RADCOM

شرکت رادکام

مروری بر استانداردهای امنیتی نرم افزار

بهار ۱۳۹۴

فهرست

مقدمه

امروزه در دنیای توانمند فناوری تکنولوژی، "اطلاعات" دارایی حیاتي برای کسب و کار سازمانها محسوب می شود. بنابراین تامین امنیت آنها بسیار مهم خواهد بود. عبارت "امنیت اطلاعات"، تنها به موضوع ساده حفاظت از نام کاربری و رمز عبور ختم نمی شود؛ مقررات و حریم خصوصی یا خط مشی های حفاظت از اطلاعات مختلف، یک تعهد پویا را برای سازمان ها به وجود مي آورد. در عین حال ویروسها، تروجان ها، فیشرها و ... برای سازمان تهدید به حساب می آیند. همچنین هکرها باعث به وجود آمدن خسارات زیادی برای سازمان می شوند، مانند دزدی اطلاعات مشتریان، جاسوسی استراتژی های کسب و کار به نفع رقبا، از بین بردن اطلاعات مهم سازمان که هر یک از آنها به تنهایی می تواند صدمات جبران ناپذیری را متوجه سازمان ها نماید. از این رو استفاده از یک سیستم مدیریت امنیت اطلاعات (ISMS) مناسب برای مدیریت موثر دارایی های اطلاعاتی سازمان الزامی به نظر می رسد.

تامین امنیت کاربردها و سرویس های ارائه شده در بستر وب و اینترنت، مانند پورتال ها و وب سایت ها با توجه به استفاده روز افزون از این خدمات توسط کاربران، کاری نیازمند توجه و سرمایه مناسب است. همزمان با توسعه تکنولوژی در این حوزه، مباحث تامین امنیت نیز از ساختار، روشها و توصیه های عملکردی فراتر رفته است و در هر لایه از بستر ارتباطات بین کاربر نهایی و سرویس دهنده استانداردها، روشها و فرا روشهای زیادی تدوین گردیده است. امروزه کلیه ابزارها و کاربردها بیشتر از آن که وصله های توسعه کاربردی داشته باشند، با تعدد زیاد، وصله های تکامل تمهیدات امنیتی دارند. بخش عمده ای از سرمایه توسعه در تمامی بخش های بستر وب، به تکامل تمهیدات امنیتی اختصاص دارد.

در کنار این مسئله که کلیه ارائه دهندگان سرویس ها، خدمات، ابزارها و تجهیزات بکار رفته در اینترنت، امروزه بخشی از موفقیت خود را در امن سازی هر چه بیشتر محصول و خدمات خود می دانند، نهادهای مستقل از بخش تجاری نیز، دست به کار شده اند و به صورت پیوسته، استاندارد هایی را چه برای تعاریف، و چه معیارهای ارزیابی و سنجش نفوذ پذیری و یا میزان امن بودن کاربردها و سرویس های مبتنی بر وب و زیرساخت ها، تدوین و تکمیل می نمایند.

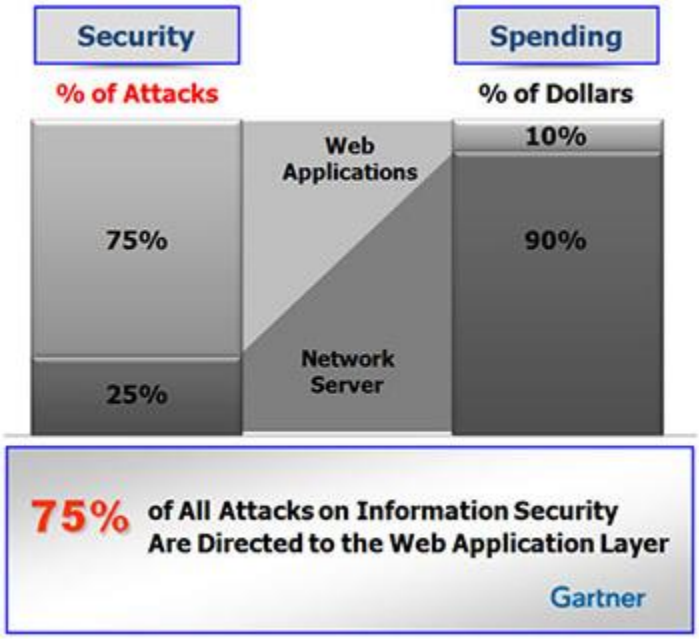
فصل اول: اصول امنیتی

بررسی حجم حملات نفوذ در حوزه های مختلف وب و اینترنت

برای بررسی آسیب پذیری‌ها و به لحاظ حوزه ای با چشم پوشی از بعضی جزئیات می توان انواع حملات نفوذ را در بخش های ذیل دسته بندی نمود:

- ✓ معماری شبکه، سرویس ها و تجهیزات (پیکربندی سوئیچها، روترها، DNS و...)
- ✓ نرم افزارهای وب سرور و سیستم عامل (... ,WINDOWS, LINUX ... ,APACHE, IIS)
- ✓ پلتفورم وب / تکنولوژی توسعه (... ,PHP, Java EE, .NET)
- ✓ سرور پایگاه داده و انباره اطلاعات (... ,MySQL, MS-SQL, ORACLE, SYBASE)
- ✓ برنامه ها و کاربردهای وب (... ,Portal, WebSite, WebService, Blog, Forum)
- ✓ کاربران و سرویس گیرندگان (... ,Client App, Browser, Mobile App)

از بین کلیه بحش های ذکر شده مراقبت همه جانبه در مقابل حملات به برنامه ها و کاربرد های وب از اهمیت بسیار زیادی برخوردار است زیرا براساس گزارش موسسه تحقیقات گارتنر، ۷۵% از حملات نفوذ امنیتی به برنامه ها و کاربردهای وب و ۲۵% مابقی روی سایر حوزه های ذکر شده در بالا متمرکز بوده است. این در حالی است که فقط ۱۰% از سرمایه گذاری برای ایجاد امنیت در خصوص برنامه ها و کاربردهای وب انجام می شود و ۹۰% سرمایه گذاری در بخش ایجاد تمهیدات امنیتی سایر حوزه ها به ویژه امنیت شبکه انجام می شود.



شکل۱- نتیجه تحقیقات گارتنر

لذا با توجه به این که حجم حملات نفوذ امنیتی صورت گرفته روی لایه کاربرد وب زیاد است و از طرفی در حال حاضر میزان سرمایه گذاری آن در برابر حملات بسیار پایین تر از سایر حوزه ها است، مراقبت و امنیت در این حوزه اهمیت ویژه ای پیدا خواهد کرد.

زمینه های ارزیابی و تحلیل امنیت

ارزیابی و تحلیل امنیت یک سیستم می تواند در زمینه های زیر بررسی شود:

۱. شناسايي شبكه و ساختار آن: در اين بخش به كمک ابزارها و روش هاي مختلف، سعي مي شود اطلاعات شبكه انتخابي تا حد زيادي استخراج گردد.
۲. كشف و پويش پيرامون سيستم هاي عامل مختلف: با توجه به اهميت سيستم عامل ميزبانها، در اين بخش اطلاعات مربوط به سيستم هاي عامل مهم اعم از Server ويا Client استخراج مي شود. از جمله موارد مي توان به استخراج پورتهاي باز، بررسي حفاظها و تجهيزات امنيتي (Firewall)، بررسي سرويسها و ... اشاره نمود.
۳. پويش پورتها در شبكه: با توجه به اهميت پورتهاي باز، در اين بخش به بررسي دقيق تر پورتها در بخش هاي مختلف شبكه مي پردازيم.
٤. بررسي كلمات رمز عبور: براي تجهيزات مهم و Server ها، از روش هاي مختلف جهت كشف رمزهاي عبور استفاده مي شود.
٥. آزمون بر روي تجهيزات: Cisco با توجه به اهميت تجهيزاتCisco، در اين بخش در چندين گام تجهيزات موجود از شركت Cisco به صورت خاص مورد آزمون و حمله قرار مي گيرند.
٦. آزمون بر روي Server ها به صورت خاص: هر Server متناسب با سرويس هايي كه دارد پتانسيل حمله و نفوذ دارد. به همين دليل Serverها بر اساس سرويس هاي خود (DB، WEB، MAIL و...) مورد آزمون قرار مي گيرند.
۷. بررسي شبكه هاي بي سيم: با توجه به اهميت امنيت شبكه هاي بيسيم و در صورت وجود چنين شبكه هايي، آزمون هاي مختلف بر روي آن انجام مي شود.
۸. تخمين آسيب پذيري: در اين بخش با استفاده از پويشگرهاي مختلف (مانند NESSUS و...) و با توجه به دانش به دست آمده و به كمک پايگاه هاي اطلاعاتي آسيب پذيري ها، ميزبانهاي فهرست شده مورد آزمون قرار مي گيرند.
۹. نفوذ: براساس دانش و اطلاعات بخشهاي قبلي، در صورت امكان و تمايل مشتري، حملات مختلف مانند DoS ، arp poisoning و ... بر روي ميزبان ها و شبكه انجام مي شود.

۱۰. استخراج و تهیه گزارش تحلیلي

راهکار امنیت در نرم افزارهای تحت وب

سیستم‌های مبتنی بر وب، ضمن کاهش هزینه‌ها، حجم بیشتر و سطح دسترسی بالاتری از اطلاعات را به کارکنان و مشتریان سازمان‌ها ارائه می‌دهند. به همین دلیل موضوع "امنیت" در این سیستم‌ها اهمیت ویژه‌ای پیدا می‌کند .توسعه‌دهندگان نرم‌افزار نیز، نگاه جدی به موضوع امنیت داشته و راهکارهای آن را در طراحی‌های خود مدنظر قرار داده‌اند. در این زمینه، نرم‌افزارهای اداری تحت وب باید گواهی بلوغ امنیتی را از مرکز تحقیقات انفورماتیک ایران دریافت کنند. این گواهینامه، ویژگی‌های محرمانگی، صحت داده‌ها، صحت سیستم و مدیریت امنیت تائید می‌کند .

برخی راهکارهای امنیتی نرم‌افزارهای تحت وب عبارتند از:

احراز هویت دو عامله با استفاده از توکن های امنیتی

سیستم های اتوماسیون اداری تحت وب با امکان جدید احراز هویت دوعامله به کاربران خود امکان می دهند که با اطمینان بیشتری وارد سیستم های خود شوند. در این راه حل از توکن های سخت افزاری به عنوان عامل دوم امنیت در کنار سیستم کلمات عبور سابق استفاده میشود. به این صورت که، کاربران به هنگام ورود به سیستم علاوه بر وارد نمودن کلمه عبور خود، لازم است توکن سخت افزاری خود را نیز وارد سیستم نمایند تا احراز هویت صورت پذیرد.

مدیریت نشست کاربران

در سیستم های اتوماسیون اداری تحت وب هنگام شناسایی کاربران و همچنین مدیریت نشست آنها موارد امنیتی متعددی لحاظ شده است. این موارد در بخش های مختلف سیستم در نظر گرفته شده است. از جمله این موارد می توان به نکات زیر اشاره کرد:

- خروج خودکار از سیستم پس از گذشت زمان مشخص بدون فعالیت
- خروج خودکار از سیستم در صورت استفاده تکراری از شناسه کاربری
- غیر فعال شدن شناسه کاربری در صورت چند بار تلاش ناموفق جهت ورود به سیستم
- اعمال محدودیت در ورود تعداد کاربران برخط با استفاده از قفل سخت افزاری
- امکان مشاهده لیست کاربران برخط و امکان انقضای نشست آنها توسط راهبر
- الزام به تغییر کلمه عبور در اولین ورود به سیستم

پشتیبانی از SSL و پروتکلhttps

پروتکل SSL از لحاظ لغوی مخفف Secure Sockets Layer می‌باشد و در واقع یکی از پروتکل‌های انتقال اطلاعات روی وب است. در حال حاضر رایج‌ترین پروتکل انتقال امن اطلاعات در وب می‌باشد، به شکلی که مرورگر اینترنتی از وجود چنین امکانی در سرور باخبر شده و از یک Public Keyموجود در مرورگر استفاده کرده و اطلاعات را به صورت کد شده به سرور می‌فرستد و این تنها سرور است که با استفاده از Private Key خود اطلاعات دریافتی را می‌تواند Decodeکند. به علت اینکه آن Private Keyتنها در سرور نصب شده است، هیچ نرم افزار دیگری در بین راه نمی‌تواند آن اطلاعات را مشاهده کند. علاوه بر اینکه اطلاعات و داده‌ها بین مرورگر و سرور با استفاده از این پروتکل بطور امن مبادله می‌شوند، ارتباط بین سرور و سرورهای پست الکترونیک (ایمیل)، دورنویس (فکس) و پویش (اسکن) هم می‌تواند با استفاده از این پروتکل، امن شود.

پشتیبانی از امضای دیجیتال اسناد موجود در برنامه

در سیستم اتوماسیون اداری تحت وب، کاربر دارای مجوز امضای دیجیتال یک توکن سخت‌افزاری حاوی کلید خصوصی دارد که مختص اوست. به هنگام امضای سند، کاربر توکن سخت‌افزاری خود را به پورت USBکامپیوتر خود متصل می‌کند و سند مذکور با استفاده از کلید خصوصی کاربر که در توکن ذخیره شده است، امضاء می‌شود. قبل از امضاء کردن، سیستم با مکانیزم خاصی مانند بررسی کد ملی و یا شماره سریال توکن، از تعلق توکن به کاربر مورد نظر اطمینان حاصل می‌کند و سپس به وی اجازه امضاء کردن را می‌دهد. امضای دیجیتال در سند از نوع PDF درج می‌شود و بررسی صحت و درستی امضاء و کسب اطمینان از عدم تغییر محتوای سند، در PDF انجام می‌شود.

امکان تعریف سیاست های تعریف و نگهداری کلمه عبور

ایجاد و مدیریت کلمات عبور(Password Policy) ، امکان کنترل چگونگی ایجاد و مدیریت کلمات عبور برای افزایش امنیت را فراهم می‌کند. مثلا می‌توان حداکثر زمان استفاده از یک کلمه عبور را قبل از آن که کاربر مجبور به تغییر آن شود، تعیین نمود. تغییر کلمات عبور امکان نفوذ اشخاص غیر مجاز را به داخل سیستم کاهش می‌دهد. مجبور ساختن کاربران در تغییر کلمات عبور موجب می‌شود اگر یک کاربر غیر مجاز نام یک کاربر و کلمه عبور را به دست آورد، دیگر نتواند وارد سیستم شود. تنظیمات دیگری نیز در Password Policyبرای افزایش امنیت در سیستم اتوماسیون وجود دارد. برای مثال، می‌توان برای کلمات عبور حداقل طول مشخص کرد. طولانی بودن کلمه رمز سبب می‌شود که تشخیص آن بسیار مشکل شود. ملزم ساختن کاربران به استفاده از کلمات عبور طولانی، الزام به ترکیبی از حرف و عدد بودن کلمات عبور، تعیین سیاست‌هایی برای منقضی شدن کلمات عبور، جلوگیری از استفاده مجدد از کلمات عبور منقضی شده و تکراری و سیاست‌های امنیتی دیگر موجب افزایش امنیت در سیستم اتوماسیون اداری تحت وب خواهد شد.

سایر مواردی که در امنیت سیستم در نظر گرفته می شود عبارتند از:

- مقابله با تهدیدهای امنیتی در وب از جمله SQL & code injection ، Sniffingو...
- کد کردن متن نامه ها و نگهداری آنها در داخل پایگاه داده
- رویدادنگاری تمام وقایع سیستمی
- امکان تعریف حقوق دسترسی در سطح Record Level به منابع سیستم
- امکان تعریف پروفایل امنیتی جهت کنترل محدوده زمانی ورود به سیستم
- امکان تعریف پروفایل امنیتی جهت کنترل IP کلاینت ها

RCII

مرکز تحقیقات صنایع انفورماتیک

شماره: ۴۸۵۳ - ر - ۹۲

گواهی سطح بلوغ امنیتی محصول

نرم افزار اتوماسیون	نسخه: ۱۱۱۷	فایرا
ردیف	حوزه ارزیابی	وضعیت محصول
۱	شناسایی	٪۱۰۰
۲	اعتبار سنجی: الزامات عمومی	٪۱۰۰
۳	اعتبارسنجی: الزامات مکانیزم	٪۸۱
۴	محرمانگی	٪۱۰۰
۵	صحت داده	٪۱۰۰
۶	بررسی لاگ‌ها (ممیزی)	٪۸۹
۷	منهدم کردن داده	٪۱۰۰
۸	صحت سیستم	٪۱۰۰
۹	مدیریت امنیت	٪۷۱
۱۰	راهنما	٪۱۰۰
۱۱	عدم انکار	٪۱۰۰

جهت کسب اطلاعات بیشتر به گزارش گواهی پیوست این گواهی رجوع نمایید.

