بسم الله الرحمن الرحیم

ISMS

INFORMATION SECURITY MANAGEMENT SYSTEM

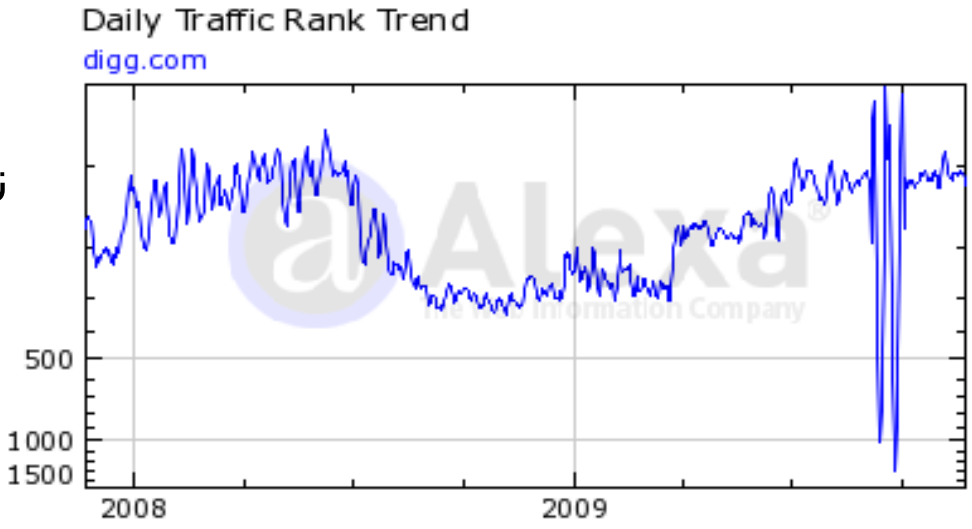
سیستم مدیریت امنیت اطلاعات

مدرس:
علیرضا حبیبی

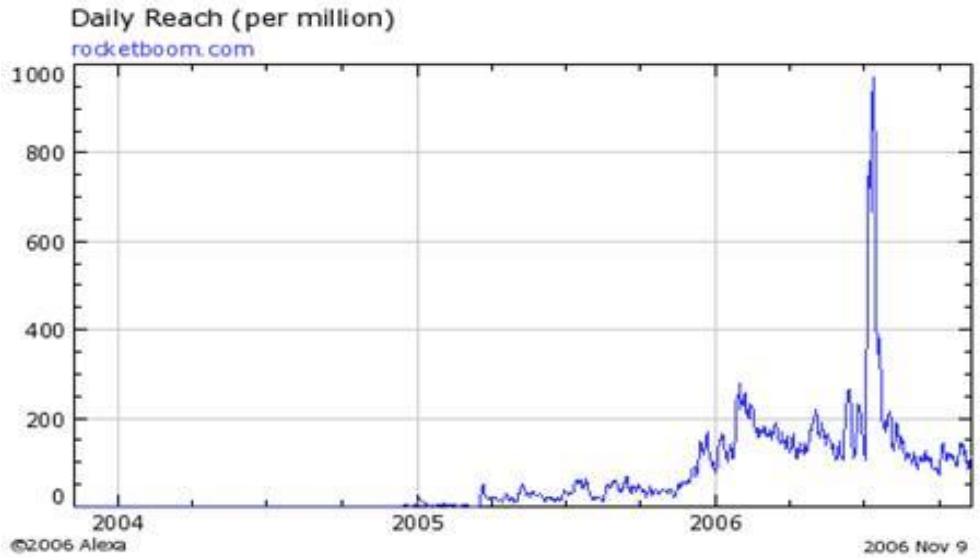
اهمیت امنیت در وب و تاثیرات آن

- سقوط ارزش سهام

- کاهش رادیکالی تعداد بازدید کنندگان

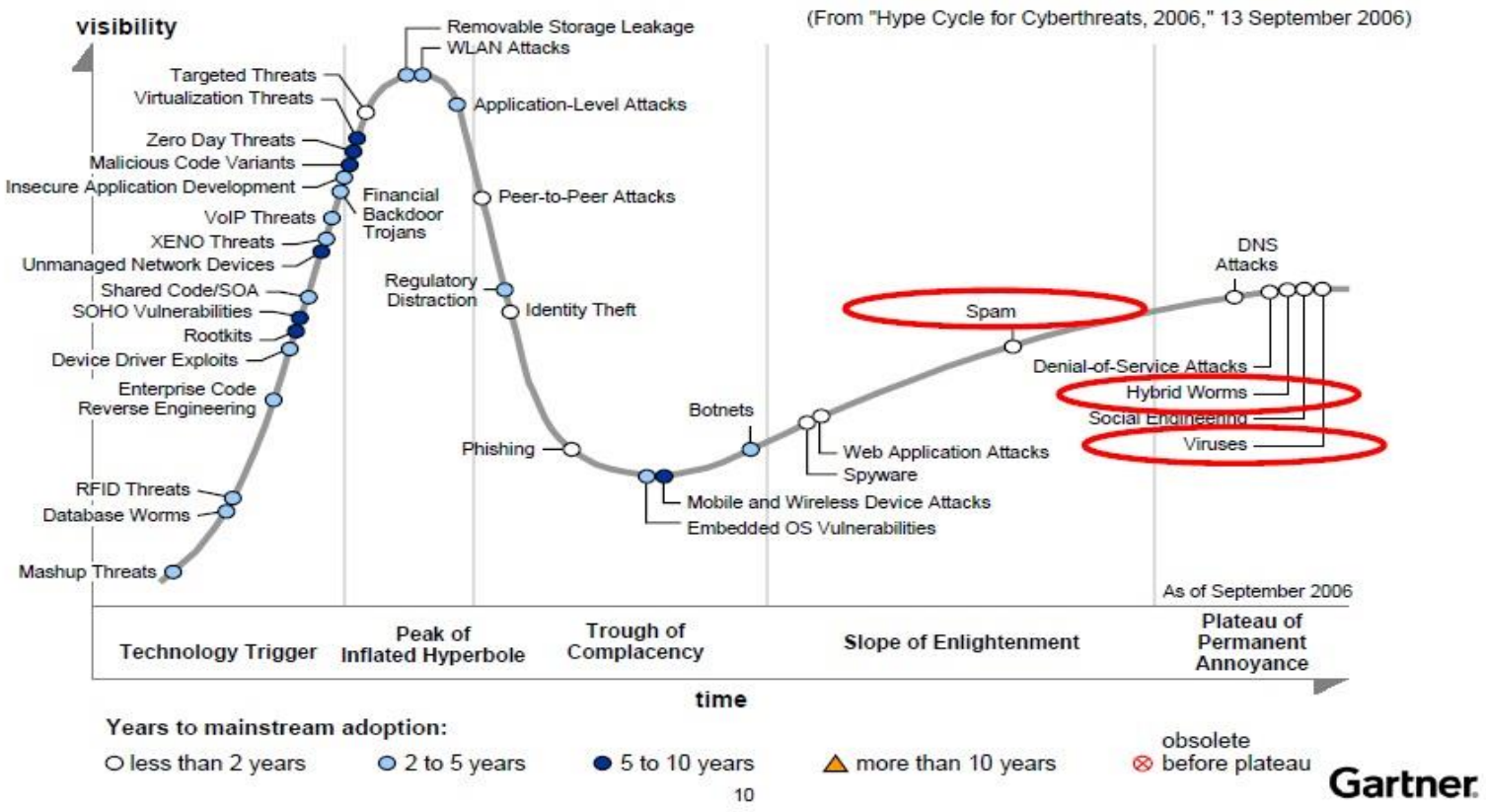


آثار حملات نفوذگران



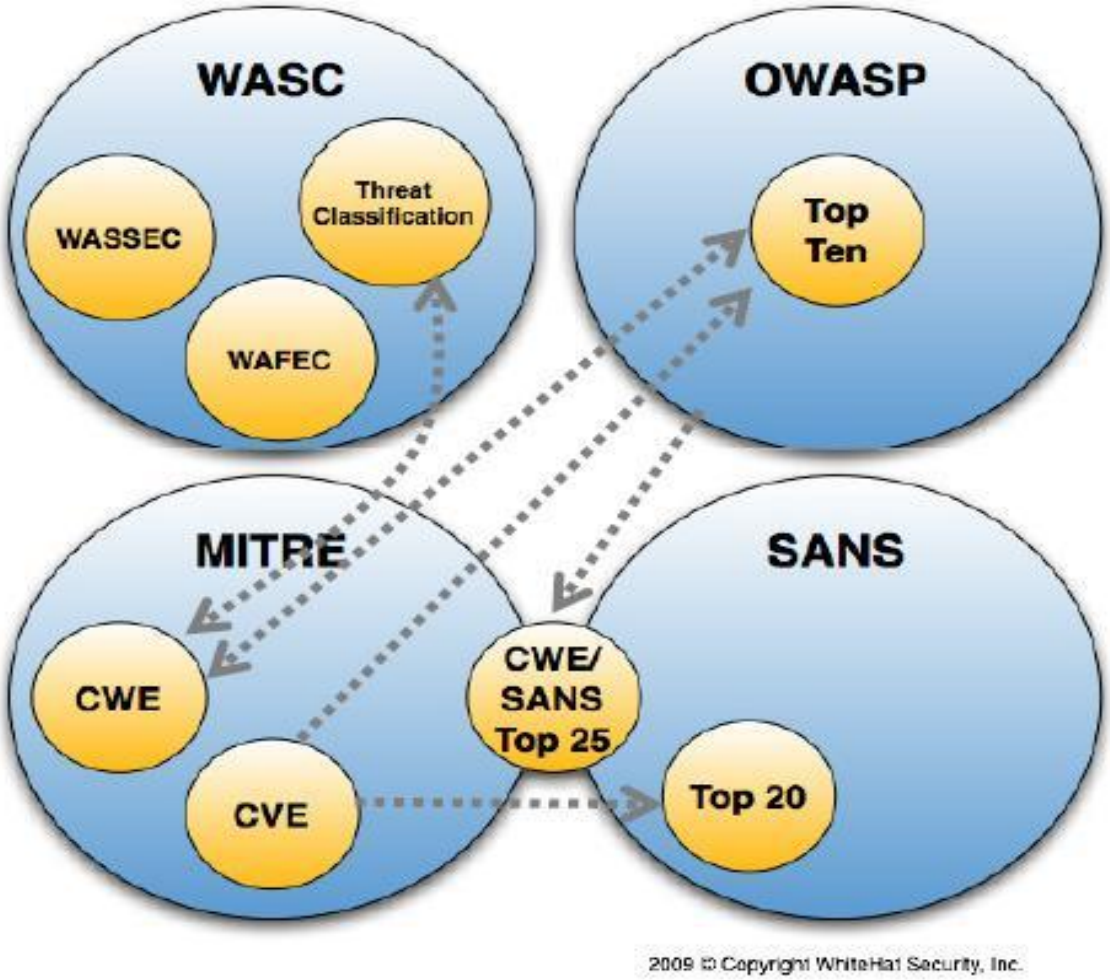
پراکندگی موضوعات امنیتی

Gartner 2006
Information Security Threats Hype Cycle



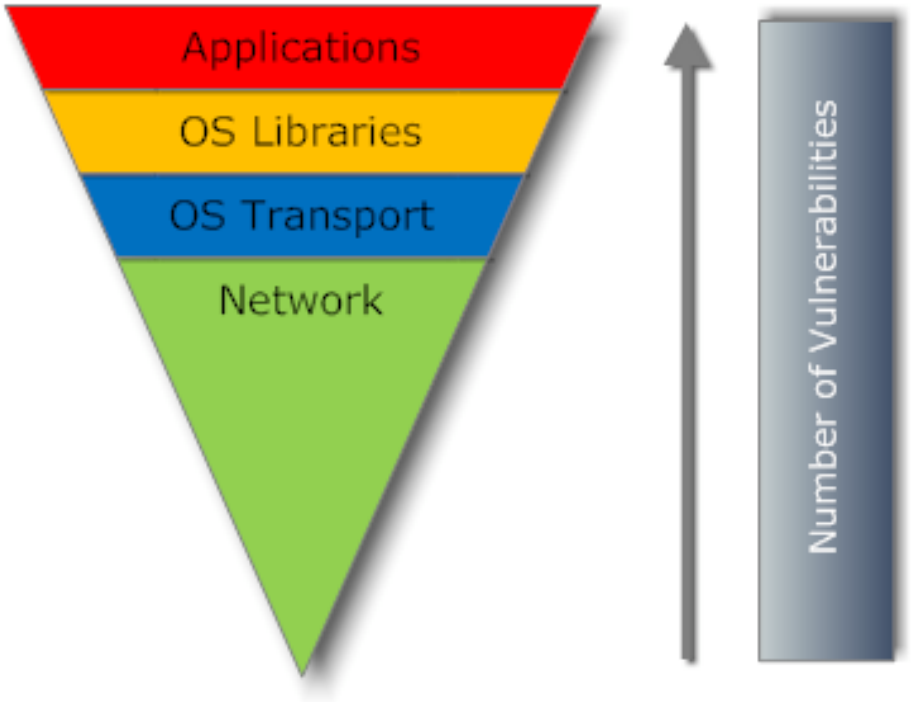
10

جایگاه OWASP از نظر MITRE از نظر یافتن آسیب پذیریها

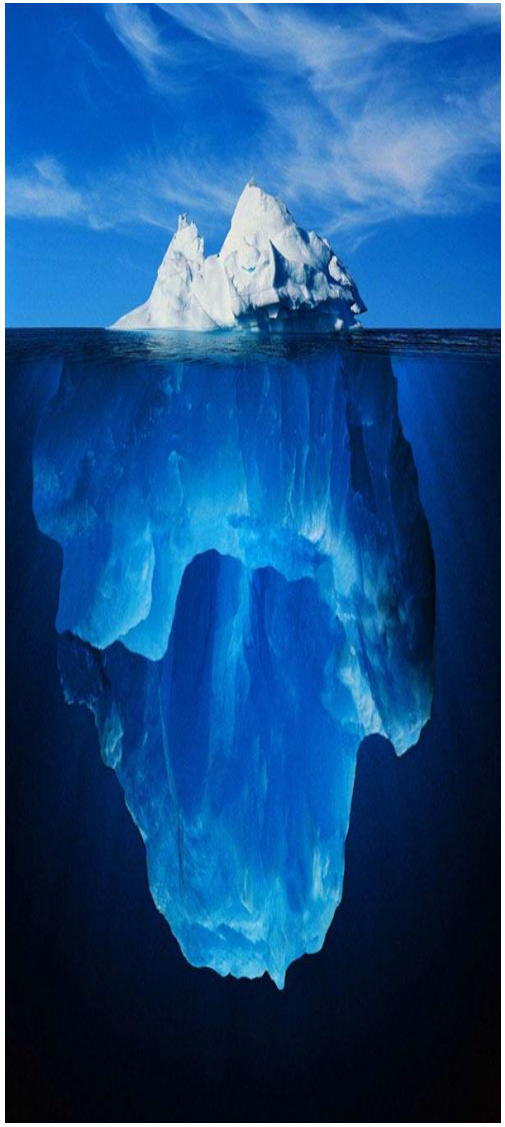


نرخ حملات
SANS - TOP CYBER SECURITY RISKS

- Sept 2009 Report with data from TippingPoint IPS and vulnerability data by Qualys.
- Web Applications have largest # of Vulnerabilities.



پیچیدگی وضع موجود



- تکنولوژی های زیاده از حد گسترش یافته در WEB
- خواندن دوبارۀ کد ها سخت تر از ساخت دوبارۀ آنهاست
- آمار ها نشان می دهد که ۵ تا ۱۵ ایراد در هر ۱۰۰۰ خط کد وجود دارد.

Us Dept. of Defense and the software Engineering Institute

- یافتن هر یک از این ایراد ها ۲ تا ۹ ساعت زمان نیاز دارد.

5 year pentagon study

- مطالعه سالانۀ اسناد آسیب پذیری ها در بهترین حالت بیش از ۷۰۰ ساعت زمان نیاز دارد.

Intel white paper, CERT, ICSA Labs

ضرورت نیاز به مدیریت امنیت اطلاعات

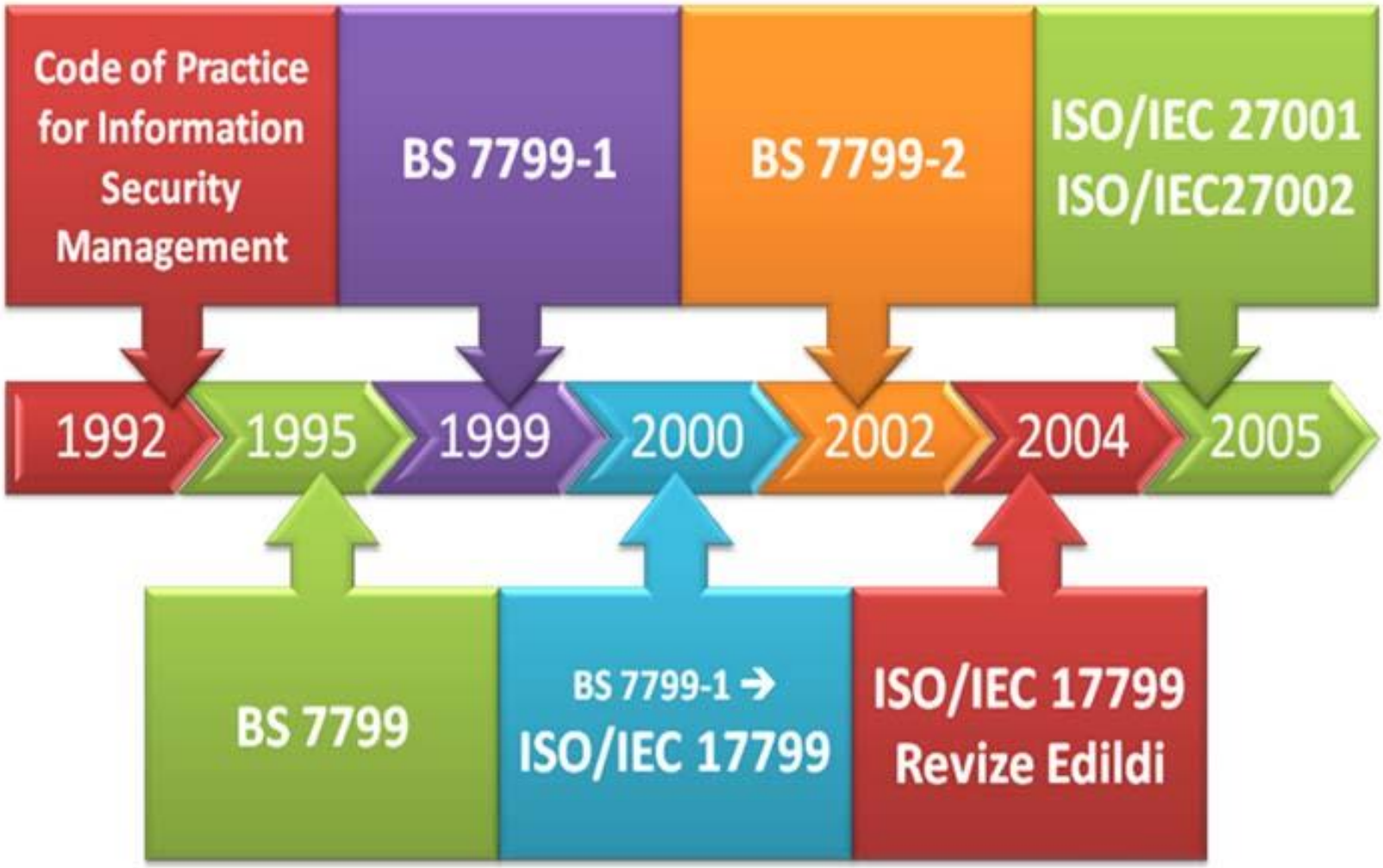
- بیش از ۱۰ میلیارد ویروس در اینترنت در سال ۲۰۱۴ شناسایی شده است.
- بیش از ۵۰۰۰ حمله توسط هکرها در روز به وب سایت ها انجام می شود.
- ۳۹ درصد رشد در حمله به سازمان ها از طریق ارسال لینک های آلوده گزارش شده است.
- ۵۸ درصد نفوذ به سازمان ها توسط هکرها انجام می گیرد (۳۹ درصد ناشی از غفلت کارکنان)

ISMS تعریف ها

- ISMS برای پیاده‌سازی کنترل‌های امنیتی می‌باشد و با اجرای زیرساخت مورد نیاز، ایمنی اطلاعات تضمین می شود. حفاظت از اطلاعات در سه مفهوم زیر لحاظ قرار می گیرد.
  - قابل اطمینان
  - صحت
  - در دسترس بودن اطلاعات مورد

- ISMS برای شناسایی، مدیریت و به حداقل رساندن احتمال وقوع تهدیداتی امنیتی که باعث تخریب اطلاعات در سازمان ها و شرکت ها می شود.
- ISMS برای تمامی تهدیدها (داخلی، خارجی، اتفاقی و خطاهای عمدی و غیر عمدی) راهکارهای پیشگیرانه و امنیتی ارائه دهد.

تاریخچه



تاریخچه

