SECURITY

M. Rasti-Barzoki
Website: rasti.iut.ac.ir
92-2

مقدمه

- اطلاعات مانند سایر دارائی‌های سازمانی به عنوان یک دارائی مهم و باارزش برای هر سازمان به حساب می‌آید و در نتیجه نیازمند ارائه راهکارهای حفاظتی لازم برای نگهداری آنها، می‌باشند.
  - نتایج تحقیقات انجام شده، بیانگر این واقعیت است که سالانه نیمی از کاربران کامپیوتر، اطلاعات خود را به اشکال مختلف از دست می دهند. بروز نقص در تجهیزات ذخیره سازی داده ها، خطاهای انسانی، سرقت کامپیوترها، حملات ویروسی و خطاهای نرم افزاری و نیز حوادثی نظیر آتش سوزی و زلزله، از شایع ترین عوامل تخریب و از دست دادن اطلاعات و داده های کامپیوتری و دیجیتال است.
- امنیت اطلاعات به وسیله اجرای یکسری از کنترل‌های مناسب، حاصل خواهد شد. این کنترل‌ها میتوانند به صورت خط‌مشی‌ها، رویه‌ها، ساختارهای سازمانی و یا نرم‌افزارهای کاربردی باشند.

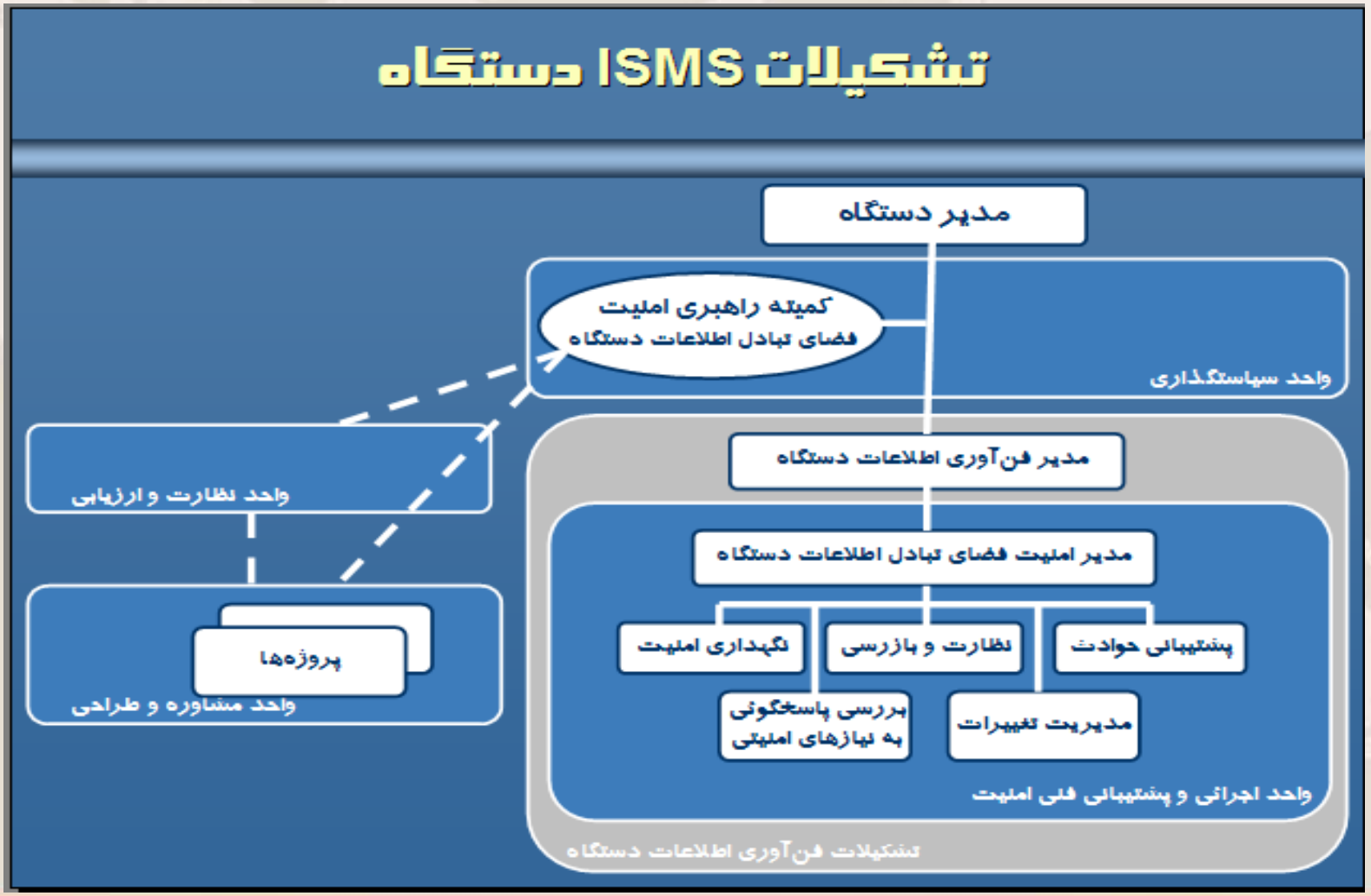
ISMSیا سیستم مدیریت امنیت اطلاعات

- تامین کننده امنیت اطلاعات در هر سازمان.
- سیستم مدیریت امنیت اطلاعات بر اساس استاندارد ISO 27001 در کنار دیگر سیستمهای مدیریت به خصوص استاندارد ISO 9001 و تحت نظارت و مدیریت مستقیم مدیریت ارشد شرکت مستقر می‌گردد.
- این سیستم برای پیاده سازی از استانداردها و متدولوژی های گوناگونی مانند ISO/IEC 17799 و ISO 15408 بهره می گیرد.

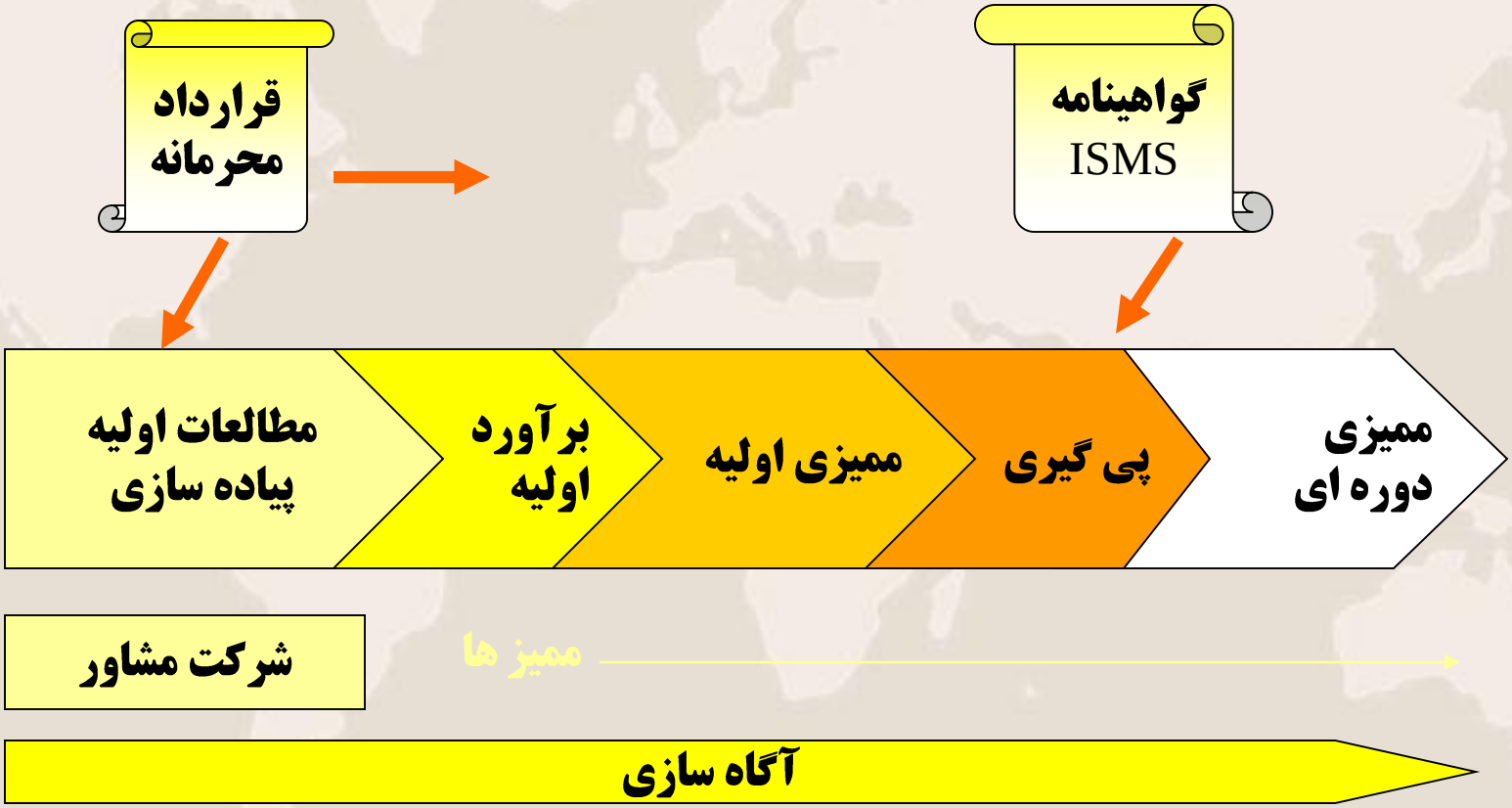
سیستم مدیریت امنیت داده ها –ISMS براساس استاندارد BS7799و27001

