اهداف دوره

- آشنایی با مفاهیم و مقدمات امنیت اطلاعات
- معرفی سیستم مدیریت امنیت اطلاعات و استاندارد مرجع
- روش های پیاده سازی ISO 27001:2013
- نگاه مدیریت ریسک به امنیت اطلاعات
- آشنایی با مستندات مرجع سیستم مدیریت امنیت اطلاعات
- ارائه تجارب پیاده سازی ISMS در کشور

سرفصل های دوره

- بخش اول: مفاهیم و تعاریف امنیت اطلاعات
- بخش دوم: معرفی استاندارد ۲۷۰۰۱:۲۰۱۳
- بخش سوم: مرور استاندارد ISO 27001
- بخش چهارم: مدیریت ریسک

بخش اول

مفهوم و تعاریف امنیت اطلاعات

- تعاریف و مدل های امنیت اطلاعات
- تعریف سیستم مدیریت امنیت اطلاعات

مفهوم ISMS

اطلاعات چیست؟

- اطلاعات بر روی مستندات

- اطلاعات موجود در شبکه ها

- اطلاعات یک کارمند

- اطلاعات الکترونیکی

- اطلاعات صوتی و تصویری

اطلاعات به عنوان دارایی (Asset)

از منظر سازمان

اطلاعات مانند سایر دارایی هایی که در کسب و کار تأثیر دارند یک دارایی با ارزش برای سازمان است که باید اقدامات لازم را برای حفاظت از آن فراهم نمود.

از منظر داده کاوی و استخراج دانش

امنیت اطلاعات چیست؟

" یک سطح قابل قبولی از آسودگی خیال برای اینکه ریسکهای موجود و کنترل های بکار گرفته شده در تعادل هستند."

Jim Anderson, Inovant (2002)

عناصر امنیت اطلاعات

امنیت اطلاعات چیست؟

- ISO 27000 امنیت اطلاعات را اینگونه تعریف می نماید؛

صیانت از:

✓ **محرمانگی:**

محافظت از اطلاعات در برابر دسترسی غیرمجاز.

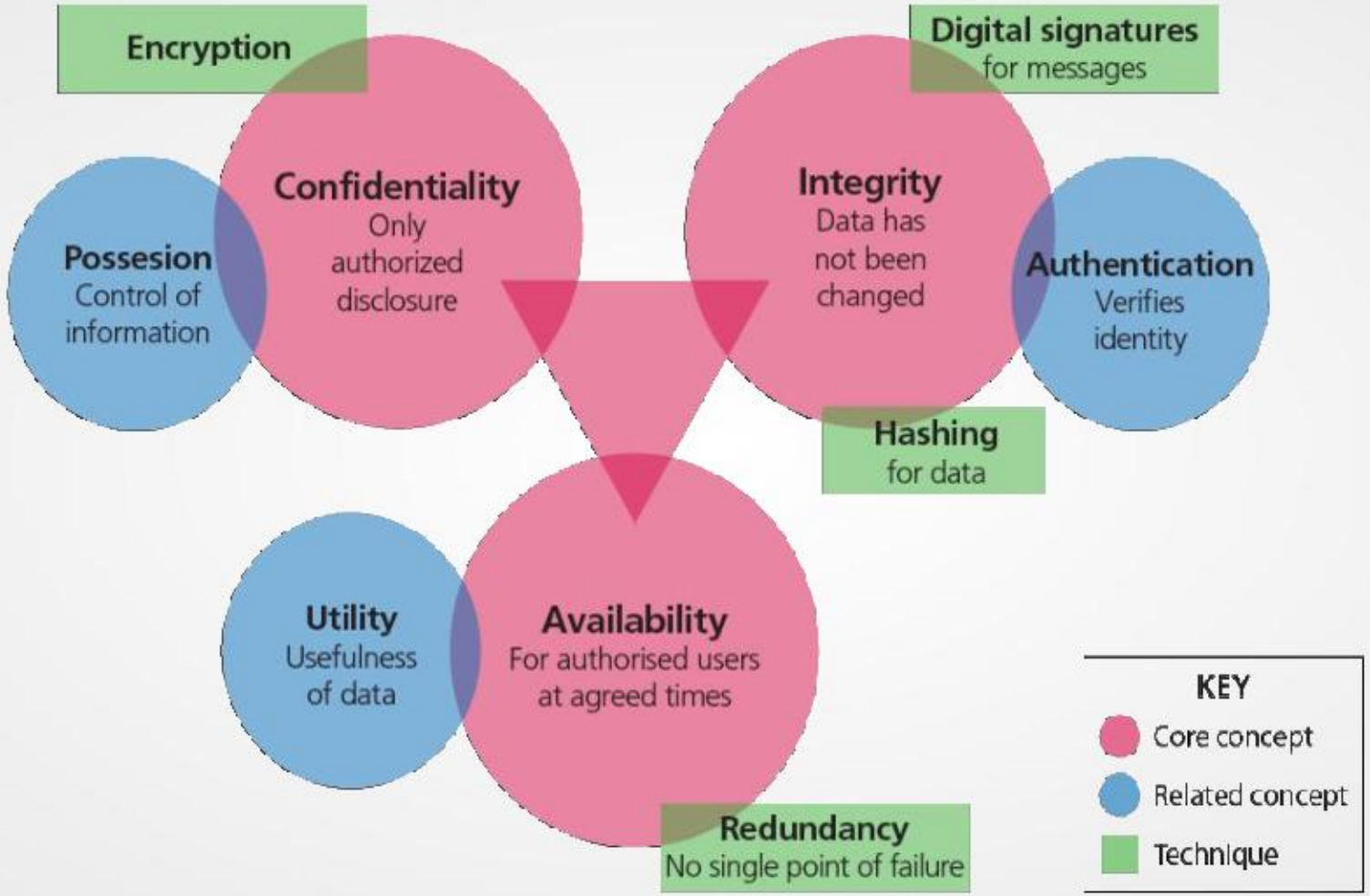
✓ **یکپارچگی:**

محافظت از اطلاعات در برابر تغییر یا پاک شدن غیرمجاز.

✓ **در دسترس بودن:**

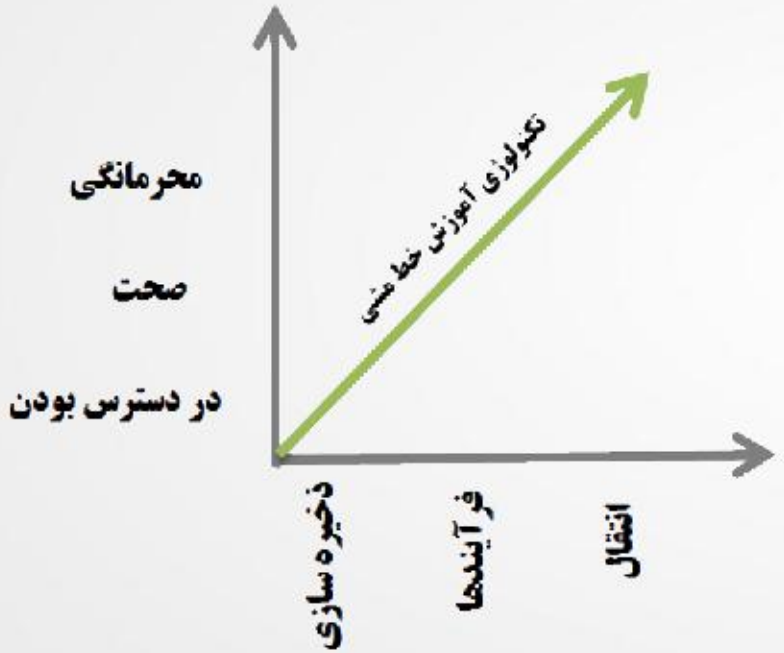
اطمینان از اینکه کاربران مجاز به اطلاعات دسترسی دارند و زمانی که دارایی های اطلاعاتی را بخواهند برای آنها فراهم باشد و بتوانند به آن متصل شوند.

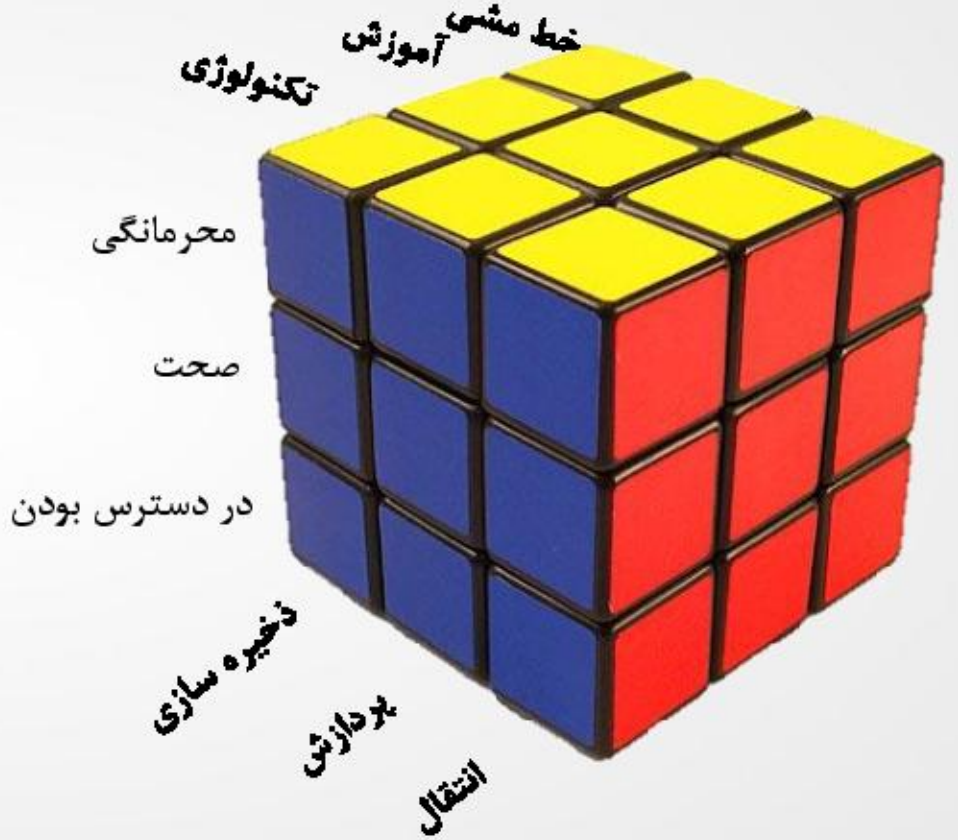
عناصر امنیت اطلاعات



(Jim Clinch, 2010)

مفهوم – مدل امنیت NSTISSC

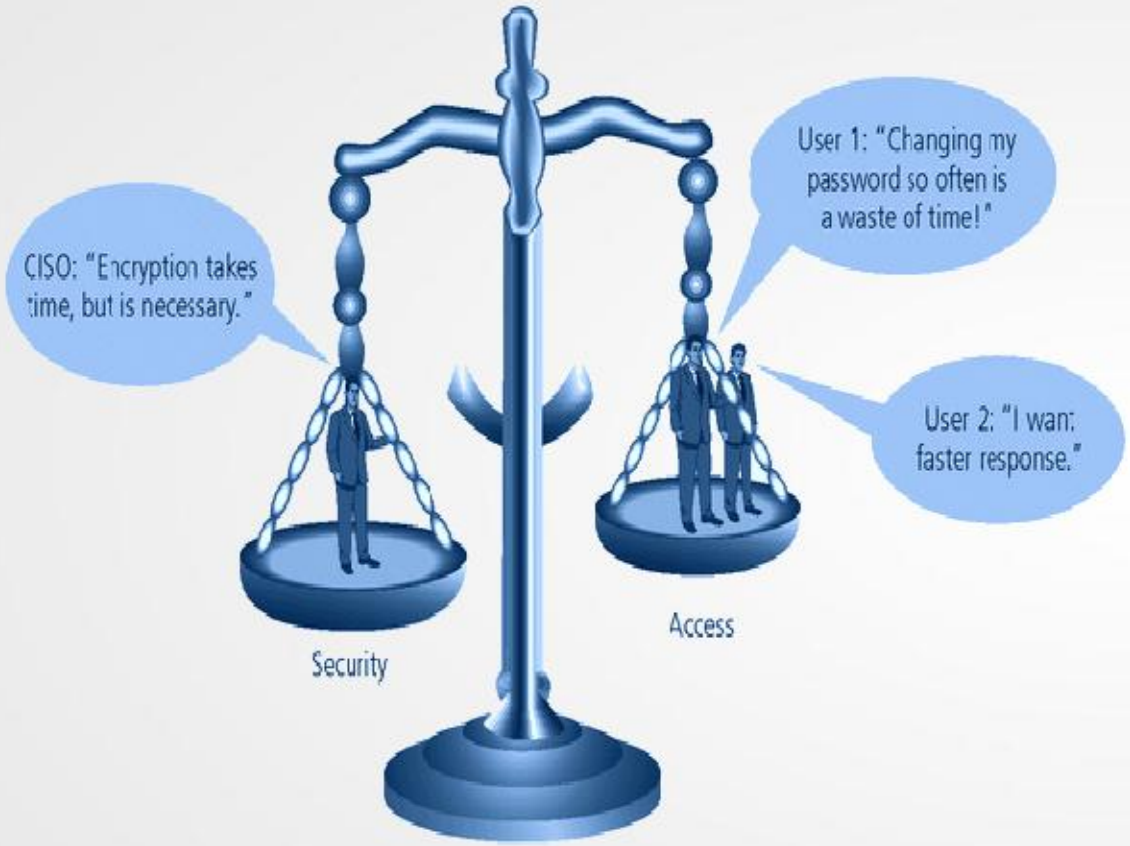




تحول و بلوغ امنیت در طول زمان

(Jared M. Lunsford, 2004)

امنیت و دسترسی به تعادل



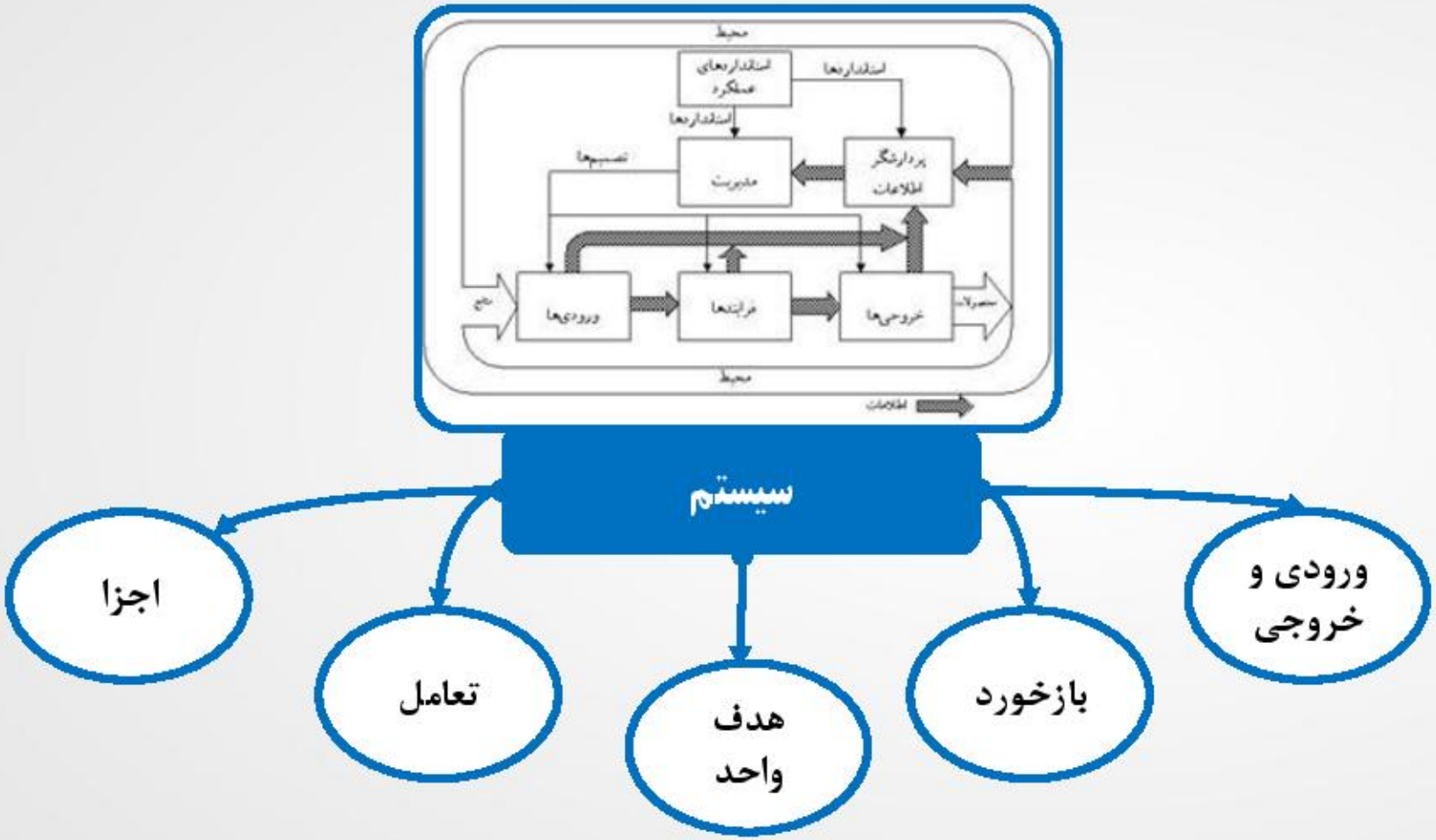
- امنیت به صورت ۱۰۰٪ وجود ندارد.
- باید تعادل بین امنیت و در دسترس بودن و سهولت استفاده وجود داشته باشد.