طرح ها وبرنامه های امنیتی مورد نیاز

- اهداف،راهبردها و سیاست های امنیتی فن آوری اطلاعات سازمان
- طرح امنیت فن آوری اطلاعات سازمان
- طرح ارزیابی مخاطرات امنیتی فن آوری اطلاعات سازمان
- طرح پشتیبانی حوادث امنیتی فن آوری اطلاعات سازمان
- طرح تداوم عملکرد و ترمیم خرابی های فن آوری اطلاعات سازمان
- برنامه آگاهی رسانی،تربیت نیروی انسانی و آموزش امنیت فن آوری اطلاعات سازمان

بخشی از پیامدهای منفی یک ایراد امنیتی

- افزایش هزینه سازمان
- زیر سوال رفتن شهرت و اعتبار سازمان
- ازدست رفتن داده های مهم و پیامدهای بعدی آن
- عدم اعتماد مشتریان و سرمایه گذاران

از مزایای استفاده از سامانه مدیریت امنیت اطلاعات

- حفاظت از منابع و تجهیزات شرکت و سازمان
- برقراری امنیت در تمامی سطوح (مانند امنیت فیزیکی، پرسنلی و ارتباطات)
- کاهش تبلیغات منفی علیه سازمان و افزایش وجهه و اعتبار سازمان
- کاهش هزینه های سازمان به خاطر اجرای الزامات امنیتی
- آموزش پرسنل و افزایش سطح دانش آنها
- ....

OSI AND DOD MODEL

<table>
<tr><th>OSI Model</th><th>TCP/IP Model
(DoD Model)</th><th colspan="3">TCP/IP _Internet
Protocol Suite</th></tr>
<tr><td>Application</td><td rowspan="3">Application</td><td rowspan="3">HTTP
HTTPS</td><td rowspan="3">SMTP/IMAP4 -
Telnet- FTP -MIME
-S/MIME-DNS-
RPC- SSH- net
Bios-SMB</td><td rowspan="3">SNMP-POP3-DNS -SSH-
SNMP</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport</td><td colspan="2">TCP
(Transmission Control Protocol)</td><td>UDP
(User Datagram Protocol)</td></tr>
<tr><td>Network</td><td>Internet</td><td colspan="3">IP(internet Protocol)
ICMP(Internet Control Message Protocol)</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Access</td><td colspan="3">IP -ICMP - ARP - RARP - SLIP</td></tr>
<tr><td>Physical</td><td colspan="3">Ethernet - PPP - ADSL
ISO 802.3 802.2</td></tr>
</table>

طراحی پیاده سازی ISMS

- دریافت تأییدیه مدیریت جهت اجرای ISMS
- تعیین محدوده ISMS، مرزها و خط مشی‌ها
- آنالیز نیازهای امنیت اطلاعات سازمان
- ارزیابی ریسک و برنامه‌ریزی تعامل با مخاطرات
- طراحی ISMS

اقدامات اصلی ISMS

- لازم است هر سازمان بر اساس یک متدولوژی مشخص، اقدامات زیر را انجام دهد:

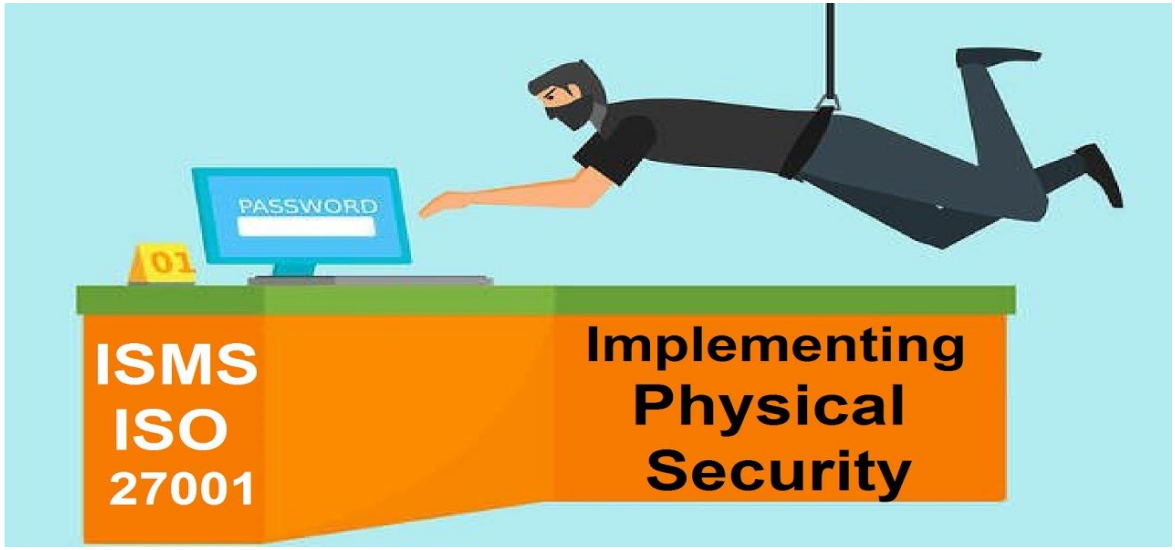
۱- تهیه طرح‌ها و برنامه‌های امنیتی موردنیاز سازمان

