
بسم الله الرحمن الرحيم


انتخاب ملت ایران در مقابل جبهه استکبار «ایستادگی، عدم تسلیم و وابستگی، حفظ استقلال و تقویت درونی نظام و کشور» است.
برای پیشرفت عادلانه و حل مشکل فقر حرکت به سمت اقتصاد دانش بنیان باید کرد.
ما در جنگ به این نتیجه رسیدیم که باید روی پای خودمان بایستیم

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

دکتر ناصر مدیری

مدیریت سرمایه ها و دارایی ها سایبری
IT Asset Management (ITAM)

دکتر ناصر مدیری

مرداد ۱۴۰۱

کسب و کار رقابتی

رقابتی شدن محیط کسب و کار، ضرورت ایجاد یکپارچگی درون سازمانی و بین سازمانی در محیط زنجیره تامین و تحول گسترده در حوزه‌های فناوری سیستم‌های اطلاعاتی، عوامل اصلی شکل گیری سیستم‌های برنامه‌ریزی منابع سازمانی بوده اند.

با ایجاد یکپارچگی مدیریتی و عملیاتی درون سازمانی و بین سازمانی و تسهیل و تسریع فرایندهای کسب و کار، کارایی و اثر بخشی عملیاتی سازمان‌ها را افزایش داده و آنها را برای حضور در بازار رقابتی آماده می کند.

مفهوم توکل

"توکل" در اصل از ماده "وکالت" به معنای انتخاب وکیل کردن است یعنی اعتماد و تکیه بر غیر کردن و او را نایب خود قرار دادن است

منظور از توکل بر خدا، این است که انسان تلاشگر، کار خود را به او واگذارد و حلّ مشکلات خویش را از او بخواهد، خدائی که از تمام نیازهای او آگاه است و قدرت به حل هر مشکلی را دارد.

مهم نیست چقدر امکانات در اختیار دارید.

اگر ندانید چگونه از آنها استفاده کنید، هیچگاه کافی نخواهند بود.

سخنی گهربار از امام جعفر صادق علیه السلام

(من انتظر عاجله الفرصه مواجله الاستقصإ سلبته الایام فرصته, لان من شإن الایام السلب و سبیل الزمن الفوت) (۱)

به هرکس **فرصتی** دست دهد و او به **انتظار** بدست آوردن **فرصت کامل** آن را تإخیر اندازد، روزگار همان فرصت را نیز از او برباید، زیرا کار ایام، بردن است و روش زمان، از دست رفتن.

طرح مسئله

امنیت سرمایه ها و دارائی های سایبری

فهرست

ارائه در یک نگاه

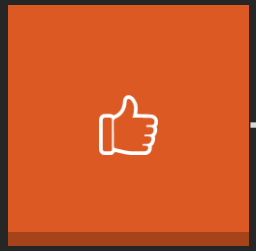
مقدمه

بیان مسئله

- ✓ مسائلی که تلاش می شود در این تحقیق حل شوند

اهمیت و ضرورت

- مرحله شناسایی در معماری NIST
- جایگاه و مرحله شناسایی در CIS



اهداف

تلاش می کنیم به اهداف مشخص شده در رویکرد پیشگیرانه سایبری دست یابیم

تعاریف تحقیق

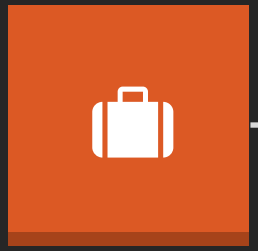
- دارایی
- آسیب پذیری
- تهدید
- ریسک

مدیریت دارایی ها

- چرخه عمر دارایی
- اجزای سیستم مدیریت دارایی
- ITAM
- معیارهای مهم ارزیابی ابزارهای مدیریت دارایی
- چالش ها و توصیه نامه ها

ارزیابی مدیریت دارائی

- مراحل مدیریت دارایئ را شرح خواهیم داد
- مزایا و چالش های مدیریت دارائی



منابع

پایان

امنیت

آرامش در زندگی بدون امنیت امکانپذیر نیست.

همیشه باید نگران باشیم.

5 C's of Cyber Security

سازمان با امنیت =

Change, Compliance, Cost, Continuity, and Coverage

سازمان یکپارچه

دکتر ناصر مدیری

چالش های شبکه های کامپیوتری

Computer Viruses, Backdoors

Ransom ware

Worms

Torjan Horses

Rootkits

Keyloggers

Dialers

Spywares

Adwares

Computer Containment

Proliferation

Concealment

Vulnerability

- Security Defects
- Insecure Design
- User Errors
- Over-privileged Users
- Over-privileged Codes

Grayware

Malware Expolits

Cross Site Cooking

Cross Site Scripting

Cross Site Tracing

Browser Hijacking

Computer Insecurity

Window Insecurity

Cyber Spying

Identity Theft

Industrial Espionage

Riskware

Clickjacking

Browser Expolit

Browser Insecurity

DNS Rebinding

Form Grabbing

Http Cookie

Http Header Injection

Http Response Splitting

Botnet

Zombie Computer

Malbot

Scare Ware

چالش های شبکه‌های کامپیوتری

Anti-Viruses

Anti-Spyware

Anti-Keyloggers

Anti-Malware

Anti-Malware Strategies

Network Monitoring

One-Time Passord (OTP)

Security Tokens

On-Screen Keyboards

Speech Recognition

S/W Keyloggers:

- Hypervison Based
- Kernal Based
- API Based
- Form Feed Based
- Memory Injection Based
- Packet Analyzers

H/W Key

- Wireless
- Acoustics
- Optical
- Physical

Out of Date PC Software

Session Fixation

Session Hijacking

Session Poisoning

Social Jacking

XSS Worm

Eavesdropping

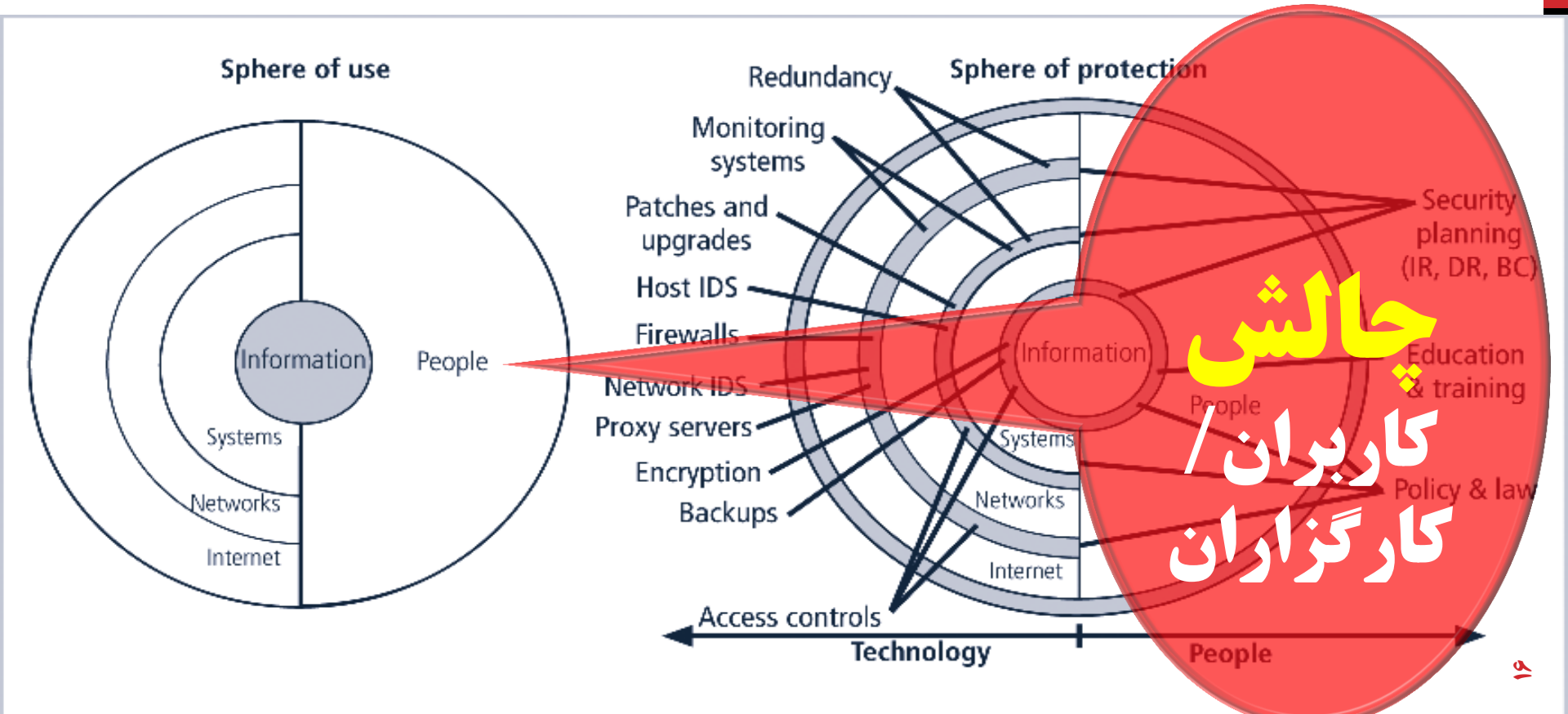
Social Engineering

Human Error

Indirect Attack – public Anonymzing

Network Monitoring

محدوده امنیت



بیان مسئله

شناسایی پیشگیرانه امنیت سایبری شبکه

شناسایی و ارزیابی پیشگیرانه امنیت شبکه و شناسایی خطرات سیستم های حیاتی و داده های حساس و همچنین نقاط ضعف و قوت تجهیزات، سرویس ها و خدمات در جهت شناسایی نقاط تهدید، ریسک و آسیب پذیری ها و در نتیجه پیشبرد اهداف امنیتی در طول چرخه عمر آنها، بر پایه امکانات و منابع

پایه گذاری، پیاده سازی، بهره برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات و پیاده سازی صحیح این نوع مدیریت در راستای کاهش ریسک های پیرامونی به عنوان عامل مهم، در تضمین سطح امنیتی تعریف شده برای شبکه و در نهایت سازمان.

زیرساخت فناوری اطلاعات

- ژنراتورها و **UPS**
- شبکه زیرساخت (شامل تلفن، داده و ارتباطات صوتی)
- اتاق سرور
- سرورها و آرایه های ذخیره سازی
- سیستم های کابل کشی ساخت یافته

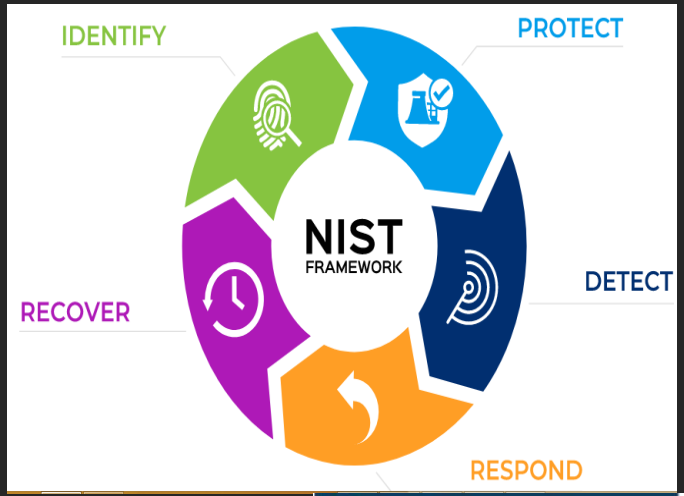
برنامه ها و نرم افزارهای فناوری اطلاعات

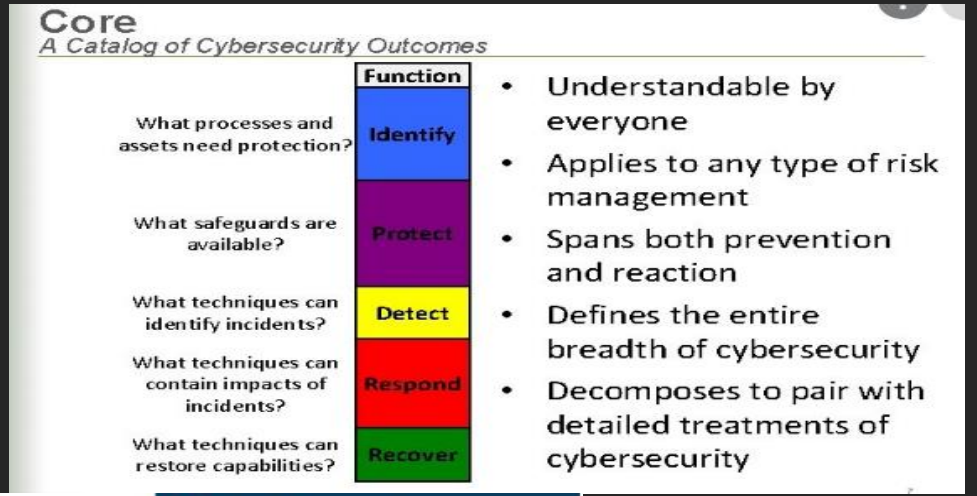
- نرم افزار بهره وری دسکتاپ
- برنامه های سازمانی
- برنامه های تخصصی
- ابزارهای مدیریت خدمات فناوری اطلاعات