چشم انداز کسب وکار

سیستم مدیریتی چیست؟

- **پنج وظیفه اصلی مدیریت:**

۱- برنامه ریزی Planning
۲- سازماندهی Organizing
۳- به کار گماردن Staffing
۴-رهبری / هدایت Directing
۵-نظارت / کنترل Control



بخش دوم

معرفی استاندارد ۲۷۰۰۱:۲۰۱۳

- ضرورت و نیاز به امنیت اطلاعات
- معرفی استاندارد **ISMS**
- معرفی خانواده استاندارد **ISO 27000**
- حوزه های امنیت اطلاعات

نیاز به امنیت اطلاعات

- **وابستگی سازمانها به اطلاعات و سیستم های اطلاعاتی باعث آسیب پذیرتر شدن آنها نسبت به تهدیدات امنیت اطلاعات شده است؛**

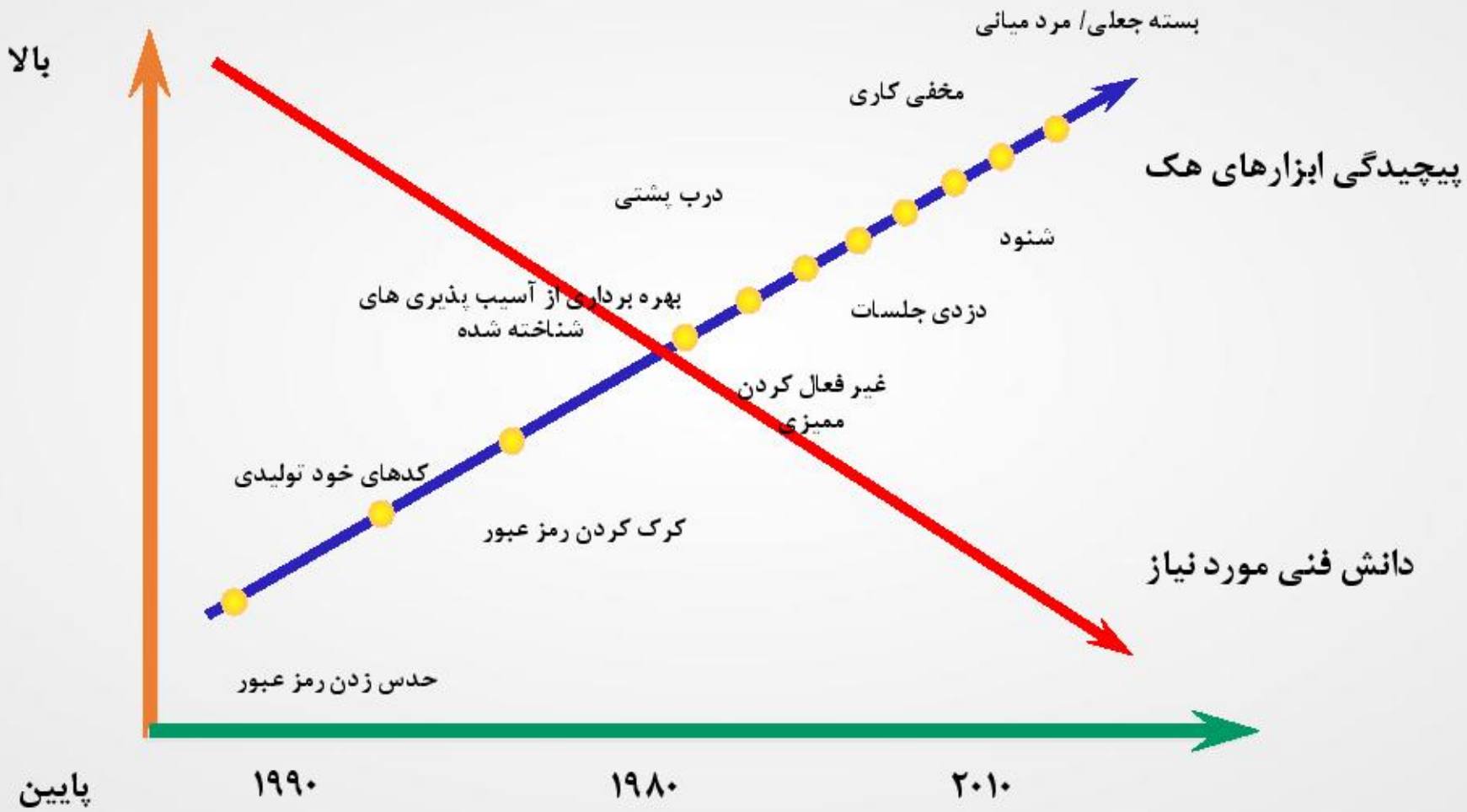
برخی از این تهدیدات عبارتند از:

- هک و نفوذ
- ویروس ها و کرم های کامپیوتری
- کلاهبرداری های رایانه ای
- دستکاری و تغییر اطلاعات
- حملات تخریب سرویس
- جاسوسی
- خرابکاری
- سیل، زلزله و سایر بلایای طبیعی

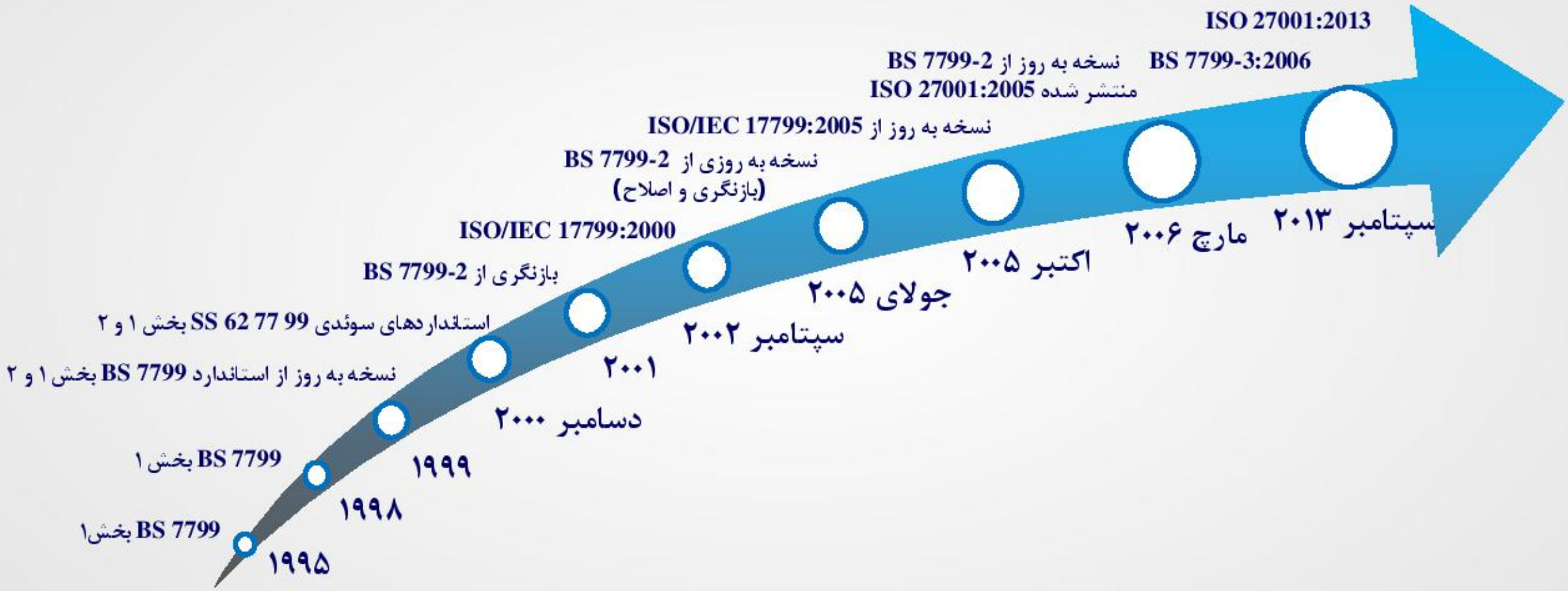
دسته بندی تهدید

طبقه بندی تهدیدات	مثال
۱. اشتباه یا خطای انسانی	حوادث و اشتباهات کارکنان
۲. عدم سازگاری با مالکیت معنوی	دزدی و نقض قوانین حق کپی رایت و تکثیر
۳. اعمال عمدی جاسوسی	دسترسی های غیر مجاز و یا جمع آوری داده ها
۴. اعمال عمدی دشمنی یا خرابکاری عمدی	تخریب سیستم و یا اطلاعات
۵. سرقت	مصادره غیر قانونی تجهیزات و یا اطلاعات
۶. حملات نرم افزاری عمدی	ویروس ها، کرم ها، ماکروها، قطع خدمات
۷. عوامل طبیعت	آتش سوزی، سیل، رعد و برق و زلزله
۸. انحراف در کیفیت خدمات ارائه دهندگان خدمت	اینترنت، شبکه، برق
۹. خرابی فنی سخت افزار یا خطاها	خرابی تجهیزات
۱۰. خرابی فنی نرم افزار یا خطاها	اشکالات، مشکلات کد، نقاط ضعف ناشناخته
۱۱. فناوری های قدیمی	فناوری های کهنه و یا منسوخ شده

قابلیت های بیشتر، تهدید خطرناک و استفاده آسان تر



تاریخچه استاندارد ISO 27001

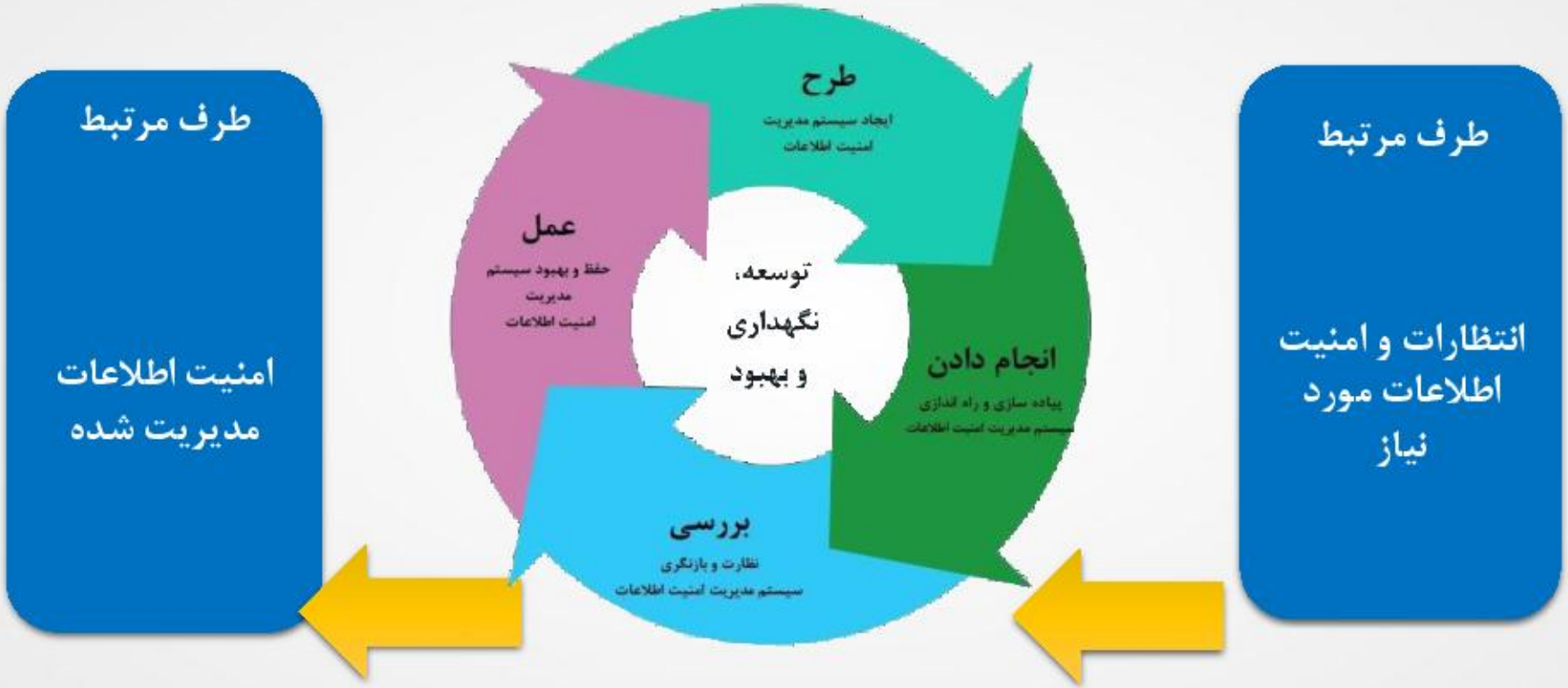


استاندارد های منتشرشده خانواده ۲۷۰۰۰

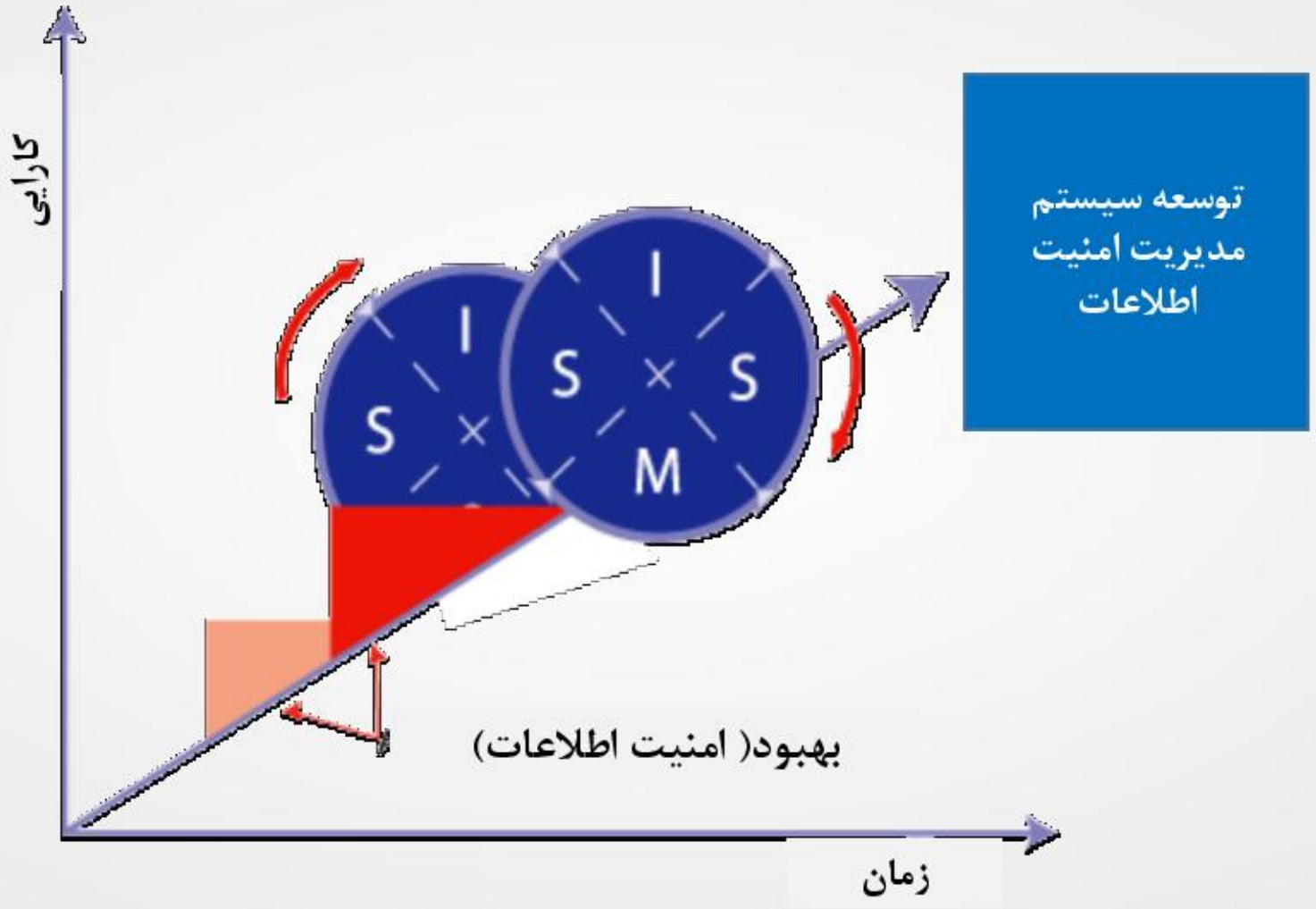
- ایزو ۲۷۰۰۰ سیستم‌های مدیریت امنیت اطلاعات - مرور و لغتنامه
- ایزو ۲۷۰۰۱ سیستم‌های مدیریت امنیت اطلاعات - نیازمندی‌ها
- ایزو ۲۷۰۰۲ راهنمای عملی مدیریت امنیت اطلاعات
- ایزو ۲۷۰۰۳ راهنمای پیاده سازی سیستم‌های مدیریت امنیت اطلاعات
- ایزو ۲۷۰۰۴ سیستم‌های مدیریت امنیت اطلاعات - اندازه گیری
- ایزو ۲۷۰۰۵ مدیریت ریسک امنیت اطلاعات
- ایزو ۲۷۰۰۶ نیازمندی‌های اشخاص بازرس و صادرکنندگان گواهی سیستم‌های مدیریت امنیت اطلاعات
- ایزو ۲۷۰۱۱ خط مشی‌های مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی بر اساس ایزو ۲۷۰۰۲
- ایزو ۲۷۰۳۱ خط مشی آماده سازی تکنولوژی اطلاعات و مخابرات برای ادامه کسب و کار
- ایزو ۱-۲۷۰۳۱ مقدمه و مفاهیم امنیت شبکه
- ایزو ۲۷۰۳۵ مدیریت حوادث امنیتی
- ایزو ۲۷۷۹۹ مدیریت امنیت اطلاعات در سلامت با استفاده از ایزو ۲۷۰۰۲