۲- ایجاد تشکیلات موردنیاز جهت ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان

۳- اجرای طرح‌ها و برنامه‌های امنیتی سازمان

استانداردها

- در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات سازمان‌ها ارائه شده‌اند
  - استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
  - استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
  - گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد
  - استاندارد مدیریتی ISO/IEC 27001

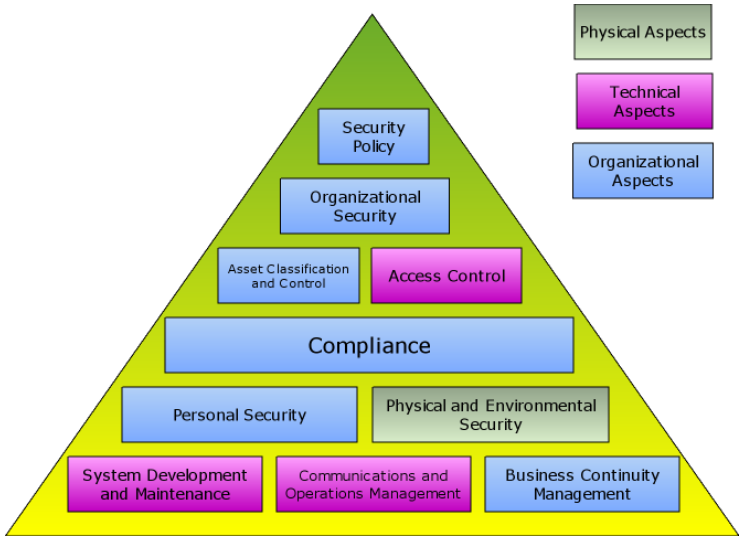


استاندارد BS7799 موسسه استاندارد انگلیس

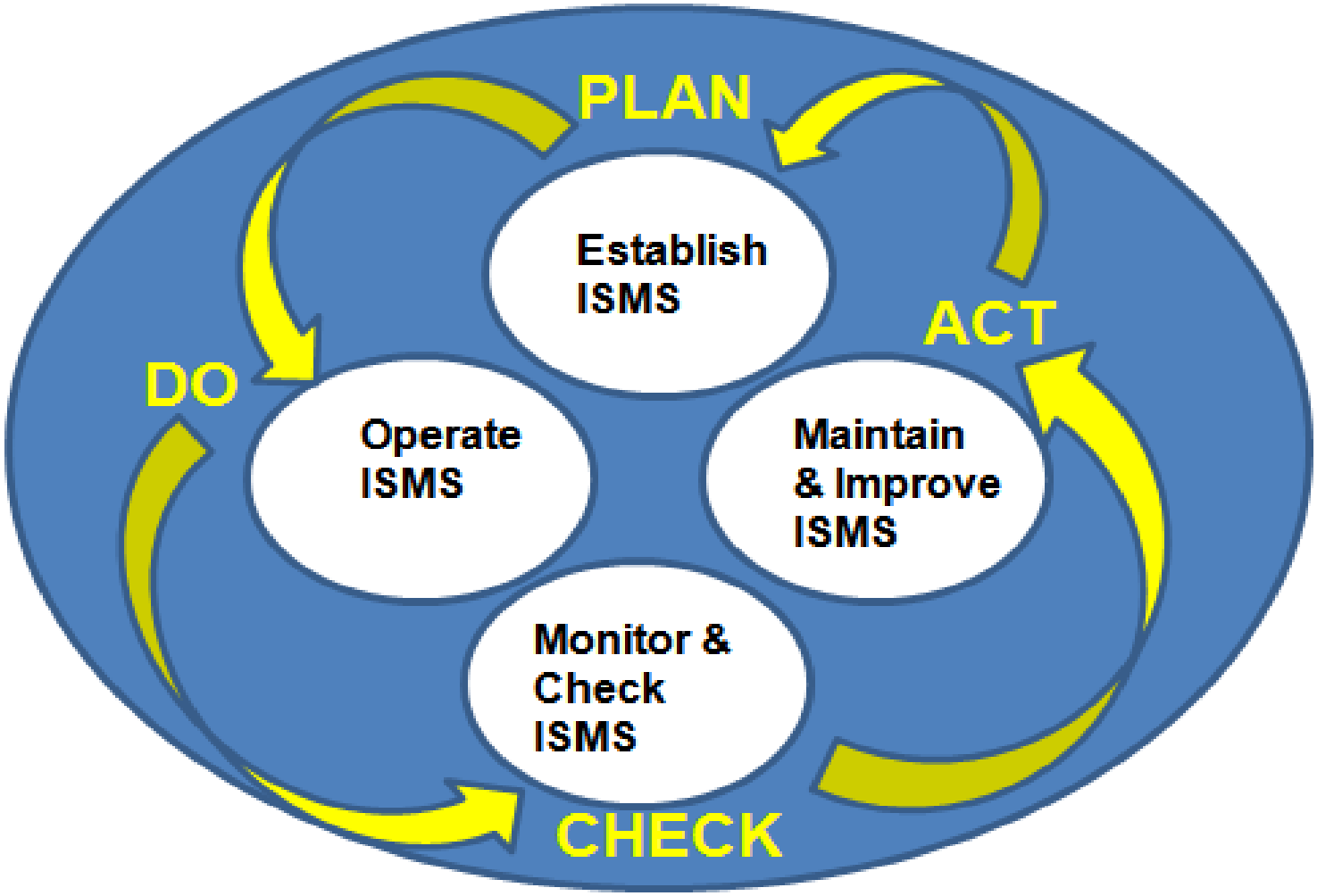
- استاندراد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است
  - نسخه اول آن (BS7799:1) در سال ۱۹۹۵ منتشر شد.
  - نسخه دوم این استاندارد (BS7799:2) که در سال ۱۹۹۹ ارائه شد، علاوه بر تغییر نسبت به نسخه اول، در دو بخش ارائه گردید.
  - آخرین نسخه این استاندارد، (BS7799:2002) نیز در سال ۲۰۰۵
- در دو بخش منتشر گردید
  - بخش اول، مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ۱۰دسته‌بندی کلی است
  - بخش دوم برای تامین امنیت اطلاعات و ارتباطات سازمان، مطابق یک چرخهٔ ایمن سازی شامل ۴ مرحلهٔ طراحی، پیاده سازی، تست و اصلاح ارائه شده

بخش اول استاندارد BS7799

1. تدوین سیاست امنیتی سازمان
2. ایجاد تشکیلات تامین امنیت سازمان
3. دسته‌بندی سرمایه‌ها و تعیین کنترل‌های لازم
4. امنیت پرسنلی
5. امنیت فیزیکی و پیرامونی
6. مدیریت ارتباطات
7. کنترل دسترسی
8. نگهداری و توسعه سیستم‌ها
9. مدیریت تداوم فعالیت سازمان
10. پاسخگوئی به نیازهای امنیتی



بخش دوم استاندارد BS7799



PLAN

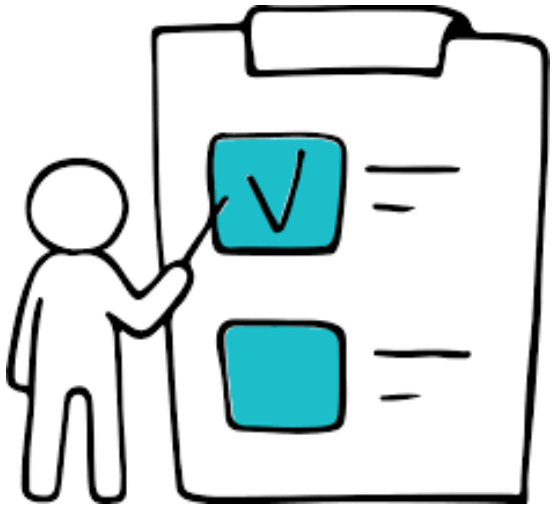
- ISMS را برنامه ریزی کن
  - این فاز در واقع مرحله مشخص شدن تعاریف اولیه پاده سازی ISMS می باشد. تهیه سیاست های امنیتی، مقاصد، تعریف پردازش های مختلف درون سازمانی و روتین های عملیاتی و ... در این مرحله تعریف و پیاده سازی می شوند.

DO

- انجام بده (ISMS را پیاده نموده و از آن بهره برداری کن):
  - پیاده سازی و اجرای سیاست های امنیتی،کنترل ها پردازش ها در این مرحله انجام میشود.
  - در واقع این مرحله اجرای کلیه مراحل فاز اول را طلب میکند.

CHECK

- کنترل کن (ISMS را پایش کرده و مورد بازنگری قرار بده)
  - در این مرحله ارزیابی موفقیت پیاده سازی سیاست های مختلف امنیتی، همچنین تجربه های عملی و گزارش های مدیریتی گرد آوری خواهند شد.



ACT

- رفتار کن (**ISMS** رانگهداری نموده و آنرا بهبود ببخش)
  - اجرای موارد ترمیمی و باز نگری در نحوه مدیریت طلاعات،همچنین تصحیح موارد مختلف در این فاز انجام میشود.

استاندارد ISO/IEC 17799 موسسه بین‌المللی استاندارد

- در سال ۲۰۰۰، بخش اول استاندارد BS7799:2 بدون هیچگونه تغییری توسط موسسهٔ بین المللی استاندارد بعنوان استاندارد ISO/IEC 17799 منتشر شد.

استاندارد ISO 27001

- استاندارد ایزو ۲۷۰۰۱ به موضوع مدیریت امنیت اطلاعات می پردازد
- نسخه دوم این استاندارد در سال ۲۰۱۳ ارائه گردیده
- استاندارد ISO/IEC 27000نمای کلی و واژگان سیستم های مدیریت امنیت اطلاعات را توصیف نموده و مرجع خانواده استاندارد سیستم مدیریت امنیت اطلاعات اصطلاحات ه همراه تعاریف مرتبط با آن است.
  - ISO/IEC 27003
  - ISO/IEC 27004
  - ISO/IEC 27005)
- اهم موارد مطروحه در این استانداردها به شرح زیر می‌باشند:
  - تعیین مراحل ایمن سازی و نحوه شکل گیری چرخه امنیت
  - تکنیک‌های مورد استفاده در هر مرحله از ایمن سازی و جزئیات آن
  - خط مشی امنیتی و طرح‌ها و برنامه‌های تدوین شده و مورد نیاز سازمان در این زمینه
  - شناسایی، ارزیابی و تدوین راه‌کارهای برخورد با مخاطرات (Risks) در سازمان
  - نیاز و نحوه ایجاد تشکیلات سیاست گذاری، اجرائی و فنی در زمینه امنیت فضای تبادل اطلاعات (افتا)
  - کنترل‌های امنیتی مورد نیاز برای حفاظت از سیستم‌های اطلاعاتی و ارتباطی

ISO/IEC TR13335

www.bigdata-ir.com

Telegram: @BigData_Channel

مدرس:
علیرضا حبیبی

راهنماي فني ISO/IEC TR13335

- راهنمای فنی ISO/IEC TR13335 موسسه بین‌المللی استاندارد
- این گزارش فنی در قالب ۵ بخش مستقل در فواصل سالهای ۱۹۹۶ تا ۲۰۰۱ توسط موسسهٔ بین المللی استاندارد منتشر شده است
- این گزارش فنی به عنوان استاندارد ISO منتشر نشد و عنوان Technical Report بر آن نهاده شد
- تنها مستندات فنی معتبری است که جزئیات و تکنیکهای مورد نیاز مراحل ایمن سازی اطلاعات و ارتباطات را تشریح نموده و در واقع مکمل استانداردهای مدیریتی BS7799 و ISO/IEC 17799 می باشد.

بخش های اصلی ISO/IEC TR13335

- بخش اول
  - در این بخش که در سال ۱۹۹۶منتشر شد، **مفاهیم کلی** امنیت اطلاعات از قبیل سرمایه، تهدید، آسیب پذیری، ریسک، ضربه و ... روابط بین این مفاهیم و مدل مدیریت مخاطرات امنیتی، ارائه شده است.
- بخش دوم
  - که در سال ۱۹۹۷منتشر شد ، **مراحل ایمن سازی و ساختار تشکیلات** تامین امنیت اطلاعات سازمان ارائه شده است . بر اساس این گزارش فنی ، چرخهٔ ایمن سازی به ۵ مرحله شامل تدوین سیاست امنیتی سازمان، تحلیل مخاطرات امنیتی، تعیین حفاظها و ارائهٔ طرح امنیت، پیاده سازی طرح امنیت و پشتیبانی امنیت اطلاعات، تفکیک شده است.
- بخش سوم
  - در این بخش که در سال ۱۹۹۸منتشر شد، **تکنیکهای طراحی، پیاده سازی و پشتیبانی** امنیت اطلاعات از جمله محورها و جزئیات سیاستهای امنیتی سازمان، تکنیکهای تحلیل مخاطرات امنیتی، محتوای طرح امنیتی، جزئیات پیاده سازی طرح امنیتی و پشتیبانی امنیت اطلاعات، ارائه شده است.
- بخش چهارم
  - در این بخش که در سال ۲۰۰۰ منتشر شد، ضمن **تشریح حفاظهای فیزیکی**، سازمانی و حفاظهای خاص سیستم‌های اطلاعاتی، نحوهٔ انتخاب حفاظهای مورد نیاز برای تامین هریک از مولفه‌های امنیت اطلاعات، ارائه شده است.
- بخش پنجم
  - در سال ۲۰۰۱ منتشر شد، ضمن افزودن مقولهٔ ارتباطات و مروری بر بخشهای دوم تا چهارم این گزارش فنی، تکنیکهای تامین امنیت ارتباطات از قبیل شبکه‌های خصوصی مجازی، امنیت در گذرگاه‌ها، تشخیص تهاجم و کدهای مخرب، ارائه شده است.

