت تسهیلات مسئول مدیریت مراکز داده، اتاق‌های کامپیوتر و سراچه‌های بازیابی است. مدیریت تسهیلات همچنین پروژه‌های در مقیاس بزرگ، مانند تقویت مرکز داده یا تقویت سرور را هماهنگ می‌کند.

2.2.5 استراتژی بهبود مستمر سرویس (Continual Service Improvement)

هدف بهبود مداوم سرویس، مرتب سازی و بهینه سازی دوباره سرویس های IT، برای تغییر نیازهای تجاری، بوسیله تعریف و پیاده سازی بهبودها در سرویس های IT یی است که فرآیند تجاری را پشتیبانی می کنند. دورنمای بهبود مداوم سرویس در بهبودها، دورنمای تجاری کیفیت سرویس است، حتی با اینکه بهبود مداوم سرویس، می خواهد تاثیرات فرآیندها و بازدهی و هزینه موثر



فرآیندهای IT را در تمامی طول چرخه حیاتشان بهبود ببخشد. بر اساس بهبود مدیریت، بهبود مداوم سرویس باید بصورت کاملا روشن و واضح، تعریف کند که چه چیزی باید کنترل و اندازه گیری شود تا منجر به بهینه سازی مطلوب سرویس ها گردد. مرتب سازی و بهینه سازی دوباره سرویس های IT به منظور همخوانی با تغییر نیازهای تجاری در سازمان انجام می شود (به آن دلیل که ثبات، باعث رو به زوال رفتن سازمان و یا تنزل و رکود در سرویس دهی های آن می شود). در بخش بهبود مداوم سرویس، باید مانند سایر تجربیات موفق عمل شود. آنها نیازمند یک برنامه ریزی بالا به پیش رو (upfront)، آموزش و اطلاع رسانی صحیح، زمان بندی مداوم، ایجاد نقش ها، نسبت دادن به خود و فعالیت ها براساس میزان موفقیت آنها شناسایی می شوند. بهبود مداوم سرویس باید مانند فرآیندها با فعالیت های تعریف شده، ورودی ها، خروجی ها، نقش ها و گزارش ها، برنامه ریزی و زمان بندی گردد. مادامی که سازمان در حال شناسایی سرویس‌هایش است (اینکه چه سرویس‌هایی دارد)، همچنین فرآیند توسعه و پیاده سازی مدیریت سرویس فن آوری اطلاعات (IT Service Management - ITSM) آن سرویس ها را قابل استفاده می نماید.

بسیاری بر این باورند که کار مشکل انجام شده است. آنها سخت در اشتباهند! کار واقعی تازه آغاز شده است. اینکه سازمان ها چگونه برای استفاده از فرآیندهای جدید درگیر می شوند (چگونه بر اساس فرآیند جدید کار می کنند)؟ سازمان ها چگونه می سنجند، گزارش می گیرند و از اطلاعات برای بهبود نه تنها فرآیندهای جدید بلکه بهبود مداوم سرویس های مهیا شده اقدام می کنند؟ این کار مستلزم یک بحث خردمندانه برای آداپته کردن بهبود مداوم سرویس با ورودی ها، خروجی ها و نقش های تعریف شده و مسئولیت ها و اهداف و رویه هایی است که بطور واضح تعریف شده و یا مستندسازی شده اند، می باشد. برای موفقیت هر چه بیشتر در این قسمت، روند بهبود و بهینه سازی مداوم سرویس باید با فرهنگ هر سازمان سازگار و بومی (embed) شود. فاز بهبود مداوم سرویس در تمام فازهای چرخه حیات سرویس درگیر می‌باشد و مسئولیت سنجش سرویس و فرآیندها (سنجش سرویس - Service Measurement)، و مستندسازی نتایج (گزارش گیری سرویس - Service Reporting) براساس بهبود کیفیت سرویس و سنجش فرآیندها (بهبود سرویس - Service Improvement) را بر عهده دارد . این بهبودها در بازه بعدی چرخه حیات سرویس پیاده سازی خواهند شد، مجددا با استراتژی سرویس آغاز می‌شوند و سپس با طراحی و انتقال سرویس، فاز عملیات سرویس -البته برای عملیات مدیریتی- درطول تمامی بازه های سرویس ادامه می یابند.

پس از چند بازه بهینه‌سازی سرویس‌ها، " سود و زیان " شروع می کند به سودرسانی و پس از چند دوره همکاری تجاری (بسته به پیچیدگی و تنوع سرویس‌ها و نیز انعطاف پذیری کسب و کار)، سود و منافع ثابت می شوند، که این بدان معناست که سازمان های IT محور، به سطح صحیحی از سنجش در مدیریت فرآیندها و سرویس‌های خود و نیز به سطح صحیحی از کارآیی در برآورده‌سازی نیازمندی های سطح سرویس (Performance in meeting the Service Level Requirements) در سازمان متبوع خود رسیده‌اند.

بهبود مستمر سرویس (CSI) از طریق اندازه گیری و بهبود مداوم سرویس و به طور کلی افزایش بلوغ چرخه حیات مدیریت سرویس های IT و فرآیندهای زیر مجموعه آن ارزش را برای مشتریان فراهم می نماید .CSI با ترکیب قوانین، تجارب و روش های مدیریت کیفیت، مدیریت تغییرات و بهبود قابلیت ها هر مرحله از چرخه حیات سرویس (شامل سرویس موجود، فرآیندها و فعالیت ها و تکنولوژی های مربوط به آن) را بهبود می بخشد.

هدف

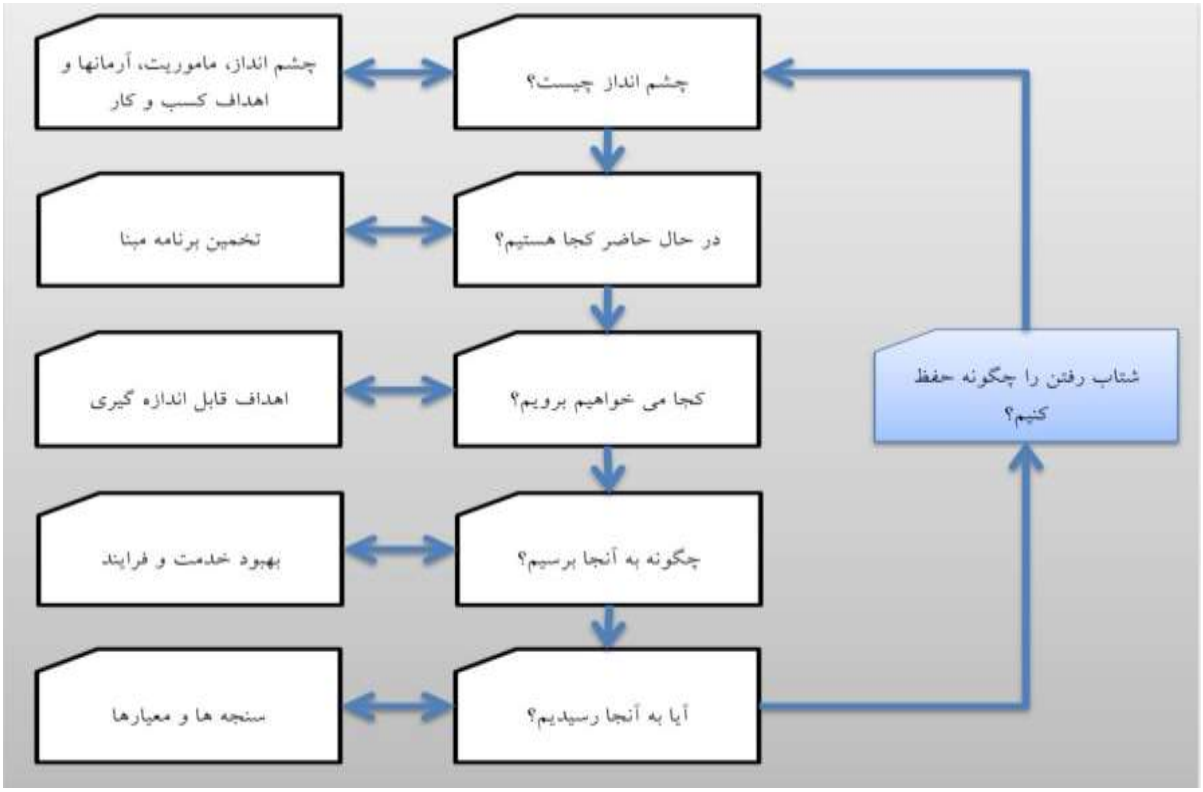
بهبود مستمر خدمت (CSI) با حفظ ارزش برای مشتری از طریق ارزیابی مستمر و بهبود کیفیت خدمات و بلوغ کلی چرخه عمر خدمت ITSM و فرایندهای مربوطه است.

CSIمسئولیت‌ها، شیوه‌ها و روش‌های مدیریت کیفیت، مدیریت تغییر و بهبود قابلیت، کار برای بهبود هر مرحله در چرخه عمر خدمت و نیز خدمات جاری، فرایندها و تکنولوژی و فعالیت‌های مرتبط ترکیب می‌نماید.

CSIمفهوم جدیدی نیست، اما برای بیشتر سازمان‌ها این مفهوم فراتر از مرحله بحث نرفته است. برای بسیاری از سازمان‌ها، هنگامی‌که چیزی شکست خورده و اثر جدی بر کسب‌وکار می‌گذارد CSIدر قالب یک پروژه مطرح می‌شود. هنگامی‌که مورد حل شد این مفهوم تا مشکل بزرگ بعدی

به‌طور کامل به دست فراموشی سپرده می‌شود. پروژه‌های گسسته با زمان محدود هنوز هم نیاز هستند، اما برای موفقیت می‌بایست CSI در فرهنگ‌سازمانی جای داده شده و به‌صورت فعالیت روتین دربیاید.

مدل CSI که در شکل زیر نشان داده شده است راهی برای یک سازمان به‌منظور شناسایی و مدیریت بهبودهای مناسب به‌وسیله شفاف‌سازی موقعیت و ارزش (ارائه‌شده به کسب‌وکار) جاری خود با اهداف و مقاصد بلندمدتشان و شناسایی فواصل موجود (بین اهداف و وضعیت جاری) ارائه می‌کند. این مهم بر اساس استمرار انجام‌شده است تا تغییرات در نیازمندی‌های کسب‌وکار، تکنولوژی و اطمینان از حفظ کیفیت بالا را اداره کند.



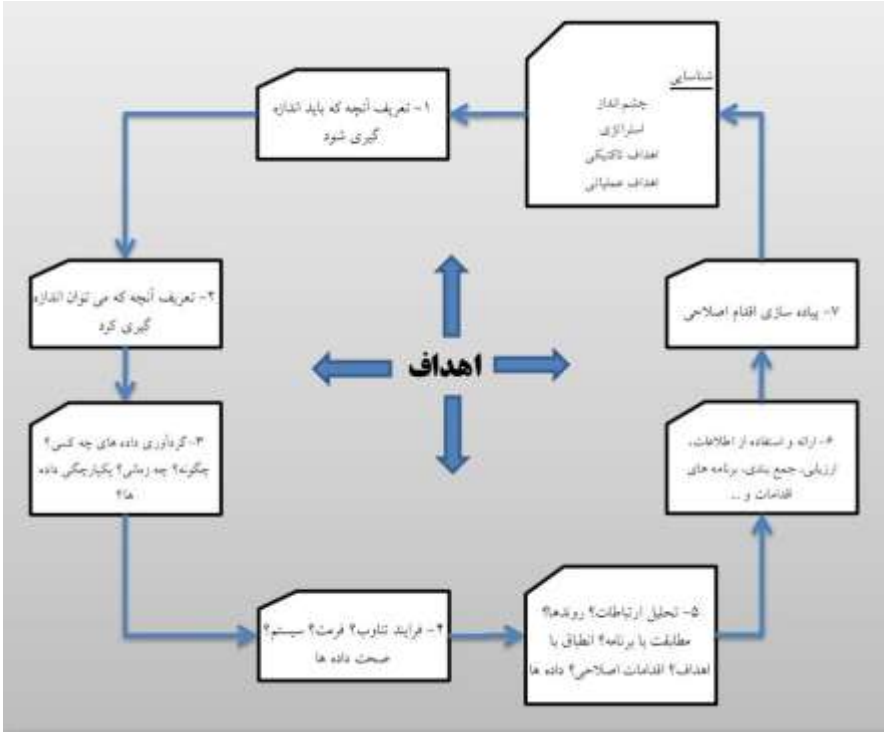
مدل بهبود مستمر خدمات

فعالیت‌ها و فرآیندهای کلیدی

CSIسه فرایند کلیدی برای پیاده‌سازی مستمر معرفی می‌کند، فرایند بهبود ۷ گامی، سنجش خدمت و گزارش خدمت.

فرایند بهبود ۷ گامی

فرایند بهبود ۷ گامی مراحل موردنیاز برای جمع‌آوری داده‌های معنی‌دار، تحلیل این داده‌ها برای شناسایی روند و مشکلات، ارائه اطلاعات برای مدیریت و اولویت‌بندی آن‌ها و توافق رو آن‌ها و پیاده‌سازی بهبودها را پوشش می‌دهد.



فرایند بهبود مستمر ۷ گامی

هر گام متأثر از اهداف استراتژیک، تاکتیکی و عملیاتی تعریف‌شده در استراتژی خدمت و طراحی خدمت است.

گام ۱ – آنچه باید سنجش شود

می‌بایست مجموعه‌ای از اندازه‌گیری‌ها تعریف شود که به‌طور کامل اهداف سازمانی را پشتیبانی نماید. می‌بایست تمرکز روی تعریف آنچه برای دستیابی کامل اهداف نیاز است، باشد صرف‌نظر از اینکه آیا در حال حاضر داده‌ها در دسترس هستند.

ممکن است سازمان‌ها دریابند که محدودیت‌هایی در آنچه واقعاً می‌توانند سنجش کنند دارند، اما تشخیص این فاصله‌های موجود و مخاطراتی که ممکنات منتج به آن شوند بسیار مفید خواهد بود.

گام 2 – آنچه باید تحلیل شود

تحلیل فاصله باید بین آنچه امروز سنجش شده یا می‌توان سنجش کرد و آنچه به‌طور ایدئال به آن نیاز است، انجام شود. این فاصله‌ها و پیامدها می‌تواند متعاقباً به کسب‌وکار، مشتریان و مدیر فناوری اطلاعات گزارش داده شود. ممکن است ابزارها و سفارشی‌سازی‌های جدید در برخی مراحل نیاز باشد.

گام ۳ – گردآوری داده

این مرحله جمع‌آوری و نظارت بر داده را پوشش می‌دهد. ترکیبی از ابزارهای نظارت و فرایندهای دستی می‌بایست به‌منظور جمع‌آوری داده‌های موردنیاز برای سنجش‌های تعریف‌شده، به کار گرفته شوند.

کیفیت، هدف کلیدی نظارت برای CSI است؛ بنابراین نظارت روی اثربخشی خدمت، فرایند، ابزار، سازمان یا بخش‌های پیکربندی (CI) دارد. تأکید روی شناسایی بهبودهایی است که می‌تواند برای سطح خدمت موجود یا عملکرد فناوری اطلاعات، به‌طور عمومی به‌وسیله تشخیص استثناها و راه‌حل‌ها، اجرا شود.

CSIنه‌تنها در استثنائات وارد می‌شود. اگر یک توافقنامه سطح خدمت به‌صورت مداوم اضافه ارائه داشته باشد، CSIدر تعیین سطح عملکردی که با کمترین هزینه به ثبات برسد یا نیاز به ارتقا تا ارائه عملکرد بهتر، وارد می‌شود.

گام ۴ – پردازش داده

داده‌های خام به فرمت موردنیاز پردازش می‌شود، به‌طورمعمول تهیه یک دیدگاه انتها به انتها از عملکرد خدمات و یا فرایندها.

پردازش داده یک فعالیت مهم CSI است که اغلب نادیده گرفته می‌شود. درحالی‌که نظارت و جمع‌آوری داده روی یک جزء زیرساختی منفرد مهم است، نکته کلیدی درک این موضوع است که اجزا، روی خدمت فناوری اطلاعات زیرساخت بزرگ‌تر تأثیرگذارند.

گام ۵ – تحلیل داده

تحلیل داده، اطلاعات را به دانش- از رویدادهای تأثیرگذار بر سازمان-تبدیل می‌کند.

هنگامی‌که داده به اطلاعات پردازش می‌شود، نتایج می‌توانند به‌منظور پاسخ به سؤالات زیر تحلیل شوند:

- آیا به اهداف رسیده‌ایم؟
- آیا روندهای واضحی وجود دارد؟
- آیا اقدامات اصلاحی نیاز است؟ هزینه آن چقدر است؟

گام ۶ – ارائه و استفاده از اطلاعات

حالا دستاورد این دانش می‌تواند در فرمتی که فهمش ساده است ارائه شود و به کسانی که اطلاعات را دریافت می‌کنند اجازه می‌دهد تصمیمات استراتژیک، تاکتیکی و عملیاتی اتخاذ کنند. لازم است اطلاعات در سطح درست و راه درست برای مخاطبان در نظر گرفته شده، ارائه شود. این گام می‌بایست ارزش ارائه کند، توجه به استثنائات برای خدمت و برجسته کردن تمامی منافعی که طی یک دوره زمانی شناسایی‌شده اند.

در حال حاضر فناوری اطلاعات می‌بایست بیش از پیش زمان برای فهم اهداف کسب‌وکار و ترجمه معیارهای فناوری اطلاعات به‌منظور بازگرداندن یک اثر در برابر این اهداف صرف نماید.

اگرچه بیشتر گزارش‌ها بر تمرکز روی عملکرد ضعیف متمایل‌اند، اخبار خوب نیز می‌بایست گزارش شوند. یک گزارش که روندهای بهبود رانشان دهد بهترین حامل بازاریابی خدمات فناوری اطلاعات است.

گام ۷ – پیاده‌سازی اقدام اصلاحی

دستاورد این دانش برای بهینه‌سازی، بهبود و اصلاح خدمات، فرایندها و تمامی دیگر فعالیت‌ها و تکنولوژی‌ها کاربرد دارد. اقدامات اصلاحی که برای بهبود خدمت نیاز هستند می‌بایست به سازمان شناسانده و ابلاغ شوند.

CSIبسیاری از فرصت‌های بهبود را شناسایی خواهد کرد و یک سازمان نیاز خواهد داشت اولویت‌های خود را بر اساس اهداف و منابع و سرمایه‌های در دسترسش تعیین نماید.

چهار دلیل اساسی برای نظارت و سنجش وجود دارد:

- تصدیق تصمیمات اتخاذشده قبلی.
- هدایت فعالیت‌ها به‌منظور دستیابی به اهداف تعیین‌شده. این شایع‌ترین دلیل برای نظارت و سنجش است.
- توجیه اینکه یک دوره از اقدامات موردنیاز است، با دلیل و مشاهده واقعی.
- مداخله در مقطع مناسب و انجام اقدام اصلاحی.

نظارت و سنجش CSI و فرایند بهبود ۷ گامی را پایه‌ریزی می‌کند و یک قسمت ضروری آن توانمندسازی به‌منظور مدیریت خدمات و فرایندها بوده و ارزش را به کسب‌وکار ارائه می‌کند.

سه نوع معیار وجود دارد که یک سازمان برای جمع‌آوری به‌منظور پشتیبانی فعالیت‌های CSI همچنین دیگر فعالیت‌های فرایند نیاز دارد.

- معیارهای تکنولوژیکی: اغلب همراه با اجزا و برنامه‌های کاربردی بر اساس معیارهایی مانند کارایی، دسترس‌پذیری
- معیارهای فرایندی: در قالب عوامل اصلی موفقیت (CSFs) و شاخص‌های کلیدی عملکرد (KPIs) گنجانده‌شده‌اند.
- معیارهای خدمت: نتایج خدمت انتها به انتها.

معیارهای اجزا/تکنولوژیکی برای محاسبه معیارهای خدمت استفاده می‌شوند.

لازم است یک چارچوب سنجش خدمت یکپارچه به اجرا گذاشته شود تا معیارها و داده‌های خام موردنیاز را تعریف و جمع‌آوری نماید و گزارش دهی و تفسیر از داده را پشتیبانی کند.

گزارش خدمات

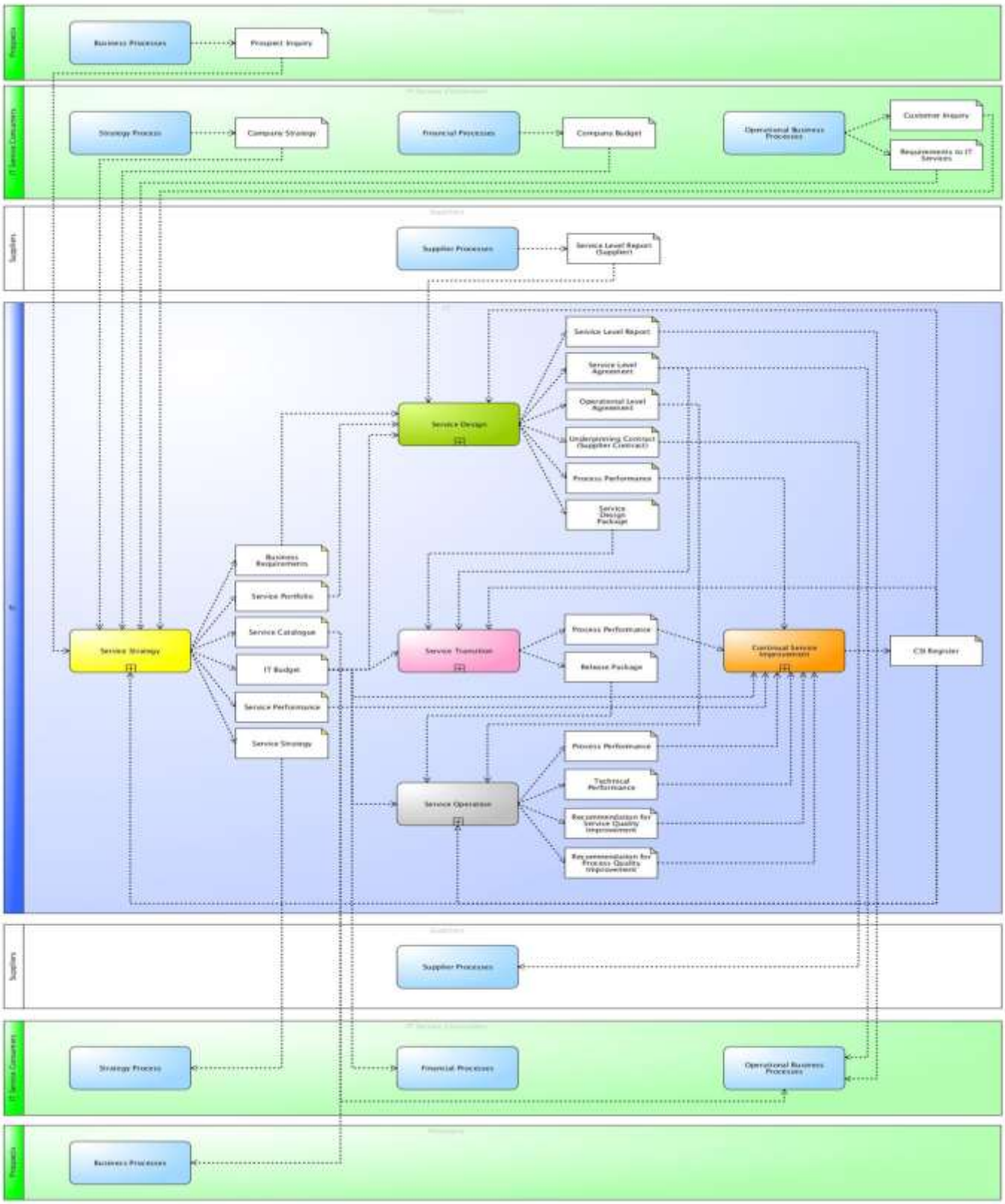
مقدار قابل‌توجه ای از داده در تحویل روزانه خدمت کیفی به کسب‌وکار توسط فناوری اطلاعات تطبیق و نظارت می‌شود، اما فقط زیرمجموعه کوچکی موردعلاقه و دارای اهمیت واقعی برای کسب‌وکار است. کسب‌وکار علاقه‌مند به دیدن نمایشی از پیشینه عملکرد دوره گذشته است تا تجاربش را به تصویر بکشد، اما بیشتر با رویدادهایی سروکار دارند که در ادامه به تهدید بدل شوند و چطور فناوری اطلاعات قصد کاهش این تهدیدات را دارد.

ارائه گزارش‌هایی مبنی بر نمایش پایبندی به SLA کفایت نمی‌کند. فناوری اطلاعات نیاز دارد یک روش قابل‌اجرا برای گزارش دهی بسازد، به‌عنوان‌مثال چه اتفاق رخ‌داده است، فناوری اطلاعات چه‌کار انجام داده، چگونه فناوری اطلاعات عدم تأثیر آن را تضمین خواهد کرد و فناوری اطلاعات چگونه برای بهبود عمومی ارائه خدمت عمل می‌کند.

مشخصات گزارشی که روی آینده به همان شدت گذشته تمرکز می‌کند مفاهیمی برای فناوری اطلاعات به بازار ارائه می‌دهد که پیشنهادهایش به‌درستی با تجارب مثبت و منفی کسب‌وکار منطبق شده است.

مسئولیت‌ها و نقش‌های کلیدی

مادامی‌که مدیر CSI مسئول تمامی فعالیت‌های CSI در یک سازمان است، بیشتر جزئیات بهبود مرتبط با کار در هر یک از مراحل، فرایندها و فعالیت‌های چرخه عمر پیش برده شده است.


Business Processes
Prospect Inquiry
Strategy Process
Company Strategy
Financial Processes
Company Budget
Operational Business Processes
Customer Inquiry
Requirements for IT Services
Supplier
Supplier Processes
Service Level Report (Supplier)
IT
Service Level Report
Service Level Agreement
Operational Level Agreement
Underpinning Contract (Supplier Contract)
Process Performance
Service Design Package
Service Design
Business Requirements
Service Portfolio
Service Catalogue
IT Budget
Service Performance
Service Strategy
Service Strategy
Service Transition
Process Performance
Release Package
Continual Service Improvement
CSI Register
Process Performance
Technical Performance
Recommendation for Service Quality Improvement
Recommendation for Process Quality Improvement
Service Operation
Supplier
Supplier Processes
IT Service Consumers
Strategy Process
Financial Processes
Operational Business Processes
Prospects
Business Processes

2.2.6 مراجع

1- **کتاب** *ITIL® v3 Foundation Study Guide* ***از شرکت*** *taruu* ***(****www.taruu.com****)***

2- https://www.danapardaz.net/site/itil-introduction
3- https://www.axelos.com/best-practice-solutions/itil
4- https://taksasystem.com/solutions/itil
5- https://servicedesk.medanet.ir/servicedesk-training/itil/
6- https://wiki.en.it-processmaps.com/index.php/History_of_ITIL
7- http://blog.armandar.com/post/itil-4-zero-to-100
8- https://taksasystem.com/solutions/itil
9- https://www.sysaid.com/resources/what-is-itsm
10- https://advisera.com/20000academy/knowledgebase/itsm-standards-and-frameworks/
11- https://www.motadata.com/fa/blog/what-is-itsm/
12- https://www.certguidance.com/problem-management-itil-itsm/

3 چرخه مدیریت عملکرد فرآیند ها

3.1 مدیریت رخداد در ITIL

مدیریت رخداد (Incident management) معمولا همراستا با Service Desk می‌باشد service desk) تنها نقطه تماس برای همه کاربرانی است که با IT در ارتباط هستند). آنچه در هنگام مختل شدن سرویس یا عدم ارائه عملکرد توافق شده از سرویس در ساعات نرمال سرویس دهی ضرورت دارد، بازگرداندن مجدد سرویس به عملکرد نرمال در سریعترین زمان ممکن است. همچنین هر شرایطی که احتمال اختلال یا خرابی سرویس در آن وجود دارد باید با ایجاد یک پاسخ به موقع، مانع از وقوع قطعی خرابی شود. این موارد، اهداف مدیریت رخداد هستند.

پرسنل Service desk معمولا به عنوان پشتیبانی سطح یک که شامل فعالیت‌های زیر است، شناخته می‌شوند:

- شناسایی رخداد(Incident identification)
- ثبت رخداد(Incident logging)
- دسته بندی رخداد(Incident categorization)
- اولویت بندی رخداد(Incident prioritization)
- تشخیص اولیه(Initial diagnosis)
- ارجاع به پشتیبانی سطح دوم (در صورت لزوم)
- برطرف کردن رخداد(Incident resolution)
- بستن رخداد(Incident closure)
- برقراری ارتباط با عموم کاربران در طول حیات رخداد

چرخه حیات فرآیند های یک خدمت در فناوری اطلاعات وارتباطات

لیست کامل 25 فرایند ITIL

مطالب زیادی در خصوص مراحل چرخه ی حیات یک خدمت در فناوری اطلاعات و ارتباطات در سایت ها موجود است که البته کمتر به ریز فرایندهای هر مرحله پرداخته شده و بی تردید می دانید که در برخی از نرم افزار های مدیریت خدمات یا سرویس دسک تعداد پشتیبانی از این فرایند به یک معیار انتخاب نرم افزار سرویس دسک مبدل شده برخی از انها 23 فرایند برخی 14 برخی 8 و مابقی 1 الی 3 فرایند را پشتیبانی میکنند اساسا نرم افزارهایی که ماهیت هلپ دسک رادارند حداثر یک فرایند و آن هم مدیریت رخداد را ساپورت میکنند بنابر این در انتخاب ابزار پیاده سازی ITIL دقت کنید.

هدف :مدیریت حادثه قصد دارد چرخه عمر همه حوادث (برنامه‌ریزی نشده و یا کاهش کیفیت خدمات IT را مدیریت کند .هدف اولیه این فرآیند ITIL برگرداندن خدمات IT به کاربران به سریع‌ترین شکل ممکن است.

در نسخه 9 سرویس دسک پلاس از 10 فرایند اصلی مدیریت رخداد ، مدیریت مشکل، مدیریت تغییر، مدیریت دارایی یا CMDB بهمراه سایر فرایندهای ارتباط کسب و کار ، مدیریت مالی، کاتالوگ خدمات، مدیریت دانش،مدیریت سطح ارائه خدمات و همچنین مدیریت انتشار نیز استفاده می شود و مابقی فرایندها نظیر مدیریت رخداد ، مدیریت دسترسی ، و... در سایرمحصولات manageenine نظیر Opmanager-Admanager-ADaudit و... که همگی امکان ادغام با سرویس دسک پلاس رادارند استفاده میگردد.

در این بحث سعی شده تا به دقت تمامی فرایند های ITIL نسخه 3 را به تفکیکو به ترتیب ذکر نماییم:

ITIL نسخه 3 دارای 5 مرحله اصلی است که این مراحل ، چرخه حیات یک سرویس IT را مشخص میکند:

1.استراتژی خدمات ITIL

2.طراحی خدمات ITIL

3.انتقال خدمات ITIL

4.عملیات سرویس ITIL

5.بهبود خدمات مداوم خدمات ITIL

در تمامی این مراحل مجموعه 25 فرایند برای مدیریت خدمات ارائه شده بنابراین ITIL دارای 25 فرایند اصلی است که در بسیاری از نرم افزارها و سیستم های مدیریت خدمات فناوری یا ITSM بکار رفته است که به شرح زیر است:

استراتژی خدمت

1.مدیریت استراتژی برای خدمات فناوری اطلاعات

2.خدمات مدیریت نمونه کارها

3.مدیریت مالی خدمات فناوری اطلاعات

4.مدیریت تقاضا

5.مدیریت ارتباط کسب و کار

طراحی خدمت

6.هماهنگی طراحی

7.کاتالوگ خدمات

8.مدیریت سطح خدمات

9.مدیریت ظرفیت

10.مدیریت تداوم خدمات (TSCM)

11.سیستم مدیریت امنیت اطلاعات

12.مدیریت تامین کننده

13. مدیریت دسترسی

انتقال خدمت

14.برنامه ریزی و پشتیبانی انتقال

15.مدیریت تغییر

16.مدیریت خدکات و مدیریت پیکر بندی

17.مدیریت انتشار و استقرار

18.اعتبار سنجی و تست سرویس
19.تغییر ارزیابی
20.مدیریت دانش

عملیات خدمت

21.مدیریت رویداد
22.مدیریت حوادث
23.تکمیل درخواست
24.مدیریت مشکل
25.مدیریت دسترسی

فرایندهای دیگر

موارد زیر به عنوان توابع توسط ITIL ذکر شده است(با این حال انها معمولا به فرایندهای قبلی ارجاع داده می شوند):

26.میز خدمات
27.مدیریت برنامه

وظیفه مدیریت رخداد، تحلیل ریشه اصلی مشکل و شناسایی علت وقوع رخداد نمی‌باشد. بلکه تمرکز آن بر روی انجام فعالیت های لازم جهت بازگرداندن سرویس است. این کار نیازمند استفاده از یک راه حل یا اصلاح موقت است. یک ابزار مهم برای تشخیص رخدادها، پایگاه داده خطاهای شناخته شده (KEDB) است که توسط مدیریت مشکل (problem management) نگهداری می‌شود KEDB .هرگونه خطای شناخته شده یا مشکلی که منجر به وقوع رخدادها در گذشته شده است را شناسایی کرده و اطلاعاتی در خصوص راه حل های شناسایی شده ارائه می‌کند.