رایانه ها و دستگاه ها

- تجهیزات سمعی بصری
- تلفن های رومیزی
- دسکتاپ و لپ تاپ
- چاپگرها، اسکنرها و پلاترها
- تلفن همراه و تبلت

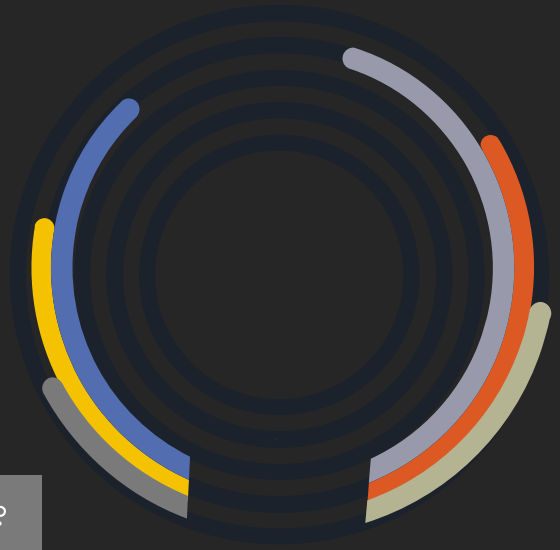
اهمیت مرحله شناسایی در رویکرد پیشگیرانه





اهداف

برخی از اهداف امنیتی که با انجام صحیح فرآیند شناسایی دارایی ها، ریسک ها و تهدیدات به آنها دست خواهیم یافت



دارایی‌های بلا استفاده را کاهش می‌دهد.

با اطمینان از اینکه نرم افزار به درستی وصله/به روز شده است، سطح حمله ماشین ها را کاهش می دهد.

ارائه آمار استفاده از مجوز نرم افزار (برای شناسایی فرصت های کاهش هزینه)

انعطاف‌پذیری امنیت سایبری را افزایش دهده و به تحلیلگران امنیتی کمک کند تا روی ارزشمندترین یا حیاتی‌ترین دارایی‌ها تمرکز کنند.

با اطلاع از مکان، پیکربندی و مالک دستگاه، پاسخ سریع‌تر به هشدارهای امنیتی را فعال می‌کند.

مهندسی امنیت اطلاعات

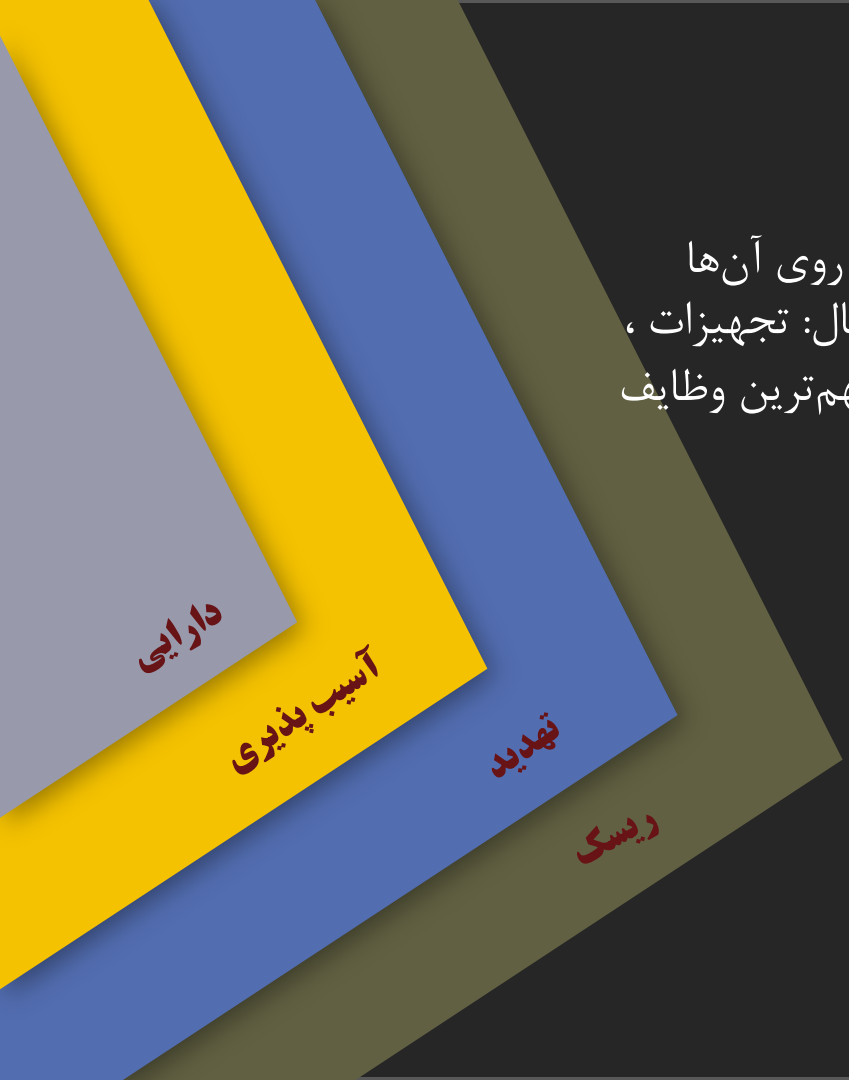
مهندسی امنیت مجموعه فعالیت‌هایی است برای حصول و نگهداری سطوح مناسبی از:

- محرمانگی (Confidentiality)
- یکپارچگی (Integrity)
- قابلیت دسترسی (Availability)
- اصالت (Authenticity) – تصدیق – Authentication
- اجازه قانونی – Authorization
- حساب پذیری (Accountability)
  - دسترسی پذیری – Access Control
  - عدم انکار – Non-Reputation
  - قابلیت اطمینان (Reliability)

مفاهیم و اصطلاحات

دارایی(Asset): دارایی‌ها تمامی چیزهایی هستند که سازمان روی آن‌ها سرمایه‌گذاری کرده و برای سازمان ارزشمند می‌باشند. به‌عنوان‌مثال: تجهیزات ، کارکنان، کامپیوترها، داده‌ها و... . حفاظت از دارایی‌ها یکی از مهم‌ترین وظایف امنیت شبکه می‌باشد.

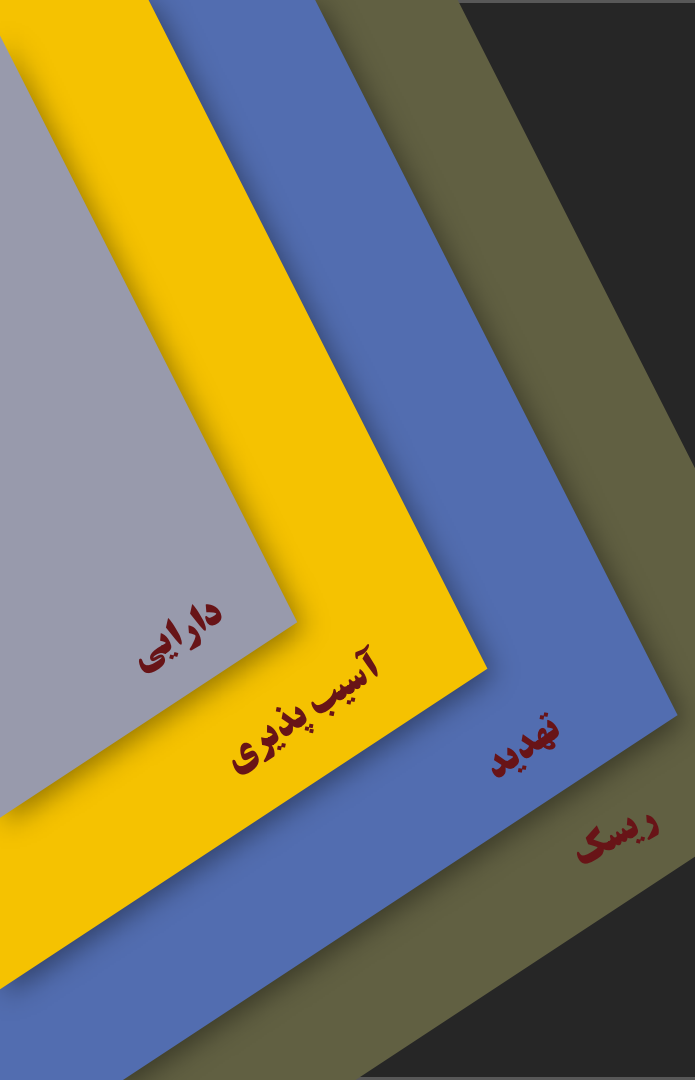
آسیب‌پذیری‌ها (Vulnerability): آسیب‌پذیری را می‌توان ضعف سیستمی و یا ضعف در طراحی این سیستم‌ها تعریف کرد. سیستم‌ها توسط افراد ساخته‌شده‌اند. شانس وجود خطا و اشتباه در هر سیستمی که توسط انسان ساخته‌شده می‌باشد.
آسیب‌پذیری‌ها همیشه در نرم‌افزارها، پروتکل‌های شبکه، سیستم‌عامل و... وجود دارند. هکرها از این آسیب‌پذیری‌ها برای ورود به شبکه امن داخلی سازمان استفاده می‌کنند.



مفاهیم و اصطلاحات

تهدید(Threat): تهدید را می‌توان به‌عنوان هر چیزی که برای دارایی‌ها خطرناک باشد تعریف کرد یا به عبارت دیگر هر عاملی که به طور بالقوه بتواند منجر به وقوع رخدادهای خطرناک شود. تهدیدات می‌توانند به‌صورت تصادفی به وجود آمده و یا از پیش برنامه‌ریزی شوند.

خطر (Risk): ریسک را می‌توان هر عاملی برای از دست دادن، خراب کردن، خسارت زدن و یا هر نتیجه منفی برای دارایی‌های سازمان نامید. خطرها از طریق حملات، استفاده از آسیب‌پذیری‌ها و تهدیدات ایجاد می‌شوند. ریسک تأثیرات منفی بر روی دارایی‌های سازمان دارد.