بخش اول ISO/IEC TR13335

- در این بخش که در سال 1996 منتشر شد، مفاهیم کلی امنیت طلاعات و روابط بین این مفاهیم و مدل مدیریت مخاطرات امنیتی، ارائه شده است . از قبیل:

  - سرمایه دارایی‌های که بایستی حفاظت شوند (Assets)
  - تهدیدات (Threats)
  - عامل تهدید
  - رخنه‌ها یا آسیب پذیری (Vulnerabilities)
  - آسیبها (Impacts)
  - مخاطرات (Risks)
  - روش‌های مقابله (Safeguards)
  - ریسک باقی مانده (Residual Risks)
  - ضربه

اصطلاحات و تعاریف :

- **Assetیا دارایی** : هر چیزی که در سازمان شما دارای ارزش (مادی یا معنوی) باشد دارایی شما محسوب می شود.
- **Threatیا تهدید** : فعالیت ها یا رویدادهایی که می توانند باعث آسیب رساندن به دارایی های شما شوند.
- **Threat Agentیا عامل تهدید** : شخص یا منبعی که قدرت ایجاد یک تهدید را داشته باشد.
- **Vulnerabilityیا آسیب پذیری** : نقطه ضعف ای که می تواند توسط عامل تهدید مورد استفاده قرار گرفته و امنیت را دچار اختلال کند.
- **Riskیا خطر** : احتمال اینکه عامل تهدید از آسیب پذیری موجود سوء استفاده کند.

اصطلاحات و تعاریف :

- **دارایی**: هر چیزی که برای سازمان دارای ارزش باشد .
- **دسترس پذیری**: ویژگی در دسترس و قابل استفاده بودن ، به محض تقاضای یک موجودیت مجاز شده .
- **محرمانگی**: ویژگی که اطلاعات در دسترس افراد ، موجودیت ها یا فرآیند های غیر مجاز قرار نگرفته یا فاش نشود .
- **یکپارچگی**: ویژگی حفظ صحت و تمامیت دارایی ها
- **امنیت اطلاعات**: حفظ محرمانگی ، یکپارچگی و دسترس پذیری اطلاعات همچنین ، ویژگی هایی از قبیل سندیت پاسخگویی ، انکار ناپذیری و قابلیت اطمینان ، می تواند لحاظ شود .
- **رویداد امنیت اطلاعات**: رخداد شناسایی شده یک سیستم ، سرویس یا شبکه ، که **دلالت بر نقض** احتمالی خط مشی امنیت اطلاعات یا نقض حفاظتی ، یا وضعیتی که ممکن است با امنیت مرتبط بوده و قبلا شناخته نشده دارد .
- **حادثه امنیت اطلاعات**: یک یا مجموعه ای از رویدادهای امنیت اطلاعات نا خواسته یا پیش بینی نشده که به احتمال زیاد عملیات کسب و کار را به **خطر** انداخته و امنیت اطلاعات را تهدید کنند .
- **سیستم مدیریت امنیت اطلاعات (ISMS) :** قسمتی از سیستم مدیریت کلان بنا شده بر دیدگاه ریسک های کسب و کار ، به منظور ایجاد ، پیاده سازی ، اجرا ، پایش ، بازنگری و بهبود امنیت اطلاعات .
  - نکته : سیستم مدیرتی ، شامل ساختار سازمانی ، خط مشی ها ، طرح ریزی فعالیت ها ، مسوولیت تجارب روشهای اجرایی ، فرآیندها و منابع است .

اصطلاحات و تعاریف :

- **ریسک باقیمانده**: ریسک باقیمانده پس از برطرف سازی ریسک
- **پذیرش ریسک**: تصمیم برای پذیرش یک مخاطره
- **تحلیل ریسک**: استفاده نظام مند از اطلاعات به منظور شناسایی منابع و تخمین ریسک
- **ارزیابی ریسک**: فرآیند مقایسه ریسک تخمین زده شده ، با معیار ریسک ارایه شده ، به منظور تعیین اهمیت ریسک
- **برآورد ریسک**: فرآیند کلی تحلیل و ارزیابی ریسک
- **مدیریت ریسک**: فعالیت های هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به ریسک
- **برطرف سازی ریسک**: فرآیند انتخاب و پیاده سازی معیارهایی برای تعدیل ریسک
  - نکته : در این استاندارد ، واژه کنترل به عنوان مترادف تمهید (Meaure) بکار رفته است
- **بیانیه کاربست پذیری (Statement of applicability)**: بیانیه مستند شده ای که اهداف کنترلی و کنترل های وابسته و بکار برده شده در سیستم مدیریت امنیت اطلاعات سازمان را تشریح می کند .
  - نکته : اهداف کنترلی و کنترل ها ، برمبنای نتایج و استنتاج از فرآیند های برآورد و بر طرف سازی ریسک ، الزامات قانونی یا آیین نامه ای ، تعهدات قرار دادی و الزامات کسب و کار سازمان برای امنیت اطلاعات پایه ریزی می شود .
- **تمامیت**: منظور از آن تامین دقت و تمامیت دارایی ها می باشد.

بخش دوم ISO/IEC TR13335

- این بخش که در سال1997 منتشر شد ، مراحل ایمن سازی و ساختارتشکیلات تامین امنیت اطلاعات سازمان ارائه شده است .

تحلیل مخاطرات (RISK)

جدیت	احتمال وقوع			
		به ندرت	بعضی اوقات	غالبا
	کم اهمیت	۱	۲	۳
	جدی	۴	۵	۶
	خیلی جدی	۷	۸	۹

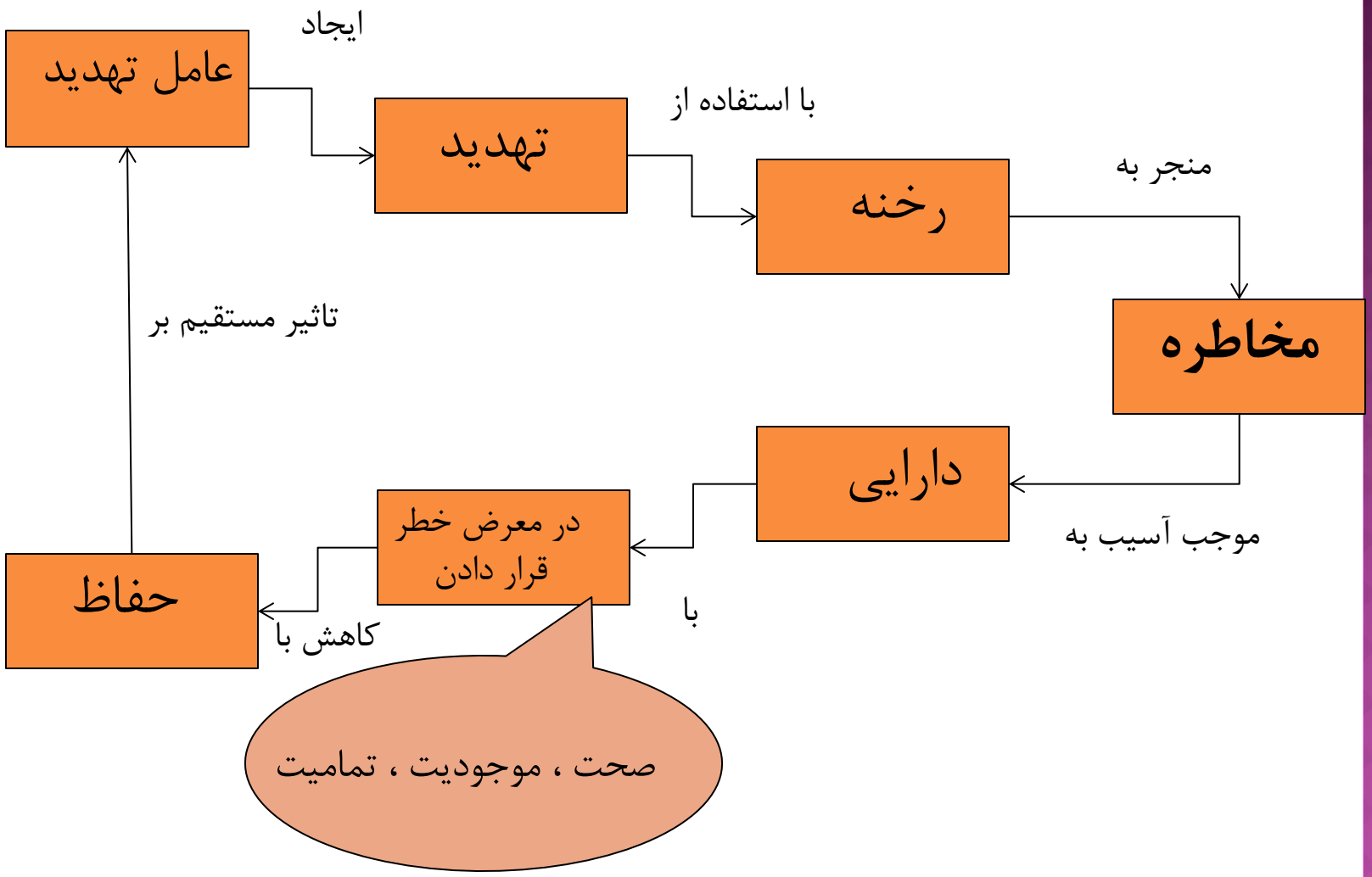
بخش سوم ISO/IEC TR13335

- در این بخش که در سال 1998 منتشر شد، تکنیکهای طراحی، پیاده سازی و پشتیبانی امنیت اطلاعات از جمله محورها و جزئیات سیاستهای امنیتی سازمان، تکنیکهای تحلیل مخاطرات امنیتی، محتوای طرح امنیتی، جزئیات پیاده سازی طرح امنیتی و پشتیبانی امنیت اطلاعات، ارائه شده است.

بخش چهارم ISO/IEC TR13335

- در این بخش که در سال 2000 منتشر شد، ضمن تشریح حفاظهای فیزیکی، سازمانی و حفاظهای خاص سیستم‌های اطلاعاتی، نحوهٔ انتخاب حفاظهای مورد نیاز برای تامین هریک از مولفه‌های امنیت اطلاعات، ارائه شده است.

مدیریت مخاطرات



بخش پنجم ISO/IEC TR13335

- در این بخش که در سال 2001 منتشر شد، ضمن افزودن مقولهٔ ارتباطات و مروری بر بخشهای دوم تا چهارم این گزارش فنی، تکنیکهای تامین امنیت ارتباطات از قبیل شبکه‌های خصوصی مجازی، امنیت در گذرگاه‌ها، تشخیص تهاجم و کدهای مخرب، ارائه شده است.