چرخه دمینگ (PDCA)

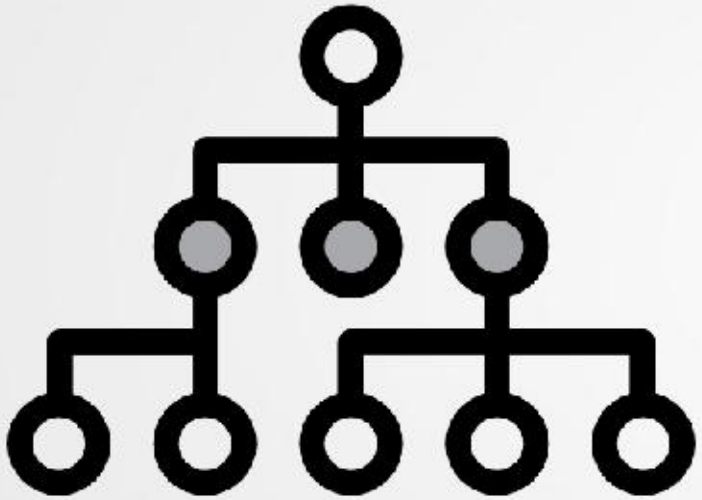
رویکرد مدیریت ISMS



بهبود مستمر ISMS



ساختار ISO 27001:2013



- ۰. مقدمه
- ۱. محدوده
- ۲. مراجع اصلی
- ۳. واژگان و تعاریف
- ۴. فضای سازمان
- ۵. رهبری
- ۶. برنامه ریزی
- ۷. پشتیبانی
- ۸. عملیات
- ۹. ارزیابی کارایی
- ۱۰. بهبود
- ضمیمه الف – کنترل ها

دامنه های ISO 27001:2013

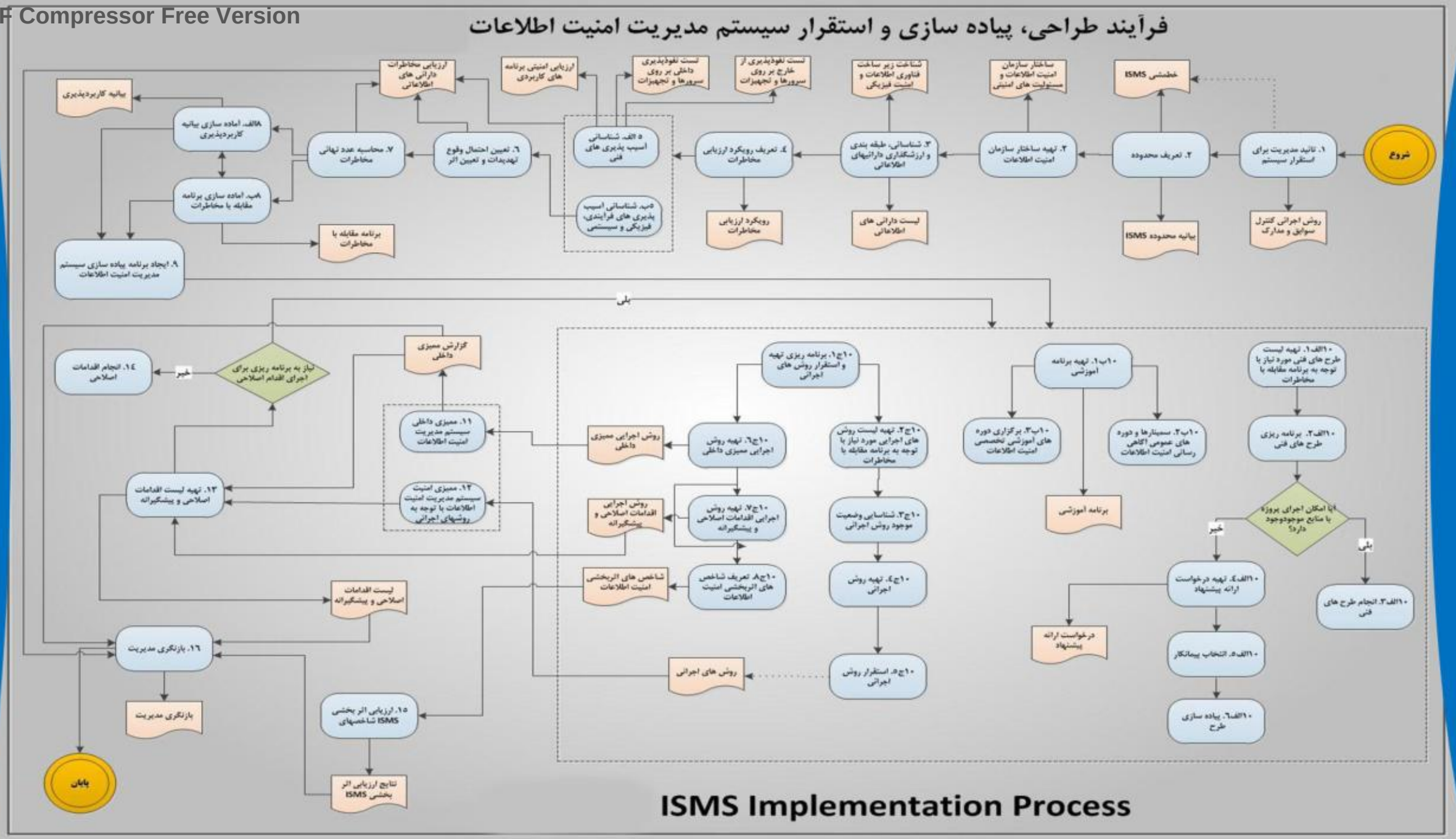
- از انتقال اطلاعات حساس و محرمانه خود از طریق فضاها و کانال‌های ارتباطی غیرامن خودداری نمایید.

بخش سوم

مرور استاندارد ISO 27001

29

فرآیند طراحی، پیاده سازی و استقرار سیستم مدیریت امنیت اطلاعات



ISMS Implementation Process

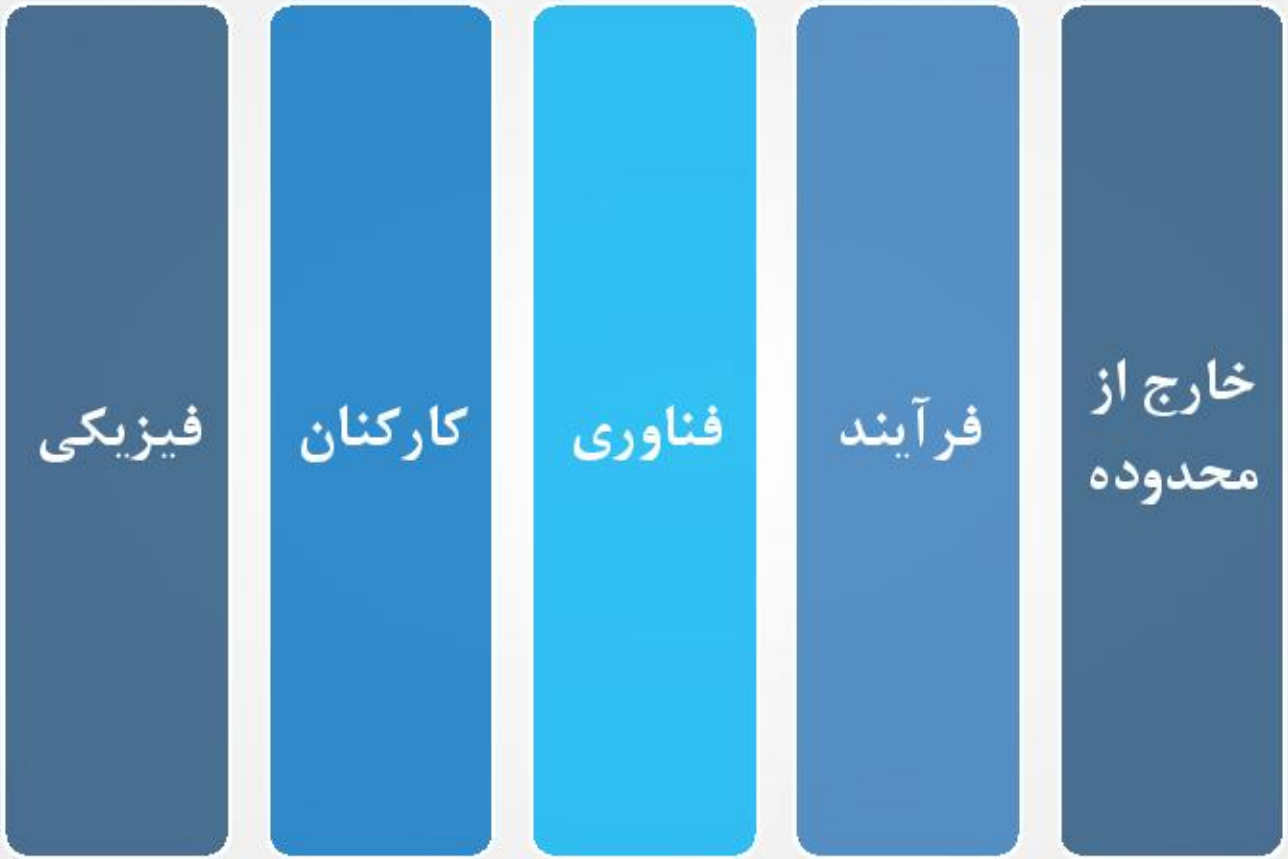
کلیات استاندارد

- ۰) مقدمه
- ۱) محدوده
- ۲) مراجع اصلی
- ۳) واژگان و تعاریف

فضای سازمان

- سازمان و فضای آن
- درک نیازها و انتظارات ذی‌نفعان
- تعیین دامنه سیستم مدیریت امنیت اطلاعات
- سیستم مدیریت امنیت اطلاعات

تعیین محدوده



۵. رهبری

- رهبری و تعهد
- خط‌مشی
- نقش‌ها، مسئولیت‌ها و اختیارات سازمانی

- **فعالیت‌هایی برای اشاره به ریسک‌ها و فرصت‌ها**
  - کلیات
  - ارزیابی ریسک امنیت اطلاعات
  - برنامه مقابله با ریسک امنیت اطلاعات
- **اهداف امنیت اطلاعات و برنامه دستیابی به آنها**

بخش چهارم

مدیریت ریسک امنیت اطلاعات

- مدیریت ریسک امنیت اطلاعات
- ارزیابی و مقابله با ریسک

36

اصطلاحات

دارایی اطلاعاتی (Information Asset):

داده و اطلاعاتی که برای سازمان ارزشمند است.

آسیب پذیری (Vulnerability):

ضعف یک **دارایی** یا **کنترل** که می تواند توسط یک **تهدید** مورد سواستفاده قرار گیرد.

تهدید (Threat):

علت بالقوه یک حادثه ناخواسته که می تواند برای یک سیستم یا سازمان خطر آفرین باشد.

کنترل (Safeguard/Control):

ابزار مقابله با ریسک شامل آموزش، تکنولوژی، خط مشی

حمله (Attack):

اقدام به تخریب، تغییر، تحریف، از کار اندازی یا دسترسی غیر مجاز و یا استفاده غیر مجاز از یک دارایی.

آنالیز ریسک (Risk Analysis):

استفاده نظام مند از اطلاعات برای شناسایی و **تخمین ریسک**

تخمین ریسک (Risk Estimation):

اختصاص مقادیر به احتمال و اثر **ریسک**

معیار ریسک (Risk Criteria):

معیارها و مراجعی که میزان اهمیت ریسک تخمین زده شده را مشخص می کند.

سنجش ریسک (Risk Evaluation):

فرآیند مقایسه ریسک تخمین زده شده با معیار ریسک، به منظور تعیین میزان اهمیت ریسک

ارزیابی ریسک (Risk Assessment):

فرآیند آنالیز ریسک و تشخیص ریسک

ریسک قابل قبول (Risk Acceptance):

تصمیم برای قبول ریسک/ بازه مورد قبول ریسک

ریسک امنیت اطلاعات (Information Security Risk):

پتانسیل استفاده یک تهدید از یک آسیب پذیری در دارایی

برنامه مقابله با ریسک(Risk Treatment Plan-RTP):

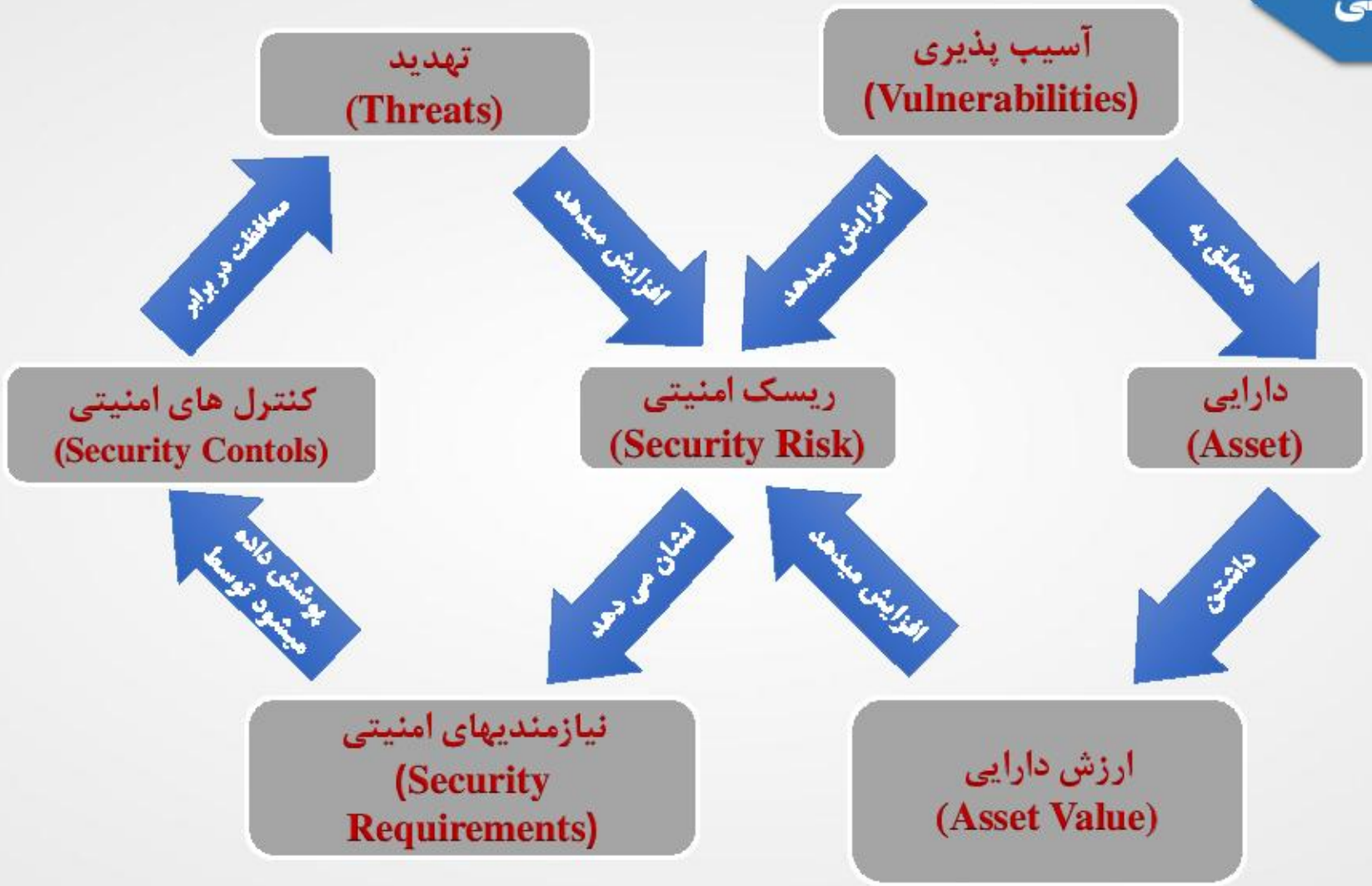
طرح ها، برنامه ها و پروژه های درنظر گرفته شده برای مقابله با ریسک های غیر قابل قبول

مدیریت ریسک (Risk Management):