ابزار دیگری که توسط مدیریت رخداد مورد استفاده قرار می‌گیرد، مدل رخداد (incident model)نام دارد. رخدادهای جدید اغلب شبیه رخدادهایی هستند که در گذشته اتفاق افتاده است. یک مدل رخداد به تعریف موارد زیر می‌پردازد.

- مراحلی که باید برای کنترل و مدیریت رخداد انجام شود، ترتیب مراحل و مسئولیت‌ها.
- اقدامات پیشگیرانه ای که قبل از برطرف کردن رخداد باید انجام شود.
- بازه زمانی جهت برطرف ساختن رخداد
- روال‌های ارجاع به مرجع بالاتر(Escalation procedures)
- نگهداری و محافظت از اسناد

مدل رخداد، فرآیند را ساده کرده و ریسک را کاهش می‌دهد Incident management .وابستگی و ارتباط نزدیکی با سایر فرآیندهای مدیریت سرویس دارد .این فرآیندها عبارتند از:

- مدیریت تغییر .(Change Management) برطرف کردن یک رخداد ممکن است نیازمند ایجاد یک درخواست تغییر باشد. همچنین، از آنجا که درصد زیادی از رخدادها ناشی از اجرای تغییرات هستند، تعداد رخدادهای ناشی از تغییر به عنوان شاخص کلیدی عملکرد (KPI) برای مدیریت درنظر گرفته می‌شود.
- مدیریت مشکل .(Problem management) همانطور که پیش تر به آن پرداخته شد، مدیریت رخداد از یک KEDB که توسط مدیریت مشکل نگهداری می‌شود، استفاده می‌کند Problem management .نیز جهت انجام مسئولیت‌های خود در راستای تشخیص خطاها و مشکلات به مجموعه کامل و دقیقی از داده های رخدادها نیاز است.
- مدیریت پیکربندی و دارایی سرویس .CMS (Service asset and configuration management) یک ابزار مهم و ضروری برای رفع رخداد است زیرا ارتباطات بین اجزاء سرویس را شناسایی کرده و همچنین امکان یکپارچه سازی داده های پیکربندی را با داده های مشکلات و رخدادها فراهم می‌سازد.

- مدیریت سطح سرویس .(Service level management) نقض سطح خدمات به خودی خود یک رخداد بوده و عاملی برای فرآیند مدیریت سطح سرویس است. همچنین توافق نامه های سطح سرویس (SLAs) ممکن است روش‌های زمانبندی و ارجاع به مراحل بالاتر را برای انواع مختلفی از رخدادها تعریف کنند.

ITIL، رخداد را یک وقفه پیش بینی نشده یا کاهش کیفیت سرویس IT تعریف می‌کند. توافق نامه سطح سرویس نیز به تعریف سطح سرویس توافق شده بین سرویس دهنده و مشتری می‌پردازد.

رخدادها با درخواست‌ها و مشکلات تفاوت دارند. رخداد، باعث قطع شدن سرویس‌های نرمال می‌شود. مشکل به وضعیتی گفته می‌شود که بواسطه یکسری رخدادهای متعدد با علائم مشابه شناسایی می‌شود Problem management .ریشه مشکل را شناسایی و رفع می‌کند Incident management .سرویس‌های IT را به حالت نرمال برمی‌گرداند. درخواست‌های اجرا جزو درخواست‌های رسمی بوده که ارائه کننده مواردی از قبیل آموزش، اطلاعات حساب، سخت افزار جدید، تخصیص مجوز و هر آنچه که IT service desk ارائه می‌کند، می‌بلشند. یک درخواست ممکن است قبل از اجرا به تاییدیه نیاز داشته باشد.

رخدادها عملکرد نرمال سرویس را مختل می‌کنند، مانند زمانی که کامپیوتر یک کاربر خراب می‌شود، یا زمانی که اتصال VPN برقرار نمی‌شود و یا زمانی که پرینتر از کار می افتد. اینها وقایع غیر منتظره ای هستند که نیازمند رسیدگی از جانب سرویس دهنده بوده تا مجددا به حالت نرمال خود بازگردانده شوند.

هنگامی که اکثر مردم درباره فناوری اطلاعات فکر می کنند، مدیریت رخداد فرایندی است که معمولا به ذهن آنها می‌رسد. این فرآیند تنها بر مدیریت و ارجاع رخداد به سطوح بالاتر و بازگرداندن سرویس به سطوح تعریف شده تمرکز دارد Incident . managementبا تحلیل علل بوجود آورنده رخداد و یا حل مشکلات سر و کار ندارد. هدف اصلی آن دریافت رخدادهای گزارش شده کاربران و رفع آنها و در نهایت بستن این رخدادها است. مدیریت رخداد مؤثر، ارزش مداوم برای کسب و کار ایجاد می‌کند. بعلاوه این امکان را فراهم می‌اورد تا رخدادها در بازه زمانی پیش بینی نشده برطرف شوند. برای اکثر سازمان ها، این فرایند از رفت و برگشت ایمیل‌ها به یک سیستم تیکتینگ رسمی با اولویت بندی، طبقه بندی و الزامات SLA پشتیبانی می‌کند. ایجاد ساختارهای رسمی زمانبر است اما خروجی بهتری برای کاربران، تیم پشتیبانی و کسب و کار دارد. داده های جمع آوری شده از پیگیری رخدادها به مدیریت بهتر مشکلات و تصمیم گیری های کسب و کار کمک می‌کند. ایجاد مدل‌های رخداد نیز در مدیریت رخداد انجام شده و به کارکنان پشتیبانی کمک می‌کند تا بصورت کارامد مشکلات و مسائل تکراری را برطرف نمایند. این مدل‌ها به کارکنان پشتبانی امکان می‌دهند تا رخدادها را از طریق فرآیندهای تعریف شده برای کنترل رخدادها به سرعت رفع کنند. در برخی سازمان‌ها، یک تیم اختصاصی برای مدیریت رخداد در نظر گرفته شده است. در اکثر کسب و کارها، این وظیفه به service deskو صاحبان آن، مدیران و سهامداران واگذار می شود. در دسترس بودن مدیریت رخداد، پیاده سازی و پشتیبانی از آن را آسان کرده است، زیرا ارزش آن برای کاربران در تمام سطوح سازمان آشکار است. هر فردی با مسائل و مشکلاتی روبه رو می‌شود که برای حل و رسیدگی سریع به آنها ، به دانش و مهارت تیم پشتیبانی نیاز دارد.

مدیریت مؤثر رخدادها به چندین بخش کلیدی نیاز دارد:

1. توافق نامه سطح سرویس بین سرویس دهنده و مشتری که اولویت‌ها، مسیرهای ارجاع و مدت زمان پاسخ و رفع رخداد را تعریف می‌کند.
2. مدل‌های رخداد یا الگوها که قادر است رخدادها را بطور مؤثر رفع کند.
3. دسته بندی انواع رخدادها برای جمع آوری بهتر داده ها و مدیریت مشکلات
4. توافق بر اولویت‌ها، دسته بندی ها و وضعیت‌های رخدادها
5. ایجاد یک فرآیند اصلی پاسخگویی به رخداد
6. توافق بر تخصیص نقش مدیریت رخداد

مورد شماره پنج در مدیریت رخداد اهمیت ویژه ای دارد. مدیر رخداد مسئول رسیدگی به رخدادهایی است که نمی توانند در قالب SLAهای توافق شده برطرف شوند، مانند مواردی که service desk قادر به برطرف کردن آنها نمی‌باشد .مدیر رخداد در بسیاری از سازمان‌ها ممکن است مدیر عملیات IT یا سرپرست فنی ITباشد.

عملکرد اصلی مدیریت رخدادThe service desk :

مدیریت رخداد چندین زیرمجموعه دارد. مهم ترین زیرمجموعه مدیریت رخداد، service deskاست Service desk .با نام help deskنیز شناخته می‌شود Service desk .تنها نقطه تماس برای کاربران جهت گزارش رخدادها است. بدون وجود service deskکاربران بدون هیچ گونه محدودیتی در ساختار یا اولویت‌ها، با تیم پشتبانی تماس می‌گیرند. این بدین معناست که ممکن است هنگامیکه تیم پشتیبانی در حال رسیدگی به رخدادی با اولویت پایین است، رخدادهای با اولویت بالا نادیده گرفته شوند. رخدادهایی که اولویت پایینی دارند مانند تعمیر ایستگاه dickingنامناسب که ممکن است چند هفته حل نشده باقی بماند زیرا کارکنان پشتیبانی IT در حال رسیدگی به مسائل مهمی هستند که در آن زمان به آنها داده شده است. ساختار service deskامکانی فراهم می آورد تا تیم پشتیبانی با سرعت به مشکلات همه رسیدگی کند، مدل‌های سلف- سرویس ایجاد کند، روند داده های It را جمع آوری کند، انتقال دانش بین کارکنان پشتیبانی را افزایش دهد و از problem management پشتیبانی کند.

Service deskبه دو لایه پشتیبانی تقسیم می‌شود. لایه اول برای مسائل و مشکلات اساسی است، مانند بازنشانی رمز عبور و عیب یابی های اصلی کامپیوتر .رخدادهای لایه اول غالبا به مدل‌های رخداد تبدیل می‌شوند، زیرا الگوهای ایجاد آنها ساده بوده و این رخدادها اغلب رخ می‌دهند. به عنوان مثال، یک مدل الگو برای بازنشانی رمز عبور، شامل دسته بندی رخداد (دسته "حساب" و نوع "Reset Password"، برای مثال)، الگویی از اطلاعاتی است که کارکنان پشتیبانی انها را تکمیل کرده (مانند نام کاربری و تاییدیه) و به مقالات پایگاه دانش داخلی و خارجی جهت پشتیبانی از رخداد، پیوست می‌کنند. رخدادهای لایه اولی که اولویت پایینی دارند در هیچ شرایطی بر روی کسب و کار اثر نداشته و می‌توانند توسط کاربران برطرف شوند.

لایه دوم مربوط به مسائل و مشکلاتی است که به مهارت، آموزش یا دسترسی بیشتری نیاز دارند. برای مثال ممکن است بازنشانی RSA tokenنیازمند ارجاع به لایه دوم است. برخی سازمان‌ها رخدادهایی که توسط VIP ها گزارش شده اند را به عنوان رخداد لایه دومی درنظر می‌گیرند تا کیفیت بالاتری از خدمات را برای این کارکنان فراهم کنند. رخدادهای لایه دوم ممکن است مسائل و مشکلاتی با اولویت متوسط باشند که نیازمند پاسخ سریع از service desk هستند.

تخصیص درست لایه ها و اولویت بندی ها زمانی صورت می‌گیرد که اکثر رخدادها به لایه اول / اولویت پایین، برخی رخدادها به لایه دوم و تعداد کمی از رخدادها به لایه سوم انتقال یابند. رخدادهایی که نیاز به تشدید فوری دارند، به عنوان رخدادهای اصلی در نظر گرفته شده و میبایست با مشارکت کل تیم پاسخ داده شوند. رخدادهای اصلی در ITIL به رخدادهایی گفته می‌شود که نشان دهنده اختلالات عمده در کسب و کار هستند. این رخدادها همیشه اولویت بالایی دارند و به سرعت توسط service desk و کارکنان سطوح بالاتر پاسخ داده می‌شوند. این رخدادها در ساختار پشتیبانی لایه ای، سومین لایه محسوب می‌شوند و برای problem managementگزینه های مناسبی هستند.

فرآیند رخداد

درITIL ، رخدادها از یک جریان کاری ساختاریافته عبور کرده و بهترین نتایج و کارایی را برای سرویس دهندگان و مشتریان به ارمغان می آورند. بر اساس توصیه های ITIL ، فرآیند مدیریت رخداد مراحل زیر را در بر می‌گیرد:

- شناسایی رخداد
- ثبت رخداد
- دسته بندی رخداد
- اولویت بندی رخداد

- پاسخ رخداد
- تشخیص اولیه
- ارجاع رخداد به سطوح بالاتر
- تحقیق و تشخیص
- اجرا و بازیابی
- بستن رخداد

فرآیند رخداد امکان کنترل بهتر رخداد را فراهم کرده و بهبود مستمر سرویس را تضمین می‌کند.

اولین مرحله در زمان حیات رخداد، شناسایی رخداد است. رخدادها از جانب کاربران و به شیوه مجاز سازمان، ایجاد می‌شوند.

.منابع گزارش های رخداد عبارتند از پاکسازی، خدماتself-service ، تماس های تلفنی، ایمیل‌ها، گفتگوهای پشتیبانی و اخطارهای خودکار مانند نرم افزار مانیتورینگ شبکه یا ابزارهای پویش سیستم. در گام بعدی، service deskدر خصوص اینکه مساله بوجود آمده آیا واقعا یک رخداد است یا یک درخواست، تصمیم گیری می‌کند. طبقه بندی و کنترل درخواست‌ها با رخدادها متفاوت بوده و رخدادها زیرمجموعه ای از درخواست‌ها هستند.

پس از شناسایی رخداد، service deskرخداد را به عنوان یک درخواست ثبت می‌کند. این درخواست باید شامل اطلاعاتی همچون نام کاربری و اطلاعات تماس، شرح رخداد و زمان و تاریخ گزارش رخداد) برای انطباق با (SLA باشد. همچنین فرآیند ثبت (logging process) شامل دسته بندی،اولویت بندی و مراحلی است که service deskآنها را تکمیل می‌کند.

دسته بندی رخدادها یک مرحله مهم و ضروری در فرآیند مدیریت رخداد است .دسته بندی شامل تخصیص یک دسته و حداقل یک زیر شاخه به رخداد است. این عمل چندین هدف را دنبال می‌کند. نخست به service desk امکان می‌دهد تا رخدادها را بر اساس دسته بندی و زیرشاخه های آنها، مرتب و مدل سازی کند. همچنین امکان اولویت بندی خودکار برخی رخدادها را فراهم می آورد. برای مثال، یک رخداد ممکن است در دسته بندی "شبکه" با زیر شاخه "قطعی شبکه" قرار گیرد .این دسته بندی در برخی سازمان‌ها به عنوان یک رخداد با اولویت بالا در نظر گرفته می‌شود که نیاز به یک پاسخ سریع دارد. هدف سوم فراهم سازی امکان پیگیری دقیق رخدادها می‌باشد. هنگامیکه رخدادها دسته بندی می‌شوند، الگوها شکل می‌گیرند. به آسانی می‌توان اندازه گیری کرد که رخدادهای خاص هر چند وقت یکبار رخ می‌دهند و بر اساس روند وقوع رخدادها، بخش هایی را که به آموزش یا problem managementدارند، مشخص نمود. برای مثال، هنگامیکه مدیر ارشد مالی اطلاعات کافی برای تصمیم گیری در خصوص محصول جدید سخت افزاری داشته باشد، به سادگی برای خرید محصول متقاعد خواهد شد.

اولویت بندی رخدادها برای تبعیت از مواردی که در توافق نامه سطح سرویس لحاظ شده، بسیار اهمیت دارد. اولویت یک رخداد بر اساس میزان تاثیر آن بر کاربران و کسب و کار و همچنین فوریت آن، تعیین می‌شود. فوریت بدین معناست که درخواست با چه سرعتی انجام شود. سطح تاثیر به معنای اندازه گیری میزان آسیب‌های احتمالی است که یک رخداد ممکن است وارد کند.

1. رخدادهای با اولویت پایین به رخدادهایی گفته می‌شود که در عملکرد کاربران و شرکت خللی وارد نکرده و قابل سازماندهی هستند.
2. رخدادهای با اولویت متوسط بر تعداد کمی از کارکنان تاثیر گذاشته و تا حدودی کار آنها را مختل می‌کنند. مشتریان نیز ممکن است کمی تحت تاثیر قرار گرفته و یا دچار مشکل شوند.
3. رخدادهای با اولویت بالا بر گستره وسیعی از کاربران یا مشتریان اثر گذاشته، کسب و کار را مختل کرده و ارائه سرویس را تحت تاثیر قرار می‌دهد .این رخدادها تقریبا همیشه بخش‌های مالی را نیز تحت تاثیر قرار می‌دهند.

پس از آنکه رخداد شناسایی، دسته بندی، اولویت بندی و ثبت گردید، service deskمی‌تواند رخداد را کنترل و برطرف کند. یک رخداد در پنج مرحله برطرف می‌شود:

شناسایی اولیه :(Initial Diagnosis) این اتفاق زمانی رخ می‌دهد که کاربر مشکل خود را شرح داده و سوالات عیب یابی (Troubleshooting)را پاسخ می‌دهد.

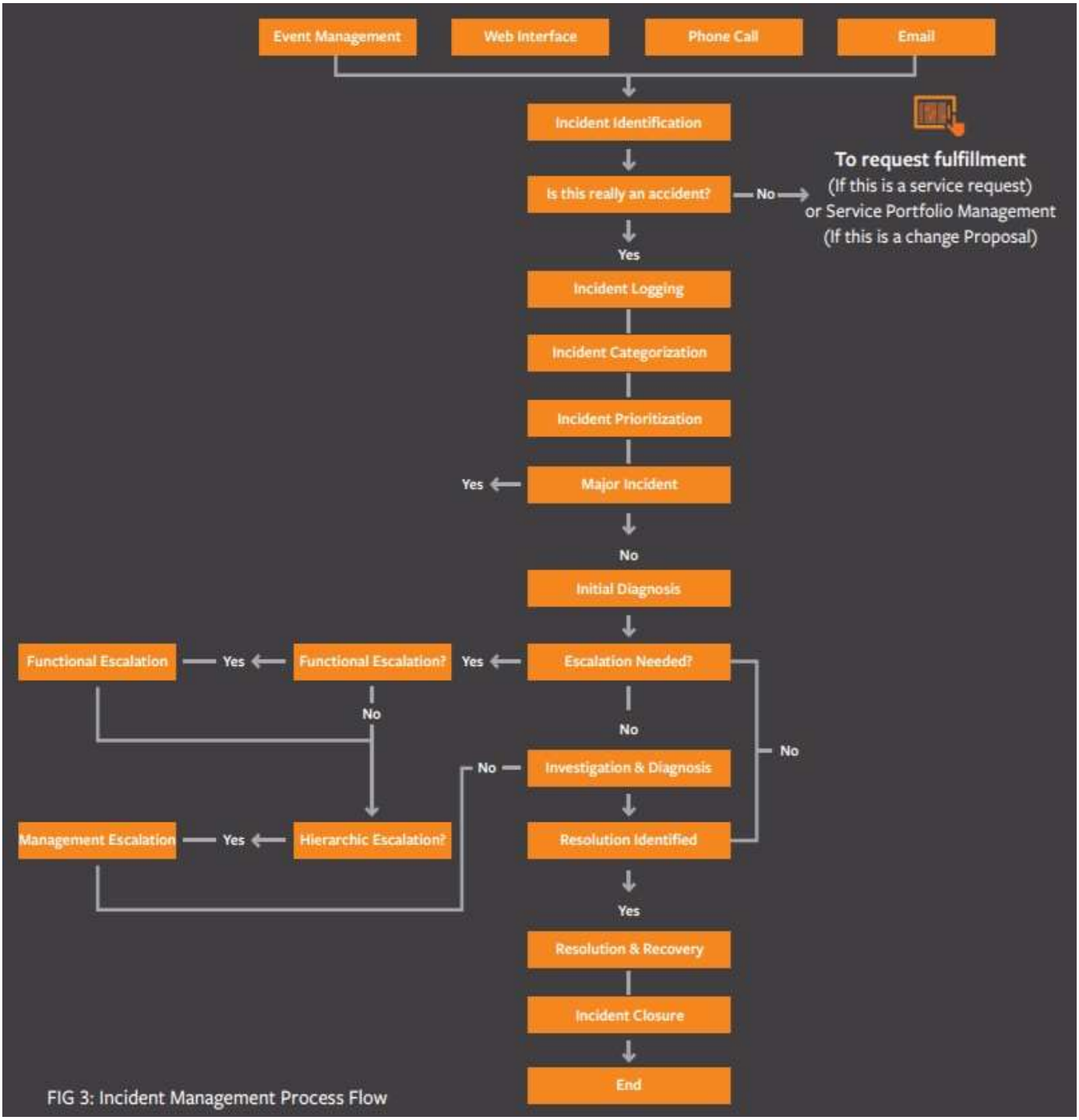
ارجاع رخداد به سطوح بالاتر :(Incident Escalation) این اتفاق زمانی رخ می‌دهد که یک رخداد به پشتیبانی حرفه ای نیاز داشته باشد، مانند اعزام کارشناس در محل یا درخواست کمک از کارکنان آموش دیده در بخش پشتیبانی .همانطور که پیش تر مطرح گردید، اکثر رخدادها باید توسط کارکنان پشتیبانی در لایه نخست برطرف شده و به لایه های بالاتر ارجاع داده نشوند.

بررسی و تشخیص :(Investigation and Diagnosis) این فرآیندها در طول عیب یابی و در زمانی که فرضیه اولیه رخداد صحیح باشد، رخ می‌دهند. بعد از آنکه رخداد تشخیص داده شد، کارکنان می‌توانند راه حل ارائه کنند، مانند تغییر تنظیمات نرم افزار، ارائه patch نرم افزار، یا سفارش سخت افزار جدید.

برطرف ساختن رخداد و بازیابی :(Resolution and Recovery) این کار زمانی انجام می‌شود که service desk تایید کند سرویس کاربر به سطح SLA مورد انتظار، بازیابی شده است.

بستن رخداد :(Incident Closure) در این مرحله رخداد بسته شده و فرآیند رخداد به پایان می‌رسد.

نمودار جریان فرآیند مدیریت رخداد(Incident management process flow diagram)



وضعیت‌های رخداد(Incident statuses)

وضعیت‌های رخداد نشان دهنده فرآیند رخداد هستند. این وضعیت‌ها عبارتند از:

- جدید(New)

- تخصیص یافته(Assigned)
- در جریان(In progress)
- در انتظار(On hold or pending)
- حل شده(Resolved)
- بسته(Closed)

وضعیت "جدید" نشان هنده آن است که service desk رخداد را دریافت کرده اما هنوز آن را به عوامل پشتیبانی تخصیص نداده است.

وضعیت "تخصیص یافته" نشان دهنده آن است که رخداد به یکی از کارکنان service desk تخصیص یافته است.

وضعیت "در جریان" نشان دهنده آن است که رخداد به یکی از عوامل پشتیبانی تخصیص داده شده اما برطرف نشده است.

وضعیت "در انتظار" نشان دهنده آن است که رخداد نیازمند اطلاعات یا پاسخی از سوی کاربر یا شخص ثالث دیگری است. هنگامیکه رخداد به وضعیت "در انتظار "می‌رود، مدت زمان مجاز پاسخ که در SLA تعریف شده تا زمانیکه پاسخی از سمت کاربر یا فروشنده دریافت نشود، ثابت باقی می‌ماند.

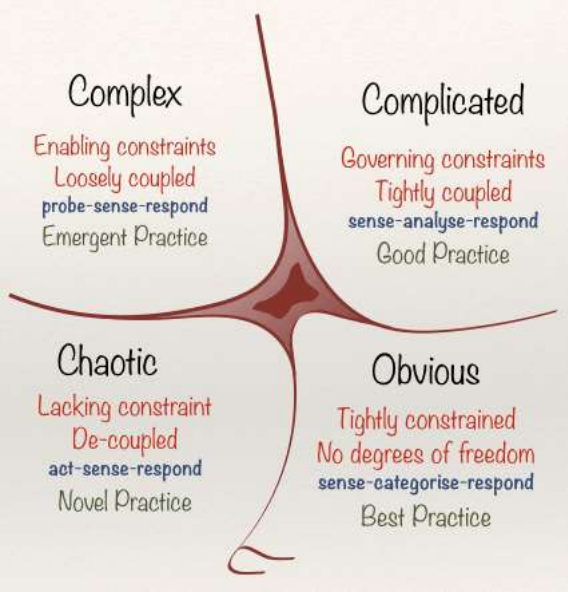
وضعیت "حل شده" بدین معناست که service desk تایید کند رخداد برطرف شده و سرویس کاربر به سطح توافق شده در SLAبازگشته است.

وضعیت "بسته" نشان دهنده آن است که رخداد برطرف شده است و هیچ اقدام دیگری نمی‌تواند انجام شود.

مدیریت رخداد، رخدادها را از طریق service desk دنبال کرده تا در جریان روند رخدادها در دسته بندی های انجام شده و همچنین زمان هر وضعیت قرار گیرد. آخرین بخش از مدیریت رخداد، ارزیابی اطلاعات جمع آوری شده است. داده های رخدادها به سازمان‌ها کمک می‌کند تا در خصوص بهبود کیفیت سرویس‌های ارائه شده تصمیم گیری کنند و حجم رخدادهای گزارش شده را کاهش دهند. مدیریت رخداد تنها یکی از فرآیندهای چارچوب service operation است.

مقایسه مدیریت ریسک و مدیریت رخداد/مشکل

تفاوت مهم میان مدیریت رخداد/مشکل و مدیریت ریسک، در جایگاه سازمانی آن ها است. مدیر مشکل معمولاً یک متخصص فنی است که قادر به حل مشکلات پیچیده ای که نیازمند تصمیمات مدیریتی هستند، نمی باشد. مدیریت صحیح ریسک از سطح هیئت مدیره آغاز شده و تمام سازمان را پوشش می دهد. ریسک های فناوری اطلاعات ممکن است برای کل سازمان مضر باشند و اگر صرفاً با دید فنی به آن ها نگاه شود؛ ممکن است این مضرات نادیده گرفته شوند.



در چارچوب کانِوین(Cynefin) ، فرآیندهای مدیریت رخداد و مشکل تنها در حوزه های Obvious و Complicated قابل بکارگیری هستند. مشکلات ساده را می توان دسته بندی نمود و راهکار شناخته شده ای برای آن ها وجود دارد. از سوی دیگر، مشکلات Complicated قابل دسته بندی نیستند، اما می توان از طریق تجزیه و تحلیل، آن ها را حل نمود. متأسفانه، بسیاری از مشکلات مهم در حوزه های Complex و Chaotic قرار دارند و راه حل آن ها عموماً نیازمند تصمیمات راهبردی و مدیریتی می باشد.

استاندارد ایزو 31000، منبع مناسبی برای مدیریت ریسک است. در این مقاله تنها بخش بسیار کوچکی از مدیریت ریسک ارائه شده و توصیه می شود تمام فعالان حوزه خدمات فناوری اطلاعات، این استاندارد را مطالعه کنند.

به زبان ساده می توان ITIL را یک استاندارد در حوزه IT دانست ، اما واقعیت این است که ITIL یک استاندارد نیست . در واقع ITILیک سری تجربه موفق (best practice) است که سازمان ها و شرکت های دولتی مرتبط با IT در دولت انگلستان ، برای مدیریت کارهایشان از آن استفاده می کنند، به زبان ساده می توان گفت که دولت انگلستان برای سازمان دهی فعالیت های مرتبط با IT ، یک سری Design Patter ارائه کرده که با انجام آنها شرکت ها و سازمان های حوزه IT می توانند بهتر به نتیجه برسند.

مزایای استفاده ازITIL

- شفاف سازی همه جانبه
- سازگاری با استاندارد ISO2000
- افزایش پایایی و توان عملیاتی خدمات
- (بهینه سازی استفاده از منابع IT) ، مالی ، نیروی انسانی، دانش فنی و...
- قابلیت اندازه گیری کیفیت خدمات
- بهبود کیفیت در برنامه ریزی ها ، فرهنگ استفاده از خدمات و برقراری نظم در امور
- مستقل از سکوهای عملیاتی

مدیریت رخدادها طبق استانداردITIL

مروری بر مدیریت رخداد - ITIL فرآیند ، نقش ها و مسئولیت ها

business همیشه برای دستیابی به مهارت و بهره وری بیشتر ، خدمات بی وقفه را هدف قرار می دهد. مدیریت رخداد اولین قدم است که توسط اکثر شرکتها برای دستیابی به بازیابی سریع مورد استفاده قرار می گیرد.

ITIL این رخداد را "یک وقفه ناخواسته در یک سرویس یا عدم موفقیت یک مؤلفه از یک سرویس که هنوز تأثیر آن را تحت تأثیر قرار نداده است" تعریف می کند. " علاوه بر این ، بیایید در مورد مدیریت حادثه ITIL و روند مرتبط ، نقش ها و مسئولیت های آن بحث کنیم.

درITIL ، به هر اختلال یا وقفه‌ای در عملکرد خدمت که ممکن است به اختلال در خدمت یا افت کیفیت آن منجر شود، رخداد (Incident)گفته می‌شود. موارد خطا و خرابیِ مؤلفه های خدمت که ممکن است در آینده به اختلال خدمت منجر شوند نیز رخداد تلقی می شوند. به مدیریت چرخه عمر رخدادها، از زمان اعلام یا شناسایی تا خاتمه‌ی آن، به نحوی که رخداد به سرعت حل و فصل شده و خدمت متأثر از آن بازیابی شود، نیز مدیریت رخداد می‌گویند.

کارکردهای مختلفی در مدیریت حوادث دخیل است و مهمترین آنها میز خدمات است. میز خدمات تنها نقطه تماس کاربران برای گزارش هرگونه حادثه است. بدون در دسترس بودن میز خدمات ، کاربران مجبورند بدون اولویت بندی با کارمندان پشتیبانی تماس بگیرند. این بدان معناست که کارکنان ممکن است با حادثه با اولویت پایین مشرف به حادثه دارای اولویت باشند .بنابراین ، داشتن یک میز خدمات ساخت یافته ، کارکنان پشتیبانی را قادر می سازد که به سرعت با همه مسائل رسیدگی کنند ، داده های IT را گردآوری کرده و از مدیریت مشکل به روشی کارآمد پشتیبانی کنند.

طبقه بندی استاندارد بر اساس اهمیت یک رویداد:

- **(*INFO*** *Informational*: **این رویداد نیازی به اقدام فوری ندارد و یک استثناء نیست. آنها در پرونده های ثبت شده ثبت می شوند و برای یک دوره از پیش تعیین شده نگهداری می شوند. از این نوع رویداد برای بررسی وضعیت دستگاه یا خدمات ، تأیید وضعیت فعالیت ، تولید آمار استفاده می شود (ورود کاربر ، کار دسته ای به پایان رسید ، روشن کردن دستگاه ، تعداد کاربرانی که در یک برنامه وارد شده اند)**
- **(WARN / ALERT)** Warning: **این رویداد هنگامی ایجاد می شود که یک دستگاه یا خدمات ، (برنامه / ابزار) ، به یک آستانه توافق شده (KPI) نزدیک می شوند. هشدارها برای اطلاع از گروه / فرآیند / ابزار به منظور انجام اقدامات لازم برای جلوگیری از وقوع استثناء در نظر گرفته شده است.**
- **(ERROR)** Exception: **به این معنی است که یک سرویس یا دستگاه در حال حاضر زیر پارامترهای / شاخصهای عادی (از پیش تعریف شده) کار می کند. این بدان معناست که سرویس تجاری تحت تأثیر قرار می گیرد و دستگاه یا خدمات یک خرابی ، تخریب عملکرد یا از بین رفتن عملکرد را نشان می دهند (سرور وب ، پوشش CS از بین رفته برای چندین سایت). خرابی دستگاه یک خطا است.**

مدیریت رخداد یا Incident Management در بخش Service Operation در چارچوب ITIL معرفی شده است. رخداد به هر اتفاقی گفته می‌شود که جزو کارهای عادی و استاندارد عملیات سازمان نبوده و ممکن است منجر به توقف در اجرای سرویس شده و یا کیفیت سرویس را کاهش دهد. برای درک بهتر مفهوم رخداد به مثال زیر توجه کنید:

آیا روشن نشدن کامپیوتر یک رخداد است؟ آیا وقتی مدیر فناوری اطلاعات از شما می‌خواهد تعداد رخدادهای ماه گذشته را به او اعلام کنید شما به سراغ آمار همه درخواستهای ماه گذشته می‌روید؟

جواب :روشن نشدن کامپیوتر می‌تواند رخداد باشد! چنانچه پس از بررسی کارشناس فناوری اطلاعات مشخص شد که دستگاه ایراد داشته (مثلا خرابی قطعه یا مشکل ویندوز) در این صورت یک رخداد اتفاق افتاده ولی چنانچه مشخص شود آن دستگاه به برق متصل نبوده این دیگر رخداد نیست بلکه اشکال کاربری می‌باشد.