گزارش گواهی شامل ۱۴ صفحه و تمام صفحات ممهور به مهر برجسته مرکز می‌باشد.

شکل ۲- نمونه گواهی بلوغ امنیتی محصول

استاندارد های امنیتی

امروزه استانداردهاي مختلفي در زمينه‌ي امنيت اطلاعات وجود دارد که منجر به امنیت اطلاعات می شوند و هر كدام از ازويه‌ي مشخصي به اين مهم مي‌پردازند. از جمله‌ي اين استانداردها مي‌توان به موارد زير اشاره نمود:

۱. استاندارد معيار عام (CC) و متدولوژي‌هاي مربوطه(CEM)

در آزمون مبتنی بر[1]CC ، با توجه به تهدیدات وارده به یک محصول فناوری اطلاعات، اهداف امنیتی مربوطه تعریف گشته و بر اساس این اهداف، عملیات انطباق با کلاس‌های وظیفه‌مندی و کلاس‌های ارزیابی انجام شده و آزمون مرتبط با محصول، در هر سطح با توجه به آن اجرا می‌شود. CC به آزمون محصولات IT از منظر امنيت مي‌پردازند. اين استاندارد داراي هفت سطح امنيتي است كه از EAL1 تا EAL7نامگذاري شده‌اند. به دليل كاربرد بسيار بالاي آن، در حال حاضر اين استاندارد با نام ISO/IEC 15408شناخته مي‌شود.

گواهی‌های EAL یا Evaluation Assurance Level مطابق استاندارد امنیتی Common Criteria یا ISO/IEC 15408 تعیین می‌شوند و یک رتبه‌بندی عددی (از ۱ تا ۷) از میزان دقت و عمق تست‌هایی هستند که برای امنیت یک محصول انجام شده است.

تفاوت EAL1 با EAL7 در نحوه‌ی تست‌هایی است که انجام می‌شود و دقتی که این تست‌ها دارند و ارتباط مستقیمی با میزان امنیت یک محصول ندارد بلکه در واقع نشان می‌دهد چقدر می‌توان به نتیجه تست اعتماد کرد.

- ✓ EAL1: تست عملکرد

کاربرد این تست زمانی است که نیاز به اعتماد سازی در عملکرد صحیح باشد اما تهدید های امنیت زیاد جدی نیست. این تست در مواردی که مستقل بودن باید تضمین شود برای حمایت مشاجره در حفاظت اطلاعات شخصی یا عمل مشابه آن ارزشمند خواهد بود.

این تست یک ارزیابی از هدف به عنوان مشتری دارد که شامل تست غیروابسته بودن برخلاف خصوصیات و بررسی اسناد هدایت است. این تست می تواند بدون کمک از توسعه ارزیابی تست به صورت موفقیت

[1] Common Criteria

آمیز و با هزینه اندک انجام شود. در این مرحله ارزیابی باید شواهدی مبنی بر این که ارزیابی هدف بنا به شیوه اسناد است و حفاظت در مقابل تهدیدات مفید ایجاد می کند.

بر طبق این گواهی، سیستم مزبور، مجوز استفاده از نشان امنیت و کیفیت را خواهد داشت. آزمایشگاه های «امنیت و کیفیت نرم‌افزار»، این محصول را در حوزه های مختلفی چون محرمانگی و رازداری، امنیت پایگاه داده، مدیریت امنیت، تسخیر کوتاه مدت، قابلیت استفاده، کارآیی، قابلیت اطمینان و ... ارزیابی و در نهایت سطح کسب شده را بر اساس امتیازات لازم احراز می نمایند.

- ✓ **EAL2: تست ساختار**

EAL2 نیاز شرکت ها از نظر تحویل طراحی اطلاعات و نتایج تست را بررسی می کند، اما بهتر است نسبت به سازگار بودن با تجارت خوب تلاش بیشتری در بخش برنامه نویسی تقاضا نشود. به همین دلیل بهتر است سرمایه گذاری در هزینه ها و زمان به طور قابل ملاحظه ای افزایش یابد. همچنین در مواردی که برنامه نویسان و کاربران به یک سطح امنیتی مستقل و پایین در نبود دسترسی به سابقه کامل توسعه، همانند سییستم های قدیمی، نیاز دارند استفاده می شود.

- ✓ **EAL3: تست متد و بررسی**

اجازه به دست آوردن بالاترین تضمین از مهندسی امنیت در سطح طراحی بدون تحول ذاتی در توسعه های موجود به برنامه نویس وظیفه شناس را می دهد. این استاندارد در مواقعی که برنامه نویسان و کاربران به سطح امنیتی مستقل و میانه نیاز دارند و نیز به رسیدگی کامل به TOE[۲] و توسعه بدون مهندسی اساسی مجدد نیاز است، استفاده می شود.

- ✓ **EAL4: تست و بررسی متد طراحی شده**

اجازه به دست آوردن بالاترین تضمین از مهندسی امنیت مثبت بر اساس توسعه تجاری خوب که هر چند سخت، نیاز به دانش و مهارت و منابع تخصصی ندارد، را به برنامه نویسان می دهد. EAL4 بالاترین سطحی است که به طور مشابه به صورت اقتصادی مقاوم سازی خط محصول موجود را امکان پذیر می سازد. بنابراین آن موقعیت هایی که برنامه نویسان و کاربران نیاز به سطح امنیتی مستقل در محصول مرسوم TOE را امکان پذیر می کند و موجبات امنیت خاص و اضافه ای برای هزینه های مهندسی را مهیا می کند. در EAL4 سیستم های عامل تجاری مرسوم که ویژگی امنیت بر اساس کاربران را فراهم می کنند، ارزیابی می شوند. مانند سیستم های عامل AIX, HP-UX, FreeBSD, Oracle Linux, Novell NetWare, Solaris, SUSE Linux Enterprise Server 9, SUSE Linux Enterprise Server

[2] Target Of Evalution-محصول یا سیستمی که مورد ارزیابی قرار می گیرد

10,[3] Red Hat Enterprise Linux 5, Windows 2000 Service Pack 3, Windows 2003, Windows XP, Windows Vista, Windows 7, Windows Server 2008 R2 z/OS version 2.1 and z/VM version 6.3

در سیستم های عاملی که چندین سطح امنیتی را فراهم می کنند، EAL4 در پایین ترین سطح ارزیابی شده است. مانند Trusted Solaris, Solaris 10 Release 11/06 Trusted Extensions, an early version of the XTS-400, and VMware ESXi version 3.0.2, 3.5, 4.0 and 5.0 (EAL 4+)

این گواهینامه بدین معنا است که اکنون امکان استفاده کاملا امن و قابل اطمینان بر پایه محصولات مبتنی بر لینوکس و بر اساس استانداردهای دولتی وجود دارد.

- ✓ EAL5: طراحی و آزمون نیمه رسمی

اجازه به دست آوردن بالاترین تضمین از مهندسی امنیت بر اساس توسعه تجاری دقیق که توسط برنامه و تکنیک های مهندسی امنیت مخصوص تضمین می شوند را به برنامه نویسان می دهد. همانند TOE که احتمالا با هدف دستیابی به ضمانتEAL5 طراحی و توسعه داده می شود. به طور مشابه برای EAL5 هزینه های اضافه نسبت به توسعه دقیق با به کار بردن تکنیک های خاص که بزرگ نخواهد بود، نیاز است. لذا EAL5 برای شرایطی که برنامه نویسان و کاربران به نیاز به سطح امنیتی بالایی از کاربرد امنیت مطمئن و مستقل در نقشه توسعه و نیز توسعه دقیق بدون پرداخت بی دلیل هزینه عوارض برای تکنیک های مهندسی امنیت خاص نیاز دارند، خواهد داشت.

دستگاه های کارت های هوشمند متعدد با EAL5 توسعه داده شده اند. مانند دستگاه های ایمن چند سطحی مانند رابط های تعاملی Tenix و سیستم عاملXTS-400 که با هدف عمومی با EAL5 ارزیابی شده است. LPAR روی سیستم نیز IBM گواهینامه EAL5 را دارد.

- ✓ EAL6: تایید طراحی و آزمون نیمه رسمی

اجازه به دست آوردن بالاترین تضمین از مهندسی امنیت از کاربرد تکنیک های مهندسی امنیت به توسعه دقیق به منظور تولید TOE برای حفاظت از ارزش دارایی بالا بر خلاف خطر های قابل توجه را به برنامه نویسان می دهد. لذا EAL6 برای توسعه امنیت TOE برای وضعیت هایی با خطر بالا که از دارایی هایی که هزینه های اضافه را تراز می کند، محافظت می کند، کاربرد خواهد داشت.

نرم افزار INTEGRITY-178B گواهینامه EAL6 دارد.

- ✓ EAL7: تایید طراحی و آزمون رسمی

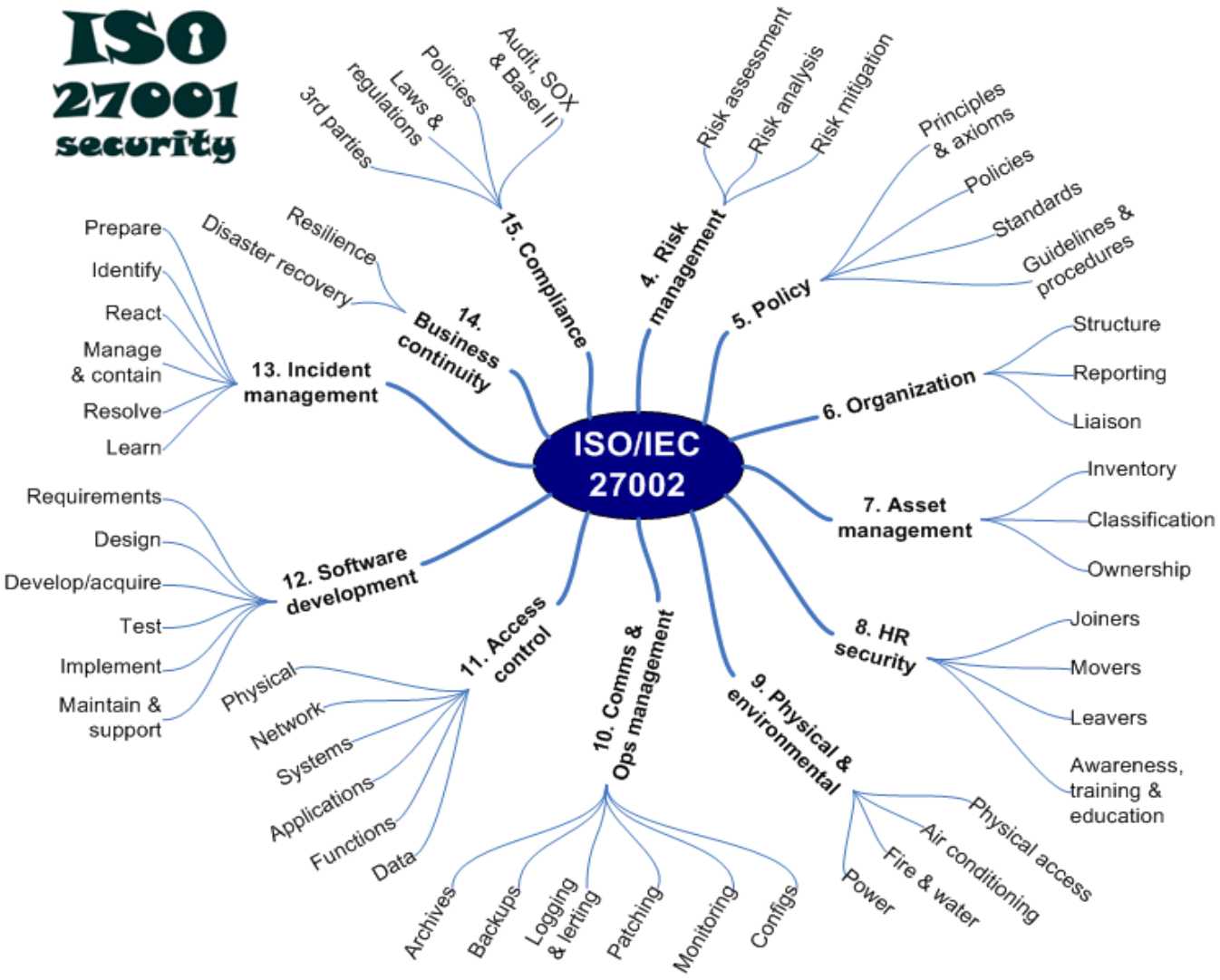
EAL7 در توسعه امنیت برنامه های TOE با وضعیت های خطر بسیار بالا و مواردی که دارایی های تراز هزینه بالاتری دارند، کاربرد دارد. اخیرا برنامه های عملی EAL7 به TOE ها با تمرکز زیاد بر روی قابلیت امنیت که متمایل به تحلیل رسمی و وسیع است، محدود شده اند. رابط تعاملی Tenix و Fox-IT مدعی داشتن گواهینامه EAL7 هستند.

سیستم های CEM برای کنترل دسترسی های امنیتی به کار می رود. در لیست زیر مواردی که جهت تنظیم سیستم های CEM در کانادا استفاده می شود لیست شده است:

۱. تصمیم در مورد این که از چه ویژگی های یکپارچه ای استفاده می شود.
۲. ایستگاه های خودکار تنظیم شود.
۳. دنبال کردن تراکنش های خودکار تنظیم شود.
۴. سنجش تراکنش های بلادرنگ تنظیم شود.
۵. بررسی این که ویژگی های یکپارچگی به درستی عمل می کنند.

۲. استاندارد ISO 27001

جهت تولید و توسعه‌ي سیاست‌هاي امنیتي یك سازمان استفاده مي‌شود. این استاندارد فرایند کامل امنیت را در یك سازمان بیان مي‌کند. استاندارد بین المللی ISO27001 الزامات ایجاد، پیاده سازی، پایش، بازنگری، نگهداری و توسعه ISMSدر سازمان را مشخص می کند. این استاندارد برای ضمانت انتخاب کنترل های امنیتی به جا و مناسب برای حفاظت از دارایی های اطلاعاتی، طراحی شده است. زمانی که یک سازمان موفق به دریافت گواهینامه مربوط به استاندارد ISO27001امی گردد، به این معنی است که آن سازمان توانسته امنیت را در زمینه اطلاعات خود مطابق با بهترین روش های ممکن مدیریت نماید. این استاندارد (به خصوص نسخه ۲۰۱۳ آن) برای پیاده سازی در انواع سازمان های دولتی، خصوصی، بزرگ و یا کوچک مناسب است. در ایران با توجه به تصویب سند افتا توسط دولت و الزامات سازمان هاي بالادستي در صنعت هاي مختلف، کلیه سازمان ها و نهادهای دولتی، ملزم به پیاده سازی ISMSگردیده و اکثر این سازمان ها به پیاده سازی الزامات استاندارد ISO27001 رو آوردند. علاوه بر این که استاندارد ISO27001 خود حاوی کنترل های امنیتی جامعی جهت تضمین امنیت سازمان است، همچنین می تواند به عنوان یک بستر مدیریتی جهت پیاده سازی کنترل های امنیتی بیشتری که در استانداردهای دیگر وجود دارد، مورد استفاده قرار گیرد.