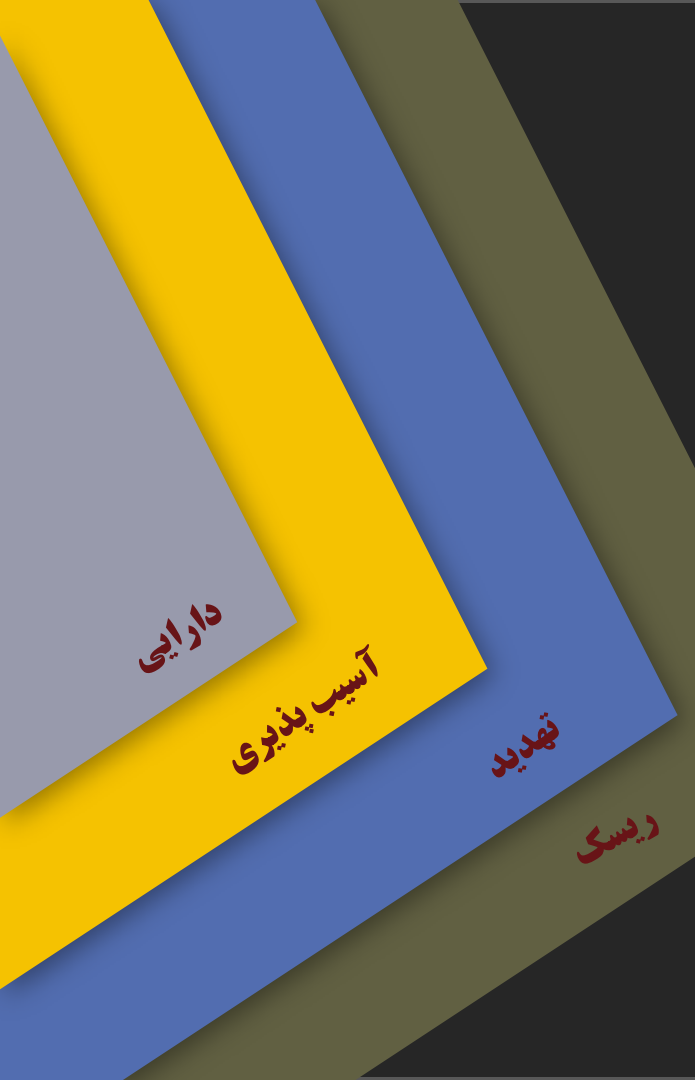


خطر = دارایی + تهدید + آسیب‌پذیری

مفاهیم و اصطلاحات

تهدید(Threat): تهدید را می‌توان به‌عنوان هر چیزی که برای دارایی‌ها خطرناک باشد تعریف کرد یا به عبارت دیگر هر عاملی که به طور بالقوه بتواند منجر به وقوع رخدادهای خطرناک شود. تهدیدات می‌توانند به‌صورت تصادفی به وجود آمده و یا از پیش برنامه‌ریزی شوند.

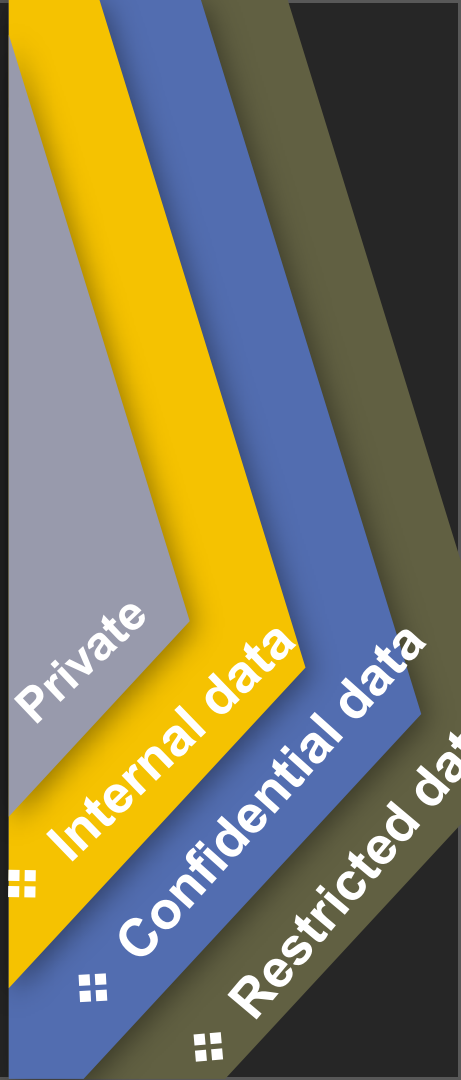
خطر (Risk): ریسک را می‌توان هر عاملی برای از دست دادن، خراب کردن، خسارت زدن و یا هر نتیجه منفی برای دارایی‌های سازمان نامید. خطرها از طریق حملات، استفاده از آسیب‌پذیری‌ها و تهدیدات ایجاد می‌شوند. ریسک تأثیرات منفی بر روی دارایی‌های سازمان دارد.



خطر = دارایی + تهدید + آسیب‌پذیری

مفاهیم و اصطلاحات

- Common Criteria replaced Orange Book - obsolete
- **Data Classification :**
  - **ISO 27001**
  - General Data Protection Regulation (GDPR)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Health Insurance Portability and Accountability Act (**HIPAA**)
  - **Data Classification for NIST 800-53**
  - **5 Data Classification types**



مفاهیم و اصطلاحات

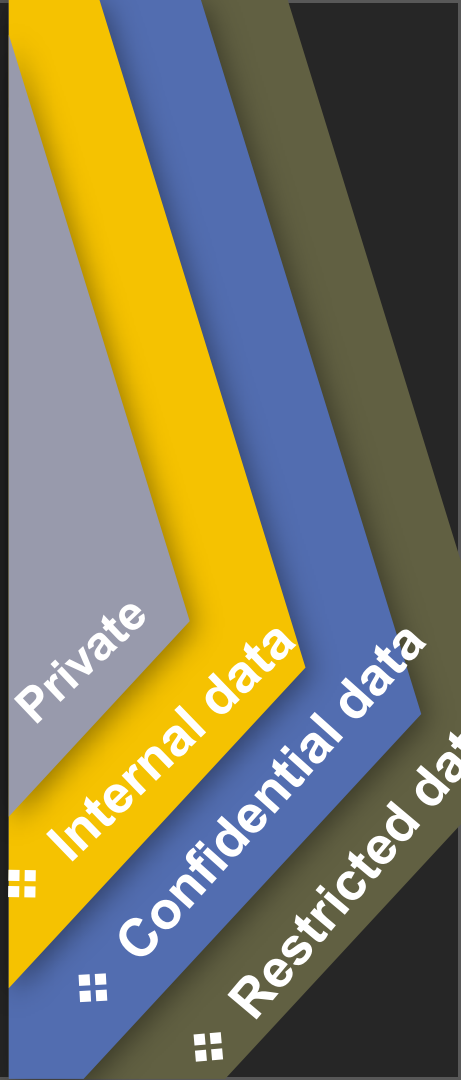
Controlled Unclassified Information

Controlled

Top Secret, Secret, Confidential, Sensitive, and Unclassified

C1: Contact information
C2: Identity data
C3: Communication data
C4: Digital information data

Content-based classification
Context-based classification
User-based classification



مفاهیم و اصطلاحات

Class 1 data is **Institutional Data that requires the highest level of protection and monitoring due to legal, regulatory, administrative, contractual, rule, or policy requirements**.

Class 2 data is Institutional Data classified as private due to legal, regulatory, administrative, or contractual requirements; intellectual property or ethical considerations; strategic or proprietary value; and/or other special governance of such data.

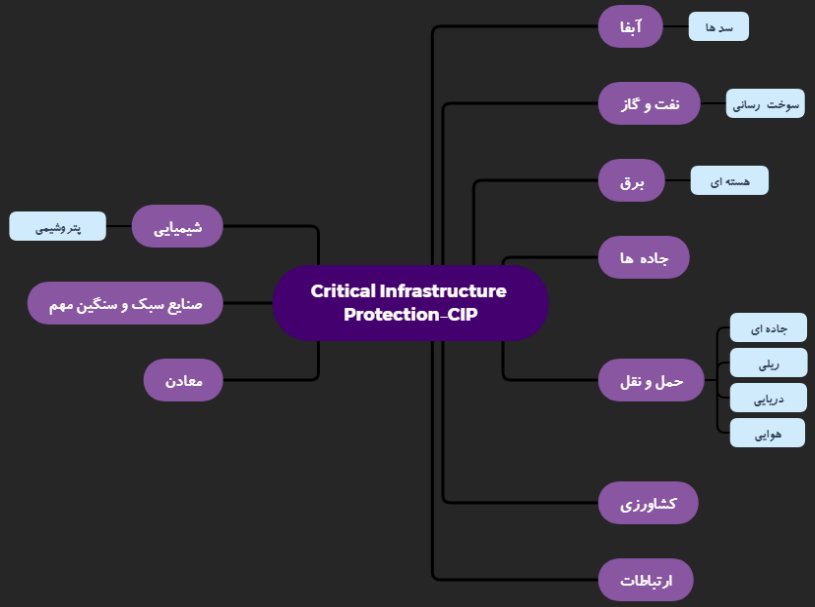
Class 3 is protected confidential data, which comprises identity and financial data that, if improperly disclosed, could be used for identity theft or to cause financial harm to an individual or WCSU. Security at this level is very high (highest possible).

Class 4 data is Institutional Data that is intended for public use and has no access or management restrictions. Additionally, data and systems are categorized as Class 4 when their risk factors are defined.

مفاهیم و اصطلاحات

تاب آوری زیر ساخت های حیاتی عملیاتی Critical Infrastructure Operational Networks (CIONs)

تاب آوری زیر ساخت های حیاتی اطلاعاتی Critical Informational Infrastructure Systems (CIIS)



زیرساخت اطلاعات حیاتی Critical Informational Infrastructure Protection (CIIP)

مفاهیم و اصطلاحات

ثروت:

- از ثروت عایدی کسب میشود.
- حفظ ارزش

سرمایه:

- ساختمان
- نقدینگی
- گواهی ها/باندها/سهام/رمز ارز/حقوق مالکیت/
- سخت افزار/نرم افزار

دارائی (مادی/غیر مادی):

- اطلاعات پیکربندی
- نوع خدمات و سرویس های ارایه شده/نوع ارتباطات آنها
- برنامه ها، برنامه ریزی ها، نیروی کار/انتخاب ها
- اطلاعات، پردازش ها، دانش، هوشمندی، هوش، درک، آگاهی، شناختی
- نقاط قوت/فرصت ها/چالش ها/دانش ضعف ها
- رویکردها/روش ها/رویه ها
- جریان روزانه کارکنان/حافظه سازمانی (گردآوری، سازمان دهی، توزیع/استفاده

ریسک های دارائی:

- ناشناخت ها
- بیش از حد یا کمتر از حد تحت تعمیر و نگهداری
- عملکرد نامناسب
- مدیریت نامناسب ریسک
- سیستم مدیریت ارزیابی غیر بهینه

مفاهیم و اصطلاحات

Assets Management:

- Digital AM
- IT AM
  - Enterprise AM
  - Infrastructure AM

Asset Management Process:

- Planning and Controlling the Acquisition
- Operation
- Maintenance
- Renewal
- Relocation
- Track/Trace
- Disposal

of Organizational Assets

Inventory Management:

- Track stock levels
- Stock Movements.
- Sales
- Shipping
- Inventory Optimizes levels
- Raw Materials
- Works-In-Process
- Maintenance, Repair and Operations = MRO

فرآیند مدیریت دارایی:

- برنامه ریزی و کنترل اکتساب
- عملیات
- نگهداری
- بازسازی
- ردیابی/پیگیری
- جا به جا کردن
- از بین بردن/ دفع کردن

دارایی های سازمانی

مدیریت موجودی:

- پیگیری سطوح موجودی
- حرکات جا به جایی
- فروش/حمل
- سطوح بهینه موجودی
- مواد خام، تعمیر و نگهداری و عملیات = MRO

IMPACT LEVEL

Data processed and stored by public sector organizations can be categorized according to the impact on organization assets, operations, or individuals.