آنچه که بیش از همه برای یک مدیر اهمیت دارد شناسایی رخدادها و بررسی علت آن است. مدیر می‌خواهد بداند چه تعداد درخواست ثبت شده و چند درصد از آنها رخداد بوده است. به عنوان مثال ممکن است گزارش نشان دهد که ماه گذشته تعداد

100درخواست ثبت شده و فقط 15 تا از آنها رخداد بوده است که این آمار خوبی است (البته به شرطی که زمان توقف زیاد نبوده باشد) یا برعکس ممکن است تعداد رخدادها زیاد باشد (در اینجا مدیر باید سریعا علت را ریشه‌یابی کند).

درITIL ، به هر اختلال یا وقفه‌ای در عملکرد خدمت که ممکن است به اختلال در خدمت یا افت کیفیت آن منجر شود، رخداد (Incident)گفته می‌شود. موارد خطا و خرابیِ مؤلفه های خدمت که ممکن است در آینده به اختلال خدمت منجر شوند نیز رخداد تلقی می شوند. به مدیریت چرخه عمر رخدادها، از زمان اعلام یا شناسایی تا خاتمه‌ی آن، به نحوی که رخداد به سرعت حل و فصل شده و خدمت متأثر از آن بازیابی شود، نیز مدیریت رخداد می‌گویند.

حل و فصل رخداد معادل واژه‌ی Resolveاست. هدف از حل و فصل رخداد، یافتن خطای نهفته‌ای نیست که منجر به وقوع رخداد شده، بلکه هدف آن است که به هر طریقی، حتی به کمک یک روش موقت، خدمت به سرعت بازیابی شود.

هر شخصی که به نوعی با خدمت در ارتباط است، می‌تواند اعلام‌کننده‌ی یک رخداد باشد، مانند کاربران، از طریق ابزارهای پایش، یا متخصصین فنی و...

در سازمان‌ها، در فرآیند مدیریت رخداد، معمولاً واحد کارکردی پیشخوان خدمت وظیفه‌ی مدیریت و پاسخ‌گویی به رخدادها را برعهده دارد.

در فرآیند مدیریت رخداد، رویکردی فرآیندگرا در حوزه ای که سازمان با مشتریان در ارتباط است، استقرار می‌یابد. ازاین‌روست که استقرار این فرآیند در هر سازمان یا شرکت ارائه دهنده‌ی خدمت، خیلی زود از طرف فضای کسب و کار و مشتریان درک شده و به اصطلاح به چشم می آید. بنابراین، ارزش مدیریت اثربخش رخداد برای واحدهای کسب و کار، در مقایسه با سایر حوزه‌های عملیات خدمت، ساده‌تر و سریع‌تر نمود پیدا می‌کند و به همین علت است که بیشتر پروژه‌های استقرار مدیریت خدمات فناوری اطلاعات (ITSM)با این فرآیند آغاز می‌شوند.

یکی از مزایای شروع پروژه‌ی استقرار مدیریت خدمات فناوری اطلاعات با فرآیند مدیریت رخداد این است که، در نتیجه‌ی استقرار این فرآیند، مشخص می‌شود که عملکرد کدامیک از حوزه ها و فرآیندهای دیگر سازمان، نیازمند بهبود است. این یکی از عللی است که مدیران فناوری اطلاعات هرگز به فرآیند مدیریت رخداد نه نمی‌گویند .در ادامه بر برخی از دیگر ارزش‌های مدیریت رخداد برای کسب و کارها اشاره می‌کنیم.

توانایی تشخیص و حل و فصل رخدادها به کاهش زمان خرابی (Downtime) سیستم در کسب و کارها می‌انجامد. به بیان دیگر، با تشخیص رخداد و حل و فصل آن در اسرع وقت، زمان فعال بودن سیستم یا به اصطلاح آپ بودن (UP) آن افزایش می‌یابد. بیشتر شدن زمان فعالیت سیستم، افزایش قابلیت اطمینان (Reliability)و در نتیجه افزایش دسترس‌پذیری (Availability) را در پِی خواهد داشت.

- اطلاعات بسیاری که از بررسی روند رخدادها به دست می‌آید، به مدیریت فناوری اطلاعات در شناسایی اولویت‌های کسب‌وکار، تخصیص منابع به شکلی پویا و متناسب با نیازمندی‌ها، و در نهایت هم‌سویی فناوری اطلاعات با اولویت‌های کسب و کار کمک می‌کند.
- تشخیص اقلام پیکربندی مرتبط با هر رخداد و ریشه یابی رخدادها، امکان شناسایی آن خدمات و دارایی‌هایی را که بیشتر در معرض اختلال بوده‌اند یا عوامل کلیدی مسبب بروز یک رخداد را فراهم می‌کند. این امر منجر به شناسایی زمینه‌های بهبود هر خدمت خواهد شد.
- پیشخوان خدمت در حین رسیدگی به رخدادها، می‌تواند نیازمندی‌های آموزشی، مهارتی، نرم‌افزاری، سخت‌افزاری، زیرساختی و... را شناسایی کند.
- بهره‌گیری از مدل رخدادها تکرارپذیری رویه‌ی رسیدگی به رخدادهای مختلف را بالا می‌برد. چنانچه این تکرارپذیری خودکارسازی نشود، می‌تواند به یک بروکراسی آزاردهنده بیانجامد. بنابراین، پیشنهاد می‌شود که مدل‌های رخداد را، با بهره‌گیری از ابزارهای مناسب خودکارسازی کنید.

بسیاری از رخدادها تکراری هستند. یعنی قبلاً اتفاق افتاده‌اند و به احتمال فراوان دوباره هم اتفاق می‌افتند. به همین علت، بسیاری از سازمان‌ها می‌توانند رخدادها را در قالب مدل‌های استاندارد دسته‌بندی کرده و برای حل و فصل، آن‌ها را به صورت رویه‌های از پیش تعیین‌شده طرح ریزی نمایند.

مدل رخداد روشی از پیش تعریف‌شده، شامل اقدامات لازم برای رسیدگی به یک نوع خاصِ رخداد است که تمامی ذی‌نفعان بر انجام آن توافق دارند.

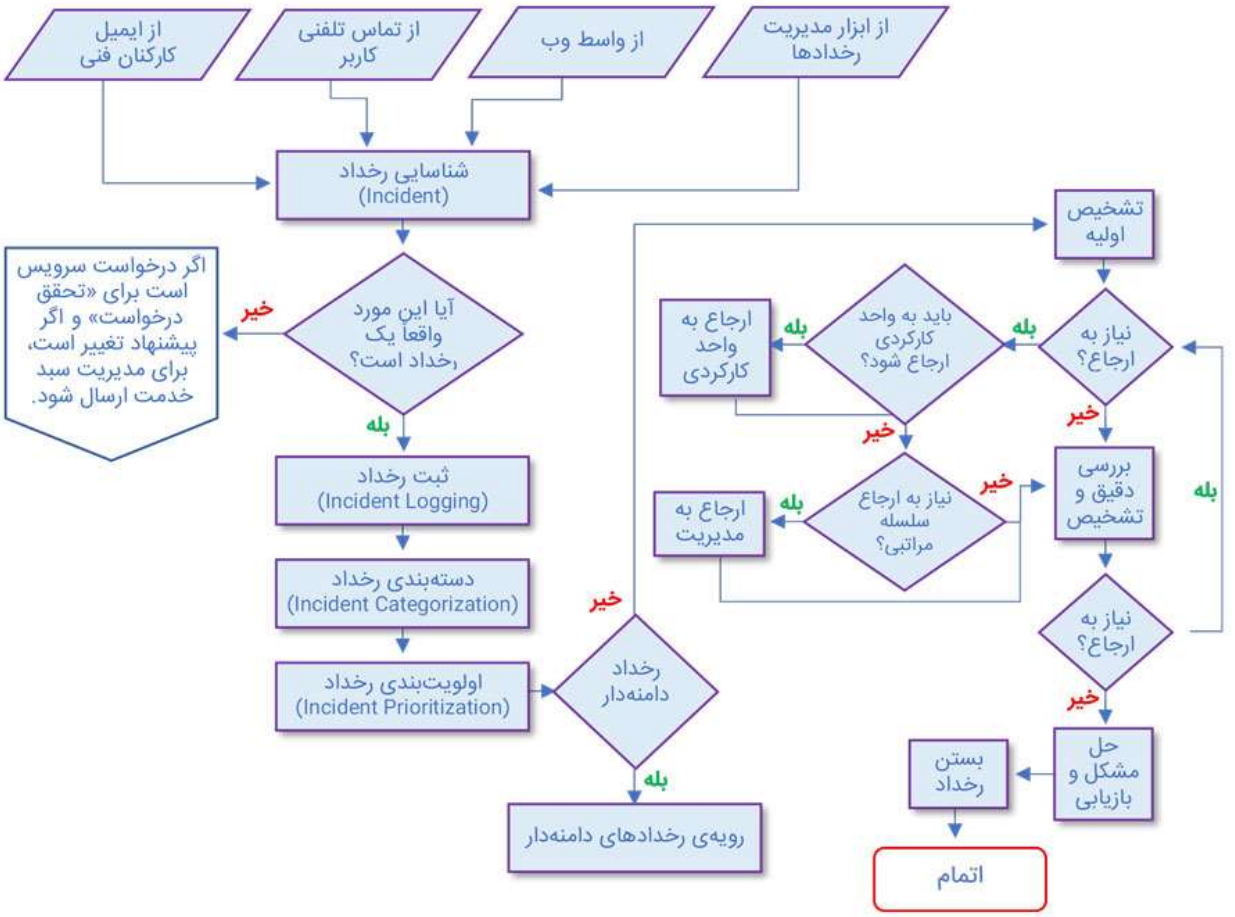
خودکارسازی مدل رخدادها، از طریق ابزارهای مدیریت خدمات، ضامن رسیدگی به رخداد مطابق روش توافق‌شده و بر اساس محدودیت‌های زمانی تعیین‌شده خواهد بود.

موارد زیر باید در مدل رخداد مشخص شوند:

- مراحل طی‌شده برای مدیریت یک رخداد، از زمان شناسایی تا زمان حل و فصل آن؛
- زمان‌بندی و وابستگی بین مراحل (تقدم و تأخر)؛
- اقدامات لازم‌الاجرا، پیش از رسیدگی به یک رخداد؛
- نقش‌ها، اختیارات و مسئولیت‌ها و ارتباط آن‌ها با مراحل رسیدگی به رخداد؛
- بازه‌های زمانی و آستانه‌ها(Thresholds) ، برای تکمیل فعالیت‌های مراحل مختلف؛
- رویه‌های ارجاع به سطوح بعدی (Escalation) که مشخص می‌کند یک رخداد در چه شرایطی باید به سطوح بعد ارجاع داده شود و چه کسی، در سطوح بعدی، پاسخ‌گوی این رخداد خواهد بود؛
- کارهای لازم برای فراهم آوردنِ دلایل و شواهد بروز یک رخداد.

جریان کاری در فرآیند مدیریت رخداد

در شکل زیر می‌توانید جریان کاری فرآیند مدیریت رخداد را مشاهده کنید .هریک فعالیت‌های این فرآیند را در ادامه، به تفصیل، بررسی خواهیم کرد.



ثبت رخداد مقوله ای مهم است که برخی از سازمان‌ها به ارزش واقعی آن واقف نیستند، چراکه این مهم نه‌تنها به شکل‌گیری یک پایگاه دانش، برای پیگیری و بهبود عملکرد فرآیند مرتبط کمک می‌کند، بلکه به پیگیری و بهبود دیگر فرآیندهای سازمان هم کمک کرده و برای آن‌ها ارزش‌آفرینی می‌کند .

ده گام اولیه برای برخورد با یک رخداد امنیتی کامپیوتری

زمانی که یک رخداد امنیتی کامپیوتری رخ می‌دهد و شما برای آن آمادگی ندارید، این ده گام را دنبال کنید:

گام اول: خونسردی خود را حفظ کنید. حتی یک رخداد بسیار ساده نیز به شما فشار و استرس تحمیل می‌کند. در این حالت برقراری ارتباط با دیگران و هماهنگی با آنها سخت می‌شود. آرامش شما می‌تواند از ارتکاب خطاهای جدی توسط دیگران جلوگیری نمایند.

گام دوم: از یادداشت‌های مناسب استفاده کنید. فرم‌هایی را که در انتهای این مجموعه مقالات ارائه می‌شوند، مورد استفاده قرار دهید. به این منظور، با فرمی که «معرفی رویداد» نام دارد آغاز کنید. سپس کار خود را با سایر فرم‌های مرتبط ادامه دهید. همانطور که فرم‌ها را

تکمیل می‌کنید، به خاطر داشته باشید که یادداشت‌های شما می‌توانند به عنوان مدرک در دادگاه مورد استفاده قرار گیرند. در مورد پاسخ‌های خود به چهار سوال «چه کسی»، «چه چیزی»، «چه زمانی» و «کجا» اطمینان حاصل کنید. همچنین بهتر است که به سوالات «چگونه» و «چرا» نیز توجه کنید.

گام سوم: به افراد مناسب اطلاع داده و از آنها کمک بخواهید. این کار را با اطلاع رسانی به هماهنگ کننده امنیتی و مدیر خود آغاز کنید. بخواهید که یکی از همکاران برای کمک به هماهنگ کردن روال مدیریت رخداد اختصاص داده شود. یک کپی از دفتر تلفن شرکت گرفته و با خود همراه داشته باشید. از همکار خود بخواهید که یادداشت‌های دقیقی از صحبت‌های تمامی افراد بنویسد. خود شما نیز همین کار را انجام دهید.

گام چهارم: جزئیات رخداد را به کمترین تعداد افراد ممکن منتقل کنید. به آنها تاکید کنید که افراد قابل اعتمادی هستند و سازمان شما روی احتیاط آنها حساب می‌کند.

گام پنجم: اگر کامپیوترهای شما مورد سوء استفاده قرار گرفته اند، از آنها برای بحث‌های مدیریت رخداد استفاده نکنید. به جای این کار از تلفن و فاکس استفاده نمایید. اطلاعات مربوط به رخداد را با ایمیل و چت منتقل نکنید. ممکن است این اطلاعات توسط مهاجمان مورد شنود قرار گیرند و وضعیت بدتر گردد. زمانی که از کامپیوتر برای انتقال اطلاعات استفاده می‌کنید، تمامی ایمیل‌های مربوط به مدیریت رخداد را رمزگذاری نمایید.

گام ششم: مشکل را محدود کنید. گام‌های لازم برای جلوگیری از بدتر شدن مشکل را به کار ببندید. این مساله اغلب به معنای حذف سیستم آسیب دیده از شبکه است. البته ممکن است مدیریت تصمیم بگیرد به منظور به دام انداختن فرد مهاجم، ارتباطات این سیستم را باز بگذارد.

گام هفتم: هر چه سریع‌تر یک نسخه پشتیبان از سیستم‌های آسیب دیده تهیه کنید. برای این کار از ابزار ذخیره سازی جدید و استفاده نشده ای استفاده کنید. در صورت امکان، یک نسخه پشتیبان دودویی یا بیت به بیت تهیه نمایید. ابزارهایی مانند SafeBack، یا Norton Ghost می‌توانند پشتیبان‌های دودویی اجرایی بر روی پلت‌فورم‌های اینتل تهیه کنند. اگر فرصت کافی برای یادگیری ابزار «dd» را پیش از وقوع رخداد داشته باشید، می‌توانید این ابزار را برای هر دو سیستم عامل ویندوز و یونیکس مورد استفاده قرار دهید. البته این کار نیاز به تمرین دارد.

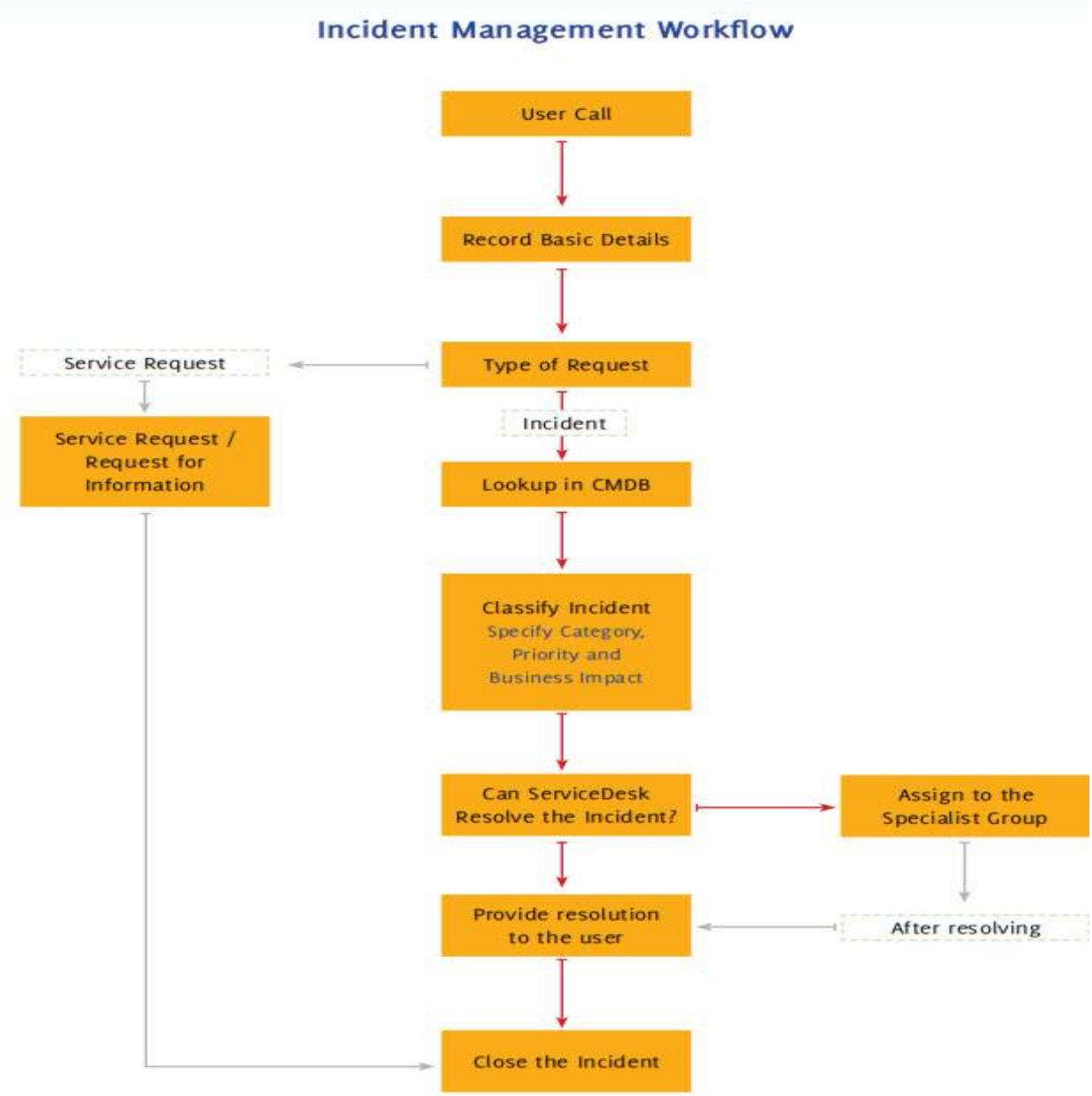
گام هشتم: از شر مشکل خلاص شوید. اگر می‌توانید مشخص کنید که چه چیزی باعث ایجاد مشکل شده است. گام‌هایی را برای تصحیح نواقصی که باعث رخ دادن مشکل شده بودند به کار ببندید.

گام نهم: به کار خود برگردید. پس از چک کردن نسخه های پشتیبان و حصول اطمینان از اینکه مورد سوء استفاده قرار نگرفته اند، سیستم خود را از طریق این نسخه های پشتیبان بازیابی کنید. سپس سیستم را به دقت کنترل کنید تا مطمئن شوید که می‌تواند وظایف خود را انجام دهد. چند هفته همچنان سیستم را تحت نظارت داشته باشید تا اطمینان حاصل کنید که مجددا مورد سوء استفاده قرار نگرفته باشد.

گام دهم: از این تجربه درس بگیرید. بنابراین در هنگام روی دادن رخداد بعدی آماده خواهید بود. این مجموعه مقالات به شما کمک خواهد کرد تا یک روش سیستماتیک برای مدیریت رخدادها در اختیار داشته باشید.

افراد بسیار کمی وجود دارند که تجربه کافی مدیریت رخداد برای راهنمایی دادن در مورد تمامی انواع رخدادها و برای تمامی انواع سازمان‌ها را دارا باشند. این مجموعه مقالات، تجربه مدیریت رخداد بیش از 50 سازمان مختلف تجاری، دولتی و آموزشی را یک جا

گرد آورده است. اگر سازمان مطبوع شما یک سازمان بسیار کوچک است، فقط قسمت‌هایی از این راهنما را که می‌توانید پیاده سازی نمایید. در قسمت‌های آینده این مجموعه مقالات، شش مرحله اصلی مدیریت رخدادهای امنیت کامپیوتری را به تفصیل شرح خواهیم داد.



منابع:

ITIL Service Operation – 2011 Edition
https://it.vanderbilt.edu
https://www.researchgate.net
https://www.it.northwestern.edu

3.2 مدیریت مشکلات

مدیریت مشکل یکی از جنبه های پیاده سازی ITIL است که باعث نگرانی بسیاری از سازمان‌ها شده است. مشکلی که در اینجا وجود دارد شباهت بین مدیریت رخداد (incident management) با مدیریت مشکل (problem management) است. این دو فرآیند بسیار با یکدیگر هم راستا بوده و تمایز بین فعالیت‌های آنها برای تازه کارهای ITIL دشوار است. در چه نقطه ای این دو فرآیند به یکدیگر تبدیل می‌شوند؟ در برخی سازمان‌ها، این دو فرآیند با یکدیگر مرتبط بوده و با هم ترکیب می‌شوند. با این حال، تفاوت‌های بین این فرآیندها نیز مهم هستند زیرا این دو فرآیند یکسان نبوده و اهداف متفاوتی دارند.

اصطلاح "مشکل (problem)" به علت ناشناخته ای اشاره دارد که منجر به وقوع یک یا چند رخداد می‌شود. یک تشبیه مفید و کاربردی برای درک ارتباط بین مشکلات و رخدادها، این است که فکر کنید رابطه بین یک بیماری و علائم آن چیست. در این تشبیه، مشکل همان بیماری است و علائم بیماری نیز رخدادها هستند. درست همانطور که یک پزشک از علائم برای تشخیص بیماری استفاده می‌کند، مدیریت مشکل نیز از رخدادهای بوجود آمده برای تشخیص مشکل استفاده می‌کند.

هنگامی که رخدادها اتفاق می افتد، نقش مدیریت رخداد، بازگرداندن سرویس در سریع‌ترین زمان ممکن است بدون آنکه نیازی به شناسایی یا برطرف ساختن علت رخداد باشد. اگر رخدادها به ندرت رخ دهند یا تاثیر ناچیزی داشته باشند، در چنین حالتی دلیلی برای تخصیص منابع جهت انجام تجزیه و تحلیل علت ریشه ای رخداد، وجود ندارد. با این حال، اگر یک رخداد مجزا یا دنباله ای از رخدادهای تکراری باعث تاثیر قابل توجهی شوند، مدیریت مشکل به تشخیص علت اصلی رخدادها و در نهایت شناسایی ابزاری برای از بین بردن این علت می‌پردازد.

اولین فعالیت problem management این است که مشکل را تشخیص داده و راه حل های موجود را شناسایی کند. Problem management از یک پایگاه داده مشکل برای پیگیری مشکلات و مرتبط سازی راه حل های مشخص شده با آنها استفاده می‌کند. پس از آنکه مشکل و راه حل آن مشخص شد، این مشکل به عنوان یک "خطای شناخته شده" در نظر گرفته می‌شود. این خطاها در پایگاه داده خطاهای شناخته شده (KEDB) که ممکن است یک پایگاه داده فیزیکی همانند پایگاه داده مشکل باشد، مستند می‌شوند. KEDB ابزار مهمی برای مدیریت رخدادها در حل رخداهای ناشی از خطاهای شناخته شده است.

پس از شناسایی خطای شناخته شده، مرحله بعدی تعیین نحوه رفع آن است. اینکار معمولا شامل یک تغییر در یک یا چند CI می‌باشد، بنابراین خروجی فرآیند مدیریت مشکل، یک درخواست تغییر است که پس از آن توسط فرآیند مدیریت تغییر ازریابی شده و یا در فهرست CSI لحاظ می‌شود.

Problem management به عنوان یک فرآیند واکنشی در نظر گرفته می‌شود که پس از وقوع رخداد اتفاق می افتد، اما در حقیقت یک فرآیند پیشگیرانه است، زیرا هدف آن این است که اطمینان حاصل کند رخدادها در آینده رخ نخواهند داد یا اگر رخ دهند، تاثیر آنها را به حداقل خواهد رساند.

Problem management یک گام فراتر از مدیریت رخداد در مرحله عملیات سرویس در چرخه حیات ITIL است. Incident management هرگونه وقفه پیش بینی نشده یا کاهش کیفیت سرویس فناوری اطلاعات را کنترل و مدیریت می‌کند، درحالیکه problem management علت اصلی رخدادها را کنترل و مدیریت می‌کند. به بیان ساده تر، incident management سرویس‌ها را بازیابی می‌کند در حالیکه problem management علت شکست سرویس‌ها را برطرف می‌کند.

"مشکل" در ITIL به عنوان علت یک یا چند رخداد تعریف می‌شود. برخی رخدادها مانند یک موس خراب در یک ایستگاه کاری کاربر، نشانگر مشکل نیستند. در خصوص سایر رخدادها همچون قطع شدن مکرر شبکه بدلیل آنکه مرتبا تکرار می‌شوند باید مشکل را بررسی نمود. در چنین شرایطی problem management بصورت واکنشی عمل می‌کند. مدیریت مشکل پیشگیرانه شامل رسیدگی به وضعیت سخت افزار، نرم افزار و فرآیندها و همچنین رسیدگی به مسائل قبل از آنکه رخدادهای بیشماری را بوجود آورند. مدیریت رخداد و مدیریت درخواست هیچکدام قادر نیستند همانند مدیریت مشکل، بصورت پیشگیرانه عمل کنند.

هنگامیکه کاربران بطور مداوم با رخدادهای مشابهی که برطرف نشده اند، مواجه شوند، اعتماد خود را نسبت به قابلیت desk service در حل مشکلات از دست خواهند داد. از این رو، هدف اصلی مدیریت مشکل، شناسایی، عیب یابی، مستندسازی و برطرف ساختن علل اصلی و ریشه رخدادهای تکراری است. اطلاعات مربوط به رخدادها در problem management فیلتر شده و در نتیجه problem management خطاهای شناخته شده و اطلاعات مربوط به راه حل مورد نیاز جهت مقابله با مشکلات در کوتاه مدت را برای service desk فراهم می‌کند.

مشکلات شامل مسائلی از قبیل خرابی سخت افزار یا ناکارامد بودن query تنظیم شده پایگاه داده است. Problem management تعداد رخدادها را در طولانی مدت کاهش می‌دهد.کاهش رخداد، بار کاری service desk را کاهش داده و رضایت کاربر نهایی را افزایش می‌دهد، بعلاوه هزینه های مربوط به کاربران و خرابی سرویس را در طولانی مدت کاهش می‌دهد. هنگامیکه مشکلات برطرف نشود، problem management با service desk همکاری کرده تا بتواند میزان اثرگذاری رخدادهای مرتبط را کاهش دهد. هدف نهایی problem management همواره باید کاهش تعداد کلی رخدادهای قابل پیشگیری و در نتیجه افزایش کیفیت خدمات ارائه شده باشد.

Problem management وظایف و نقش‌های زیادی دارد که مهم‌ترین آن service desk است. با اینکه service desk، با عنوان "help desk" نیز شناخته می‌شود، اما اصطلاح مورد قبول ITIL نبوده و باید از بکارگیری آن خودداری نمود. این نقش در ITIL به عنوان تنها نقطه تماس برای مشتریان سرویس‌ها جهت گزارش رخدادها و ارسال درخواست‌های سرویس عمل می‌کند. بدون وجود یک نقطه تماس، کاربران ممکن است با کارکنان تماس گرفته و انتظار داشته باشند سرویس‌ها را فوری و بدون هیچ گونه محدودیت اولویت بندی دریافت کنند. متاسفانه، این بدان معناست که رخدادهای فوری نادیده گرفته شده و رخدادهایی که تاثیر چندانی بر کسب و کار نمی‌گذارند، در ابتدا انجام می‌شوند. یکی دیگر از سناریوهای معمول این است که رخدادهای مهم اما کم اهمیت برای هفته ها رسیدگی نمی‌شوند، زیرا کارمندان پشتیبانی فناوری اطلاعات مشغول رسیدگی به مسائل فوری در service desk خود بوده و زمانی برای مسائل کوچکتر صرف نمی‌کنند. Service desk به سرویس دهندگان امکان می‌دهد تا بطور پیوسته و فوری به مسائل و مشکلات هر فرد رسیدگی کند. همچنین به انتقال دانش بین دپارتمان‌ها کمک کرده و داده های مربوط به روندهای IT را جمع آوری و امکان مدیریت مشکل را فراهم می‌کند.

این نقش می‌تواند به سطوح پشتیبانی مجزا یا به عبارتی چند لایه مجزا تقسیم شود. لایه نخست برای مشکلات پایه ای است. این مشکلات شامل مسائلی با اولویت پایین هستند مانند عیب یابی اولیه کامپیوتر. رخدادهای لایه اول به احتمال زیاد به مدل های رخداد تبدیل می‌شوند، زیرا به سادگی قابل حل بوده و اغلب رخ می‌دهند. رخدادهای لایه اول تاثیری بر کسب و کار و سایر کاربران نمی‌گذارند. تا زمانیکه این رخدادها توسط service desk برطرف می‌شوند، به راحتی می‌توان بر آنها غلبه کرد. برای مثال خطای Outlook مایکروسافت می‌تواند از طریق جایگزینی با برنامه ایمیل مبتنی بر وب برطرف شود.

سطح پشتیبانی لایه دوم آن دسته از مشکلاتی را که تنها بر کاربر تاثیر داشته اما بر روی کسب و کار اثری ندارد را کنترل و مدیریت می‌کند. معمولا حل این گونه رخدادها به مهارت یا دسترسی بیشتری نیاز دارد. رخدادهای لایه دوم، دارای اولویت متوسط بوده و به پاسخ‌های فوری بیشتر و سطح بالایی از دسترسی یا آموزش نسبت به رخدادهای لایه اول نیاز دارند.

رخدادهای لایه سوم، کل سازمان و بسیاری از کاربران را تحت تاثیر قرار می‌دهند. در برخی موارد، ممکن است یک کاربر VIP به دسته بندی سطح دوم یا سطح سوم رفته تا زمان پاسخگویی به این کاربران سریع‌تر شود. این رخدادها اغلب وارد فرآیند اصلی پاسخ به رخداد (Major Incident Response) می‌شوند. بر اساس تعریف ITIL، اینها همان رخدادهایی هستند که منجر به بروز اختلالات عمده در کسب و کار می‌شوند. این رخدادها همیشه اولویت بالایی دارند. رخدادهایی که به فرآیند اصلی پاسخ به رخداد نیاز دارند، کاندیدهای خوبی برای مشکلات احتمالی هستند، زیرا آنها بر کسب و کار اثر گذاشته و به احتمال زیاد علت اصلی وقوع آنها با رخدادهای معمولی تفاوت دارد.

هنگامیکه اکثر رخدادها در لایه نخست با اولویت پایین قرار داشته و تعداد کمتری از رخدادها در لایه دوم و تنها تعداد بسیار کمی نیز در لایه سوم قرار دارند، بدین معناست که لایه ها و اولویت‌ها را به دقت ارزیابی کرده اید.