شكل۳- استاندارد ISO27002

۳. استاندارد COBIT

يك چارچوب و مجموعه‌اي از ابزارها براي مديريت IT مي‌باشد كه توسط انجمن ISACA و انستيتوي ISTGطراحي شده‌است. اين استاندارد شامل كنترل‌هاي سطح بالا براي امنيت سيستم مي‌باشد و شامل امنيت مديريت شده، كنترل‌هاي دسترسي منطقي، امنيت داده‌هاي برخط، كنترل‌ها و امنيت حساب‌هاي كاربري، معماري‌هاي حفاظ (Firewall) و رده‌بندي داده‌ها مي‌باشد. COBIT یک گواهینامه است که توسط ISACA و موسسه مدیریت IT (ITGI) در سال ۱۹۹٦ به وجود آمد. این استاندارد چارچوبی برای مدیریت فناوري اطلاعات است. این استاندارد با رویکردی فرآیندگرا در ٤ دامنه و ۳٤ فرآیند و مجموعه ای از ۳۱۸ هدف کنترلی در حوزه ارزیابی فناوری اطلاعات تدوین شده است و مجموعه ای از سنجه ها، شاخص ها، فرآیندها و بهترین تجارب را برای کمک به مدیران، ممیزان و کاربران IT ارائه می دهد.

COBIT دارای پنج حوزه تمرکز بر مدیریت فناوري اطلاعات است: تنظیم استراتژیک، تحویل ارزش، مدیریت منابع، مدیریت ریسک، اندازه گیری کارایی . پیاده سازی و به کارگیری COBIT در سازمان ها، برای مدیران چارچوبی را فراهم می آورد تا به کمک آن بتوانند برنامه استراتژیک IT، معماری اطلاعاتی، نرم افزارها و سخت افزارهای مورد نیاز IT و کنترل عملکرد سیستم های IT سازمان خود را طراحی نمایند و با کمک این ابزارها به تصمیم گیری و سرمایه گذاری های مرتبط با فناوری اطلاعات بپردازند.

٤. استاندارد PCI DSS

استاندارد امنیت اطلاعات در صنعت کارت پرداخت (PCI DSS) یک استاندارد امنیت اطلاعات جهانی است که توسط انجمن استانداردهای امنیت صنعت کارت پرداخت برای افزایش امنیت کارت های اعتباری ایجاد شد. این استاندارد اختصاصاً برای سازمان هایی مفید است که در زمینه کارت های اعتباری، کیف الکترونیک، ATM، POS و... اطلاعات مشتریان را نگهداری، پردازش یا مبادله می کنند. اعتبار این استاندارد به صورت سالیانه بررسی می شود. برای سازمان های بزرگ بررسی انطباق توسط یک ارزیاب مستقل انجام می شود اما سازمان های کوچکتر می توانند انطباق خود را توسط پرسشنامه خود ارزیابی بررسی نمایند.

٥. استاندارد ITIL

ITIL یک چارچوب عمومی است که بر پایه تجارب موفق در مدیریت سرویس های IT در سازمان های دولتی و خصوص در سطح بین المللی به وجود آمده است. ITIL در اصل یک استاندارد نیست بلکه چارچوبی است با نگاهی نوین برای بهبود ارائه و پشتیبانی خدمات فناوری اطلاعات که امروزه از سوی سازمان های ارائه دهنده خدمات فناوری اطلاعات بسیار مورد توجه قرار گرفته است. هدف اولیه این چارچوب این است که مطمئن شود سرویس های IT با نیازهای کسب و کار سازمان منطبق است و در زمانی که کسب و کار به آن نیاز دارد پاسخگوی این نیاز است. ITIL به عنوان مجموعه ای از کتاب ها به وجود آمده و بر پایه مدل دمینگ و چرخه PDCA ایجاد شده، نسخه ی فعلی ITIL که مورد استفاده است، نسخه سوم می باشد که ۵ بخش اصلی را در بر دارد: استراتژی خدمات، طراحی خدمات، تحویل خدمات، اداره خدمات، بهینه سازی پیوسته خدمات. همانطور که بیان شد، ITIL بیشتر در شرکت هایی که کسب و کار IT دارند مورد توجه قرار گرفته است.

٦. انستيتوي NIST

رهنمودهاي مهمي را در زمينه‌ي آزمون‌هاي امنيتي شبکه به خصوص در رابطه با سيستم‌هاي عامل بيان مي‌کند.

۷. استاندارد BASEL II

يك استاندارد امنيتي براي بانكداري اينترنتي مي‌باشد. اين استاندارد شامل كنترل‌هاي امنيتي متعددي از جمله "تصديق هويت مشتريان"، "فرايند عدم انكار تراكنش‌هاي برخط"، "كنترل‌هاي مجوزدهي"، "جامعيت داده‌ها در تراكنش‌هاي برخط"، "روش‌هاي وارسي" و "محرمانگي اطلاعات بانكي" مي‌باشد.

۸. استاندارد ISO 21188

چارچوبي براي زيرساخت كليد عمومي (PKI) در سرويس‌هاي مالي تعيين مي‌كند. همچنين راه‌حل‌هاي مبتني بر گواهي‌هاي امنيتي را در زمينه‌ي بانكداري اينترنتي بيان مي‌كند.

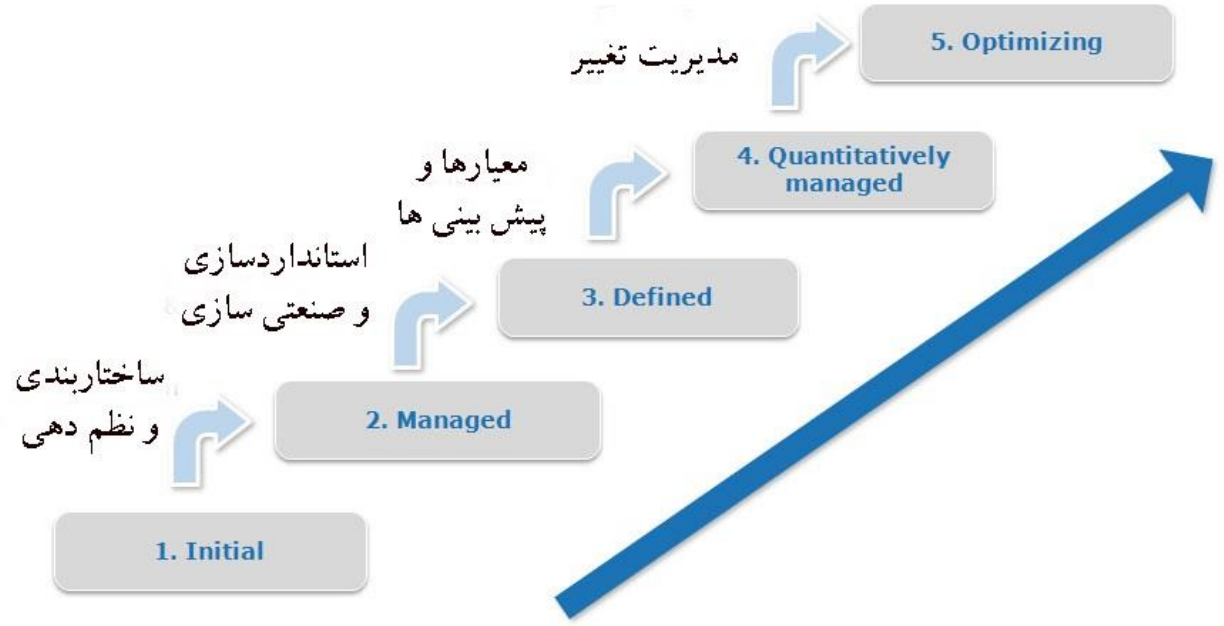
۹. FISCAM

جهت ارزيابي كنترل‌هاي كاربردي و عمومي براي سيستم‌هاي مالي طراحي شده‌است. اين استاندارد براي طراحي و توليد يك نرم‌افزار و يا برنامه‌ي كاربردي امنيتي بسيار مفيد است.

۱۰. CMMI

مدل بلوغ فرآیندی (Capability Maturity Model Integration, CMMI[3]) یک چهارچوب ثابت شده در صنعت است که برای بهبود کیفیت محصولات و توسعه ی کارایی برای نرم افزار و سخت افزار می باشد و دارای پنج مرحله برای توصیف سطح بلوغ سازمان است. مدل بلوغ CMMI ، با بکارگیری دانش و تجارب در مدیریت فرآیندها و با تکیه بر این اصل که « کیفیت سیستم یا محصول شدیدا متاثر از فرآیندی است که در توسعه و نگهداشت آن به کار رفته است»، ایجاد شده است. این مدل بارویکردی سیستمی و فراگیر، سازمان را در جهت بهبود فرآیندها و رسیدن به اهداف کسب وکار به پیش می‌برد. بسیاری از شرکت ها مانند موتورولا و اریکسون در ارائه ی این تعریف از CMMIدخیل بوده اند CMMI . به عنوان مدلی برای بهبود و پیشرفت کسب و کار بینان نهاده شده است.

[3] Capability Maturity Model Integration



شکل ۴- سطوح CMMI

سطوح CMMI

سطح بلوغ ۱، آغاز (Initial): سطح بلوغ اول با فرآیندهای انجام شده سر و کار دارد، در این سطح فرآیندها غیرقابل پیش بینی، کنترل ضعیف و به صورت واکنشی و انفعالی هستند. عملکرد فرآیندها، ثابت نمی ماند و به اهداف خود مانند کیفیت، هزینه و زمان بندی نمی رسد، اما کارهای مفیدی می تواند انجام گیرد.

سطح بلوغ ۲، مدیریت شده در سطح پروژه ها (Managed at the Project Level): این سطح از بلوغ با فرآیندهای مدیریت شده سر و کار دارد. فرآیندها در این سطح دارای برنامه ریزی، مستندسازی، کنترل و نظارت هستند اما هم چنان به صورت واکنشی و انفعالی انجام می گیرند. یک فرآیند مدیریت شده، فرآیند انجام شده ای است که:

- ✓ **برنامه ریزی شده و اجرا شده بر اساس سیاست ها و رویه هاست.**
- ✓ **افراد ماهر را به کار می گیرد.**
- ✓ **خروجی ها کنترل شده هستند.**
- ✓ **ذینفعان را درگیر می کند.**
- ✓ **فرآیند برای تطبیق با نیازمندی های بازبینی و ارزیابی می شوند.**
- ✓ **یک فرآیند مدیریت شده به دستیابی به اهدافی چون کیفیت، هزینه و زمانبندی نزدیک تر است.**

سطح بلوغ ۳، تعریف شده در سطح سازمانی (Defined at the Organizational Level): این سطح با فرآیندهای تعریف شده و مشخص شده سر و کار دارد. یک فرآیند تعریف شده فرآیندی است که :

- ✓ به خوبی در تمام سطوح سازمان تعریف شده و به اجرا درآمده است.
- ✓ فرآیندها، استانداردها، رویه ها، ابزار و ... در سطح سازمانی تعریف شده اند
- ✓ فرآیندها به صورت کنشی و منفعل هستند.

سطح بلوغ ٤، مدیریت کمی (Quantitatively Managed): در این سطح، علاوه بر فرآیندها و زیرفرآیندهای پروژه ها، سازمان نیز بر اساس آمار و ارقام مدیریت می شوند.

سطوح بلوغ ٥، بهینه سازی (Optimizing): بهینه سازی عملکرد به منظور شناسایی و حذف معایب درون فرآیندها در این سطح انجام می گیرد و سپس فعالیتهای بهبود برای شناخت و استقرار ابزارهای جدید برای دستیابی به اهداف کسب و کار انجام می شوند.

ویژگی های یک CMMI موفق

- ✓ تعهد- تعهد سازمان و مدیریت به رویه ها و سیاست و منابع برای انجام کار
- ✓ توانایی- به کارگیری کارمندان و ابزارهای مناسب و توانا برای انجام کار
- ✓ فعالیت های انجام شده - مستندسازی و مصاحبه برای اطمینان از پیاده سازی رویه ها و سیاست ها
- ✓ سنجش و تحلیل- به کارگیری سنجه ها و دیگر ابزارها برای ارزیابی اثربخشی فرآیندها
- ✓ بازبینی پیاده سازی- اجرای یک بازبینی و ارزیابی مستقل فرآیندها

۱۱. PMMM

مدل بلوغ مدیریت پروژه PMMM راهنمایی برای دستیابی سازمان ها به بلوغ است. پروفسور هارولد کرزنر، توسعه دهنده این مدل، معتقد است که بلوغ یک سازمان زمانی اتفاق می افتد که آن سازمان قادر به برنامه ریزی راهبردی و استراتژیک برای مدیریت پروژه باشد. ارزیابی توسط این مدل در واقع یک خودارزیابی پیشرفته است که سازمان می تواند از آن برای طریق سطح بلوغ خود را ارتقاء دهد، صنعت مورد توجه این مدل صنعت IT و دانش پشتیبان آن PMBOK است. این مدل هم معیارهای توانمندساز و هم معیار های نتیجه گرا را مدنظر قرار می دهد.

این مدل از پنج سطح تشکیل شده است. هر سطح از مدل، معرف سطحی از بلوغ مدیریت پروژه است. در این مدل برای ارزیابی هر سطح، پرسش نامه ای طراحی شده است که مجموع سوالات مربوط به تمام سطوح ۱۸۳ سوال می باشد. سوالات این پرسش نامه بر اساس استاندارد PMBOK اما با رویکرد خاص

مدل تدوین شده است. نحوه اندازه گیری نتایج، برای هر سطح به طور جداگانه ارائه شده است. در شکل زیر سطوح بلوغ تعریف شده در این مدل نشان داده شده است.

مزایا	معایب
سادگی و قابل فهم بودن مفاهیم	عدم ارائه روشی برای اولویت بندی فرآیندهای بهبود
سطح تفصیل مناسب	عدم توجه به عملکرد فرآیندها
کاربرد عام و غیر انحصاری	عدم توجه به مدیریت پورتفولیو
مبتنی بر استراتژی سازمان	
ارزیابی تحت وب	
ارایه راهکارهای برتر برای بهبود	
حکایت موسسات بین المللی	
ایجاد رابطه بین کارآمدی مدیریت پروژه و موفقیت پروژه	
توجه به مدیریت برنامه	
ارائه روشی برای اولویت بندی فرآیندهای بهبود	
ارائه متدولوژی ارزیابی	
ارائه رهنمودهایی در مورد راهکارهای برتر	

جدول۱- معایب و محاسن مدل بلوغ کرزنر

P-CMM .۱۲

PCMM[4] الگوی بلوغ قابلیت کارکنان، نقشه مسیر و راهنمایی است برای تشخیص، طراحی و پیاده سازی و اجرای فرایندهای مرتبط با منابع انسانی که به گونه‌ای مستمر منجر به ارتقای قابلیتهای منابع انسانی می‌شود . ازآنجا که یک سازمان نمی تواند تمام بهترین فعالیتها را در مدت بسیار کوتاهی پیاده سازی کند، P-CMMآنها را در ۵ سطح بلوغ و ۲۲ ناحیه فرایندی ارائه می‌دهد. هر سطح-P CMMتحول بی‌نظیری در فرهنگ سازمان به وسیله تجهیز آن با فعالیتهای قدرتمند فراوان برای جذب، توسعه ، سازماندهی ، انگیزش و نگهداری نیروی کار به وجود می آورد (Curtis, 2001).
از نظر دیدگاههای منابع انسانی، این الگو در زمره الگوی مدیریت استراتژیک منابع انسانی است که بر فرایندهای منابع انسانی با توجه به جهت گیریهای استراتژیک سازمان تاکید دارد.