NEW GENERATION FIREWALL

www.bigdata-ir.com

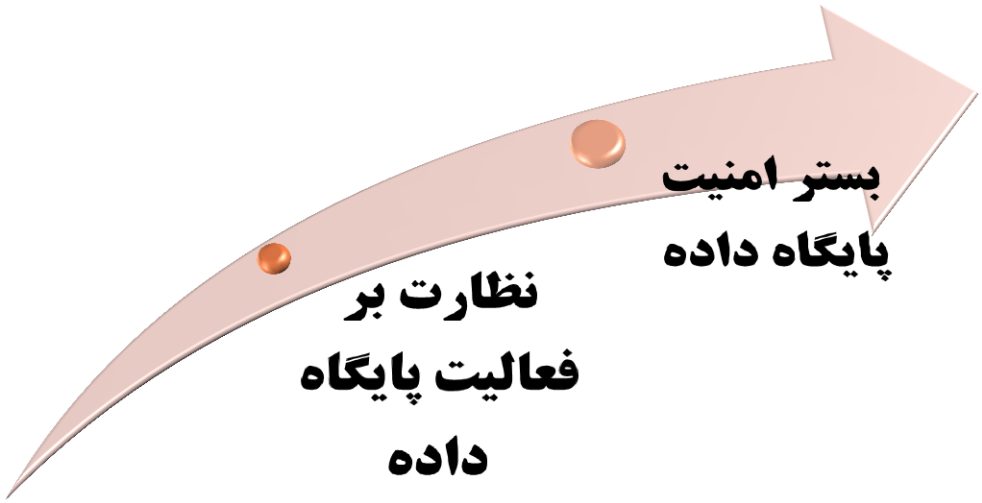
Telegram: @BigData_Channel

مدرس:
علیرضا حبیبی

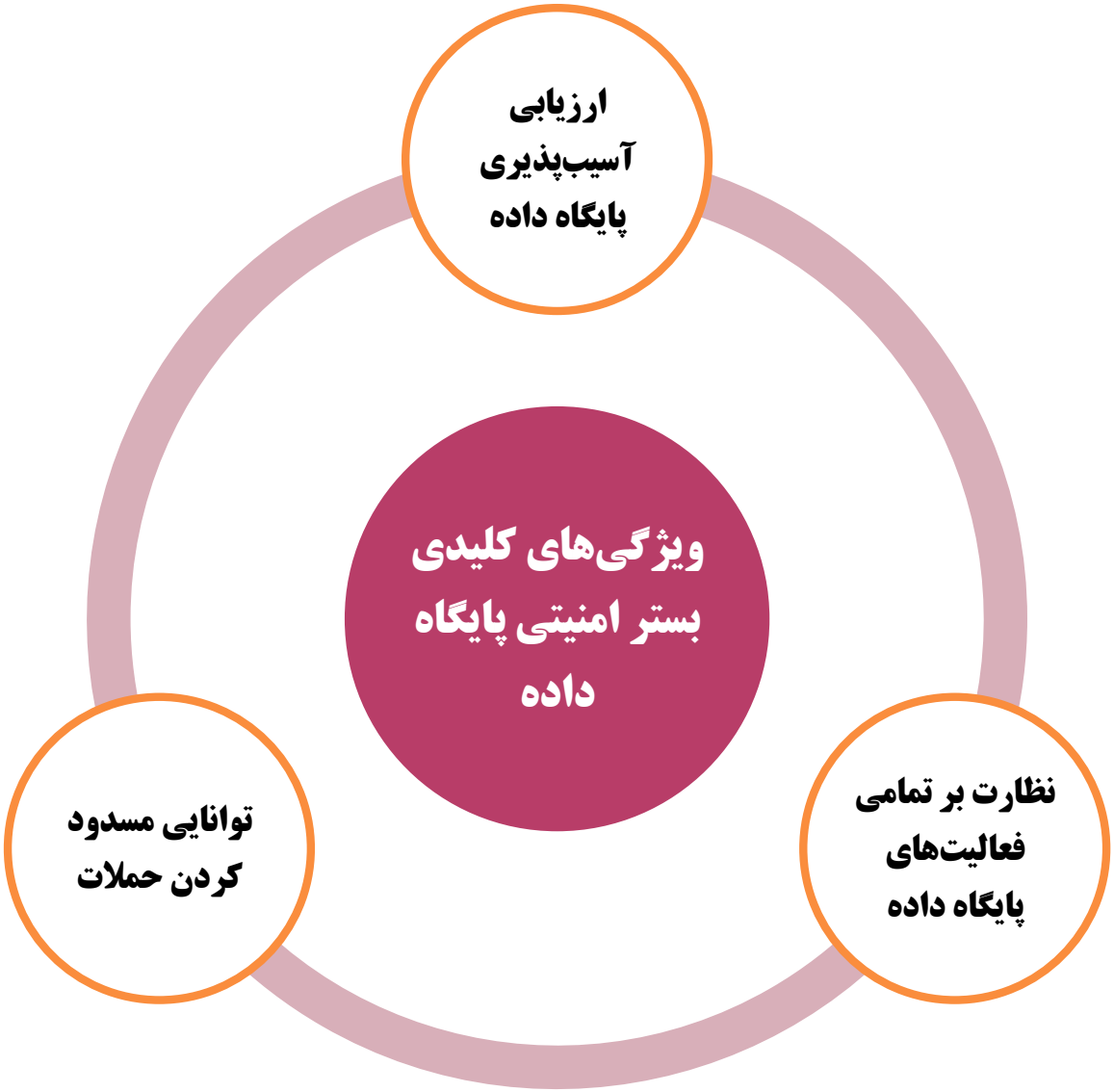
سیر پیشرفت

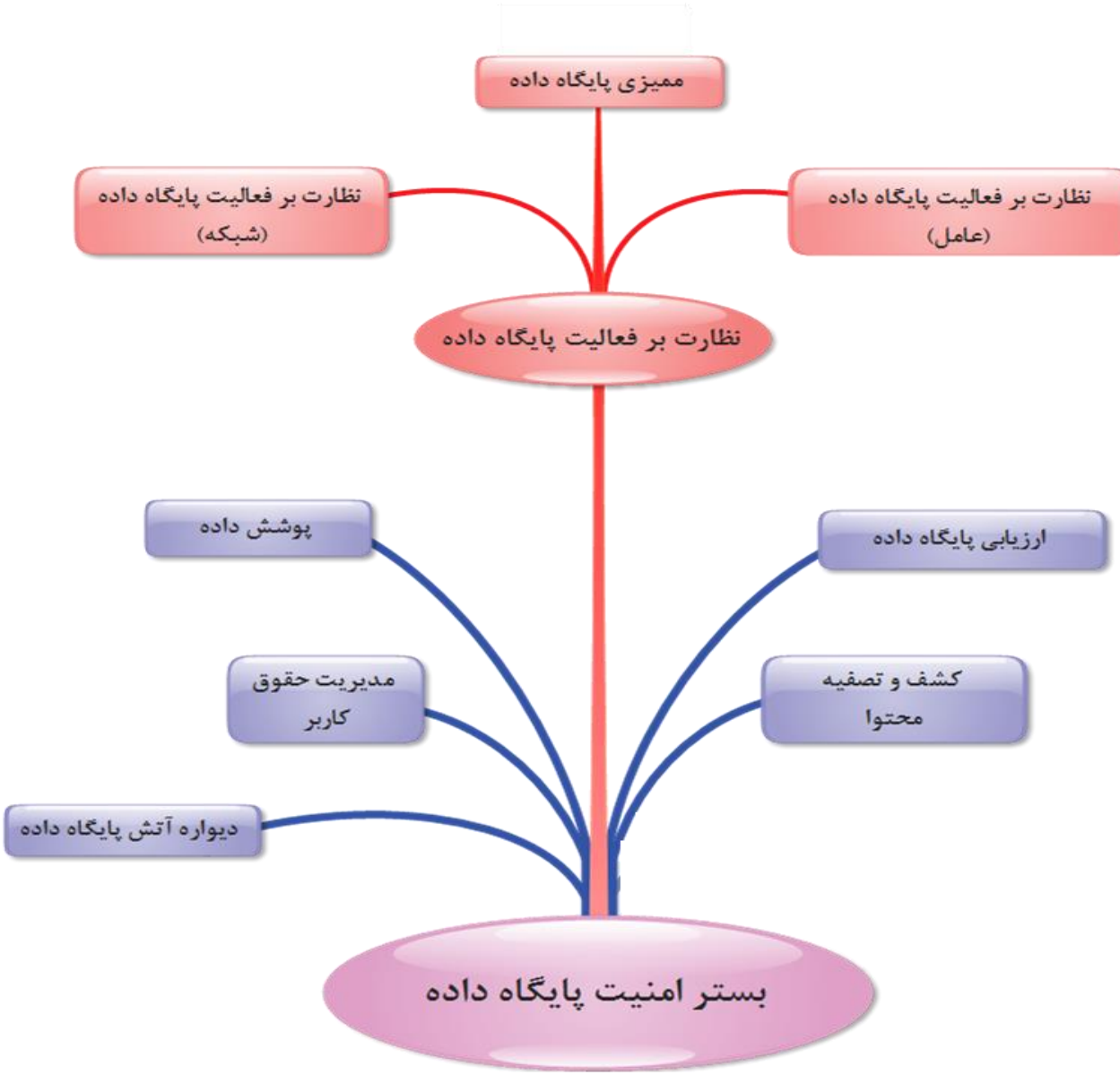
در سال‌های اخیر، پیش از آنکه شرکت‌های تولیدکننده محصولات امنیتی پایگاه داده، نام دیواره آتش پایگاه داده را به صورت تجاری مطرح کنند محصول دیگری به نام نظارت بر فعالیت‌های پایگاه داده مهم‌ترین بستر امنیتی برای پایگاه داده‌ها محسوب می‌گردید.
(Database Activity Monitoring (DAM))

سیر پیشرفت



بسترهای امنیتی پایگاه داده، امنیت پایگاه داده را ارزیابی نموده و تمام فعالیت‌های پایگاه داده را به صورت بی‌درنگ یا تقریباً بی‌درنگ (شامل فعالیت‌های مدیر)؛ در میان چندین نوع بستر پایگاه داده ثبت نموده و هر گونه تخطی از سیاست‌ها را هشدار داده و مسدود می‌کند.





ویژگی‌های مورد نیاز یک بستر امنیتی پایگاه داده

- جلوگیری از حملات شناخته‌شده بر روی پروتکل SQL
- جلوگیری از حملات داخلی
- وارسی برآورده شدن محدودیت‌های مربوط به زمان و آدرس IP در پرس‌وجو
- وارسی ترافیک بازگشتی و مسدود نمودن آن در صورت مشاهده‌ی امضای حمله
- پوشش‌گذاری داده‌های حساس
- ردیابی کاربران در سطح پایگاه داده
- بازنویسی پرس‌وجو

- نظارت بر فعالیت‌های پایگاه داده
- شناسایی حملات در سطح برنامه‌ی کاربردی
- دیده‌بانی نمودن کاربران صاحب امتیاز
- ممیزی نمودن تمامی دسترسی‌ها به پایگاه داده
- متمرکزسازی ترافیک ممیزی
- نظارت بر فعالیت‌های پرونده
- تولید گزارش‌های ویژه مرتبط با قواعد PCI، SOX و...

- کشف پایگاه‌های داده و طبقه‌بندی داده‌ها
- کشف محتوا
- پویش آسیب‌پذیری‌های پایگاه داده
- انجام آزمون‌های مناسب با نوع پایگاه داده
- معرفی وصله‌های امنیتی مورد نیاز پایگاه داده
- اعمال توصیه‌های امن‌سازی بر روی پایگاه داده
- اعمال وصله‌های مجازی در صورت نیاز

- یادگیری ترافیک مجاز ارسالی به سوی پایگاه داده
- مسدود نمودن ترافیک در صورت مشاهده‌ی تخطی
- نگهداری حالات مربوط به ترافیک
- تحلیل محتوا به صورت پویا

مقایسه قابلیت‌های تولیدکنندگان محصولات امنیتی پایگاه داده

نام محصول / قابلیت	Imperva	SQL/ Protect	GreenSQL	Oracle DB firewall	IBM Guardium	FortiDB
کشف تزریق SQL	√	√	√	√	√	√
وصله‌سازی مجازی	√	❊	√	√	√	❊
حالت عملیاتی	یادگیری، محافظت‌شده، نادیده گرفتن	یادگیری، فعال غیرفعال	یادگیری، فعال غیرفعال	مسدود نمودن و نظارت بر خط ،نظارت بر خط تنها،مدل مسدود نمودن و نظارت پروکسی ،نظارت خارج از محدوده	تجمیع کننده ،مدیریت مرکزی/جمع‌آوری	فعال ، غیرفعال
یادگیری ترافیک	√	√	√	√	√	√
پوشش گذاری داده‌ها	❊	❊	√	√	√	❊
حالت پروکسی	√	❊	√	√	√	❊
نظارت بر پایگاه داده	√	√	√	√	√	√
رمزگذاری	❊	❊	❊	√	√	❊
کشف داده‌ها و طبقه‌بندی	√	❊	√	کشف داده‌های حساس با کشف حالت برنامه‌ی کاربردی	√	√

مقایسه قابلیت‌های تولیدکنندگان محصولات امنیتی پایگاه داده

نام محصول / قابلیت	Imperva	SQL/ Protect	GreenSQL	Oracle DB firewall	IBM Guardium	FortiDB
ابزارهای ارزیابی آسیب‌پذیری	✓	❋	❋	✓	✓	✓
پشتیبانی از سکوهای پایگاه داده	Oracle MS SQL Server DB2 ,IMS Informix, Netezza SAP Sybase Teradata MySQL PostgreSQL Progress OpenEdge	Postgresql	MS SQL Server MySQL Oracle PostgreSQL MS SQL Azure MariaDB	Oracle MS SQL Server IBM DB2 SAP Sybase MySQL	Oracle DB2 Informix MySQL Netezza PostgreSQL Sybase Teradata	Apache Derby , PostgreSQL, Oracle, MS SQL Server
امنیت شبکه	• تزریق SQL • دیواره‌ی آتش نگهدارنده حالت • تشخیص نفوذ • پیشگیری از DoS	• تزریق SQL • دیواره‌ی آتش نگهدارنده حالت	• تزریق SQL • دیواره‌ی آتش نگهدارنده حالت • تشخیص و پیشگیری از نفوذ	• تزریق SQL • دیواره‌ی آتش نگهدارنده حالت	• تزریق SQL • دیواره‌ی آتش نگهدارنده حالت • تشخیص و پیشگیری از نفوذ	• تزریق SQL • دیواره‌ی آتش نگهدارنده حالت

www.bigdata-ir.com

Telegram: @BigData_Channel

مدرس:
علیرضا حبیبی

TEST

- Security Testing
- Unit Testing
- Integration Testing
- Functional Testing
- System Testing
- Stress Testing
- Performance Testing
- Usability Testing
- Acceptance Testing
- Regression Testing
- Beta Testing
  - Beta testing is the testing which is done by end users