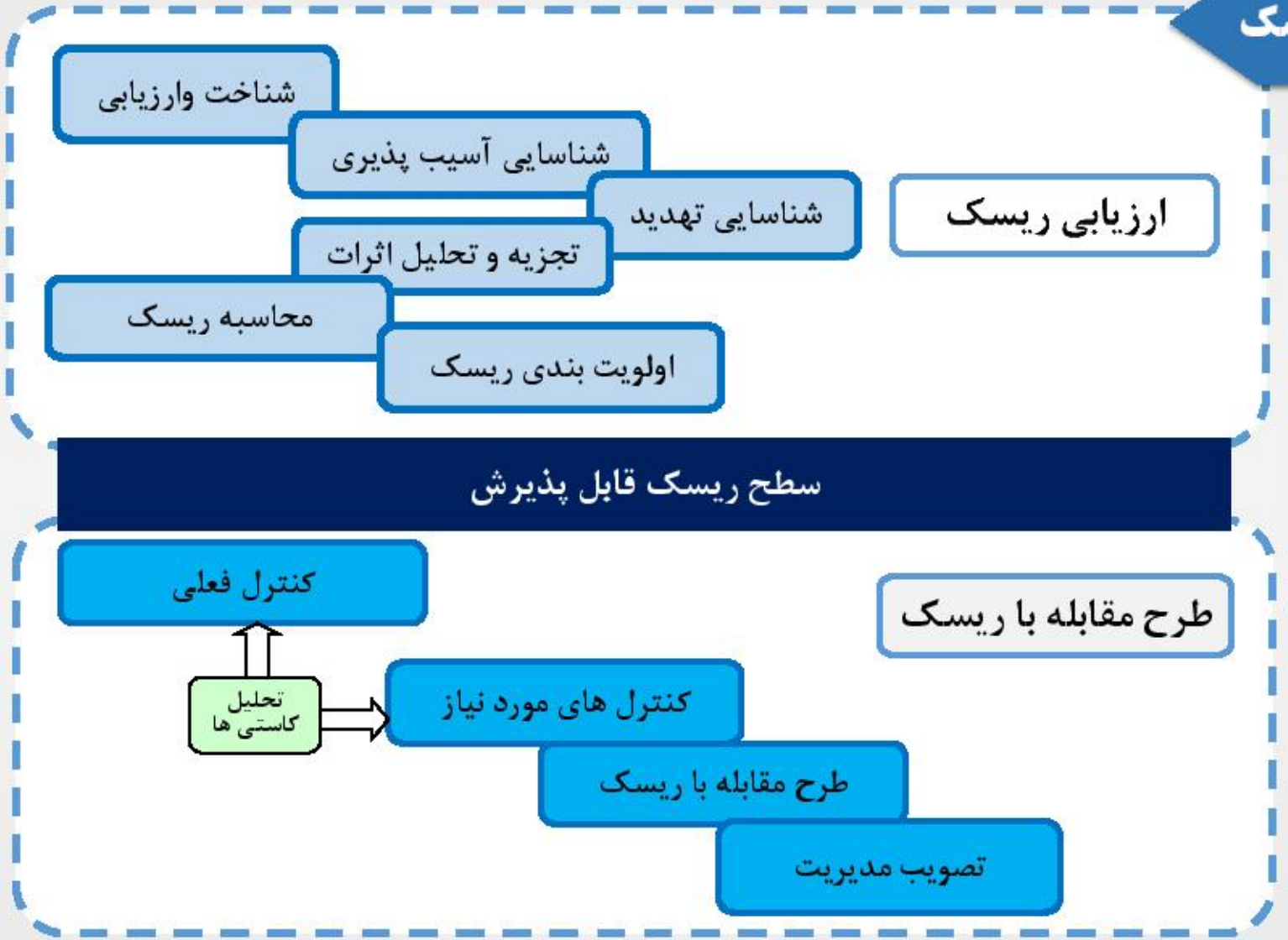
کلیه فعالیت های هدایت شده به منظور راهبری و کنترل ریسک.

آسیب پذیری، تهدید، ریسک

مفهوم ریسک امنیتی

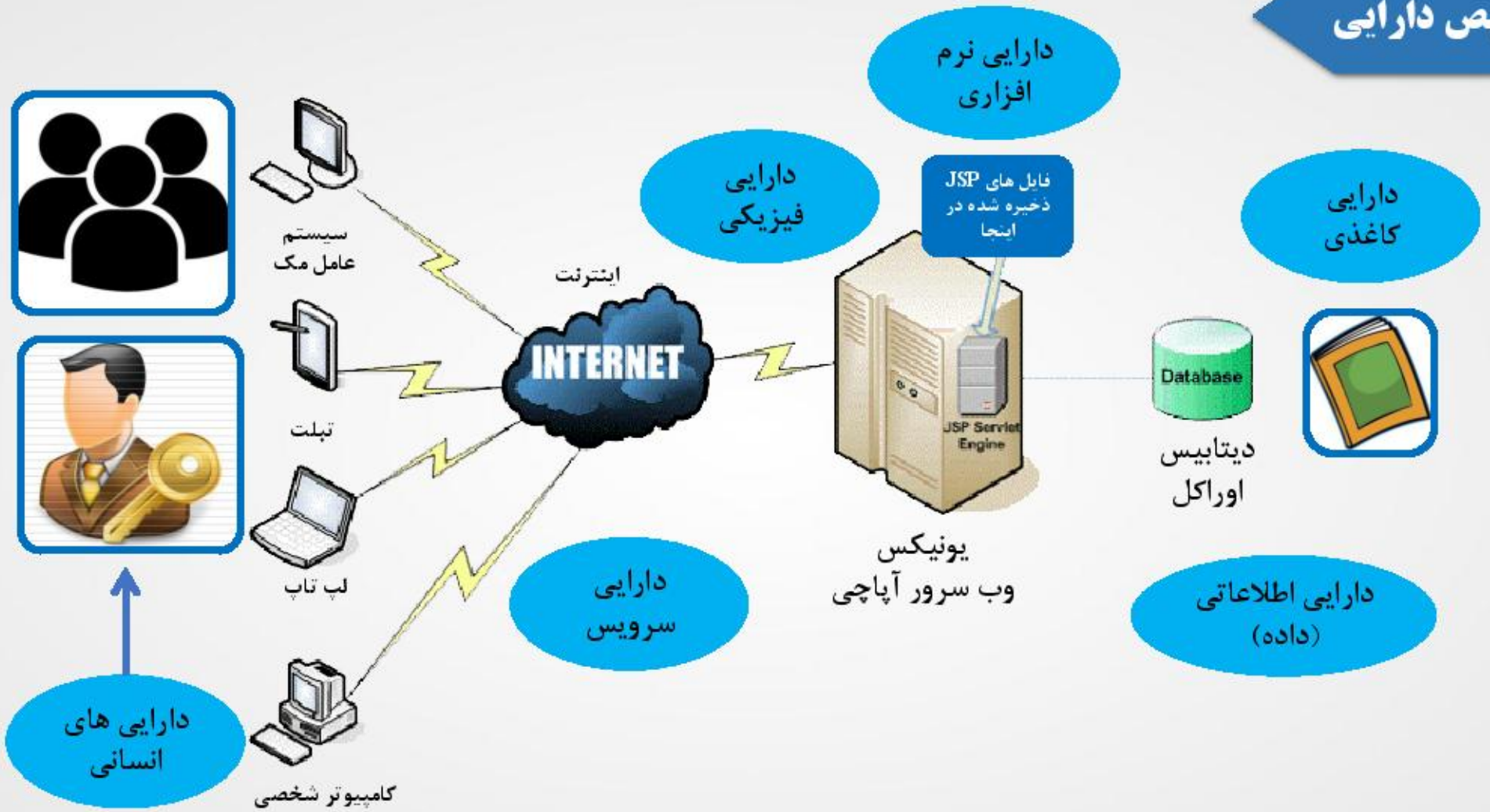


مراحل مدیریت ریسک



مراحل مدیریت ریسک

تشخیص دارایی



طبقه بندی دارایی ها

- ✓ نرم افزارهای تجاری
- ✓ نرم افزار داخلی توسعه یافته
- ✓ سخت افزار عمومی
- ✓ زیر ساخت
- ✓ سیستم عامل و سرویس
- ✓ نامشهود
- ✓ پرسنل
- ✓ ساختمان
- ✓ داده

تجهیزات حفاظت ساختمان
نرم افزار تجاری
کالا
رسانه های کامپیوتر
تجهیزات حفاظت کامپیوتر
سند الکترونیکی
منابع خارجی
خدمات خارجی
مبلمان و تجهیزات
سخت افزار عمومی
زیر ساخت
منابع داخلی
خدمات داخلی
نرم افزار داخلی توسعه یافته
رسانه ها
اسناد کاغذی
محل
ارتباطات
پرسنل

ارزش گذاری امنیتی دارایی ها

کسب و کار و اعتبار سازمان

صحت

دردسترس بودن

زمان انقطاع قابل پذیرش

تعداد کاربران

گستردگی کاربران

محرمانگی

محدوده افراد مطلع

کسب و کار و اعتبار سازمان

ارزش گذاری امنیتی دارایی ها

کارکنان	ساختمان‌ها	تجهیزات زیربنایی	سخت افزارها	سیستم عامل‌ها	نرم افزارهای تجاری	نرم افزارهای داخلی	داده‌ها	کاغذی	نامشهود

عنوان	شناسه دارایی	شرح دارایی	در دسترس بودن			محرمانگی		صحت	ارزش نهایی دارایی اطلاعاتی		
			محدوده کاربران	زمان انقطاع قابل پذیرش	وضعیت جایگزین	کسب و کار واعتبار	محدوده اطلاع افراد	کسب و کار واعتبار	در دسترس بودن (A)	محرمانگی (C)	صحت (I)
SQL server	CSW-۰۰۳	پایگاه داده	کمتر از یک ساعت	جایگزین موقت	کل شرکت	راهبر/مدیر	اعتبار شرکت	اعتبار شرکت	۶۶	۸۳-۵	۶۷
Elastix	CSW-۰۰۴	نرم افزار تلفن	یک ساعت یا یک روز	جایگزین موقت	کل شرکت	واحد	داخلی	داخلی	۷۱-۶۱	۵۰	۳۳
شیرپوینت	CSW-۰۰۶	۲۰۱۳	یک ساعت یا یک روز	جایگزین موقت	کل شرکت	واحد	برون شرکتی	داخلی	۷۱-۶۱	۸۳-۵	۳۳
SQL Central	CSW-۰۰۷	پایگاه داده مرکزی	کمتر از یک ساعت	جایگزین موقت	افراد محدود	راهبر/مدیر	اعتبار شرکت	اعتبار شرکت	۴۳-۸۹	۸۳-۵	۶۷
SharePoint App	CSW-۰۰۸	نرم افزار شیرپوینت	کمتر از یک ساعت	جایگزین اجباری	واحد	واحد	اعتبار شرکت	اعتبار شرکت	۳۸-۶۱	۶۷	۶۷

ذخیره برگردن

تشخیص آسیب پذیری و ارزش گذاری

ضعف در مدیریت سطوح دسترسی

۵۰

سطح آسیب پذیری

آیا قابلیت کنترل دسترسی بر روی سیستم عامل/ سرویس مورد نظر فعال می باشد؟

آیا از نام های کاربری منحصربفرد (Unique) جهت ورود به سیستم عامل استفاده می شود؟

آیا برای هر نام کاربری مجوزها (Privileges) های مورد نیاز تعریف شده است؟

آیا نام های کاربری غیرضروری غیرفعال و یا حذف شده اند؟

آیا میزان دسترسی ها و مجوزها مستند می باشند؟

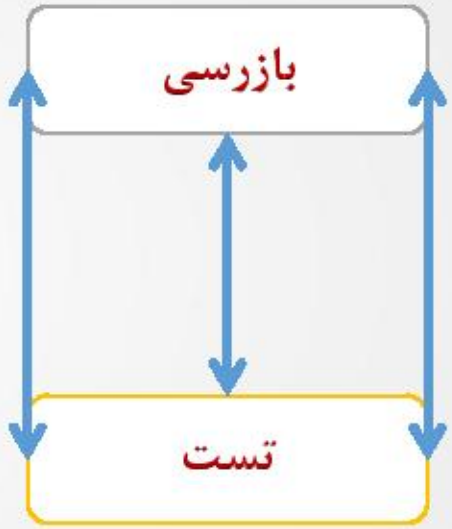
آیا میزان دسترسی ها و مجوزها مورد بازنگری و تایید قرار می گیرد؟

تایید

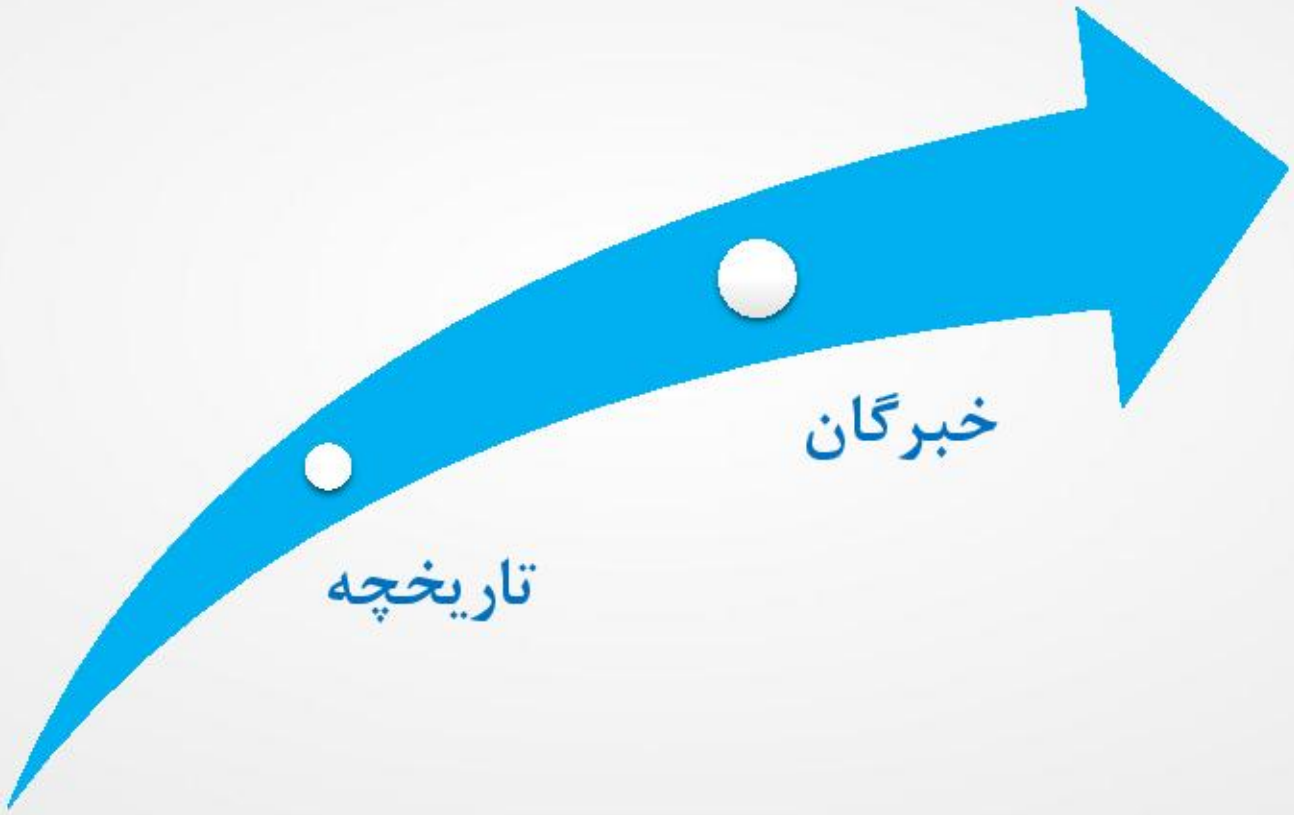
وضعیت سطح آسیب پذیری	عدد آسیب پذیری سطح
بلی	۱۰۰
بلی	۸۳
بلی	۶۷
خیر	۵۰
خیر	۳۳
خیر	۱۶.۵