Service desk به چندین روش با تیم problem management ارتباط برقرار می‌کند. اولین تعامل هنگامی است که یک مشکل بالقوه مطرح می‌شود. این ارتباط زمانی برقرار می‌شود که یک رخداد برای service desk غیر قابل حل بوده و میبایست ارجاع داده شود و یا هنگامیکه یک رخداد با وجود عیب یابی های انجام شده و حل شدن مجددا تکرار می‌شود. در نهایت، هنگامیکه تیم problem management یا continual service improvement (بهبود مستمر سرویس) مشکلات را پیش از مواجهه با آنها شناسایی می‌کنند، در چنین شرایطی ممکن است جهت کسب اطلاعات بیشتر یا آمار رخدادها با service desk تماس برقرار کنند.

فرآیند مدیریت مشکل

فرآیند problem management در ITIL مراحل زیادی دارد و هر مرحله برای موفقیت فرآیند و کیفیت سرویس‌های ارائه شده اهمیت بسیاری دارد.

اولین مرحله تشخیص مشکل است. یک مشکل یا از طریق ارجاع از service desk ایجاد می‌شود یا از طریق ارزیابی الگوهای رخداد پیش از وقوع رخداد و هشدارهایی که از سمت مدیریت رویداد و فرآیندهای بهبود مستمر سرویس می آید. نشانه های یک مشکل شامل موارد زیر است:

- رخدادهایی که در سراسر سازمان با شرایط یکسان رخ می‌دهند.
- رخدادهایی که با وجود عیب یابی موفقیت آمیز، تکرار می‌شوند.
- رخدادهایی که در service deskقابل حل نیستند.

دومین مرحله ثبت مشکل است. در چارچوب ITIL، مشکلات در یک رکورد مشکل (problem record) ثبت می‌شوند. یک رکورد مشکل، تلفیقی از همه مشکل در یک سازمان است. ثبت این مشکلات در داخل یک رکورد امکانی است که از طریق یک سیستم تیکتینگ برای انواع درخواست‌های مشکل فراهم می‌شود. داده های مربوط به مشکلات همچون زمان و تاریخ وقوع، رخدادهای مرتبط، علائم، مراحل عیب یابی های قبلی و دسته بندی مشکلات همگی به تیم مدیریت مشکل کمک می‌کند تا ریشه مشکلات را پیدا کنند.

سومین مرحله به دستبه بندی مشکلات اختصاص دارد. دسته بندی مشکلات میبایست با دسته بندی رخدادها مطابقت داشته باشد. این مرحله در چندین روش سودمند است. یک مزیت آن است که به service desk امکان می‌دهد تا رخدادها را بطور منظم مرتب سازی و مدل سازی کند. مدلسازی امکان تخصیص خودکار اولویت‌ها را فراهم می‌سازد. سومین و مهم‌ترین مزیت، داشتن قابلیت جمع آوری داده ها و گزارش دهی از داده های service desk است. این داده ها به سازمان امکان می‌دهد که نه تنها روند مشکلات را پیگیری کرده، بلکه بتواند تاثیر آنها را بر میزان تقاضای سرویس و ظرفیت سرویس دهنده ارزیابی کند.

مرحله چهارم مربوط به اولویت بندی کردن مشکلات می‌باشد. اولویت یک مشکل بر اساس میزان تاثیر آن بر کاربران و کسب و کار و همچنین فوریت آن تعیین می‌شود. فوریت بدین معنا است که سازمان چقدر سریع مشکلات را برطرف می‌کند. تاثیر نیز به معنای اندازه گیری میزان آسیب احتمالی است که این مشکل می تواند در سازمان ایجاد کند. اولویت بندی کردن مشکلات به سازمان امکان می‌دهد که از منابع تحقیقاتی بطور مؤثر استفاده کند. همچنین به سازمان کمک می‌کند تا میزان تخطی از توافق نامه سطح سرویس را از طریق تخصیص مجدد منابع به محض شناخت مساله (مشکل)، کاهش دهد.

مرحله پنجم یک فرآیند دو مرحله ای شامل بررسی و تشخیص مشکل است. سرعت بررسی و تشخیص مشکل به اولویت تخصیص داده شده به آن مشکل دارد. مشکلاتی که اولویت بالایی دارند باید همیشه در ابتدا رسیدگی شوند زیرا تاثیر آنها بر سرویس‌ها بیشتر است. دسته بندی صحیح در اینجا کمک می‌کند، زیرا شناسایی روند ها در زمانی که دسته بندی مشکلات با دسته بندی

رخدادها مطابقت دارد، آسان تر است. تشخیص مشکل معمولا شامل تجزیه و تحلیل رخدادهایی است که منجر به گزارش مشکلات و همچنین تست‌های بیشتری که احتمالا در سطح service desk امکان پذیر نیست، می‌شود، مانند تحلیل پیشرفته log.

مرحله ششم به شناسایی راه حل مشکل اختصاص دارد. یک راه حل همیشه باید نشان داده شود، زیرا مشکلات در سطح رخداد حل نمی‌شوند. راه حل، service desk را قادر می‌سازد تا سرویس‌ها را هنگامیکه مشکل در حال رفع شدن است، بازیابی کند. حل یک مشکل می تواند از یک ماه تا چند ماه به طول بینجامد، بنابراین وجود یک راه حل برای آن بسیار حیاتی است. یک مشکل تا زمانیکه حل نشود، در وضعیت "باز" باقی می‌ماند، بنابراین یک راه حل باید تنها به عنوان یک معیار موقت در نظر گرفته شود.

مرحله هفتم مربوط به ایجاد رکوردی از خطاهای شناخته شده است. هنگامی که راه حل شناسایی شد، باید به عنوان یک خطای شناخته شده به کارکنان درون سازمان اعلام شود. اینکار روش خوبی برای ثبت خطای شناخته شده در پایگاه دانش رخداد و هم در پایگاه داده خطاهای شناخته شده (KEDB) است. مستندسازی راه حل ها به service desk امکان می‌دهد تا رخدادها را به سرعت حل کرده و از وقوع مشکلات بیشتر که بر اثر همان رخدادها بوجود می آیند، جلوگیری کند.

مرحله هشتم به حل مشکلات می‌پردازد. مشکل باید هر زمان که امکان پذیر است، حل شود. راه حل ها، علت اصلی مجموعه ای از رخدادها را برطرف کرده و از وقوع مجدد آن ها جلوگیری می‌کند. برخی از این راه حل ها ممکن است به هیئت مدیره بخش change management نیاز داشته باشند زیرا ممکن است سطوح سرویس را تحت تاثیر قرار دهند. برای مثال، switchover شدن database ممکن است باعث ایجاد کندی در طول دوره switchover شود. پیش از پیاده سازی راه حل، همه ریسک های آن باید ارزیابی شود. مراحل انجام شده جهت حل مشکل را در داخل پایگاه دانش سازمان، مستند نمایید.

مرحله نهم، بستن مشکل است. این مرحله فقط باید بعد از ایجاد، دسته بندی، اولویت بندی، شناسایی، تشخیص و حل مشکل رخ دهد. با وجود آنکه بسیاری از سازمان‌ها کار را در این مرحله متوقف می‌کنند، اما برای ITIL پایان کار نیست.

آخرین مرحله، بازنگری مشکل است. بازنگری مشکل اصلی یک فعالیت سازمانی است که از وقوع مشکلات آینده جلوگیری می‌کند. در طول مرحله بازنگری، تیم problem management مستندات مشکل را ارزیابی کرده و مشخص می‌کند که چه اتفاقی رخ داده و علت وقوع آن چیست. درسهای آموخته شده، مانند شکاف های موجود در فرآیند، اشتباهی که رخ داده و آنچه که به آن کمک کرده، باید مورد بحث قرار گیرد. این جایی است که داشتن log کامل از مشکلات کمک خواهد کرد. یک log کامل به مراتب بهتر از تلاش برای گرفتن جزئیات از حافظه، عمل می‌کند. بازنگری مشکل باید منجر به بهبود فرآیندها، آموزش کارکنان یا مستندات کامل‌تر شود.

نمودار جریان فرآیند مدیریت مشکل

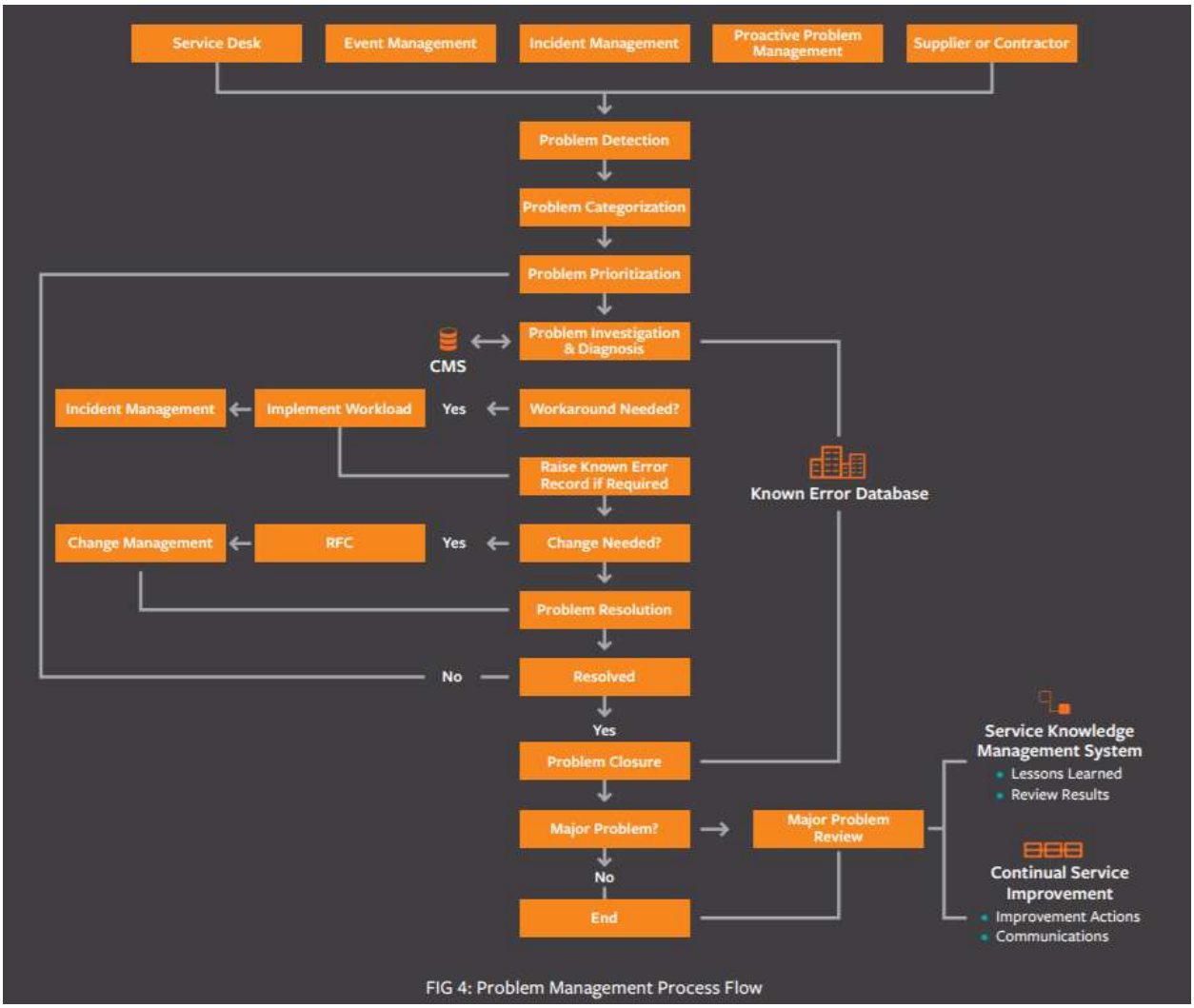


FIG 4: Problem Management Process Flow

چگونه مدیریت مشکل را به ITILمتصل می کند

Problem management تنها یک جزء از چرخه حیات مدیریت سرویس ITIL است. مدیریت مشکل در فرآیند اصلی Problem management وجود دارد و به عنوان یک فرآیند با بسیاری از بخش‌های ITIL ارتباط دارد. با توجه به ارتباط Problem management با service desk، آن را به طور مستقیم تحت تاثیر قرار داده و بر مدیریت رخداد نیز تاثیر می‌گذارد. همچنین از آنجا که تاثیر مالی یک مشکل در مراحل اولویت بندی و حل مشکل مشاهده می شود، با مدیریت مالی نیز ارتباط دارد. هنگامیکه مشکلات قبلی و مشکلات احتمالی در طول فرآیند طراحی IT مشاهده می‌شود، با service design نیز ارتباط برقرار می‌کند. با مدیریت دانش هنگامیکه خطاهای شناخته شده در آن ذخیره می‌شوند، ارتباط برقرار می‌کند. در نهایت نیز با بهبود مستمر سرویس در زمانی که مدیریت مشکل بصورت پیشگیرانه عمل می‌کند، ارتباط برقرار می‌کند، زیرا هدف هر دو بهبود کیفیت سرویس‌های ارائه شده به مشتریان داخلی و خارجی است.

این فرآیند برای موفقیت ارائه طولانی مدت سرویس‌ها بسیار ضروری است و در نتیجه نباید در هنگام طراحی سرویس های قدرتمند فناوری اطلاعات (چه در داخل و چه در خارج قرار داشته باشد) نادیده گرفته شود.

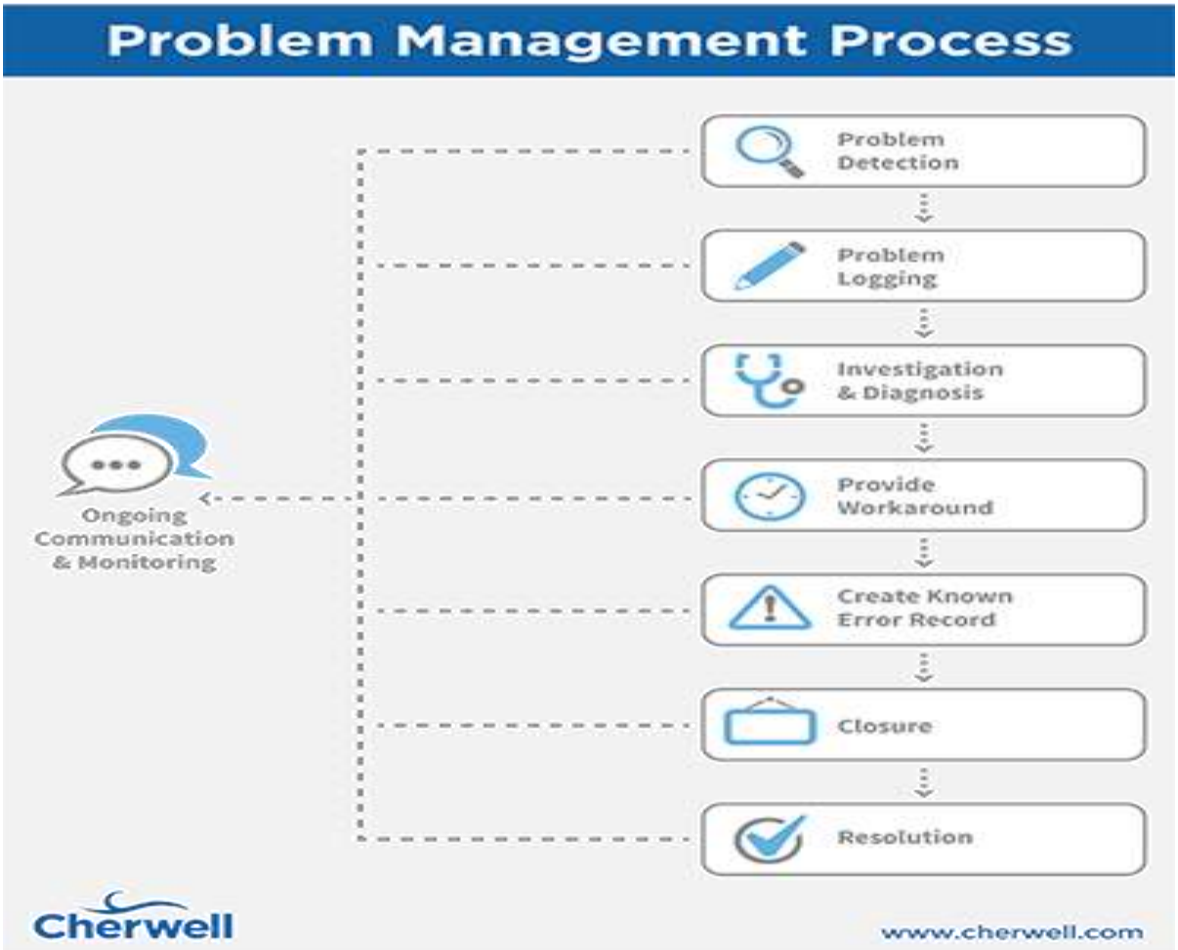
اولین فعالیت problem management این است که مشکل را اصطلاح "مشکل (problem)" به علت ناشناخته ای اشاره دارد که منجر به وقوع یک یا چند رخداد می‌شود. یک تشبیه مفید و کاربردی برای درک ارتباط بین مشکلات و رخدادها، این است که فکر کنید رابطه بین یک بیماری و علائم آن چیست. در این تشبیه، مشکل همان بیماری است و علائم بیماری نیز رخدادها هستند. درست همانطور که یک پزشک از علائم برای تشخیص بیماری استفاده می‌کند، مدیریت مشکل نیز از رخدادهای بوجود آمده برای تشخیص مشکل استفاده می‌کند.

هنگامی که رخدادها اتفاق می افتد، نقش مدیریت رخداد، بازگرداندن سرویس در سریع‌ترین زمان ممکن است بدون آنکه نیازی به شناسایی یا برطرف ساختن علت رخداد باشد. اگر رخدادها به ندرت رخ دهند یا تاثیر ناچیزی داشته باشند، در چنین حالتی دلیلی برای تخصیص منابع جهت انجام تجزیه و تحلیل علت ریشه ای رخداد، وجود ندارد. با این حال، اگر یک رخداد مجزا یا دنباله ای از رخدادهای تکراری باعث تاثیر قابل توجهی شوند، مدیریت مشکل به تشخیص علت اصلی رخدادها و در نهایت شناسایی ابزاری برای از بین بردن این علت می‌پردازد.

تشخیص داده و راه حل های موجود را شناسایی کند. Problem management از یک پایگاه داده مشکل برای پیگیری مشکلات و مرتبط سازی راه حل های مشخص شده با آنها استفاده می‌کند. پس از آنکه مشکل و راه حل آن مشخص شد، این مشکل به عنوان یک "خطای شناخته شده" در نظر گرفته می‌شود. این خطاها در پایگاه داده خطاهای شناخته شده (KEDB) که ممکن است یک پایگاه داده فیزیکی همانند پایگاه داده مشکل باشد، مستند می‌شوند. KEDB ابزار مهمی برای مدیریت رخدادها در حل رخداهای ناشی از خطاهای شناخته شده است.

پس از شناسایی خطای شناخته شده، مرحله بعدی تعیین نحوه رفع آن است. اینکار معمولا شامل یک تغییر در یک یا چند CI می‌باشد، بنابراین خروجی فرآیند مدیریت مشکل، یک درخواست تغییر است که پس از آن توسط فرآیند مدیریت تغییر ازریابی شده و یا در فهرست CSI لحاظ می‌شود.

Problem management به عنوان یک فرآیند واکنشی در نظر گرفته می‌شود که پس از وقوع رخداد اتفاق می افتد، اما در حقیقت یک فرآیند پیشگیرانه است، زیرا هدف آن این است که اطمینان حاصل کند رخدادها در آینده رخ نخواهند داد یا اگر رخ دهند، تاثیر آنها را به حداقل خواهد رساند.



هدف مدیریت تغییر

هنگامیکه کاربران بطور مداوم با رخدادهای مشابهی که برطرف نشده اند، مواجه شوند، اعتماد خود را نسبت به قابلیت service desk در حل مشکلات از دست خواهند داد. از این رو، هدف اصلی مدیریت مشکل، شناسایی، عیب یابی، مستندسازی و برطرف ساختن علل اصلی و ریشه رخدادهای تکراری است. اطلاعات مربوط به رخدادها در problem management فیلتر شده و در نتیجه problem management خطاهای شناخته شده و اطلاعات مربوط به راه حل مورد نیاز جهت مقابله با مشکلات در کوتاه مدت را برای service desk فراهم می‌کند.

مشکلات شامل مسائلی از قبیل خرابی سخت افزار یا ناکارامد بودن query تنظیم شده پایگاه داده است. Problem management تعداد رخدادها را در طولانی مدت کاهش می‌دهد.کاهش رخداد، بار کاری service desk را کاهش داده و رضایت کاربر نهایی را افزایش می‌دهد، بعلاوه هزینه های مربوط به کاربران و خرابی سرویس را در طولانی مدت کاهش می‌دهد. هنگامیکه مشکلات برطرف نشود، problem management با service desk همکاری کرده تا بتواند میزان اثرگذاری رخدادهای مرتبط را کاهش دهد. هدف نهایی problem management همواره باید کاهش تعداد کلی رخدادهای قابل پیشگیری و در نتیجه افزایش کیفیت خدمات ارائه شده باشد.

دامنه مدیریت مشکل

Problem management دامنه بسیار محدودی داشته و شامل فعالیت‌های زیر است:

- تشخیص مشکل(Problem detection)
- ثبت مشکل(Problem logging)
- دسته بندی مشکل(Problem categorization)
- اولویت بندی مشکل(Problem prioritization)
- تحلیل و بررسی مشکل(Problem investigation and diagnosis)
- ایجاد رکوردی از خطای شناخته شده(Creating a known error record)
- حل مشکل و بستن آن(Problem resolution and closure)
- بازنگری مشکل اصلی(Major problem review)

نقش اصلی مدیریت مشکل

Problem management وظایف و نقش‌های زیادی دارد که مهم‌ترین آن service desk است. با اینکه service desk، با عنوان "help desk" نیز شناخته می‌شود، اما اصطلاح مورد قبول ITIL نبوده و باید از بکارگیری آن خودداری نمود. این نقش در ITIL به عنوان تنها نقطه تماس برای مشتریان سرویس‌ها جهت گزارش رخدادها و ارسال درخواست‌های سرویس عمل می‌کند. بدون وجود یک نقطه تماس، کاربران ممکن است با کارکنان تماس گرفته و انتظار داشته باشند سرویس‌ها را فوری و بدون هیچ گونه محدودیت اولویت بندی دریافت کنند. متاسفانه، این بدان معناست که رخدادهای فوری نادیده گرفته شده و رخدادهایی که تاثیر چندانی بر کسب و کار نمی‌گذارند، در ابتدا انجام می‌شوند. یکی دیگر از سناریوهای معمول این است که رخدادهای مهم اما کم اهمیت برای هفته ها رسیدگی نمی‌شوند، زیرا کارمندان پشتیبانی فناوری اطلاعات مشغول رسیدگی به مسائل فوری در service desk خود بوده و زمانی برای مسائل کوچکتر صرف نمی‌کنند. Service desk به سرویس دهندگان امکان می‌دهد تا بطور پیوسته و فوری به مسائل و مشکلات هر فرد رسیدگی کند. همچنین به انتقال دانش بین دپارتمان‌ها کمک کرده و داده های مربوط به روندهای IT را جمع آوری و امکان مدیریت مشکل را فراهم می‌کند.

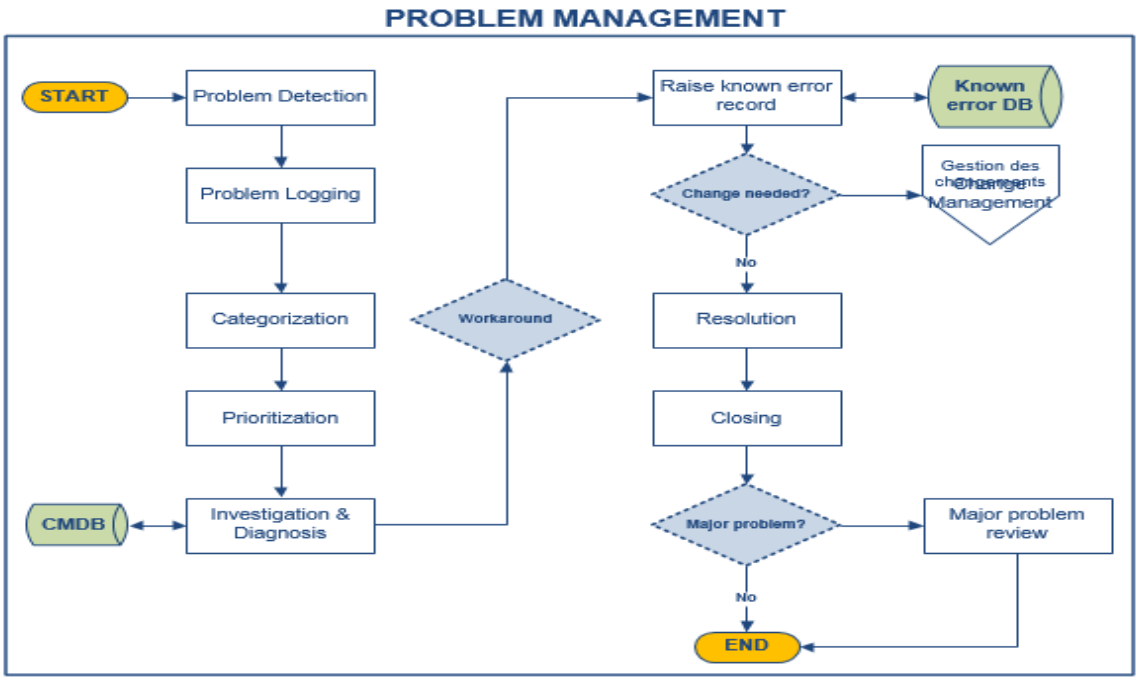
این نقش می‌تواند به سطوح پشتیبانی مجزا یا به عبارتی چند لایه مجزا تقسیم شود. لایه نخست برای مشکلات پایه ای است. این مشکلات شامل مسائلی با اولویت پایین هستند مانند عیب یابی اولیه کامپیوتر. رخدادهای لایه اول به احتمال زیاد به مدل های رخداد تبدیل می‌شوند، زیرا به سادگی قابل حل بوده و اغلب رخ می‌دهند. رخدادهای لایه اول تاثیری بر کسب و کار و سایر کاربران نمی‌گذارند. تا زمانیکه این رخدادها توسط service desk برطرف می‌شوند، به راحتی می‌توان بر آنها غلبه کرد. برای مثال خطای Outlook مایکروسافت می‌تواند از طریق جایگزینی با برنامه ایمیل مبتنی بر وب برطرف شود.

سطح پشتیبانی لایه دوم آن دسته از مشکلاتی را که تنها بر کاربر تاثیر داشته اما بر روی کسب و کار اثری ندارد را کنترل و مدیریت می‌کند. معمولا حل این گونه رخدادها به مهارت یا دسترسی بیشتری نیاز دارد. رخدادهای لایه دوم، دارای اولویت متوسط بوده و به پاسخ‌های فوری بیشتر و سطح بالایی از دسترسی یا آموزش نسبت به رخدادهای لایه اول نیاز دارند.

رخدادهای لایه سوم، کل سازمان و بسیاری از کاربران را تحت تاثیر قرار می‌دهند. در برخی موارد، ممکن است یک کاربر VIP به دسته بندی سطح دوم یا سطح سوم رفته تا زمان پاسخگویی به این کاربران سریع‌تر شود. این رخدادها اغلب وارد فرآیند اصلی پاسخ به رخداد (Major Incident Response) می‌شوند. بر اساس تعریف ITIL، اینها همان رخدادهایی هستند که منجر به بروز اختلالات عمده در کسب و کار می‌شوند. این رخدادها همیشه اولویت بالایی دارند. رخدادهایی که به فرآیند اصلی پاسخ به رخداد نیاز دارند، کاندیدهای خوبی برای مشکلات احتمالی هستند، زیرا آنها بر کسب و کار اثر گذاشته و به احتمال زیاد علت اصلی وقوع آنها با رخدادهای معمولی تفاوت دارد.

هنگامیکه اکثر رخدادها در لایه نخست با اولویت پایین قرار داشته و تعداد کمتری از رخدادها در لایه دوم و تنها تعداد بسیار کمی نیز در لایه سوم قرار دارند، بدین معناست که لایه ها و اولویت‌ها را به دقت ارزیابی کرده اید.

Service desk به چندین روش با تیم problem management ارتباط برقرار می‌کند. اولین تعامل هنگامی است که یک مشکل بالقوه مطرح می‌شود. این ارتباط زمانی برقرار می‌شود که یک رخداد برای service desk غیر قابل حل بوده و میبایست ارجاع داده شود و یا هنگامیکه یک رخداد با وجود عیب یابی های انجام شده و حل شدن مجددا تکرار می‌شود. در نهایت، هنگامیکه تیم problem management یا continual service improvement (بهبود مستمر سرویس) مشکلات را پیش از مواجهه با آنها شناسایی می‌کنند، در چنین شرایطی ممکن است جهت کسب اطلاعات بیشتر یا آمار رخدادها با service desk تماس برقرار کنند.



3.3 مدیریت تغییرات

change management فرآیندی است که برای درک و به حداقل رساندن ریسک‌ها در هنگام تغییر فناوری اطلاعات طراحی شده است. کسب و کارها دو انتظار عمده از سرویس‌های ارائه شده توسط فناوری اطلاعات دارند:

- سرویس‌ها باید پایدار، قابل اطمینان و قابل پیش بینی باشند.
- سرویس‌ها باید قادر به تغییر سریع به منظور برآورده ساختن نیازهای کسب و کار باشند.

این انتظارات با یکدیگر در تداخل هستند. هدف Change management این است که مدیریت سرویس IT را قادر سازد تا هر دو انتظار را برآورده سازد. بدین معنا که بتواند در حالی که احتمال وقفه (خرابی یا قطعی) در سرویس‌ها را به حداقل می‌رساند، به سرعت نیز تغییر کند.

با اینکه Change management یک فرآیند در مرحله Service Transition از چرخه حیات است، اما در برخی موارد تصمیم گیری در خصوص تایید یک تغییر پیشنهادی نوعی تصمیم استراتژیک محسوب می‌شود و در نتیجه انتظار می‌رود تا در صورت لزوم فرآیند Change management با فرآیند مدیریت سبد خدمات (portfolio management process) همکاری کند.

Change managementیک فرآیند رسمی را برای انجام تغییرات بکار گرفته و در نتیجه گاهی اوقات با افزودن تشریفات اداری، ایجاد تغییرات را سخت تر می‌کند. اما یک فرآیند change management که به درستی اجرا شده، می‌تواند حجم بالایی از تغییرات مفید را در مقایسه با زمانی که این فرآیند به درستی اجرا نشده، ایجاد کند

مدل های مدیریت تغییرات

مدل های تغییرات شامل چهار مرحله است

1. **تعیین نیاز به تغییر**
2. **آماده سازی و برنامه ریزی برای تغییر**
3. **تغییرات را اجرا کنید**
4. **تغییرات را حفظ کنید**

3.3.1 فرایند مدیریت تغییرات

ایجاد درخواست برای تغییر

در صورت ایجاد درخواست تغییر ، شما مسئول مستندسازی جزئیاتی هستید که به دیگران کمک خواهد کرد تا درک کنند چه تغییری باید انجام شود و چرا این درخواست را ایجاد می‌کنید. ارسال درخواست تغییر اولیه اغلب شامل جزئیاتی در مورد ریسک و مراحل پیاده سازی است، اگر آغازکننده این اطلاعات را بداند .با این حال، این اطلاعات در این زمان مورد نیاز نیست.

جزئیاتی که ممکن است در یک درخواست تغییر یافت شوند عبارتند از:

- رخدادهایی که انجام تغییر را ملزم می‌دارند.
- توصیف چگونگی اجرای تغییر.
- تاثیری که ممکن است یک تغییر بر روی همه سیستم‌های مربوطه داشته باشد.
- ارزیابی ریسک.
- اطلاعات تماس برای هر فردی که در تغییر حضور دارد.
- یک تصویر کلی از تمام افرادی که باید تغییر را تایید کنند.
- یک برنامه بکاپ گیری برای شرایطی که تغییر با شکست مواجه می‌شود.

بازبینی و ارزیابی درخواست تغییر

اگر شما مسئول بازبینی درخواست تغییر هستید، باید درخواست را بر اساس کاربرد و اولویت آن ارزیابی کنید. وظیفه شما این است که تعیین کنید آیا درخواست منطقی است یا خیر و همچنین بازخورد مربوط به درخواست را بدهید. اگر درخواست ها مربوط به مشکلاتی باشد که قبلا به آنها پرداخته شده است و یا مربوط به درخواست‌هایی که اجرای آنها مفید نیست، در اینصورت این درخواست‌ها کنار گذاشته خواهند شد.

