بسمه تعالی

مدیریت امنیت اطلاعات

ISMS

بخش چهارم

محاسبه و ارزیابی ریسک های امنیت اطلاعات



دکتر سیدرضا کامل

دکتری مهندسی شبکه و ارتباطات

دانشیار و عضو هیات علمی گروه کامپیوتر

دانشگاه آزاد اسلامی واحد مشهد

بهار ۱۴۰۵

سرفصل ها ...

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑
- مدیریت ریسک (Risk Management - RM) ☑

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑
- مدیریت ریسک (Risk Management - RM) ☑
- محاسبات و ارزیابی ریسک ها (Risk Calculation) ☑

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑
- مدیریت ریسک (Risk Management - RM) ☑
- محاسبات و ارزیابی ریسک ها (Risk Calculation) ☑
- مدیریت ریسک های امنیت اطلاعات (Information Security Risk Management)

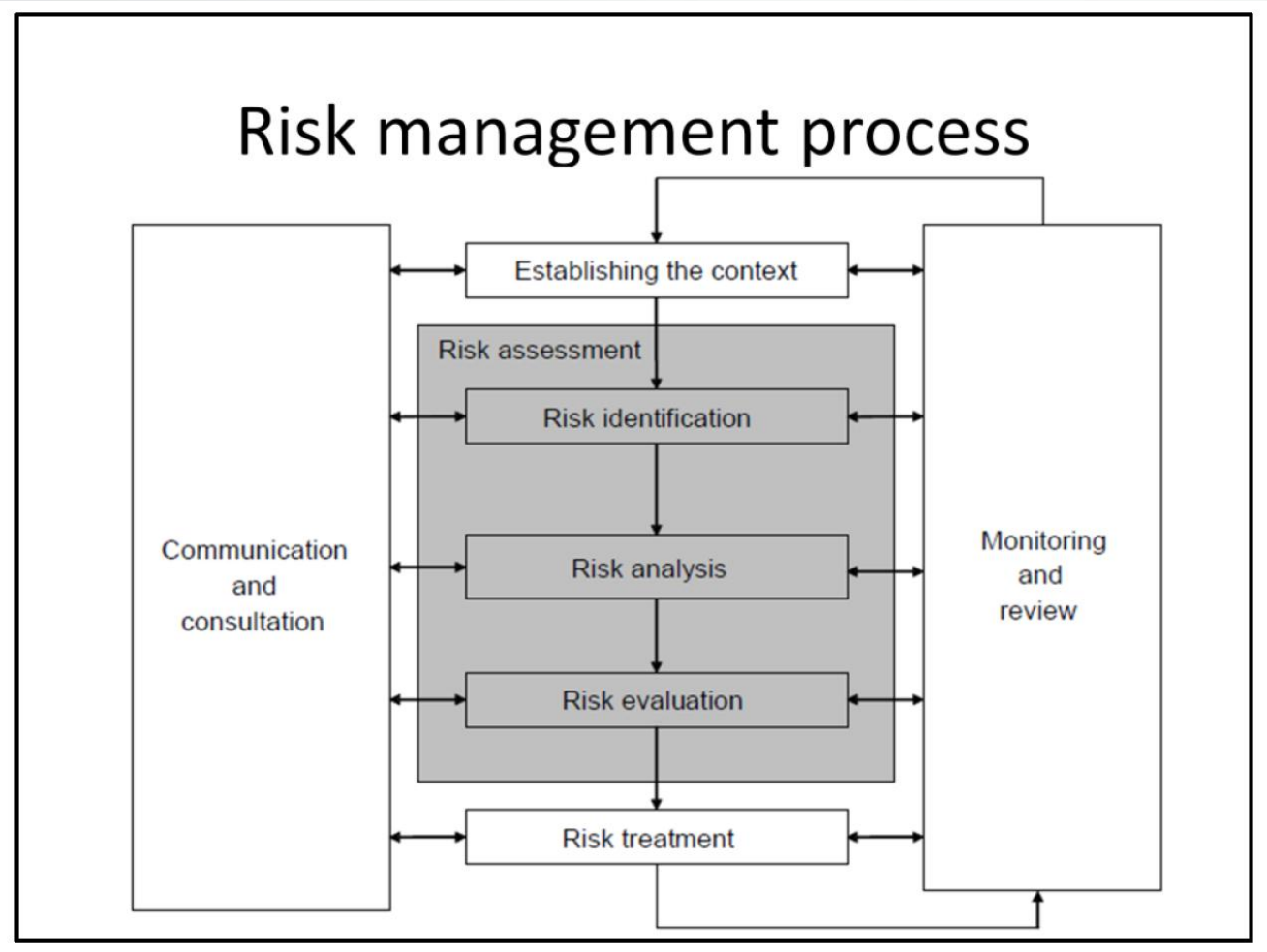
مدیریت ریسک های امنیت اطلاعات (ISRM)

مدیریت ریسک های امنیت اطلاعات (ISRM)

فرایندهای کلی مدیریت ریسک های امنیت اطلاعات (طبق استاندارد ISO 27000) ...

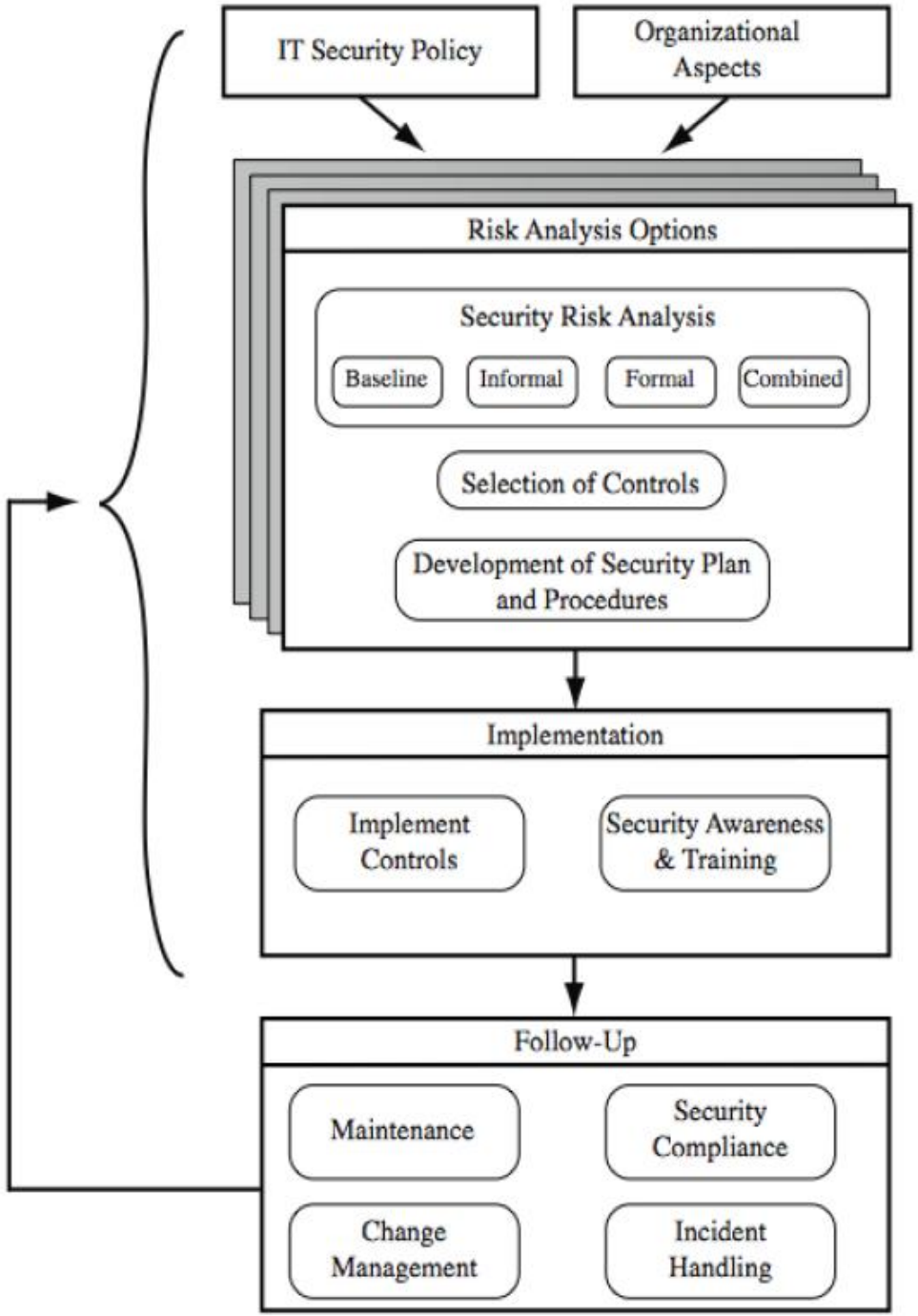


مدیریت ریسک (یادآوری ...)