- **مطالب اصلی:**
  - سیستم مدیریت امنیت داده ها
  - سیاست امنیتی
  - امنیت در سازمان
  - دسته بندی و مدیریت منابع
  - امنیت کارکنان
  - امنیت فیزیکی و محیطی
  - مدیریت عملیات و ارتباطات
  - کنترل دسترسی
  - توسعه و تولید سیستم ها و نگه داری آنها
  - مدیریت تداوم فعالیت سازمان
  - بازنگری و تطبیق

اجزاء و ساختار تشکیلات امنیت اطلاعات سازمان



دریافت گواهینامه چه زمانی اتفاق میافتد؟



سیاست های امنیتی

امنیت سخت افزار، وسائل جانبی و دیگر تجهیزات

- **زیر بخش شماره یک: خرید و نصب سخت افزار**
  - مشخص کردن نیازمندیهای امنیت شبکه و اطلاعات برای سخت افزارهای جدید
  - مشخص کردن نیازمندیهای کاربردی تفصیلی برای (تهیه) سخت افزار جدید
  - نصب سخت افزار جدید
  - تست سیستمها و تجهیزات

- **زیر بخش شماره دو: کابل کشی، UPS، پرینترها و مودم‌ها**
  - تهیه برق دائم و پیوسته برای تجهیزات حیاتی و حساس
  - مدیریت و نگهداری مولد برق جانشین
  - استفاده از ماشینهای فاکس/ Fax modems
  - استفاده از مودم‌ها/ اتصالات DSL و ISDN
  - استفاده از پرینترهای منفرد، تحت شبکه و یا مرکزی
  - نصب و نگهداری کابل های شبکه

سیاست های امنیتی

امنیت سخت افزار، وسائل جانبی و دیگر تجهیزات

- **زیر بخش شماره سه: مواد مصرف شدنی در حوزه فناوری اطلاعات**
  - کنترل مواد مصرف شدنی در حوزه فناوری اطلاعات
  - استفاده از رسانه‌های ذخیره سازی قابل پاک شدن (مانند دیسکت‌ها و CD ها)
- **زیر بخش شماره چهار: کار بصورت برون‌سپاری فرآیندها و فعالیت‌های کاری**
  - برون سپاری فعالیت‌ها
  - اختصاص Laptop / کامپیوترهای قابل حمل به پرسنل
  - انتقال سخت افزارها از مکانی به مکان دیگر
  - استفاده از تلفن‌های موبایل
  - استفاده از تسهیلات مرکزی سازمان

سیاست های امنیتی

امنیت سخت افزار، وسائل جانبی و دیگر تجهیزات

- **زیر بخش شماره پنج: استفاده از محل‌های ذخیره‌سازی امن**
  - استفاده از مکانهای ذخیره سازی قفل‌دار
- **زیر بخش شماره شش: مستند سازی سخت افزار**
  - مدیریت و استفاده از مستندات سخت افزاری
  - نگهداری لیست اموال تجهیزات سخت افزاری

سیاست های امنیتی

- زیر بخش شماره هفت: سایر موارد امنیتی مربوط به سخت افزارها
  - کنترل تجهیزات منسوخ و از رده خارج شده
  - ثبت و گزارش خطاهای سخت افزاری
  - بیمه تجهیزات سخت افزاری
  - خاموشی میز/ صفحه پاک
  - log on / Log off
  - نگهداری سخت افزارها به دو صورت onsite و offsite
  - آسیب رساندن به تجهیزات