درخواست‌های مفید و کاربردی بر اساس موارد زیر ارزیابی خواهند شد:

- ایجاد کننده درخواست
- تاثیری که این تغییر ممکن است بر روی شرکت داشته باشد

- بازگشت هرگونه سرمایه ای که در رابطه با این درخواست تخمین زده شده است
- منابع مورد نیاز برای اجرای درخواست
- شما همچنین مسئول اجرای درخواست و توانایی پیاده سازان جهت تخصیص زمان برای ایجاد تغییر را مشخص خواهید کرد.

برنامه ریزی تغییر

هنگامی که یک درخواست تغییر ایجاد می‌شود، شما باید تغییر را به گونه ای برنامه ریزی کنید که گویی اتفاق می افتد. یک برنامه تغییر (یا طرح تغییر) مسیر اجرای تغییر، منابعی که برای تکمیل تغییر مورد نیاز هستند و یک جدول زمانبندی را برای تغییر مشخص می‌کند.

تست تغییر

اگر یک تغییر مربوط به رفع خطاهای نرم افزاری یا تغییر یک سیستم باشد، ممکن است نیاز باشد تا شما این تغییر را پیش از آنکه تایید شود، تست کنید .تست کردن در مقیاس کوچک ، بعلاوه تست تغییر این فرصت را برای شما فراهم می‌آورد تا هرگونه مشکلی را که در روش‌های توسعه شما وجود دارد، حل کنید.

ایجاد طرح پیشنهادی تغییر

طرح پیشنهادی تغییر، نوع تغییر، اولویت مرتبط با یک درخواست و نتایج حاصل از عدم ایجاد درخواست تغییر را مشخص می‌کند. طرح شما به افرادی که مسئول صدور مجوز تغییر هستند، داده خواهد شد، در نتیجه بسیار اهمیت دارد که شما توضیح کاملی از علت نیاز به ایجاد تغییر را ارائه دهید. برای مثال، یک تغییر با اولویت بالا که ممکن است باعث بروز خرابی هایی شود که بر مشتریان تاثیر گذاشته و منجر به هدر رفتن سرمایه شود. درصورتیکه که شما کاری انجام ندهید، افرادی که مجوز تغییرات را صادر می‌کنند، باید از شدت تاثیر آنها آگاهی داشته باشند.

پیاده سازی تغییرات

پیاده سازی تغییر، فرآیند ساده ای نیست. تغییر باید در طول فرآیند برنامه ریزی ایجاد شود و پیاده سازی تنها یک مرحله از فرآیند مدیریت تغییر (change management process)است. هنگامی که تغییری ایجاد می‌شود، باید تست‌هایی انجام شود تا تعیین شود که آیا نتایج مورد نظر به دست آمده است یا خیر. اگر تغییر موفقیت آمیز نباشد، ممکن است یکسری روش های اصلاحی جهت مشخص شدن اشتباهی که رخ داده و اجرای برنامه پشتیبان گیری برای رفع مسائلی که درخواست تغییر را ضروری می سازد، مورد استفاده قرار دهد.

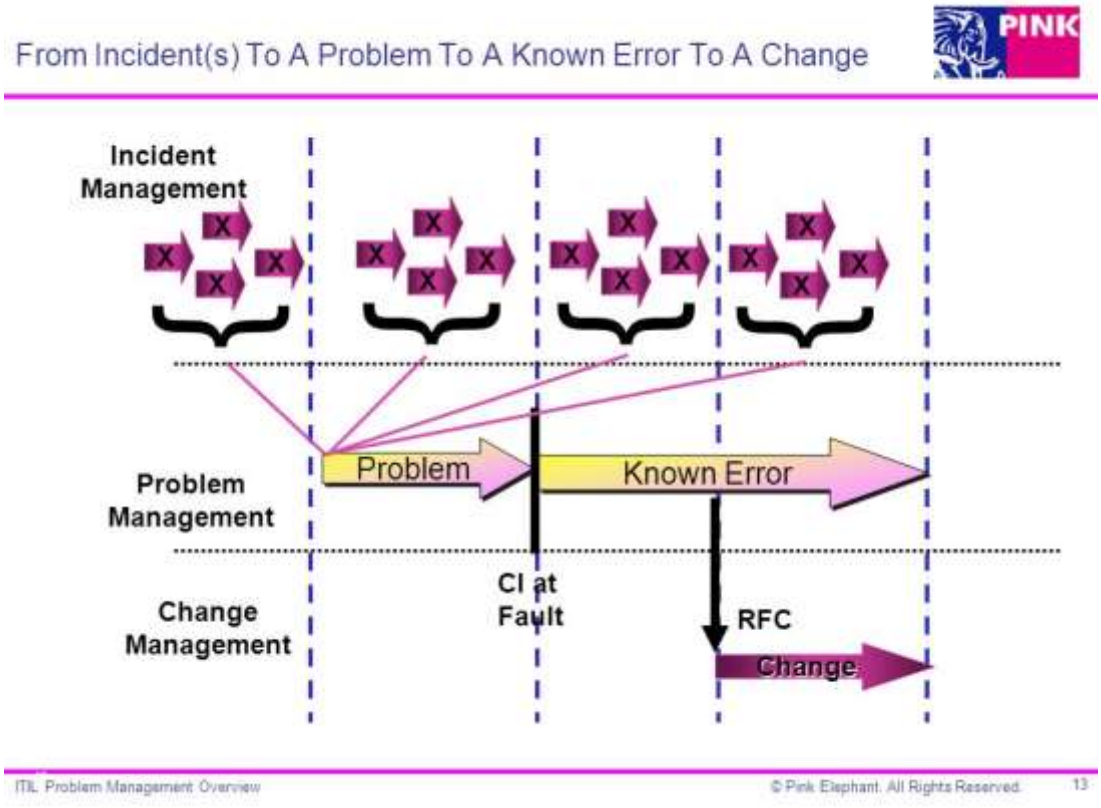
بازبینی عملکرد تغییر

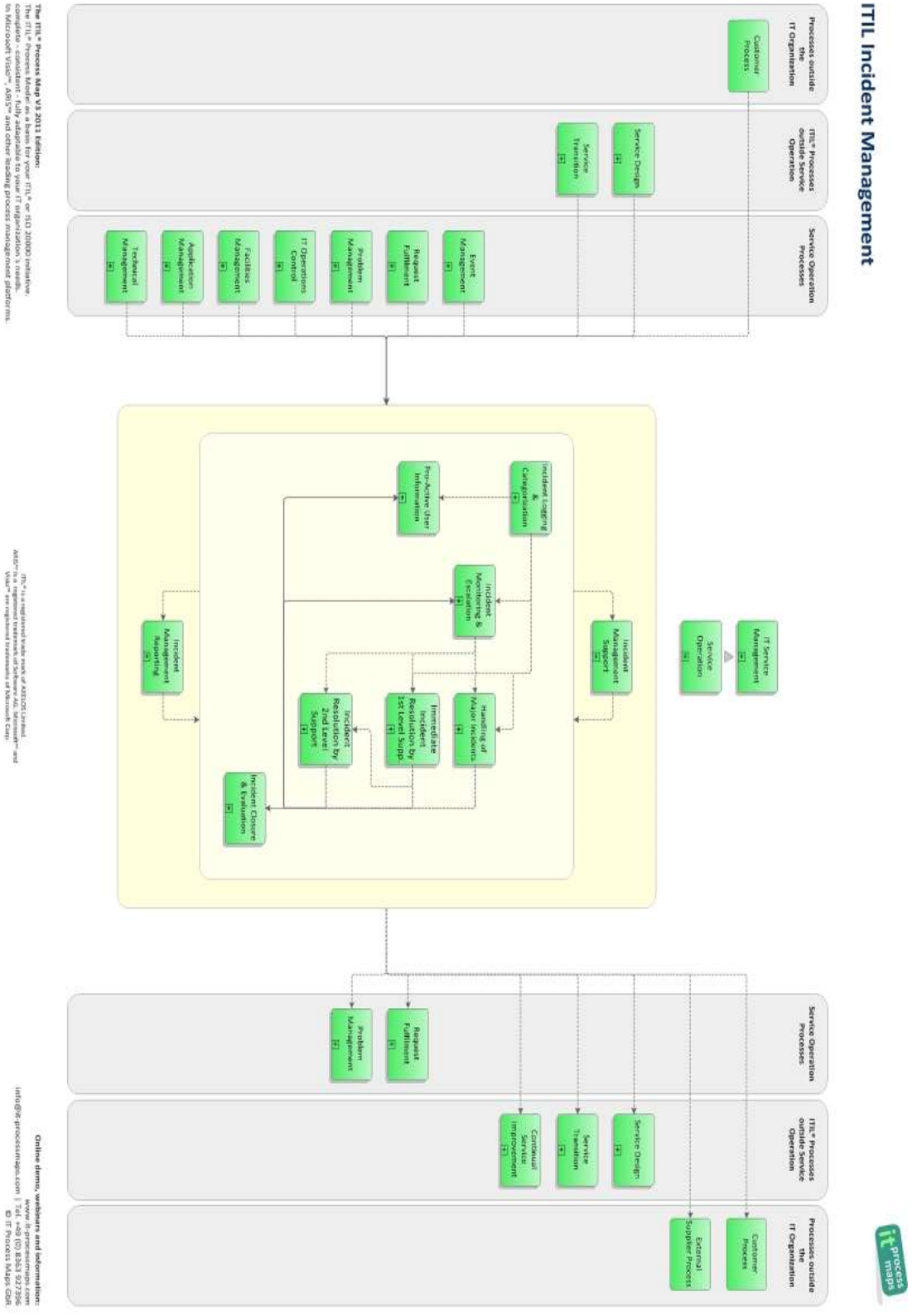
بازبینی بعد از پیاده سازی بخش مهمی از فرآیند مدیریت تغییر است. شما به عنوان یک کارشناس IT می‌خواهید بدانید که آیا روال‌های تغییر شما آنچنان که انتظار می‌رود، کار می‌کنند. این شامل بازبینی رکوردها برای تعیین اینکه آیا تغییر موفقیت آمیز بوده یا شکست خورده است و ذخیره جزئیات در خصوص زمان و هزینه تغییر برای تعیین صحت تخمین‌هایی که پیش از انجام تغییر . بازبینی عملکرد تغییر به شما این امکان را می‌دهد که فرآیند مدیریت تغییر خود را برای کسب نتایج بهتر در آینده، بهینه سازی کنید.

بستن فرآیند

پس از تکمیل فرآیند تغییر، باید اطمینان حاصل کنید که کل فرآیند در داخل پایگاه داده ثبت شده است و همه ذینفعان می‌توانند به آن دسترسی داشته باشند. هنگامی که این مستندات تکمیل شدند، فرآیند بسته می‌شود.

نکته خیلی مهم: در فرایند تغییر در صورتی که تغییر موفقیت آمیز نبود سیستم باید امکان roll back داشته باشد


From Incident(s) To A Problem To A Known Error To A Change
PINK
Incident Management
Problem Management
Change Management
Problem
Known Error
CI at Fault
RFC
Change
ITIL Problem Management Overview
© Pink Elephant. All Rights Reserved.
13


ITIL Incident Management
Processes outside the IT Organization
Customer Process
ITIL® Processes outside Service Operation
Service Design
Service Transition
Service Operation Processes
Event Management
Request Fulfilment
Problem Management
IT Operations Control
Facilities Management
Application Management
Technical Management
IT Service Management
Service Operation
Incident Management Support
Incident Logging & Categorisation
Pro-Active User Information
Incident Monitoring & Escalation
Handling of Major Incidents
Immediate Incident Resolution by 1st Level Supp.
Incident Resolution by 2nd Level Support
Incident Management Reporting
Incident Closure & Evaluation
Service Operation Processes
Problem Management
Request Fulfilment
ITIL® Processes outside Service Operation
Continual Service Improvement
Service Transition
Service Design
Processes outside the IT Organization
External Supplier Process
Customer Process
The ITIL® Process Map V3 2011 Edition:
Online demos, webinars and information:
www.it-processmaps.com
info@it-processmaps.com | Tel: +49 (0) 8153 927356
© IT Process Maps GbR

4 شاخص کلیدی عملکرد فناوری اطلاعات

شاخص کلیدی عملکرد یک معیار برای سنجش موفقیت هر کسب‌وکاری است. بنابراین ساختن آن می‌تواند شما را یک گام به اهداف خود نزدیک‌تر کند.

شاخص کلیدی عملکرد، یک متغیر قابل اندازه‌گیری است که نشان می‌دهد یک شرکت تا چه اندازه به اهداف کلیدی خود نزدیک شده است. این شاخص میزان عملکردهای مهم و اساسی شرکت را ارزیابی می‌کند. درواقع سازمان‌ها از این شاخص برای ارزیابی موفقیت‌هایی استفاده می‌کنند که آن‌ها را یک قدم به اهدافشان نزدیک‌تر می‌کند. شاخص KPI برای تمامی صنایع، سازمان‌ها و حتی کارهای شخصی می‌تواند استفاده شود. این شاخص باید در دوره‌های زمانی مشخص ارزیابی شود و با معیارهای عملکرد در زمان گذشته مورد مقایسه قرار بگیرد.

شرکت‌ها بدون اندازه‌گیری و بررسی شاخص کلیدی عملکرد، هیچ بازخورد مناسبی از نحوه‌ی عملکرد خود نخواهند داشت. شاید بعد از گذشت مدتی احساس کنند که در کار خود پیشرفت کرده‌اند، اما نمی‌توانند زمینه‌ی موفقیت را به درستی مشخص کنند یا آن را توسط یک معیار مناسب بسنجند. شما با استفاده از KPI می‌توانید اهداف دقیقی را برای خودتان مشخص کرده و استراتژی‌های مناسبی را برای ارزیابی آن‌ها مشخص کنید. همچنین این امکان برای شما فراهم می‌شود که تاریخچه‌ای از عملکرد کسب‌وکار خود به دست آورید و ذخیره کنید.

بررسی شاخص کلیدی عملکرد نیز به اندازه‌ی دیگر کارهای شرکت مهم و حیاتی است. گاهی اوقات شرکت‌ها از شاخص‌های کلیدی عملکرد شناخته شده در صنعت استفاده می‌کنند. سپس متوجه می‌شوند که این شاخص نمی‌تواند جوانب کاری آن‌ها را در نظر بگیرد. درنتیجه نمی‌تواند هیچ تغییر مثبتی در روند کارهای شرکت داشته باشد. یکی از مهم‌ترین مشخصات KPI این است که آن‌ها نوعی از ارتباطات هستند. درنتیجه مانند هر ارتباطات دیگری از قوانین خاصی تبعیت می‌کنند. هرچقدر اطلاعات شفاف و واضح‌تر باشند، نتیجه‌ی به دست آمده نیز قابل فهم‌تر می‌شود.

اعضای تیم شما برای ساختن یک KPI باید با اطلاعات پایه و اولیه شروع کنند. این افراد باید اطلاعات خوبی از اهداف سازمان و برنامه‌ریزی حرکت به سمت آن‌ها داشته باشند. ساختن KPI یک فرآیند تعاملی است که باید در تمام مراحل ساخت آن از تحلیل‌گران و مدیران بازخورد گرفته شود.

چگونه شاخص کلیدی عملکرد بسازیم؟

در این بخش به معرفی ۵ گام کلیدی در مراحل ساخت یک KPI قابل اندازه‌گیری می‌پردازیم. همان‌طور که پیش‌تر گفتیم KPI برای هر نوع کسب‌وکاری می‌تواند استفاده شود. ما در این ۵ مرحله KPI مورد نظر برای سنجش عملکرد وب‌سایت را در نظر گرفته‌ایم.

مرحله‌ی اول: مشخص کردن اهداف

قبل از اینکه ترافیک وب‌سایت را اندازه‌گیری کنیم، بهتر است که هدف ساخت وب‌سایت را برای خودمان روشن کنیم. شاید انجام این کار غیرضروری به نظر برسد. اما معمولا وب‌سایت‌ها با ۲ هدف ساخته می‌شوند: افزایش فروش یا کاهش هزینه‌ی حمایت از مشتری. در ادامه به معرفی مثال‌هایی از هر ۲ هدف می‌پردازیم:

افزایش میزان فروش:

- تولید لید

- شناساندن برند
- فروشگاه اینترنتی
- شبکه‌ی اجتماعی
- سرگرمی

این سایت‌ها میزان درگیری کاربران و درنتیجه فروش محصولات را افزایش می‌دهند. شاید این سایت‌ها محصولات خود را مستقیما از طریق از وب‌سایت به فروش نرسانند، اما میزان شناسایی و درگیری برند را افزایش می‌دهند. درنتیجه میزان شناخت مردم از برند بیشتر شده و فروش محصولات بالا می‌رود.

کاهش قیمت‌ها:

- آموزش مشتری‌ها
- سلف سرویس
- سرویس مشتری
- اطلاعات
- اینترانت

این سایت‌ها امکان انتشار اطلاعات و پاسخ دهی آنلاین را فراهم می‌کنند تا میزان هزینه‌ی حمایت از مشتری‌ها را کاهش دهند. مطمئنا نوشتن یک صفحه اطلاعات هزینه‌ی بسیار کمتری نسبت به استخدام چند فرد متخصص برای حمایت از مشتری‌ها دارد.
داشتن درک درست از هدف راه‌اندازی وب‌سایت، به اندازه‌گیری میزان فعالیت وب‌سایت و بهبود عملکرد آن کمک می‌کند. اندازه‌گیری یکسری معیارها نیز به مرور زمان کمک می‌کنند که ببینیم بخش‌های مختلف سایت تا چه اندازه بهبود پیدا کرده‌اند. از آنجایی که هیچ گزارش تحلیلی نمی‌تواند اطلاعات کاملی از نزدیکی شما به اهدافتان بدهد، بنابراین خودتان باید یکسری از معیارها را زیر نظر داشته باشید. برای روشن‌تر شدن این موضوع ۲ مثال زیر را در نظر گرفته و مراحل ساخت KPI را روی آن‌ها توضیح می‌دهیم:

- **مثال A**: افزایش میزان فروش
- **مثال B**: کاهش هزینه‌ی حمایت از مشتری‌ها

مرحله‌ی دوم: مشخص کردن فاکتورهای موفقیت یا CSF

فاکتورهای موفقیت، تعدادی از فعالیت‌های کلیدی هستند که یک شرکت، سازمان یا حتی یک فرد برای رسیدن به موفقیت باید روی آن‌ها تمرکز کند. فاکتورهای موفقیت شرایط مشخص شده‌ای هستند که میزان دسترسی به اهداف یک کسب‌وکار را در بازه‌های زمانی اندازه‌گیری می‌کنند. یک CFS خوب با یک فعل عملی آغاز می‌شود و سپس چیزهای که باید مورد توجه قرار بگیرد را مشخص می‌کند. این افعال عبارت‌اند از: جذب کردن، اجرا کردن، گسترش دادن، نظارت کردن، مدیریت کردن و افعال مشابه دیگر. فاکتورهای موفقیت همیشه ۲ عنصر را باهم ترکیب می‌کنند: فعالیت قابل اندازه‌گیری و بازه‌ی زمانی مشخص.

- مثال A: افزایش دادن میزان لیدها به اندازه‌ی ۲۵ درصد در بازه‌ی زمانی ۱۲ ماه
- مثال B: کاهش دادن میزان تماس‌های مرکز پشتیبانی به اندازه‌ی ۲۰ درصد در بازه‌ی زمانی ۱۲ ماه

مرحله‌ی سوم: درست کردن KPI از روی فاکتورهای موفقیت

همه‌ی فاکتورهای موفقیت لزوما KPI نیستند. فاکتورهای موفقیت عناصر ضروری برای موفقیت یک استراتژی هستند. در حالی که KPI ها معیارهای محاسبه شده‌ای هستند که کمیت فاکتورهای موفقیت را تعیین می‌کنند. شاخص‌های کلیدی عملکرد، محاسباتی از متریک‌ها هستند که در مراحل بعدی مشخص می‌شوند. شاخص کلیدی عملکرد در مرحله‌ی سوم شناخته می‌شود اما محاسبات آن در مرحله‌ی پنجم انجام می‌شود. در ۲ مرحله‌ی بعدی متوجه خواهید شد که معیارها و متریک‌های زیادی برای سنجش وجود دارند. اما تنها تعداد کمی از این متریک‌ها اطلاعات مفیدی از عملکرد وب‌سایت را در اختیار ما قرار می‌دهد. تنها متریک‌هایی می‌توانند اطلاعات مفید به ما بدهند که KPI باشند. فراموش نکنید که تمام KPI ها متریک هستند اما همه‌ی متریک‌ها KPI نیستند. البته این مفهوم بعد از خواندن مراحل چهارم و پنجم کامل‌تر می‌شود.

- KPI مثال A: درصدی از بازدیدکننده‌ها که در یک ماه اخیر تبدیل به مشتری برند شده‌اند
- KPI مثال B: نسبت تماس با مرکز خدمات مشتری در مقایسه با نرخ یک ماه گذشته

حال که KPI ها مشخص شدند باید معیارهای سازنده‌ی این KPI ها را مشخص کنیم. مثال A درصدی از بازدیدکننده‌ها هستند که تبدیل به مشتری برند شده‌اند. بنابراین ابتدا باید این معیارها و محاسبات لازم برای مشخص کردن آن‌ها را پیدا کنیم. در مثال B ما باید معیارها مرتبط با مرکز تماس و پشتیبانی آنلاین مشتری‌ها را جمع‌آوری کنیم.

مرحله‌ی چهارم: جمع‌آوری معیارها

معیارها یکسری اعداد خام هستند که می‌توان اطلاعات مفیدی را از آن‌ها استخراج کرد. این معیارها اگر به هم ربط داده شوند، می‌توانند اطلاعات مفیدتری را استخراج کنند. معیارها، پایین‌ترین سطح جزئیات در گزارش‌های تحلیلی وب‌سایت‌ها، پایگاه داده‌ی شرکت‌ها و گزارشات مرکز تماس هستند. ابتدا معیارها باید جمع‌آوری شوند تا ما بتوانیم متریک‌ها را در مرحله‌ی پنجم مشخص کنیم. این معیارها به یک اندازه برای مثال A و B ارزش دارند:

- تعداد بازدید از صفحات
- تعداد بازدیدکنندگان
- تعداد دانلودها
- تعداد تماس‌های روزانه با مرکز پشتیبانی
- داده‌ی کمپین‌ها (مانند تبلیغات کلیکی)

مرحله‌ی پنجم: محاسبه‌ی متریک‌ها از روی معیارها

متریک‌ها محاسباتی از معیارها هستند و همیشه به‌عنوان نرخ، میانگین، نسبت یا درصد بیان می‌شوند. ما می‌توانیم معیارها را به روش‌های مختلف تحلیل کنیم در نتیجه بی‌نهایت متریک خواهیم داشت. متریک‌ها همچنین با یک بازه‌ی زمانی تعریف می‌شوند. همان‌طور که در مرحله‌ی سوم گفتیم، تمام KPI ها متریک هستند اما همه‌ی متریک‌ها KPI نیستند. یک متریک برای اینکه بتواند به KPI تبدیل شود باید اطلاعات مفیدی از عملکرد سایت در اختیار ما قرار دهد. ۲ متریکی که در مثال A و B بررسی کردیم را در نظر بگیرید:

- درصد بازدیدکنندگانی که طی یک ماه اخیر تبدیل به مشتری شده‌اند (KPI مثال A)
- نسبت تماس‌های مرکز پشتیبانی آنلاین در مقایسه با یک ماه اخیر (KPI مثال B)
- تعداد صفحه‌های بازدید شده در هر بازدید در مقایسه با بازه‌ی زمانی قبلی
- تعداد خریدها به ازای هر بازدید در مقایسه با بازه‌ی زمانی قبلی
- نرخ تبدیل بازدیدکننده‌ها به مشتری
- درصد بازدیدکننده‌های جدید در مقایسه با بازه‌ی زمانی قبلی
- مدت زمان حضور هر بازدیدکننده در مقایسه با بازه‌ی زمانی قبلی
- انجام سرویس‌های آنلاین در مقایسه با تماس‌های مرکز خدمات پشتیبانی

مثال A

KPI مثال A درصد تبدیل بازکننده به مشتری است. بنابراین اگر میزان آن از ۸ درصد به ۱۰ درصد تغییر کند، یعنی وب‌سایت ما نرخ تبدیل خوبی داشته است. این موضوع یعنی میزان فروش نیز در آینده بالا خواهد رفت.

مثال B

KPI مثال B نسبت تماس‌های خدمات مشتری آنلاین در مقایسه با تماس‌های ماه گذشته است. اگر این نسبت کاهش پیدا کند یعنی خدمات بیشتری از طریق پشتیبانی آنلاین به مشتری‌ها داده می‌شود. این یعنی سایت شما عملکرد خوبی داشته و هزینه‌ی پشتیبانی کاهش پیدا خواهد کرد.

تفاوت متریک و معیار

تفاوت متریک و معیار:

- تعریف متریک: متریک یک معیار قابل اندازه‌گیری است که برای ارزیابی و پیگیری یک فرآیند خاص مورد استفاده قرار می‌گیرد.
- تعریف معیار: معیارها اعداد یا ارزش‌هایی هستند که می‌توانند جمع زده شوند یا میانگین گرفته شوند. مانند فروش، فاصله، مدت زمان، دما و وزن.
- تفاوت: معیار، یک اصل بنیادی یا یک اصطلاح خاص است. یک متریک می‌تواند از یک یا تعداد بیشتری معیار تشکیل شود. به همین دلیل لغت متریک، هدف و عملکرد دقیق‌تری دارد.

شاخص کلیدی عملکرد یا KPI

شاخص :

یک نشانه که به شما در مورد یک وضعیت اطلاعات می دهد و توجه شما را به آن جلب می کند . معمولا یک عدد ، درصد یا کد رنگ است که سریعا شما را از وجود یک خواستنی یا ناخواستنی را آگاه می سازد .

کلیدی :

یک جنبه مهم و حیاتی . به این معنی که شما باید اولویت بندی کنید . گرچه به این معنی نیست که باید چیزی را روی لیست کارها جا بیاندازید . هرچیزی که قابلیت اندازه گیری شدن داشته باشد را نمیتوان به عنوان یک متریک کلیدی در نظر گرفت .با یک عدد قابل مدیریت شروع کنید . معمولا سازمان ها بین 3 تا 7 شاخص کلیدی عملکرد تعریف می کنند .

عملکرد :

رفتاری که در آن موردی فعالیت ،کارکردی و یا برخوردی دارد . درست مثل عملکرد موتور که فقط با میزان مصرف سوخت در هر کیلومتر اندازه گیری نمی شود ، عملکرد یک شرکت هم فقط با متریک های سود شرکت بررسی نمی شود .

شاخص های کلیدی عملکرد (KPI)

یکی از پرکاربردترین مفاهیم در کسب وکار و مدیریت هستند . بسیار معمول است که هر متریک یا داده ای را زبان مدیریت ترجمه میکنیم . اما نقش KPI خیلی کلیدی تر و مهم تر است . در حقیقت KPI یکی از مهم ترین نقاط راهبری کسب و کار است .

بهترین تعریف KPI:

KPI ها کارت های امتیاز دهی هستند که به شما کمک می کنند استراتژی خود را در مسیر مشخص راهبری کنید . آنها برای شما امکان مدیریت ، کنترل و رسیدن به نتیجه دلخواه را فراهم می کنند .

داشبورد KPI:

برای نگه داری کل کسب و کارتان بر روی مسیر استراتژی از پیش تعیین شده باید از داشبورد KPI استفاده کنید .داشبورد KPI ارائه گرافیکی مناسب از تمام شاخص های کلیدی عملکرد تعریف شده و یا مهم شما است که وضعیت در لحظه موضوع مورد بررسی و میزان فاصله تان تا مقدار هدف را در کمتر از 30 ثانیه به شما نشان می دهد . لازم نیست تعداد زیادی KPI را انتخاب کنید فقط باید با دقت انتخاب کنید ، در زمان های مناسب به صورت دوره ای ارزیابی کنید و برای بهبود وضعیت تلاش کنید .

چطور KPI انتخاب کنیم ؟

- نتیجه دلخواه تان را شناسایی کنید :

همیشه با شناخت کامل بر خواسته ها و ایده آل هایتان شروع به ساخت KPI کنید . مشکلی نداره که فقط بگید : " می خواهم بیشتر بفروشم " ، اما سعی کنید دقیق تر باشید. چگونه اینکار را انجام می دهید ؟ آیا چرخه فروش خود را نصف می کنید ؟ آیا 50٪ بیشتر مخاطب جذب میکنید ؟ آیا موقعیت مصرف جدیدی ایجاد می کنید ؟ آیا مشتری های وفادار خود را مجبور می کنید 30 ٪ بیشتر خرید کنند ؟ اگر در مورد کاری که می خواهید انجام دهید مطمئن باشید آنگاه می توانید KPI تولید کنید .

- کارت های امتیاز : حالا باید تعدادی متغیر و فاکتور کمی با کیفی انتخاب کنید (معمولا کمتر از 6 تا) که بنا به تشخیص شما مهم ترین عوامل برای رسیدن به اهدافتان هستند .

برای مثال : اگر در مدیریت فروش کسب و کار آنلاین خود می خواهید چرخه فروش را نصف کنید می توانید موارد زیر را بررسی کنید :

- کلمات کلیدی (مواردی که توضیح دهنده ی نیاز هاییست که برند شما تامین می کند)
- تعداد بازدید کنندگان خاص وبسایت
- "bounce rate " وبسایت برای فهمیدن آنکه آیا وبسایت شما مرتبط هست ؟آیا افراد بیش از یک صفحه را بازدید می کنند ؟

- فروش
- میانگین ارزش مشتریان – از آنجایی که خرید بیشتر نشان دهنده ی نزدیک شدن شما به هدفتان است.

4.1 نقاط کلیدی عملکرد [1] (Key Performance Indictors-KPIs)

واحد مدیریت فناوری اطلاعات بر مبنای بهروش های APQC

نام حوزه فرآیندی	مدیریت فناوری اطلاعات
گروه‌های فرآیندی	فرآیندها
مدیریت کسب‌وکار فناوری اطلاعات (فاوا)	1. توسعه استراتژی فناوری اطلاعات سازمان
	2. تعریف معماری سازمانی
	3. مدیریت سبد فاوا
	4. انجام تحقیقات و نوآوری فاوا
	5. ارزیابی و اطلاع رسانی ارزش و عملکرد کسب وکاری فناوری اطلاعات
توسعه و مدیریت ارتباطات مشتری فناوری اطلاعات	6. توسعه استراتژی سرویس ها و راهکارهای فاوا
	7. توسعه و مدیریت سطوح سرویس فاوا
	8. مدیریت تقاضا برای خدمات فاوا
	9. مدیریت رضایتمندی مشتریان فاوا
	10. ارزیابی خدمات و راهکارهای فاوا
توسعه و پیاده سازی امنیت، محرمانگی، کنترل و حفاظت داده	11. استقرار راهبردها و سطوح امنیت اطلاعات، محرمانگی و حفاظت داده ها
	12. آزمون، ارزیابی و پیاده‌سازی امنیت اطلاعات و محرمانگی و کنترل های حفاظت داده ها
مدیریت اطلاعات سازمان	13. توسعه راهبردهای مدیریت اطلاعات و محتوا
	14. تعریف معماری اطلاعات سازمان
	15. مدیریت منابع اطلاعاتی
	16. مدیریت ترک کار
	17. مدیریت داده و محتوای سازمان
توسعه و نگهداشت راهکارهای فناوری اطلاعات	18. تدوین راهبرد توسعه فناوری اطلاعات
	19. برنامه‌ریزی چرخه عمر خدمات و راهکارهای فاوا
	20. توسعه و نگهداری معماری خدمات و راهکارهای فاوا

[1] برای اندازه گیری عملکرد واحد فاوا سازمان

	21. ایجاد خدمات و راهکارهای فاوا
	22. نگهداری و پشتیبانی خدمات و راهکارهای فاوا
استقرار راهکارهای فناوری اطلاعات	23. توسعه راهبرد استقرار فاوا
	24. برنامه ریزی و پیاده سازی تغییرات
	25. برنامه ریزی و مدیریت استقرار راهکارها
ارائه و پشتیبانی خدمات فناوری اطلاعات	26. توسعه راهبرد ارائه خدمات و راهکارهای فاوا
	27. تدوین استراتژی پشتیبانی فاوا
	28. مدیریت منابع زیرساختی فاوا
	29. مدیریت عملیات زیرساخت فاوا
	30. پشتیبانی خدمات و راهکارهای فاوا

5 مدیریت شبکه‌های کامپیوتری

مدیریت شبکه‌های کامپیوتری مجموعه‌ای از فعالیت‌ها، روش‌ها، فرآیند و ابزراهایی است که به بهبود عملکرد شبکه کمک کرده و باعث افزایش کارایی آن می‌شود. این فعالیت‌ها می‌توانند توسط نیروی انسانی انجام شده و یا به صورت هوشمند و توسط سیستم‌های کامپیوتری صورت گیرد.