مدیریت ریسک های امنیت اطلاعات (ISRM)

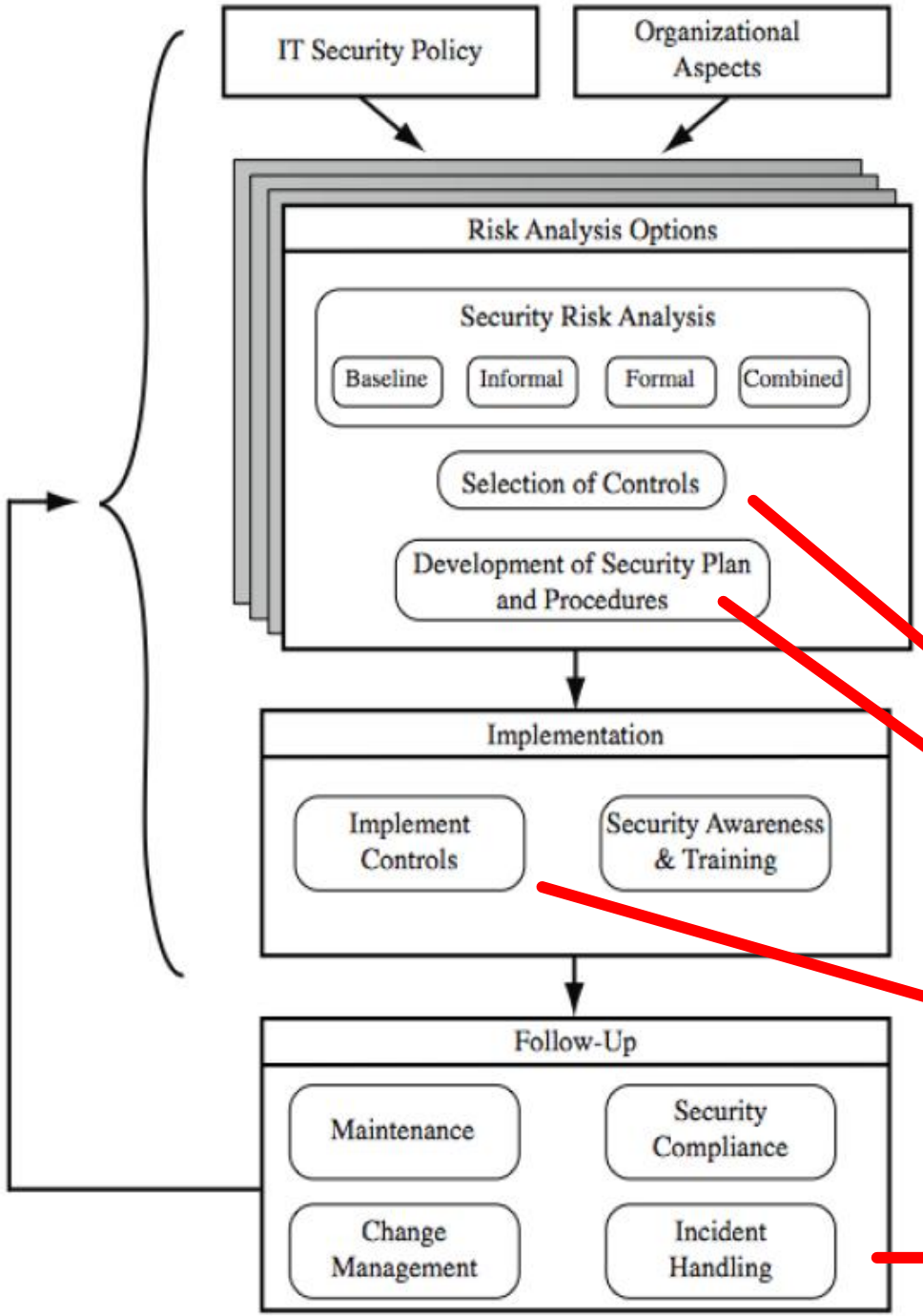
فرایندهای کلی مدیریت ریسک امنیت اطلاعات در سطح کلان سازمان

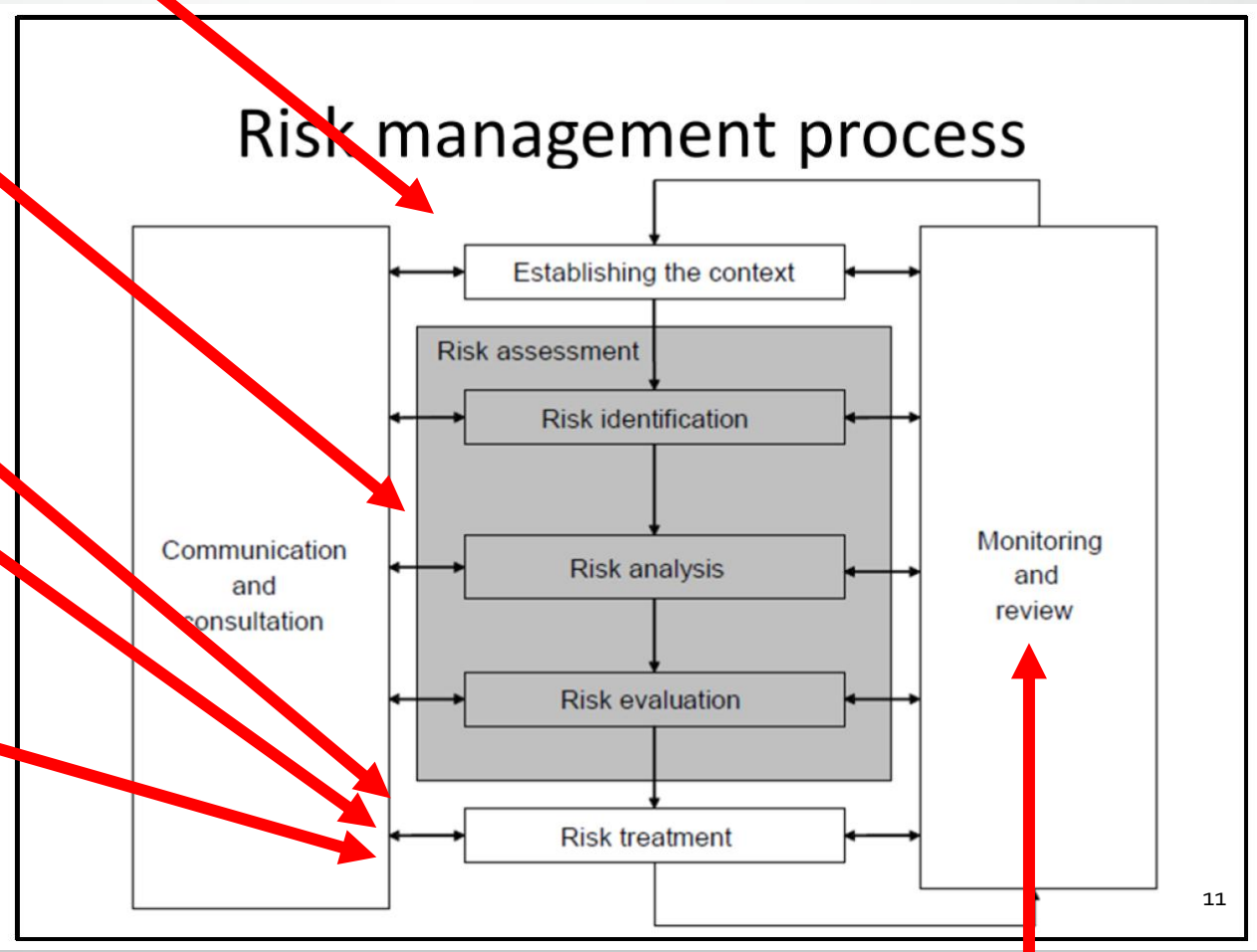


مدیریت ریسک های امنیت اطلاعات (ISRM)

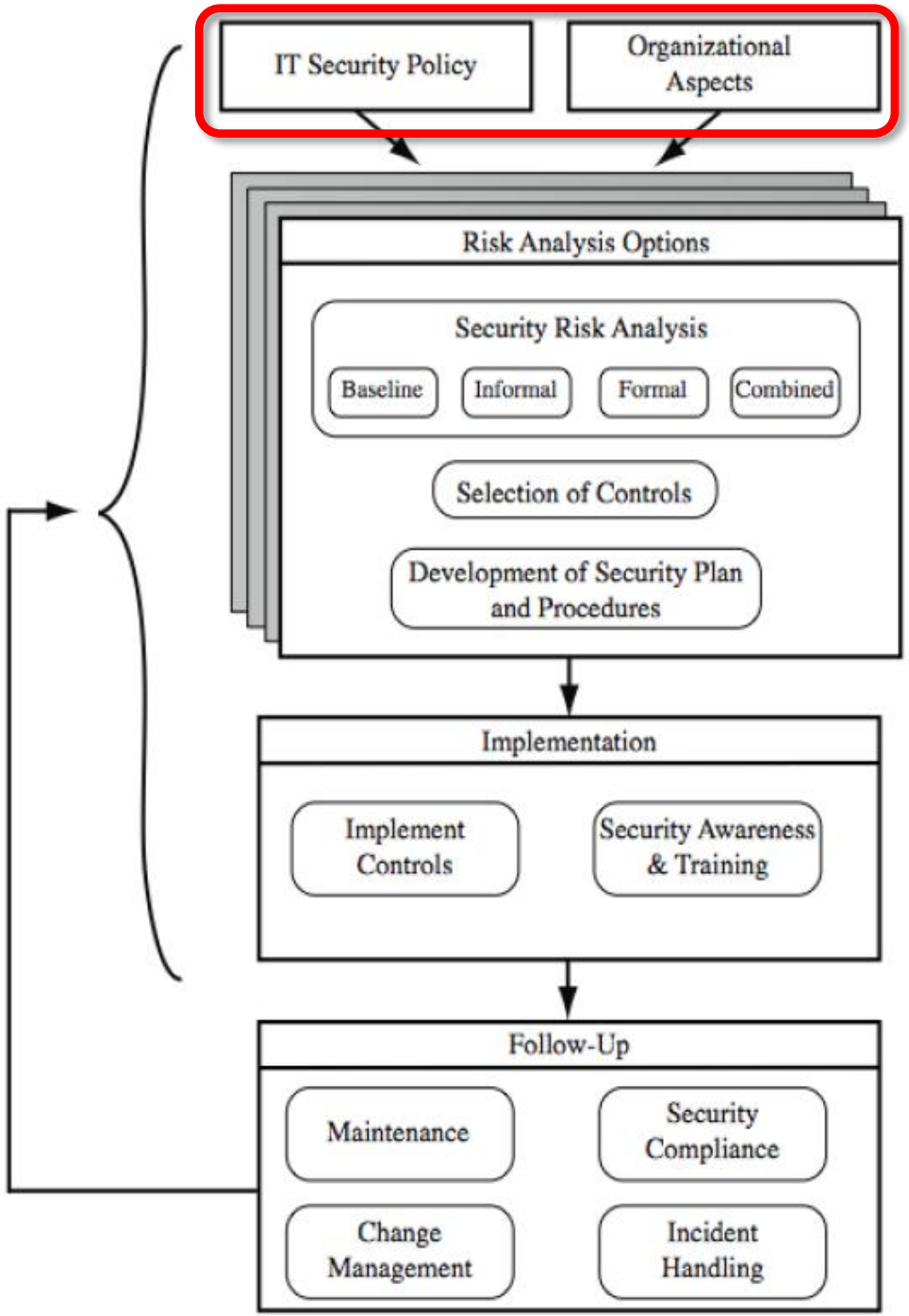
نگاشت فرایندهای کلی مدیریت ریسک امنیت اطلاعات در سطح کلان سازمان