[4] People-Capability maturity model

۱. ساختار اولیه این مدل در سال ۱۹۸۰ توسط واتس هامفری در شرکت IBM شکل گرفت . این شرکت به دلیل عملکرد پایین نرم افزارهای تولیدی ، با رکود در فروش روبه‌رو شد. بر این اساس، تیم مطالعاتی پس از بررسیهای متعدد، دریافتند که الف: چون کیفیت نرم افزار تابعی از عملکرد فرایند تولید است آنها می‌بایستی با تغییر و بهبود فرایند بر این مشکل فائق آیند . ب: به علت اینکه سازمانها به طور ناخواسته درگیر طراحی و پیاده سازی نرم افزارهای مختلف می شوند ، آنها می‌بایستی بر ارائه نرم افزارهای استراتژیک تمرکز کنند. ج: به دلیل اینکه سیستم‌ها دارای رویکرد تکاملی هستند می‌بایستی ابتدا سیستم‌های بسترساز بنا شده، سپس سیستم‌های متعالی به کار گرفته شوند . با توجه به نتایج به دست آمده چارچوب بلوغ فرایندها ارائه شد که با حمایت وزارت دفاع آمریکا این چارچوب توسط انجمن مهندسی نرم افزار دانشگاه کارنگی ملون به عنوان الگوی بلوغ قابلیت کارکنان مطرح شد . این الگو برای نخستین بار در سال ۱۹۹۵ انتشار یافت و از آن زمان در سراسر ایالات متحده، کانادا، اروپا ، استرالیا و هند برای راهنمایی و هدایت فعالیتهای بهبود سازمانی استفاده شده است به گونه‌ای که از سال ۲۰۰۱ بیشترین میزان به‌کارگیری P-CMMدر هند بوده است. از مهمترین شرکتهایی که این الگو را به‌کار گرفته اند عبارت‌اند از : IBM , Citibank , Ericsson , Boeing , Oracle (Curtis,2001)

ارزشهای محوری این مدل که بیانگر نگرش جامع آن به توسعه قابلیتهای منابع انسانی است، شامل :

۱- در سازمانهای بالغ قابلیتهای منابع انسانی به طور مستقیم با عملکرد کسب و کار مرتبط است .
۲- قابلیتهای منابع انسانی یک موضوع رقابتی و یک منبع ایجاد مزیت رقابتی است .
۳- قابلیتهای منابع انسانی بایستی بر اساس جهت گیریهای استراتژیک تعریف شود .
۴- کانون توجه سازمانها از عناصر شغلی به قابلیتها، تغییر کرده است .
۵- قابلیتهای منابع انسانی در سطوح فردی، گروهی و سازمانی قابل سنجش و ارتقا هستند .
۶- سازمان باید در قابلیتهایی از منابع انسانی سرمایه گذاری کند که آن قابلیتها برای انجام قابلیت محوری Core Competencyبنگاه حیاتی باشد .
۷- سازمانها مسئول فراهم کردن فرصتهای رشد و توسعه افراد بوده، افراد مسئول بهره برداری از آنها هستند .
۸- مدیریت میانی و عملیاتی مسئول قابلیتهای منابع انسانی می باشند .
۹- ارتقای قابلیتهای منابع انسانی به مجموعه ای از فرایندها و رویه های مناسب نیاز دارد .
۱۰- در حالی‌که تکنولوژی و اشکال سازمان دچار دگرگونی و تکامل می شوند، سازمانها باید به گونه‌ای مستمر قابلیتهای منابع انسانی را پرورش داده، تکامل بخشند(Curtis, 2001) .

قابلیت :(capability)سطح یا میزان دانش مهارت وتوانمندیهای فرایندی منابع انسانی که برای انجام فعالیتهای بنگاه یا دستیابی به هدفهای بنگاه استفاده می شود و به عبارت دیگر میزان آمادگی سازمان

برای انجام فعالیتهای کلیدی را نشان می دهد.
قابلیت محوری :(core-competency) ترکیب تکنولوژی و مهارتهای سازمان، کیفیت ، سرعت ، هزینه ، کانالهای توزیع، خلاقیت ، نوآوری و... است که موجب ایجاد محصولات و خدماتی برخوردار از وجه تمایز یا مزیت رقابتی در بازار، نسبت به سایر سازمانها می شود.

ساختار P-CMM
الگوی بلوغ قابلیت افراد دارای ۵ سطح بلوغ ، ۲۲ ناحیه فرایندی و هر فرایند در بر گیرنده ۳ تا ۵ هدف و چندین فعالیت است . اجزای ساختاری P-CMM شامل موارد زیر است :
۱- سطح بلوغ : بیانگر سطح جدیدی از قابلیتهای منابع انسانی است که از راه طراحی یا تحول یک یا تعدادی از فرایندهای منابع انسانی به وجود آمده است.
۲- نواحی فرایندی : مجموعه ای از فعالیتهای مرتبط که به گونه‌ای جمعی و توأمان برای دستیابی به مجموعه‌ای از هدفها و مشارکت در ایجاد قابلیتهای ویژه یک سطح خاص می شود.
۳- هدف ها : نتایج منحصر به فرد و مورد انتظار هر یک از نواحی فرایندی است . هر یک از نواحی فرایندی دارای ۲تا۵ هدف است که یکی از آنها نهادینه سازی است.
۴- فعالیت ها : مسیرهای تحقق هدفهای نواحی فرایندی هستند .
در ادامه به توصیف مختصر هر یک ازسطوح و نواحی فرایندی آنها می‌پردازیم:

5-1 سطح بلوغ ۱: سطح اولیه :(Initial) در این سطح سازگاری و پایداری در فعالیتهای سازمان وجود ندارد. برخی ویژگیهای این سطح شامل این موارد است: ۱) سازمان فاقد یک شیوه منسجم و یکپارچه برای انجام کارها وامور مرتبط با منابع انسانی است.۲) اکثر فرایندها موقت هستند و بر اساس هر موقعیت مورد بازبینی قرار می گیرند. ۳)شیوه های انجام کار اغلب نامنظم وپرآشوب به نظر می‌آیند. ۴) امکان بهبود امور وجود ندارد .
5-2سطح بلوغ ۲: سطح مدیریت شده :(Managed) هدف از این سطح تقبل مسئولیت اداره انسانها و پرورش آنهاست. برخی از ویژگیهای این سطح را می توان به طور خلاصه شامل این موارد دانست:
(1سازمان بایدپایه‌ای را بنا نهد تا فرایندهای مشترک را به کار گیرد .۲)مدیریت بایستی محیطی پایدار برای انجام کار حرفه ای ایجاد کند .۳) شرایط لازم برای کنترل‌های پایه ای مدیریت فراهم می‌شود.
۴)افراد را قادر به تکرار فعالیتها سازد.
5-2-1نواحی فرایندی سطح بلوغ ۲
کارگزینی: منظور از کارگزینی، ایجاد یک فرایند رسمی است، به‌گونه ای که کار محوله با منابع واحد مطابقت داشته، افراد مناسب انتخاب ، استخدام و منصوب شده‌اند.
ارتباطات و هماهنگی: منظور از ارتباطات و هماهنگی، اطمینان یافتن از ارتباطات بهنگام در سراسر سازمان است و اینکه افراد و نیروی کار مهارتهایی برای توزیع اطلاعات و هماهنگی فعالیتهایشان به‌گونه‌ای کارآمد ، داشته باشد.

محیط‌کاری: منظور از محیط کاری، ایجاد و حفظ شرایط فیزیکی کار و فراهم آوردن منابعی است که افراد و گروههای کاری وظایفشان را به طور کارآمد و بدون اختلال انجام دهند.
مدیریت عملکرد : منظور از مدیریت عملکرد تعیین هدفهای مرتبط با کار محوله است ، به‌گونه ای که عملکرد واحد و فرد قابل اندازه گیری بوده ، عملکرد نسبت به هدفهای مورد بحث قرار گرفته، به طور مستمر بهبود یابد.
آموزش و توسعه: منظور از آموزش و توسعه، اطمینان یافتن از اینکه تمام افراد مهارتهای مورد نیاز برای انجام وظایفشان را دارا بوده، فرصتهای مناسب توسعه فراهم شده است.
جبران خدمات: منظور از جبران خدمات، فراهم آوردن پرداختیها و مزایا بر اساس مشارکت افراد و ارزش آنها برای سازمان است.
5-3سطح بلوغ۳: سطح تعریف شده :(Defined) هدف این سطح، تدوین و پرورش قابلیتهای نیروی کار و یکپارچه سازی آنها با جهت گیریهای استراتژیک بنگاه است. از ویژگیهای این سطح می‌توان به این موارد اشاره کرد:
(1سازمان بهترین فعالیتها را شناسایی کرده،آنها را با فرایندهای مشترک همسو می‌سازد(2 .فرایندهای ویژه محیط منحصر به فرد، با فرایندهای ویژه محیط پایدار ترکیب، مستند سازی و یکپارچه می‌شوند.۳) سازمان فرایندهای استانداردی برای انجام فعالیتهای کسب وکار تعریف می کند که این عمل منجر به پیدایی بستری اساسی، برای فرهنگ حرفه ای می شود.
5-3-1نواحی فرایندی سطح بلوغ ۳
تحلیل شایستگی: منظور از تحلیل شایستگی شناسایی دانش، مهارتها و تواناییهای فرایندی مورد نیاز برای انجام فعالیتهای کسب و کار سازمان بوده به گونه‌ای که ممکن است آنها توسعه یافته به عنوان مبنایی برای فعالیتهای نیروی کار مورد استفاده قرار گیرند.
برنامه ریزی نیروی کار: منظور از برنامه‌ریزی نیروی کار هماهنگی فعالیتهای نیروی کار با نیازهای کسب و کار حال و آینده در دو سطح سازمانی و واحد است .
پرورش شایستگی: منظور از پرورش شایستگی ارتقای مستمر قابلیت نیروی کار برای انجام وظایف و مسئولیتهای محوله است.
توسعه مسیر پیشرفت شغلی : منظور از توسعه مسیر پیشرفت شغلی اطمینان یافتن از این است که برای افراد فرصتهایی برای توسعه شایستگی فراهم شده که آنها را قادر به دستیابی هدفهای شغلی‌شان می‌سازد.
فعالیتهای شایستگی محور: منظور از فعالیتهای شایستگی محور، اطمینان یافتن از این است که تمامی فعالیتهای نیروی کار تا یک اندازه در توسعه شایستگی های نیروی کار بنا شده اند.
توسعه گروههای کاری : منظور از توسعه گروههای کاری، سازماندهی کار به دور تواناییهای فرایندهای شایستگی محور است.
فرهنگ مشارکتی: یک فرهنگ مشارکتی امکان می دهد سازمان از تمام قابلیت نیروی کار، برای

تصمیماتی که بر عملکرد سازمان تاثیرگذار است ، بهره مند شود .
5-4سطح بلوغ ۴: سطح پیش بینی‌پذیر :(Predictable) توانمندسازی و یکپارچه سازی قابلیتهای نیروی کار و مدیریت عملکرد به صورت کمی هدفهای این سطح می باشند . ویژگی این سطح این است که دیدگاه کمیت‌گرا بایستی بر فرایند طراحی، پیاده سازی و بهره برداری از سیستم‌های منابع انسانی حاکم شود.

5-4-1نواحی فرایندی سطح بلوغ ۴
یکپارچگی شایستگی‌ها : منظور از یکپارچگی شایستگی‌ها بهبود کارایی و چالاکی کارها با درجه وابستگی بالا از راه یکپارچه سازی قابلیتهای فرایندی شایستگی های مختلف نیروی کار است.
گروههای کاری خودگردان : منظور از گروههای کاری خودگردان اعطای مسئولیت و اختیار برای تعیین چگونگی هدایت فعالیتهای گروه با بیشترین اثربخشی است.
داراییهای شایستگی محور: منظور از داراییهای شایستگی محور، به کارگیری دانش ، تجربه و مصنوعات توسعه یافته در اجرای فرایندهای شایستگی محور، برای افزایش و ارتقای شایستگی و عملکرد است.
مدیریت عملکرد کمّی: منظور از مدیریت عملکرد کمّی، پیش بینی و مدیریت قابلیت فرایندهای شایستگی محور برای دستیابی به هدفهای عملکردی قابل سنجش است.
مدیریت قابلیت سازمانی: منظور از مدیریت قابلیت سازمانی، شایسته سازی و مدیریت قابلیت نیروی کار و فرایندهای شایستگی محور حیاتی است که آنها انجام می دهند.
مربیگری: منظور از مربیگری انتقال دروس و تجربه‌های بزرگ در یک شایستگی نیروی کار، برای بهبود قابلیت سایر افراد یا گروههای کاری است.
5-5سطح بلوغ ۵: سطح بهینه سازی :(Optimization) هدف از این سطح، بهبود مستمر و یکپارچه سازی قابلیتهای فردی گروه و سازمان است. ویژگیهای این سطح شامل این مواردست:
(1سازمانها از دانش عمیق وکمی برای بهبود مستمر در فرایندها استفاده می کنند. ۲)سازمان بر اساس داده ها تشخیص می‌دهد که کدام یک از فرایندها بهتر می‌تواند از فعالیتهای بهبود مستمر بهره‌مند شود(3 .مدیریت تحول به عنوان یک فرایند سازمانی استاندارد و بهبود فرایندها، مانند یک تفکر پایدار و جاودان در سراسر سازمان به وجود می آید.

5-5-1نواحی فرایندی سطح بلوغ ۵
بهبود مستمر قابلیت: منظور از بهبود مستمر قابلیت، فراهم آوری زمینه ای برای افراد و گروههای کاری است، تا به گونه‌ای مستمر قابلیتهایشان را برای انجام فرایندهای شایستگی محور بهبود بخشند.
همسویی عملکرد سازمانی :منظور از همسویی عملکرد سازمانی، تقویت (افزایش) همسویی نتایج عملکرد در بین افراد ، گروههای کاری و واحدها با عملکرد سازمانی و هدفهای کسب و کار است.
نوآوری مستمر نیروی کار: منظور از نوآوری مستمر نیروی کار ، شناسایی و ارزیابی فعالیتهای بهبود یافته و ابداعی نیروی کار و تکنولوژی و تحقق بیشترین تعهدات (وعده ها) در سراسر سازمان است.

با توجه به اجزای ساختاری عنوان شده، ساختارP-CMM در شکل ۲ نمایش داده شده است.
منظور از فعالیتهای پیاده سازی در هر ناحیه، فرایندی فعالیتهایی است که می‌بایستی انجام شوند تا به هدفهای ناحیه فرایندی دست یابیم. نهادینه‌سازی مجموعه فعالیتهایی است که به طراحی و پیاده سازی گسترده ، مستمر و اثربخش فرایندهای منابع انسانی کمک می کند. نهادینه سازی خود دارای ۴ بعد است.1 :تعهد اجرایی (تدوین استراتژی ، سیاست‌ها و ...) ۲.توانایی اجرایی (پیش زمینه‌های لازم، مانند: منابع ، ساختارها و ...) ۳. اندازه گیری و تحلیل) تدوین شاخص و اندازه گیری آنها در مورد هر فرایند). ۴. ممیزی (بررسی میزان همسویی فعالیتها و فرایندها با هدفها ، سیاستها ، ماموریتها و...

مزایای پیاده سازی الگوی بلوغ قابلیت کارکنان
مزیت به کارگیری فرایندهای منابع انسانی در مطالعات متعددی به گونه ای تجربی نشان داده شده است.
سازمانهایی که یک استراتژی یکپارچه منابع انسانی را به کار گرفته‌اند، به گونه‌ای قابل ملاحظه در ردیف سازمانهای کلاس جهانی هستند .(Appleby, 2000) در برخی حالات ، حتی آثار شهرت آنها در رابطه با فعالیتهای منابع انسانی به طور مستقیم با افزایش بهای سهامشان ارتباط داشته است Hannon) (96,تجزیه تحلیل نمونه های مختلف در سال ۱۹۹۰ ، یک رابطه بسیار قوی (مثبت) را بین عملکرد بالای فعالیتهای کاری و عملکرد مالی سازمان نشان می دهد . (Becker, 98) در یک مطالعه فعالیتهای نیروی کار که تقریباً در هزار شرکت انجام شده است ، آمده است که: به کارگیری چنین فعالیتهایی باعث ۷/۰۵ درصد کاهش در ترک خدمت شده است و به ازای هر یک از کارکنان ۲۷/۰۴۴ دلار فروش بیشتر و 841/18دلار افزایش در ارزش بازار و ۳/۸۱۴ دلار افزایش سوددهی به دنبال داشته است . (Huselid, 95) .
حال می توان با توجه به موارد توصیفی یادشده، مزایای P-CMM را به این شرح دسته بندی کرد :
(1توجه به قابلیت به جای عناصر شغلی، ۲) ایجاد یک بستر مناسب برای برپایی نظامهای متعالی، ۳) دارا بودن نظامهای جامع منابع انسانی، ۴) تکرارپذیری فعالیتها، ۵) فعالیتهای دقیق و شفاف برای اجرای نظامها، ۶)کاهش انحرافات در عملکرد، ۷) بهبود مستمر فعالیتها، ۸)تسری بهترین فعالیتها در سراسر سازمان، ۹)نهادینه سازی نظامها.