جایگاه فعالیت مدیر امنیت اطلاعات در کدام موارد زیر است؟

- مدیریت امنیت در سطح شرکت
- مدیریت امنیت در سطح سازمان
- مدیریت امنیت در سطح استراتژیک

WHAT IS NEW

- DBF
- PWAF
- Big data security
- Safety
- Pen test vs. Security test
- Tempest
- Defense In Depth
- Google hacking
- OSINT
- SIGINT
- Intelligence
- Availability Vs. Security
- Top of seven layer
- Cyber security
- Deep Web
- Dark Web
- economic
- Social
- Bad attack
- miss use case
- Tor network
- Recourse management
- Data mining Security
- Data diode
- Type of test
- فریب

آشنایی با معانی دقیق واژه ها

- Intelligence
- Security
- safety

OSINT

پول و اولویت

مهندسی امنیت

www.bigdata-ir.com

Telegram: @BigData_Channel

مدرس:
علیرضا حبیبی

سرمایه ها / اهداف	سخت افزارها	نرم افزارها	اطلاعات	ارتباطات	کاربران شبکه
محرمانگی(Confidentiality)			■	■	
صحت(Integrity)	■	■	■	■	
قابلیت دسترسی(Availability)	■	■	■	■	
محافظت فیزیکی(Physical Protection)	■				
تشخیص هویت(Authenticity)					■
حدود اختیارات(Authority)					■
پاسخ گویی(Accountability)					■
حریم خصوصی(Privacy)					■
آگاهی رسانی(Security Awareness)					■
حساب پذیری یا ممیزی (Auditing)					■
فریب (evasion)					■

تعریف مهندسی امنیت

مهندسی امنیت مجموعه فعالیت‌هایی است که برای حصول و نگهداری سطوح مناسبی از :

-محرمانگی (Confidentiality)

-صحت (Integrity)

-قابلیت دسترسی (Availability)

-حساب پذیری (Accountability)

- اصالت (Authenticity) و

– قابلیت اطمینان (Reliability)

به صورت قاعده مند در یک سازمان انجام می‌شود.

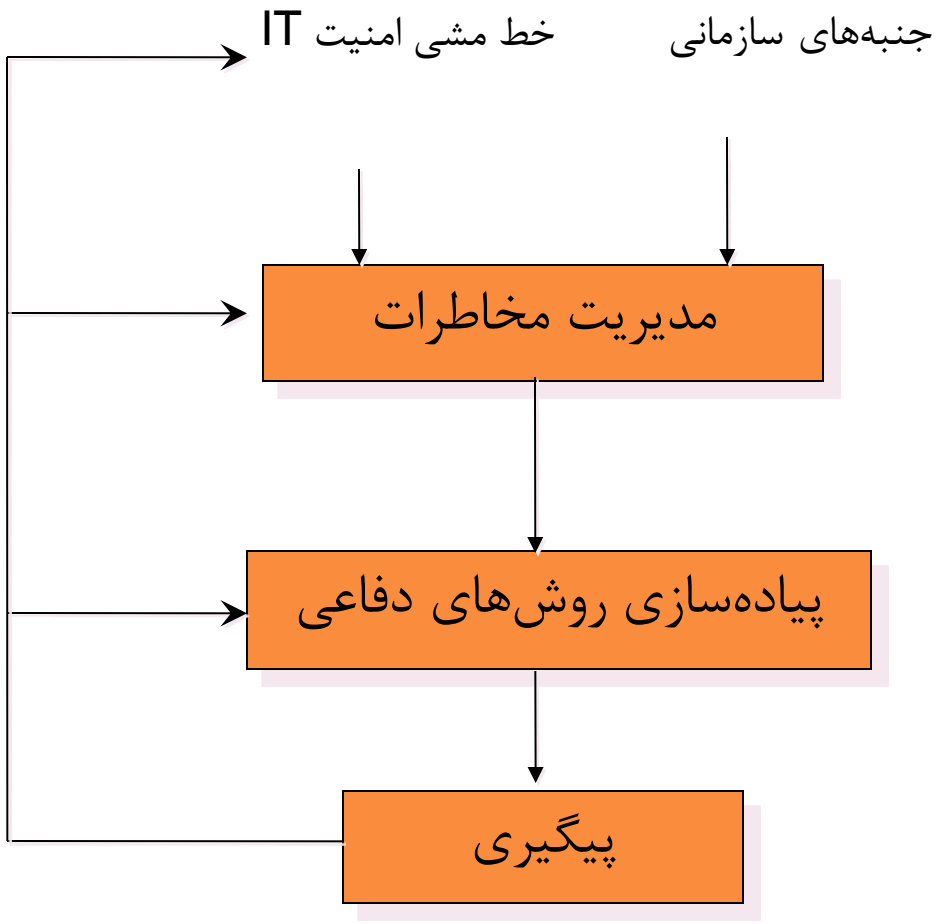
اصول مهندسی امنیت

- امنیت فضای تبادل اطلاعات مفهومی کلان و مبتنی بر حوزه های مختلف دانش است.
- امنیت هر سیستم تعریف مخصوص به خود دارد .
- امنیت ابزاری برای رسیدن به هدف سیستم است.
- امنیت نسبی است.

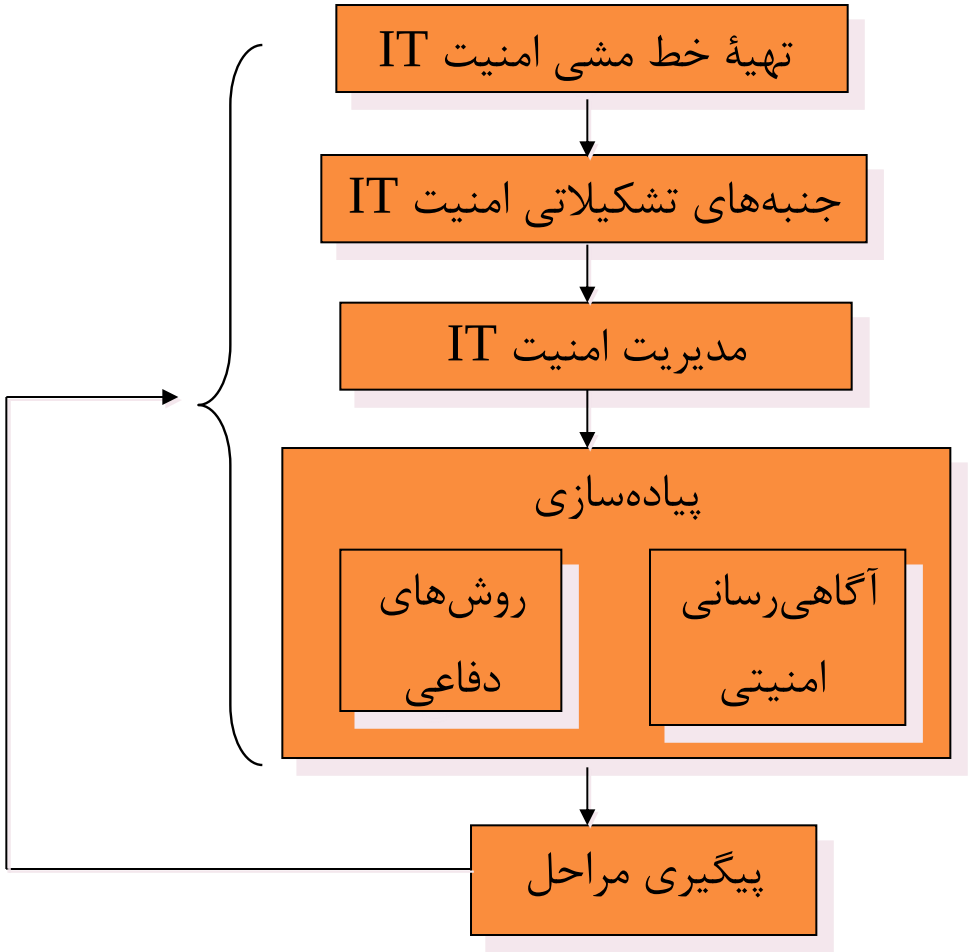
اصول مهندسی امنیت

- امنیت سیستم یک طرح یکپارچه و جامع می‌طلبد.
- حیطهٔ مسئولیتها و مقررات امنیتی باید کاملاً شفاف و غیرمبهم باشد.
- طرح امنیتی باید مقرون به صرفه باشد.
- امنیت هر سیستم توسط عوامل اجتماعی محدود می‌شود.
- امنیت هر سیستم باید بطور متناوب مورد ارزیابی مجدد قرار گیرد.