جمع آوری داده به روش RIIOT

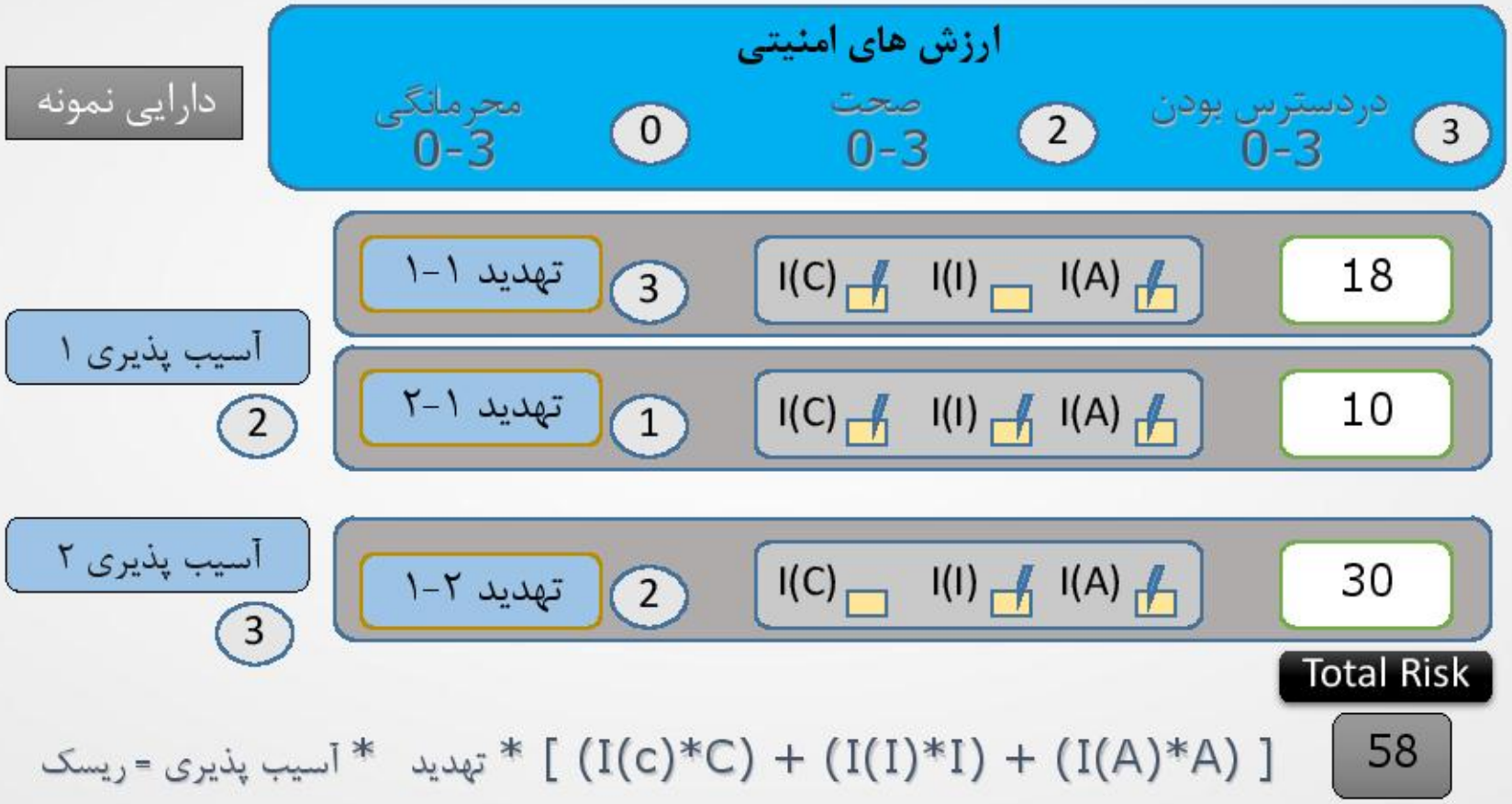
R	بازنگری اسناد
I	مصاحبه با کارمندان کلیدی
I	بازرسی کنترل های امنیتی
O	مشاهده رفتار پرسنل
T	تست عملکرد کنترل های امنیتی



تشخیص تهدید و تجزیه و تحلیل احتمال وقوع



متدولوژی ارزیابی ریسک



مالک دارایی و مالک ریسک

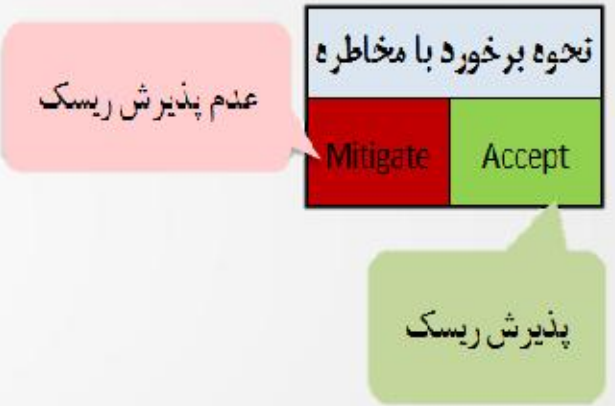
- مالک دارایی: فرد، واحد یا ماهیتی است که از سوی مدیریت، مسئولیت نگهداری و کنترل دارایی را بر عهده دارد.
- مالک ریسک: فرد، واحد یا ماهیتی است که در صورت رخ دادن ریسک، آسیب به او وارد می شود.

سطح ریسک قابل قبول

- پس از انجام فعالیت های مربوط به ارزیابی ریسک، باید با استفاده از یک مکانیزم مناسب، ریسک های قابل قبول را از ریسک های غیرقابل قبول جدا نماییم.
- ریسک قابل قبول، به ریسکی گفته می شود که با تایید مدیریت یا مالک ریسک، مورد قبول قرار گرفته و نیاز به فعالیتی برای برخورد ندارد

ناحیه های ریسک – تعیین سطح قابل قبول

ماتریس مقابله با مخاطرات										
۳			۲			۱			اسیب پذیری	
۳	۲	۱	۳	۲	۱	۳	۲	۱	ضربه	
I Mitigate	H Mitigate	G Accept	F Mitigate	E Accept	D Accept	C Accept	B Accept	A Accept	۳	۰
R Mitigate	Q Mitigate	P Mitigate	O Mitigate	N Mitigate	M Accept	L Accept	K Accept	J Accept	٦	٤
@ Mitigate	Z Mitigate	Y Mitigate	X Mitigate	W Mitigate	V Accept	U Accept	T Accept	S Accept	۹	۷



ریسک باقی مانده

- به میزان ریسکی که پس از فرض اجرای روش ها و طرح های تقابلی همچنان باقی می‌ماند، ریسک باقی مانده نامیده می شود.
- ریسک باقی مانده باید توسط مدیریت ارشد و یا مالک ریسک به تایید برسد.
- اتخاذ تصمیم برای استراتژی برخورد با ریسک و همچنین اختصاص کنترل های تقابلی باید به نحوی صورت پذیرد که ریسک باقی‌مانده، پایین تر از سطح قابل قبول ریسک در سازمان قرار گیرد.

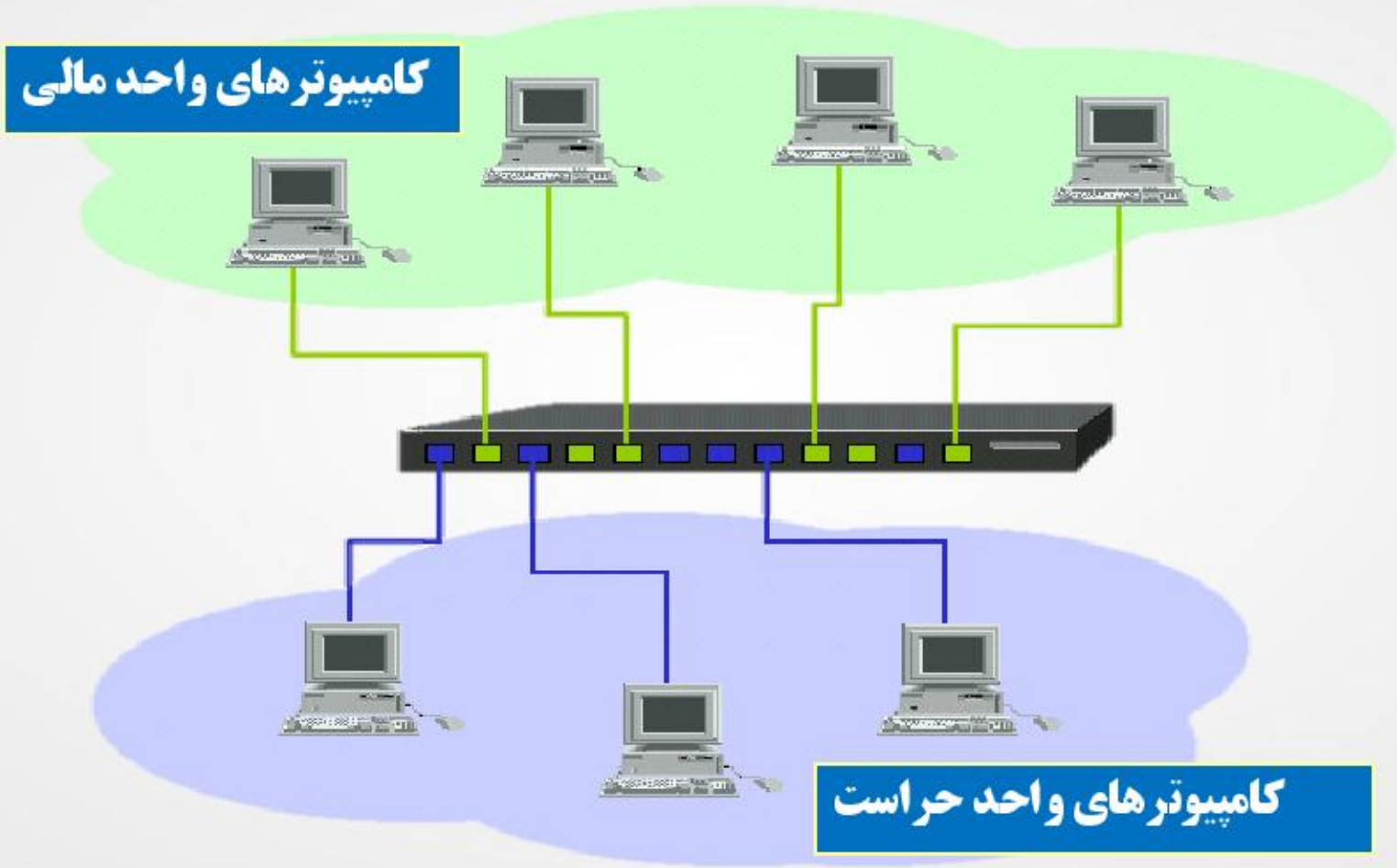
استراتژی های برخورد با ریسک

BS 25999	4T Law
تداوم	تسکین دادن Treat
پذیرش	تحمل کردن Tolerate
انتقال	انتقال Transfer
تغییر دادن، تاخیر و توقف	خاتمه دادن Terminate

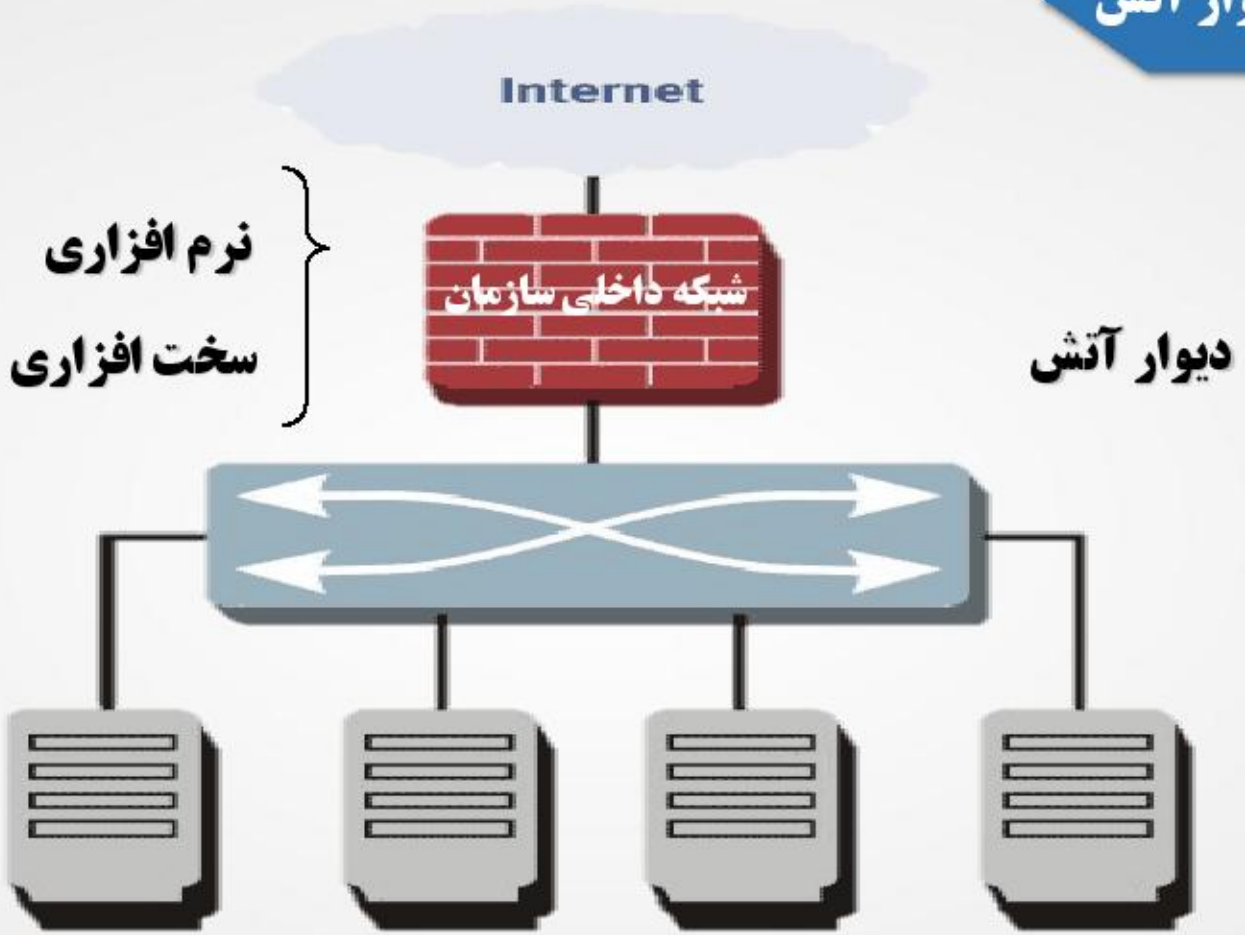
طرح مقابله با ریسک (RTP)

کد سناریو	آسیب پذیری	ارزش	تهدید	احتمال	ضربه	مخاطره	توضیحات	معیار پذیرش	کنترل ۱	کنترل ۲	کنترل ۳	استراتژی
R-SER-۰۱		۶۷	دسترسی غیرمجاز	متوسط	۳۰	۵۰		قابل پذیرش	A.۹.۱.۱	A.۹.۲.۱	A.۹.۲.۳	
R-SER-۰۲		۳۳	عدم ثبت زمان وقایع در هنگام رخداد	کاربر ناپخیر	۳۰	۱۰		قابل پذیرش	A.۱۲.۴.۴			
R-SER-۰۳		۷۵	وجود حوادث غیرمترقبه از جمله آتشسوزی	کاربر ناپخیر	۱۰	۴۰		غیر قابل پذیرش	A.۱۲.۳.۱	A.۱۷.۲.۱	A.۱۳.۱.۱	تغییر
آموزش: دوره +security مهلت: ۱۳۹۵/۰۵/۰۹			طرح: امنیت شبکه مهلت: ۱۳۹۵/۰۵/۰۹		سیاست: پشتیبان گیری مهلت: ۱۳۹۵/۰۵/۰۹		مسئول: آرش مرادی ریسک ثانویه:					
R-SER-۰۴		۷۵	عدم توانایی بازگرداندن اطلاعات	کاربر ناپخیر	۱۰	۴۰		غیر قابل پذیرش	A.۱۲.۳.۱	A.۱۷.۲.۱	A.۱۳.۱.۱	کاهش
آموزش: سمینار آگاهی رسانی امنیت مهلت: ۱۳۹۵/۰۴/۱۹			طرح: ----- مهلت: ۱۳۹۵/۰۴/۲۵		سیاست: روش اجرایی نسخه پشتیبان مهلت: ۱۳۹۵/۰۵/۰۹		مسئول: میلاد یدالهی ریسک ثانویه:					