به فرایندهای کلی مدیریت ریسک





مدیریت ریسک های امنیت اطلاعات (ISRM)



مدیریت ریسک های امنیت اطلاعات (ISRM)

IT Security Policy

Organizational Aspects

سیاست های کلان
فن اوری اطلاعات

درک سازمان، شرایط و
کسب و کار





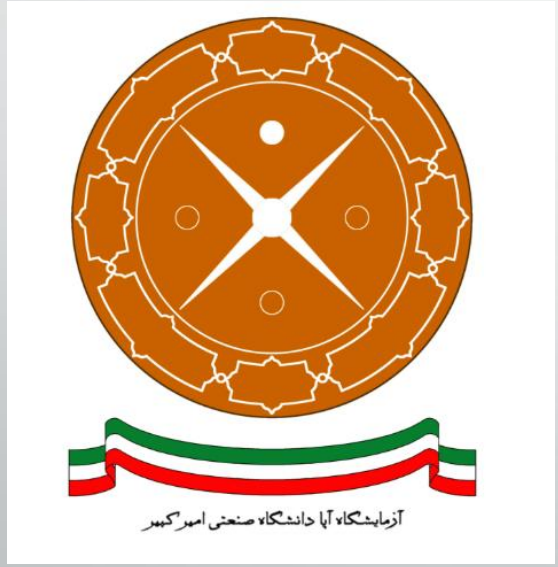


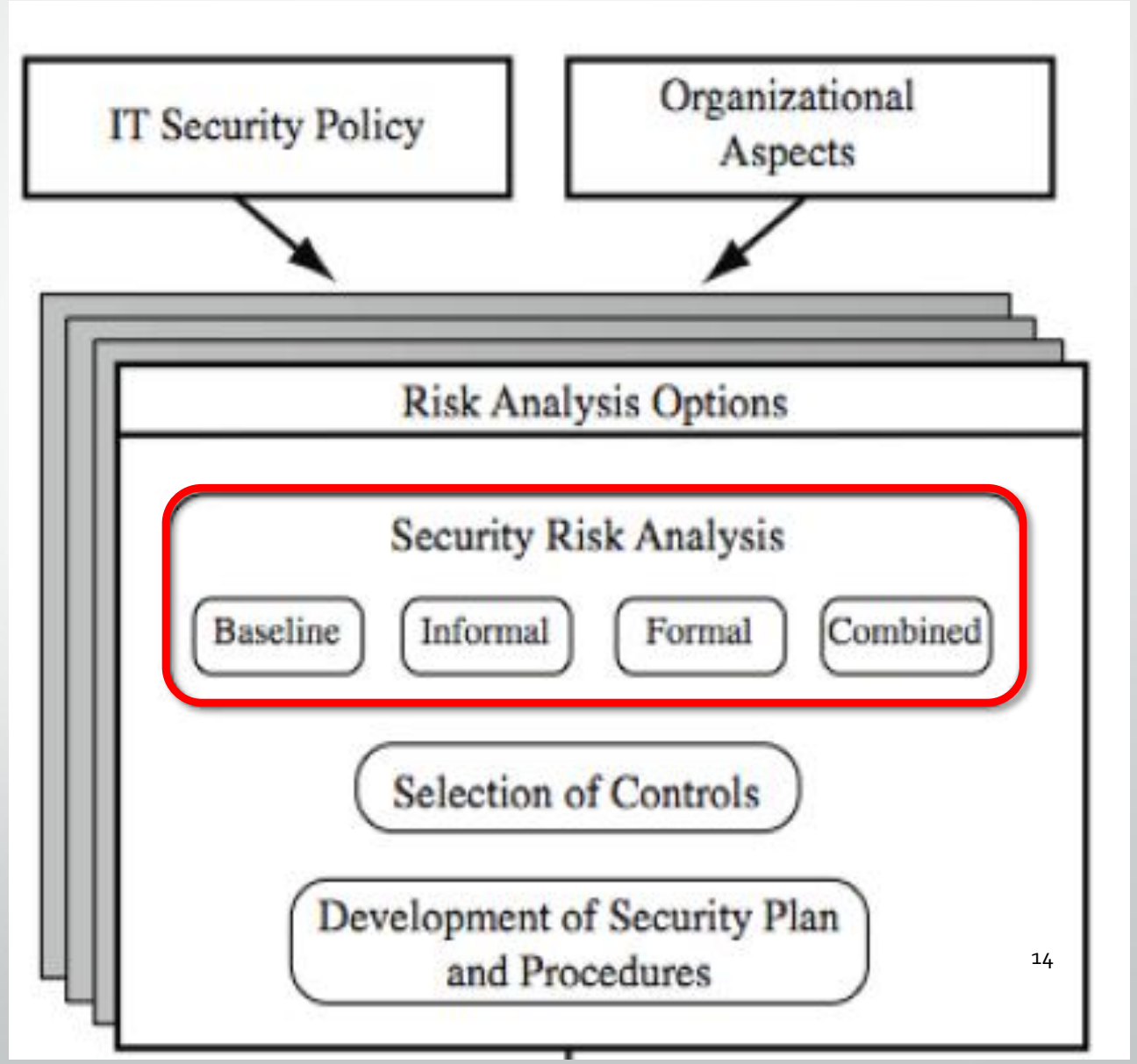


- سرویس های حیاتی سازمان
- شرایط جغرافیایی ، منطقه ای، سیاسی و اجتماعی
- میزان اهمیت اعتبار (اهمیت برند) و دارایی های سازمان (مالی)
- میزان اهمیت امنیت برای سازمان
- منابع موجود و منابع آماده تخصیص به حوزه پدافند غیرعامل (اعتبار)
- توجه به قوانین، مقررات و چهارچوب های الزام کننده یا محدود کننده

مدیریت ریسک های امنیت اطلاعات (ISRM)



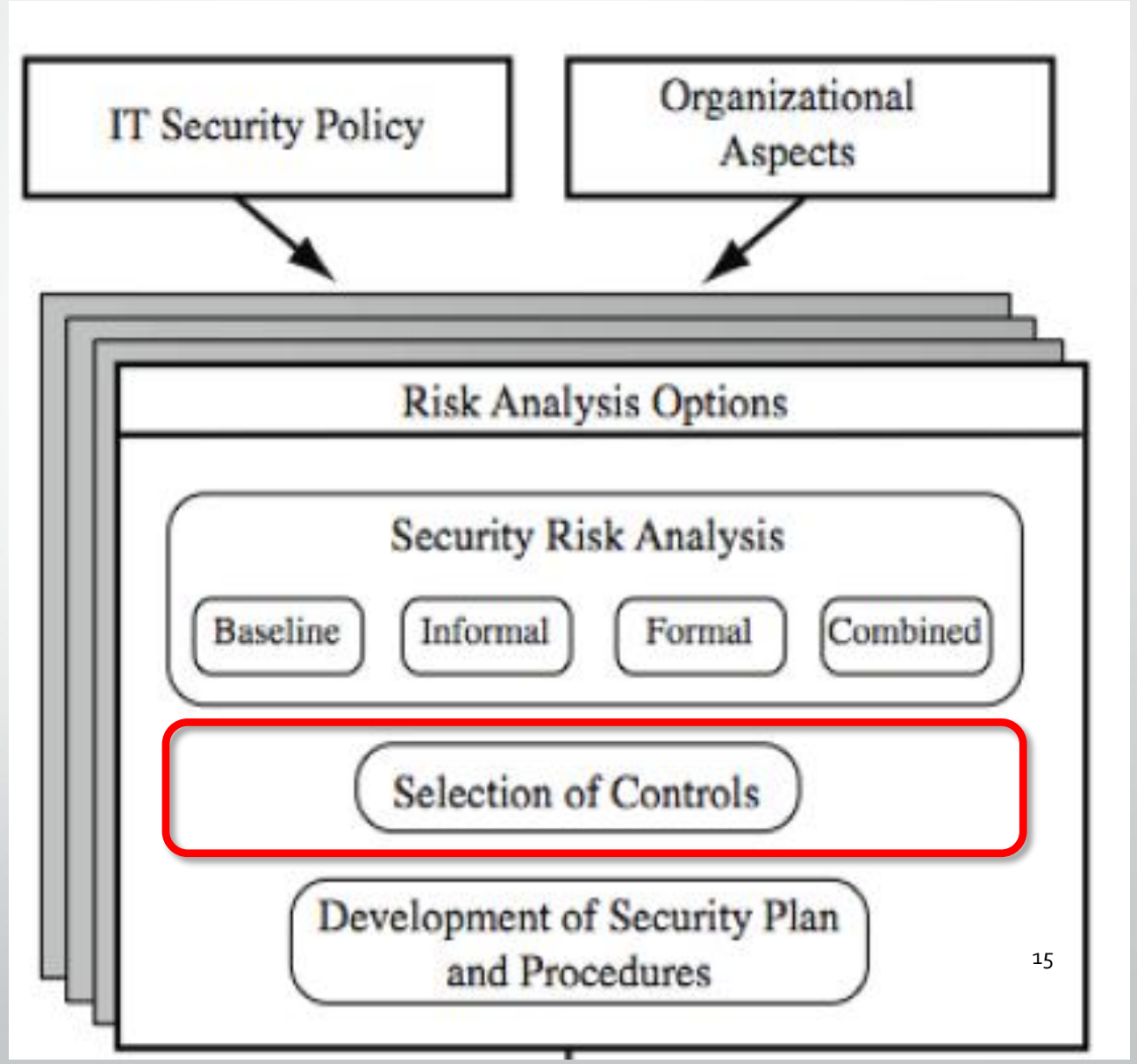




مدیریت ریسک های امنیت اطلاعات (ISRM)