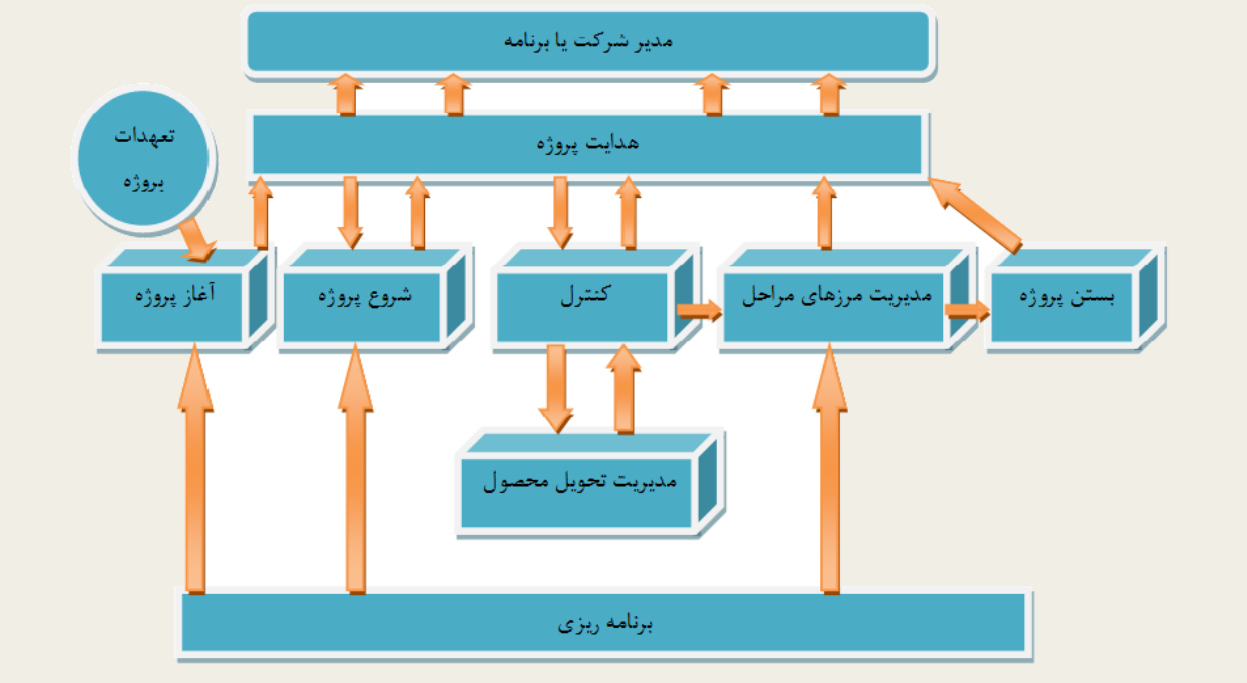
PRINCE2.۱۳

یک روش فرآیندی برای مدیریت موثر پروژه است. PRINCE2 استانداردی است که دولت انگلستان به طور گسترده از آن استفاده کرده و به طور گسترده در بخش خصوصی شناخته شده و استفاده می‌گردد.

ویژگی‌های اصلی PRINCE2 عبارتند از:

- تمرکز بر توجیه کسب و کار
- یک ساختار سازمانی تعریف شده برای تیم مدیریت پروژه
- رویکرد برنامه‌ریزی بر اساس محصول
- تأکید بر تقسیم پروژه به مراحلی که قابلیت مدیریت و کنترل داشته باشند
- انعطاف پذیری برای کاربرد در سطحی که برای پروژه مناسب است

PRINCE2 یک رویکرد فرآیندی برای مدیریت پروژه است که روشی قابل اصلاح و مقیاس پذیر برای مدیریت انواع مختلف پروژه ایجاد می‌کند. هر فرآیندی با خروجی و ورودی های اصلی و همچنین اهداف خاصی که باید به آن ها دست یابد و فعالیت هایی که باید انجام دهد، تعریف می شود. در شکل زیر به طور شماتیک مدل فرآیندی PRINCE2 نشان داده شده است.



شکل ۵- مدل فرآیندی PRINCE2

هدایت پروژه DP

فرآیند هدایت یک پروژه از آغاز تا بستن پروژه اجرا می شود. انجام این فرآیند وظیفه هیات پروژه است. هیات پروژه به وسیله استثنائات مدیریت کرده، به وسیله گزارش‌ها نظارت می کند و توسط نقاط تصمیم گیری کنترل را انجام می دهد.

فرآیندهای انجام شده توسط هیات پروژه به ۴ حیطه به شرح زیر تقسیم می شود:

۱. آغاز پروژه
۲. مرزهای مراحل (اختصاص منابع بیشتر پس از کنترل نتایج به دست آمده)
۳. هدایت غیر رسمی (نظارت بر پیشرفت، پیشنهاد و راهنمایی، عکس العمل نسبت به موقعیت های استثنایی)
۴. بستن پروژه (تایید نتیجه پروژه و پایان کنترل شده آن)

فرآیند هدایت پروژه، فعالیت های روزمره مدیر پروژه را پوشش نمی‌دهد.

شروع پروژه SU

شروع اولین فرآیند PRINCE2 است. این فرآیند در برگیرنده مرحله قبل از آغاز پروژه است، و منظور اطمینان از برآورده شدن پیشنیازهای آغاز پروژه طراحی شده است. برای انجام این فرآیند وجود سند تعهد پروژه که مبین شرایط سطوح بالا، دلیل انجام پروژه و نتیجه خواسته شده می باشد، ضروری است. فرآیند آغاز یک پروژه باید بسیار کوتاه باشد.

وظیفه فرآیند حول تولید ۳ عنصر زیر قرار دارد:

۱. اطمینان از در دسترس بودن اطلاعات مورد نیاز برای تیم پروژه
۲. طراحی و انتصاب تیم مدیریت پروژه
۳. تهیه برنامه مرحله آغاز

اهداف آغاز یک پروژه عبارتند از:

- توافق بر سر این موضوع که آیا توجیه کافی برای پیشروی پروژه وجود دارد یا خیر
- ایجاد یک اساس مدیریتی مستحکم برای پیشروی پروژه
- مستندسازی و تایید این که یک موقعیت تجاری قابل قبول برای پروژه موجود است
- توانمندسازی و تشویق هیات پروژه برای در اختیار گرفتن پروژه
- ایجاد یک مسیر برای فرآیندهای تصمیم گیری مورد نیاز در طول عمر پروژه
- اطمینان از این که سرمایه گذاری صورت گرفته در زمان و تلاش مورد نیاز برای پروژه، با در نظر گرفتن ریسک های موجود، به شکلی عاقلانه انجام شده است

مدیریت مرز مراحلSB

این فرآیند نقاط مختلف تصمیم گیری برای بررسی ادامه پروژه را برای هیئت پروژه ایجاد می‌کند. اهداف این فرآیند عبارتند از:

- اطمینان بخشیدن به هیات پروژه که تمامی فعالیت‌های برنامه ریزی شده برای مرحله کنونی، به گونه تعریف شده کامل شده‌اند.
- ایجاد اطلاعات لازم برای هیات پروژه به منظور ارزیابی امکان ادامه پروژه
- ایجاد اطلاعات لازم برای هیات پروژه به منظور تایید تکمیل مرحله کنونی و دادن مجوز برای شروع مرحله بعد و همچنین میزان تفویض اختیار مجاز
- ضبط هرگونه اندازه گیری و آموزه‌ای که به مراحل بعدی پروژه یا پروژه‌ها دیگر کمک می‌کند.

کنترل یک مرحله

این فرآیند فعالیت های نظارت و کنترل مدیر پروژه که به منظور اطمینان از شرایط عادی هر مرحله و عکس‌العمل نسبت به وقایع غیرقابل انتظار آن انجام می شود را توصیف می کند. این فرآیند هسته اصلی تلاش های مدیر پروژه را شکل می دهد و فرآیندی است که مربوط به مدیریت روزانه پروژه است. درون یک مرحله یک سیکل شامل موارد زیر وجود دارد:

- ایجاد مجوز برای کارهایی که باید انجام شوند
- جمع‌آوری اطلاعات پیشرفت کار
- عکس‌العمل نسبت به تغییرات
- مرور وضعیت
- گزارش دهی
- اتخاذ اقدامات اصلاحی لازم
- این فرآیند موارد فوق را پوشش داده و همچنین کار مستمر مدیریت ریسک و کنترل تغییر را انجام می دهد.
- مدیریت تحویل محصول
- هدف این فرآیند اطمینان از تولید و تحویل محصولات برنامه‌ریزی شده به وسیله مراحل زیر است:
- اطمینان از این که کارهای انجام شده بر روی محصولات که به اعضای تیم اختصاص داده شده است، به طور موثری مورد قبول واقع شده و دارای مجوز است همچنین تایید و کنترل بسته‌های کاری
- اطمینان از تطابق کار با نیازمندی به واسط های تعریف شده در بسته کاری
- اطمینان از انجام کار
- ارزیابی پیشرفت کار و پیش‌بینی به صورت منظم
- اطمینان از این که محصولات تکمیل شده نیازهای کیفی را برآورده ساخته اند
- گرفتن تاییدیه برای محصولات تکمیل شده

- بستن یک پروژه
- هدف این فرآیند اجرای یک پایان کنترل شده برای پروژه است. این فرآیند پوشش دهنده وظیفه مدیر پروژه در جمع‌بندی پروژه در پایان یا مراحل نزدیک به پایان است. بیشتر حجم کار مربوط به فراهم آوردن ورودی برای هیات پروژه به منظور گرفتن تاییدیه اتمام احتمالی پروژه است.
- اهداف بستن یک پروژه عبارتند از:
- کنترل میزان برآورده شدن اهداف و مقاصد تنظیم شده در سند ابتدایی پروژه (PID)
- تایید میزان برآورده شدن سند ابتدایی پروژه (PID) و رضایت مشتری از از محصولات تحویل شده
- گرفتن تاییدیه رسمی محصولات
- اطمینان از میزان تحویل و تایید مشتری در مورد محصولات مورد انتظار
- تایید اینکه هماهنگی های نگهداری و عملیات انجام شده صورت گرفته است
- ارائه پیشنهاد برای عملیات بعدی
- اقتباس آموزه های ناشی از انجام پروژه و تکمیل گزارش آموزه های فراگیری شده
- ایجاد گزارش نهایی پروژه
- اطلاع دادن به سازمان میزبان از خواست تیم پروژه به منظور منحل کردن ساختار پروژه و منابع
- برنامه ریزی (PL)
- برنامه‌ریزی یک فرآیند قابل تکرار است و نقش مهمی در فرآیندهای دیگر داراست که اهم آن ها به شرح زیر است:
- برنامه ریزی یک مرحله آغازی
- برنامه ریزی یک پروژه
- برنامه ریزی یک مرحله
- ایجاد یک برنامه برای مواقع استثنایی
- PRINCE یک شروع بر پایه محصول برای فعالیت برنامه ریزی فراهم می آورد. همچنین یک چارچوب برنامه ریزی ایجاد می‌کند که می‌تواند در مورد هر پروژه ای به کار رود. این چارچوب شامل:
- تعیین این که چه محصولاتی مورد نیاز است
- تعیین ترتیبی که بر اساس آن محصولات باید تولید شوند
- تعیین شکل و محتوای هر محصول
- واضح سازی این که چه فعالیت هایی برای تولید و تحویل محصولات مورد نیاز است.

۱٤. OPM3

OPM3[5] مخفف عبارت مدل بلوغ سازمانی مدیریت پروژه است. استانداردی که تحت نظارت موسسه مدیریت پروژه و در ادامه استانداردهای منتشر شده توسط این موسسه به چاپ رسیده است. محتوای مدل بلوغ سازمانی مدیریت پروژه بر مبنای اطلاعات گسترده ای است که از مشاوران و متخصصان مدیریت پروژه به دست آمده و منطبق با مطالب و فرآیندهای کتاب پیکره دانش مدیریت پروژه می باشد. این مدل، در یک دوره تقریبا شش ساله و با مطالعه بیش از ۲۷ مدل بلوغ سازمانی موجود، توسعه یافته است. در طی این فرآیند، بیش از ۸۰۰ داوطلب و متخصص مدیریت پروژه از تقریبا تمامی صنایع از ۳۵ کشور جهان به صورت فعالانه در این پروژه درگیر بوده اند.

هدف از ایجاد این استاندارد، کمک به سازمان ها برای درک مدیریت پروژه سازمانی و سنجش میزان بلوغ آن ها در مقایسه با معیارهایی است که از آن ها با عنوان راهکارهای برتر مدیریت پروژه سازمانی یاد می شود. استاندارد OPM3 این راهکارها را در قالب فهرست های مرجع معرفی می کند. در حقیقت می توان گفت یکی از وجوه تمایز و تفوق OPM3 نسبت به استاندارد PMBOK که مرجع شناخته شده ای در مدیریت پروژه می باشد، معیارها و ضوابط مشخص و مدونی است که در قالب همین فهرست های مرجع عرضه شده است. همچنین OPM3 به سازمان هایی که خواهان افزایش بلوغ سازمانی خود در مدیریت پروژه هستند، کمک می کند تا برنامه ریزی بهبود انجام دهند.

OPM3 از سه بخش تشکیل می شود:

متن تشریحی، مفاهیم اساسی OPM3 را به همراه چندین پیوست مرتبط جهت درک مفاهیم اولیه، ارائه می کند.

خودارزیابی، ابراز پیشنهادی OPM3 برای ارزیابی اولیه سازمان به منظور تعیین میزان بلوغ و مشخص شدن نقاط قوت و ضعف آن می باشد. خودارزیابی از ۱۲۵ پرسش شده است که پاسخ آن ها را تیم ارزیابی کننده سازمان در خلال مصاحبه ها و جلسات مستمر و نیز مطالعه مستندات موجود در سازمان استخراج می کند.

فهرست های راهنما، در حقیقت فهرست های مرجعی هستند که پس از ارزیابی اولیه و مشخص شدن جایگاه بلوغ سازمان در رتبه بندی بلوغ، موجود در استاندارد، جهت تعیین نقاط ضعف سازمان و ارائه راهکارهای بهبود به کار گرفته می شود.

برای پیاده سازی OPM3، ۳ عنصر اصلی آن را می توان به ترتیبی که در شکل ۵ اشاره شده، مد نظر قرار داد. دانش، موتور محرک کلیه فعالیت ها در فرآیندها پیاده سازی استاندارد OPM3 است. تسلط به

[5] Organizational Project Management Maturity Model

مفاهیمی مانند اداره کردن سازمانی پروژه ها و نگرش سیستمی به مجموعه پروژه های موجود در یک سازمان و مهم تر از همه، رسیدن به مرتبه بلوغ در این زمینه، نیازمند آن است که اولا تیم ارزیابی کننده از افراد متحصصی که خود، در زمینه مدیریت پروژه به بلوغ نسبی رسیده باشند، تشکیل شود و ثانیا همکاری از جانب کلیه سطوح مدیریتی سازمان، جهت ارزیابی اولیه و پیاده سازی بهبود ها در سازمان صورت پذیرد.

مزایا	معایب
ارزیابی کارآمدی سازمان ها در زمینه مدیریت پروژه	عدم ایجاد رابطه بین کارآمدی مدیریت پروژه و موفقیت پروژه
توجه به مدیریت طرح پورتفولیو	عدم ارائه متدولوژی ارزیابی
سادگی و قابل فهم بودن مفاهیم	تمرکز اصلی بر ارزیابی فرآیندها
سطح تفصیل مناسب	عدم توجه روشن به نتایج
کاربرد عام و غیرانحصاری	عدم مشخص بودن سطوح بلوغ
مبتنی بر بهبود مستمر	ساختار امتیازدهی بلی و خیر
پشتیبانی و به روز رسانی مدل	
مبتنی بر استراتژی سازمان	
ارزیابی تحت وب	
ارائه راهکارهای برتر برای بهبود	
گرایش گسترده به استفاده از مدل	
توجه به عملکرد فرآیندها	
حمایت موسسات بین المللی	

جدول۲- معایب و محاسن مدل OPM3

COSO.۱۵

در واقع کوزو، سازمانی است که در سال ۱۹۸۵ برای حمایت از کمیسیون ملی برای پیشگیری از گزارشگری مالی متقلبانه تشکیل شد. این سازمان متعلق به بخش خصوصی بوده و راهنمایی هایی جهت بکارگیری عوامل مختلف برای جلوگیری از تقلبات گزارشگری مالی ارایه می کند. همچنین سازمان مذکور توصیه هایی برای شرکتهای سهامی عام و حسابرسان مستقل آن، برای کمیسیون بورس و اوراق بهادار (SEC) و سایر قانون گذاران در این حوزه و نیز برای موسسات آموزشی منتشر می کند . مضافاً کوزو توسط پنج نهاد حرفه ای، انجمن حسابداران آمریکا ، انجمن حسابداران خبره عمومی آمریکا ، انجمن مدیران مالی بین المللی ، انجمن حسابداران مدیریت و انجمن حسابرسان داخلی حمایت می شود.

