دورکاری و امنیت ارتباط از راه دور

امیر عموزیدی
پیشنهادهای سازمان ملی استاندارد و تکنولوژی
NIST

- امروزه بسیاری از کارمندان سازمانها و و پیمانکاران از گستره وسیعی از تکنولوژیهای ارتباط راه دور جهت انجام امور کاری خود استفاده می نمایند. هدف اغلب دورکارها استفاده از تکنولوژیهای ارتباط از راه دور ،دسترسی به منابع الکترونیکی و کامپیوتری داخل سازمان بوده که برای عموم آزاد نمی باشد.
- طبیعت دورکار و تکنولوژیهای ارتباط از راه دور، نیاز به دسترسی از محیط های خارج سازمان و یا میزبانهای خارج از سازمان را دارد که آنرا در معرض ریسک بالاتری به نسبت تکنولوژیهای مورد استفاده در داخل سازمان قرار می دهد.

کلیه ابزارهای دورکاری و راه حلهای دسترسی از راه دور شامل تجهیزات کاربر، سرورهای دسترسی از راه دور و منابع داخلی به اشتراک گذاشته شده توسط آنها، باید در برابر تهدیدهای پیش بینی شده و بر اساس مدلهای شناسایی شده تهدید حفاظت گردند.

اصلی ترین این تهدید ها شامل:

۱- عدم کنترل بر امنیت فیزیکی.
۲- استفاده از شبکه های ناامن.
۳- ارتباط تجهیزات آلوده به شبکه داخلی.
۴- اطمینان از در دسترس بودن منابع برای دورکارها.

اهداف این سمینار

- طراحی سیستهای امنیتی دورکار و ارائه کنترل ها با فرض تهدیدات دشمن در محیط خارج از سازمان.
  - عدم ذخیره اطلاعات در کامپیوتر دورکار.
  - استفاده از تکنیکهای رمز گذاری در ارتباطات و کامپیوتر دورکار.
  - استفاده از آنتی ویروسها و ضد بد افزارها و NAC.
  - جدا نمودن شبکه دورکار از شبکه داخل سازمان.
- تدوین سیاستهای امنیتی دورکار به نحوی که نیازمندیهای دورکار و دسترسی از راه دور را تعریف نماید.
  - کدام تکنولوژی ارتباط از راه دور مجاز می باشد؟
  - کدام تجهیزات راه دور اجازه استفاده از کدام تکنولوژی را دارد؟(موبایل، لپ تاپ، webmail)
  - سرورهای دسترسی از راه دور چگونه مدیریت می شوند و سیاستها چگونه بر روی آنها به روز میشود؟

- اطمینان از حفاظت موثر سرورهای دسترسی از راه دور و اعمال تنظیماتی که دورکار را ملزم به پیروی از سیاستها بنماید.
  - Fully patched
  - Perimeter
  - Hardening
  - Manage from trusted host
- حفاظت تجهیزات دورکار در برابر تهدیدهای معمول و تداوم در حفظ امنیت آنها.
  - Firewall
  - Encryption
  - Antivirus
  - Hardening

مدل نمودن تهدید

۱-قبل از طراحی و اجرا ابتدا ریسک حفره ها، تهدیدها و کنترلهای امنیتی بر اساس ترکیب معیارهای مختلفی ارزش گذاری میشوند که سه شاخص اصلی آنها شامل:

الف: محرمانگی **confidentiality**
ب: تمامیت **integrity**
ج: در دسترس بودن **availability**

مدل نمودن تهدید ها به معنای شناسایی منابعی که پتانسیل پذیرش نفوذ و تهدید را دارند، سپس اندازه گیری احتمال موفقیت هر یک از آنها و در نهایت آنالیز این اطلاعات جهت شناسایی مکانهایی که کنترلهای امنیتی نیاز به اضافه شدن یا بهبود را دارند.

۲- در این مرحله نیازمندیهای امنیتی بدست آمده متدهای دسترسی از راه دور را میتوان طراحی نمود.