کنترل ها مرتبط با ...

- Network شبکه
- Operating system سیستم های عامل
- Database and Data داده ها و پایگاه داده
- Application برنامه های کاربردی و نرم افزارها
- Environment Physical محیط فیزیکی
- Staff نیروها و منابع انسانی

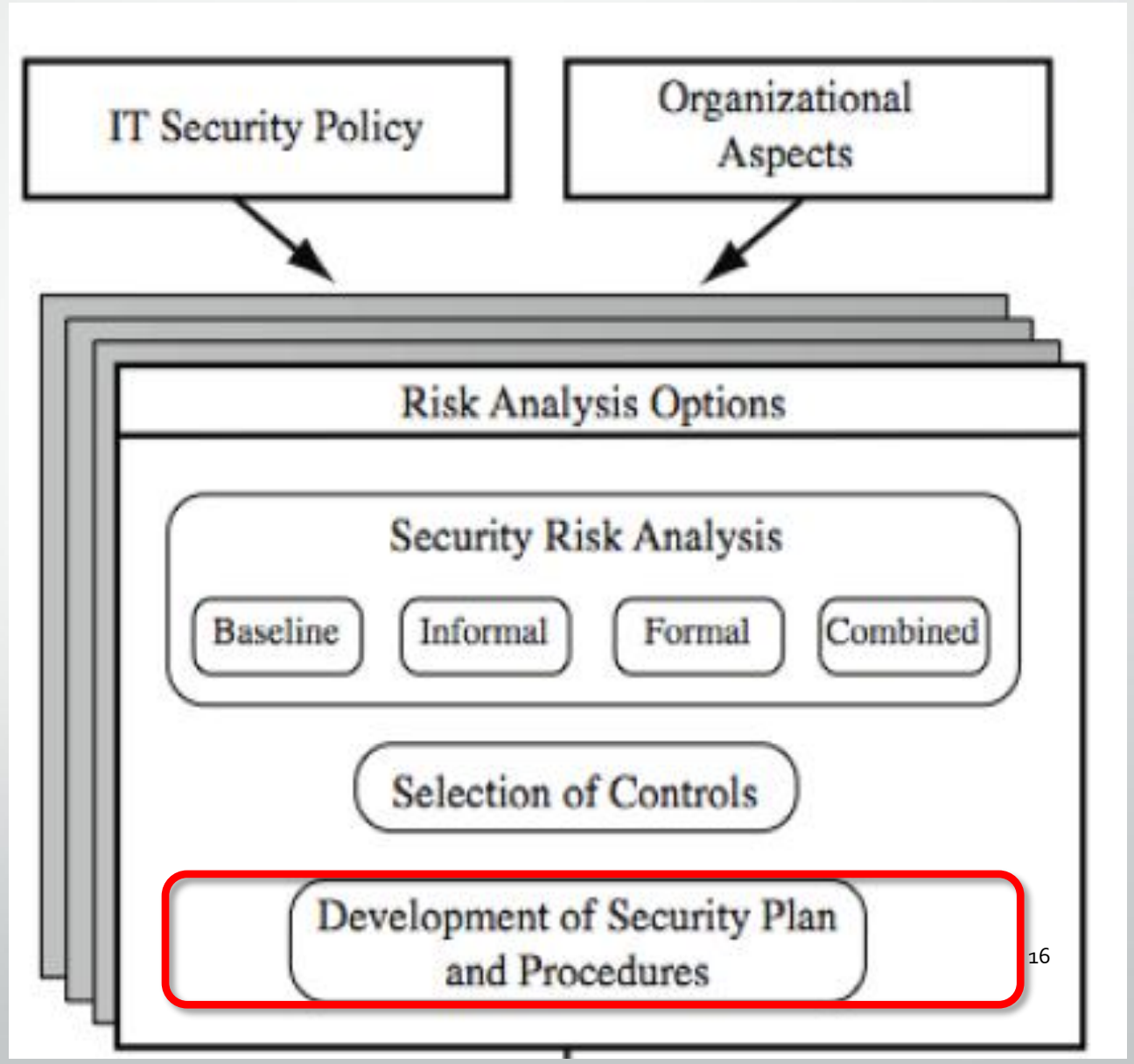


مدیریت ریسک های امنیت اطلاعات (ISRM)



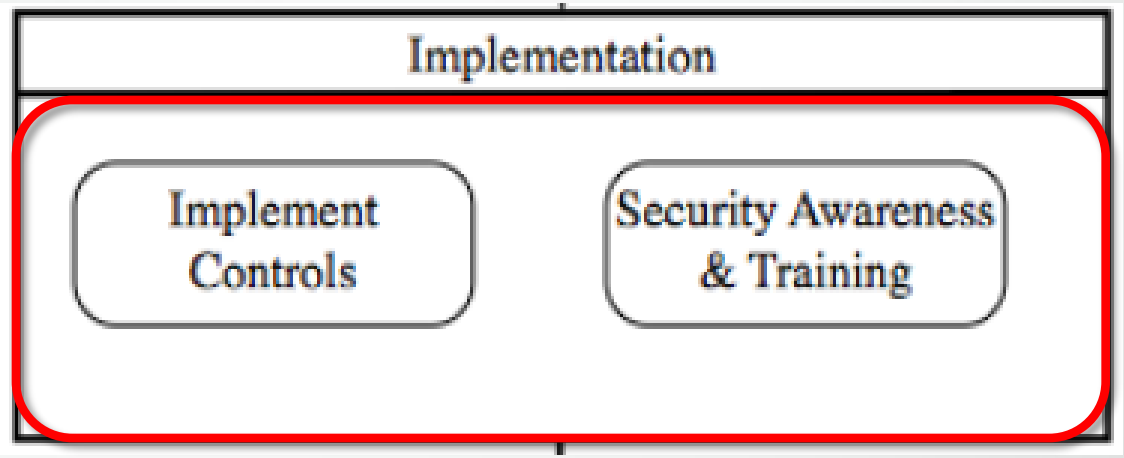






مدیریت ریسک های امنیت اطلاعات (ISRM)