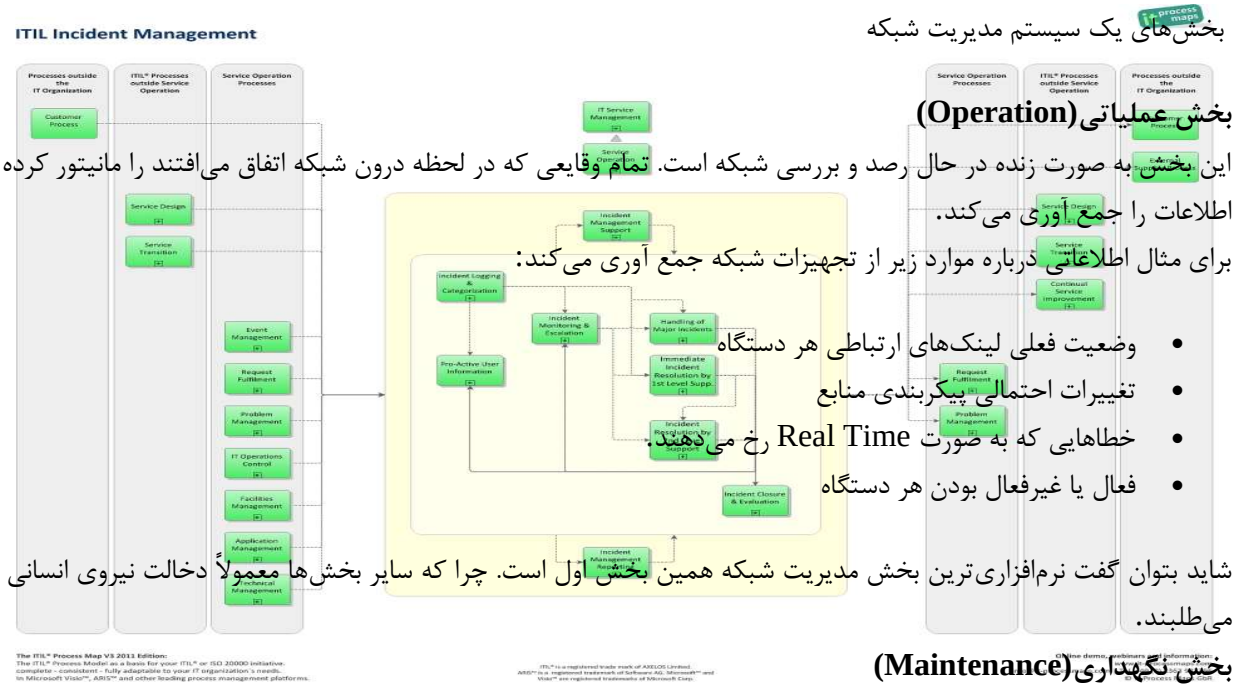
مجموعه‌ای از فعالیت‌ها و روش‌ها که هدف آن‌ها صحت عملکرد شبکه می‌باشد را مدیریت شبکه می‌نامند.

قبل از مدیریت شبکه، نیاز است کنترل شبکه نیز انجام شود. کنترل شبکه به معنای مانیتور کردن تجهیزات یک شبکه است. عملیات مانیتور کردن می‌تواند به صورت فعال (Active) یا منفعل (Passive) انجام گیرد.

5.1 ساختار مدیریت شبکه کامپیوتری

همانطور که گفته شد، مدیریت شبکه مجموعه‌ای از فرآیندها و کارهاست. گاهی این فعالیت‌ها را برای درک بهتر به سه بخش جداگانه تقسیم‌بندی می‌کنند.

بخش‌های یک سیستم مدیریت شبکه



بخش عملیاتی(Operation)

این بخش به صورت زنده در حال رصد و بررسی شبکه است. تمام وقایعی که در لحظه درون شبکه اتفاق می‌افتند را مانیتور کرده و اطلاعات را جمع آوری می‌کند.

برای مثال اطلاعاتی درباره موارد زیر از تجهیزات شبکه جمع آوری می‌کند:

- وضعیت فعلی لینک‌های ارتباطی هر دستگاه
- تغییرات احتمالی پیکربندی منابع
- خطاهایی که به صورت Real Time رخ می‌دهند.
- فعال یا غیرفعال بودن هر دستگاه

شاید بتوان گفت نرم‌افزاری‌ترین بخش مدیریت شبکه همین بخش اول است. چرا که سایر بخش‌ها معمولاً دخالت نیروی انسانی را می‌طلبند.

بخش نگهداری(Maintenance)

بخش نگهداری دو وظیفه اصلی دارد.

1. هنگامی که بخش اول به وجود آمدن مشکلی را به سیستم گزارش می‌کند، بخش نگهداری می‌بایست اقدام به رفع مشکل پیش آمده در شبکه کند.
2. در هنگام گسترش شبکه، نیاز به راه اندازی و پیکربندی تجهیزات جدید در شبکه خواهد بود. فرآیندهای مورد نیاز برای افزودن تجهیزات جدید جزء وظایف این بخش است.

بخش تدارکات(Provisioning)

وظیفه این بخش از مجموعه فرآیندهای مدیریت و کنترل شبکه، تحقیق و توسعه امکانات و تجهیزات شبکه است. از آن‌جا که شبکه‌های کامپیوتری هر روز در حال توسعه و پیشرفت هستند و تکنولوژی‌های موجود در این زمینه نیز رو به رشد هستند، لازم است شبکه را توسعه داده و یا با بهترین فناوری‌ها به‌روزرسانی کنیم.

شاخص های اصلی عملکرد مبتنی بر ITIL v3 برای مدیریت رخدادها

ITIL v3 Suggested Incident Management KPIs

شاخص KPIs	تعریف Definition
میانگین زمان پاسخ اولیه Average Initial Response Time	میانگین زمانی بین زمانیکه کاربر یک حادثه گزارش می دهد و زمانی که میز خدمت پاسخ می دهد گرفته می شود. Average time taken between the time a user reports an Incident and the time that the Service Desk responds to that Incident
تعداد رخدادها Number of Incidents	تعداد حوادث ثبت شده توسط میز خدمت Number of incidents registered by the Service Desk گروه بندی به شاخص ها grouped into categories
زمان حل یک رخداد Incident Resolution Time	میانگین زمان برای حل یک حادثه Average time for resolving an incident گروه بندی به شاخص ها grouped into categories
تعداد تکرار رخدادها Number of repeated Incidents	تعداد رخدادهای مکرر، با روش های حل شناخته شده است. Number of repeated Incidents, with known resolution methods
رخداد های حل شده است از راه دور Incidents resolved Remotely	تعداد رخدادهای حل شده است از راه دور توسط سرویس میزبان (بدون انجام کار در محل کاربر). Number of Incidents resolved remotely by the Service Desk (i.e.without carrying out work at user's location).
تعداد تعدیل رخدادها (ارجاع به سطح بالا) Number of Escalations	تعداد تعدیل رخدادهاکه در زمان توافق حل نشده است Number of escalations for Incidents not resolved in the agreed resolution time
نرخ رفع رخداد برای بار اول First Time Resolution Rate	درصد رخدادهای که در مراجعه اول به سرویس میزبان حل و فصل شد Percentage of Incidents resolved at the Service Desk during the first call گروه بندی به شاخص ها grouped intocategories.
حل فصل رخداد ها طبق قطعنامه SLA قرارداد تضمین سرویس Resolution within SLA	نرخ رخدادها رفع شده در مدت زمان حل و فصل حوادث طبق توافق در SAL Rate of incidents resolved during solution times agreedin SLA گروه بندی به شاخص ها grouped into categories.

میزان تلاش برای حل رخداد Incident Resolution Efforts	میانگین تلاش برای حل رخداد Averge work effort for resolving incidents گروه بندی به شاخص ها grouped into categories

شاخص های اصلی عملکرد مبتنی بر ITIL v3 برای مدیریت تغییرات

Suggested Change Management KPIs 3ITIL v

درصد وقفه ناشی از تغییرات (عدم دسترسی برنامه ریزی شده) ٪ of outage due to changes (planned unavailability)	درصد قطع (عدم دسترسی) به دلیل اجرای تغییرات برنامه ریزی شده، نسبت به ساعات سرویس. Percentage of outage (unavailability) due to implementation of planned changes, relative to the service hours
درصد درخواستهای تغییر باقیمانده / نادیده گرفته شده ٪of backlogged/neglected change requests	درخواستهای تغییری باقیمانده است که باید انجام شود اما به دلیل محدودیت های زمان / هزینه هنوز هم برجسته است. Backlogged change requests are change requests that should have been implemented but due to for example time/cost constraints are still outstanding
میانگین مدت زمان بستن هر تغییر Average change closure duration	میانگین زمان بین ثبت نام تغییرات و بسته شدن آنها(به عنوان مثال در روز) Average amount of time between the registration of changes and (their closure. (e.g. in days
درصدی از تغییرات خارج از برنامه ریزی شده پنجره تعمیر و نگهداری ٪ of changes scheduled outside maintenance window	درصد تغییرات خارج ازبرنامه ریزی شده هر پنجره تعمیر و نگهداری از پیش تعیین شده یا توافق.شده است . یک پنجره تعمیر و نگهداری زمان از پیش تنظیم شده است، که یک سیستم درصورت می تواند خارج از خط برای تعمیر و نگهداری داشته باشد. Percentage of changes scheduled outside pre-defined/pre-agreed maintenance window. A maintenance window is a prescheduled time when a system can be taken off-line for maintenance, if necessary.
درصدی از تغییرات فوری ٪ of urgent changes	تعداد تغییرات باز، تغییر فوری نسبت به تعداد کل تغییرات باز شده در یک دوره زمانی معین. این KPIsنشان دهنده میزان خطر بالقوه تغییرات فوری در کیفیت و عملکرد فرایند مدیریت تغییر است Number of opened, urgent changes relative to the total number of changes opened in a given time period. This KPI reflects the size of the potential risk of urgent changes on the quality and performance of the change management process.
درصدی از تغییرات انجام شده غیر مجاز ٪ of unauthorized implemented changes	تعداد تغییرات اعمال شده غیر مجاز نسبت به کل تغییرات اعمال شده در یک دوره زمانی داده شده، تغییرات غیر مجاز را می توان از طریق یکپارچه سازی پایگاه داده مدیریت پیکربندی (CMDB) شناسایی نمود هر تغییر در زیرساخت هایی که تغییری برای آن ثبت نشده غیرقانونی است/ umber of unauthorized implemented changes relative to all implemented changes within a given time period. An

	unauthorized change can be detected through consolidation of the Configuration Management Database (CMDB). A change in infrastructure for which there is not a change registered is considered as unauthorized..
درصدی از قطع برنامه ریزی نشده یا عدم دسترسی برای تغییرات ٪of unplanned outage /unavailability due to changes	درصد قطع ناخواسته (عدم دسترسی) به دلیل اجرای تغییرات در زیرساخت ها. برنامه ریزی نشده به این معنی است که قطع (یا بخشی از قطع) قبل از اجرای تغییر، برنامه ریزی نشده بود. Percentage of unplanned outage (unavailability) due to the implementation of changes into the infrastructure. Unplanned means that the outage (or part of the outage) was not planned before implementation of the change.
درصدی از تغییرات که نیاز به بازگرداندن پشتیبان ٪ of changes that required restoration of backup	درصد تغییرات مورد نیاز برای بازگرداندن پشتیبان در طی اجرای Percentage of changes that required restoration of backup during the implementation.
درصدی از تغییرات بسته انجام نشده ٪ of backed-out changes	تعداد تغییرات بسته شده که انجام نشده و یا برگشت داده شده نسبت به تعداد کل تغییرات بسته شده در یک دوره زمانی داده شده Number of closed changes which were not carried out or were rolled back relative to the total number of changes closed in a given time period.
نسبت تعداد حوادث در مقایسه با تعداد تغییرات Ratio of number of incidents versus number of changes	نسبت تعداد حوادث در مقایسه با تعداد تغییرا Ratio of number of incidents versus number of changes
درصدی ازتغییراتی که باعث حوادث می شوند ٪ of changes that cause incidents	تعداد تغییرات اعمال شده که سبب حوادث شده است، نسبت به تمام تغییرات اعمال شده در یک دوره زمانی این پیش نیاز برای KPIs است که حوادث با تغییرات مرتبط هستند. Number of implemented changes that have caused incidents, relative to all implemented changes within a certain time-period. Prerequisite for measuring this KPI is that incidents are correlated to changes.
تغییر نرخ صف Change queue rate	تعداد تغییرات بسته شده است، نسبت به تعداد تغییراتی که در یک دوره زمانی معین باز شده است The number of changes closed, relative to the number of changes opened in a given time period
درصدی از تغییرات عقب افتاده ٪ of overdue changesnges	تعداد تغییرات عقب افتاده (بسته شده و حل نشده در فریم زمان مشخص شده) نسبت به تعداد تغییرات باز بسته نشده اما هنوز هم در فریم زمان پا برجای هستند Number of overdue changes (not closed and not solved within the established time frame) relative to the number of open

	changes (not closed but still within the established time frame).
درصدی از تغییرات اعمال شده که تایید نشده توسط مدیریت یا هیئت مشاوره تغییرات ٪ of implemented changes not approved (by management / CAB	درصد تغییرات پیاده سازی شدکه تصویب نشده توسط مدیریت یا هیئت مشاوره تغییرات به تمام تغییرات اعمال شده در طول دوره اندازه گیری Percentage of implemented changes not approved (by Change Advisory Board or CAB, or management), relative to all implemented changes within the measurement period
درصدی از تغییرات توسط CAB رد شد % of refused changes by CAB	درصد تغییرات رد شده توسط CAB Percentage of refused changes by CAB
درصدی از زمان هماهنگ سازی تغییرات ٪ of time coordinating changes	درصد زمان (در ساعت کار) استفاده می شود برای هماهنگی تغییرات نسبت به تمام زمانهایی که برای پیاده سازی (و هماهنگ کردن) تغییرات استفاده می شود.. Percentage of time (in labour hours) used to coordinate changes relative to all time used to implement (and coordinate) changes
تعداد حوادث ناشی از تغییرات در مقایسه با تعداد حوادث Number of incidents caused by changes versus total number of incidents	تعداد حوادث ناشی از تغییرات در مقایسه با تعداد حوادث. Number of incidents caused by changes versus total number of incidents.
درصدی از حوادث ناشی از اسناد ناقص ٪ of incidents caused by deficient documentation	درصدی از حوادث ناشی از اسناد ناقص و نا کارا Percentage of incidents that are caused by deficient documentation..

شاخص های اصلی عملکرد مبتنی بر ITIL v3 برای مدیریت مشکل
Suggested problem Management KPIs 3ITIL v

تعداد مشکلات Number of problems	تعداد مشکلات ثبت شده توسط مدیریت مشکل Number of Problems registered گروه بندی به دسته بندی مشکلات Grouped into categories
زمان حل مسئله Problem Resolution time	میانگین زمان حل مشکلات Average time for resolving Problems گروه بندی به دسته بندی مشکلات Grouped into categories
تعداد مشکل حل نشده Number of unresolved Problem	تعداد مشکلاتی که علت اصلی آن در یک زمان مشخص شناخته نشده است Number of Problems where the underlying root cause is not known at a particular time
تعداد رخدادها در هر مشکل شناخته شده Number of Incidents per known Problem	تعداد رخدادهای گزارش شده مربوط به هر مشکل شناسائی شده Number of reported Incidents Linked to the same Problem after problem identification
مدت زمان شناسائی یک مشکل Time Until Problem Identification	میانگین زمان اولین وقوع یک رخداد و شناسائی علت اصلی آن Average time between first occurance of an Icident and indentification of the root cause
فعالیت های لازم برای حل مشکل Problem Resolution effort	متوسط تلاش کاری برای حل مشکل Average work effort for resolving Problems گروه بندی مشکلات به دسته بندی های Grpuped into categories

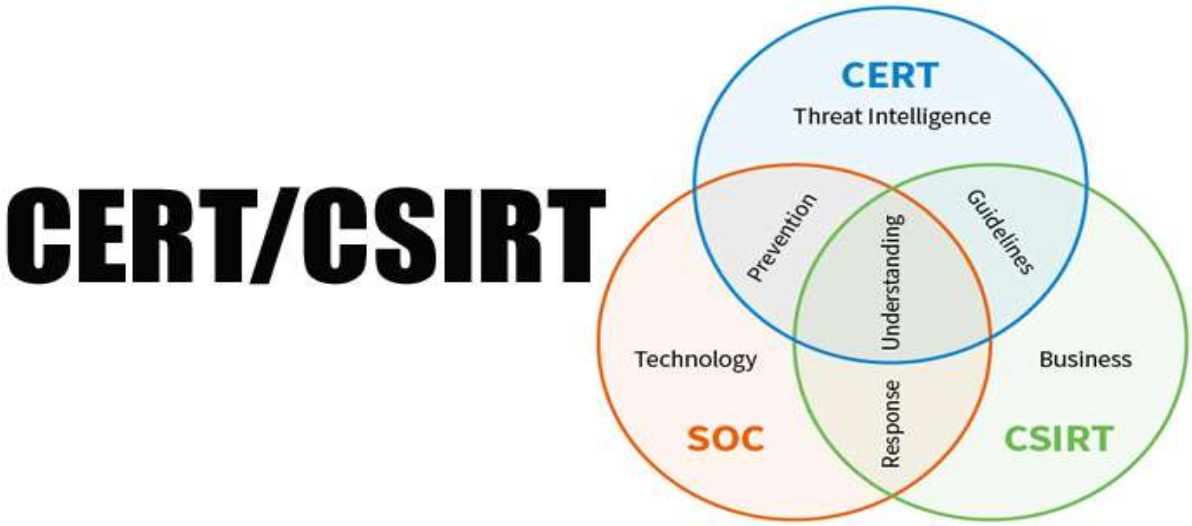
6 روش اجرایی پاسخگویی به رخدادهای رایانه ایی در مرکز ماهر(CERT[2])

امروزه کامپیوترها جزء لاینفک سازمان‌های تجاری و دولتی شده‌اند. بسیاری از دارایی‌های باارزش سازمان‌های دولتی و تجاری در معرض ریسک‌ها و خطرات کامپیوتری هستند که بر روی خطوط اینترنت قراردارند. برای مثال اطلاعات مشتریان ممکن است در معرض خطر سرقت متخلفان قرار گیرد. گستردگی استفاده از دیتابیس‌هایی که اطلاعات افراد را نگهداری می‌کنند، در معرض خطر هستند.

اتکاء ما به اینترنت و انجام مبادلات از طریق آن دائماً در حال افزایش است. متأسفانه حملات سایبری در این محیط روز به روز در حال افزایش است و می‌تواند در عرض چند دقیقه با گسترش در کل شبکه تمام شبکه را تحت تأثیر خود قرار دهد، در نتیجه نیاز به افزایش توانایی در برخورد با این حملات سایبری در میان بخش‌های مختلف کاری بیش از بیش احساس می‌شود.

مرکز امداد و نجات رایانه ای [CERT/CSERT]

سازمان یا تیمی است که خدمات و پشتیبانی‌های لازم را از یک قلمرو تعریف شده برای جلوگیری، بررسی و پاسخگویی به حوادث امنیت رایانه به عمل می‌آورد.



اهداف CERT متناسب با اهداف سازمان و جامعه قلمرو آن تعیین می‌گردد. غالباً محافظت از سرمایه‌های حیاتی اطلاعات به عنوان هدف بنیادین مورد قبول بوده و لذا در صورت وقوع حادثه، حداقل‌کردن خرابی‌ها و کنترل آن، پاسخ موثر، بازیابی اطلاعات و جلوگیری از حوادث مشابه در آینده، بعنوان اهداف اساسی مورد اجماع می‌باشد.

CERT جهت تحقق اهداف فوق اطلاعات جامعی از حوادث، ضعف‌های امنیتی و آسیب پذیری‌های سامانه ها و نرم افزارهای مورد استفاده در زیر ساختهای سازمانی و جامعه قلمرو را جمع آوری می‌نماید و به یک نقطه کانونی و منبعی قابل اعتماد تبدیل می-گردد CERT .بعنوان یک پایگاه مرکزی اطلاعات ، اجازه می‌یابد که کلیه موارد مرتبط با امنیت را در سطح سازمان جمع آوری و

[2] کلمه CERT از ترکیب کلمات Computer Emergency Response Team به معنای گروه پاسخگویی امداد رایانه (آپا) می باشد.

ساماندهی نماید. این امر فرصتی جهت تجزیه وتحلیل و ارتباط دهی کلیه وقایع که هر یک به تنهایی مرتبط به نظر نمی‌رسند را فراهم آورده و نقش CERT را بعنوان یک عنصر کلیدی در حداقل‌کردن تلفات و کاهش مخاطرات ارتقاء می‌بخشد.

CERT ها به روشهای مختلف دسته بندی می‌شوند:

- بر اساس اهداف و وظایف
- بر اساس ساختار سازمانی
- بر اساس قلمرو

گامهای مهم برای ایجاد CERT

1. درک و فهم دست اندرکاران از ایجاد CERT ملی و فراهم کردن محرکهای کاری برای راه‌اندازی.CERT
2. شناسایی کسانی که در بحث های مربوط به ایجاد تیم درگیر خواهند شد، کسانی‌که درگیر توسعه و ارتقای CERTخواهند شد و کسانی که جز تیم تصمیمم گیری و توسعه فرایند خواهند شد.
3. تهیه نقشه نیازمندیهای CERT که شامل مجموعه اطلاعات مشخص بر ساس CERT می‌باشد. قوانینی که کارایی CERT را بهبود می‌بخشد.
4. اعلان عمومی درباره راه اندازی CERT و در نظر گرفتن جایی که اطلاعات جانبی قابل دستیابی باشد (اعلان راجع به تیم، دلایلی برای توسعه، گزارش نیازمندی‌ها).
5. توسعه CERT بر اساس نتایج ارزیابی
6. شرکت در اقدامات مشترک اطلاعاتی و پشتیبانی برای توسعه استانداردها برای اشتراک‌گذاری اطلاعات بین حوزه های نمایندگی دیگر گروه های CERT
7. بهبود کیفیت اقدامات CERT با بهبود روشها، کارآگاه های آموزشی و کنفرانس‌های مهمی که پیرامون روند حمله و استراتژی پاسخگویی بحث می‌کنند.

فرایند ۱: اعلام رخداد توسط کاربران حقیقی یا حقوقی و اعلام حسگرها و سیستم های هانی پات

جمع آوری و ورود اطلاعات اولیه

از طریق ارسال نامه

از طریق اعلام تلفنی

از طریق اعلام سنسورها و حسگرهای نصب شده در زیرشبکه استانهای کشور

فرایند ۲ : فیلترینگ

فیلتر نمودن کلیه ورودی ها و خارج نمودن درخواست های کاذب از طریق اجرای فرایند احراز هویت ، تکمیل نمودن فرم مخصوص پاسخگویی به رخداد و ثبت رخداد.

فرایند ۳: اولویت بندی

تعیین اولویت پاسخگویی به رخدادها بر اساس ضریب اهمیت تعیین شده

فرایند ۴: جستجو در پایگاه اطلاعاتی و رصد واحدی

بررسی پایگاه اطلاعاتی به منظور مشخص شدن تکراری بودن درخواست ، در صورت تکراری

بودن اطلاعات نهایی موجود در پایگاه اطلاعاتی بعنوان راهکار به متقاضی ارائه می گردد

تهیه گزارشات عملکرد

پیمانکار**الف: رصد آسیب پذیریهای حوزه افتا**

۱ -دریافت گزارش اولیه جدیدترین آسیب پذیریها و تهدیدات رایانه ای از منابع معتبر امنیتی داخلی یا خارجی

۲ -بررسی میزان ارتباط و صحت اطلاعات رخداد با سازمانهای مخاطب کشور

۳ -انتخاب گزارشات با اهمیت بیشتر)بر حسب شدت آسیب پذیری و سطح حساسیت سازمانهای مخاطب(جهت تحلیل و ارائه راهکار)

۴ -تحلیل گزارشات مربوط به اسیب پذیری ها و تهدیدات

۵ -تهیه و ارائه گزارشات تحلیل و ابزار تهیه راهکارها

۶ -صحت سنجی و تکمیل راهکارهای ارائه شده

۷ -تعیین مخاطبین سازمانی رخداد شناسایی شده

۸ -تهیه مکاتبات محرمانه مربوط به رخداد و راهکارهای مربوطه

۹ -تایید محتوای مکاتبات مربوط به رخداد و راهکارهای مربوطه توسط مدیر مرکز

۱۱ -پاسخگویی به سوالات و ابهامات ارسال شده از گروه پاسخگویی نسبت به سازمانها در خصوص محتوای گزارشات تکمیلی

۱۱ -درج اتمام هشدار

ب: تحلیل تهدیدات

۱ -دریافت گزارش مربوط به رخدادهای به وقوع پیوسته در سطح کشور از گزارش مراجع امنیتی بین المللی و یا مراجع اطلاعاتی داخلی

۲ -دریافت اطلاعات تکمیلی از مراکز یا سازمانهای هدف با هماهنگی مراجع اطلاعاتی کشور

۳ -تحلیل و صحت سنجی وقوع رخداد با استفاده از گردآوری اطلاعات تکمیلی از مراکز همکار، آپا و سازمانهای هدف و...

۴ -ارجاع رخداد جهت تحلیل دقیق و فنی به مراکز آپا با توجه به حوزه فعالیت و تعیین اولویت زمانی

۵ -بررسی خروجی ها و تایید نتایج

۶ -تعیین احتمال متاثر بودن سازمانها و نهادهای حیاتی و حساس کشور با توجه به نوع رخداد

۷ -آماده سازی زیرساخت ارتباطی سریع با نمایندگان سازمانها

۸ -ارائه نتایج تحلیل اولیه مرکز به سازمانهای هدف و راهکارهای مقابله و کاهش پیامد

۹-دریافت و جمع آوری خروجی ها و نتایج اعمال راهکارها در سازمانها

۱۱ -بررسی و تحلیل مجدد اطلاعات کسب شده به منظور پوشش کامل رخداد و ارائه راهکارهای پاکسازی قطعی با همکاری مراکز اپا

۱۱ -پاسخگویی به سوالات و ابهامات مطرح شده در خصوص راهکارها و گزارشات ارائه شده به سازمانهای هدف

ج: تدوین بولتن

۱ -دریافت اخبار امنیتی به روز در خصوص رخدادهای گزارش شده در سطح بین المللی

۲ -بررسی اخبار مرتبط با دارایی های اطلاعاتی کشور و یا با سطح ریسک بالا

۳ -تحلیل اخبار مرتبط در حوزه افتا

۴ -بررسی تحلیل ها و گزارشات تهیه شده در حوزه اخبار افتا

۵ -تدوین و ویرایش بولتن خبری در خصوص حوزه اخبار افتا

۶ -تایید محتوای بولتن خبری توسط مدیر مرکز

۱۲ -تعیین مخاطبین سازمانی رخداد شناسایی شده

۷ -تهیه مکاتبات محرمانه مربوط به رخداد و راهکارهای مربوطه

د: پاسخگویی

۱ -ارسال مورد پاسخگویی از گروه پاسخگویی

۲ -تحلیل و بررسی مشکل ارسال شده با توجه به الویت زمانی آن

۳ -تدوین اطلاعات تکمیلی درخواستی از سازمان جهت تحلیل بیشتر مشکل و ارائه به مسئول گروه پاسخگویی

۴ -تحلیل بیشتر مشکل مورد بحث با توجه به دریافت اطلاعات تکمیلی

۵ -ارجاع مشکل جهت تحلیل دقیق تر به مراکز آپا) در صورت لزوم)

۶ -ارائه راهکارها و پیشنهادات جهت رفع مشکل به گروه پاسخگویی

و: توصیه نامه

۱.بررسی منابع مطالعاتی در حوزه افتا به منظور استخراج موضوعات و مفاهیم کلیدی و پایه این حوزه

۲.انتخاب موضوع دارای اهمیت بالا در حوزه افتا برای مخاطبین عام

۳.بررسی و جستجوی روشها و راهکارهای تکمیلی در خصوص پوشش آسیب پذیریهای امنیتی

۴.بیان و تبدیل راهکارهای فنی و تخصصی در سطح کاربران عام

۵.تهیه و تدوین توصیه نامه امنیتی در خصوص مشکلات کاربران و راهکارهای پوشش آنها

۶.تایید محتوای توصیه نامه امنیتی

۷.ارسال توصیه نامه امنیتی در سطح سازمان، وزارت و زیر ساخت

فرایند ۵: تحلیل رخداد و آزمایشگاهی

درصورت بروز حمله تیم امداد اقدام به بررسی موضوع می نماید این بررسی می تواند از طریق کنترل IP های مهاجم یا رهگیری مهاجم از طریق شرکتهای میزبانی کننده شبکه صورت پذیرد درصورتیکه فایل بدافزار در اختیار باشد تیم تحلیل بدافزار اقدام به کدخوانی یا رمزگشایی می کند و با تهیه شناسنامه فنی بدافزار آنرا مورد پایش و بررسی قرار می دهند

الف: شناسایی تهدیدات جدید ناشی از انتشار بدافزارها و کدهای مخرب

۱۳ -دریافت نمونه از شبکه هانی نت ملی

۱۴ -دریافت نمونه از طریق وبسایت مرکز

۱۵ -نمونه برداری از سطح سازمانها و فضای سایبری کشور

۱۶ -دریافت نمونه بدافزارها و کدهای مخرب از طرق ارتباطی مختلف

۱۷ -تحلیل نمونه های دریافتی و ارزیابی سطح تهدیدات آنها

۱۸ -تهیه گزارش از موارد با اهمیت

۱۹ -اطلاع به مراجع بالادست

ب: جمع آوری و ذخیره سازی جدیدترین بدافزارهای گسترش یافته

۱جمع آوری نمونه ها از طریق اشتراک در سرویس های بین المللی

۲ -جمع آوری نمونه ها از طریق مراوده با گروه های فعال در زمینه بدافزار در داخل و خارج کشور

۳ -تهیه و توسعه ابزار های شناسایی سریع گونه های تهدید کننده

۴ -ذخیره سازی نمونه ها در بانک اطلاعات بدافزار

۵ -ارسال مدیریت شده نمونه ها به تولید کنندگان آنتی ویروس داخلی و مراکز تحقیقاتی

ج: پیگیری اخبار حوزه بدافزارها از منابع مختلف رسمی و غیر رسمی جهت آگاهی سریع از رویدادها

۸ -پیگیری جدیدترین اخبار منتشر شده توسط شرکت های فعال در حوزه بدافزار

۹ -تماس مستقیم با متخصصین داخلی و خارجی برای دستیابی به اخباری که منتشر نشده و یا هرگز منتشر نخواهند شد.

۱۱ -عضویت در گروه های تخصصی این حوزه جهت دریافت آخرین اخبار و اطلاعات

۱۱ -تهیه گزارش از مهمترین اخبار

۱۲ -ارائه موارد با اهمیت به مراجع بالادست

د: ارائه گزارش جهت ایجاد آمادگی و مقابله با رویدادها

۷ -ارائه گزارش در خصوص عملکرد بدافزارهای ناشناس جمع آوری شده توسط هانی پات

۸ -ارائه گزارش در خصوص تهدیدات امنیتی با ریسک زیاد

۹ -ارائه گزارش در خصوص مهمترین تهدیدات امنیتی به وجود آمده

ه: ارائه ابزار و راهکار مقابله با تهدیدات واقع شده

۱ -تشخیص و تفکیک رویداد های خاص با اهمیت بالا

۲ -تهیه دستورالعمل مقابله و ارائه گزارش مربوطه

۳ -ارائه ابزار مناسب جهت شناسایی و پاکسازی

۴ -ارسال ابزار و راهنمای استفاده به سازمانها و انتشار عمومی آن در صورت نیاز

فرایند ۶: مشاوره

درصورتیکه از طریق دانش موجود نتوان به ماهیت حمله با بدافزار پی برد از طریق تشکیل اتاق فکر و یا دعوت مشاوران متخصص برای حمله بوجود آمده تدبیری اتخاذ می گردد که البته برای هرنوع حمله تدبیری خاص و منحصر به فرد لازم است.