الف- ریسک عدم کنترل فیزیکی

- تجهیزات کاربران دورکار در انواع مکانهای خارج از کنترل سازمان استفاده میشوند: خانه، هتل، کافی شاپ، کنفرانس.
- ماهیت قابل حمل بودن این دستگاهها آنها را در معرض خطر دزدی یا مفقودی بیشتری قرار می دهد و باید آگاه بود که نرم افزارها و ابزارهای فراوانی وجود دارند که اطلاعات حساس را از این دستگاهها استخراج میکنند.
- اصلی ترین راهکار استفاده از کد گذاری اطلاعات یا استفاده از DRM هایی میباشد که تمام نرم افزارهای سازمان را پشتیبانی نماید و یا اینکه اطلاعات حساس بر روی کامپیوتر کاربر ذخیره نگردد.
- Shoulder watching

ب- ریسک شبکه های نا امن

- به دلیل آنکه تقریبا بستر تمام ارتباطات از راه دور از طریق اینترنت صورت می پذیرد، سازمانها معمولا کنترلی بر روی امنیت شبکه های دورکار ندارند از آن جمله می توان ریسک های زیر را نام برد.

  استراق سمع eavesdropping

  شخص میانی Man In The Middle

- این ریسک ها را می توان کاهش داد اما نمی توان حذف نمود.

  مکانیزمهای هویت شناسی بین دو نقطه (Authentication)

  مکانیزمهای رمزنگاری ارتباط (Encryption)

ج-ریسک تجهیزات آلوده در شبکه داخلی

- تجهیزات کاربر دورکار خصوصا لپ تاپ اغلب در شبکه های خارجی استفاده شده سپس به داخل شبکه سازمان آورده می شود. هکر یا ویروس حتی با دسترسی فیزیکی خارج از سازمان می تواند بد افزارها را بر روی لپ تاپ نصب نموده تا پس از اتصال به شبکه داخلی گسترش یابد.

راهکار:

- ✓ استفاده از ضد ویروسها و ضد بدافزارها بر روی تجهیزات دورکار.
- ✓ سازمانها باید از راه حلهای NAC جهت بررسی امنیت کامپیوتر دورکارها قبل از اتصال به شبکه داخلی استفاده نمایند.
- ✓ از شبکه های مجزایی جهت اتصال کامپیوتر دورکار به شبکه داخلی استفاده گردد.

د-ریسک دسترسی خارجی به منابع داخلی

- دسترسی از راه دور امکان دسترسی به منابع داخلی ای را از خارج فراهم می سازد، که قبلا از خارج قابل دسترس نبوده است.
- از هر نوع تکنولوژی ارتباط از راه دوری که استفاده شود این تهدید را افزایش میدهد و در نهایت منجر به یک سازش در پذیرش ریسک می شود.
- سازمانها باید با احتیاط، تعادلی را بین منافع بدست آمده از ارتباط از راه دور و احتمال سازش با ریسک بوجود آمده برقرار سازند.
- سازمانها باید دسترسی به تمام منابع قابل دسترس از راه دور را توسط دیوار آتش (Firewall) و مکانیزمهای کنترل دسترسی تا آنجایی که امکان دارد محدود سازند.

