امن سازی فضای تبادل اطلاعات سازمان‌ها:

رویکردها و راهکارها

بهروز ترک لادانی

مسئول امنیت شبکه شرکت پیام‌پرداز – عضو هیات علمی گروه کامپیوتر دانشگاه اصفهان

ladani@eng.ui.ac.ir

دیماه ۱۳۸۸

پیام‌پرداز

طرح مسئله

- امنیت شبیه ترمز است:
  - ✓ وظیفه آن کند کردن است
  - ✓ ولی هدف آن بالا بردن امکان تند رفتن!

با مشکلات مدیریتی، بودجه‌ای، پرسنلی، مطلع تخصصی و امکانات سازمان سازگار باشد...

استاندارد و سیستماتیک (سامان یافته) باشد...

- به سرعت در سازمان ما است در حالی که از مخاطرات امنیتی این فناوری بیمناکیم.
  - ✓ آیا رویکرد علمی و عملی مناسبی برای برخورد با آن وجود دارد؟

www.payampardaz.net

به دنبال یک رویکرد علمی ...

- 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 سیستماتیک در یک سازمان انجام می‌شود.

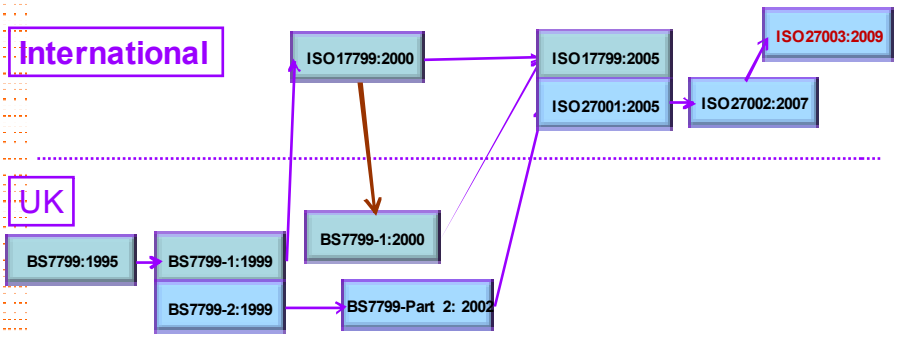
چرخه حیات توسعه سیستم های امنیتی
Security Systems Development Life Cycle (SSDLC)

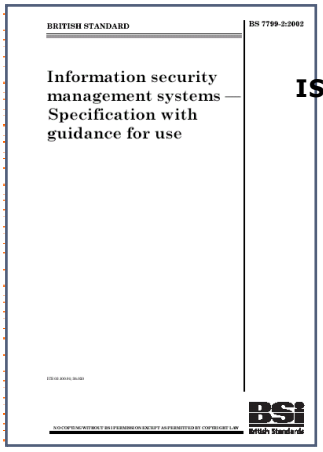
- **یک روش سنتی برای ایجاد امنیت به صورت سیستماتیک**
- **مراحل:**
  - بررسی و شناخت (سیاست های سازمانی، روال ها و ...)
  - تحلیل مخاطرات امنیتی
  - طراحی منطقی (معماری امنیتی، استفاده از استانداردها و ...)
  - طراحی فیزیکی (انتخاب تکنولوژی، نوع پیکربندی اجزاء سیستم و ...)
  - پیاده سازی
  - نگهداری و مدیریت تغییرات

سیستم مدیریت امنیت اطلاعات (ISMS)

- **رویکردی جدیدتر مبتنی بر استاندارد ISO 17799**
  - یک متدولوژی ساخت‌یافته و معتبر بین‌المللی است.
  - یک فرآیند تعریف شده برای ارزیابی، پیاده‌سازی، نگهداری و مدیریت امنیت اطلاعات ارائه می‌کند.
  - مجموعه‌ای از سیاستها، استانداردها، روالها و رهیافت‌های متناسب با اغلب سازمانها را ارائه می‌کند.
- **سیستم مدیریت امنیت اطلاعات**
  - ISMS یک الگوی سامان یافته برای مدیریت اطلاعات حساس سازمان است تا از امنیت آنها اطمینان حاصل شود.