سیاست های امنیتی

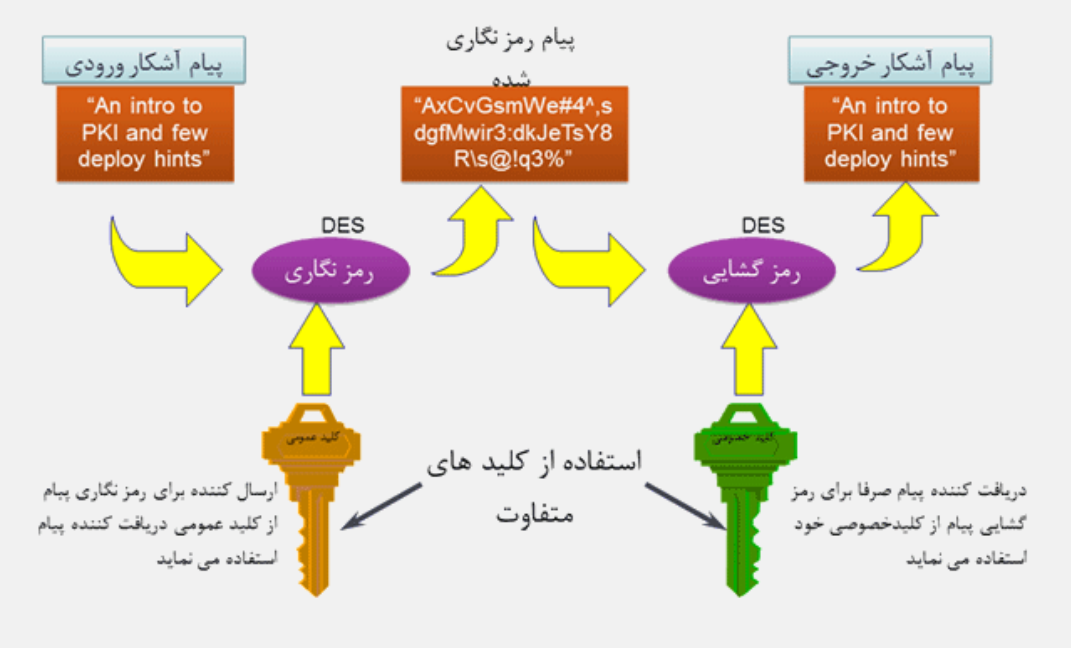
کنترل دسترسی به اطلاعات و سیستم‌ها

- مدیریت استانداردهای کنترل دسترسی
- مدیریت دسترسی کاربر
- امنیت ایستگاههای کاری بدون مراقبت
- مدیریت کنترل‌های دسترسی به شبکه
- کنترل دسترسی به نرم‌افزارهای سیستم عامل
- مدیریت پسوردها
- امنیت در مقابل دسترسی‌های فیزیکی غیر مجاز
- محدود کردن دسترسی‌ها
- بازبینی دسترسی‌های سیستمی و استفاده از آنها
- اختصاص دسترسی به مستندات و فایل‌ها
- مدیریت دسترسی سیستم‌هایی با ریسک بالا
- کنترل دسترسی کاربر از راه دور