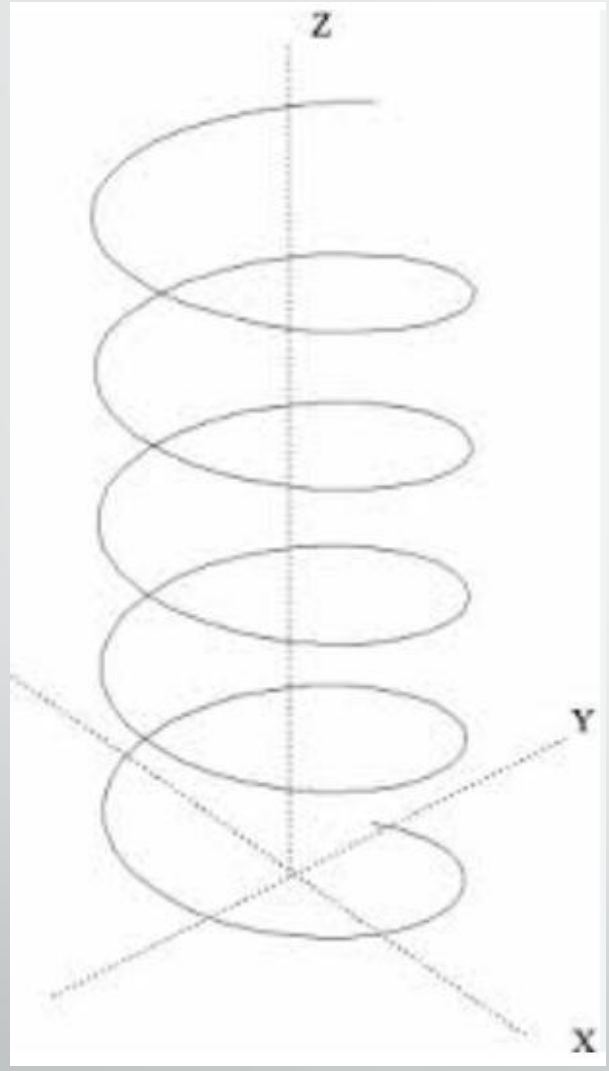


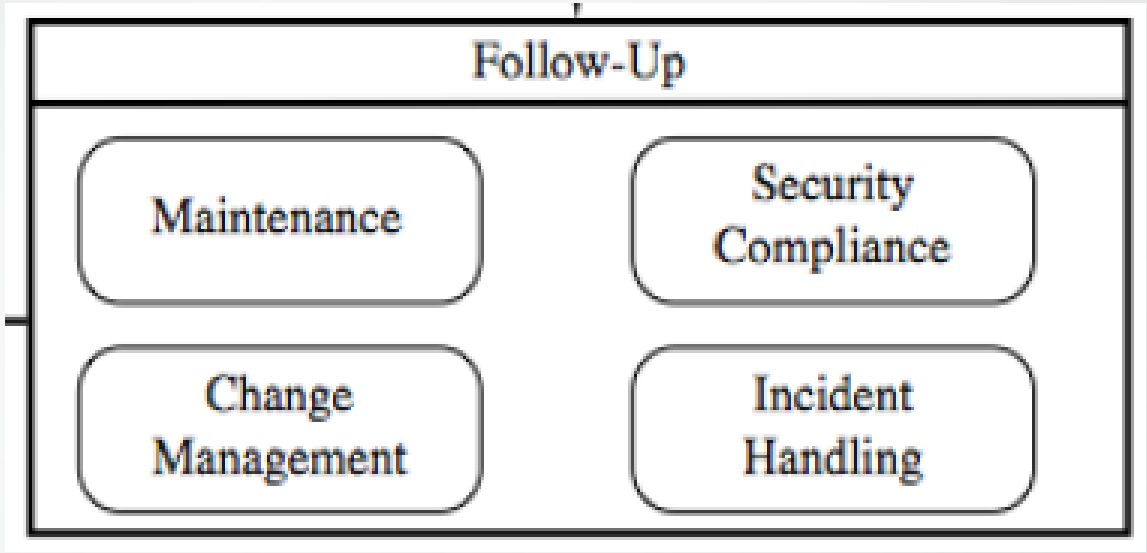
و اما ... فرهنگ سازی /
همراهی نیروهای سازمان
(ایمان نه اجبار)





مدیریت ریسک های امنیت اطلاعات (ISRM)









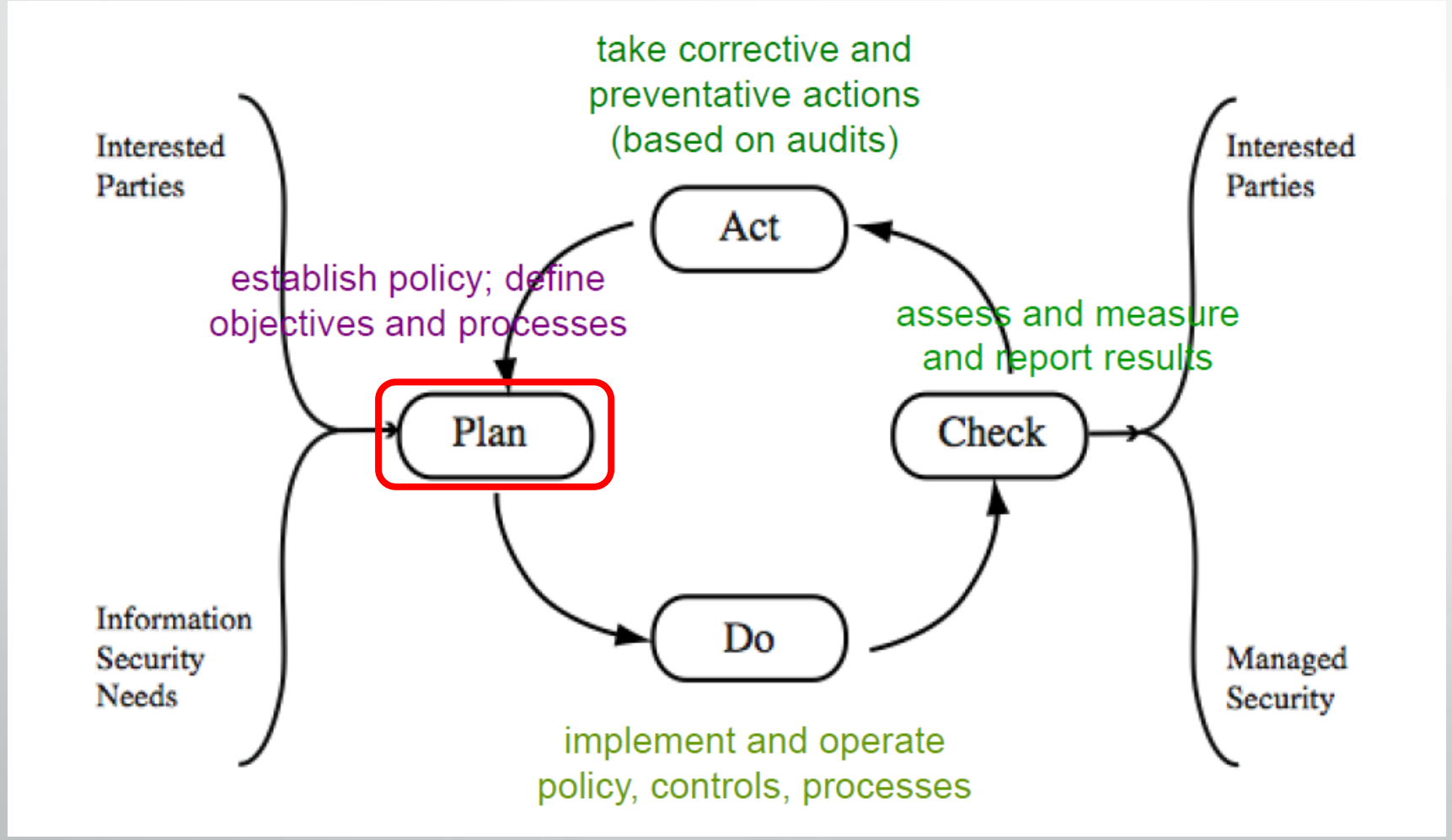


مدیریت ریسک های امنیت اطلاعات (ISRM)

چرخ تکراری آقای دمینگ (PDCA)

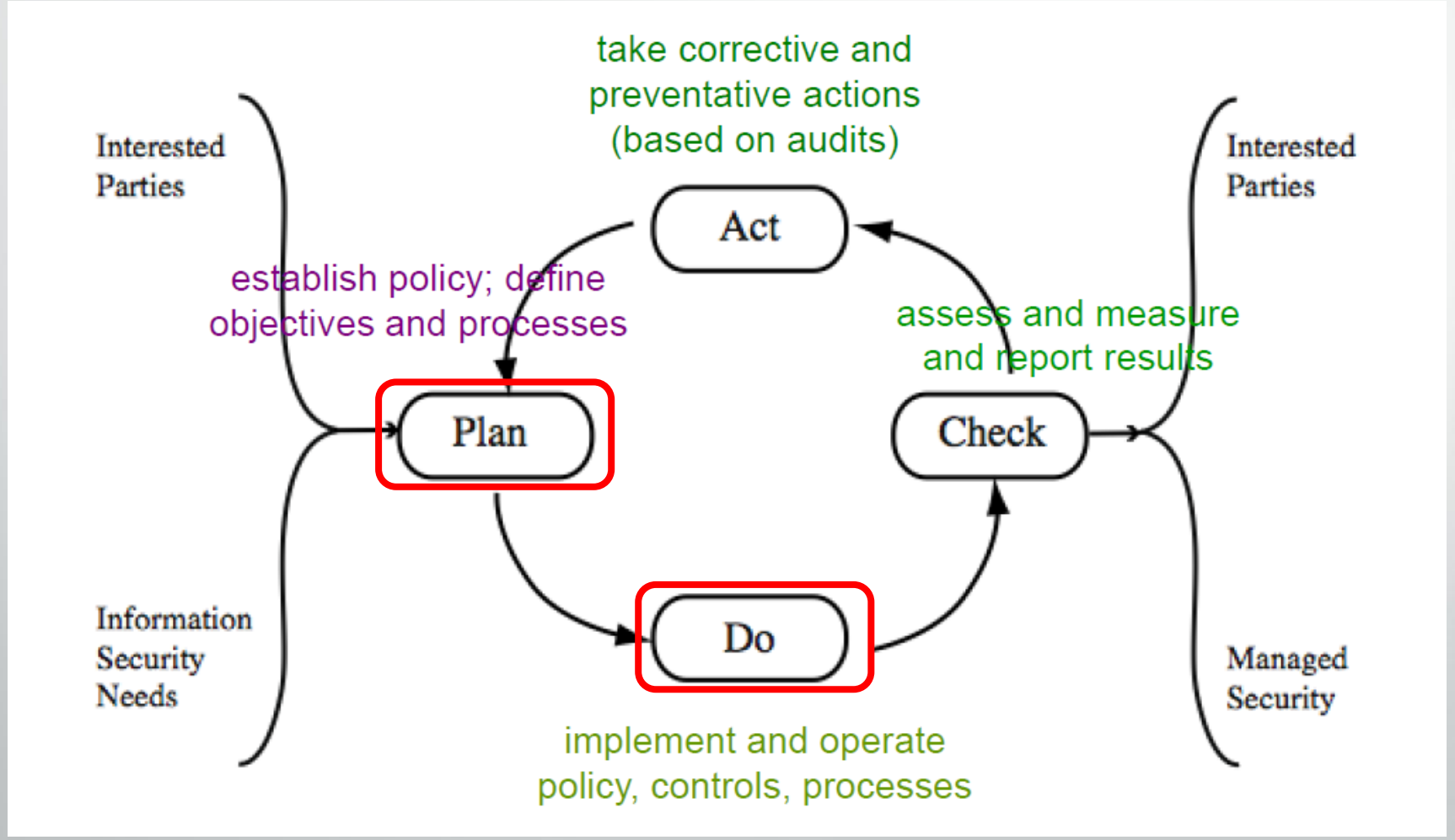
مدیریت ریسک های امنیت اطلاعات (ISRM)