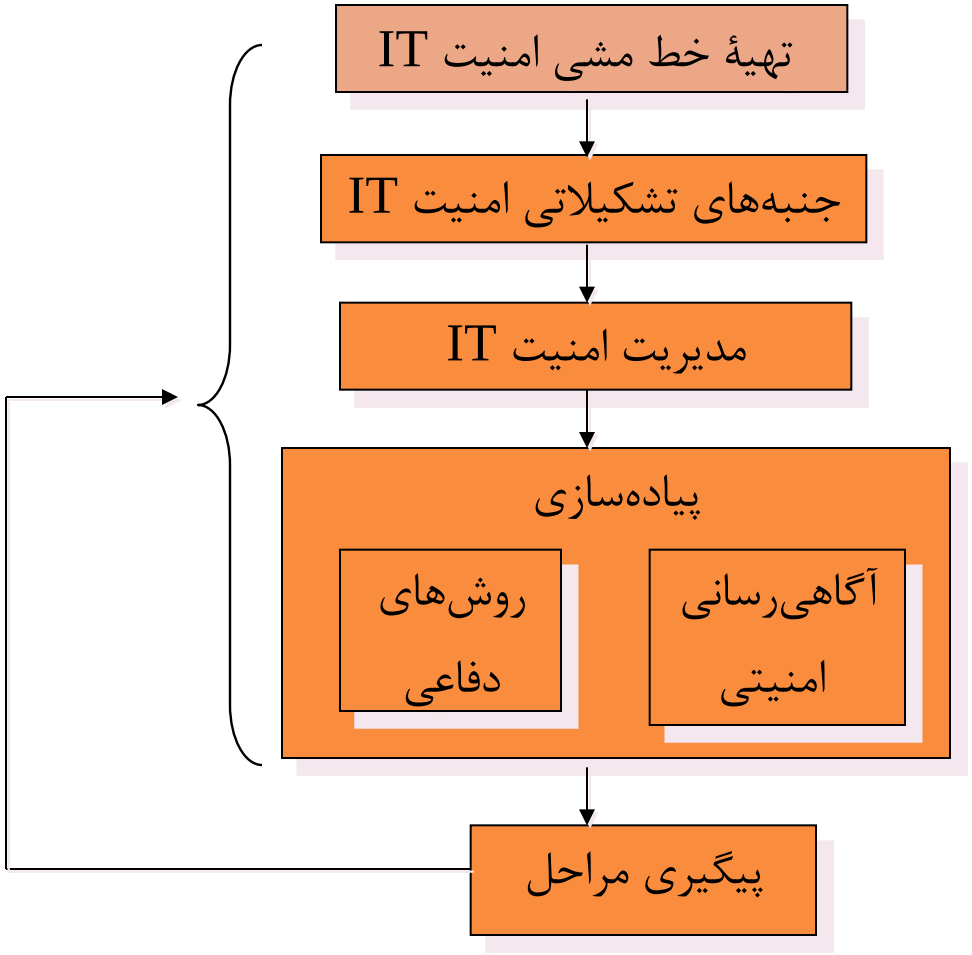
چرخه ی حیات مهندسی امینت



چرخه ی حیات مهندسی امینت



تهیهٔ خط مشی امنیت IT



تهیهٔ خط مشی امنیت IT

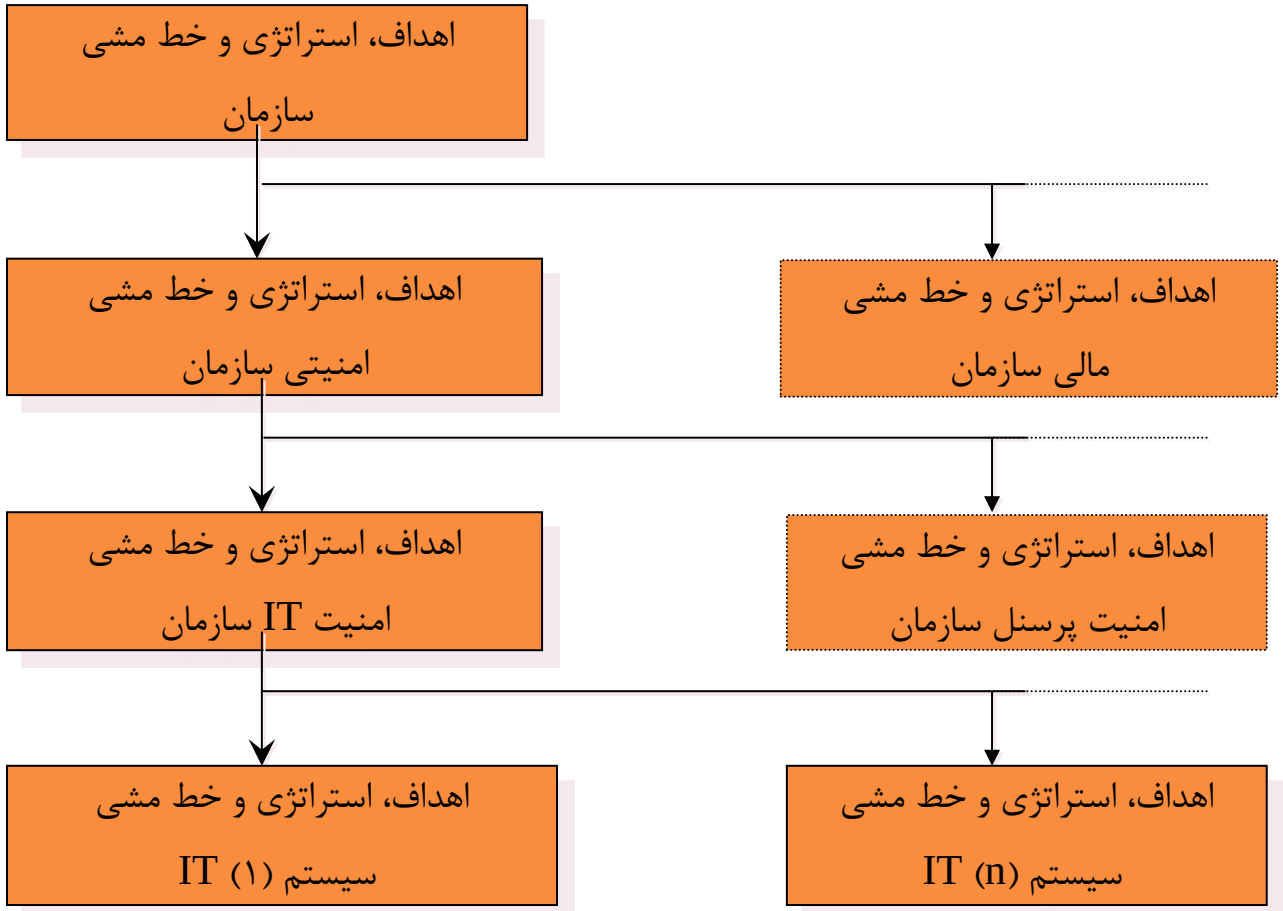
برای ایجاد امنیت در یک سازمان، اولین قدم تدوین اهداف، استراتژی و خط مشی امنیتی سازمان است.

اهداف (Objectives)

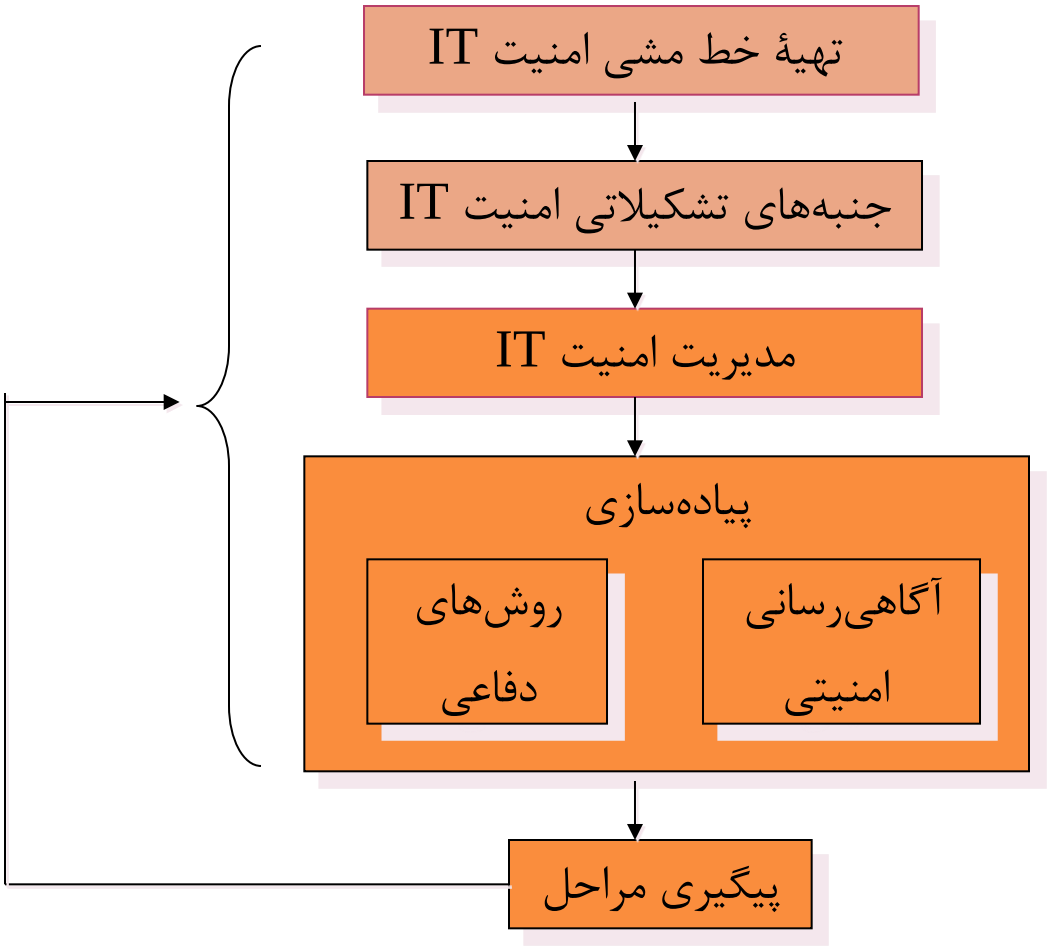
استراتژی (Strategy)

خط مشی (Policy)

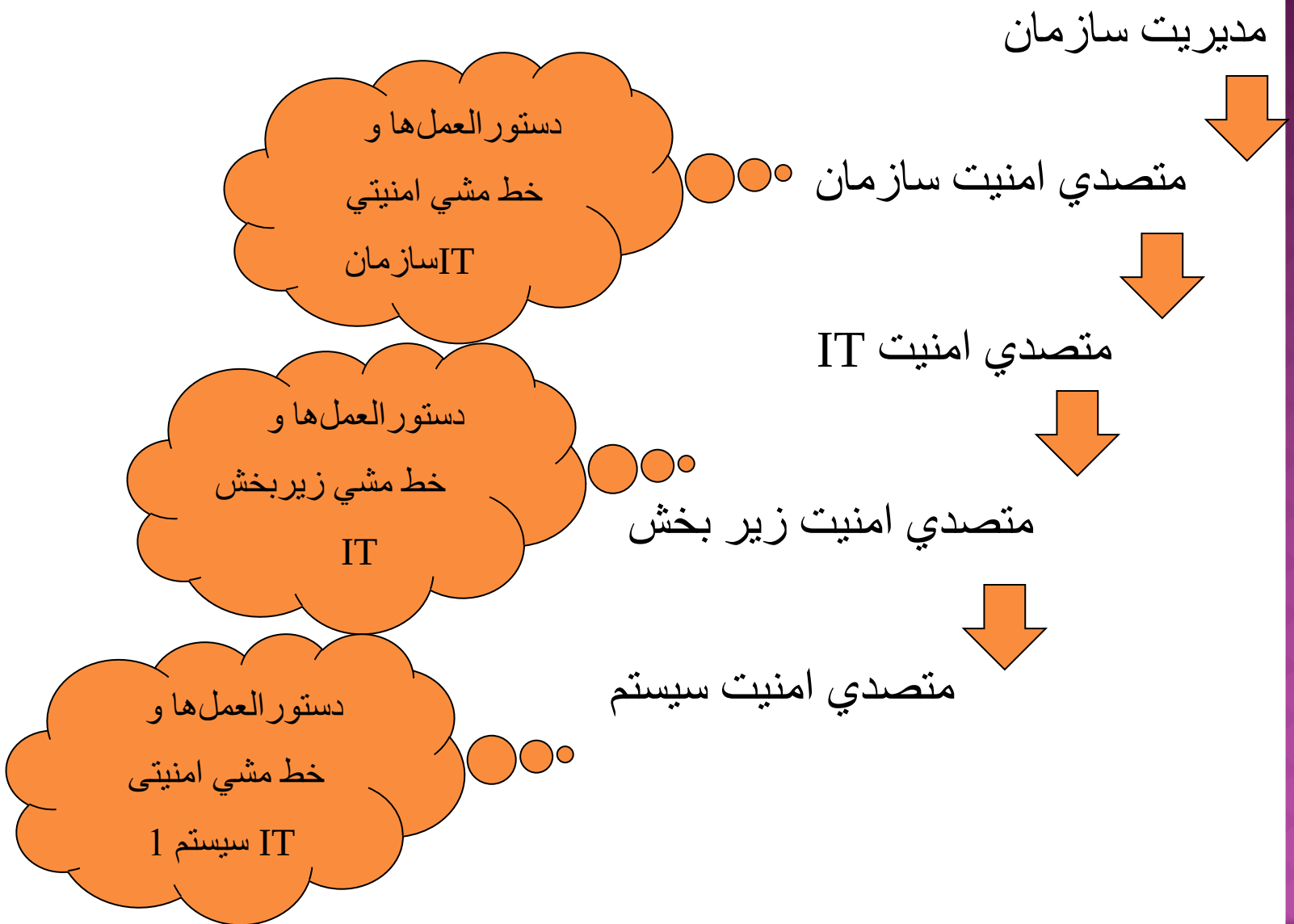
سلسله مراتب اهداف، استراتژی و خط مشی



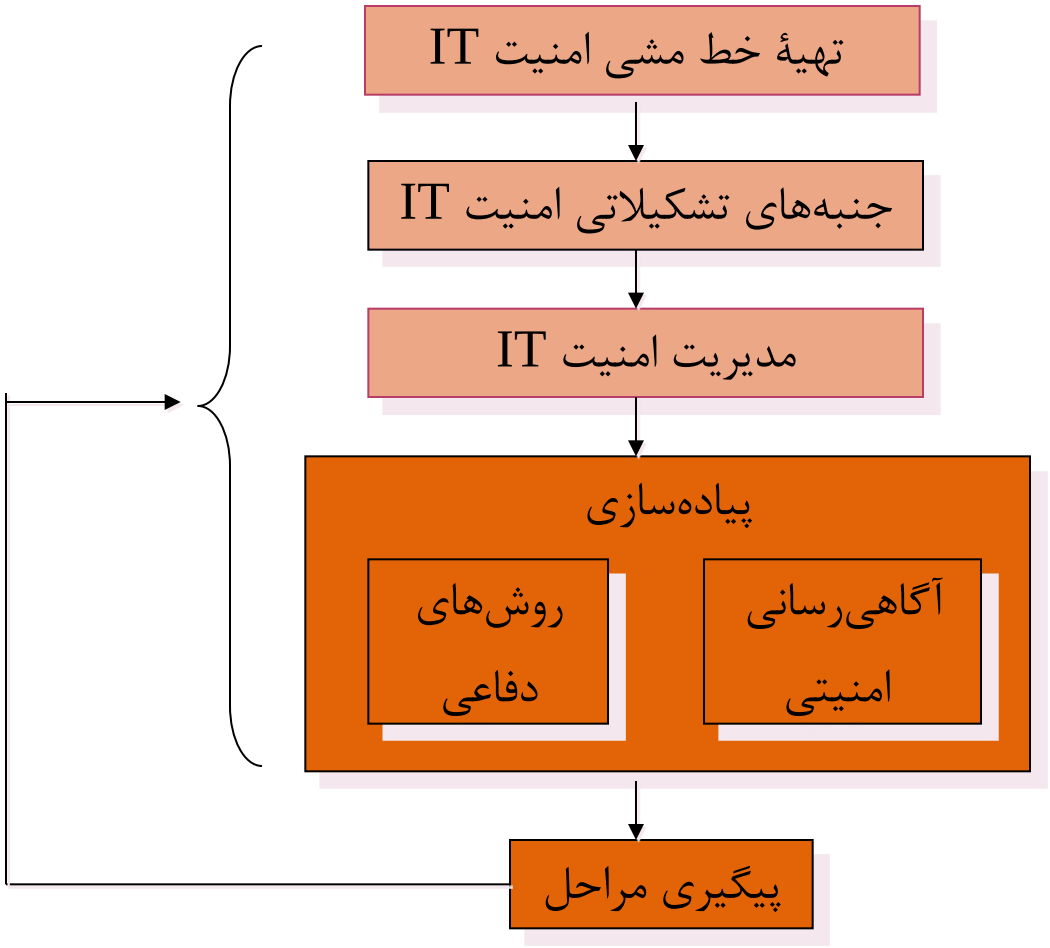
جنبه‌های تشکیلاتی امنیت IT



جنبه‌هاي تشكيلاتي امنيت IT



مدیریت امنیت IT



مدیریت امنیت IT

- مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه روزآمد نگه دارد.