تاریخچه استانداردهای ISMS

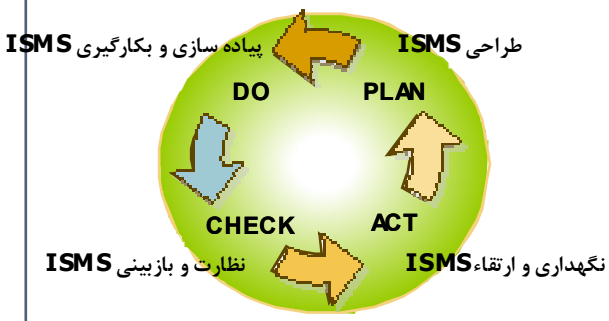



BRITISH STANDARD

BS 7799-2:2002

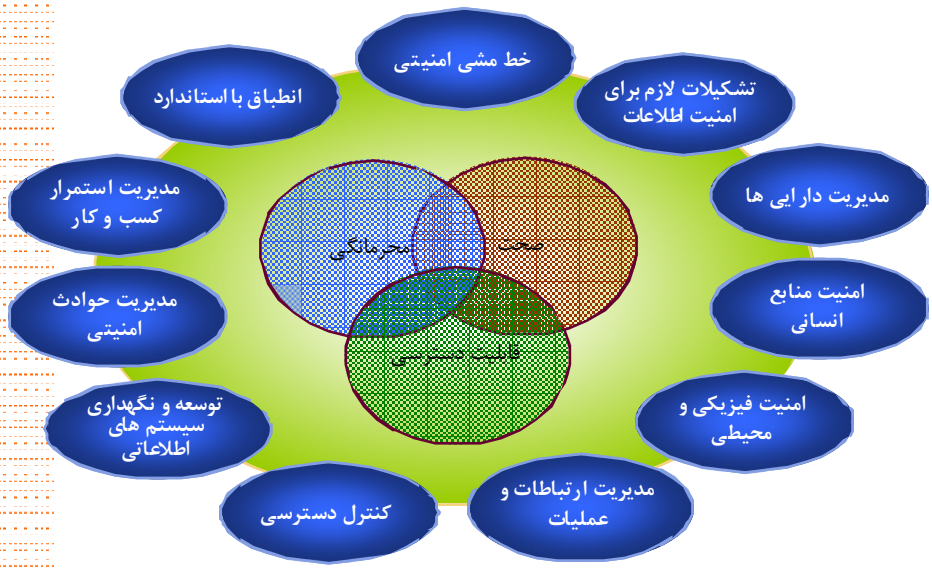
Information security management systems — Specification with guidance for use