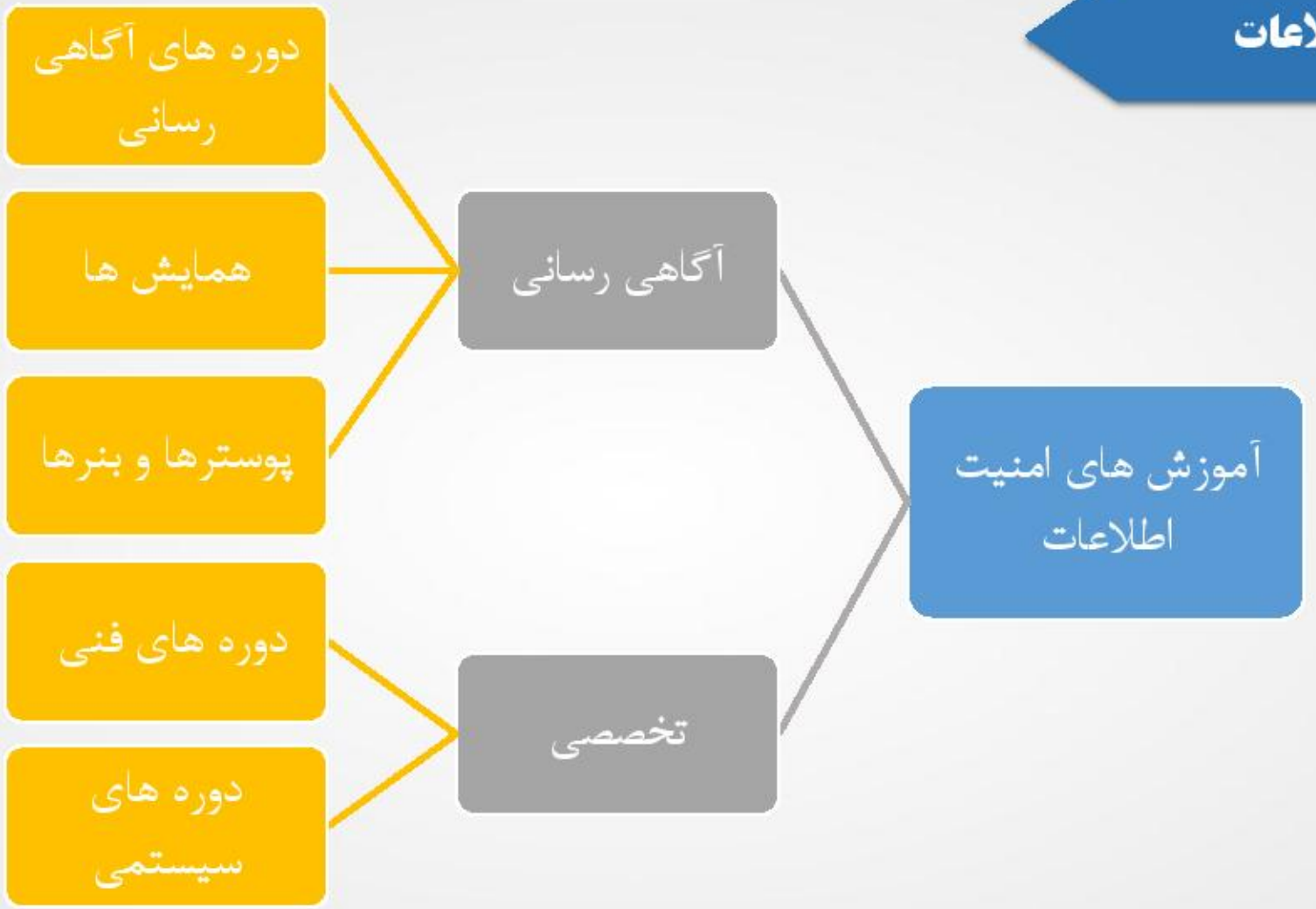
مثال طرح های فنی – شبکه محلی مجازی VLAN



مثال طرح های فنی – دیوار آتش



آموزش امنیت اطلاعات



سیاست ها و روش های اجرایی

۱- کنترل مستندات و سوابق	۷- نسخه پشتیبان	۱۳- استفاده از اینترنت	۱۹-ممیزی امنیت	۲۵- امنیت برنامه های کاربردی
۲- مقابله با کدهای مخرب وسیار(آنتی ویروس)	۸- تبادل اطلاعات	۱۴- امنیت منابع انسانی	۲۰- ممیزی داخلی	۲۶- استفاده از رسانه های قابل حمل
۳- کنترل دسترسی به اطلاعات و سیستم های اطلاعاتی	۹- سازگاری با الزامات قانونی و قراردای	۱۵- امنیت شخص ثالث	۲۱- اقدام اصلاحی	۲۷- مدیریت تغییرات
۴- روش اجرایی امنیت فیزیکی و محیطی	۱۰- پشتیبانی حوادث	۱۶- مدیریت تداوم کسب و کار	۲۲- سنجش اثربخشی	۲۸- جداسازی امن شبکه
۵- امحاء دارایی های اطلاعاتی	۱۱- کلمه عبور	۱۷- همزمان سازی ساعت سیستم	۲۳- بازنگری مدیریت	۲۹- امنیت پست الکترونیک
۶- مدیریت دارایی های اطلاعاتی	۱۲- رویکرد ارزیابی ریسک	۱۸- ساختار سازمانی امنیت	۲۴- پاسخگویی به خطاهای سیستم	۳۰- استفاده مجاز

۷. پشتیبانی

- منابع
- صلاحیت
- آگاهی
- ارتباط
- اطلاعات مستند شده
  - کلیات
  - ایجاد و به روز رسانی
  - کنترل اطلاعات مستند شده

۸. عملیات

- برنامه عملیاتی و کنترل
- ارزیابی ریسک امنیت اطلاعات
- برنامه مقابله با ریسک امنیت اطلاعات

۹. سنجش عملکرد

- پایش، اندازه گیری، تحلیل و سنجش
- ممیزی داخلی
- بازنگری مدیریت

تدوین روش اجرایی اندازه گیری شاخص های اثر بخشی

ISMS Indicators measurement

هدف

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- ارزیابی اثربخشی اقدامات و تصمیمات، مطابق با روش های اجرایی و خط مشی های سیستم مدیریت امنیت اطلاعات
- اطمینان از سلامت و عملکرد صحیح سیستم مدیریت امنیت اطلاعات

SMART

شاخص اثر بخشی

شاخص کمی به منظور کنترل اثر بخشی فرآیند ها می باشد.

پایش

عبارت است از نظارت بر نحوه تحقق فرآیند مبتنی بر هدف وجودی آن که بر مبنای معیارهای تعریف شده صورت می پذیرد.

فعالیت های اجرایی

یک سیستم مدیریت امنیت اطلاعات باید به اثر بخش بودن سیستم پیاده سازی شده اطمینان داشته باشد و آن را تحت کنترل داشته باشد

این رویه به منظور حفظ روند حرکتی سازمان در راستای تحقق اهداف کلان و پایش شاخص های پیش بینی شده تعیین گردیده است .

پایش عبارتست از نظارت بر نحوه تحقق فرآیند مبتنی بر هدف وجودی آن و بر مبنای معیارهای تعریف شده صورت می پذیرد .

مدیر امنیت اطلاعات در دوره های زمانی مشخص، شاخص های تعیین شده را مورد پایش و اندازه گیری قرار می دهد

مسئولیت نظارت و پیگیری اجرای برنامه های بهبود بر عهده کار گروه ممیزی می باشد .

مدیر امنیت اطلاعات شاخص های شناسایی شده را درون لیست شاخص های اثربخشی وارد نموده و مقدار مطلوب شاخص را تعیین می نماید .

اهداف کلان سازمان توسط مدیر امنیت اطلاعات و اعضای شورای راهبردی به اهداف خرد تر که قابل پایش و اندازه گیری هستند تبدیل میکند و متناسب با آن اهداف، شاخص هایی را شناسایی می نماید .

تدوین روش اجرایی ممیزی داخلی

Internal Audit

هدف

❖هدف از تدوین و پیاده سازی این روش اجرایی:

- بررسی عملکرد و اثر بخشی سیستم مدیریت امنیت اطلاعات به منظور بهبود آن در شرکت یا سازمان
- آگاهی از میزان تطابق سیستم پیاده سازی شده با الزامات امنیت اطلاعات استاندارد بین‌المللی ISO27001:2013.

تعاریف

سوابق سیستم مدیریت امنیت اطلاعات

مدارکی که در آن نتایج به دست آمده ذکر می شود یا شواهدی را دال بر انجام فعالیت ها فراهم می آورد.

ممیزی موردی

ممیزی موردی ممیزی است که از یک یا چند حوزه از استاندارد بر حسب نیاز به عمل می آید.

ممیزی عادی

ممیزی است که به منظور حصول اطمینان از عملکرد صحیح و کافی سیستم مدیریتی امنیت اطلاعات در دوره های مشخص صورت می گیرد.

عدم انطباق ماژور

برآورده نشدن یک الزام و یا خواسته اصلی استاندارد مطابق با الزامات

عدم انطباق مینور

برآورده نشدن بخشی از الزامات استاندار یا روش های اجرایی تعریف شده

نقاط قابل بهبود

مدارکی که در آن نتایج به دست آمده ذکر می شود یا شواهدی را دال بر انجام فعالیت ها فراهم می آورد.

فعالیت های اجرایی

- تهیه و تنظیم برنامه زمان بندی
- ممیزی موردی با درخواست مدیریت امنیت اطلاعات یا در شرایط حساس

- انتخاب تیم ممیزی با مدیر امنیت اطلاعات
- تیم ممیزی شامل دو بخش فنی و سیستمی
- سر ممیز و تیم ممیزی را می بایست از بین افراد آموزش دیده و صاحب صلاحیت انتخاب نمایند.

- ارائه زمان بندی دقیق اجرای ممیزی
- معرفی تیم ممیزی در حوزه ها و بخش های مختلف

- معرفی تیم ممیزی
- تشریح برنامه ممیزی و زمان بندی حضور در واحد ها و آمادگی ها آن ها
- تشریح اهداف و اهمیت ممیزی

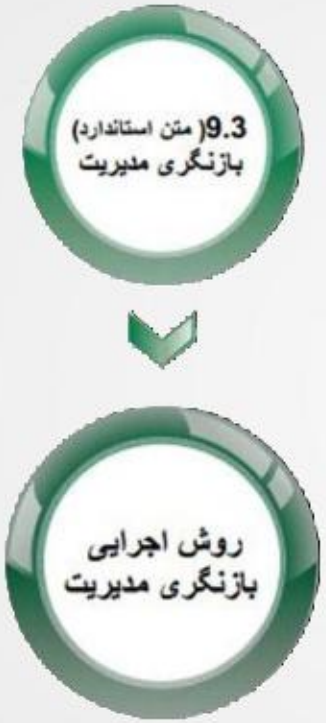
- ارائه گزارش ممیزی در قالب فرم گزارش مغایرت های ممیزی داخلی سیستم مدیریت امنیت اطلاعات توسط سر ممیز

- تعریف اقدام اصلاحی و پیشگیرانه جهت رفع مغایرت ها

تدوین روش اجرایی بازنگری مدیریت

Management Review

هدف



❖**هدف از تدوین و پیاده سازی این روش اجرایی:**

- حصول اطمینان از کارکرد موثر سیستم مدیریت امنیت اطلاعات؛
- ایجاد بهبود مستمر و ارتقاء اثر بخشی سیستم مدیریت امنیت اطلاعات؛
- برگزاری جلسات بازنگری مدیریت جهت اصلاح و پشتیبانی از سیستم مدیریت امنیت اطلاعات.

فعالیت های اجرایی

ورودی

- آمار حوادث و نتایج ممیزی های داخلی و خارجی ISMS
- بازنگری های ISMS و نتایج اقدامات مصوبات جلسات قبلی

- وضعیت اقدامات اصلاحی و پیشگیرانه انجام یافته در مدت فاصله بین دو بازنگری
- گزارش های وضعیت اضطراری

- گزارش ها، تصمیمات و یا صورت جلسات کارگروه اجرایی
- گزارش های درخواستی مدیریت از عملکرد کلی سیستم
- گزارش های فرآیند مدیریت ریسک

خروجی

- ارتقاء اثر بخشی ISMS در سازمان
- بروز رسانی و تجدید نظر در برنامه ارزیابی و مقابله با ریسک

- تامین و تصویب منابع مورد نیاز
- بهبود چگونگی ارزیابی اثر بخشی کنترل ها و اصلاح رویه هایی که امنیت اطلاعات را تحت تاثیر قرار می دهند

- پاسخگویی به رخدادهای داخلی و خارجی که ممکن است بر روی سیستم مدیریت امنیت اطلاعات تاثیر بگذارد.

- عدم انطباق و اقدام اصلاحی
- بهبود مستمر

مجموعه کنترل‌های استاندارد

ISO27001:2013

❖ A.5.1: خط مشی های امنیت اطلاعات

- هدف کنترل: فراهم نمودن هدایت و حمایت مدیریت از امنیت اطلاعات مطابق با نیازمندی‌های کسب و کار و قوانین و مقررات مرتبط.

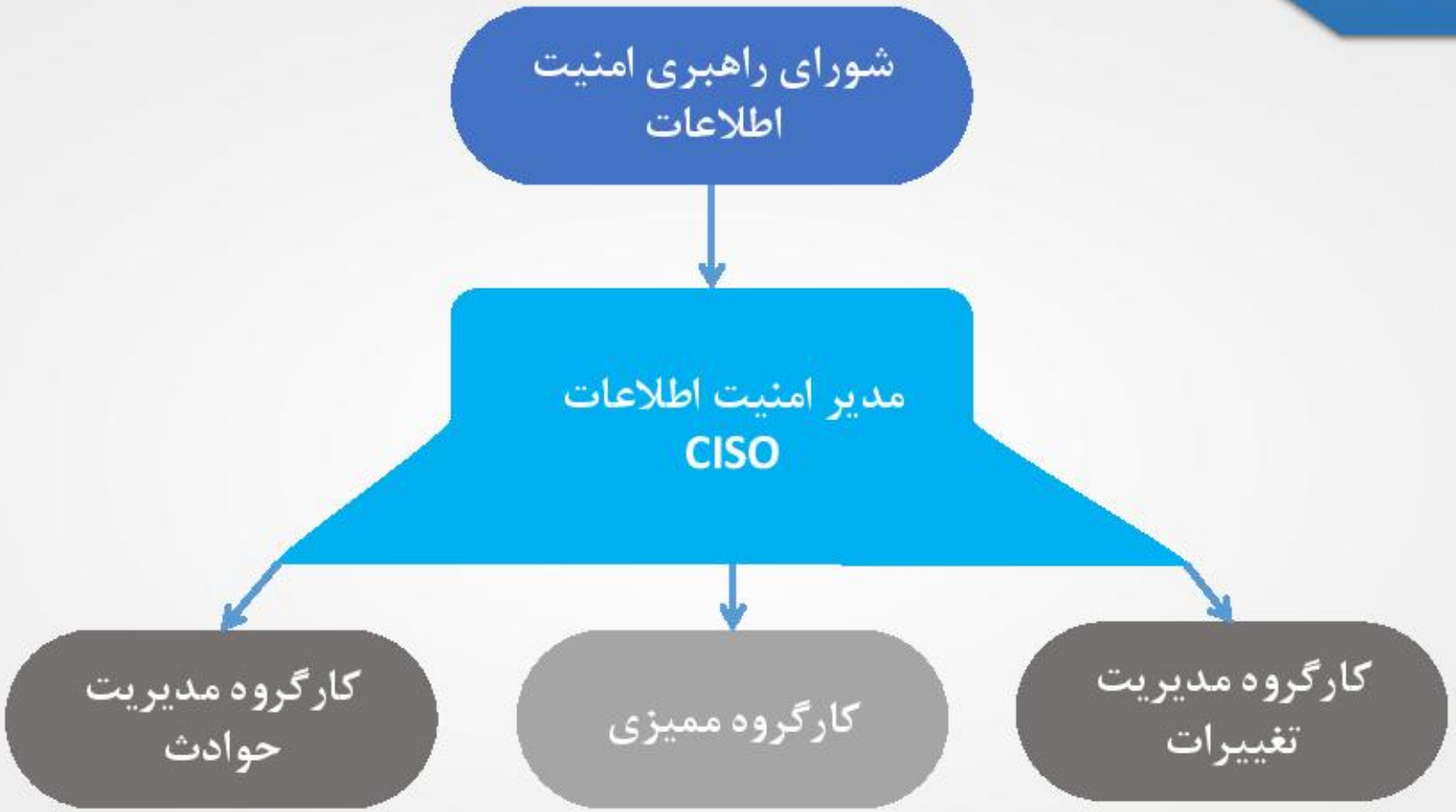
❖A.6.1: سازمان داخلی

- هدف کنترل: ایجاد یک چارچوب مدیریتی برای شروع و کنترل پیاده سازی و عملیاتش امنیت اطلاعات در درون سازمان.

❖A.6.2: تجهیزات سیار و کار از راه دور

- هدف کنترل: حصول اطمینان از امنیت کار از راه دور و استفاده از تجهیزات سیار

ساختار سازمانی امنیت



❖ A.7.1: قبل از استخدام

- هدف کنترل: برای اطمینان از اینکه کارمندان و پیمانکاران از مسئولیت‌های خود آگاه بوده، شایستهٔ نقش های محول شده به آنان باشند.

❖ A.7.2: حین خدمت

- هدف کنترل: اطمینان از اینکه تمامی کارمندان و پیمانکاران از مسئولیت‌های خود در قبال امنیت اطلاعات آگاهی دارند و آنها را انجام می دهند.

❖ A.7.3: خاتمه یا تغییر در استخدام

- هدف کنترل: حفظ منافع سازمان، به عنوان بخشی از فرآیند خاتمه یا تغییر کار.

تدوین روش اجرایی امنیت منابع انسانی

Human Resource Management

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- حفاظت از محرمانگی، صحت و در دسترس بودن اطلاعات در شرکت یا سازمان قبل از استخدام، در حین استخدام و خاتمه یا تغییر در استخدام، با استفاده از تفاهم نامه عدم افشاء اطلاعات
- اطمینان از نحوه تغییر یا خاتمه کار کارمندان طبق ضوابط مشخص سازمانی
- حصول اطمینان از آگاهی افراد از مسئولیت های خود و خط مشی های امنیتی
- کاهش ریسکهای ناشی از خطای انسانی و استفاده نادرست از امکانات

کنترل های مربوط به این روش اجرایی

فعالیت های اجرایی

پیش از استخدام

- تعریف نقش ها و مسئولیت های امنیتی فرد
- بررسی پیشینه داوطلبین استخدام
- امضاء تفاهم نامه عدم افشاء اطلاعات

حین استخدام

- مسئولیت های مدیریت جهت آگاهی رسانی خط مشی ها و سیاست های امنیتی به پرسنل
- آگاهی رسانی، تربیت و آموزش امنیت اطلاعات به پرسنل
- اعمال فرآیند های انضباطی در صورت تخلف

خاتمه استخدام

- اعلام خاتمه استخدام از طریق فرم تسویه حساب به واحد فناوری اطلاعات
- امضاء فرم تسویه حساب توسط واحد فناوری اطلاعات بعد از قطع دسترسی ها

❖ A.8.1: مسئولیت دارایی‌ها

- هدف کنترل: شناسایی دارایی های سازمانی و تعریف مسئولیت های مناسبی برای حفاظت از آنها.

❖ A.8.2: طبقه‌بندی اطلاعات

- هدف کنترل: اطمینان از اینکه دارایی‌های اطلاعاتی، با توجه به اهمیتشان برای سازمان، از سطح امنیت مناسبی برخوردارند.

❖ A.8.3: اداره رسانه ها

- هدف کنترل: جلوگیری از افشای عمدی، تغییر، انتقال غیرمجاز یا صدمه به اطلاعات ذخیره شده در رسانه ها..