۲- متدهای دسترسی از راه دور

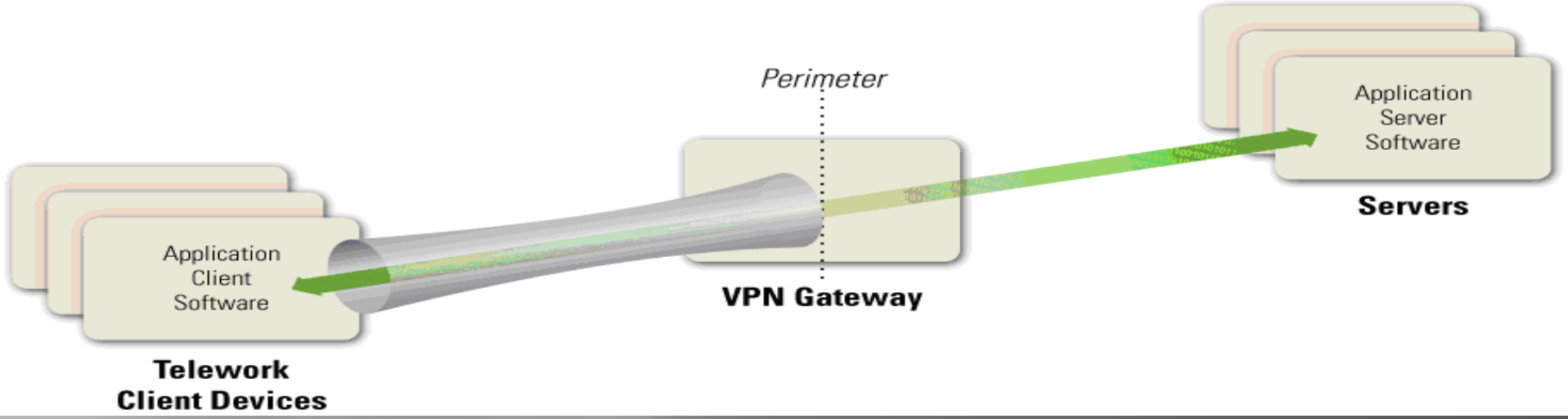
Tunneling

- متدهای ارتباط از راه دور فراوانی قادر به برقراری یک تونل امن میباشند، اما معمولترین آنها تکنولوژی VPN میباشد.
- زمانیکه یک VPN بین دورکار و سرور برقرار میگردد امکان دسترسی به بسیاری از منابع کامپیوتری را به صورت امن برای کاربر فراهم میسازد. که شامل:

۱- رمز نگاری اطلاعات

۲- تشخیص هویت

۳- مدیریت و کنترل دسترسی پروتوکلها و منابع



اگر چه ارتباط بین دورکار و سرور VPN امن است اما:

۱- ارتباط بین سرور VPN و منابع داخلی نا امن می باشد.

۲- نرم افزار و اطلاعات در کامپیوتر کاربر همچنان نا امن است.

پروتوکلهای پر کاربرد تونل شامل:

۱- IPsec (Internet Protocol Security)

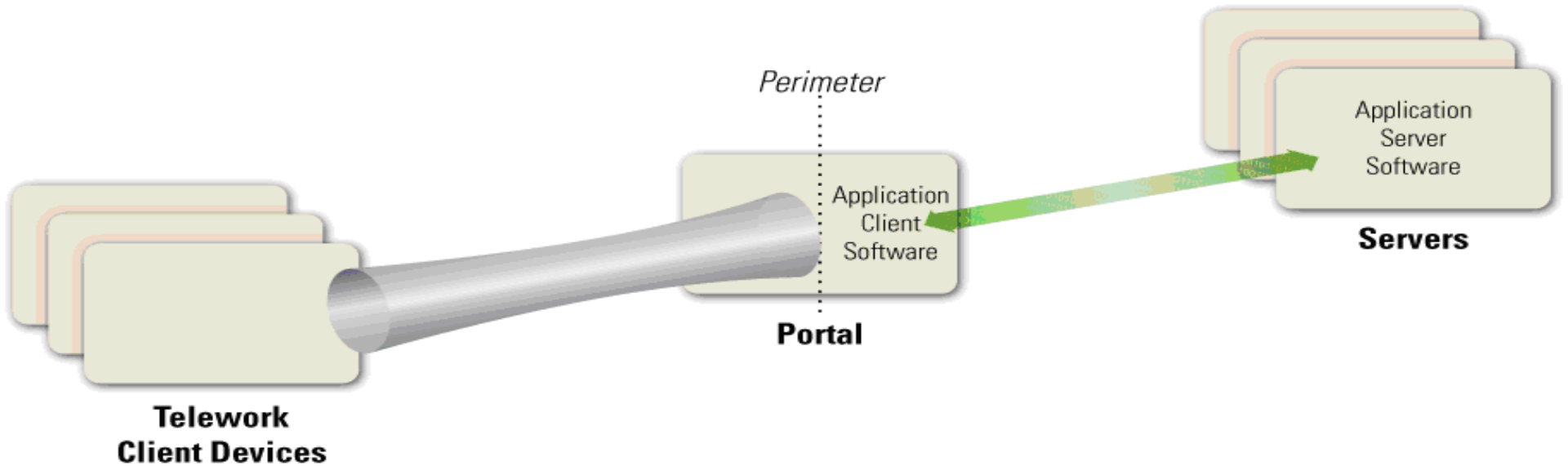
۲- SSL (Secure Sockets Layer)

۳- SSH (Secure Shell)

۴- L2TP,MPLS,PPTP

ب) پورتالهای نرم افزاری

- پورتال سروری است که دسترسی به یک یا چند نرم افزار را از طریق یک پنجره رابط مرکزی فراهم می سازد.که اغلب آنها تحت وب می باشند.
- نرم افزاری بر روی سرور پورتال نصب میگردد که از طریق آن ارتباط سرور پورتال با دیگر سرور نرم افزارها برقرار میگردد.