مدل PDCA

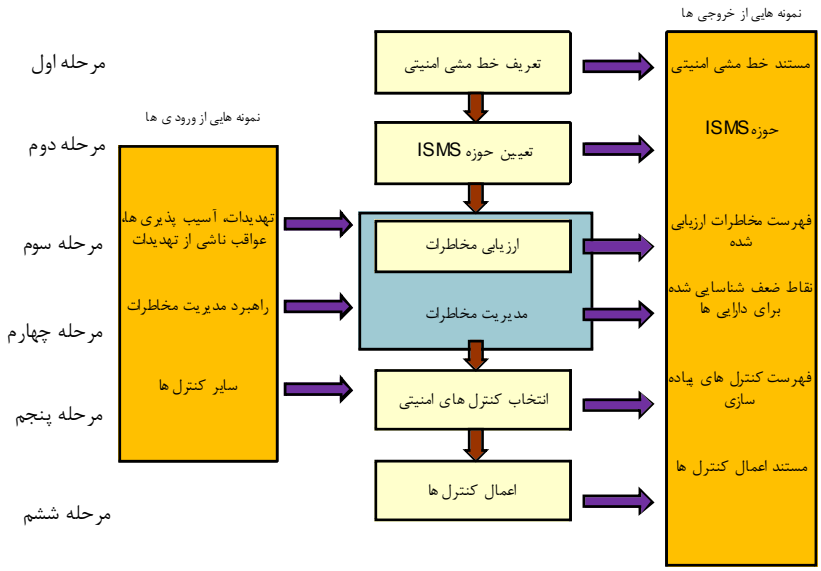


چارچوب کلی ارتقاء مستمر مدیریت امنیت اطلاعات در سازمان

یازده بخش اصلی در استاندارد ISO 17799



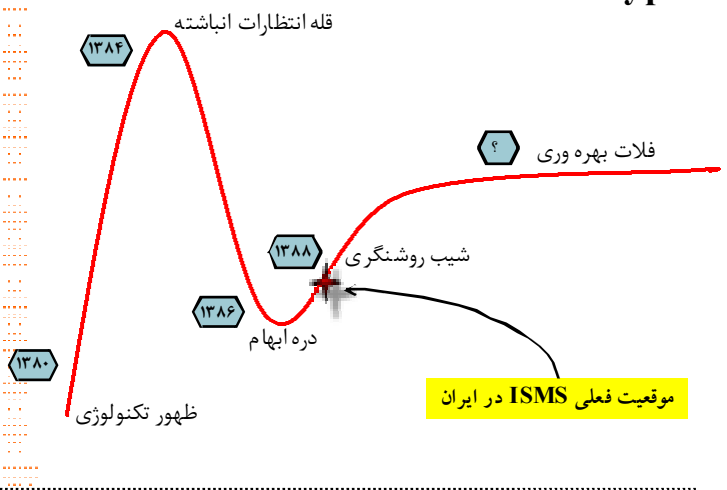
فرآیند اجرای ISMS



آیا رویکرد علمی مطرح شده عملی است؟

ISMS در ایران

- چرخه Hype



www.payampardaz.net

آماده نبودن برای شروع پروژه ISMS

- نرسیدن سازمان به سطح مناسب **بلوغ سازمانی**
- فرایندگرا نبودن سازمان و یا نداشتن فرایندهای سالم
- عدم آگاهی مدیریت نسبت به ضرورت امنیت
- فقدان زیر ساخت مناسب فناوری اطلاعات
- اولویت نداشتن امنیت در سازمان
- ندادن آگاهی به شیوهٔ مناسب (و به میزان کافی) به افراد در سازمان

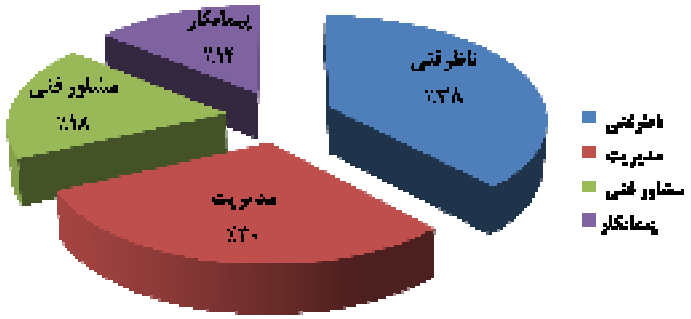
مشکلات در نحوه اجرای پروژه

- عدم اطمینان به سرانجام پروژه
- عدم تخصیص بودجه کافی
- عدم وجود یک متولی خاص برای ISMS
- عدم استفاده از مشاور جهت تحلیل نیازها، تهیه RFP و ...
- عدم بهره‌گیری از کمک ناظر در پروژهٔ ISMS
- فقدان تخصص و تجربه کافی شرکت های پیمانکار

ترک لادانی، موزرانی، میرعلایی، شیخ زین الدین، تأملی بر چالش های استقرار ISMS در سازمان های دولتی ایران، مجله تکفا –ویژه نامه امنیت اطلاعات، آذر و دی ماه ۱۳۸۶