چرخ تکراری آقای دمینگ (PDCA)



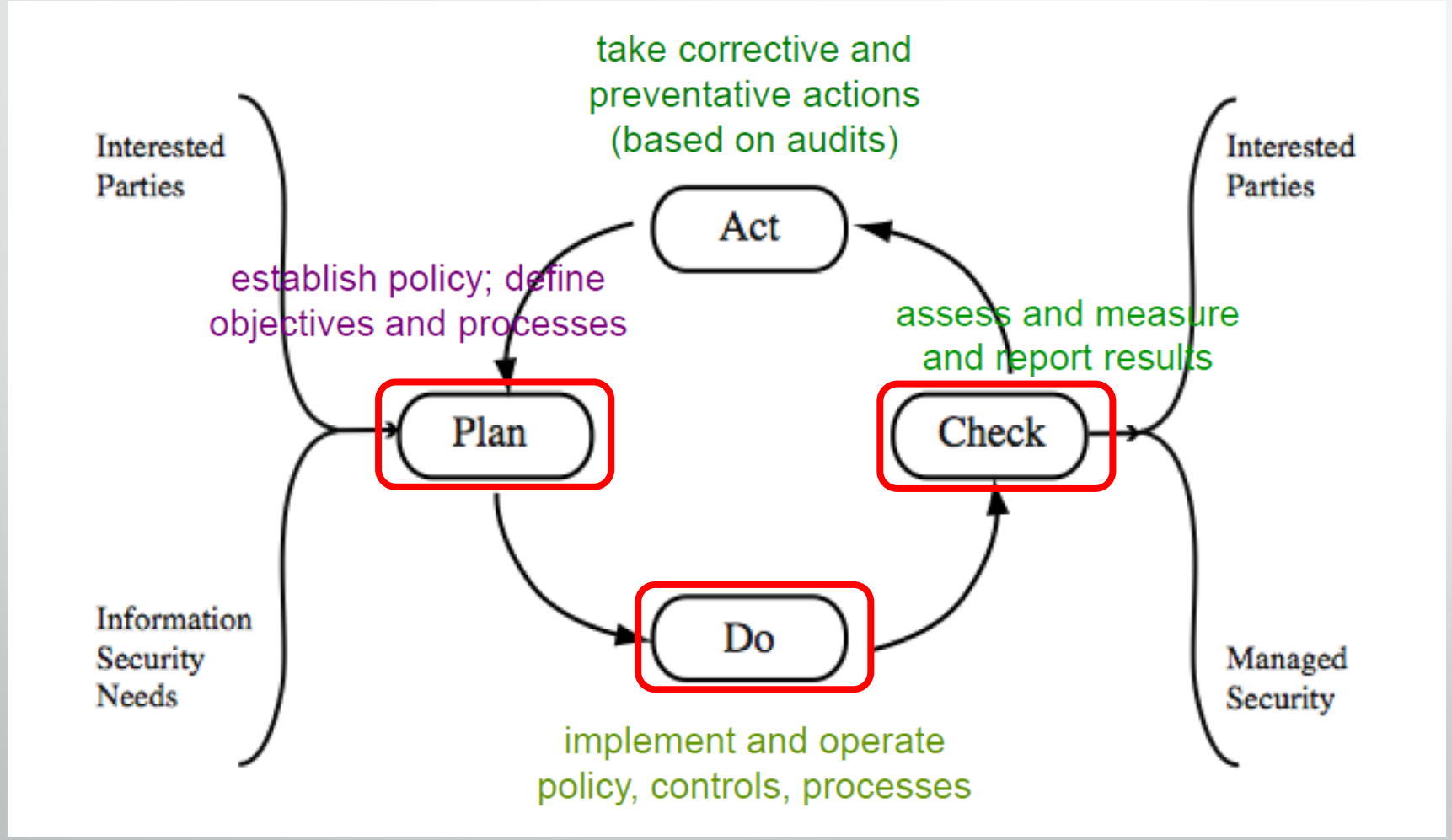
مدیریت ریسک های امنیت اطلاعات (ISRM)

چرخ تکراری آقای دمینگ (PDCA)



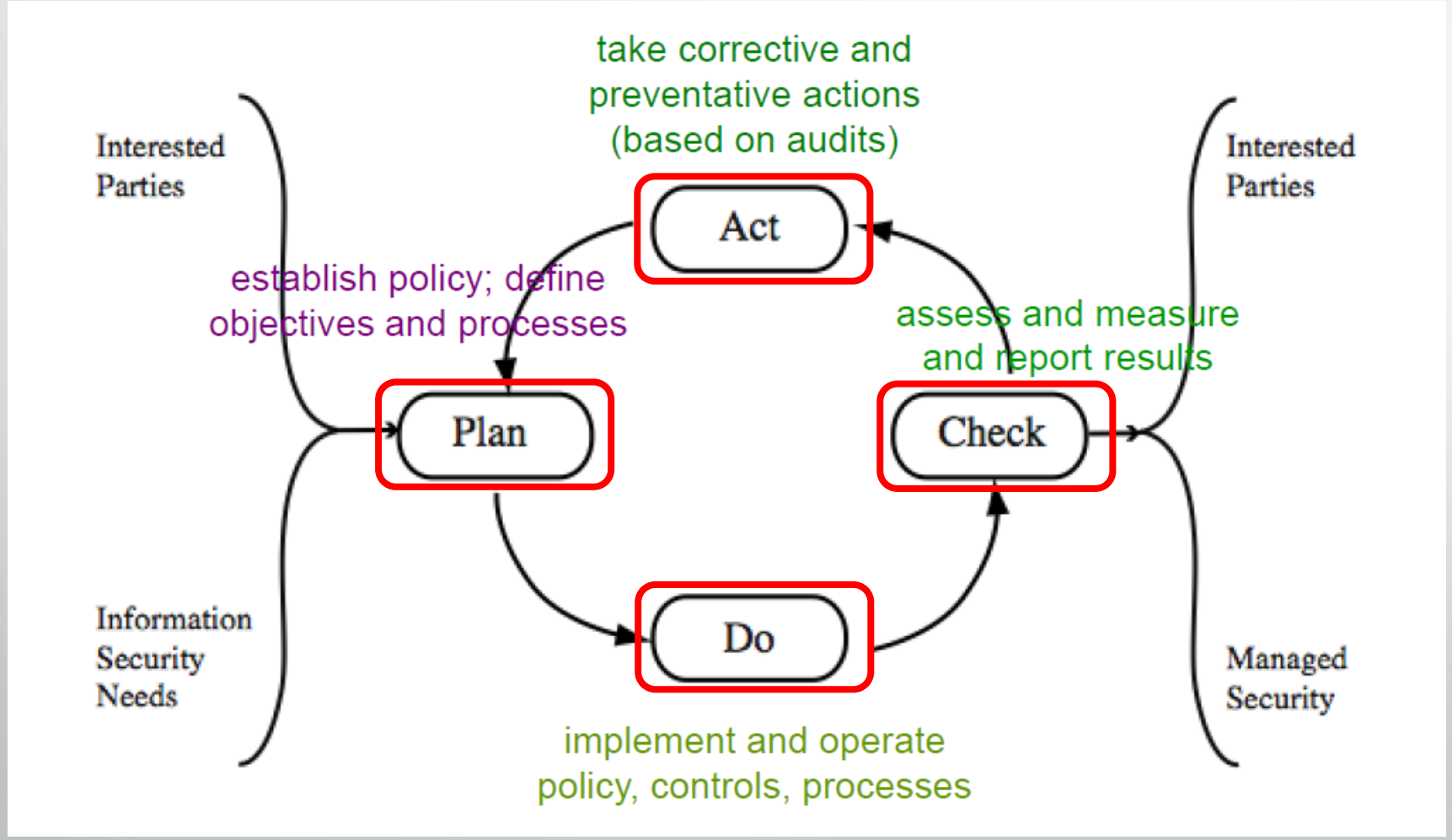
مدیریت ریسک های امنیت اطلاعات (ISRM)

چرخ تکراری آقای دمینگ (PDCA)



مدیریت ریسک های امنیت اطلاعات (ISRM)

چرخ تکراری آقای دمینگ (PDCA)