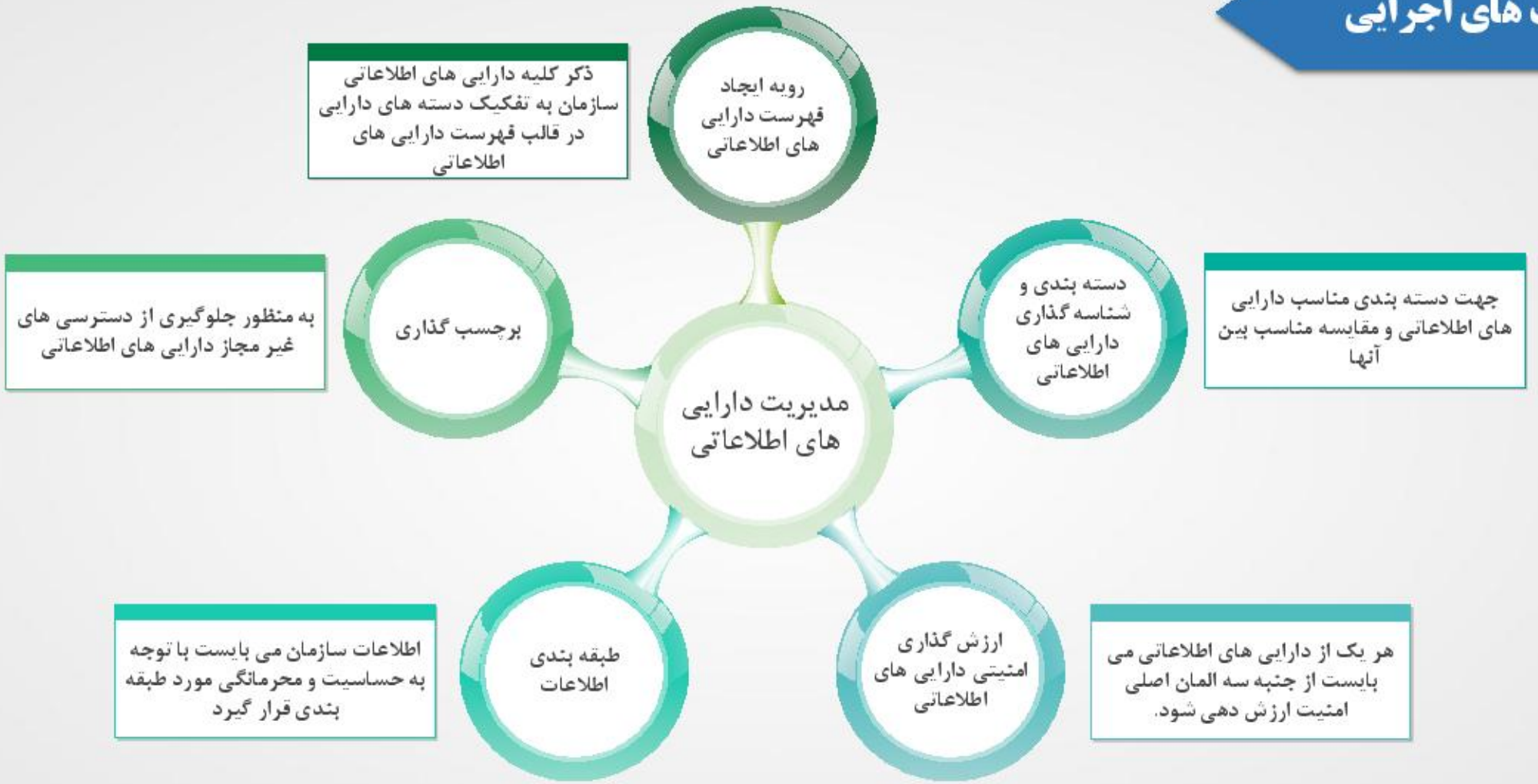
تدوین روش مدیریت دارایی‌های اطلاعاتی

Information Asset Management

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- شناسایی صحیح دارایی های اطلاعاتی
- لیست کردن دارایی ها
- طبقه بندی صحیح آنها
- تدوین قوانین قابل قبول از دارایی های اطلاعاتی

فعالیت های اجرایی



- دسترسی به اطلاعات محرمانه سازمان برای افراد غیر مجاز ممنوع می باشد

- حریم اطلاعات و فضاهای محرمانه را با استفاده از نشانه گذاری مناسب مشخص نمایید.

تدوین روش اجرایی کاربری مجاز

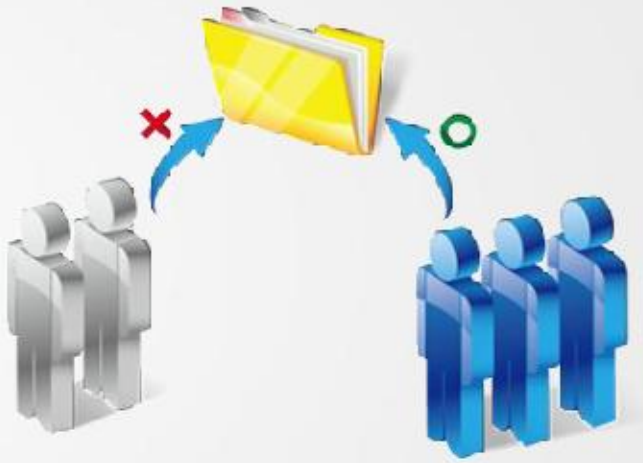
Acceptable Usage Policy-AUP

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- آگاهی رسانی به راهبران و کاربران در خصوص نکات امنیتی استفاده از رایانه‌های شخصی و تمامی سیستم ها و تجهیزات مورد استفاده توسط آنها؛
- ایجاد راهکارهایی برای کاهش ریسک‌های موجود در شرکت یا سازمان

- نام کاربری و رمز عبور شما جزء اطلاعات هویتی و محرمانه شما می باشد. از آنها به خوبی محافظت نمایید و در اختیار دیگران قرار ندهید.

A9: کنترل دسترسی



- **A.9.1: الزامات کسب و کار در کنترل دسترسی**
  - هدف کنترل: محدودکردن دسترسی به اطلاعات و امکانات پردازش اطلاعات.
- **A.9.2: مدیریت دسترسی کاربر**
  - هدف کنترل: اطمینان از اینکه حقوق دسترسی به کاربر مجاز داده می‌شود و از دسترسی غیرمجاز به سرویس ها و سیستم‌ها جلوگیری می‌گردد.
- **A.9.3: مسئولیت‌های کاربر**
  - هدف کنترل: مسئول نمودن کاربران برای نگهداری امن از اطلاعات تصدیق اصالت خود.

تدوین روش اجرایی کنترل دسترسی

Access Control

هدف

❖ **تعریف فرآیند کنترل دسترسی مطابق با استاندارد ISO27001:2013 به منظور :**

- مدیریت اطلاعات
- مدیریت سیستم های اطلاعاتی
- مدیریت کاربران سیستم های اطلاعاتی و تعیین حقوق دسترسی ها
- جلوگیری از دسترسی غیر مجاز به اطلاعات و سیستم های اطلاعاتی

کنترل های مربوط به این روش اجرایی

فعالیت های اجرایی

ایجاد، حذف و تغییر دسترسی کاربر

- ارسال درخواست
- تائید درخواست توسط مدیر مربوطه
- ارسال از مدیر مربوطه به واحد فناوری اطلاعات
- بررسی و احراز هویت کاربر مطابق با لیست مشاغل
- ارسال برای راهبر مربوطه
- امضاء تعهد نامه استفاده از خدمات شبکه و اینترنت

بازنگری دسترسی ها و حقوق دسترسی اعطاء شده به کاربر

- بررسی لیست کاربران، دسترسی ها و حقوق دسترسی اعطاء شده در بازه های زمانی مشخص توسط مالک سیستم

نرم افزارهای مجاز جهت دسترسی کاربران

- تکمیل فرم نرم افزارهای مجاز
- تکمیل فرم ذکر شده به صورت جداگانه برای هر واحد

دسترسی از راه دور

- دسترسی برای موارد خاص و با تائید مالک سیستم
- ارائه دسترسی برای زمان موقت و مشخص

تدوین روش اجرایی کلمه عبور

Password

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- به وجود آوردن روالی منظم و شفاف جهت ایجاد، تعریف و تغییر کلمه عبور سیستم ها، سرویس ها و تجهیزات به منظور ارتقاء سطح امنیت اطلاعات؛
- ارائه راهنمایی هایی برای کاربران جهت تعریف و محافظت از کلمات عبور.

فعالیت های اجرایی

مدیریت کلمه عبور

- تصدیق هویت کاربران برای دسترسی به سیستم های اطلاعاتی شامل سیستم ها، سرویس ها و تجهیزات:
- کلمه عبور می بایست جهت حفظ محرمانگی، مدیریت و کنترل شود:

تخصیص کلمه عبور به کاربر

- سیاست های کلمه عبور کاربران
- سیاست های کلمه عبور راهبران

(حداقل تعداد کاراکتر، زمان تعویض کلمه عبور، پیچیدگی، تعداد کلمات عبور قبلی که نباید انتخاب شود، تعداد دفعات مجاز ورود نادرست و مدت زمان عدم استفاده از سیستم در صورت قفل شدن می‌بایست در موارد فوق رعایت شود.)

نگهداشت کلمه عبور

- کلمه عبور در مرتبه اول ورود به سیستم می بایست توسط کاربر تغییر کند.
- نگهداری کلمه عبور به صورت فیزیکی در شرکت مجاز نمی باشد.
- در صورت فراموشی کلمه عبور درخواست تغییر کلمه عبور به واحد مربوطه اعلام شود.

پیچیدگی کلمه عبور

استفاده هم زمان از حروف کوچک، حروف بزرگ، اعداد و کاراکتر ها در انتخاب کلمه عبور به منظور ایجاد یک کلمه عبور مناسب.

- **A.10.1: کنترل‌های رمزنگاری**
  - هدف کنترل: اطمینان از استفاده مناسب و موثر از رمزنگاری برای محافظت از محرمانگی، صحت، و یا یکپارچگی اطلاعات.

A.11.1: حوزه‌های امن

- هدف کنترل: جلوگیری از دسترسی فیزیکی غیرمجاز، آسیب رساندن و اخلال در اطلاعات سازمان و تجهیزات پردازش اطلاعات.

A.11.2: تجهیزات

- هدف کنترل: جلوگیری از گم شدن، خسارت، سرقت یا تحت تأثیر قرار گرفتن دارایی‌ها و وقفه در عملکرد سازمان.

تدوین روش اجرایی امنیت فیزیکی و محیطی

Physical and Environmental Security

ورود و خروج هرگونه رایانه و رسانه قابل حمل (USB Flash، CD/DVD و...) به سازمان **ممنوع** می‌باشد.

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- تهیه راهنمایی جهت حفظ امنیت فیزیکی اتاق های امن نظیر سرور و ساختمان ها؛
- کنترل ورود و خروج به شرکت/ سازمان
- تهیه رویه ای به منظور اجتناب از دسترسی افراد غیر مجاز جهت محافظت از در دسترس بودن و محرمانگی اطلاعات.

کنترل های مربوط به این روش اجرایی

فعالیت های اجرایی

کنترل فیزیکی ورود و خروج

- ورود و خروج به سازمان
- ورود و خروج به اتاق سرور

خروج تجهیزات سخت افزاری

- جهت خروج تجهیزات به منظور تعمیرات و یا غیره می بایست توسط مدیر امنیت تائید شود.

دفاتر، اتاق ها و محل های امن

- استفاده از سامانه مانیتورینگ
- استفاده از دوربین
- امنیت فیزیکی اسناد فیزیکی(استفاده از گاو صندوق، قفل کردن درب های اتاق و غیره)

تجهیزات خارج از شرکت

- می بایست بازدید دوره‌ای از تجهیزات خارج از سازمان انجام شود.

تدوین روش اجرایی امحاء دارایی های اطلاعاتی

Information Asset Disposal

- اسناد و اطلاعات محرمانه خود را قبل از دورریختن به صورت کامل امحاء کنید تا توسط افراد خرابکار قابل بازیابی نباشند.

- **هدف از تدوین و پیاده سازی این روش اجرایی:**
  - جلوگیری از فاش شدن اطلاعات محرمانه شرکت یا سازمان از طریق دور انداختن بدون مراقبت تجهیزات و یا ارسال آنها برای تعمیرات؛
  - پایان یافتن زمان نگهداری مستندات دارایی ها، با استفاده از روش های امن که شرکت یا سازمان تائید کرده است.

کنترل های مربوط به این روش اجرایی

فعالیت های اجرایی

A.12: امنیت عملیات

A.12.1: مسئولیت‌ها و روش‌های اجرایی عملیات

- هدف کنترل: برای اطمینان از صحت و امنیت عملیات تجهیزات پردازش اطلاعات.

A.12.2: محافظت در برابر بد افزارها

- هدف کنترل: اطمینان از اینکه اطلاعات و تجهیزات پردازش اطلاعات در برابر بد افزارها محافظت شده‌اند.

تدوین روش اجرایی مدیریت رسانه ها و تجهیزات سیار

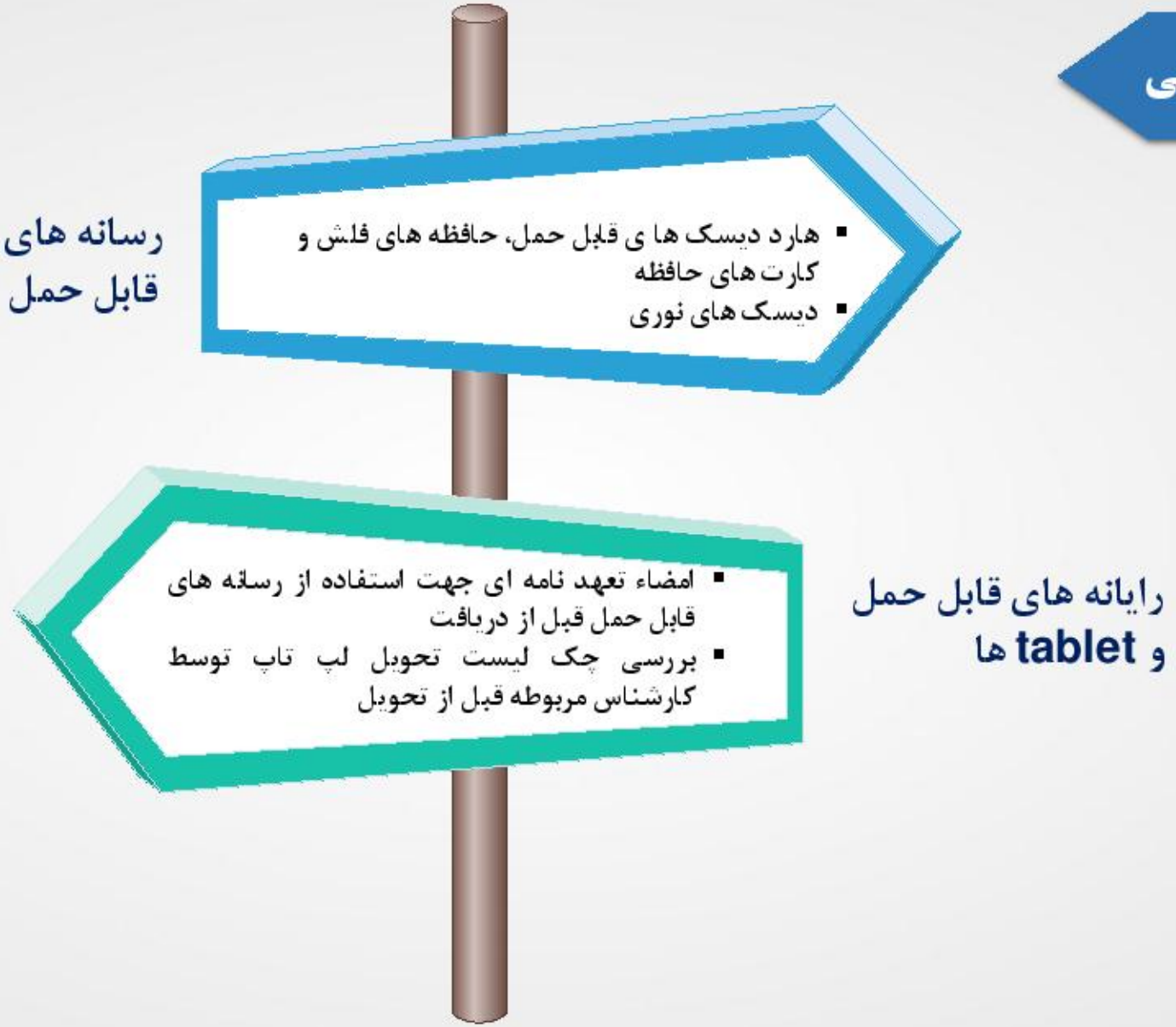
Media Handling

- همـواره رسـانه‌های خـود را (CD/DVD، USB، FLASH و...) در محلـی امـن و دور از دسـترس افراد غیرمجاز نگهداری نمایید.

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- پیشگیری از سرقت و سوء استفاده و یا از بین بردن اطلاعات محرمانه و حیاتی شرکت یا سازمان؛
- تضمین صحت اطلاعات موجود در واحدهایی که در آن ها از رسانه ها و تجهیزات قابل حمل استفاده می شود.