www.payampardaz.net

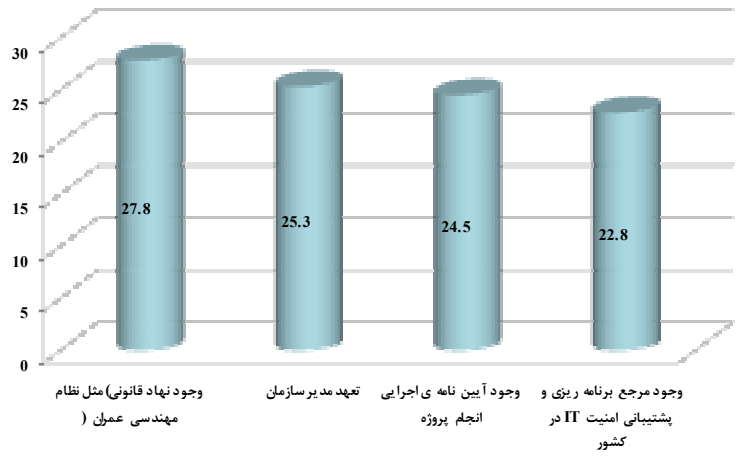
نقش نسبی ارکان پروژه امن سازی در سازمان



صدرعاملی، چالش یابی و ارائه راهکار های مناسب استقرار ISMS در سازمان ها با الگو برداری از نظام های موفق مهندسی در کشور، پایان نامه کارشناسی ارشد در حال انجام

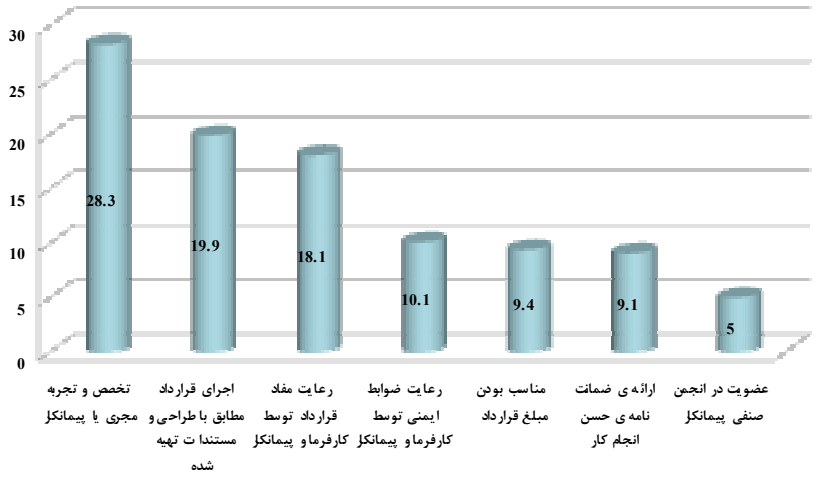
www.payampardaz.net

نقش نسبی پارامترهای مدیریتی مؤثر بر پروژه امن سازی



www.payampardaz.net

نقش نسبی پارامترهای اجرایی (پیمانکار) مؤثر بر پروژه امن سازی



www.payampardaz.net

به نظر می رسد رویکرد علمی با شرایط موجود چندان عملی نیست .... راه حل چیست؟

- حرکت به سمت رفع مشکلات و موانع مدیریتی در سازمان ها
  - ✓ ارتقاء بلوغ سازمانی
  - ✓ توسعه زیرساخت فناوری اطلاعات
  - ✓ ایجاد نظام های مناسب اجرای پروژه (کارفرما، مشاور، ناظر، پیمانکار)
  - ✓ ارتقاء سطح تخصص پیمانکاران
  - ✓ ....
- توجه به **رویکرد امنیت پایه**

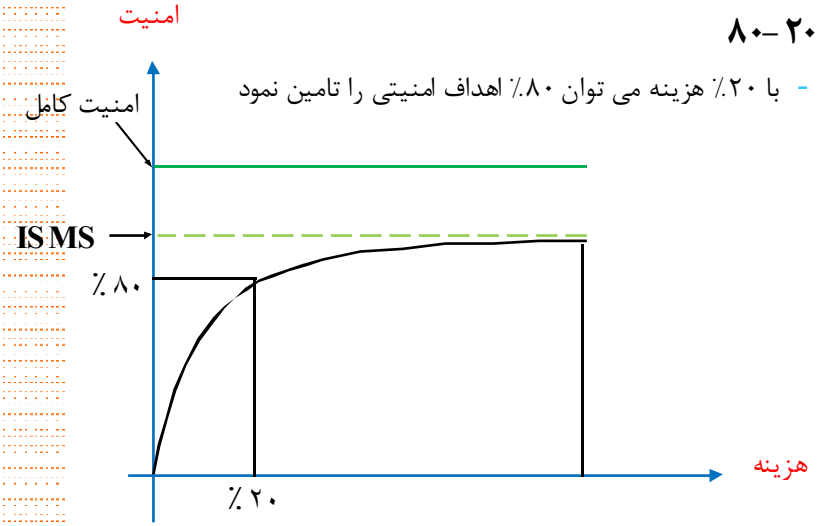
www.payampardaz.net

- مجموعه ای حداقلی از کنترل ها متناسب با بودجه و سطح پذیرش سازمان برای امن سازی بخشهای حساس فناوری اطلاعات سازمان تعیین و پیاده سازی شود.