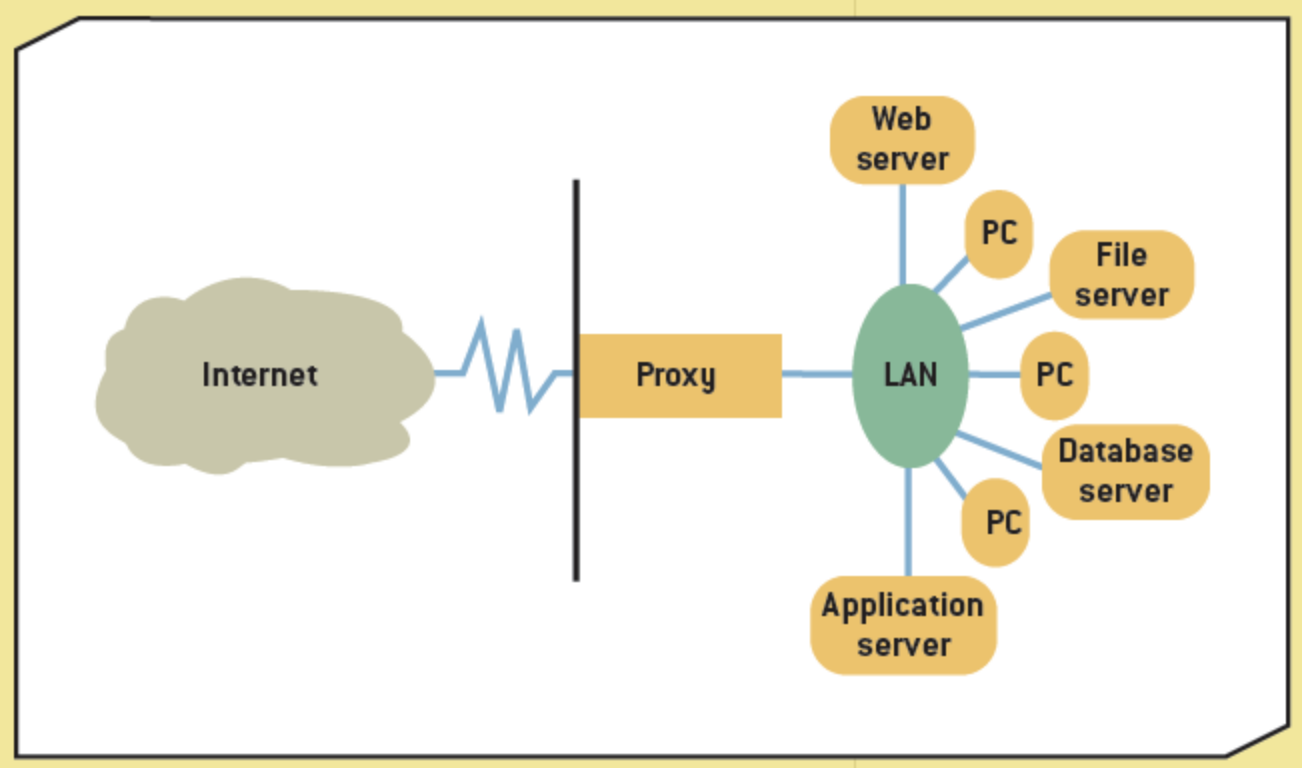
Security

- **زیر ساخت کلید عمومی / نظام مدیریت امنیت داده ها(نماد)**

– زیر ساخت کلید عمومی یا PKI، معمولا به مجموعه ای از استانداردها،سیستم ها و روش هایی اطلاق می گردد که هدف از بکارگیری آنها، شناسایی و تعیین هویت و اعتبار اشخاصی است که از طریق یک یا چند شبکه ارتباطی اقدام به ارسال پیام و یا انجام تراکنش های مالی و غیر مالی می نمایند.



Management Information Systems



مثال (فعالیت های یک شرکت)

- **بازیابی اطلاعات دیجیتال بر مبنای مکانیزم تهیه نسخه های پشتیبان**
  - طراحی و پیاده سازی روال های تهیه نسخه های پشتیبان از داده های دیجیتال
  - مانیتورینگ روال های تهیه نسخه های پشتیبان از لحاظ صحت عملکرد
  - آزمایش نسخه های پشتیبان از لحاظ یکپارچگی و کارایی
- **حفاظت از داده های دیجیتال در برابر تخریب و دسترسی غیر مجاز**
  - پیاده سازی سطوح دسترسی به داده ها
  - پیاده سازی مکانیزم های رمز نگاری بر روی داده ها
- **تامین امنیت سیستم های کامپیوتری**
  - پیاده سازی حداقل الزامات امنیتی بر روی سیستم های کامپیوتری برای مقابله با تهدیدهای نرم افزاری
  - مانیتورینگ سیستم های کامپیوتری از لحاظ امنیت و صحت عملکرد مکانیزم های امنیتی
- **ذخیره سازی امن و پایدار داده های کامپیوتری**
  - پیاده سازی مکانیزم های پایدار ذخیره سازی داده ها بر روی کامپیوتر سرور
  - مانیتورینگ مکانیزم ها و تجهیزات ذخیره سازی داده ها از لحاظ صحت و کیفیت عملکرد
  - مدیریت طول عمر تجهیزات ذخیره سازی داده ها

پیامبر صلی الله علیه و آله:

اقربکم غدا منّی فی الموقف اصدقکم للحدیث و ادّاکم للامانة و اوفاکم بالعهد و احسنکم خلقا و اقربکم من النّاس.

نزدیک ترین شما به من در قیامت،

راستگوترین، امانتدارترین، وفادارترین به عهد، خوش اخلاق ترین و نزدیک ترین شما به مردم است.

(بحارالأنوار، ج75، ص94، ح12)

پایان