فعالیت های اجرایی



- **A.12.3: نسخه پشتیبان**

  هدف کنترل: محافظت در برابر از بین رفتن اطلاعات

- **A.12.4: ثبت وقایع و پایش گری**

  هدف کنترل: ثبت وقایع و تولید شواهد و مدارک

- **A.12.5: کنترل عملکرد نرم‌افزار**

  هدف کنترل: اطمینان از یکپارچگی سیستم‌های عملیاتی

تدوین روش اجرایی نسخه پشتیبان

Backup

- همیشه از اطلاعات مهم خود نسخه پشتیبان تهیه نمایید.

هدف

- **هدف از تدوین و پیاده سازی این روش اجرایی، حفاظت از اطلاعات حیاتی به منظور:**
  - اطمینان از در دسترس بودن اطلاعات حساس؛
  - اطمینان از استمرار کسب و کار شرکت یا سازمان؛
  - کاهش زمان و هزینه ای که صرف جمع آوری اطلاعات شده؛
  - اهمیت و ارزش بسیار بالای اطلاعات جمع آوری شده؛
  - اطمینان از اینکه یک نسخه دیگر از اطلاعات در سازمان موجود است.

دلیل اهمیت تهیه نسخه پشتیبان

اطمینان از عدم به خطر
افتادن کسب و کار سازمان

افزایش رو به رشد
ریسکها و بدافزار ها

فعالیت های اجرایی

تدوین روش اجرایی مدیریت ثبت وقایع

Log and Monitoring

هدف

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- ثبت رویدادها و فعالیت های کاربران و راهبران در سامانه های اطلاعاتی، سرویس دهنده ها و تجهیزات شبکه
- رعایت اصل عدم انکار و پاسخگویی سریع و مناسب به رخدادها و رویدادهای امنیتی در شرکت یا سازمان

فرآیند ثبت لاگ

ثبت لاگ ها:
ثبت لاگ های نرم افزارها، ابزارها و سیستم های مختلف بر روی یک لاگ سرور متمرکز

ثبت لاگ های فعالیت های راهبران سیستم های کاربردی و شبکه:
بررسی کلیه عملکرد راهبران و یا تمامی افرادی که دسترسی سطوح بالا دارند توسط مدیر امنیت اطلاعات در بازه های زمانی مشخص

پیگیری لاگ ها:
در صورت مشاهده هر گونه سوء استفاده مانند استفاده از حریم شخصی کاربران، ایجاد مزاحمت، استفاده از اطلاعات محرمانه سازمان برای مقاصد شخصی و غیره

نظارت بر استفاده از سیستم:
نظارت بر عملکرد کاربران در سیستم های حیاتی سازمان جهت پیگیری حوادث و موارد رخدادهای امنیتی

هم زمان سازی ساعت سیستم ها:
کلیه دارایی های اطلاعاتی سخت افزاری واقع در سازمان اعم از سرویس دهنده ها ،برنامه های کاربردی، تجهیزات فعال شبکه، دیواره های آتش، دوربین ها، سیستم های کنترل دسترسی اتاق سرور می بایست ساعت خود را با NTP سرور هم زمان سازند.

- **A.12.6: مدیریت آسیب‌پذیری فنی**

  هدف کنترل: جلوگیری از بهره‌برداری از آسیب‌های فنی.

- **A.12.7: ملاحظات بازرسی سیستم‌های اطلاعاتی**

  هدف کنترل: اطمینان از یکپارچگی سیستم‌های عملیاتی

- **A.13.1: مدیریت امنیت شبکه**

هدف کنترل: اطمینان از محافظت اطلاعات در شبکه و تجهیزات پشتیبانی پردازش اطلاعات.

- **A.13.2: انتقال اطلاعات**

هدف کنترل: برای حفظ امنیت اطلاعات منتقل شده در سازمان با هر نهاد خارجی دیگر.

تدوین روش اجرایی تبادل اطلاعات

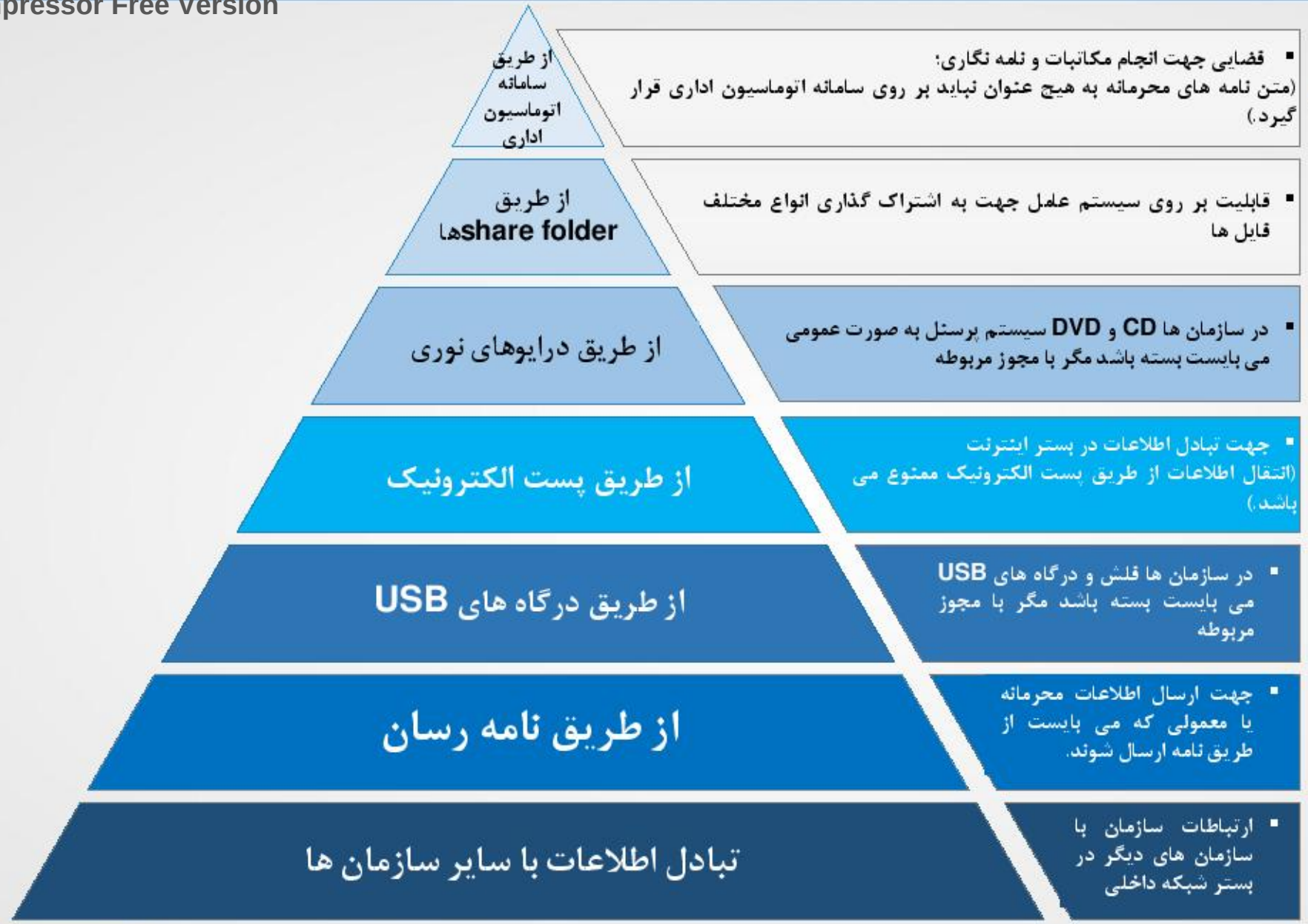
Information Transfer

هدف

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- حفاظت از امنیت اطلاعات در تبادل اطلاعات از طرق مختلف امکانات ارتباطی، حفاظت از اطلاعات مرتبط با ارتباطات داخلی سیستم های اطلاعاتی

فعالیت های اجرایی



A.14.1: الزامات امنیتی اطلاعات سیستم‌ها

هدف کنترل: اطمینان از اینکه امنیت اطلاعات، بخش جدایی ناپذیر سیستم‌های اطلاعاتی در سراسر چرخه عمرشان می‌باشد. همچنین شامل الزاماتی برای سیستم‌های اطلاعاتی می‌باشد که سرویس‌هایی برای شبکه‌های عمومی ارائه می‌کنند

A.14.2: امنیت در تولید و فرآیندهای پشتیبانی

هدف کنترل: اطمینان از اینکه امنیت اطلاعات در چرخه عمر تولید سیستم‌های اطلاعاتی طراحی و اجرا شده است.

◆ A.14.3: داده‌های تستی

هدف کنترل: اطمینان از محافظت داده مورد استفاده برای آزمایش کردن

تدوین روش اجرایی امنیت برنامه های کاربردی

Application Security

❖ حصول اطمینان از امنیت برنامه های کاربردی؛

- رعایت ملاحظات امنیتی حین تولید، خرید، ارتقاء و برون سپاری برنامه های کاربردی.

فعالیت های اجرایی

تولید برنامه های کاربردی

- اعلام نیاز برنامه کاربردی
- تحلیل نیاز تولید برنامه کاربردی
- بررسی امنیتی جهت تائید تولید برنامه کاربردی

خرید برنامه های کاربردی

- پیروی از استانداردها (مانند نماتن)
- بررسی قابلیت های برنامه کاربردی مطابق با موارد ذکر شده در فرم تحلیل نیاز تولید

نصب و ارتقاء برنامه های کاربردی

- نصب: بررسی با توجه به نرم افزارهای مجاز تائید شده
- ارتقاء: به روز رسانی برنامه کاربردی با توجه به وصله های امنیتی

◆ A.15.1: امنیت اطلاعات در ارتباطات تامین کنندگان

هدف کنترل: برای اطمینان از محافظت از دارایی های سازمان که بوسیله تامین کنندگان قابل دسترسی است.

◆ A.15.2: مدیریت ارائه خدمات تامین کنندگان

هدف کنترل:به منظور نگهداری سطح توافق شده امنیت اطلاعات و ارایه سرویس های بر خط با توافق تامین کنندگان.

تدوین روش اجرایی امنیت شخص ثالث

Third party Security

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- کاهش ریسک ناشی از تهدیدات مرتبط با شخص ثالث نظیر افشاء اطلاعات و دسترسی و استفاده غیر مجاز از اطلاعات تدوین شده؛
- ارائه چارچوبی برای ارتباط با کلیه پیمانکاران، مشاوران، مشتریان و یا هر سازمان یا شخص دیگری که نیاز به دسترسی به منابع اطلاعات این شرکت یا سازمان را دارد.

کنترل های مربوط به این روش اجرایی

فعالیت های اجرایی

- امضاء قرارداد
- نظارت بر اجرای خدمات
- کنترل دسترسی شخص ثالث
- مدیریت تغییرات در شرح خدمات شخص ثالث

- کارفرما (واحد در ارتباط با شخص ثالث) می بایست در هنگام تهیه درخواست ارائه پیشنهاد ریسک های ناشی از سپردن فعالیت ها به اشخاص یا سازمان های دیگر را در نظر بگیرد.
- اعطای دسترسی ها به سرورها، سرویس ها و یا پایگاه های داده مطابق با روش اجرایی کنترل دسترسی به درخواست دسترسی برای شخص ثالث
- مسئولیت انطباق شرح خدمات، فعالیت ها و توافق نامه ارائه خدمات توسط شخص ثالث بر عهده کارفرما یا نماینده قانونی
- کلیه تغییرات مرتبط با فناوری اطلاعات که توسط شخص ثالث انجام می گردد و یا هرگونه تغییر در سطوح دسترسی اشخاص ثالث می بایست مطابق با روش اجرایی مدیریت تغییرات باشد

A.16: مدیریت رخدادهای امنیت اطلاعات

◆ A.16.1: مدیریت رخدادهای امنیت اطلاعات

هدف کنترل: برای اطمینان از نا متناقض بودن و موثر بودن اهداف به منظور مدیریت نمودن حوادث امنیت اطلاعات، شامل ارتباط با رخدادهای امنیتی و ضعف های امنیتی.

هدف

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- اطمینان از شناسایی به موقع، گزارش، مستند سازی و انجام اقدامات لازم حین وقوع رخدادهای امنیتی در جهت کاهش اثرات و تکرار این وقایع و رخدادها در شرکت یا سازمان می‌باشد.

تدوین روش اجرایی پشتیبانی رخدادهای امنیتی

Incident Handling

فعالیت های اجرایی

رویداد امنیتی

- ✓ اعلام رویداد از طریق تلفن های مربوطه یا از طریق Help desk
- ✓ ارائه گزارش ماهانه از خرابی سیستم ها توسط مسئول Help desk

آسیب پذیری های امنیتی

- ✓ اعلام آسیب پذیری هایی که منجر به بروز رخداد امنیتی از طریق فرم گزارش آسیب پذیری امنیت اطلاعات توسط کارمندان، پیمانکار و کاربران شخص ثالث

رخدادهای امنیتی

- ✓ اطلاعات مربوط به تجهیزات در ارتباط با رخداد امنیتی
- ✓ اطلاعات مربوط به رخدادهای امنیتی
- ✓ اقدامات اصلاحی

A.17: جنبه های مدیریت تداوم کسب و کار امنیت اطلاعات

- **A.17.1: تداوم امنیت اطلاعات**

هدف کنترل: تداوم امنیت اطلاعات باید در سیستم مدیریت تداوم کسب و کار جای گیرد.

- **Redundancies :A.17.2**

هدف کنترل: به منظور اطمینان از در دسترس بودن تجهیزات پردازش اطلاعات.

تدوین روش اجرایی مدیریت تداوم کسب و کار

Business Continuity Management

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- حصول اطمینان از استمرار فرآیند ها و فعالیت های مرتبط با فناوری اطلاعات
- بیان نیازمندی های امنیتی استمرار کسب و کار در شرکت یا سازمان
- عملکرد بدون وقفه هر گونه واقعه برنامه ریزی نشده و ناخواسته

تعاریف

استمرار کسب و کار

توانایی استراتژیک و تاکتیکی سازمان برای برنامه ریزی و ارائه پاسخ مناسب در مواجهه با حوادث و انقطاع کسب و کار.

طرح استمرار کسب و کارBCP

مجموعه ای مکتوب از دستورالعمل ها و اطلاعات که برای استفاده سازمان در یک حادثه بکار گرفته می شود.

زمان بازیابی هدفRTO

مدت زمان تعیین شده برای از سرگیری تولید محصول و یا ارائه خدمت پس از یک حادثه.

فعالیت های اجرایی

۱ تهیه لیست فرآیند های فناوری اطلاعات (مانند مشخص کردن RTO، سطح و میزان شدت پیامد هر یک از تهدیدات و غیره)

۲ انجام تحلیل اثرات کسب و کار (**BIA**) و مشخص کردن استراتژی مقابله با هر یک از تهدیدات

۳ مشخص کردن فهرست تماس با مخاطبین طرح تداوم کسب و کار و نصب آن در نقاط مناسب و بازنگری آن در دوره های مناسب

۴ تکمیل لیست تلفن های ضروری و بازنگری آن در بازه های زمانی مناسب

۵ برگزاری مانور جهت آزمایش و ارزیابی طرح تداوم کسب و کار

◆ A.18.1: سازگاری با قانون و نیازمندی های قراردادی

هدف کنترل: به منظور جلوگیری از نقض الزامات قانونی، حقوقی، بالا دستی و قراردادی که در ارتباط با امنیت اطلاعات و نیازمندی های امنیتی می باشند.

◆ A.18.2: بازنگری های امنیت اطلاعات

هدف کنترل: به منظور اطمینان از اینکه امنیت اطلاعات پیاده سازی شده و در راستای خط مشی ها و رویه های سازمان می باشد.

تدوین روش اجرایی سازگاری با الزامات قانونی، حقوقی و قراردادی

Compliance

هدف

❖ هدف از تدوین و پیاده سازی این روش اجرایی:

- حصول اطمینان از الزام به قوانین بالا دستی ملی و بین المللی در حوزه امنیت اطلاعات
- حصول اطمینان از الزام به قوانین در کلیه قراردادها
- حصول اطمینان از انطباق با استانداردهای کاربردپذیر

فعالیت های اجرایی

تدوین RFP سیستم مدیریت امنیت اطلاعات

- تعیین محدوده
- ارزیابی ریسک فنی
- ایمن سازی فنی
- دوره های آموزشی مورد نیاز و شرایط آن
- الزامات اخذ گواهینامه و زمان بندی آن

تعیین محدوده

- محدوده فرآیندی
  - فرآیندهای واحد فناوری اطلاعات
  - فرآیندهای مبتنی بر IT سازمان
  - کل فرآیندها
- محدوده فیزیکی
- محدوده پرسنلی
- محدوده تکنولوژیکی

ارزیابی ریسک فنی

- پویش آسیب پذیری فنی
- تست نفوذپذیری
- تست نفوذپذیری از خارج
- تست نفوذپذیری از داخل شبکه
- ارزیابی امنیتی برنامه های کاربردی
- ارتباط مابین ارزیابی ریسک و تست نفوذپذیری

- ارائه چک لیست های ایمن سازی
- ارائه چک لیست های ایمن سازی و آموزش آن به راهبران سازمان
- ارائه چک لیستها و پیاده سازی آن

- لیست دوره های آموزشی
- تعداد نفرات هر دوره
- نوع گواهینامه هر دوره
- محل برگزاری دوره

- نوع گواهینامه (ملی یا بین المللی)
- زمان در نظر گرفته شده برای اخذ گواهینامه
- پیگیری عدم انطباق های اعلام شده از سوی نهاد ممیزی کننده

پـــایـــان