عملکرد حفاظتی پورتال و تونل شبیه یکدیگر میباشد و بر اساس طراحی میتواند ارتباط بین دورکار و سرور پورتال را امن نماید.

با این تفاوت که در تونل نرم افزار و اطلاعات بر روی کامپیوتر کاربر دورکار قرار میگیرد اما در پورتال بر روی سرور.

اگر چه وجود یک نرم افزار به شکل مرکزی کنترل بیشتری را بر روی نرم افزارهای پورتال برقرار می سازد اما همچنان امکان دانلود اطلاعات و ذخیره آن خارج از منطقه امن وجود دارد.

۱- تحت وب

۲- SSL

۳- Terminal Server (Application , WEB)

۴- Virtual Desktop Access (اطلاعات پس از خارج شدن نابود شود)

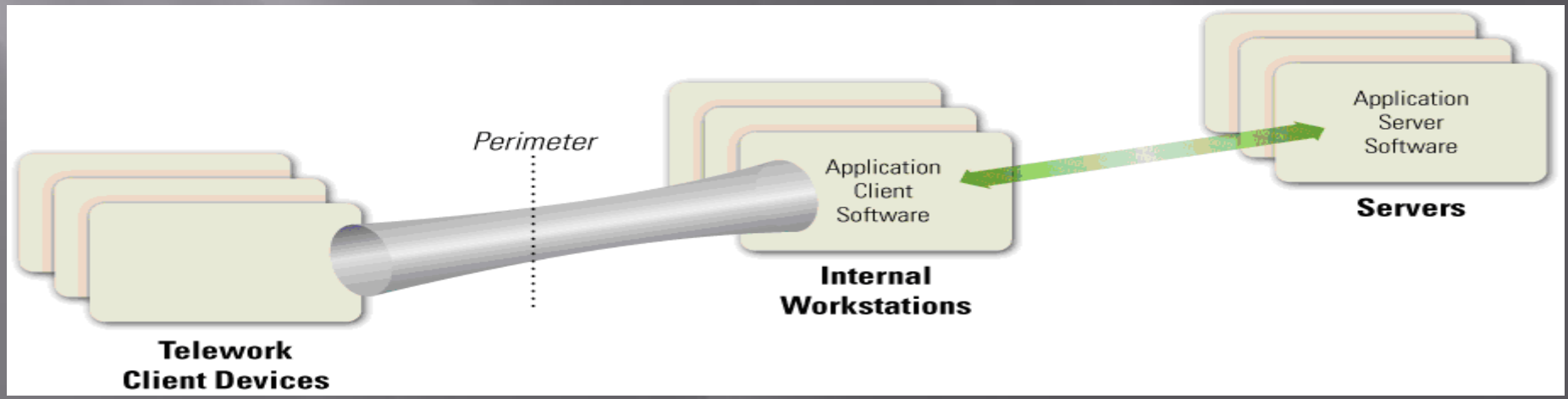
Remote Desktop (ج

1. Application
2. Web Plug-in

الف: مستقیم (به دلیل کد بودن اطلاعات بین دو نقطه مناسب IDS,IPS نیست)

ب: غیر مستقیم (مانند NAT)