مزایا	معایب
۱- نیاز به حداقل بودجه و امکانات دارد ۲- به صرفه است (Cost-effective) ۳- در حداقل زمان ممکن قابل انجام است. ۴- تجربه سازمان ها قابل استفاده مجدد است	۱- تعیین این مجموعه حداقلی زیاد آسان نیست ۲- در اثر تغییر نیازمندی های سازمان و تغییر تکنولوژی این مجموعه تغییر می کند.

- **تعادل بین:**
  - امنیت مورد نیاز در سازمان
  - بودجه سازمان
  - میزان بلوغ سازمانی
- **نحوه دستیابی به نقطه تعادل**
  - بررسی وضعیت محیطی، اهداف و ماموریت ها و اندازه سازمان
  - استفاده از تجربه سازمان های مشابه
  - استانداردها و توصیه نامه ها (از قبیل مجموعه کنترل های فنی ISO 177799)

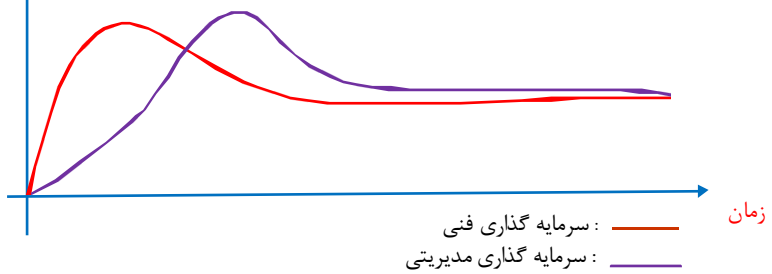
- **قانون ۲۰-۸۰**
  - با ۲۰٪ هزینه می توان ۸۰٪ اهداف امنیتی را تامین نمود



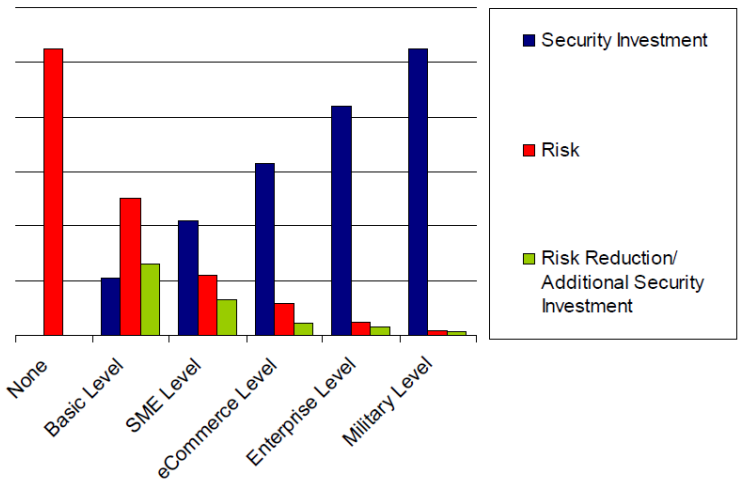
www.payampardaz.net

www.payampardaz.net

- **بر خلاف رویکرد ISMS با سرمایه گذاری بر کنترل های فنی شروع کنیم!**
  - کنترل های فنی فعال کننده انگیزه های مدیریتی است
  - قابلیت های بالفعل بیشتری در بین پیمانکاران وجود دارد
  - تمایل بیشتری بر شروع از این کنترل ها در سازمانها وجود دارد
- **نباید از کنترل های مدیریتی در ادامه غافل شد!**
- **قیاس: تغییر از متدلوژی آبشاری بهRUP در مهندسی نرم افزار**



ISM3 - Information Security Management Maturity Model



با تشکر

با تشکر