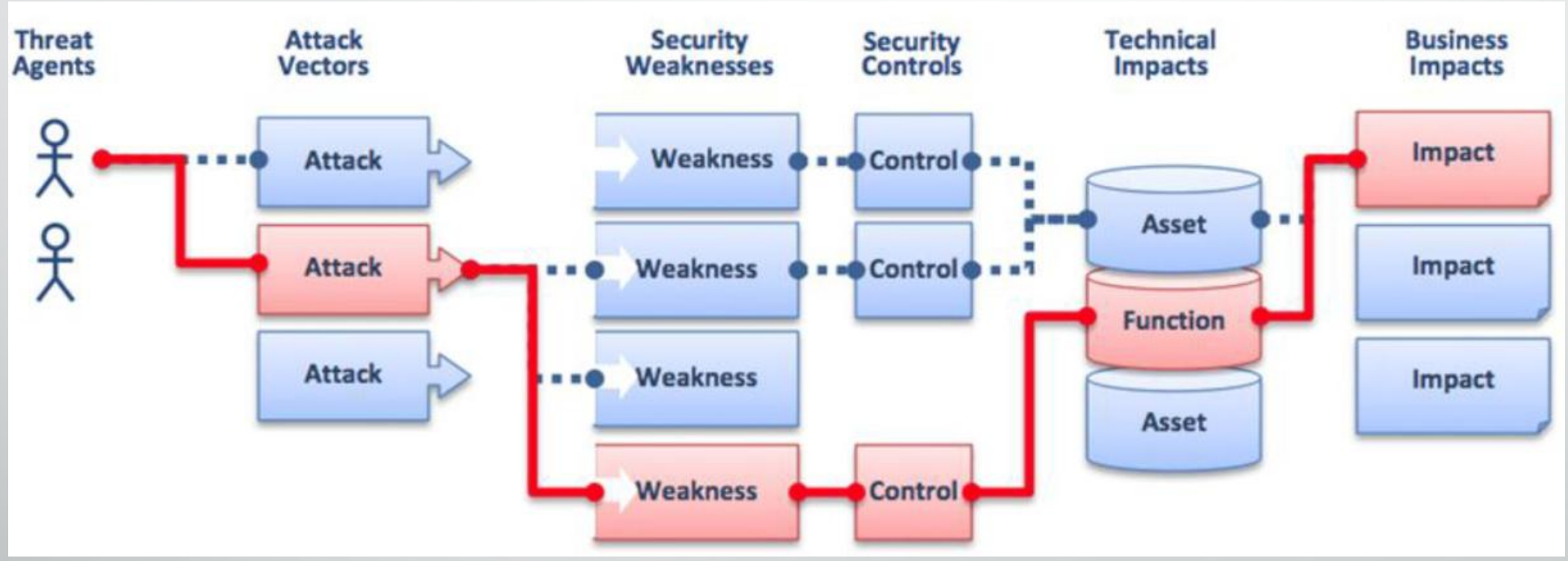
مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...



مدیریت ریسک های امنیت اطلاعات (ISRM)

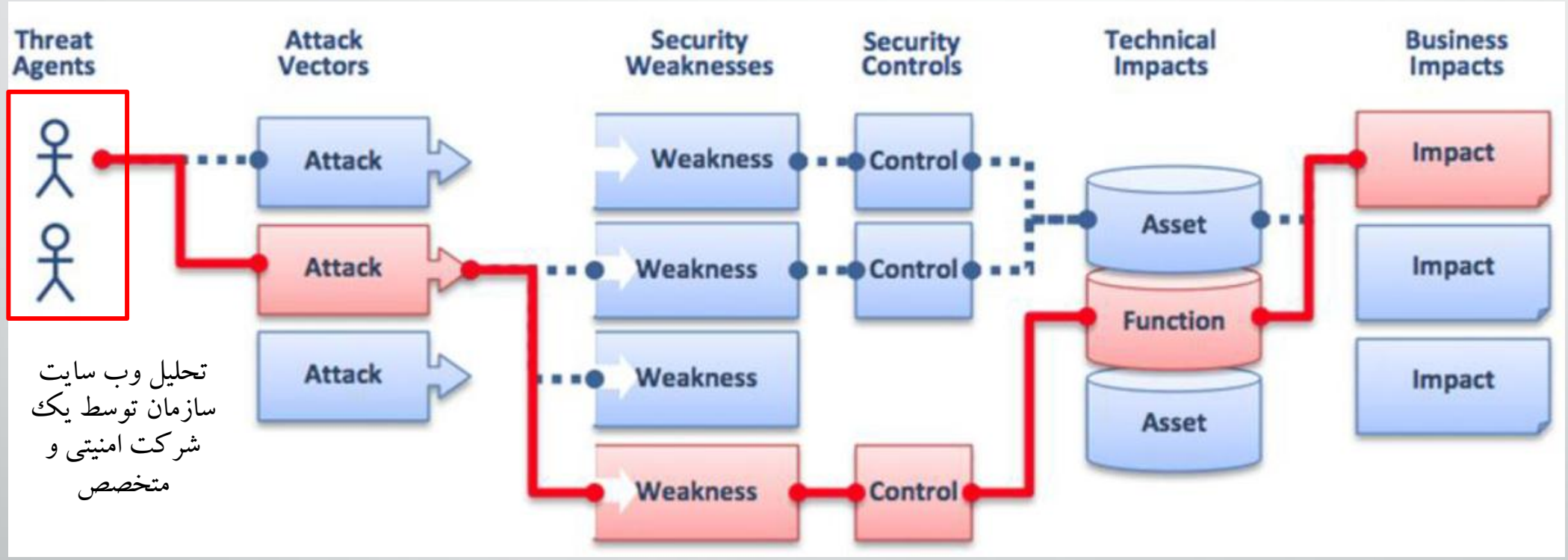
- مثال ...





مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...



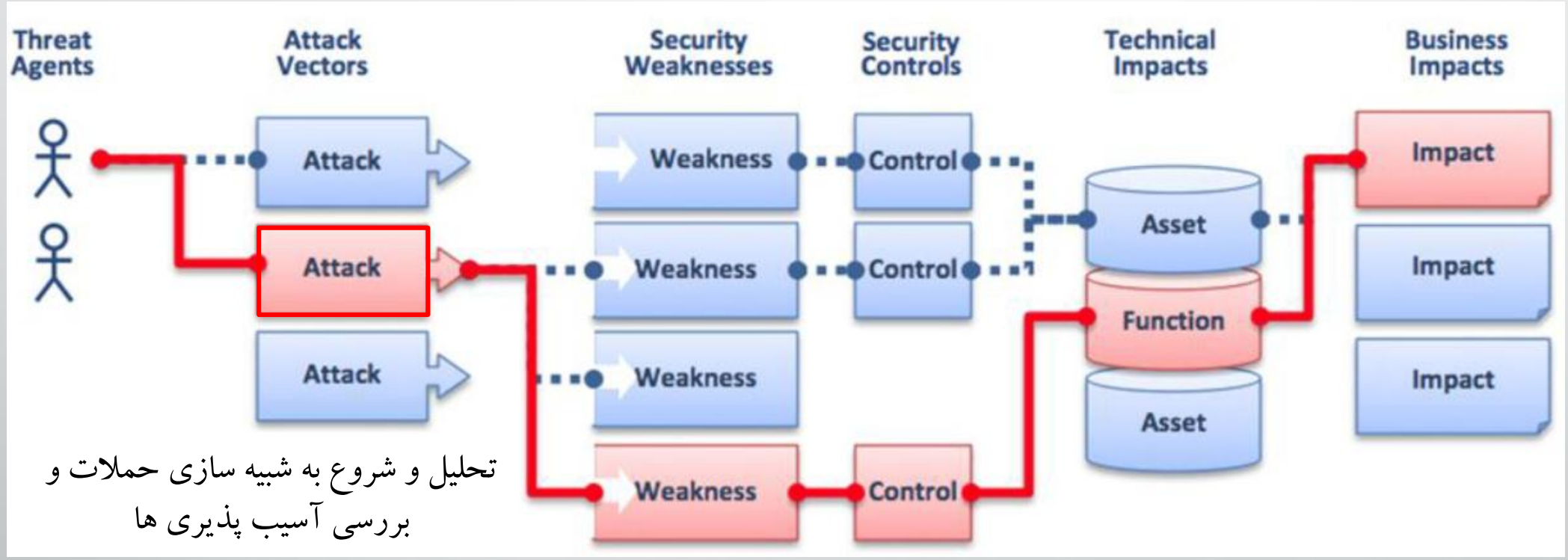






مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...



تحلیل و شروع به شبیه سازی حملات و
بررسی آسیب پذیری ها



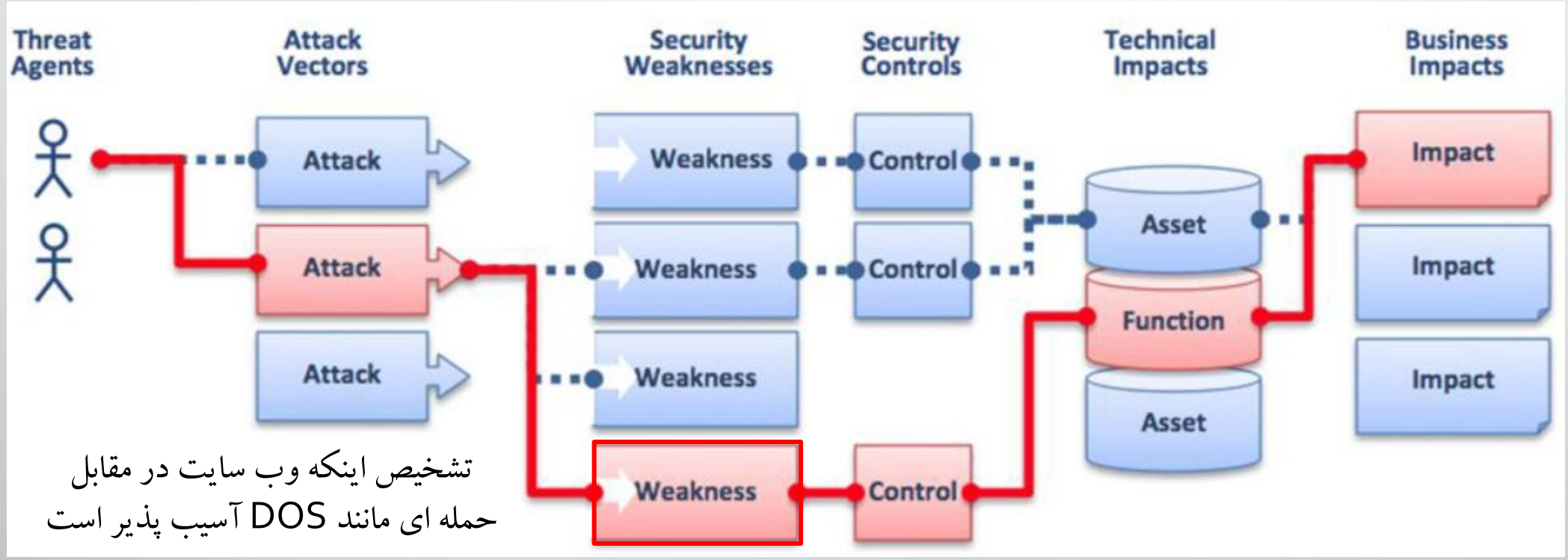






مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...