اهداف و اجزای کنترلهای داخلی یکپارچه: کوزو اهداف و اجزای کنترلهای داخلی یکپارچه چارچوب کنترلهای داخلی را اینگونه تعریف می کند که فرایندی است متاثر از هیئت مدیره، مدیران و سایر پرسنل، که برای اطمینان معقول از دستیابی به اهداف مقوله های زیر طراحی شده است:

۱. اثربخشی و کارایی عملیات
۲. قابلیت اطمینان گزارشهای مالی

۳. انطباق با قوانین و مقررات

این سه هدف به طور مستقیم با پنج جزء یکپارچه محیط کنترل ، ارزیابی ریسک ، روش های کنترلی ، اطلاعات و ارتباطات ، و نظارت مرتبط هستند .اهداف، آنچه را که سازمان می خواهد به آن برسد و اجزا آنچه را که برای رسیدن به این اهداف مورد نیاز است، مشخص می کند. در شکل شماره ۱، مکعب ارائه شده، رابطه بین سه هدف و پنج جزء و بعد سوم آن، ساختار سازمان را نشان می دهد. این معکب هر جا سخن از چارچوب کنترل داخلی و کوزو باشد، به خاطر می آید. در نظر داشته باشید که هیچ یک از دو سازمان متفاوت، نبایستی یک نوع سیستم کنترل های داخلی داشته باشند .

شکل ۶- مکعب کوزو

اصول کنترل های داخلی : اصول چارچوب کنترلهای داخلی شامل ۱۷ مورد می باشد که در طراحی، پیاده سازی، و ارزیابی اثربخشی کنترلهای داخلی بحث کرده است. این اصول به طور خاص به هر یک از جزء ذکر شده فوق مربوط هستند. بنابراین، اگر اصل مربوطه کارآمد نباشند، فرض بر است که جزء مربوط به آن نیز کارآمد نیست. در ادامه هر یک از ۵ جزء اصلی و اصول مربوط به آن را بطور گذرا نشان میدهیم :

محیط کنترلی : محیط کنترلی مجموعه ای از استانداردها ، فرآیندها و ساختار ها و همچنین پایه و اساس کنترل داخلی در سازمان ها است. پنج اصل زیر مربوط به این جزء هستند :

اصل اول: سازمان نشان دهنده تعهد به صداقت و ارزش های اخلاقی است .بنابراین اقدامات مدیریت و هیئت مدیره باید تقویت کننده این تعهدات باشند .استانداردهای رفتاری باید معرف انتظارات و ارزش های اخلاقی بوده و به وضوح قابل درک باشند. این انتظارات باید در زمان وقوع مورد بررسی قرار گرفته

و برای ارزیابی عملکرد واقعی با مورد انتظار و تعیین هر گونه انحراف بکار گرفته شده و به موقع اصلاح شوند .

اصل دوم: هیئت مدیره نشان دهنده استقلال از مدیریت و اعمال نظارت بر توسعه و عملکرد کنترل های داخلی است. در واقع، هیئت مدیره باید ضمن قبول مسئولیت نظارتی خود، مهارت ها و تخصص های مورد نیاز جهت مسئولیت پاسخگویی مناسب را تعیین و حفظ کرده وهمچنین ارزیابی دوره ای این مهارت ها را انجام دهد .

اصل سوم: اقدامات مدیریت بایستی با نظارت هیئت مدیره و ساختار و روشهای گزارشگری مناسب در دستیابی به اهداف باشند. مدیریت و هیئت مدیره همچنین بایستی ساختارهای چندگانه ای برای حمایت از دستیابی به اهداف را در نظر داشته باشند (به عنوان مثال واحدهای عملیاتی متفاوت و ارائه دهندگان خدمات برون سپاری). مضافاً باید تفویض اختیارات، تعیین مسئولیت ها و استفاده مناسب از فرآیندها و تکنولوژی ها را به گونه ای انجام دهند که پاسخگوی ذینفعان مختلف باشد .

اصل چهارم: سازمان، متعهد به جذب، توسعه توانایی ها و حفظ افراد با صلاحیت در جهت رسیدن به اهداف مورد نظر است. هیئت مدیره و مدیریت باید صلاحیت حرفه ای پرسنل را در سطوح مختلف سازمان و از جمله ارائه دهندگان خدمات برون سپاری را ارزیابی کند. بایستی نظارت و آموزش کافی در این زمینه ها صورت پذیرد .

اصل پنجم: سازمان، افراد پاسخگو جهت مسئولیت شناسی های کنترل داخلی در جهت رسیدن به اهداف کنترل های داخلی، دارد .(D'Aquila, 2013) مدیریت و هیئت مدیره باید مکانیسمی برای حفظ اشخاص پاسخگو ایجاد کنند. آنها همچنین باید اقدامات اصلاحی را در صورت لزوم و اقدامات ارزیابی مناسب عملکرد که شامل هردوی اهداف کوتاه مدت و بلند مدت در جهت اعطای مشوق ها و یا پاداش های دیگر می شود را انجام دهند. مشوق ها و پاداشها باید هم تراز با پاسخگویی مد نظر کنترل داخلی باشند. مدیریت و هیئت مدیره باید پاسخگویی افراد را ارزیابی و اندازه گیری عملکرد آنها را گسترش دهد. آنها همچنین باید عملکرد پاسخگویی کنترل داخلی را به منظور پاداش یا اعمال اقدامات انضباطی مناسب ارزیابی کنند .(D'Aquila, 2013)قابل ذکر است که در به روز رسانی ها، اساس و پایه متون، همان چارچوب اولیه است که در سال ۱۹۹۲ منشتر شده است. به صورتی گذرا در چارچوب به روز شده سال ۲۰۱۳ ، نقش عامل "پاسخگویی" در بخش محیط کنترلی پررنگ تر شده است .

ارزیابی ریسک : فرایندی پویا و تکرار شونده جهت شناسایی و تجزیه و تحلیل خطرات و ریسکهای موجود در مسیر دستیابی به اهداف سازمان است. اصول زیر مربوط به این بخش هستند :

اصل ششم: سازمان، اهداف را با وضوح کافی برای توانایی شناسایی و ارزیابی خطرات مربوط به اهداف تعیین کند. این اهداف مربوط به عملیاتها، گزارشگری و رعایت قوانین بوده و منعکس کننده تصمیمات مدیریت در مورد ساختار، ملاحظات صنعت، و عملکرد سازمانی است .

اصل هفتم: سازمان، بایستی خطرات دستیابی به اهداف خود را در سراسر سازمان شناسایی کرده و تجزیه و تحلیل این ریسکها را به عنوان یک اساس برای تعیین چگونگی مدیریت آنها، مورد توجه قرار دهد. سازمان باید هر دوی عوامل داخلی و خارجی را در زمان که شناسایی خطرات در نظر گرفته و در مکانیسم های ارزیابی ریسک در سطوح مناسب مد نظر مدیریت، پیاده سازی کند. سطوح مذکور، شامل سازمان به طور کلی، شرکت های فرعی، بخشها و واحدهای عملیاتی است. بخش مهم فرآیند ارزیابی ریسک، شامل "برآورد اهمیت بالقوه خطر و اینکه به چه نحو باید مدیریت شود" است .

اصل هشتم: سازمان، بایستی تقلب بالقوه در ارزیابی ریسک دستیابی به اهداف را در نظر گیرد. انواع تقلب به صورت کلی در سه مقوله فساد مالی ، سوء استفاده از دارایی ها و تقلب در گزارشگری مالی می باشد (تقی نتاج،۱۳۹۱) .

اصل نهم: سازمان، تغییراتی که تاثیر طور قابل توجهی بر سیستم کنترل داخلی می توانند داشته باشند را شناسایی و ارزیابی می کند. این تغییرات عبارتند از: محیط خارجی، مدل کسب و کار و رهبری . عوامل محیط خارجی شامل نظارتها و بازرسی ها، عوامل اقتصادی و محیطی است. مدل کسب و کار، مدلی است که موجب تغییرات درراه اندازی خطوط جدید کسب و کار ، تحول در خطوط کسب و کار موجود، تحصیل و یا واگذاری عملیات کسب و کار، رشد سریع و فن آوری های جدید شود. در نهایت، رهبری، نگرش مدیریت در مورد کنترل داخلی است .

در بخش ارزیابی ریسک به طور کلی ممکن است بازنگري در کنترل هاي داخلي ضرورت یابد تا بدین وسیله ریسک هاي جدید یا ریسک هایي که پیش از این جزو ریسک هاي غیرقابل کنترل قلمداد شده اند، به شیوه اي مناسب مورد بررسي قرار گیرند .(Bcbs, 1998) مضافاً لازم به ذکر است در چارچوب جدید، خطر ذاتی و خطر تقلب (دستکاری) نقش مهمی تری در ارزیابی ریسک ایفا می کنند و روند ارزیابی ریسک که شامل شناسایی ریسک، تحلیل ریسک و واکنش به آن است به طور مفصل تری مورد تاکید قرار گرفته است .

فعالیت های کنترلی : این فعالیت ها، اقداماتی است که توسط سیاست ها و روشهای سازمان برای کمک به حصول اطمینان از اجرا شدن دستورات مدیریت که در جهت کاهش خطرات در مسیر دستیابی به اهداف می باشند، ایجاد می شوند. فعالیت های کنترلی در تمام سطوح سازمان، در سراسر محیط فن آوری و تکنولوژی آن و در فرآیندهای مختلف کسب و کار صورت خواهد پذیرفت. فعالیت‌هاي کنترلي هر شرکت باید متناسب با اهداف عملیاتي، گزارشگري مالی و رعایتي آن باشد. هر چند که این فعالیت‌ها

باید بسته به اندازه، نوع عملیات، اهداف و شرایط هر شرکت طراحي و پیاده‌سازي شوند، اما فعالیت‌هاي کنترلي هر شرکت باید علاوه بر کنترل‌های عمومی و کاربردی حاکم بر سامانه‌های اطلاعاتی، دربرگیرنده و مبتنی بر اصول روبه رو باشد: بررسي‌هاي مدیریت ارشد، مدیریت مستقیم فعالیت‌ها و کارکردها، کنترل‌های اعتبار و پردازش معاملات، کنترل‌هاي فیزیکي، شاخص‌های عملکرد، تفکیك وظایف، خط مشیها و رویهها، سایر فعالیت‌های کنترلی و مستندسازی (دستورالعمل کنترل‌های داخلي ناشران پذیرفته شده در بورس اوراق بهادار تهران و فرابورس ایران،۱۳۹۱). سه اصل زیر مربوط به بخش فعالیتهای کنترلی می باشند :

اصل دهم: سازمان، بایستی ضمن مد نظر قرار دادن تاثیر عوامل محیطی ، عملیاتی و ویژگی های خاص سازمان، فعالیت های کنترلی را انتخاب کرده و توسعه دهد که به کاهش خطرات دستیابی به اهداف به سطح قابل قبول کمک کند. باید ترکیبی از انواع فعالیت های کنترلی جهت این بکار گرفته شود. فعالیت های کنترلی می توانند دستی و خودکار (Minnesota management & budge, 2012)و همچنین به عنوان عاملی بازدارنده و نظارتی باشند .

اصل یازدهم: سازمان، باید فن آوری و تکنولوژی فعالیت های کنترلی را برای حمایت از دستیابی به اهداف انتخاب کرده و توسعه دهد. مدیریت بایستی فن آوری فعالیت های کنترلی طراحی شده برای کمک به اطمینان از کامل بودن، دقیق بودن و در دسترس بودن فرآیند آن و مضافاً برای محدود کردن دسترسی کاربران مجاز متناسب با مسئولیت های شغلی خود به منظور محافظت از دارایی ها از تهدیدات خارجی و همچنین برای ارائه کنترلهایی بر تحصیل، توسعه، و حفظ فن آوری را توسعه دهد .

اطلاعات و ارتباطات : در واقع اهداف کنترلی این بخش شامل اطمینان از این است که آیا اطلاعات به وسیله سیستمهاي اطلاعاتی شناسایی، گرد آوري، پردازش و گزارش می شود و اینکه ارتباطات اثربخشی درسراسر سازمان و با اشخاص برون سازمانی برقرار می شود یا خیر (پرسشنامه ارزیابي کنترلهای داخلي مربوط به اطلاعات و ارتباطات سازمان بورس و اوراق بهادار ایران- صص ۱). اطلاعات و ارتباطات برای یک سازمان جهت انجام مسئولیت پذیری کنترلهای داخلی حمایت کننده اهداف، ضروری است. چارچوب به روز شده شرح مفصل تری از انواع تکنیکهای کنترلی و چگونگی دسته بندی آنها فراهم می کند. ارتباطات به صورت درون سازمانی و برون سازمانی، اطلاعات مورد نیاز برای انجام فعالیت های روزمره کنترل داخلی سازمان را فراهم می کنند .ارتباطات، کارکنان را قادر به درک مسئولیت پذیری های کنترل داخلی و اهمیت آنها می کند. می توان گفت ارتباطات، فرایندی پیوسته و مکرر شامل فراهم سازی، به اشتراک گذاری و کسب اطلاعات لازم می باشد. همچنین کارکنان بایستی اطلاعات خارجی و با اهمیت در تصمیم گیری را با توصیه هایی که از بالادستی ها می شود، درک کنند .(coso, 1994) اصول زیر مربوط به این بخش هستند :

اصل سیزدهم: سازمان، بایستی اطلاعات مربوط و با کیفیت مورد نیاز در جهت حمایت از عملکرد کنترل داخلی را به دست آورده یا تولید کند و قادر به شناسایی اطلاعات مورد نیاز نیز باشد. سیستم های اطلاعاتی باید داده های خام بدست آمده از منابع داخلی و خارجی را ضبط، پردازش و تبدیل به اطلاعاتی بموقع، دقیق، کامل، قابل دسترس، محافظت شده و قابل اثبات کرده و بنحو مطلوبی نگه داری کنند. لازم به ذکر است که ماهیت، مقدار، و دقت اطلاعات مربوطه باید متناسب با ماهیت و ویژگیهای دستیابی به اهداف مورد نظر باشند .

اصل چهاردهم: اطلاعات مرتبط داخلی سازمان، از جمله اهداف و مسئولیت پذیری های کنترل داخلی، برای حمایت از عملکرد کنترل داخلی مورد نیاز هستند .چنین ارتباطی باید شامل فرایندی درجهت انتقال اطلاعات مورد نیاز باشد .ارتباط بین مدیریت و هیئت مدیره هم نیاز به اطلاعات و کانال های ارتباطی جداگانه از جمله خطوط اطلاعاتی ویژه دارد. این کانالها بایستی امن بوده تا از دسترسی افراد ناشناس جلوگیری به عمل آید. در نهایت، بایستی زمان بندی، مخاطبان و ماهیت این اطلاعات در تعیین روش برقراری ارتباطات مذکور، در نظر گرفته شوند .

اصل پانزدهم: سازمان، با افراد برون سازمانی در مورد مسائل مؤثر بر عملکرد کنترل داخلی در ارتباط است. ارتباطات برون سازمانی از جمله سهامداران، شرکای تجاری، مالکان، مشتریان و تحلیل گران مالی باید به موقع و مربوط باشد. کانالهای ارتباطی باز باید اجازه ورود داده های دریافتی از مشتریان، مصرف کنندگان، تامین کنندگان، حسابرسان خارجی، تحلیل گران مالی و دیگران را به سیستم اطلاعاتی بدهد. چارچوب به روز شده، نسبت به چارچوبهای قبلی، ارتقاء کیفیت اطلاعات (لازم به ذکر است عوامل ارتقاء دهنده اطلاعات طبق چارچوب نظری جدید هیئت تدوین استاندارد های مالی یاFASB ، شامل قابلیت مقایسه ، قابلیت اثبات ، به موقع بودن و قابل فهم بودن می باشند (الزامات قانونی ، تعامل با اشخاص ثالث، امنیت و دسترسی محدود به اطلاعات، هزینه ها و منافع به دست آوردن و مدیریت اطلاعات و همچنین پیشرفت های فن آوری را بیشتر مورد توجه قرار داده است .