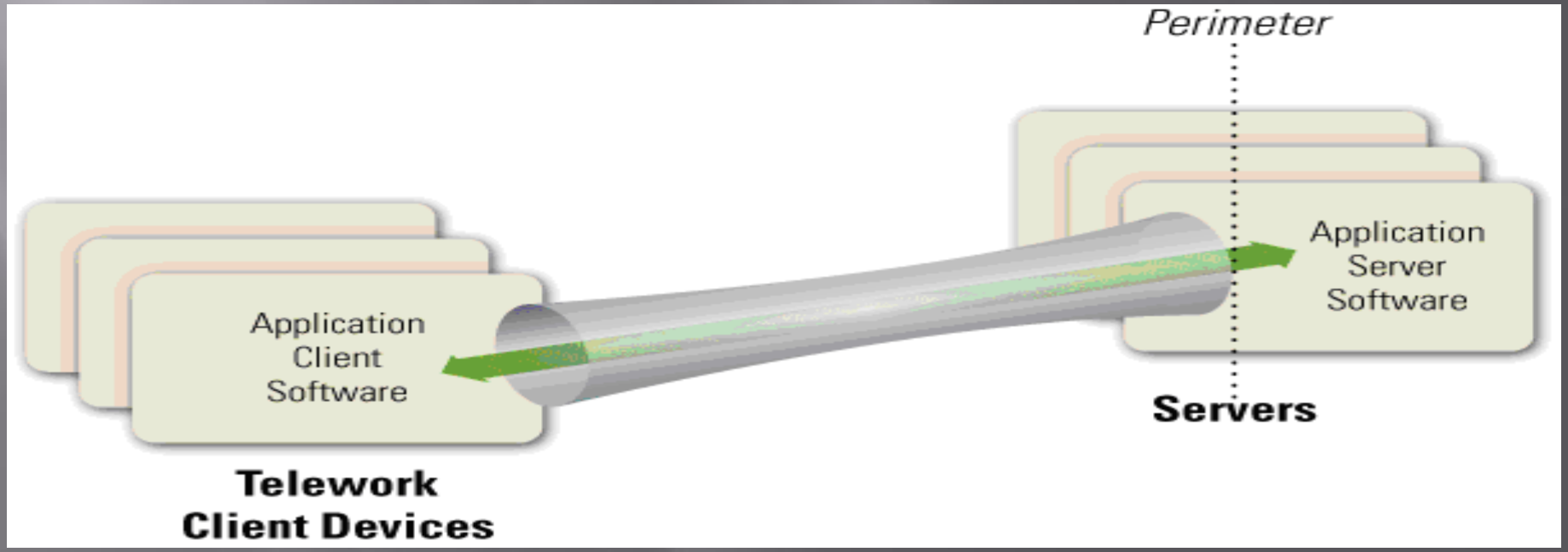
- مشکل امکان دسترسی به شبکه داخلی از طریق کامپیوتر RD آنرا در موقعیت ریسک بالاتری قرار می دهد که برای این درجه امنیت طراحی نشده است..



د) دسترسی مستقیم به نرم افزارها

در این حالت دورکار بدون استفاده از تکنولوژیهای ارتباط از راه دور با نرم افزار به صورت مستقیم ارتباط برقرار می کند. در این حالت هر نرم افزار قابلیت های امنیتی خود را دارد مانند web mail.

قرار دادن سرور در محیط DMZ از جمله الزامات این حالت است.



اهمیت حفاظت از سرورهای دسترسی از راه دور

۱- جایگاه و تعیین سطح سرورها

- **Device Performance, Traffic Examination,Traffic Not Protected by the Remote Access Solution ,NAT ,DMZ,FIREWALL**

۲- سرورهای میانی

۳- سرورهای انتهایی

تشخیص هویت، اختیار و دسترسی از راه دور

الف) تشخیص هویت Authentication

ب)تشخیص اختیار Authorization (and NAC)

ج)کنترل های دسترسی به شبکه Access Control for Network

د) کنترل های دسترسی به نرم افزار Access Control for Application

امنیت تجهیزات کاربر دورکار

الف) کامپیوتر شخصی

ب) تجهیزات مصرفی

ج) سازمان

د) دورکار

ه) اشخاص ثالث

امنیت اطلاعات کاربر دورکار

الف) کد گذاری اطلاعات از همان ابتدا

ب) ماشینهای مجازی سازی

ج) کپی پشتیبان

نکات مهم در چرخه عمر دورکار

الف) شروع و آماده سازی

ب) گسترش

ج) اجرا و پیاده سازی

د) عملیاتی کردن، حفظ و نگهداری

ه) انهدام

الف) شروع و آماده سازی

- انواع مجوزهای دسترسی از راه دور
- محدودیتهای موجود
  - حساسیت دورکار
  - میزان اطمینان از سیاستهای امنیتی
  - هزینه
  - مکان دورکار
  - محدودیت های فنی
  - مغایرتهای قانونی و سیاستهای دیگر
- نیازهای متفرقه کاربر دورکار

ب) گسترش

- معماری
- هویت شناسی
- رمز نگاری
- کنترل دسترسی
- امنیت در نقطه انتهایی

ج) اجرا و پیاده سازی

- ارتباطات
- حفاظتها
- تشخیص هویت
- نرم افزارها
- مدیریت
- گزارشها
- کارایی
- امنیت در زمان پیاده سازی
- تنظیمات پیش فرض

د) عملیاتی کردن، حفظ و نگهداری

- چک های دوره ای و به روز رسانی
- تنظیمات مجدد
- شناسایی و مستند سازی

۵) انهدام