HIGH

severe or catastrophic adverse effect

- Health Information, including Protected Health Information (PHI)
- Health Insurance policy ID numbers
- Social Security Numbers
- Credit card numbers
- Financial account numbers
- Export controlled information
- Driver's license numbers
- Passport and visa numbers

MODERATE

serious adverse effect

- Staff employment applications, personnel files, salary, birth date, personal contact information
- Non-public organization's internal policies, contracts, reports
- Organization's financial data, budgets

LOW

limited adverse effect

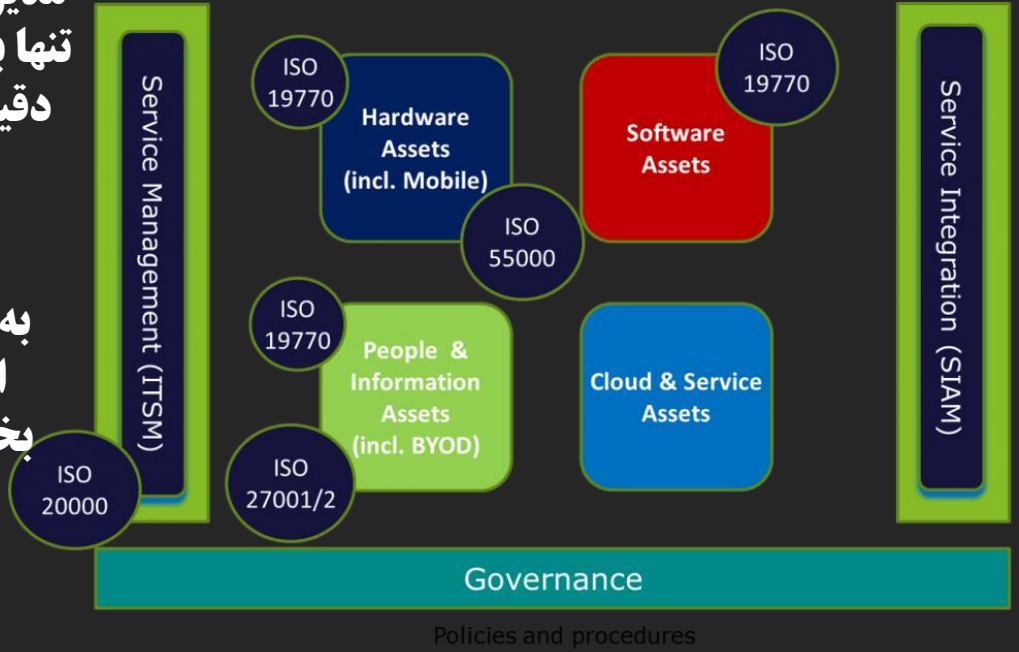
- Job postings
- Organization's contact information
- Information in the public domain

مدیریت دارایی

شناسایی، مدیریت و کاربرد سه جنبه موجود در مدیریت دارایی های امنیت شبکه.

مدیریت مؤثر دارایی ها تنها با تشخیص به موقع و دقیق امکان پذیر است

به روز رسانی دوره ای اطلاعات دارایی نیز بخش مهمی از مدیریت ایمن دارایی است.



Internal vendors (datacenter)

Hosting vendors

IaaS, PaaS, SaaS etc.

مدیریت پیکربندی، مدیریت دارایی فناوری اطلاعات نیست.

تخصیص دارایی نباید بر روی کاربر اصلی کشف شده یک رایانه باشد، همچنین نباید تخصیص مکان فیزیکی مجموعه با آدرس IP تعیین شود

ITAM اغلب با مدیریت روزانه پیکربندی آن دارایی، مدیریت مالی مجموعه‌هایی که در ثبت دارایی ثابت هستند یا نگهداری فهرستی از دارایی‌های مستقر شده اشتباه گرفته می‌شود.

برنامه مدیریت دارایی موفق

اجزای یک برنامه مدیریت دارایی IT موفق:

- ❑ پوشش کامل کل چرخه عمر دارایی IT، از درخواست تا از رده خارج شدن دارایی (یا فراتر از آن).
- ❑ فرآیندهای تعریف شده برای اطمینان از اجرای کارآمد، سازگار و دقیق وظایف و فعالیت های مدیریت دارایی فناوری اطلاعات.
- ❑ بهبود مستمر فرآیند برای دستیابی به سطوح بالاتری از بلوغ.
- ❑ ابزارهای مؤثری که پشتیبانی و اتوماسیون فرآیند را فراهم می کنند

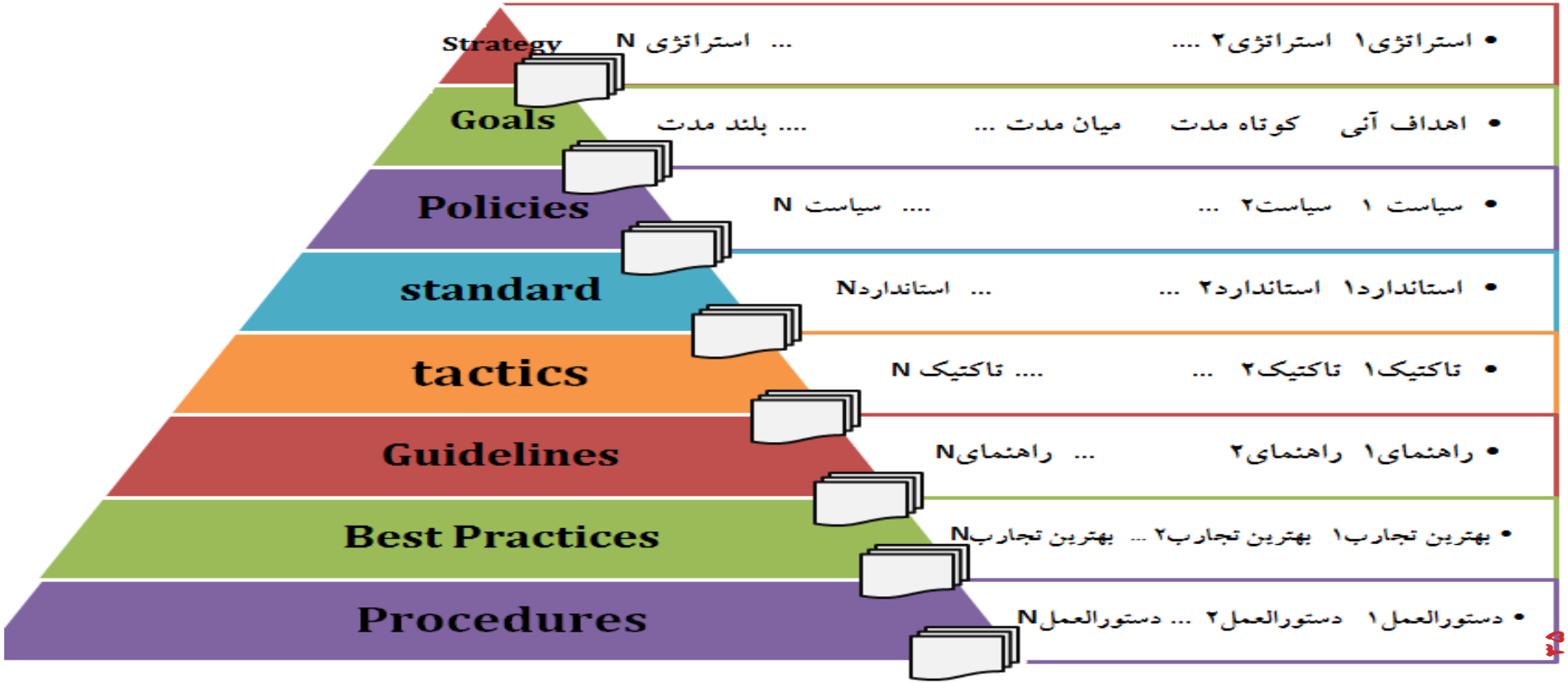
ردیابی دارایی مدیریت چرخه عمر نیست!

برنامه مدیریت دارایی موفق

چهار ابزار اصلی برای پشتیبانی از یک برنامه مدیریت دارایی فناوری اطلاعات باید ارائه شود:

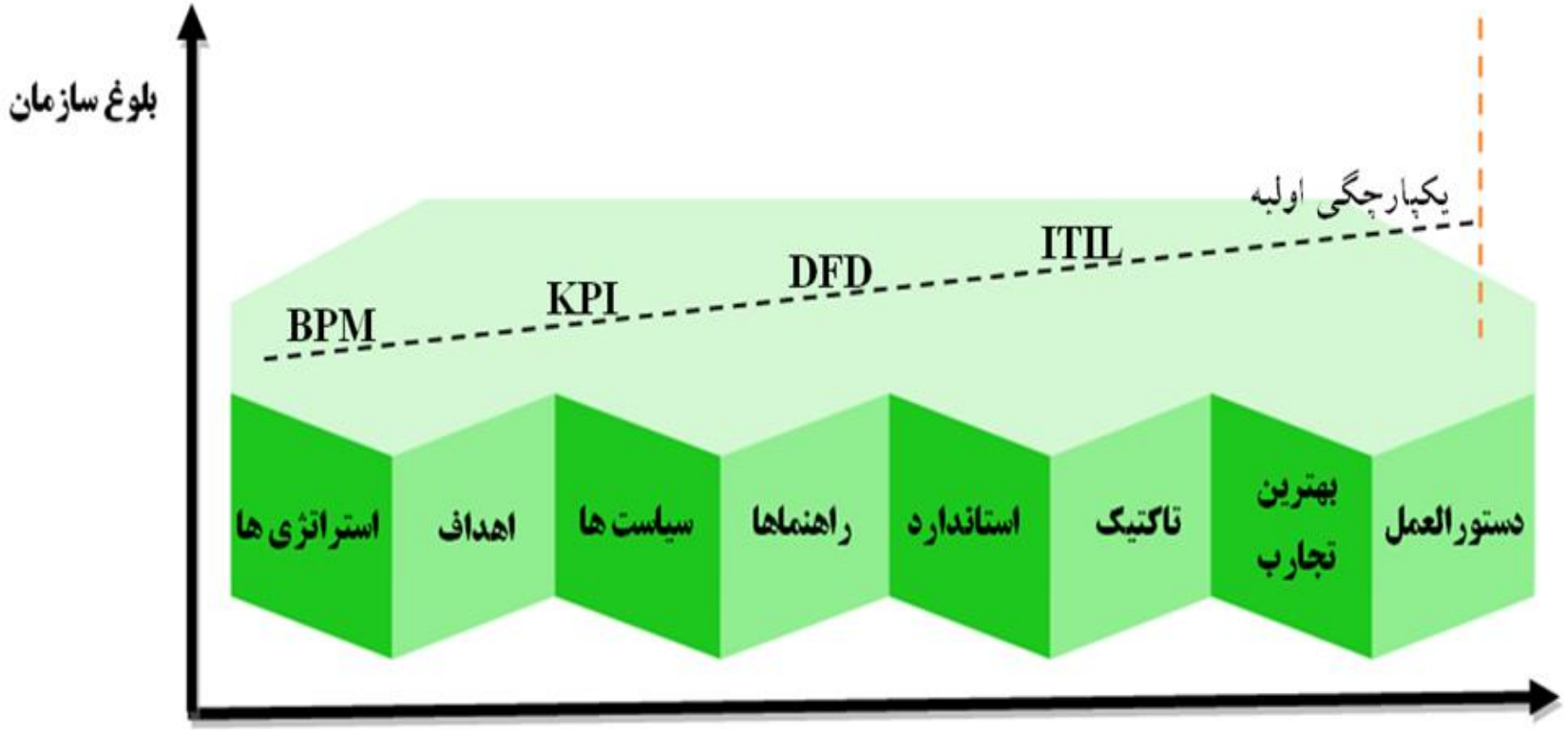
- ❖ محل نگهداری مدیریت دارایی فناوری اطلاعات.
- ❖ موجودی سخت افزار و نرم افزار و اطلاعات استفاده از آنها.
- ❖ ادغام با IT و سیستم های تجاری مجاور.
- ❖ ورود داده ها.