فرایند ۷: تائید

پس از یافتن راهکار مناسب، اخذ تائید اجرا و مصوب نمودن راهکار جهت اعلام ضروری است

فرایند ۸: بروز رسانی آرشیو و توسعه سنسورهای، حسگرها و سامانه گردآوری کننده بدافزار یا سایرابزارها

پس از اخذ مجوز اعلام نتیجه، خروجی را به اولویت بندی شده و با رعایت اولویت در اختیار گروه پاسخگویی به رخداد قرار می گیرد.

الف: شناسایی زیر شبکه های حساس

۲۱ -دریافت اطلاعات اولیه از خارج از تیم

۱ -۱دریافت وضعیت از سازمانها

۱ -۲دریافت وضعیت از تیم های داخلی مرکز ماهر

۱ -۳شناسایی زیرشبکه بصورت تصادفی

۲۱ -تعیین اولویت و فیلترینگ درخواست وارده

۲۲بررسی و امکان سنجی زیرشبکه سازمان اعلام شده بصورت غیرحضوری

ب: اقدام برای ارتقاء سطح امنیتی زیرشبکه

۱۲ -هماهنگی با مسئولین شبکه سازمان ها یا حراست های IT سازمانها

۱۳ -امکان سنجی نصب حسگر و سنسورهای گردآوری کننده بدافزار بصورت حضوری در صورت نیاز

۱۴ -مشاوره و راهنمایی به مدیرشبکه سازمان متقاضی جهت رفع موانع نصب حسگر و سنسورها

۱۵ -انجام مکاتبه با مدیر فناوری اطلاعات سازمان متقاضی و درخواست مشخصات فنی

۱۶ -انجام هماهنگی و مشاوره جهت ارائه توضیحات فنی توجیهی – تشریحی

۱۷ -دریافت پاسخ و مشخصات فنی مورد نیاز از سازمان متقاضی

۱۸ -تنظیم برنامه زمانبندی با توجه به منابع سخت افزاری و تجهیزات سخت افزاری

۱۹ -هماهنگی و درخواست مجوز ورود به سازمان متقاضی

۲۱ -ارجاع و صدور دستور کار به نصاب حسگر یا سنسورهای هانی پات

۲۱ -تحویل سرور به نصاب

۲۲ -پیکربندی نرم افزارها بر سرور

۲۳ -هماهنگی نصاب با مسئول شبکه سازمان مربوطه

۲۴ -مراجعه حضوری نصاب جهت نصب حسگر و سنسور

۲۵ -اجرای فرایند نصب

۲۶ -اجرای فرایند لینک به پورتال ملی هانی نت

۲۷ -نظارت بر دریافت برخورد توسط کارشناسان ماهر

۲۸ -تائید صحت عملکرد سنسور یا حسگر منصوبه

۲۹ -تکمیل صورتجلسه تحویل سخت افزار توسط سازمان متقاضی

۳۱ -اعلام محل نصب و مشخصات کامل سنسور به سازمان

۳۱ -صدور نام کاربری و رمز عبور برای متقاضی بصورت محرمانه

۳۲ -تکمیل و تائید فرم های آزمایش و تحویل

ج: پایش و مانیتورینگ سطح کیفی عملکرد سنسورها

۱۳ -تهیه گزارش هفتگی ثبت برخورد

۱۴ -بررسی علل عدم کاربری برخی ماشین های مجازی

۱۵ -انجام فرایند تخصصی رفع مشکل سنسورها بصورت ریموت

۱۶ -به مدار بازگرداندن سنسورهای منصوبه و ارائه گزارش اصلاحی

۱۷ -تهیه گزارش ثبت برخورد ها بصورت ماهانه

۱۸ -رفع مشکلات سنسورها از راه دور

۱۹ -ارائه گزارش اقدامات انجام شده در قالب مانیتورینگ

۲۱ -برگزاری جلسه هماهنگی در جهت رفع مشکلات تخصصی مانیتورینگ

۲۱ -اعلام مشکلات فنی یا ستادی غیر قابل رفع در تیم به مدیرمرکز

۲۲ -به روزرسانی سنسور و تست مجدد صحت کارکرد

د: گزارش

۱۱ -ارائه گزارش وضعیت کاربری سنسورها و حسگرهای منصوبه به سازمان متقاضی بصورت محرمانه

۱۱ -ارائه گزارش وضعیت کاربری سنسورها و حسگرهای مربوطه به مدیر

۱۲ -ارائه گزارش ثبت برخورد بصورت هفتگی . ماهانه و سالیانه به مدیر

۱۳ -ارائه گزارش اقدامات انجام شده در تیم مانیتورینگ به مدیر

۱۴ -ایجاد دسترسی گزارش گیری برای مرکز راهبردی افتا

درصورت نیاز به توسعه یا بکارگیری ابزاردیگر از طریق تعریف پروژه جدید و تهیه و تنظیم RFP اقدام می گردد بدین صورت که حسب RFP ارائه شده طبق نیاز بوجود آمده، اقدام به تهیه شرح خدمات می گردد و پس از قطعیت شرح خدمات آنرا به معاونت مالی اداری و تدارکاتی ارسال می دارند لذا پس از طی فرایندهای مالی و تامین اعتبار اقدام به انعقاد قرارداد جدید در جهت رفع نیاز می گردد و عملکرد پیمانکار
مربوطه طبق مفاد قرارداد بدقت مورد پایش و کنترل قرار می گیرد.

فرایند ۹: پاسخ و رفع رخداد

گروه پاسخگویی به رخداد ها حسب مورد ارجاعی اقدام به پاسخ می نمایند در صورتیکه از طریق حسگرهای هانی پات ، اطلاعات دریافت شده باشد نتایج بررسی ها به اطلاع سازمانها و مسئولین شبکه ها رسیده می شود و در صورتیکه اطلاعات از طریق درخواستهای تلفنی باشد نتایج بررسی ها طی ارسال نامه های محرمانه به اطلاع متقاضی رسیده می شود و یا از طریق انجام مکاتبات محرمانه، نتیجه اقدامات به اطلاع متقاضی رسیده می شود.

7 ابزارهای مدیریت رخداد

مدیریت حوادث (IcM) شما را ملزم می کند تا اختلال غیرمنتظره در سرویس IT را مشاهده کرده و به موقع حل مسئله را سازمان دهید. زمینه مدیریت حادثه پشتیبانی و پشتیبانی کاربران را در بر می گیرد ، بنابراین ابزارهای مدیریت حادثه به عملکردهای نرم افزار میز خدمت نزدیک هستند.

ابزار ایده آل برای مدیریت حادثه باید جامع تر از یک سیستم ردیابی رویداد رویداد راهنما باشد. همچنین باید از تحول سیستم IT حمایت کند تا از بروز مجدد خطر غیر منتظره جلوگیری شود. این بدان معنی است که مدیریت واقعه ایده آل باید شامل گزارش های گسترده و ویژگی های تحلیلی باشد. ادغام فرآیندهای ITIL نیز بسیار مفید است زیرا به محض شناسایی علت این حادثه و برنامه ریزی برای اصلاح گسل های سیستم ، به راهنمایی سازگاری سیستم کمک می کند.

SolarWinds Web Help Desk

نام SolarWinds Web Help Desk باعث می شود فکر کنید این سرویس از ابر اجرا می شود. با این حال ، این نرم افزار داخلی است که روی سرورهای خود نصب می کنید ، اما می توانید از طریق یک مرورگر به آن دسترسی پیدا کنید ، به این معنی که Cloud داخلی خود را ایجاد می کنید.
این بسته چیزی بیش از یک سیستم Help Desk نیست. این سیستم دارای ویژگی های مدیریت دارایی و کنترل نسخه است که به شما در پیگیری موجودی نرم افزار و سخت افزار کمک می کند. Luck از روال کشف خودکار دستگاه تهیه شده و این ابزار ، یک پایگاه داده از دارایی های فناوری اطلاعات را ایجاد و نگهداری می کند. این سرویس به شما امکان دسترسی سریع به بررسی های موجود و استفاده از تجهیزات IT خود را می دهد و به طور منظم از عملکرد تجهیزات شما نمایان می شود.
این نرم افزار با استفاده از فرایندهای ITIL در ذهن شما طراحی شده است و وظیفه برنامه ریزی ، پیاده سازی و تغییر هرگونه تغییر مورد نیاز برای جلوگیری از بروز مجدد خطر را آسان می کند.
در کنار این ویژگی های عالی مدیریت تغییر ، سیستم SolarWinds دارای توابع راهنما استاندارد است. این ویژگی ها با ویژگی های عالی ردیابی وظیفه و برنامه های مدیریتی تیم افزایش یافته است.
ابزارهای گزارشگری و تحلیلی که در میز راهنمائی وب ایجاد شده اند ، به مدیریت در نظارت بر SLA کمک می کند - که این نیز گزینه ای عالی را برای ارائه دهندگان خدمات مدیریت شده ایجاد می کند. می توانید پارامترهایی را در داشبورد تنظیم کنید که در صورت عدم موفقیت اهداف عملکرد ، هشدارها را انجام می دهند. این سیستم هشدار همچنین برای ردیابی حوادث مفید است و اطمینان حاصل می شود که زمان پاسخگویی برای رفع مشکل محکم است.
نرم افزار Web Help Desk روی Windows، Windows Server، Linux و Mac OS اجرا می شود. می توانید این سیستم را در یک آزمایش رایگان 14 روزه آزمایش کنید. پس از دوره آزمایشی ، می توانید استفاده از آن را متوقف کنید ، مجوز بخرید یا به Web Help Desk Free Edition بروید ، که قابلیت های کامل نرم افزار پرداخت شده را ندارد.

ManageEngine Service Desk Plus

Service Desk Plus به صورت نرم افزاری در محل یا به عنوان یک سرویس نرم افزاری که از طریق وب تحویل داده می شود ، موجود است. ManageEngine سه سطح خدمات را برای سرویس میز پلاس ارائه می دهد و ویژگی های مدیریت حادثه فقط در برنامه های بالاتر در دسترس هستند. بسته کامل شامل برنامه های مدیریت دارایی IT است که کلیه سخت افزارها و نرم

افزارهای موجود در شبکه شما یک بانک اطلاعاتی موجودی را برای شما فراهم می کند. شما همچنین می توانید رویه های مدیریت پروژه مبتنی بر ITIL را با برنامه برتر دریافت کنید.

ویژگی های مدیریت حادثه سرویس میز پلاس عملکردهای Help Desk سیستم را در بر می گیرد. این ماژول همچنین شامل نظارت بر عملکرد و ردیابی SLA است. سایر ویژگی های ITIL این ابزار شامل یک فهرست خدمات است که هم خدمات تجاری و هم فنی را در بر می گیرد. این گردآوری اطلاعات را راهنمایی می کند وقتی که یک خطر بوجود می آید و از طریق اسکریپت ها و گردش کار به تحقیقات انتقال از طریق راه حل تغذیه می شود.

خدماتی که از بروز مجدد خطرات شناسایی شده در اطراف بروزرسانی دانش دانش حاوی راهنمایی برای کاربران و تنظیمات رویه ها و اسکریپت های سرویس جلوگیری می کند تا خطای احتمالی تازه شناسایی شده را محاسبه کنند.

کمبودهای اساسی سیستم که منجر به بروز حوادث می شوند روشهای مدیریت تغییر ماشه را در سیستم Service Plus Plus اعمال می کنند. پس از برطرف شدن یک حادثه ، کار بعدی این است که اطمینان حاصل کنید که هرگز دیگر اتفاق نمی افتد و اگر علت آن مربوط به زیرساخت ها بود ، شما باید برای بهبود سیستم باشید. گردش کار در ماژول مدیریت تغییر تیم شما را از طریق فرآیند تکامل و ترمیم موجودی خود راهنمایی می کند تا از تکرار خطاها جلوگیری کند.

Service Desk Plus در سه بسته موجود است. بسته استاندارد وظایف اساسی Help Desk را در اختیارتان قرار می دهد ، که شامل تعدادی مورد نیاز برای مدیریت حادثه است. مدیریت دارایی فناوری اطلاعات تنها در صورت دسترسی به برنامه حرفه ای در دسترس است. بالاترین برنامه ، با نام Enterprise Edition ، کلیه میز خدمات و ماژول های مدیریت دارایی برنامه های پایین را شامل می شود و همچنین عملکردهای مدیریت تغییر ITIL گسترده ای دارد.

برنامه Enterprise شامل مدیریت تغییر ، فهرست خدمات ، مدیریت مشکل و مدیریت پیکربندی است. گزارش و تجزیه و تحلیل ویژگی های خدمات میز پلاس پشتیبانی عالی از مدیریت در هنگام حل مسئله و وظایف تکامل سیستم ارائه می دهد.

SolarWinds Service Desk

میز سرویس SolarWinds به عنوان یک سرویس از طریق وب ارائه می شود. با این حال ، این شرکت نرم افزاری را برای سیستم ها در اختیار مشتری قرار می دهد تا بنا به درخواست در محل نصب شود. این سرویس آنلاین طبق فرایندهای استاندارد ITIL ساخته شده است ، بنابراین تضمین می کند که سیستم های مدیریت دارایی و پشتیبانی مشتری از توانایی کامل برای مقابله با مدیریت حادثه برخوردار باشند

سیستم خدمات SolarWinds در قلب راه حل مدیریت حوادث است. این شامل سه عنصر اصلی است: بلیط فروشی ، پورتال خودیاری و پایگاه دانش. خدمات در سه سطح بسته ارائه می شود. این شرکت بسته استاندارد را به عنوان تحقق الزامات مدیریت حوادث ارائه می دهد. با این حال ، این فقط به سیستم مدیریت Help Desk اشاره دارد. برای به دست آوردن کلیه عملکردهای مورد نیاز برای چرخه حیات مدیریت حادثه تعریف شده با ITIL ، باید برای بالاترین برنامه بروید.

برنامه تجاری توابع Help Desk را به شما می دهد و همچنین مدیریت ، کاتالوگ خدمات و ردیابی عملکرد SLA را تغییر می دهد. برنامه برتر با نام حرفه ای به شما مجوز و مدیریت قرارداد و اتوماسیون پیشرفته را می دهد. گنجاندن گردش کار و اسکریپت های تحقیق در میز کار به شما کمک می کند تیم خود را هنگام تحقیق در مورد منبع گزارش شده توسط کاربر راهنمایی کنید. فرآیندهای ITIL درون نرم افزار ، مراحل تحقیق را به سمت پیشنهادهای راه حل و وظایف مدیریت پروژه گسترش می دهد.

Spiceworks Help Desk

ویژگی بارز Spiceworks Help Desk این است که استفاده از آن رایگان است. این یک معامله شگفت انگیز با در نظر گرفتن پیشرفته بودن نرم افزار است. در روند نزولی ، سیستم با تبلیغات ظاهر می شود که به طور دائم در یک صفحه جانبی داشبورد ظاهر می شود ، از تبلیغات پشتیبانی می کند. نسخه پرداختی از Spiceworks Desk Help Desk وجود ندارد.

این یک بسته نرم افزاری است که در ویندوز و Mac OS نصب شده است. می توانید به جای آن از سیستم بصورت آنلاین استفاده کنید و از عدم نیاز به نگهداری نرم افزار روی سرورهای خود خودداری کنید. عملکرد نسخه آنلاین ، که به آن Spiceworks Cloud Help Desk گفته می شود ، به اندازه نرم افزار داخلی نیست. با این حال ، به Cloud Help Desk از هر دستگاه دیگری در هر نقطه قابل دسترسی است ، بنابراین لازم نیست نگران نرم افزار و سازگاری سیستم عامل باشید و می توانید به داشبورد Help Desk خود از دستگاه های تلفن همراه دارای سیستم عامل Android یا iOS دسترسی داشته باشید.

Spiceworks دارای یک جامعه کاربری بسیار فعال است و هزاران افزونه در انجمن موجود است. این به شما امکان می دهد سیستم را به منظور ادغام با برنامه های دیگر که ممکن است از آنها استفاده کنید سازگار کنید - بسیاری از برنامه های افزودنی توسط ارائه دهندگان آن برنامه ها نوشته شده اند.

داشبورد عامل شامل یک ویژگی یادداشت برداری و پیام رسانی است که یک راه حل عالی برای راه حل های مشترک برای بروز حوادث است.

Zendesk Suite

Zendesk عمدتا یک سیستم Help Desk است. با این حال ، ماژول گزارشگری و تحلیل عالی آن باعث شده است تا در این راهنمای ابزارهای مدیریت حوادث ، شایسته ورود باشد.

Zendesk یک سیستم بسیار پرکاربرد است. این تعدادی از راه ها را به هم پیوند می دهد که به کاربران امکان می دهد تا قبل از مراجعه به کارمندان IT برای کمک ، مشکلات را حل کنند. این ویژگی ها با یک پایگاه داده مشاوره قابل جستجو در حول پایگاه دانش می چرخند. خط بعدی کمک ها مربوط به کانال های تماس است. Zendesk شامل یک پنجره گپ می باشد که پاسخ ها و حل مسئله را از طریق سوالات تعاملی سرعت می بخشد.

سیستم مدیریت بلیط در Zendesk باعث می شود تا نمایندگان به عنوان دستیار بعدی در دسترس انتخاب شوند. بلیط را می توان از طریق تماس تلفنی یا ایمیل و همچنین از طریق چت جمع آوری کرد. آنها را می توان ردیابی ، هدایت ، تقسیم و ادغام کرد.

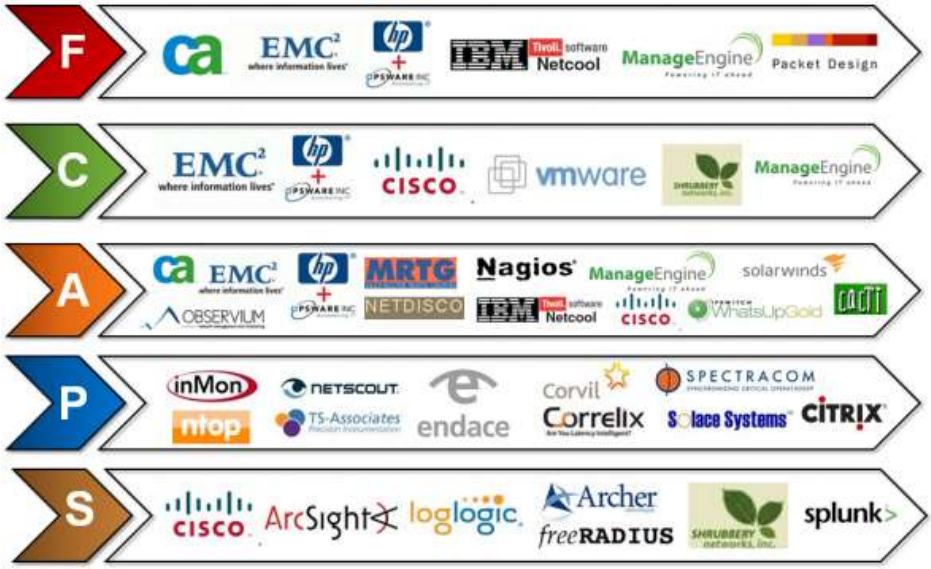
Zendesk Suite به ابر قابل دسترسی است بنابراین نیازی به نگهداری نرم افزار در سایت ندارید. عملکردهای نظارت و گزارشگری شما را قادر می سازد عملکرد عملکرد نماینده و معیار گردش مالی مورد انتظار را ارزیابی کنید. عملکرد گزارش همچنین از انطباق هدف SLA پشتیبانی می کند.

Zendesk برای هر نماینده در هر ماه شارژ می شود. این سیستم در دو سطح حرفه ای و Enterprise در دسترس است. هر دو سطح برای پشتیبانی مدیریت حادثه مناسب هستند. شما می توانید یک آزمایش رایگان از Zendesk دریافت کنید تا آن را با سرعت بیشتری طی کنید

8 مرکز کنترل عملیات شبکه

امروزه یکی از اصلی ترین و مهمترین راهکارها در مدیریت شبکه های بزرگ، پیاده سازی ساختارهای مرکز عملیات شبکه و امنیت SOC NOC می باشد. این سیستم برای سازمان ها، امکان مدیریت هر چه آسان تر تجهیزات، سرویس ها و همچنین مقابله با رخدادهای امنیتی را فراهم آورده و تدوین سیاست های کلان در جهت بهبود سرویس دهی و خدمت رسانی هر چه بهتر را برای مدیران شبکه امکان پذیر می سازد. همچنین این سیستم امکان تشخیص صحیح و به موقع از رخدادها را با توجه به خروجی های ایجاد شده، میسر ساخته و سازمان ها را در جهت کاهش خطا و بلا رفتن ضریب تصمیم گیری های صحیح، یاری می رساند. پیاده سازی این ساختار، مستلزم شناخت کافی از ابزار و نرم افزارهای مختلف و همچنین انالیز دقیق از نیاز سازمان ها و شرکت های بزرگ می باشد.

استفاده از ابزار و نرم افزارها در این حوزه، مستلزم شناخت کامل در جهت یکپارچه سازی و مدیریت آنها می باشد. در غیر این صورت سازمان ها از تمامی امکانات این سیستم بهرمند نشده و ممکن است در بلند مدت به دلیل پیچیدگی در راهبری و یا استفاده غیر علمی و مغایر با استانداردها، این راهکار کمک چندانی به بهبود عملکرد شبکه سازمان ها ننماید.



نتایج بررسی ها و تحلیل های صورت پذیرفته در بخش تحقیق و توسعه شرکت امن پایه ریزان کارن APK استانداردهای مفهومی در مدیریت شبکه ها NOC SOC را معرفی می نماید که به توصیف یک شبکه ارتباطی، و روش های بررسی آن می پردازد شبکه اصلی ارتباطات در هر حوزه

ایجاد یک چارچوب کاری، توصیف یک تصویر گسترده، و نشان دادن تفاوت زمینه های کاربرد آن و شناسایی نحوه همکاری بین بخش های مختلف آن ها می باشد.

به عنوان نمونه: این چهار چوب ها به توضیح اینکه آیا Syslog یا Trup برای اعلام رخدادها ضروری است یا خیر نمی پردازد. هیچ یک از قالب های ذکر شده به فرمت نگهداری اطلاعات Accounting نمی پردازد. این جزئیات در استانداردهای در سطح پایین تر تعیین می گردد.

توصیه های موجود مطابق با استاندارد ها، یک سند شامل مجموعه ای ازM ها را به وجود می آورد، که ۵ زمینه مدیریت را مشخص می نماید FCAPS:

- مدیریت خطا :(Fault Management) شناسایی، ایزوله کردن، اطلاع رسانی و اصلاح خطای رخ داده در شبکه

- مدیریت تنظیمات :(Configuration Management) تنظیم برخی از قسمت های تجهیزات شبکه، نظیر تنظیمات مدیریت فایل، مدیریت لیست موجودی و مدیریت نرم افزار
- مدیریت حساب های کاربری :(Accounting Management) جمع آوری اطلاعات میزان استفاده از منابع شبکه
- مدیریت عملکرد :(Performance Management) نظارت و سنجش جنبه های گوناگونی که باعث بهبود عملکرد در یک لایه ی خاص می گردد.
- مدیریت امنیت :(Security Management) امنیت دسترسی به تجهیزات شبکه، منابع شبکه و سرویس ها برای افراد مجاز

8.1 مدیریت خطا

مدیریت خطا مجموعه ای از راهکار هایی است که توانایی شناسایی، ایزوله کردن و تصحیح عملیات های غیر طبیعی را در شبکه ارتباطی به وجود می آورد. معیار تضمین کیفیت برای مدیریت خطا شامل اندازه گیری اجزای قابلیت اطمینان (Reliability)، دسترسی و پایداری (RAS) می باشد. مدیریت خطا در مرکز عملیات شبکه و امنیت NOC SOC خود شامل بخش های ذیل می باشد.

- RASایجاد تضمین کیفیت با بهره برداری از شاخص قابلیت اطمینان (Reliability) که راهنمای طراحی یک سیاست برای Redundancyتجهیزات (یک بخش از مدیریت تنظیمات) و یک سیاست از دیگر توابع گروه ها در این حیطه است می پردازد.
- نظارت بر هشدار ها به معنی قابلیت نظارت بر اجزای از کار افتاده شبکه در سریع ترین زمان ممکن است
- محلی سازی خطا بیان می دارد که چه زمانی اطلاعات اولیه یک خطا برای محلی سازی خطا کافی است. محلی سازی خطا با اطلاعات به دست آمده توسط روال های محلی سازی خطای تکمیلی، در لایه کاربردی (Application) تکمیل می گردد.
- تصحیح خطا، داده هایی درباره تصحیح یک خطا و کنترل روش استفاده از منابع اضافی موجود تا جایگزینی تجهیزات یا امکانات مشکل دار را بیان می دارد.
- بررسی و آزمایش به دو روش می تواند انجام پذیرد. در روش اول، یکی از عناصر شبکه به بررسی عملکرد های تجهیزات می پردازد، که در چه مکانی داخل شبکه پردازشی در حال اجراست. روش دیگر، روش آزمایش فعال از اجزای بیرونی تجهیزات نظیر مدارات، ارتباطات و تجهیزات مجاور آن تجهیز می باشد.
- مدیریت ایرادات، مشکلات گزارش شده توسط مشتریان و مشکلات تیکت شده توسط آزمایشات خطا یابی را مد نظر قرار می دهد.
- عملکرد پشتیبانی برای بررسی و پاک سازی مشکلات و ایجاد دسترسی به وضعیت سرویس ها و روال ها در هر خطا می باشد.

8.2 مدیریت تنظیمات

مدیریت تنظیمات، روش ها و متد هایی را برای شناسایی، جمع آوری داده های تنظیمات از دستگاه ها، ایجاد کنترل بر دستگاه ها و ارایه داده های تنظیمات برای اجزای شبکه را فراهم می نماید. مدیریت تنظیمات شامل موارد ذیل می گردد:

- نصب و راه اندازی تجهیزات سخت افزاری و تنظیمات منطقی آن ها
- برنامه ریزی و تعامل که به معرفی یک سرویس، تغییر در نحوه عملکرد سرویس های پیاده سازی شده و قطع سرویس های در حال ارایه، کمک می نماید.
- تأمین، شامل دستورالعمل های ضروری برای به حالت سرویس دهی رساندن تجهیزات، بدون نصب و راه اندازی می باشد. وضعیت یک دستگاه (در حال سرویس، خارج از سرویس، آماده به کار و یا رزرو شده) و برخی از پارامترهای انتخابی نیز توسط عملکرد تأمین، کنترل می گردد.

وضعیت و کنترل به منظور آگاهی از اینکه چه زمانی چهارچوب ها قابلیت نظارت و کنترل جنبه های مورد نظر از اجزای شبکه را در لحظه فراهم می نماید. به عنوان مثال می توان به بررسی یا تغییر وضعیت سرویس دهی اجزای شبکه (در حال سرویس؛ خارج از سرویس دهی یا آماده به کار) یا بررسی یکی از زیر قسمت ها و یا شروع تست های تشخیصی در اجزای شبکه اشاره کرد. معمولا بررسی وضعیت، اطلاعاتی را در رابطه با هر عملیات کنترلی، به منظور تأیید نتیجه مشخص می نماید(مانند بازگردانی یا احیای یک سرویس)

- برنامه ریزی و مهندسی شبکه و همچنین اعمال وابسته به آن، به مشخص کردن میزان نیاز به افزایش ظرفیت و معرفی تکنولوژی های جدید می پردازد. برنامه ریزی و مهندسی مثال های کوچکی از عملکرد های متعدد در این حوزه می باشد. زیرا آن ها مرتبط به بخش بازده از چشم انداز نظارت و بخش تنظیمات از یک چشم انداز اجرایی هستند.

8.3 مدیریت حساب های کاربری

مدیریت حساب های کاربری به شما اجازه می دهد تا میزان استفاده از سرویس های شبکه و هزینه ای که برای آن سرویس به ارایه دهنده و مشتری، برای هر بار استفاده تحمیل می شود را بدست آورد و همچنین به دانستن میزان هزینه انجام شده برای یک سرویس کمک می نماید. مدیریت حساب های کاربری شامل بخش های ذیل می گردد:

1. اندازه گیری میزان استفاده، که خود شامل بخش های ذیل می شود:
    - برنامه ریزی و مدیریت روند اندازه گیری میزان استفاده.
    - تراکم و انبوهی، همبستگی و صحت استفاده از شبکه و سرویس
    - میزان اشاعه و ترویج استفاده
    - نظارت بر استفاده
    - تست و رفع عیب
    - بررسی قوانین سنجش
    - استفاده از ابزار ذخیره سازی کوتاه مدت و بلند مدت
    - ذخیره و تأیید اطلاعات
    - مدیریت جمع آوری داده های مرتبط با میزان و شکل استفاده
    - ایجاد کاربرد برای سرویس ها
2. تعرفه بندی و قیمت گذاری
    - تعرفه برای مشخص کردن میزان پرداختی برای استفاده از یک سرویس مورد استفاده قرار می گیرد.
3. مجموعه ها و امور مالی

- قابلیت مدیریت حساب های کاربری مشتریان، اطلاعات مشتریان، تاریخ پرداخت ها و زمان دریافت هر پرداخت توسط سیستم در این بخش قرار می گیرند.

4. کنترل شرکت

- این بخش مسئول کارهای مالی شرکت نظیر بودجه بندی، ممیزی و تجزیه و تحلیل سودآوری می باشد.

8.4 مدیریت عملکرد

مدیریت عملکرد مجموعه فعالیت هایی است که به منظور ارزیابی و گزارش گیری برروی وضعیت تجهیزات ارتباطی و کارایی شبکه یا عناصر دیگر صورت می پذیرد. یکی از نقش های اصلی آن جمع آوری و تجزیه و تحلیل آماری داده ها به منظور نظارت، تصحیح وضعیت و کارایی شبکه، عناصر شبکه یا دیگر تجهیزات و همچنین به منظور کمک در برنامه ریزی، تأمین، نگهداری و ارزیابی کیفیت می باشد.

مدیریت عملکرد شامل بخش های ذیل می گردد:

- **تضمین کیفیت عملکرد :**شامل اندازه گیری کیفیت می باشد که از جمله آن، می توان به اهداف و ارزیابی عملکرد اشاره کرد.

- **نظارت بر عملکرد :**این بخش شامل مجموعه ی به هم پیوسته ای از داده ها درباره ی عملکرد اجزاء شبکه است. وضعیت خطا های بحرانی توسط هشدارهای اطلاعاتی و روش های نظارتی، تشخیص داده می شود. خطا های بسیار کم اهمیت یا با اهمیت متوسط در بخش های گوناگون متقابلا بر هم اثر نموده و نهایتا منجر به پایین آمدن کیفیت سرویس می شود که شاید توسط روش های نظارتی قابل تشخیص نباشد. نظارت بر عملکرد، به منظور سنجش کلی کیفیت و استفاده از پارامترهای بررسی شده، در جهت شناسایی هرگونه نقص صورت می پذیرد. همچنین یکی از دلایل طراحی، شناسایی الگوهای مشخص اختلال، قبل از ا پایین آمدن بیش از حد کیفیت، می باشد. نظارت بر عملکرد خود شامل بخش های زیر می باشد:

  - سیاست های نظارت بر عملکرد
  - فیلترینگ و ایجاد ارتباط بین رخدادهای نظارت بر عملکرد شبکه
  - جهت دهی و تجمیع داده ها
  - روند جمع آوری داده ها
  - وضعیت ترافیک
  - پردازش میزان آستانه هشدارها
  - تجزیه و تحلیل روندها
  - جمع آوری داده های نظارت بر عملکرد ساختار

- ردیابی، شمارش، ذخیره سازی و گزارش

- **کنترل مدیریت عملکرد :**این قسمت شامل میزان آستانه و الگوریتم های تحلیل داده ها و همچنین مجموعه ای از داده های عملکردی می باشد. لازم به ذکر است که این بخش، اثر مستقیم بر روی مدیریت شبکه ندارد. برای مدیریت ترافیک و مهندسی شبکه این بخش شامل دستورالعمل هایی است که بر روی مسیر یابی و پردازش ترافیک تأثیر می گذارد.