- مدیریت امنیت IT شامل موارد زیر است:
  - مدیریت پیکربندی
  - مدیریت تغییرات
  - مدیریت مخاطرات

مدیریت پیکربندی

فرآیندی است برای حصول اطمینان از اینکه تغییرات در سیستم تأثیر کنترل‌های امنیتی و به تبع امنیت کل سیستم را کاهش ندهد.

مدیریت تغییرات

فرآیندی است که برای شناسایی نیازمندی‌های جدید امنیتی در هنگام بروز تغییر در سیستم IT انجام می‌شود.

- انواع تغییرات در سیستم IT :

- روال‌های جدید	- بروز رسانی نرم‌افزارها
-تجدید سخت‌افزارها	- کاربران جدید
- اتصالات جدید شبکه	- ...

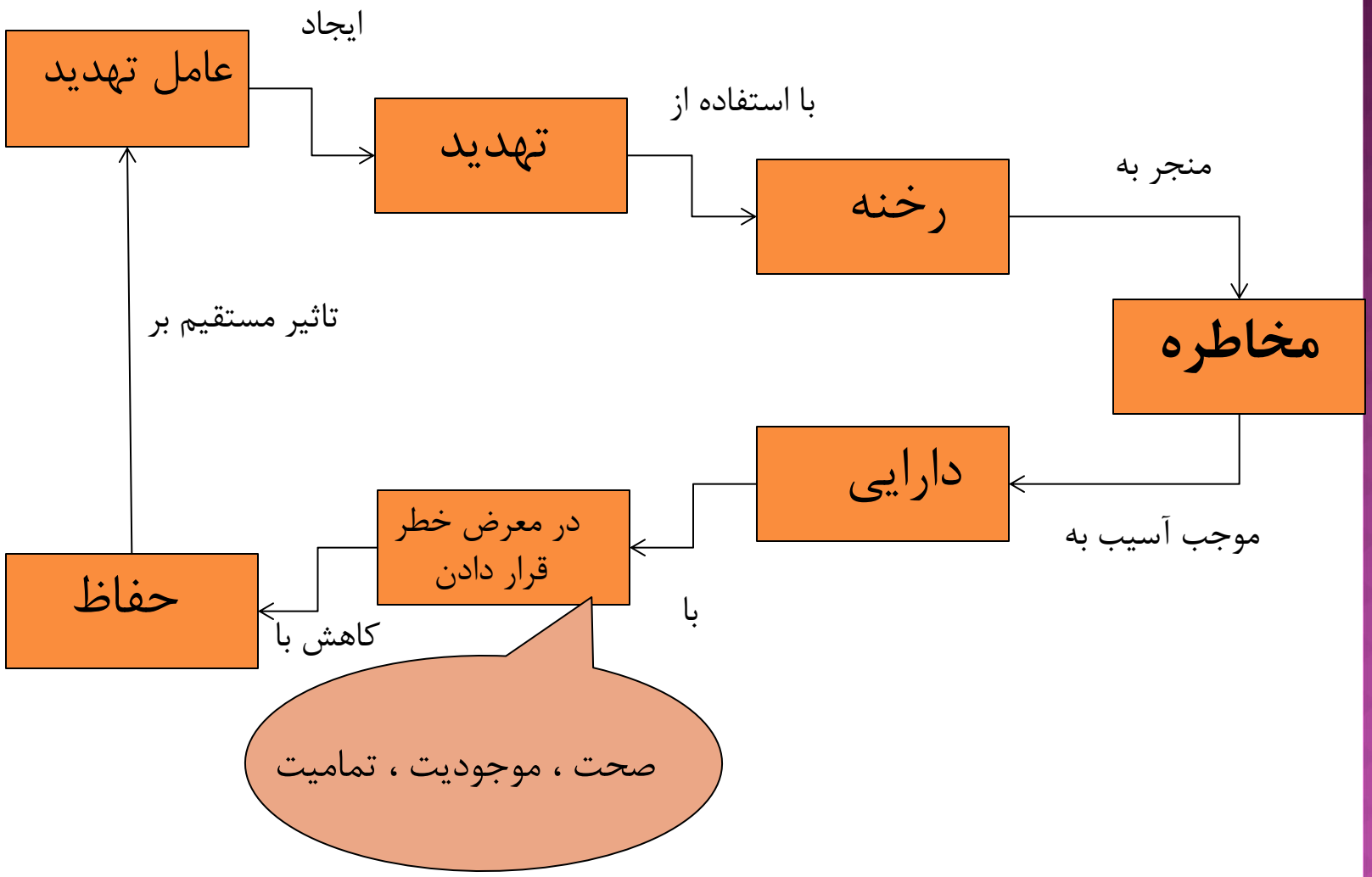
مدیریت مخاطرات

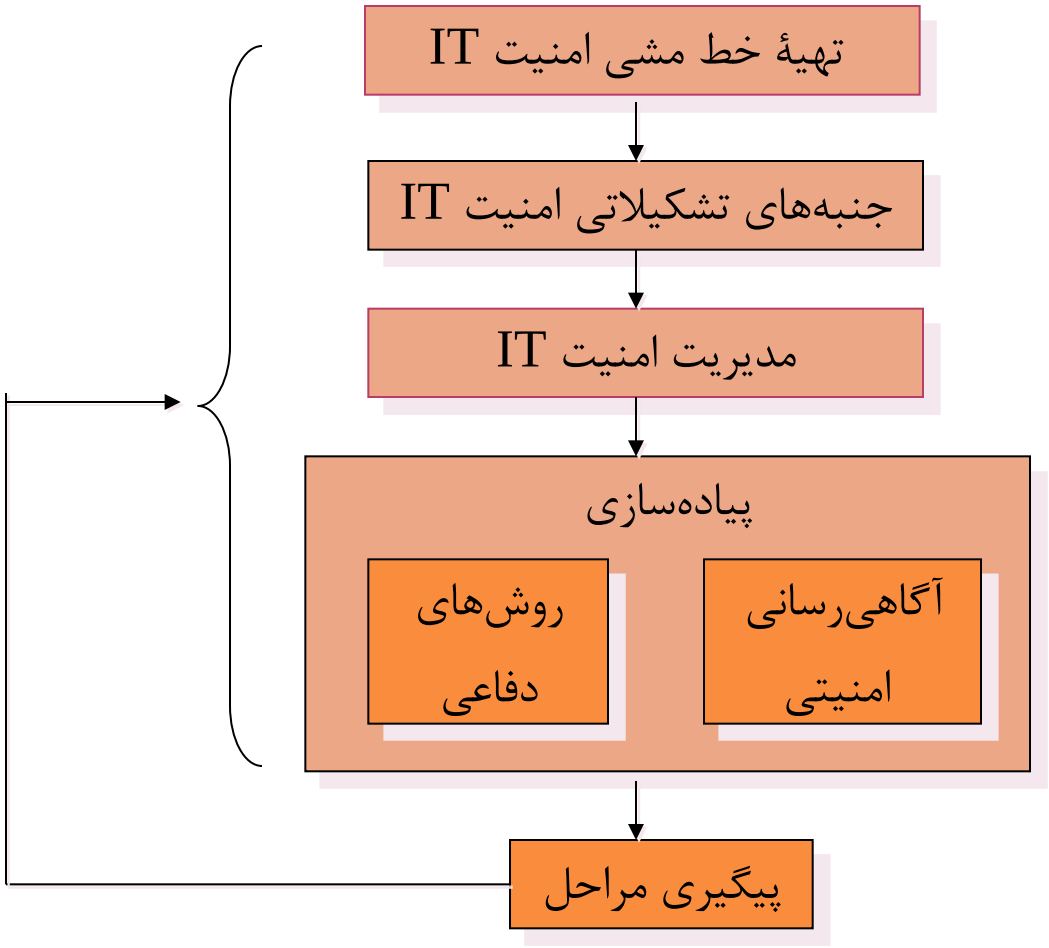
یکی از مهمترین قابلیتهای ISMS که در هر سازمانی به فراخور نیاز باید انجام می‌شود، مدیریت مخاطرات یا Risk Management است. ریسک یا مخاطره عبارت است از احتمال ضرر و زیانی که متوجه یک دارایی سازمان (در اینجا اطلاعات) می‌باشد. عدم قطعیت (در نتیجه مقیاس ناپذیری) یکی از مهمترین ویژگیهای مفهوم ریسک است. طبعا این عدم قطعیت به معنای غیر قابل محاسبه و مقایسه بودن ریسکها نیست.

مدیریت مخاطرات

- مدیریت مخاطرات فرآیندی است برای شناسایی و ارزیابی:
  - دارایی‌های که بایستی حفاظت شوند (Assets)
  - تهدیدات (Threats)
  - رخنه‌ها (Vulnerabilities)
  - آسیبها (Impacts)
  - مخاطرات (Risks)
  - روش‌های مقابله (Safeguards)
  - ریسک باقی مانده (Residual Risks)

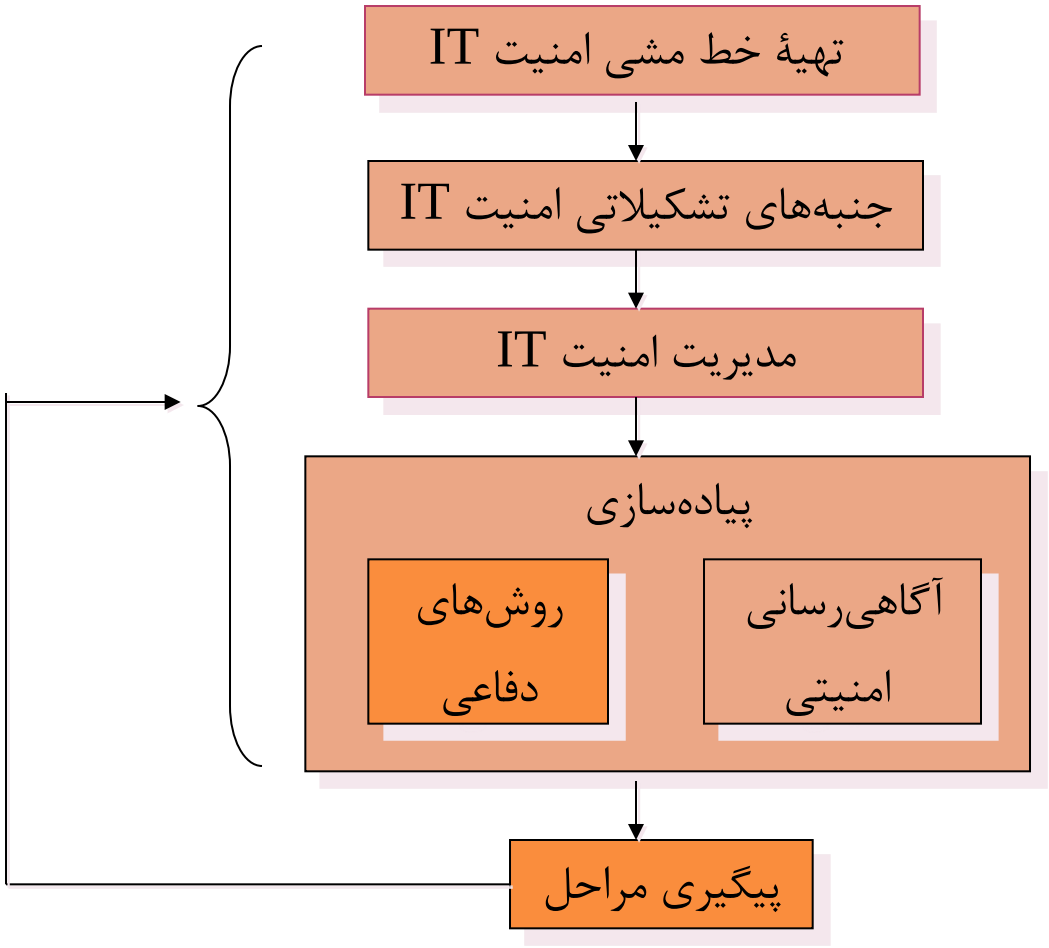
مدیریت مخاطرات





پیاده‌سازی

- آگاهی‌رسانی امنیتی
- روش‌های دفاعی



کنترل‌های امنیتی

تجربیات, روال‌ها یا مکانیزم‌های محافظت در مقابل تهدیدات

- کنترل‌های امنیتی در حوزه‌های زیر قابل اعمال هستند :

سخت‌افزار (پشتیبانی, کلیدها و ...)
نرم‌افزار (امضاء رقمی, ثبت وقایع (Log) , ابزارهای ضد ویروس)
ارتباطات (فایروال, رمزنگاری)
محیط فیزیکی (نرده و حفاظ و ...)
پرسنل (آگاهی رسانی و آموزش, روال‌های استخدام, عزل و استعفا و ...)
کنترل استفاده از سیستم‌ها (احراز اصالت, کنترل دسترسی و ...)

کنترل‌های امنیتی از یکدیگر مستقل نیستند و بایستی آنها را به صورت ترکیبی استفاده نمود.

انواع کنترل های امنیتی

- کنترلهای مدیریتی
- کنترلهای عملیاتی
- کنترلهای فنی