هشت مرحله برای ایجاد و پایداری کسب و کار سازمان



هشت مرحله برای ایجاد و پایداری کسب و کار سازمان

مراحل برای رسیدن به یکپارچگی اولیه و تصویر جامع از سازمان



جدول تهدیدات

B	C	D	E	F	G	H
قوانین حاکمیتی	مصوبات هیات دولت	عوامل سازمانی یا درونی	فرهنگ سازمانی	عوامل فناوری یا تکنولوژی	سخت افزار	سخت افزار های فرسوده
	قانون اساسی کشور		قوانین سازمانی			گواهینامه امنیتی ندارد
	قوانین مجلس		مدیریت دانش			سخت افزار های بی کیفیت
	سازمان بازرسی		بودجه IT			تعدد مدل و انواع سخت افزار
	دیوان محاسبات کشور		نوع مدیریت IT		نرم افزار	نوع نرم افزار های موجود
قوانین بین المللی	NGO		نیروی انسانی			زبان برنامه نویسی ناامن است
	کنوانسیون ها		هکرهای داخلی			استاندارد های برنامه نویسی در
	IMO		چارت سازمانی و شرح وظایف			سورس کد موجود نیست
شرایط سیاسی منطقه	جنگ و درگیری		وضعیت آموزش			نرم افزار گواهینامه امنیتی ندارد
	تصمیمات سیاسی				شبکه	طراحی شبکه (سیسم یا بیسیم)
	وضعیت فناوری کشور های					IOS
شرایط اقتصادی منطقه	فقر در کشور های همسایه					Passive
	امنیت در کشور های همسایه					دستورات & Routting
	سودآوری IT در منطقه					مشکلات WAN
شرایط اقلیمی کشور	بلایای طبیعی					عدم پشتیبانی از تجهیزات شبکه
	رطوبت					تجهیزات تقلبی
	فاصله مراکز تا دریا و جزایر				بد افزار ها	کرم ها
	آب و هوا					اسب های تراوا
	سناد – مراکز شمال و جنوب					ویروس ها

جدول تهدیدات

B	C	D	E	F	G	H
پراکندگی مراکز	فاصله تا مراکز ICT				کنترل ها IT	آنتی ویروسها
	نوع اتباط موجود در مراکز					آنی اسپمها
جنگ	جنگ فیزیکی					دسترسی ها
	جنگ نرم(براندازی)					مجوزها
	جنگ سایبری					
استاندارد کشور	استاندارد زیر ساخت					قوانین اتصال به سیستم
	استاندارد مخابرا ت					
تحریم	تحریم های فناوری و IT				استانداردد های مدیریت	استانداردهای سرویس دهی
	تحریم های مالی					استانداردد های امنیتی
	تحریم های آموزشی					استانداردهای گزارش گیری
هکر ها	سیاسی					مانیتورینگ
	اقتصادی					
	ناشناس					
مشتریان	مشتریان IT				بانک اطلاعاتی	طراحی بانک داده
	مشتریان Bissness اصلی					انتخاب بانک داده
تامین کنندگان	مشاوران Bissness اصلی					کنترل بانک داده
	شرکت های واسط Bissness					
	پیمانکاران Bissness اصلی					
	شرکا Bissness اصلی					
قوانین جهانی IT	کنوانسیون های بین المللی					

جدول طبقه بندی عوامل تهدیدات سازمان

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

سخت افزار های بی کیفیت

	A	B	C	D	E	F	G
۱	کد عامل اصلی	شرح عامل اصلی	کد عامل ثانویه	شرح عامل ثانویه	کد عامل نهایی	شرح عامل نهایی	قابلیت کنترل و تغییر از منظر ادامه کسب و کار
۲	۱	عوامل بیرونی یا محیطی	۱۰۱	قوانین حاکمیتی	۱۰۱۱	قانون اساسی کشور	کنترل ندارد
۳	۱	عوامل بیرونی یا محیطی	۱۰۱	قوانین حاکمیتی	۱۰۱۲	مصوبات هیات دولت	ایجاد کنترل و تغییر زمانبر و دشوار است
۴	۱	عوامل بیرونی یا محیطی	۱۰۱	قوانین حاکمیتی	۱۰۱۳	قوانین مجلس	ایجاد کنترل و تغییر زمانبر و دشوار است
۵	۱	عوامل بیرونی یا محیطی	۱۰۱	قوانین حاکمیتی	۱۰۱۴	سازمان بازرسی	کنترل ندارد
۶	۱	عوامل بیرونی یا محیطی	۱۰۱	قوانین حاکمیتی	۱۰۱۵	دیوان محاسبات کشور	کنترل ندارد
۷	۱	عوامل بیرونی یا محیطی	۱۰۲	قوانین بین المللی	۱۰۲۱	NGO	کنترل ندارد
۸	۱	عوامل بیرونی یا محیطی	۱۰۲	قوانین بین المللی	۱۰۲۲	کنوانسیون ها	ایجاد کنترل و تغییر زمانبر و دشوار است
۱۰	۱	عوامل بیرونی یا محیطی	۱۰۳	شرایط سیاسی منطقه	۱۰۳۱	فضای رقابتی IT	کنترل ندارد
۱۱	۱	عوامل بیرونی یا محیطی	۱۰۳	شرایط سیاسی منطقه	۱۰۳۲	تصمیمات سیاسی	کنترل ندارد
۱۲	۱	عوامل بیرونی یا محیطی	۱۰۳	شرایط سیاسی منطقه	۱۰۳۳	وضعیت فناوری کشور های همسایه	کنترل ندارد
۱۳	۱	عوامل بیرونی یا محیطی	۱۰۴	شرایط اقتصادی منطقه	۱۰۴۱	فقر	کنترل ندارد
۱۴	۱	عوامل بیرونی یا محیطی	۱۰۴	شرایط اقتصادی منطقه	۱۰۴۲	امنیت	کنترل ندارد
۱۵	۱	عوامل بیرونی یا محیطی	۱۰۴	شرایط اقتصادی منطقه	۱۰۴۳	سودآوری	کنترل ندارد
۱۶	۱	عوامل بیرونی یا محیطی	۱۰۵	شرایط اقلیمی کشور	۱۰۵۱	بلایای طبیعی	کنترل ندارد
۱۷	۱	عوامل بیرونی یا محیطی	۱۰۵	شرایط اقلیمی کشور	۱۰۵۲	رطوبت	کنترل ندارد
۱۸	۱	عوامل بیرونی یا محیطی	۱۰۵	شرایط اقلیمی کشور	۱۰۵۳	فاصله مراکز تا دریا و جزایر	کنترل ندارد

جدول طبقه بندی عوامل تهدیدات سازمان

	کد عامل اصلی	شرح عامل اصلی	کد عامل ثانویه	شرح عامل ثانویه	کد عامل نهایی	شرح عامل نهایی	قابلیت کنترل و تغییر از منظر ادامه کسب و کار
۳۷	۱	عوامل بیرونی یا محیطی	۱۱۲	تامین کنندگان	۱۱۲۳	پیمانکاران Bissness اصلی	ایجاد کنترل و تغییر زمانبر و دشوار است
۳۸	۱	عوامل بیرونی یا محیطی	۱۱۳	قوانین جهانی IT	۱۱۳۱	کنوانسیون های بین المللی	کنترل ندارد
۳۹	۲	عوامل سازمانی یا درونی	۲۰۱	فرهنگ سازمانی	۲۰۱۱	فرهنگ امنیتی	ایجاد کنترل امکانپذیر است
۴۰	۲	عوامل سازمانی یا درونی	۲۰۱	فرهنگ سازمانی	۲۰۱۲	شناخت سازمانی	ایجاد کنترل امکانپذیر است
۴۱	۲	عوامل سازمانی یا درونی	۲۰۱	فرهنگ سازمانی	۲۰۱۳	منشور اخلاقی سازمان	ایجاد کنترل امکانپذیر است
۴۲	۲	عوامل سازمانی یا درونی	۲۰۲	قوانین سازمانی	۲۰۲۱	بخشنامه ها و دستور العمل های مدون	ایجاد کنترل و تغییر زمانبر و دشوار است
۴۳	۲	عوامل سازمانی یا درونی	۲۰۲	قوانین سازمانی	۲۰۲۲	جریمه ها	ایجاد کنترل امکانپذیر است
۴۴	۲	عوامل سازمانی یا درونی	۲۰۲	قوانین سازمانی	۲۰۲۳	شیوه های انجام کار	ایجاد کنترل و تغییر زمانبر و دشوار است
۴۵	۲	عوامل سازمانی یا درونی	۲۰۳	مدیریت دانش	۲۰۳۱	شناخت دانش	ایجاد کنترل امکانپذیر است
۴۶	۲	عوامل سازمانی یا درونی	۲۰۳	مدیریت دانش	۲۰۳۲	تولید دانش	ایجاد کنترل و تغییر زمانبر و دشوار است
۴۷	۲	عوامل سازمانی یا درونی	۲۰۳	مدیریت دانش	۲۰۳۳	انتقال دانش	ایجاد کنترل امکانپذیر است
۴۸	۲	عوامل سازمانی یا درونی	۲۰۴	بودجه	۲۰۴۱	بودجه IT	ایجاد کنترل امکانپذیر است
۴۹	۲	عوامل سازمانی یا درونی	۲۰۴	بودجه	۲۰۴۲	تمرکز بودجه براهداف	ایجاد کنترل امکانپذیر است
۵۰	۲	عوامل سازمانی یا درونی	۲۰۴	بودجه	۲۰۴۳	بیش بینی بودجه اضطراری	ایجاد کنترل امکانپذیر است
۵۱	۲	عوامل سازمانی یا درونی	۲۰۵	مدیریت IT	۲۰۵۱	مدیر آشنا به مشکلات و شناخت سازمان	ایجاد کنترل امکانپذیر است
۵۲	۲	عوامل سازمانی یا درونی	۲۰۵	مدیریت IT	۲۰۵۲	مدیر آشنا به استاندارد های فناوری	ایجاد کنترل امکانپذیر است
۵۳	۲	عوامل سازمانی یا درونی	۲۰۵	مدیریت IT	۲۰۵۳	مدیر با برنامه در خصوص فناوری و هدف اصلی سازمان	ایجاد کنترل امکانپذیر است

جدول طبقه بندی عوامل تهدیدات سازمان

	کد عامل اصلی	شرح عامل اصلی	کد عامل ثانویه	شرح عامل ثانویه	کد عامل نهایی	شرح عامل نهایی	قابلیت کنترل و تغییر از منظر ادامه کسب و کار
۵۷	۲	عوامل سازمانی یا درونی	۲۰۷	هکرهای داخلی	۲۰۷۱	متخصصین عصبانی و ناراضی با دسترسی بالا	ایجاد کنترل و تغییر زمانبر و دشوار است
۵۸	۲	عوامل سازمانی یا درونی	۲۰۷	هکرهای داخلی	۲۰۷۲	متخصصین کنجکاو	ایجاد کنترل و تغییر زمانبر و دشوار است
۵۹	۲	عوامل سازمانی یا درونی	۲۰۷	هکرهای داخلی	۲۰۷۳	فضای اعتماد غیر مطلوب	ایجاد کنترل و تغییر زمانبر و دشوار است
۶۰	۲	عوامل سازمانی یا درونی	۲۰۸	چارت سازمانی و شرح وظایف	۲۰۸۱	سلسله مراتب سازمانی	ایجاد کنترل امکانپذیر است
۶۱	۲	عوامل سازمانی یا درونی	۲۰۸	چارت سازمانی و شرح وظایف	۲۰۸۲	شرح شغل و شاغل	ایجاد کنترل امکانپذیر است
۶۲	۲	عوامل سازمانی یا درونی	۲۰۸	چارت سازمانی و شرح وظایف	۲۰۸۳	تعهدات سازمانی	ایجاد کنترل امکانپذیر است
۶۳	۲	عوامل سازمانی یا درونی	۲۰۹	وضعیت آموزش	۲۰۹۱	آموزش های بدو خدمت	ایجاد کنترل امکانپذیر است
۶۴	۲	عوامل سازمانی یا درونی	۲۰۹	وضعیت آموزش	۲۰۹۲	آموزش های تخصصی حین کار	ایجاد کنترل امکانپذیر است
۶۵	۲	عوامل سازمانی یا درونی	۲۰۹	وضعیت آموزش	۲۰۹۳	آموزش های امنیتی	ایجاد کنترل امکانپذیر است
۶۶	۲	عوامل سازمانی یا درونی	۲۰۹	وضعیت آموزش	۲۰۹۴	آموزش های فرا سازمانی و مدنی	ایجاد کنترل و تغییر زمانبر و دشوار است
۶۷	۲	عوامل سازمانی یا درونی	۲۰۹	وضعیت آموزش	۲۰۹۵	برنامه آموزشی	ایجاد کنترل امکانپذیر است
۶۹	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۱	استانداردهای مدیریت سرویس دهی	ایجاد کنترل امکانپذیر است
۷۰	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۲	استاندارد های مدیریت امنیتی	ایجاد کنترل امکانپذیر است
۷۱	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۳	استانداردهای گزارش گیری	ایجاد کنترل امکانپذیر است
۷۲	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۴	مانیتورینگ پویا	ایجاد کنترل امکانپذیر است
۷۳	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۱	آنتی ویروسها	ایجاد کنترل امکانپذیر است
۷۴	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۲	آنی اسپمها	ایجاد کنترل امکانپذیر است