نظارت بر فعالیتها : از ارزیابی های در حال انجام ، ارزیابیهای جداگانه و یا ترکیبی از هر دو برای بررسی همه اجزای پنج گانه ی کنترل داخلی شامل کنترلهای موثر بر اصول در هر جزء استفاده شده و این یافته ها مورد برازش قرار گرفته و هر گونه نقصی در ارتباط با زمان بندی و مسائل پیش آمده با اهمیت، به مدیریت ارشد و هیئت مدیره گزارش می شوند. دو اصل مرتبط با بخش نظارت بر فعالیت ها به شرح زیر می باشند :

اصل شانزدهم: سازمان، بایستی ارزیابی های مداوم و / یا جداگانه را در جهت تعیین اینکه آیا اجزای کنترلهای داخلی به روز و کارا هستند را انتخاب ، توسعه، و اجرا کند. همچنین باید میزان تغییرات در کسب و کار و فرآیندهای آن را هنگام انتخاب و توسعه ارزیابیهای در حال انجام و جدا از هم در نظر گرفته

شود و ارزیابیها توسط افرادی که به اندازه کافی آگاه و دارای صلاحیت هستند صورت پذیرد. لازم به ذکر است که ارزیابی های جداگانه باید به صورت دوره ای به منظور ارائه بازخورد اهداف انجام شود .

اصل هفدهم: سازمان، باید در صورت لزوم، کمبودهای کنترل داخلی مرتبط به افرادی که مسئول اقدامات اصلاحی هستند، از جمله مدیریت ارشد و هیئت مدیره را ارزیابی کند. نتایج ارزیابیهای مذکور بایستی بررسی شده و هر گونه نقصی بلافاصله اصلاح شود. در نهایت، مدیریت باید پیگیری کند که آیا کمبودهای کشف شده به موقع اصلاح شده است یا خیر. چارچوب جدید کوزو، به طور کامل و مفصل تری استفاده از تکنولوژی و ارائه دهندگان خدمات برون سازمانی را تشریح کرده است .

در پایان مقایسه تفاوت های مهم رویکرد شناسایی، ارزیابی و مستند سازی کنترلهای داخلی حاکم بر گزارشگری مالی (با استفاده از پرسشنامه های استاندارد کنترل داخلی) با رویکرد کوزو مفید به نظر می رسد.

الف– با استفاده از رویکرد کوزو، بر خلاف روش سنتی شناسایی، ارزیابی و مستند سازی کنترلهای داخلی حاکم بر گزارشگری مالی (به کمک تکمیل پرسشنامه های استاندارد کنترلهای داخلی و ثبت سیستم از طریق شرح سیستم یا نمودار گردش عملیات)،کلیه عملیات در کاربرگی تحت عنوان "کاربرگ ارزیابی ریسک فعالیت مورد نظر" منعکس می گردد و نیازی به ثبت سیستم از طریق "شرح یا رسم نمودار گردش عملیات" بطور جداگانه نیست .

ب– استفاده از رویکرد کوزو، منتج به شناسایی عوامل ریسک دستیابی به اهداف فعالیتهای مهم مورد نظر به صورت عینی می شود. در حالی که رویکرد سنتی مندرج در بند الف، حتی عوامل ریسک مرتبط با ادعاهای مدیریت در مورد گزارشـگـری مـالـی را نیز مشخص نمی کند .

پ– رویکرد کوزو قادر به شناسایی، ارزیابی و مستند سازی کنترلهای داخلی مرتبط با فعالیتهای با ماهیت متفاوت می باشد. درحالی که رویکرد سنتی مندرج در بند الف، صرفا درمورد کنترلهای داخلی حاکم بر گزارشگری مالی کاربرد دارد .

ت– باعنایت به مطالب مندرج در بندهای الف تا پ فوق، صرفا با استفاده از رویکرد کوزو ، شناسایی، مستند سازی و ارزیابی کنترلهای مرتبط با کلیه فعالیتهای مهم مورد نظر "باماهیتهای متفاوت" امکانپذیر است. به عبارت دیگر با استفاده از روش سنتی مندرج در بند الف فوق ، ارزیابی ریسک فعالیتهای مهم بنگاه تحت هیچ شرایطی امکانپذیر نیست .

ث- استفاده ازرویکرد کوزو، زمینه لازم برای مدیریت ریسک بنگاه (ERM) را فراهم می کند .

ج- رعایت استانداردهای بین المللی حسابرسی داخلی (IIA) در مورد ارزیابی فرایندهای نظام راهبری، مدیریت ریسک و کنترل، مستلزم استفاده از رویکرد کوزو است .

SOA .١٦

بعضی از این استانداردهای فوق به دلایل مختلف چندان مورد استقبال سازمان ها قرار نگرفته است. چهار استاندارد برتر دنیا که به طور گسترده در زمینه چارچوب، ساختار و امنیت فناوري اطلاعات مورد استفاده قرار می گیرند عبارتند از :

- ✓ ISO 27001
- ✓ COBIT
- ✓ ITIL
- ✓ PCI DSS

همپوشاني حوزه هاي امنيتي

در سال 2009، یازده حوزه کنترلي اساسی معرفی شد که به EC ١١ معروف گردید این کنترل ها می بایست توسط سازمان هایی که می خواهند امنیت اطلاعات را پیاده سازی نمایند پیاده سازی شوند، اگر این کنترل ها را به عنوان معیاری برای تحقق امنیت اطلاعات در نظر بگیریم حاصل مقایسه چهار استاندارد مذکور، با توجه به این معیارها به شکل زیر خواهد بود.

ردیف	کنترل ها	ISO27001	PCIDSS	ITIL	COBIT
۱	خط مشی امنیت اطلاعات	✓	✓	✓	✓
۲	مدیریت عملیات و ارتباطات	✓	✓	×	✓
۳	کنترل دسترسی	✓	✓	✓	✓
٤	اکتساب، توسعه و نگهداری سیستم های اطلاعاتی	✓	✓	×	✓
٥	سازمان امنیت اطلاعات	✓	✓	✓	✓
٦	مدیریت دارایی	✓	✓	✓	✓
۷	مدیریت حوادث امنیت اطلاعات	✓	✓	✓	✓
۸	مدیریت تداوم کسب و کار	✓	✓	✓	✓
۹	امنیت منابع انسانی	✓	✓	×	✓
۱۰	امنیت محیط فیزیکی	✓	✓	×	✓
۱۱	انطباق	✓	✓	✓	✓

جدول۳- مقایسه استانداردها

مقایسه چهار استاندارد برتر

جهت مقایسه متناظر ویژگي هاي این استانداردها، جدول زیر برخي موضوعات قابل تأمل را مشخص مي نماید.

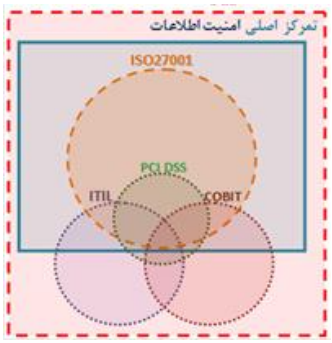
ردیف	ISO27001	PCIDSS	ITIL	COBIT
خصوصیات استانداردها	ISO یک سازمان غیردولتی است که وظیفه اصلی آن استاندارد نمودن فعالیت ها با نگرشی تسهیل کننده نسبت به تبادلات کالاها ، خدمات، بهبود همکاری در زمینه علمی، فنی، اطلاعاتی، اقتصادی و حمایتاز تولید کننده و مصرف کننده می باشد.	PCIDSS یک استاندارد امنیت اطلاعات جهانی است که توسط انجمن استانداردهای امنیت صنعت کارت پرداخت شده است. این استاندارد از کلاه برداری و خطر افشای کارت اعتباری از طریق افزایش کنترل های اطراف داده جلوگیری می کند.	ITIL یا کتابخانه زیرساخت IT از طرف دولت بریتانیا ایجاد شد. تمرکز اصلی آن بر روی بهترین روشها برای تمام مراکز داده برای تضمین خدمات IT می باشد.	COBIT مجموعه ابزار پشتیبانی و چارچوب مدیریت IT است. COBIT بر توسعه خط مشی و روش های مناسب برای کنترل IT در سراسر سازمان تکیه دارد. همچنین بر یک انطباق قاعده متد تاکید می کند که برای افزایش اثربخشی IT به سازمان کمک می کند.
گواهینامه های آموزشی	گواهینامه سری ISO27000	گواهینامه سری PCIDSS	گواهینامه سری ITIL	CRISCTM-CGEIT-CISM-CISA
حوزه	امنیت اطلاعات	امنیت تراکنش داده و اطلاعات در حساب، خرید اینترنتی، ATM و دستگاه POS	مدیریت خدمات IT	مدیریت IT
گستردگی استفاده	۱۶۳ عضو ملی از ۲۰۳ کشور جهان	۱۲۵ عضو ملی از ۲۰۳ کشور جهان	۵۰ شعبه بین المللی	۱۶۰ کشور

جدول٤- مقایسه استانداردها

انتخاب استاندارد جهت پیاده سازي امنيت اطلاعات

بسیار مهم است که استانداردی در سازمان پیاده سازی گردد که به عنوان یک معیار همگانی شناخته شده و مورد قبول اکثر سازمان ها و قوانين كشوري باشد، استاندارد ISO توسط ۲۵ کشور راه اندازی شد، این درحالی است که سه استاندارد دیگر تنها در یک کشور شروع به کار کردند. در این خصوص ISO به نسبت سه استاندارد دیگر بسیار شناخته شده تر است، ISO به طور گسترده در جهان توسط 163کشور مورد استفاده قرار گرفته است، در مقایسه با(125) PCIDSS ، (50) ITIL و ISO27001 .(160) COBIT به علت جامعيت كنترل هاي آن نسبت به سه استاندارد امنیتی دیگر، موجبات پذیرش آن توسط مشتريان، تامين كنندگان، خريداران و مديران را فراهم مي سازد. همانطور که در شکل نیز مشاهده می نمایید، امنیت اطلاعات که به عنوان جزئی از حاکمیت فن آوری اطلاعات در نظر گرفته می شود، بیشتر توسط ISO27001 پوشش داده شده، در صورتی که ITIL و COBIT سهم بیشتری در خصوص حاکمیت فناوری اطلاعات دارا می باشند، گستردگی این استانداردها در شکل مشخص شده، نواحی مشترک، نشان دهنده کنترل های امنیتی و حوزه هایی هستند که استانداردها با یکدیگر همپوشانی دارند، همچنین همانطور که مشاهده می شود PCI DSS همپوشانی زیادی با ISO27001 دارد با این تفاوت که PCI DSSدر حوزه امنیت کارت فعالیت می کند، این شکل بیانگر این موضوع است که پیاده سازی ISO27001علاوه بر اینکه به تنهایی امنیت اطلاعات را در سازمان به صورت عمومی تضمین می نماید، می تواند به عنوان بستری مناسب جهت پیاده سازی استانداردهای امنیتی دیگر متناسب با حوزه کاری هر زمانی مورد استفاده قرار می گیرد.

هر استاندارد به نوعی نقش خود را در پیاده سازی امنیت اطلاعات ایفا می کند، به عنوان مثال ISO27001بر سیستم مدیریت امنیت اطلاعات، PCIDSS بر امنیت اطلاعات مرتبط با تراکنش کسب و کار و کارت هوشمند، ITIL و COBIT بر امنیت اطلاعات و ارتباطشان با مدیریت پروژه و حاکمیت فناوري اطلاعات تمرکز دارند. به طور کلی استقبال عمومی در استفاده جهانی از استانداردها، نشان می دهد که ISO27001 برتر از سه استاندارد دیگر در سطح جهانی ظاهر شده است به خصوص براي ايجاد سيستم مديريتي امنيت اطلاعات، این استاندارد نسبت به دیگر استانداردها راحت تر پیاده سازی می شود و توسط ذينفعان (مديران ارشد، كاركنان، تأمين كنندگان، مشتريان و قانون گذاران) به خوبی قابل درک است. از این رو با در نظر گرفتن سطح بالاي قابليت استفاده و اعتماد به ISO27001 در جهان، میتوان این استاندارد را همچون زبان انگلیسی به عنوان زبان بین المللی و جهانی در استانداردها و معیارهای ISMS دانست.



شکل۷- حاکمیت فناوری اطلاعات

فصل دوم: استاندارد OWASP

مهمترین استاندارد امنیت نرم افزارهای تحت وب

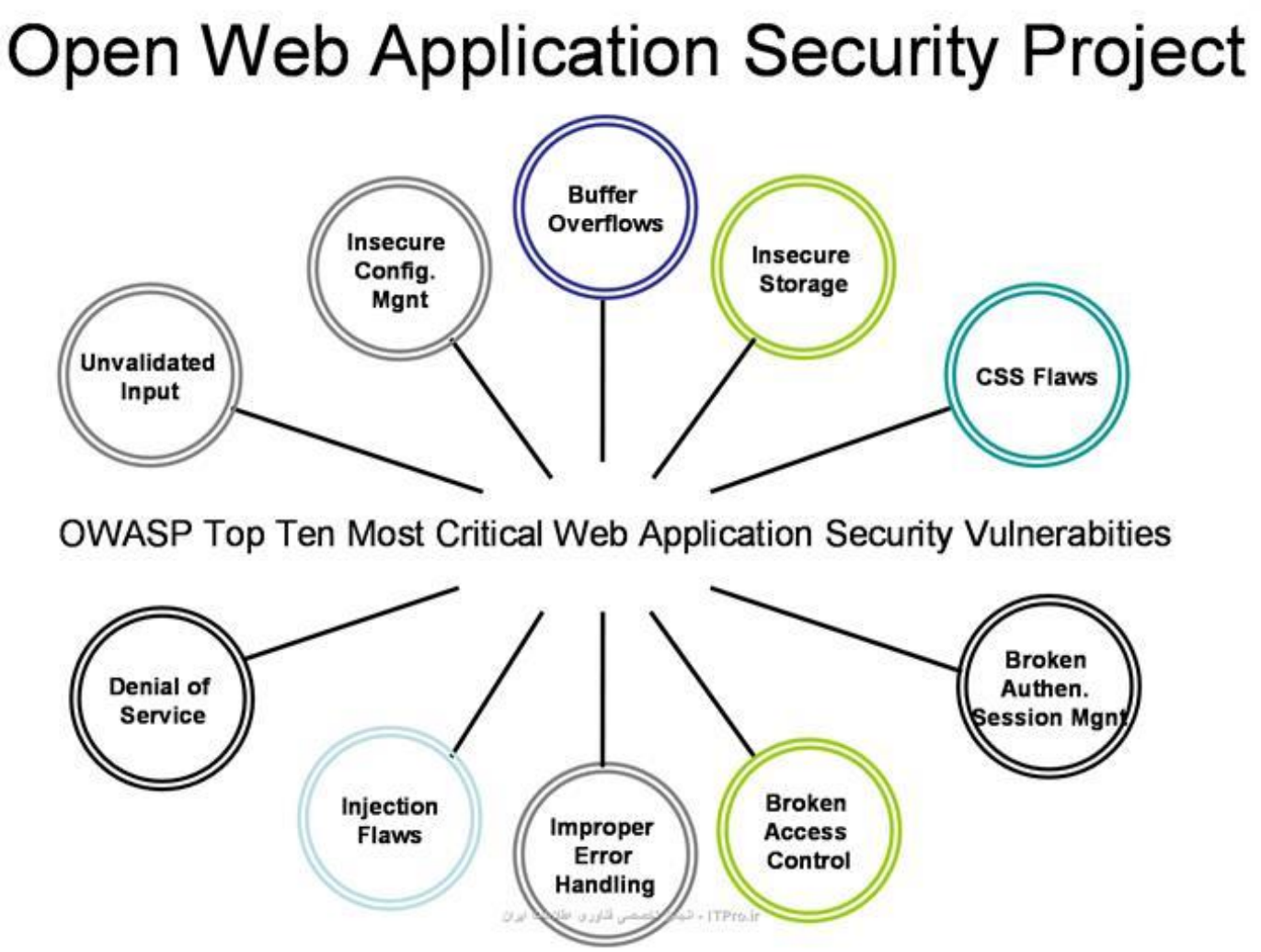
یکی از شاخه های امنیت، امنیت نرم افزار های تحت وب که شامل وب سایت ها و نرم افزارهای تحت وب و همچنین وب سرویس ها می باشد، است. با توجه به آمار سال ۲۰۱۲ vendor Cenzic بیشترین آسیب پذیری های وب سایت ها و نرم افزارهای تحت وب در این زمینه ها است:

نوع حمله	درصد آسیب
Cross-site scripting	37%
SQL injection	16%
Path disclosure	5%
Denial-of-service attack	5%
Arbitrary code execution	4%
Memory corruption	4%
Cross-site request forgery	4%
Data breach (information disclosure)	3%
Arbitrary file inclusion	3%
Local file inclusion	2%
Remote file inclusion	1%
Buffer overflow	1%
Other, including code injection (PHP/JavaScript), etc.	15%

جدول ۳- درصد حملات به نرم افزارهای تحت وب

یکی از استانداردهای مهم موجود در زمینه امنیت نرم افزارهای تحت وب OWASP است. کلمه OWASPمخفف شده Open Web Application Security Protocol Project است و یک متدولوژی یا یک پروژه غیر دولتی است که در آن به شما به عنوان یک کارشناس برنامه نویس تحت وب ، معیارهایی که بایستی برای امن تر شدن نرم افزار خود به کار ببرید تشریح شده است. OWASP یک متدولوژی است، یعنی راهکار را به ما نشان می دهد، این متدولوژی منحصر به شرکت یا فرد یا سازمان خاصی نبوده و نیست و یک پروژه کاملا متن باز (Open Source) است که هر کسی در هر جای دنیا می تواند به آن بپیوند و در آن شرکت کند. جامعه آماری که برای پروژه OWASP فعالیت می کنند در زمینه های مختلفی از جمله تولید مقالات، شرکت در تالارهای گفتمان، معرفی و تولید نرم افزارهای امنیتی وب، تولید مستندات و متدولوژی های امنیتی بصورت کاملا رایگان فعالیت می کنند و نتیجه فعالیت خود را در مستند نهایی این پروژه مشاهده می کنند. پروژه OWASP در ابتدا به عنوان یک استاندارد

مطرح نشد اما امروزه به عنوان معیار یا بهتر بگوییم Baseline امنیتی طراحی و تولید امنیت در نرم افزارهای تحت وب استفاده می شود. سازمانی بین المللی و غیر انتفاعی می باشد که در راستای ایمن سازی طراحی، پیاده سازی، توسعه و تست پروژه های نرم افزاری فعالیت می کند. تمامی مستندات، ابزارها و چک لیست های مندرج در سایت رسمی آن سازمان رایگان بوده و در جهت برطرف نمودن آسیب پذیری های امنیتی متداول در تمامی قالب های کاری نرم افزار توسعه داده شده است.چندین هزار کاربر فعال در سر تا سر جهان در این پروژه فعالیت داشته و در جهت بهبود مطالب و ابزار به این سازمان یاری می رسانند.



شکل ۴- پروژه OWASP

لیست پروژه های OWASP

پروژه OWASP با توجه به گستردگی تکنولوژی های وب و همچنین پیچیده تر شدن ساختارهای برنامه نویسی و مبحث امنیت آنها به خودی خود به چندین پروژه کوچکتر تبدیل شد و امروزه اکثر افرادی که تصور می کنند با OWASP آشنایی دارند صرفا با یک یا چند عدد از این زیر پروژه ها آشنایی دارند، OWASP امروزه متشکل از ۹ زیر پروژه یا پروژه های کوچک است که هر کدام بصورت جداگانه در خصوص یکی از موارد مرتبط با امنیت حوزه نرم افزارهای تحت وب فعالیت می کنند، این پروژه ها عبارتند از:

۱. OWASP Application Security Verification Standard یاASV

استاندارد تایید امنیت نرم افزارهای کاربردی یا ASVS همانطور که از نام این پروژه پیداست برای دریافت تاییده برای نرم افزارهای وب در خصوص رعایت استاندارد های امنیت بکار گرفته می شود. بر طبق این استاندارد یک سری تست های امنیتی بر روی نرم افزار از قبلی Cross Site Scripting و SQL Injection و حملاتی از این قبلی انجام می شود و در صورت رعایت شدن این موارد در نرم افزار ، موفق به دریافت استاندارد می شوند.

۲. OWASP XML Security Gatewayیا XSG

این استاندارد بصورت پایلوت فعلا ایجاد شده است و بصورت ویژه برای برقراری امنیت برای ساختار XMLمورد استفاده قرار می گیرد.

۳. OWASP Development Guide

راهنمای توسعه نرم افزار برای برنامه نویسان وب ایجاد شده است و شامل یک سری نمونه کدهای کاربردی و تمثیلی از زبانهای برنامه نویسی مانند J2EE و ASP.NET و PHP می باشد. در این راهنمای برنامه نویسی و توسعه نرم افزارهای وب برنامه نویس با انواع و اقسام حملات تحت وب از قبیل SQL Injection و همچنین حملات جدیدتر شامل Phishing و حتی مباحث کارت های اعتباری و امنیت تبادلات الکترونیک، Session Fixation و بسیاری دیگر از مسائل مهم اعم از مشکلات حریم خصوصی در وب سایت ها آشنا می شوند و به آنها در جهت رفع مشکلات احتمالی در خصوص این نرم افزار ها راهنمایی های لازم ارائه می شود.

٤. OWASP Testing Guide

همانطور که از نام این پروژه مشخص است راهنمایی برای تست و آزمون گرفتن از نرم افزارهای کاربری تحت وب است. این پروژه در واقع یک راهنمای مقدماتی برای برنامه نویسان وب می باشد تا بتوانند در پروژه های تست نفوذ سنجی به نرم افزارهای تحت وب از آن استفاده کرده و آن را

معیار امنیتی خود قرار بدهند. در این راهنما تکنیک های مقدماتی نفوذ و حمله به نرم افزارهای تحت وب و سرویس های تحت وب تشریح شده است.

۵. OWASP Code Review Guide

راهنمایی برای مرور کدهای نوشته شده و مستند سازی کدهای نوشته شده می باشد که برنامه نویس بتواند پس از نوشتن یا توسعه نرم افزار کاربردی وب خود آن را آزمایش کرده و نقاط ضعف در کدهای نوشته شده را برطرف کند.

٦. OWASP ZAP Project

این پروژه یک نرم افزار تست نفوذ سنجی تقریبا ساده می باشد که برای انجام تست های نفوذ سنجی به نرم افزار های کاربردی تحت وب مورد استفاده قرار می گیرد. این ابزار برای استفاده برنامه نویسان و هکرهای قانومند بسیار مناسب و کاربردی می باشد.

۷. OWASP Top Ten

هدف از این پروژه اطلاع رسانی در خصوص مشکلات امنیتی نرم افزارهای تحت وب و هشدار دهی به سازمان ها در خصوص امنیت برنامه های تحت وب می باشد. در این پروژه انواع و اقسام مختلفی از ابزارها، کد ها، راهنماها و ... معرفی و استفاده می شود.

۸. OWASP Software Assurance Maturity Model یا SAM

این پروژه یک راهنما برای سازمان ها است تا بتوانند یک چارچوب درست امنیتی و تحلیل امنیتی برای نرم افزارهای تحت وب خود ایجاد کنند تا بتوانند با مشکلات امنیتی نرم افزارهای کاربردی تحت وب و ریسک های آن بصورت هدفمند و روشمند مقابله و برخورد کنند.

۹. Webgoat

این پروژه یک نرم افزار کاربردی تحت وب می باشد که تمامی نقاط ضعفی که تا به حال توسط OWASPشناخته شده اند را بصورت مجازی و در قالب یک محیط برنامه نویسی شده شبیه سازی و در اختیار برنامه نویسان قرار می دهند.افرادی که با انواع حملات آشنایی پیدا کرده اند ولی می خواهند آن را بصورت عملی درک کنند کافیست این نرم افزار را دانلود کرده و آن را نصب و از طریق راهنمای آن تمامی حملات را بصورت شبیه سازی شده انجام دهند.

شاخص های آسیب پذیری در OWASP

این سازمان هر چند سال یک مرتبه لیستی از شاخص ترین آسیب پذیری های متداول در نرم افزار ها و سرویس های ارائه شده تحت وب در سر تاسر جهان را از طریق مستندی ارائه می کند که این لیست مبنای امنیتی نرم افزارهای تحت وب به شمار می رود. تا قبل از نوشتن این مطلب آخرین بار این لیست در سال ۲۰۱۳ ارائه شده است. هر چند سال یک مرتبه این سازمان لیستی از شاخص ترین آسیب پذیری های متداول در نرم افزار ها و سرویس های ارائه شده تحت وب در سر تاسر جهان را از طریق مستندی ارائه می دهد که این لیست مبنای امنیتی نرم افزارهای تحت وب به شمار می رود. خلاصه آخرین آسیب پذیری های منتشر شده در سال ۲۰۱۳ توسط این سازمان (OWASP Top 10 List ۲۰۱۳) شامل موارد زیر است:

۱. تزریق (Injection)

آسیب پذیری تزریق کد همانند تزریق SQL، OS و LDAP زمانی رخ می دهد که داده های نامعتبر به یک مترجم (Compiler or Interpreter) به جای دستور و یا query ارسال می گردند. هکر از

طریق داده های نامعتبر قادر به فریب مترجم شده و امکان اجرای دستورات غیر قانونی و یا روئیت اطلاعات حیاتی بدون مجوز دسترسی برای او فراهم می شود.

۲. تاییدیه شکسته شده و مدیریت جلسه (Broken Authentication and Session Management)

فانکشن های نرم افزارهای کاربردی مرتبط با اعطای مجوز دسترسی و مدیریت Session گاهی به درستی پیاده سازی نشده و این امکان را به هکرها می دهد تا به اطلاعات حیاتی همانند رمز های عبور، کلید ها، Session Token در جهت سوء استفاده و جعل هویت دسترسی پیدا کنند.

۳. اسکریپت کراس سایت (Cross-Site Scripting)

این آسیب پذیری زمانی رخ می دهد که نرم افزار کاربردی، داده های نا امن را بدون اعتبار سنجی برای کاوشگر وب ارسال نماید. هکر توسط این آسیب پذیری قادر به اجرای اسکریپت بر روی کاوشگر قربانی، دزدیدن session و یا تغییر مسیر قربانی به وب سایت های مخرب (malicious sites) خواهد بود.

٤. ارجاع نا امن به اشیاء داخلی برنامه (Insecure Direct Object References)

این آسیب پذیری زمانی رخ می دهد که برنامه نویس دسترسی ارجاع یک منبع به اشیاء داخلی برنامه را باز گذاشته باشد (همانند فایل، دایرکتوری و یا بانک اطلاعاتی). بدون کنترل دسترسی به این اشیاء هکر قادر به دستکاری منابع در جهت دسترسی به اطلاعات حیاتی خواهد بود.

۵. پیکربندی امنیتی اشتباه (Security Misconfiguration)

امنیت مناسب نیارمند تعریف و استقرار پیکربندی مناسب برای نرم افزار، قالب کاری، وب سرور، بانک اطلاعاتی و سیستم عامل می باشد. تنظیمات امن می بایستی تعریف، پیاده سازی و نگهداری شوند که البته تنظیمات پیش فرض بسیار نا امن می باشند. همچنین می بایستی همیشه نرم افزارها به روز نگهداشته شوند.

٦. افشای اطلاعات حساس (Sensitive Data Exposure)

بسیاری از نرم افزارهای کاربردی تحت وب به درستی از اطلاعات محرمانه خود (همانند اطلاعات اعتبار سنجی کاربران و اطلاعات کارت بانکی) محافظت نمی کنند. هکر با دزدیدن این اطلاعات قادر به سوء استفاده از آنها و ایجاد خرابکاری خواهد بود. اطلاعات محرمانه و حیاتی نیازمند محافظت ویژه ای می باشند که از آن جمله می توان به رمز نگاری اطلاعات در زمان تبادل اطلاعات با کاوشگر اشاره نمود.

۷- عدم سطح دسترسی مناسب برای دسترسی به فانکشن (Missing Function Level Access Control)

بسیاری از نرم افزارها قبل از اجرای فانکشن و نمایش خروجی در میانای کاربر (UI)، حق دسترسی را بررسی می نمایند. در نظر داشته باشید که نرم افزار همان سطح دسترسی را می بایستی درسمت سرور بررسی کند. در صورتی که در خواست اعتبار سنجی نگردد، هکر قادر به جعل درخواست در جهت دسترسی به فانکشن ها خواهد بود.

۸- جعل درخواست (Cross-Site Request Forgery)

این آسیب پذیری، کاوشگر قربانی وارد شده به نرم افزار را مجبور می کند که درخواست HTTP جعل شده را به همراه session's cookie قربانی و سایر اطلاعات مورد نیاز اعتبار سنجی شده را به برنامه کاربردی ارسال نماید. هکر توسط این حمله قادر به جعل هویت کاربر و جرای دستورات مخرب بر روی حساب آن خواهد بود.

۹- استفاده از کامپوننت ها با آسیب پذیری های شناخته شده (Using Components with Known Vulnerability)

کامپوننت ها همانند کتابخانه ها، قالب های کاری و سایر ماژول های نرم افزار معمولا با دسترسی کامل اجرا می گردند. در صورتی که آسیب پذیری کامپونتی افشا گردد، تخریب اطلاعات و دسترسی به سرور امکان پذیر خواهد بود. نرم افزار هایی که از کامپوننت هایی با آسیب پذیری های شناخته شده استفاده می کنند، امکان انواع حمله را برای هکر فراهم می سازند.

۱۰ - تغییر مسیر های نامعتبر (Unvalidated Redirects and Forwards)

نرم افزارهای کاربردی دائما در حال تغییر مسیر کاربران به صفحات دیگر می باشند و از داده های نا امن برای تشخیص صفحات مقصد استفاده می کنند. بدون استفاده از اعتبارسنجی مناسب، هکر قادر به هدایت قربانی به وب سایت های مخرب و فیشینگ خواهد بود.

فصل سوم: Check List استاندارد های مختلف

شرکت های مختلف استاندارد های مختلفی برای امنیت نرم افزار ها در نظر گرفته اند که در هرکدام از آن ها موارد به خصوصی برای اعطای استاندارد بررسی خواهد شد. در ادامه برخی از معروفترین check list ها آورده شده است:

۱. NIST
۲. Microsoft-WebServer
۳. Microsoft-ManagedCode
۴. Microsoft-DatabaseServer
۵. Microsoft-DataAccess
۶. Microsoft-ASP.net
۷. Microsoft-Architecture&Design
۸. ISO27002-Security-Framework-Audit-Program
۹. ISMS

منابع

۱- https://en.wikipedia.org/wiki/Web_application_security

۲- https://en.wikipedia.org/wiki/ISO/IEC_27001:2005

۳- http://www.columbia.edu/acis/security/articles/support/websecuritysoe.pdf

٤- http://www. security.itpro.ir

٥- http://www.douran.com/DesktopModules/News/NewsView.aspx?TabID=1&Site=DouranPortal&Lang=fa-IR&ItemID=1827&mid=15226&wVersion=Staging

٦- http://www.embaconference.com/portal/files/pages/EMBA2Articles/32/8239.pdf

۷- http://system.parsiblog.com/Posts/728/%D8%A7%D9%84%DA%AF%D9%88%D9%8A+%D8%A8%D9%84%D9%88%D8%BA+%D9%82%D8%A7%D8%A8%D9%84%D9%8A%D8%AA+%DA%A9%D8%A7%D8%B1%DA%A9%D9%86%D8%A7%D9%86%28/P-CMM%29

۸- http://www.placabi.com/prince2/tabid/194/Default.aspx