- **تحلیل عملکرد :**سوابق جمع شده از عملکرد ها نیاز به پردازش و تحلیل مضاعفی به منظور ارزیابی سطح کارایی و عملکرد هر یک از موجودیت ها دارد بنابر این تحلیل عملکرد شامل بخش های ذیل می باشد:
  - پیشنهاد هایی به منظور افزایش کارایی
  - تعریف سیاست های بخش آستانه ها و حد و مرزها و تعیین موارد خواص
  - پیش بینی ترافیک(روند ترافیک)
  - شرح مختصری از عملکرد (به ازاء هر شبکه ، سرویس و ترافیک مشخص)
  - تحلیل موارد خواص(به ازاء هر شبکه ، سرویس و ترافیک مشخص)
  - تحلیل ظرفیت(به ازاء هر شبکه ، سرویس و ترافیک مشخص)
  - توصیف و شرح عملکرد

8.5 مدیریت امنیت

امنیت برای تمام بخش های فعال و در حال کار یک امر ضروری است. مدیریت امنیت در مرکز عملیات شبکه و امنیت NOC SOCشامل دو بخش اصلی می باشد:

1. خدمات امنیت در حوزه ارتباطات، شامل احراز هویت، کنترل دسترسی ها، محرمانگی داده ها، صحت داده ها و عدم انکارپذیری می باشد.

این خدمات قابل ارایه و اعمال بر روی هر نوع ارتباطی بین سیستم ها، کاربران و یا مشتریان می باشد. و همچنین یک مجموعه ایی از مکانیزم های امنیت فراگیر و جامع را تبیین می نماید که به روی تمامی ارتباطات قابل اجرا می باشد.
از جمله مکانیزم ها می توان به شناسایی رخ داد، مدیریت ممیزی مستمر امنیت و بازیابی امنیتی اشاره کرد.

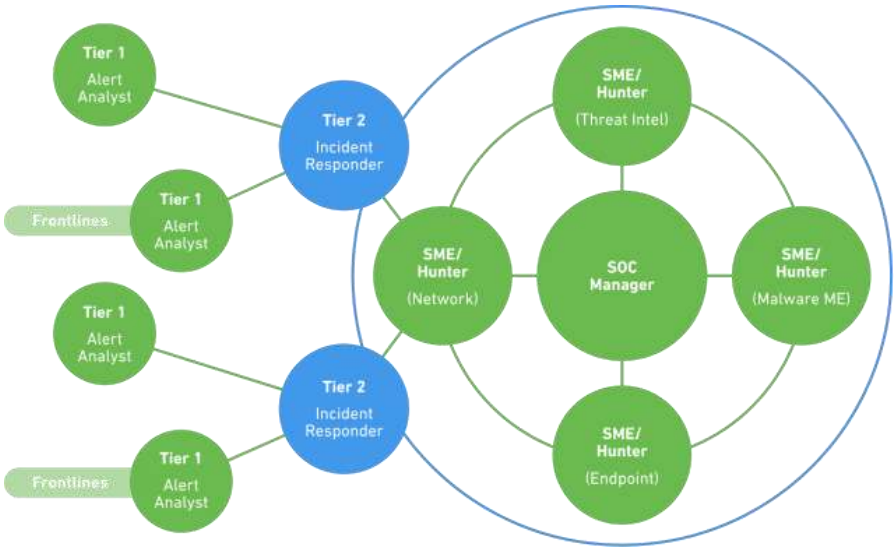
2. شناسایی رخ دادهای امنیتی و گزارش دهی از گزارش فعالیت ها که ممکن است به عنوان تخلف امنیتی تفسیر گردد.

- مدیریت امنیت شامل قسمت های ذیل می باشد:
  - پیشگیری
  - تشخیص

- مهار و بازیابی
- اجرای امنیت

مرکز عملیات امنیتSOC ، زیرساختی است که یک تیم امنیت اطلاعات را که مسئولیت نظارت و تحلیل وضعیت امنیتی یک سازمان به صورت مداوم را بر عهده دارند را در خود جای می‌دهد .هدف تیمSOC ، تحلیل کردن و واکنش نشان دادن به رخدادهای امنیت سایبری با استفاده از ترکیبی از راهکارهای فناوری و مجموعه‌ای قوی از فرایندها می‌باشد. پرسنل مرکز عملیات امنیتی معمولا تحلیل‌گران امنیتی، مهندسین و همچنین مدیرانی هستند که بر عملیات امنیتی نظارت می‌کنند. پرسنل SOC همچنین با تیم‌های واکنش به حادثه سازمانی نیز به صورت نزدیک همکاری کرده، تا پس از شناسایی مسائل امنیتی، از رسیدگی فوری به آن‌ها اطمینان حاصل کنند.

مراکز عملیات امنیتSOC ، برای یافتن فعالیت‌های غیرعادی که می‌تواند نشان‌دهنده یک حادثه، نفوذ یا تهدید امنیتی باشند، فعالیت شبکه، سرورها، EndPointها، دیتابیس‌ها، برنامه‌ها، وب سایت‌ها و سیستم‌های دیگر را تحت نظارت و تحلیل قرار می‌دهند. مرکز عملیات امنیت SOC وظیفه اطمینان حاصل کردن از شناسایی، تحلیل، دفاع و گزارش درست رخدادهای امنیتی بالقوه را بر عهده دارد.



نحوه کارکرد مرکز عملیات امنیت

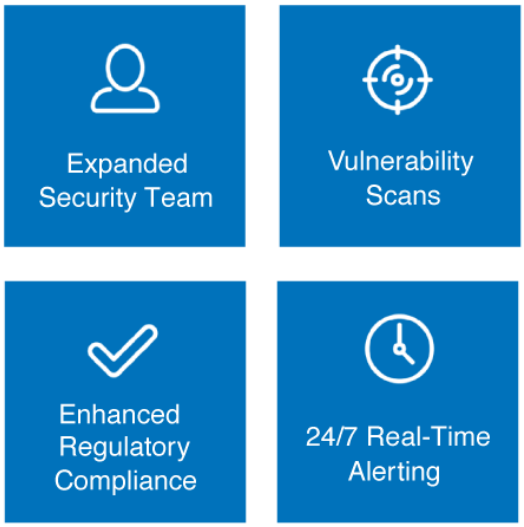
به جای تمرکز بر توسعه راهبردهای امنیتی، طراحی معماری امنیتی، یا اجرای اقدامات حفاظتی، تیم SOC مسئول بخش‌های عملیاتی و امنیت اطلاعات سازمان است. پرسنل مرکز عملیاتی امنیتی عمدتا از تحلیلگران امنیتی تشکیل شده‌است که برای شناسایی، تحلیل، واکنش، گزارش، و جلوگیری از حوادث امنیت سایبری با یکدیگر همکاری می‌کنند. سایر وظایف جانبی SOC ممکن است شامل تجزیه و تحلیل پیشرفته جرم‌شناسی، تحلیل رمز، و مهندسی معکوس بدافزارها برای تحلیل رخدادها باشد.

اولین گام در ایجاد SOC یک سازمان، تعریف واضح یک راهبرد همگام با اهداف خاص سازمان و بخش‌های مختلف آن و نیز پشتیبانی از سوی مدیران اجرایی می‌باشد. هنگامی که یک راهبرد توسعه داده‌شد، زیرساخت مورد نیاز برای پشتیبانی از آن راهبرد باید اجرا شود. زیرساخت‌های متداول SOCعبارت‌اند از: فایروال‌ها، IPSوIDS ، راهکارهای شناسایی نقص‌های امنیتی، تحقیق و تفحص و یک سیستم مدیریت داده‌ها و رخدادهای امنیتی (Security Information and Event Management System) و یا به اختصار SIEMچیست

فناوری‌های مورد نیاز برای جمع‌آوری داده‌ها از طریق جریان داده‌ها، فرآیند بررسی و انتقال داده‌ها از راه دور (Telemetry Packet Capture، syslog) و دیگر روش‌ها باید در دسترس باشد تا متخصصین SOC بتوانند فعالیت داده‌ها را همبسته کرده و تحلیل کنند. مرکز عملیات امنیت SOC همچنین شبکه وEndpoint ها را برای شناسایی آسیب‌پذیری‌ها نظارت می نماید تا از داده‌های حساس حفاظت کرده و از منطبق بودن با مقررات صنعت و دولت اطمینان حاصل گردد.

ویژگیSOC و مزایای دارا بودن مرکز عملیات امنیت

مزیت اصلی یک مرکز عملیات امنیت SOC چیست؟ بهبود شناسایی رخدادهای امنیتی از طریق نظارت مستمر و تحلیل فعالیت داده‌ها است SOC .با تجزیه و تحلیل این فعالیت‌ها در تمام شبکه‌ها، Endpointها، سرورها و دیتابیس‌های سازمان در تمام ساعات شبانه‌روز، برای اطمینان از تشخیص و واکنش به موقع به رخدادهای امنیتی بسیار حیاتی می‌باشد.



بهترین اقدامات اجرایی مرکز عملیات امنیت

بسیاری از مدیران بخش امنیت برای ارزیابی و کاهش تهدیدات به صورت مستقیم به جای اتکا به یکScript ، تمرکز خود را برای بر روی نیرو انسانی قرار داده‌اند .پرسنل SOC به طور مداوم هم در برابر تهدیدات شناخته شده و هم برای شناسایی تهدیدات جدید فعالیت می‌کنند. آن‌ها همچنین نیازهای مشتریان و نیازهای سازمان را برآورده کرده و در سطح تحمل ریسک خود فعالیت می‌کنند. در حالی که سیستم‌های فناوری مانند فایروال ها یا IPS ممکن است از حملات ساده جلوگیری کنند، برای مقابله با رخدادهای بزرگ، تحلیل انسانی لازم است.

برای کسب بهترین نتایج، SOCسازمان باید همواره از آخرین اطلاعات تهدید آگاه باشد و از این اطلاعات برای بهبود شناسایی داخلی و مکانیسم‌های دفاعی استفاده کند. همانطور که موسسه InfoSec بیان کرده است، SOCاطلاعات سازمان را از درون سازمان جمع‌آوری می‌کند و آن‌ها را با اطلاعات تعدادی از منابع خارجی مرتبط می‌کند که دید کلی نسبت به تهدیدات و آسیب‌پذیری‌ها را به ارمغان می‌آورد. این اطلاعات سایبری خارجی شامل Feed اخبار، به‌روزرسانی Signatureها، گزارش رخدادها، چکیده اطلاعات تهدیدات و هشدارهای آسیب‌پذیری می‌باشد، که SOC سازمان را در آگاه بودن از تهدیدهای سایبری در حال رشد یاری می‌کنند. برای آگاهی از جدیدترین تهدیدات، پرسنل SOC باید به طور مداوم ابزار نظارت را با اطلاعات تهدیدات تغذیه کنند SOC .سازمان همچنین باید برای تشخیص میان تهدیدات واقعی و تهدیدات اشتباها شناسایی شده، فرآیندهایی را داشته باشد.

SOCهای موفق از اتوماسیون امنیتی برای موثرتر و کارآمدتر شدن استفاده می‌کنند. با ترکیب تحلیلگران امنیتی بسیار ماهر با اتوماسیون امنیتی، سازمان‌ها قدرت تجزیه و تحلیل خود را برای بهبود تدابیر امنیتی و دفاع بهتر در برابر نقض امنیتی داده‌ها و حملات سایبری افزایش می‌دهند. بسیاری از سازمان‌ها که منابع داخلی برای تحقق این اهداف را در اختیار ندارند، این امور را به ارائه دهندگان خدمات امنیتی مدیریت شده که خدمات SOC را ارائه می‌دهند، واگذار می‌کنند.

کار در زمینه امنیت سایبری هر روز پر از تغییرات و شگفتیهای جدید است. در امنیت اطلاعات ، دقیقاً مانند یک زمین فوتبال ، اگر از شکل بازی ، نوع خواسته و تمایلات رقبای خود درک درستی نداشته باشیم ، دیگر نمی توانیم خطرات سازمان خود را درک کنیم.

برای حفظ رقابت در دنیای تجارت مدرن ، سازمانها باید به کاربران تجربه آنلاین در سطح بالا را ارائه دهند. از نظر عملی ، این بدان معنی است که وب سایت ، برنامه های کاربردی یا سایر خدمات آنلاین آن باید هم آسان باشد و هم بدون اشکال. مهمتر از آن ، آنها باید نسبت به امنیت و محافظت در برابر حملات سایبری اطمینان کامل داشته باشند.

حتی پس از همه نفوذهای اخیر و حملات هکری موفق ، بسیاری از شرکت ها و سازمان ها هنوز هم دستورالعمل های مهم امنیتی را نادیده می گیرند. علاوه بر این بسیاری از سازمان ها نفوذگران سایبری را دست کم می گیرند که همیشه حداقل دو یا سه قدم از سازمان ها جلوتر هستند.

برای تحقق این اهداف ودر برابر فضای تهدیدی سایبری امروز، تمامی شرکتها و سازمانها باید در حفظ عملکرد آنلاین خود و سیاستها در برابر فعالیتهای مخرب به صورت فعال عمل نمایند. بهترین راه برای انجام این کار سازماندهی و ایجاد تیم هایی است که عهده دار این وظایف هستند یعنی NOC و .SOC هر دو این واحدها در دنیای کسب و کار مدرن نسبتاً متداول شده اند، اما هنوز هم سردرگمی در مورد اینکه نقش های خاص آنها چیست و تفاوتهای هر کدام از آنها چگونه است، وجود دارد.

اکثر شرکتها استراتژی امنیت سایبری "نظارت و پاسخ" را اتخاذ کرده اند. این استراتژی به طور کلی در یک مرکز عملیات امنیت (SOC) یا یک مرکز عملیات شبکه (NOC) انجام می شود. در بیشتر سازمانها ، SOCو NOC عملکردهای یکدیگر را تکمیل می کنند.

اگرچه نقش SOC و NOC شباهت زیادی به هم دارد، اما اساساً متفاوت هستند SOC.و NOC مسئولیت شناسایی، تحقیق، اولویت بندی، تشدید و حل مسائل را بر عهده دارند، اما انواع موضوعات و تأثیرات آنها به طور قابل توجهی در این دو متفاوت است. در حالی که هر دوی این واحدها برای هر سازمان از اهمیت بالایی برخوردار هستند، ترکیب SOC و NOC در یک نهاد و داشتن یکی از آنها می تواند وظایف دیگر را با فاجعه روبرو سازد؛ زیرا رویکردهای آنها و مجموعه مهارتهایی که برای مدیریت آنها لازم است، بسیار متفاوت است.

در حالی که NOC در حفظ عملکرد و در دسترس بودن زیرساخت های آنلاین سازمان متمرکز است ،) SOCمرکز عملیات امنیتی) بر حفظ یکپارچگی و ایمنی دارایی های آنلاین تمرکز دارد. این شامل محافظت از مواردی مانند داده های حساس متعلق به سازمان و همچنین هر گونه اطلاعات مشتریان و سایر ذینفعان است که باید از آنها در برابر نفوذ و حمله هکرها و مجرمان سایبری محافظت نماید.

NOC

NOC حوادث و هشدارهایی را کنترل می کند که بر عملکرد و در دسترس بودن تأثیر می گذارد. کار NOC این است که توافق نامه های سطح خدمات (SLA) را رعایت کند و حوادث را به گونه‌ای مدیریت کند که خرابی را کاهش دهد. این در دسترس بودن و عملکرد تمرکز دارد.

NOCمخفف مرکز عملیات شبکه (Network Operation Center) است. وظیفه آن این است که از عملکرد و در دسترس بودن شبکه آنلاین اطمینان حاصل کند NOC . باید مشکلات مربوط به زیرساخت فناوری اطلاعات از جمله بانکهای

اطلاعاتی ، سرورها و ماشینهای مجازی را کنترل ، مدیریت و اصلاح کند. اگر وب سایت ، برنامه ها ، سرورها یا شبکه دچار خرابی شده اند ، وظیفه NOC است که مسئله را شناسایی کند ، آن را برطرف کرده و آنها را مجدداً پشتیبانی کند.

سایر مسئولیت های NOC عبارتند از:

- نظارت مداوم و ارزیابی عملکرد شبکه
- گزارش از موضوعات و توصیه های بالقوه برای بهبود
- پاسخ به موقع به حوادث خاموشی
- برنامه ریزی برای افزایش ظرفیت و اضافه بار
- تعیین مراحل افزایش سرعت و هشدار به سایر قسمتهای شرکت

اکثر NOC ها از طریق یک اتاق کنترل مرکزی فعالیت می کنند ، جایی که می توان همه جنبه های عملکرد آنلاین یک شرکت را همزمان کنترل و دستکاری کرد .با توجه به اینکه بخش قابل توجهی از تجارت سالهاست که به صورت آنلاین انجام می شود ، NOCها یک نهاد نسبتاً متداول در بین اکثر شرکتها هستند.

تفاوت NOC در مقابل SOC

یک تحلیلگر NOC باید در مهندسی شبکه، برنامه ها و سیستم ها مهارت داشته باشد، در حالی که تحلیلگران SOC به مهارتهای مهندسی امنیت احتیاج دارند.

SOC بر روی "دشمنان هوشمند" متمرکز است در حالی که NOC بیشتر با وقایع طبیعی برخورد داشته و آنها را رفع می کند.

در نتیجه ، هم SOC و هم NOC برای کار کردن با یکدیگر اما در رابطه با یکدیگر لازم هستند.

برای درک بهتر عملکرد این دو مرکز عملیات، به تمثیل زیر توجه کنید:

NOC بسیار شبیه به سیستم عصبی مرکزی در بدن شماست و فعالیتهای مختلفی را که برای عملکرد لازم دارید، کنترل و حفظ می کند. در همین حال ، SOCبا سیستم ایمنی بدن شما قابل مقایسه است و از آن در برابر ویروس ها و باکتری هایی که می

توانند عملکرد مداوم بدن را به خطر بیاندازند، محافظت می کند .اگرچه هدف هر دو سیستم در حالت کلی حفظ بقای بدن و بهبود عملکرد آن است، اما هر یک از آنها مسئول جنبه های جداگانه ای برای دستیابی به این هدف هستند.

+

حال با ذکر مثالی دیگر تفاوت بین مراکز SOC و NOC را بیان می کنیم:

فرض کنید اتوبان پر ترددی دارید که اتومبیل‌های مختلف در این اتوبان در حال حرکت هستند (بستر شبکه و کابل‌های ارتباطی)

وظیفه NOC: مراقبت از صحت و سلامت جاده، ترمیم خرابی جاده در کمترین زمان، نظارت بر سلامت تجهیزات نظارتی بر جاده، کنترل و نظارت بر حجم ترافیک و از این قبیل موارد .به عبارت کلی‌تر وظیفه تامین کارکرد صحیح شبکه.

وظیفه SOC: همانند پلیس نیروی انتظامی بوده که بر جاده نظارت می‌کند، رفتارهای پر خطر رانندگان را شناسایی، معابر ورودی و خروجی به جاده را کنترل، بر امنیت جاده نظارت و حتی بر محتویات خودروها نظارت می‌کند.

به عبارتی مرکز عملیات شبکه NOC فاقد روشی برای مدیریت متمرکزحوادث امنیتی است. فعالیت اولیه مرکز عملیات شبکه NOC نگهداری و اطمینان از صحت و سلامت شبکه و زیرساخت سازمان است در حالی که مرکز عملیات امنیت (SOC) مدیریت حوادث امنیتی را به منظور حفاظت شبکه برعهده دارد. بنابراین به منظور افزایش بازدهی و کارآیی سازمان‌ها، از طریق پاسخگویی مناسب به حوادث امنیتی مانند ویروس‌ها و حملاتی که منجر به از دست رفتن یکپارچگی شبکه می‌شود، وجود این مرکز در کنار مرکز عملیات شبکه NOC بسیار موثر خواهد بود.

فعالیتهای مرتبط با مراکز SOC و NOC به تفکیک در جدول زیر بیان شده است:

ردیف	فعالیتهای مرتبط با SOC و NOC	SOC	NOC
۱	نظارت عملیات شبکه	✓	✓
۲	عیب یابی قطعی شبکه	✓	✓
۳	تشخیص نفوذ در شبکه	✓	✓
۴	مدیریت Log و Event	✓	✓
۵	همگرایی در نظارت بر رویدادها	✓	✓
۶	پیگیری و ردیابی Ticket	✓	✓
۷	نظارت بر عملیات شبکه	✓	✓
۸	برقراری و حفظ کارکرد صحیح زیرساخت		✓
۹	مسئول عملیات شبکه		✓
۱۰	مدیریت رخدادهای امنیتی جهت حفظ شبکه	✓	
۱۱	تحلیل ریسک های امنیتی شبکه	✓	
۱۲	مدیریت متمرکز رویدادهای امنیتی	✓	
۱۳	واکنش به حوادث در محل	✓	
۱۴	مدیریت امنیت و کشف تقلب	✓	
۱۵	تجزیه و تحلیل حوادث	✓	
۱۶	بررسی حوادث	✓	

نسل جدید مرکز عملیات شبکه(Next-GEN (NOC

در دنیای فناوری اطلاعات، NOC محلی است مرکزی که تکنیسن های ITمی توانند مستقیما نرم افزارهای RMM،(Remote Monitoring & Management) را بکار برند. این تیم می بایست به صورت 24 X 7 X 365 تمامی اجزای شبکه را مانیتور نموده و در واقع به مانند چشم سازمان جهت برآورده سازی هدف تضمین 99.99٪ Uptime عمل کند. تغییر اندازه و رشد سازمان های IT منجر شد تا در گزارش 176 IT Professionals سازمان NetQOS به این امر اشاره شود که ساختار های سنتی NOC ها نیاز های امروزه سازمان ها را برآورده نمی کند. در عوض، به منظور رفع نیاز های حیاتی امروزه، NOC ها می بایست به شیوه مناسب تری از کارآیی منابع نرم افزاری و سخت افزاری خود بهره گیرند تا بتوانند هرچه سریعتر و بهتر نیازهای سازمان را در عیب یابی و رفع مشکلات برآورده سازند.

این گزارش اشاره دارد که دیدگاه مرسوم و سنتی به NOC که اغلب به صورت واحدی صرفا واکنشی بوده و به مانند آتش نشان عمل کند، باعث می شود که این واحد وسیعا وظایف خود را معطوف به مانیتور کردن شبکه کند. این گزارش متذکر می شود که عدم توانایی NOC در شناسایی تبعات حاصل از یک امر و جلوگیری از رخ دادن آن از وظایف اصلی آن است که عدم اجرای صحیح این بخش از وظایف منجر به سلب اعتبار سازمان در نگاه کاربر می گردد.

برای مثال به منظور روشن شده این بخش فرض کنید که واحد NOC ظرفیت فعلی منابع ذخیره سازی و نرخ رشد تولید محتوا را نادیده بگیرد و تنها به مانیتور کردن وضعیت سلامت شبکه و دستگاه های آن در شرایط فعلی بپردازد. در این حالت هنگامی که وضعیت منابع سخت افزاری به شرایط بحرانی رسید و تولید آلارم کرد واحد NOC متوجه این آلارم شده و واکنش نشان می دهد. در این حالت با وجود اینکه NOC وظیفه سنتی تعریف شده خود را به درستی و صحیح انجام داده است، ولی در ساختار های جدید که نقش پیشگیرانه برای NOC متصور است این وظیفه انجام نشده است و در نهایت سازمان متحمل خساراتی شد که قابل پیش بینی و جلوگیری بود.

در بخشی از این گزارش، طی مصاحبه هایی که با کارشناسان حوزهIT در صنایع مختلف از جمله صنایع انرژی، رسانه، بانکداری و ... انجام شده است در خصوص این موضوع سوال شده است که آیا پرسنل واحد NOC تنها مشکلات را اعلام می کنند و یا اینکه علاوه بر اعلام صرف مشکل جهت روشن شدن دلایل اصلی مشکل نیز همکاری دارند و راهنمایی موثر می کنند. این مصاحبه بین دو طیف از کارشناسان IT این سازمان ها انجام شده است. اشخاصی که خودشان در واحد NOC فعالیت داشتند و افرادی که در واحد های دیگر IT به غیر از NOC فعال بودند. نتیجه گزارش موردی جالب و در عین حال حساس را مشخص می کند:

تقریبا 3 درصد از مصاحبه شوندگان عقیده داشتند که این امر جزو مسئولیت های NOC نیست. لذا کاملا مشخص است که از نه تنها از دیدگاه متخصصین شبکه بلکه از دیدگاه دیگر کارشناسان IT نیز می بایست در ساختار های سنتی مسئولیت NOC تغییراتی ایجاد شود.

پاسخ گویی به عیوب و محدوده مسئولیت ها

بخش عظیمی از سازمان ها حد اقل یک فرآیند و پالیس تشدید (Escalation Policy) داشتند که طی آن در هنگام بروز مشکلات سلسله مراتب لازم جهت ارجاع و رفع مشکل انجام می شود.این سلسله مراتب شدت به ماهیت کسب و کار سازمان، اهداف، ماموریت ها، ابزار موجود و فرهنگ سازمانی وابسته است لذا نمی توان برای آن الگو و ساختار از پیش تعیین شده ای ارائه داد. نکته لازم به ذکر این است که در هر حال و در هر شرایطی می بایست واحد NOC در سازمان قوانین مدون و مشخصی جهت ارجاع در شرایط پس از وقوع رخداد داشته باشد.

جهت تعریف اینگونه ساختار ها و ماموریت ها و ظایف استفاده از Framework های استاندارد بسیار کمک کننده است. از آنجا که مبحث مورد نظر ما در واقع یکی از زیرمجموعه های IT است لذا جهت تعریف این ساختار ها، استفاده از استاندارد های ITIL توصیه می شود.

مفروضات در طراحی چهار چوب ساختاری واحد NOC

با توجه به تمامی توضیحات ارایه شده مشخص است که واحد NOC سنتی سازمان ها می بایست هرچه سریعتر پوست اندازی کرده و ساختار های تازه و پویای خود را تشکیل دهد. از آنجا که سه جزء اصلی و تشکیل دهنده این واحد **افراد، ابزار** و **فرآیند** ها هستند؛ این تغییرات می بایست نه تنها در بدنه کارشناسی و نیروی انسانی شکل گیرد، بلکه در حوزه ابزار، تکنولوژی ها و همچنین فرآیند ها نیز انجام شود. لذا چهارچوب اصلی این واحد می بایست بر اساس اصول ذیل بنا شود:

- **فرآیندهای کارا**

این مطلب به معنی زیر و رو کردن همه فرآیند ها نیست. بلکه به این مفهوم که با بررسی اهداف و ماموریت های سازمان و کلاسه بندی سرویس ها و فرآیند ها تا جای ممکن اقدام به تسهیل فرآیند های اجرایی شود. در این بخش اصل پارتو و قوانین 20-80 بسیار می تواند کمک کند به این مفهوم که غالبا 20 درصد از فرآیند ها هستند که 80 درصد از اهداف و ماموریت های سازمان را عهده دار هستند. لذا اولویت ایجاد تغییرات و تسهیل کردن آنها می بایست از همین 20 درصد فرآیند ها انجام شده و تا جای ممکن آنها رل ساده، کوتاه و قابل فهم و با خروجی های قاطع نمود.

تمرکز بر روی کارآیی

امروزه NOC ها می بایست بیشتر از دسترس پذیری تمرکز خود را برروی کار آیی معطوف دارند. به این مفهوم که در مانیتور کردن اجزا (دستگاه ها، لینک ها، سرویس ها و ...) نه تنها این مطلب را مد نظر قرار دهند که این سرویس ها در دسترس هستند؛ بلکه می بایست مد نظر قرار دهند که این سرویس ها به چه صورت و با چه کیفیتی برای مشتریان ارایه می شود. از آنجا که ارایه سرویس نا مناسب و با کیفیت پایین خود ضد تلبیغ برای سازمان و اهداف اوست لذا توجه به SLA مورد نظر و تصویب شده در مانیتورینگ می بایست مد نظر باشد.

- **کارشناسان باتجربه**

متاسفانه تجربه شخصی من این گونه نشان داده است که در بسیاری از سازمان های ما واحد NOC و یا مانیتورینگ محل ورود پرسنل جدید IT است. اشخاصی که تجربه کاری کم داشته و در واقع به این واحد تحت عنوان آموزشگاهی حین خدمت نگاه می شود. البته درست است که یکی از اصول اولیه هر سازمان تولید نیروی متخصص داخلی است زیرا نه تنها این نیرو ها بیشتر با ساختار سازمان و هنجار های آن آشنا میشوند بلکه تعهد اخلاقی و سازمانی بیشتری نیز پیدا می کنند. ولی باید به نسبت معقول بین افراد با تجربه و افراد کم تجربه تر دقت ویژه ای شود چرا که در صورت سهل انگاری در این بخش هیچکدام از اهدافی که پیشتر در باره آن توضیح داده شد میسر نمی شود.

- **ابزار های هوشمند و خودکار**

بسیاری از کارکنان NOC ها شیف کاری خود را با نشستن جلوی صفحات نمایش و اعلام رخدادها و واکنش هایی انجام می دهند که می توان آن ها را از طریق ابزار های هوشمند خودکار کرد. راهکار هایی چون EEMو Auto Alerting که توسط بسیاری از ابزار های هوشمند ارایه می شوند می تواند تا 25 درصد از وقت کارشناسان NOC را ذخیره کند. این ذخیره سازی زمان از دوجنبه برای سازمان مفید است. اول آنکه کارشناسان وقت بیشتری به منظور انجام و پیاده سازی فرآیند های پیشگیرانه و تحلیل شرایط سرویس ها دارند. و در نهایت دستیابی به SLA تفاهم شده ساده تر میسر است. دوم اینکه با 25 درصد ذخیره سازی در زمان کارشناسان NOC درواقع می توان خوش بین بود که اندازه واحد NOC نیز به نسبتی کوچکتر خواهد شد.

- **مجموعه ابزار های یکپارچه**

تعدد ابزار های مانیتوریگ و مدیریتی استفاده شده در واحد NOC در بسیاری از موارد نه تنها سود و آورده ای برای سازمان ندارد؛ بلکه به دلیل الگو های متفاوتی که این ابزار ها دارند گاها موجب سردرگمی و تحلیل های نادرست بالاخص برای کارشناسان کم تجربه تر خواهد شد. از این رو توصیه می شود تا جای ممکن از ابزار های یکپارچه و مجتمع در واحد NOC استفاده شود. علاوه بر این تعدد ابزار ها هزینه های جانبی نگهداری آنها را نیز شامل خواهد شد که این امر نیز برای سازمان ها مطلوب نیست. گفتنی است که موارد مربوط به راهکار های بشتیبان در مواقعی که ابزاری از دسترس خارج می شود کاملا معقول و پذیرفتنی است. در اینجا منظور تعدد بیرویه ابزار هایی است که نه تنها آورده ای جدید برای سازمان نداشته بلکه مشکلات و سردرگمی هایی را نیز به NOC و به طبع آن به سازمان تحمیل می کند.

- **تمرکز بر موارد امنیتی**

بنا بر تعریف ارایه شده از واحد NOC تحت عنوان چشم سازمان رعایت اصول امنیتی در این واحد بسیار حائز اهمیت است. مواردی چون حفظ محرمانگی، جلوگیری از روش های مهندسی اجتماعی، نشت اطلاعات، کلاسه بندی اطلاعات در هنگام ارجاع مشکلات و Escalation و ... همگی مواردی است که در هنگام تعریف فرآیند های اجرایی باید مد نظر قرارگیرد و پرسنل NOC ملزم به اجرای آنها گردند. از طرفی از آنجا که NOC نقطه مرکزی است که از طریق آن می توان به تمامی تجهیزات شبکه اشراف و دسترسی داشت لذا پیاده سازی الزامات امنیت در خصوص امنیت فیزیکی (تردد، پالیسی های BYOD، امنیت فیزیکی تجهیزات و ...) و همچنین امنیت ارتباطات و نرم افزار ها (استفاده است ارتباطات امن، رمز نگاری، ذخیره سازی امن اطلاعات، انتقال امن داده ها و اطلاعات،نرم افزار های مورد تایید امنیتی و ...) نیز می بایست به شدت مورد توجه قرار گیرد.

ساختار پیشنهادی جهت استقرار NOC

بر اساس توضیحات ارایه شده، ساختار نوین پیشنهادی جهت استقرار درون سازمانی واحد NOC از بخش های کلی زیر تشکیل می شود. از آنجا که گفته شد که واحد های جدید NOC مبتنی بر سرویس می بایست وظایف خود را انجام دهند؛ لذا می توان اینگونه انگاشت که واحد NOC هم سرویس های خاصی به سازمان ارایه می دهد که برای ارایه مطلوب این سرویس ها می بایست SLA مشخصی را رعایت کند. این SLA در بخش های زیر تعریف می شود و معیار های اندازه گیری آن به شرح ذیل است:

Measurement Parameter	Term
Uptime/Throughput	Network
Availability/Capacity	Service
Speed/Completion	Data Storage & Computing
Availability/Reliability	Power
Compliance	Environmental Control
Compliance	Facility Secure Access