جدول طبقه بندی عوامل تهدیدات سازمان

	A	B	C	D	E	F	G
۱	کد عامل اصلی	شرح عامل اصلی	کد عامل ثانویه	شرح عامل ثانویه	کد عامل نهایی	شرح عامل نهایی	قابلیت کنترل و تغییر از منظر ادامه کسب و کار
۶۹	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۱	استانداردهای مدیریت سرویس دهی	ایجاد کنترل امکانپذیر است
۷۰	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۲	استاندارد های مدیریت امنیتی	ایجاد کنترل امکانپذیر است
۷۱	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۳	استانداردهای گزارش گیری	ایجاد کنترل امکانپذیر است
۷۲	۳	عوامل فناوری یا تکنولوژی	۳۰۱	استاندارد های مدیریت	۳۰۱۴	مانیتورینگ پویا	ایجاد کنترل امکانپذیر است
۷۳	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۱	آنتی ویروسها	ایجاد کنترل امکانپذیر است
۷۴	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۲	آنی اسپیها	ایجاد کنترل امکانپذیر است
۷۵	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۳	دسترسی ها	ایجاد کنترل امکانپذیر است
۷۶	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۴	مجوزها	ایجاد کنترل امکانپذیر است
۷۷	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۵	فایروال ها	ایجاد کنترل امکانپذیر است
۷۸	۳	عوامل فناوری یا تکنولوژی	۳۰۲	کنترل ها IT	۳۰۲۶	قوانین اتصال	ایجاد کنترل امکانپذیر است
۷۹	۳	عوامل فناوری یا تکنولوژی	۳۰۳	شبکه	۳۰۳۱	Active	ایجاد کنترل امکانپذیر است
۸۰	۳	عوامل فناوری یا تکنولوژی	۳۰۳	شبکه	۳۰۳۲	Passive	ایجاد کنترل و تغییر زمانبر و دشوار است
۸۱	۳	عوامل فناوری یا تکنولوژی	۳۰۳	شبکه	۳۰۳۳	پهنای باند موجود و بستر های ارتباطی	ایجاد کنترل امکانپذیر است
۸۲	۳	عوامل فناوری یا تکنولوژی	۳۰۳	شبکه	۳۰۳۴	مدل طراحی شبکه (توپولوژی)	ایجاد کنترل امکانپذیر است
۸۳	۳	عوامل فناوری یا تکنولوژی	۳۰۳	شبکه	۳۰۳۵	سیستم های عامل و به روز رسانی	ایجاد کنترل امکانپذیر است
۸۴	۳	عوامل فناوری یا تکنولوژی	۳۰۳	شبکه	۳۰۳۶	نگهداری و پشتیبانی	ایجاد کنترل امکانپذیر است

جدول طبقه بندی عوامل تهدیدات سازمان

کد عامل اصلی	شرح عامل اصلی	کد عامل ثانویه	شرح عامل ثانویه	کد عامل نهایی	شرح عامل نهایی	قابلیت کنترل و تغییر از منظر ادامه کسب و کار
۱۰۲	۳	عوامل فناوری یا تکنولوژی	۳۰۷	سخت افزار	۳۰۷۵	پشتیبانی	ایجاد کنترل امکانپذیر است
۱۰۳	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۱	Mail server	ایجاد کنترل امکانپذیر است
۱۰۴	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۲	Web Server	ایجاد کنترل امکانپذیر است
۱۰۵	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۳	DNS derver	ایجاد کنترل امکانپذیر است
۱۰۶	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۴	File Server	ایجاد کنترل امکانپذیر است
۱۰۷	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۵	Domain Contoler	ایجاد کنترل امکانپذیر است
۱۰۸	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۶	Shairpont server	ایجاد کنترل امکانپذیر است
۱۰۹	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۷	BPMS Server	ایجاد کنترل امکانپذیر است
۱۱۰	۳	عوامل فناوری یا تکنولوژی	۳۰۸	سرویس ها	۳۰۸۸	Portal	ایجاد کنترل امکانپذیر است
۱۱۱	۳	عوامل فناوری یا تکنولوژی	۳۰۹	UPS	۳۰۹۱	تناسب با حجم کار و استراتژی	ایجاد کنترل امکانپذیر است
۱۱۲	۳	عوامل فناوری یا تکنولوژی	۳۰۹	UPS	۳۰۹۲	تعمیر و نگهداری	ایجاد کنترل امکانپذیر است
۱۱۳	۳	عوامل فناوری یا تکنولوژی	۳۱۰	RAK	۳۱۰۱	شاسی و تجهیزات	ایجاد کنترل امکانپذیر است
۱۱۴	۳	عوامل فناوری یا تکنولوژی	۳۱۱	اتاق سایت	۳۱۱۱	جایگاه احداث و اندازه متناسب با تجهیزات موجود	کنترل ندارد
۱۱۵	۳	عوامل فناوری یا تکنولوژی	۳۱۱	اتاق سایت	۳۱۱۲	تهویه و سرمایش	ایجاد کنترل امکانپذیر است
۱۱۶	۳	عوامل فناوری یا تکنولوژی	۳۱۱	اتاق سایت	۳۱۱۳	کنترل تردد و دسترسی	ایجاد کنترل امکانپذیر است
۱۱۷	۳	عوامل فناوری یا تکنولوژی	۳۱۱	اتاق سایت	۳۱۱۴	سازه و طراحی	کنترل ندارد
۱۱۸	۳	عوامل فناوری یا تکنولوژی	۳۱۱	اتاق سایت	۳۱۱۵	چاه Earth	کنترل ندارد

رخدادها

- حملات DDOS
- BackDoor های سیسکو و ...
- فیشینگ سایت ها
- سرقت هویت
- .....

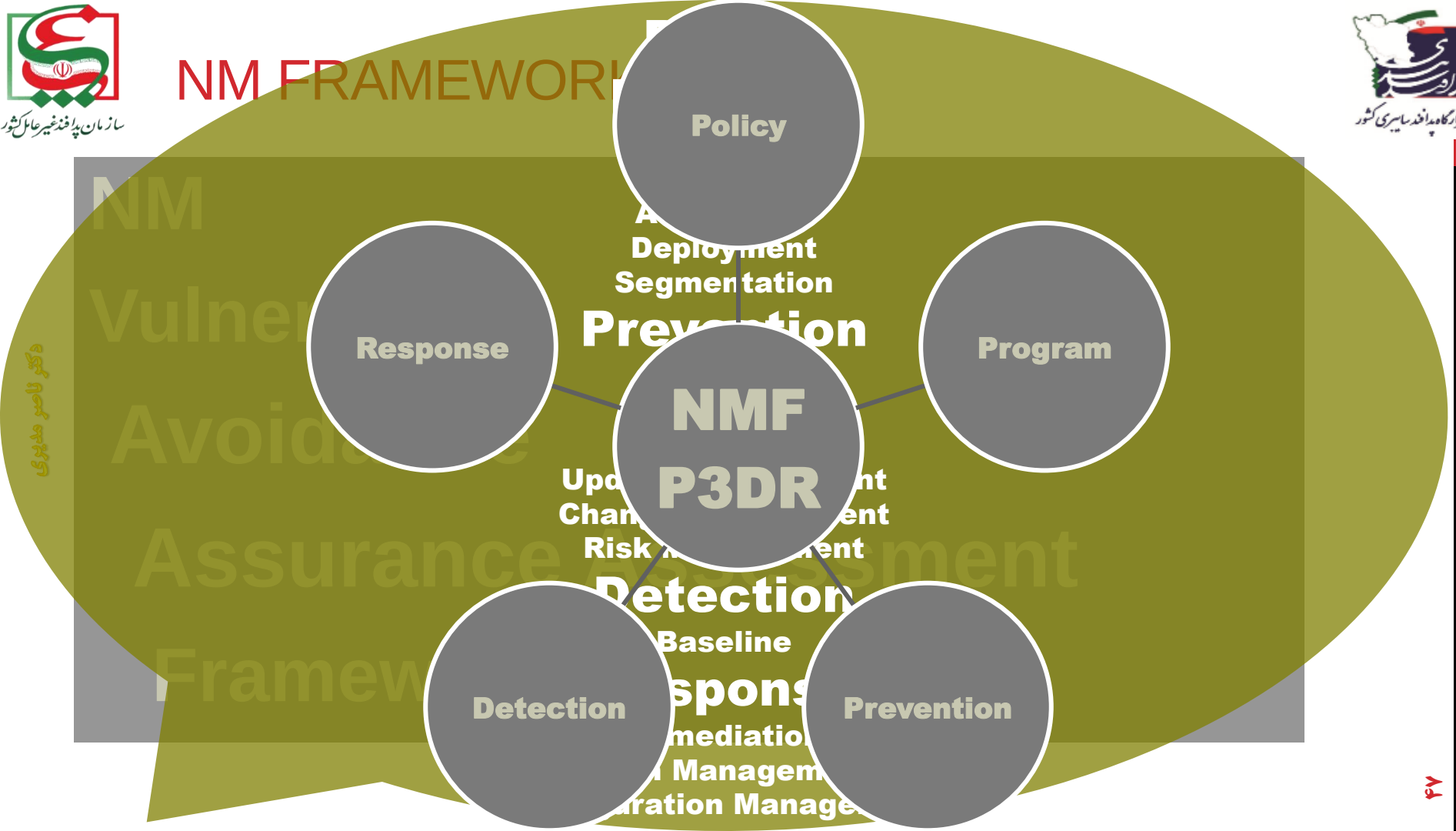
مرکز بانک اطلاعاتی ملی کاستی‌های ...
National Vulnerability Database

Policy
Program
Prevention
Detection
Response

Risk-Avoidance Assurance Assessment Model – RA3M

دکتر ناصر مدیری

NM FRAMEWORK



مدیریت امنیت اطلاعات

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 اطلاعات مشتمل بر:

- مدیریت پیکربندی
- مدیریت تغییرات
- مدیریت مخاطرات

مدیریت پیکربندی

فرآیندی است برای حصول اطمینان از اینکه تغییرات در سیستم تاثیر 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.

ایجاد روال های جدید، تجدید سخت افزارها، بروز رسانی نرم افزارها، اتصالات جدید شبکه و کاربران جدید از جمله تغییرات سیستم اطلاعات هستند.

مدیریت مخاطرات

- ریسک یا مخاطره عبارت است از احتمال ضرر و زیانی که متوجه یک دارایی سازمان (در اینجا اطلاعات) میباشد.

عدم قطعیتِ (در نتیجه مقیاس ناپذیری) یکی از مهمترین ویژگیهای مفهوم ریسک است. طبعاً این عدم قطعیت به معنای غیر قابل محاسبه و مقایسه بودن ریسکها نیست.