تشخیص اینکه وب سایت در مقابل حمله ای مانند DOS آسیب پذیر است



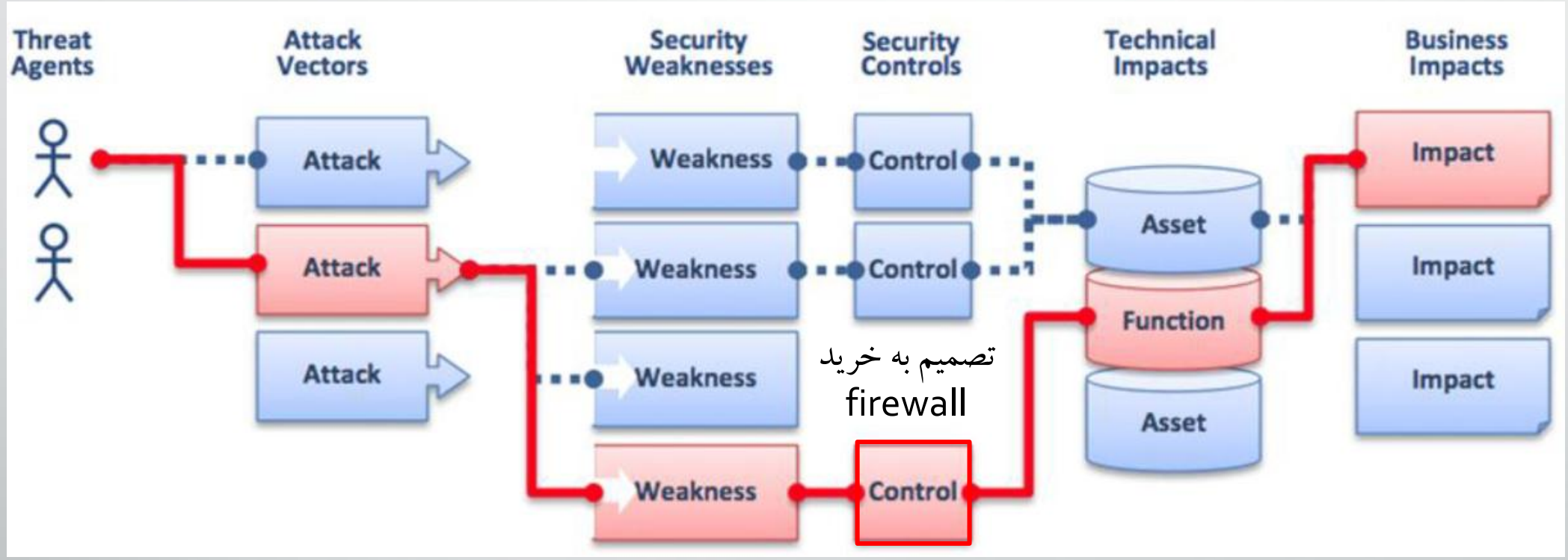






مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...







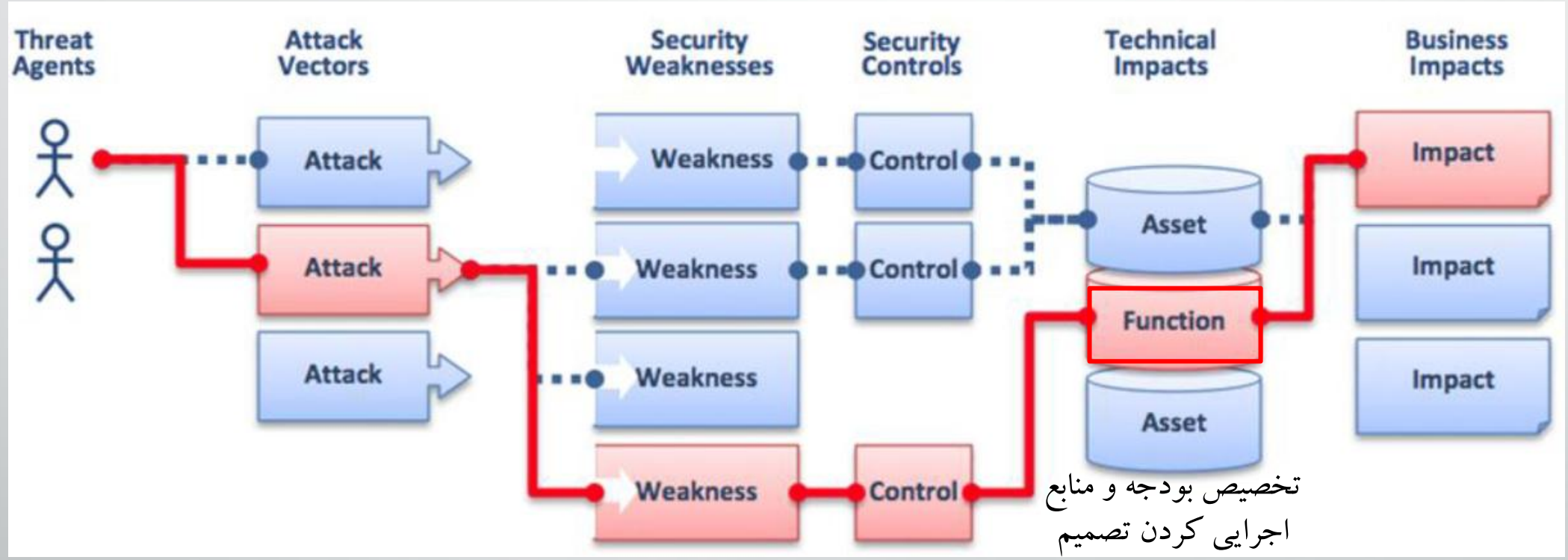






مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...



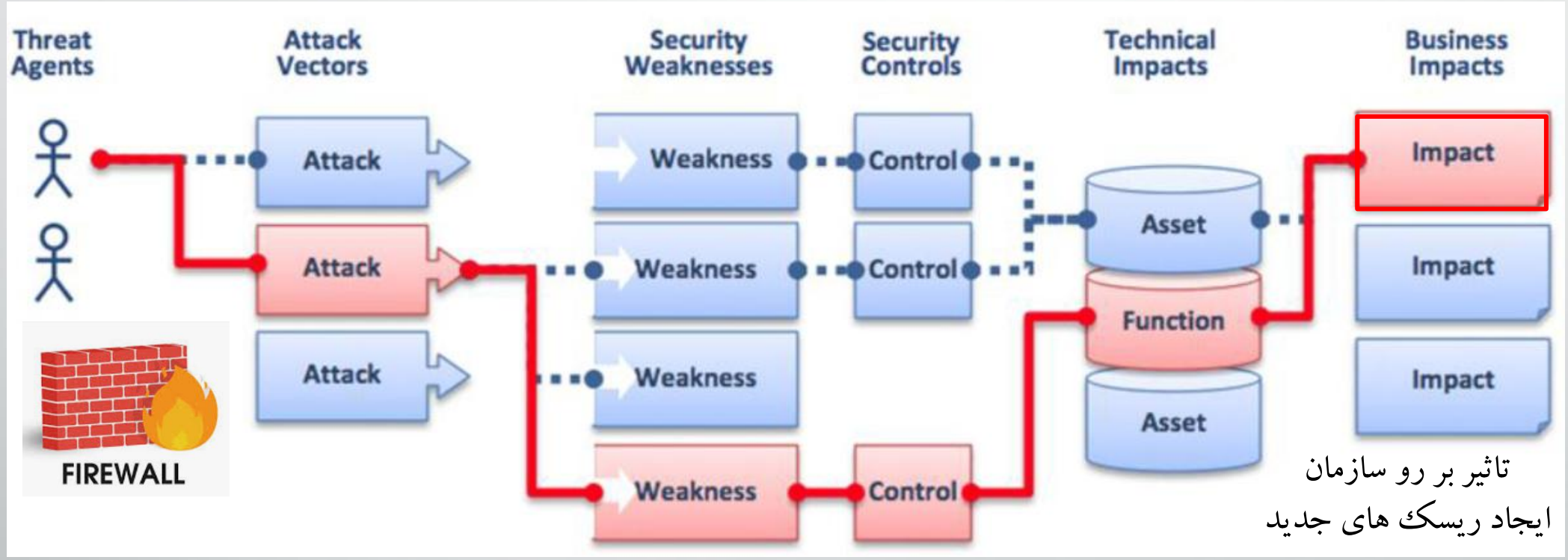
تجهیزات / نیروی انسانی / آموزش / قرارداد پشتیبانی / بروز رسانی / ...





مدیریت ریسک های امنیت اطلاعات (ISRM)

- مثال ...



تاثیر بر رو سازمان

ایجاد ریسک های جدید

دسترسی به سازمان از شرکت جدید و اعتماد
استخدام نیروی جدید یا عدم تسلط نیروهای قبلی
حملات فایروال
نگرانی های بروز رسانی و شرکت تولید کننده
و ...





با تشکر