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)

نظام رصد تهدیدات شبکه های کامپیوتری

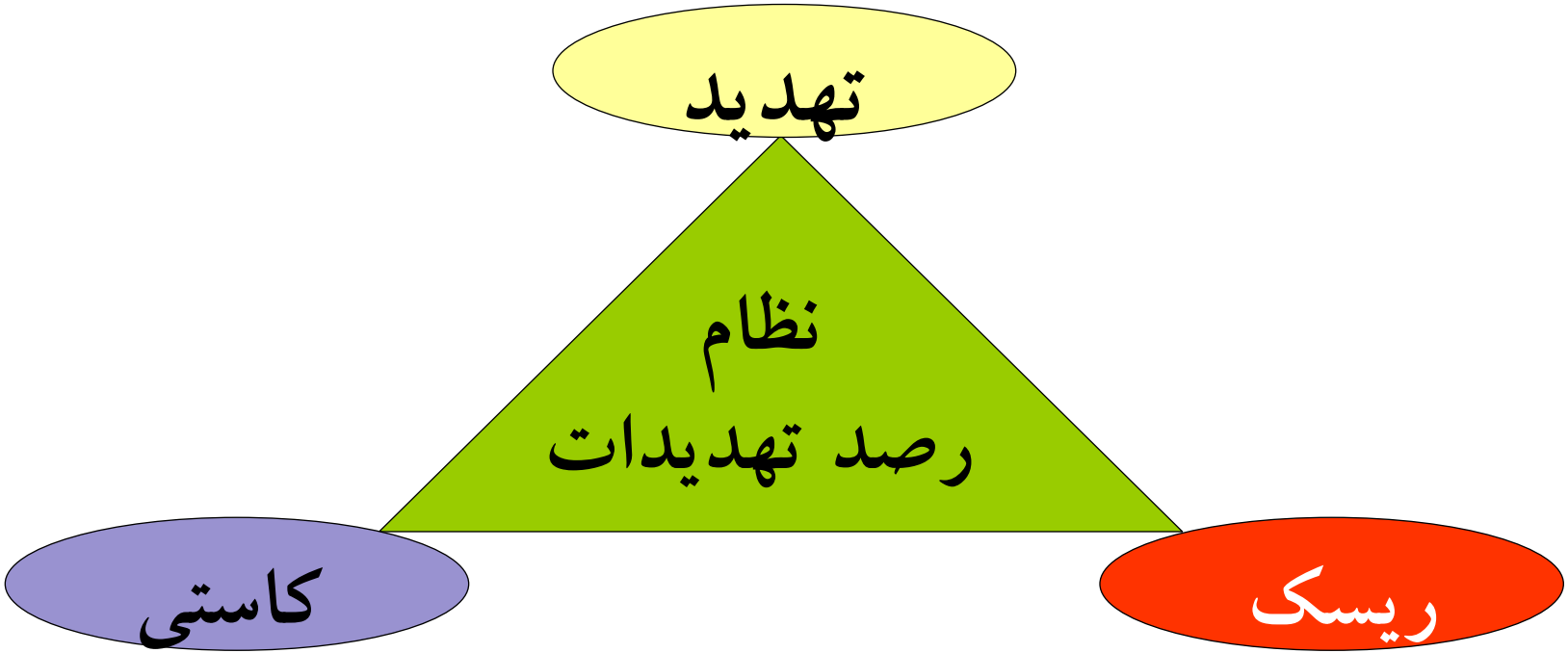
نیاز مبرم برای ایجاد ساختار جهت رصد تهدیدات شبکه ها و تدوین ساختاری که توسط آن بتوان رابطه بین سه عامل مهم زیر را در شبکه برآورد نمود:

- کاستی ها
- تهدیدات
- ریسک ها

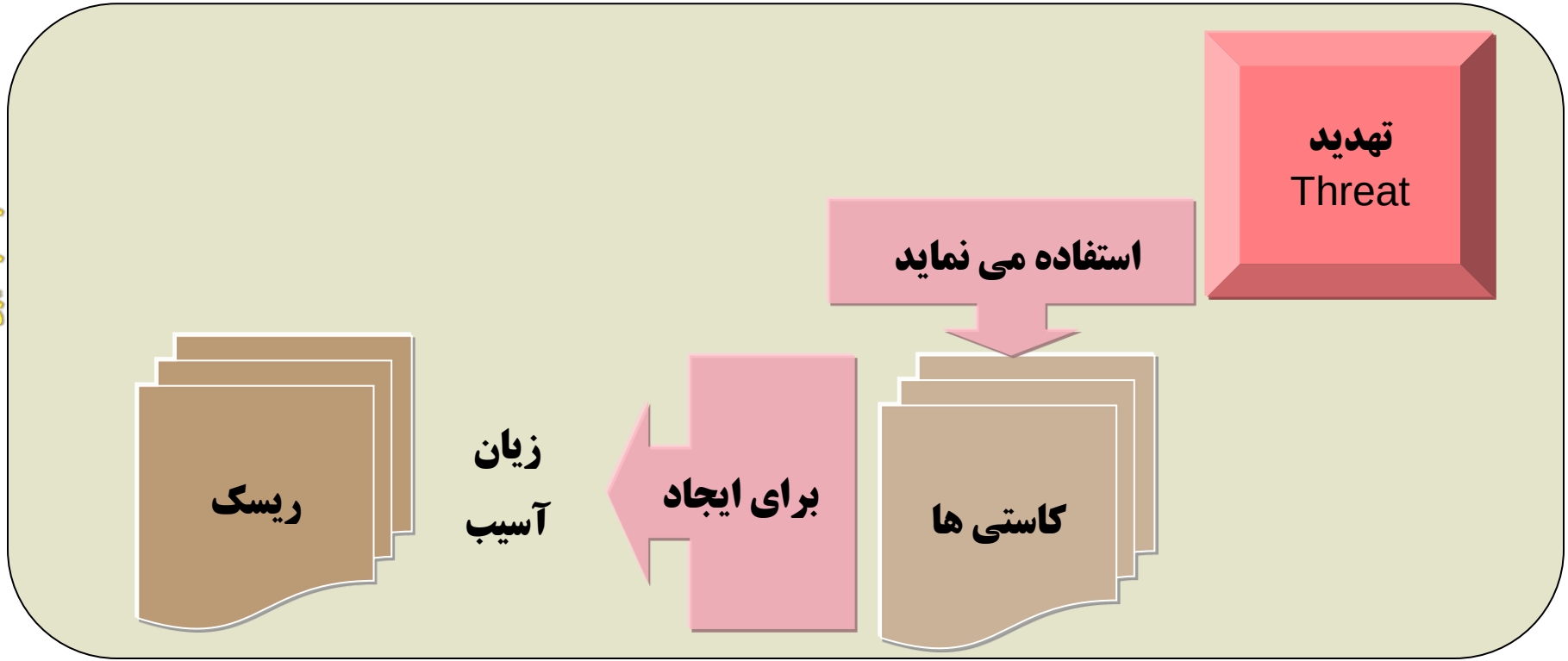
تدوین رابطه های:

- کاستی ها و تهدیدات
- تهدیدات و ریسک
- کاستی ها و ریسک
- تاثیر گذاری تهدیدات

نظام رصد تهدیدات شبکه های کامپیوتری (ادامه)



الزامات عدم امنیت



ریسک ها

ریسک ها (Risks) را میتوان از منظرهای ذیل بررسی نمود:

Dangerخطر، مخاطره، ورطه

Jeopardyخطر، مخاطره، ورطه

Perilخطر، مخاطره

Hazard، خطر کردن، به مخاطره انداختن، به بخت و طالع واگذار کردن

Menace تهدید، بیم داد، ارعاب

Threatخطر هراس، بیم داد،

Safety ایمنی، ضامن

Possibilityامکان پذیر بودن، قابل اتفاق، شودنی بودن، ممکن

Chance بخت، اقبال، احتمال، تصادف، فرصت

ریسک ها (ادامه)

Gamble به خطر انداختن

Probability احتمال وقوع

Stakeموضوع شرط بندی

Consequenceپیامد، نتیجه، برآیند

Attemptکوشش، سعی، مجاهدت، جهدکردن

Ventureبا جرعت عمل کردن

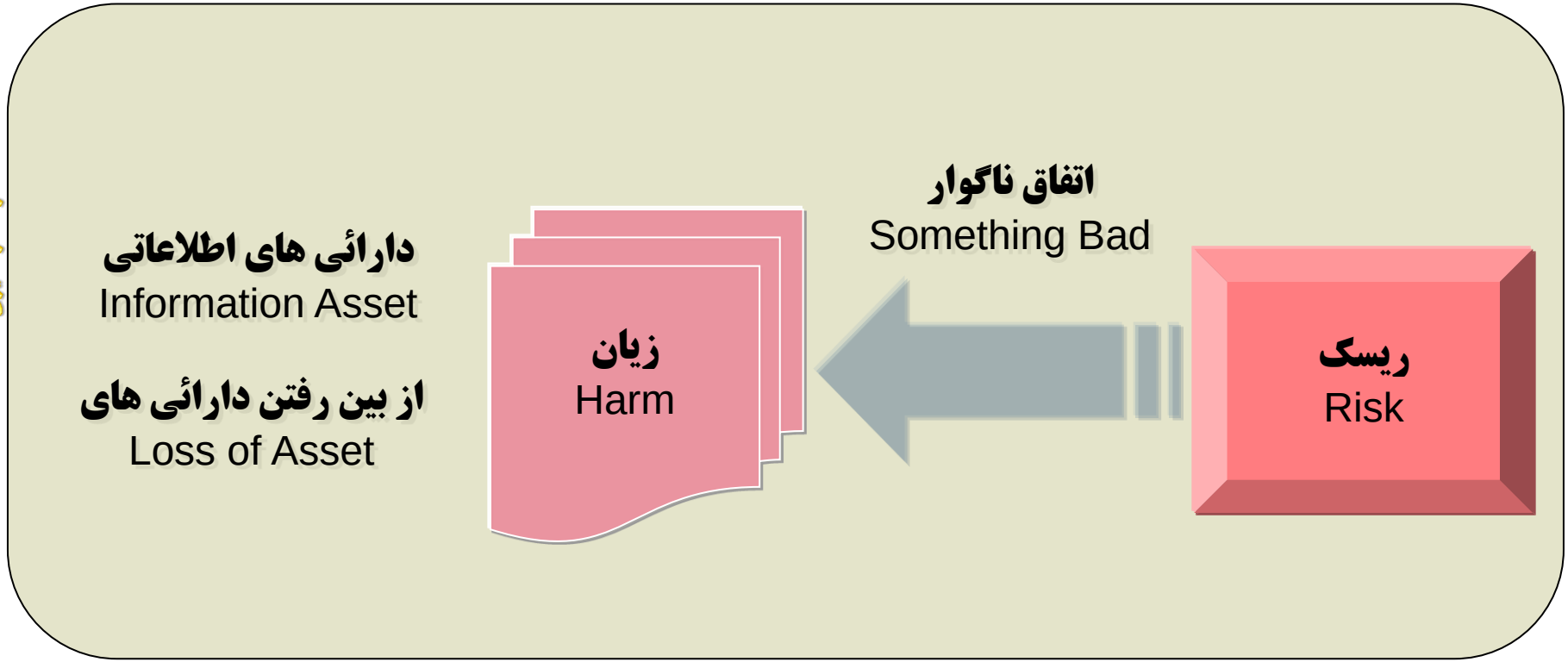
به **Endanger** خطر انداختن، به مخاطره انداختن، ورطه

Imperilبه مخاطره انداختن

Expose آشکار سازی، پرده گشایی، در معرض قرارگرفتن

ریسک ها از دیدگاه **Danger** ، **Hazard**، **Consequence**، **Endanger**، و **Expose** بررسی خواهند شد.

رابطه ریسک و امنیت (ادامه)



کاستی ها

کاستی ها (Vulnerabilities) را میتوان از منظرهای ذیل بررسی نمود:

Susceptibility مستعد بودن، استعداد، آسیب پذیری

Weaknessناتوانی، سستی، بی استحکامی، عیب، کاستی، نقص، نقطه ضعف

Defenselessnessبلادفاع

Helplessnessعجز، ناتوانی

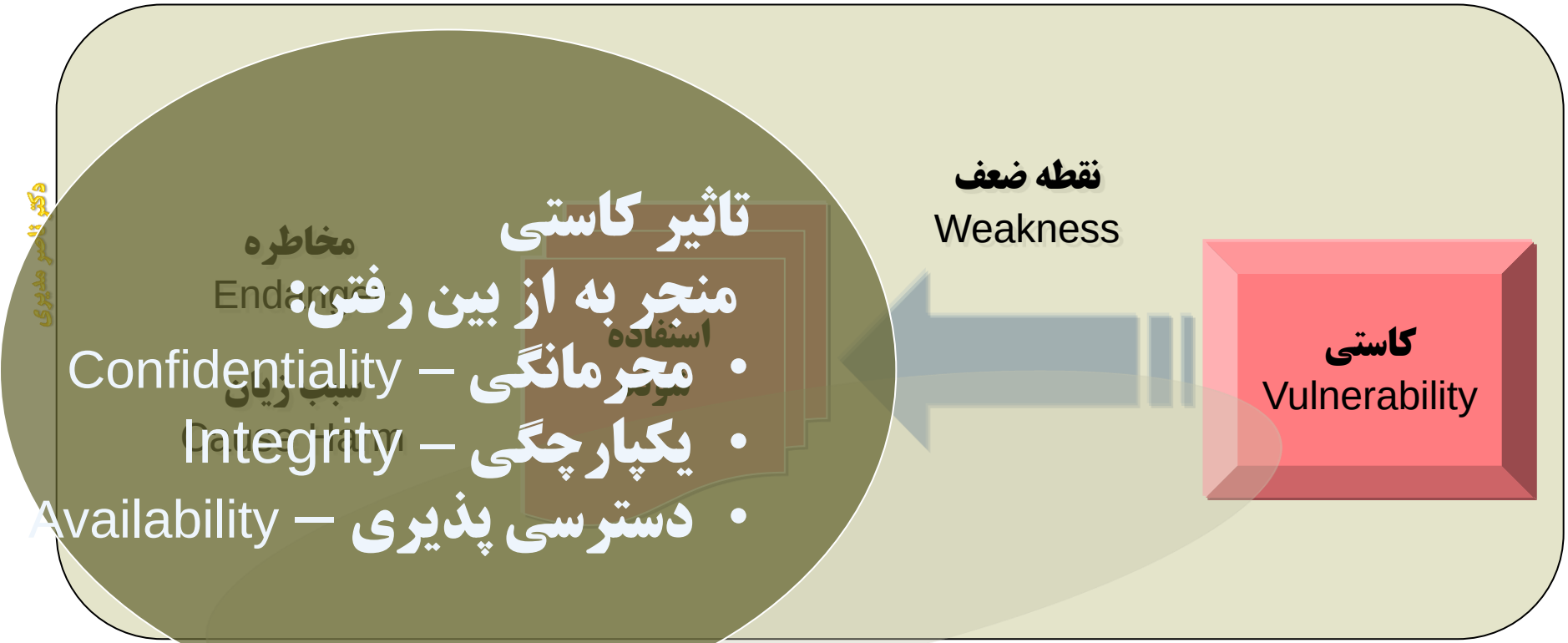
Opennessبازبودن

Exposureنمایش، در معرض قرارگرفتن

Liabilityنقطه ضعیف، عیب

تهدیدات از دیدگاه Defenselessness و Exposure بررسی خواهند شد.

رابطه کاستی و امنیت



تهدیدات

تهدیدات (Threats) را میتوان از منظرهای ذیل بررسی نمود:

Intimidation هراس انگیزی، بیم گستری

Pressure فشار، تنگنا

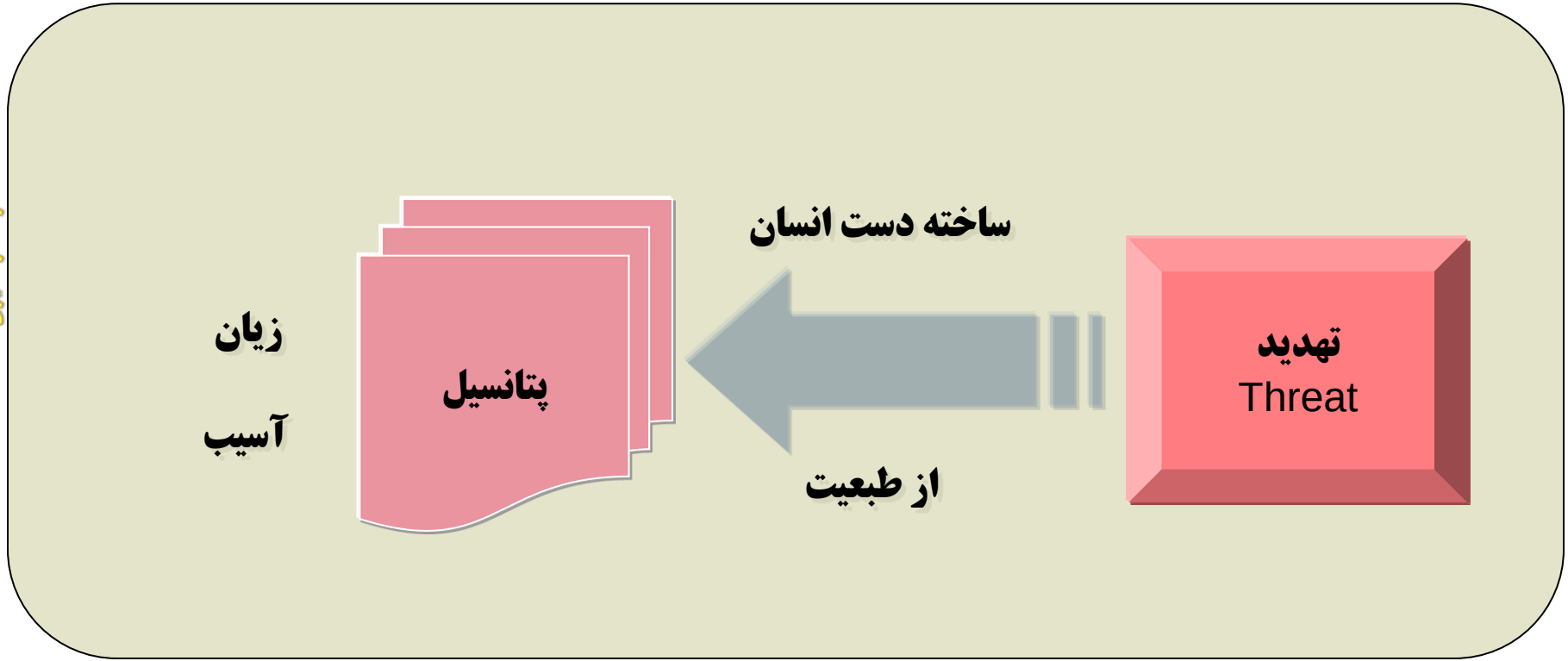
Bullying زورگویی، گردن کلفتی کردن

Terrorization مردم ترسانی، ارعاب

Coercion اعمال زور، زورگویی، فشار

تهدیدات از دیدگاه **Coercion** بررسی خواهند شد.

رابطه تهدید و امنیت



تهدیدات

تهدیدات (Threats) را میتوان از منظرهای ذیل بررسی نمود:

Intimidationهراس انگیزی، بیم گستری

Pressureفشار، تنگنا

Bullyingزورگویی، گردن کلفتی کردن

Terrorizationمردم ترسانی، ارعاب

Coercionاعمال زور، زورگویی، فشار

تهدیدات از دیدگاه Coercion بررسی خواهند شد.

کاستی ها

کاستی ها (Vulnerabilities) را میتوان از منظرهای ذیل بررسی نمود:

Susceptibilityمستعد بودن، استعداد، آسیب پذیری

Weaknessناتوانی، سستی، بی استحکامی، عیب، کاستی، نقص، نقطه ضعف

Defenselessnessبلادفاع

Helplessnessعجز، ناتوانی

Opennessبازبودن

Exposureنمایش، در معرض قرارگرفتن

Liabilityنقطه ضعیف، عیب

تهدیدات از دیدگاه Defenselessness و Exposure بررسی خواهند شد.

ریسک ها

ریسک ها (Risks) را میتوان از منظرهای ذیل بررسی نمود:

Dangerخطر، مخاطره، ورطه

Jeopardyخطر، مخاطره، ورطه

Perilخطر، مخاطره

Hazardاتفاق، خطر کردن، به مخاطره انداختن، به بخت و طالع واگذار کردن

Menaceتهدید، بیم داد، ارعاب

Threatخطر هراس، بیم داد،

Safetyایمنی، ضامن

Possibilityامکان پذیر بودن، قابل اتفاق، شودنی بودن، ممکن

Chanceبخت، اقبال، احتمال، تصادف، فرصت

ریسک ها

Gambleبه خطر انداختن

Probabilityاحتمال وقوع

Stakeموضوع شرط بندی

Consequenceپیامد، نتیجه، برآیند

Attemptکوشش، سعی، مجاهدت، جهدکردن

Ventureبا جرعت عمل کردن

Endangerبه خطر انداختن، به مخاطره انداختن، ورطه

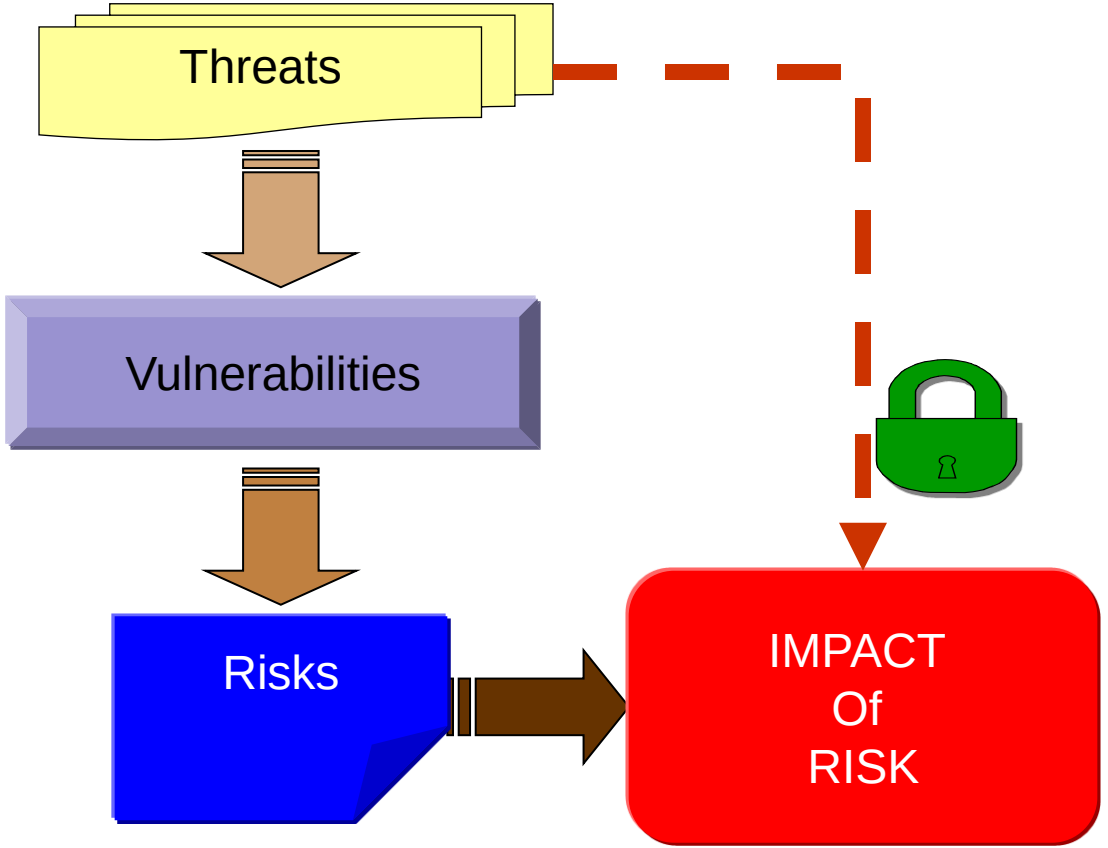
Imperilبه مخاطره انداختن

Exposeآشکار سازی، پرده گشایی، در معرض قرارگرفتن

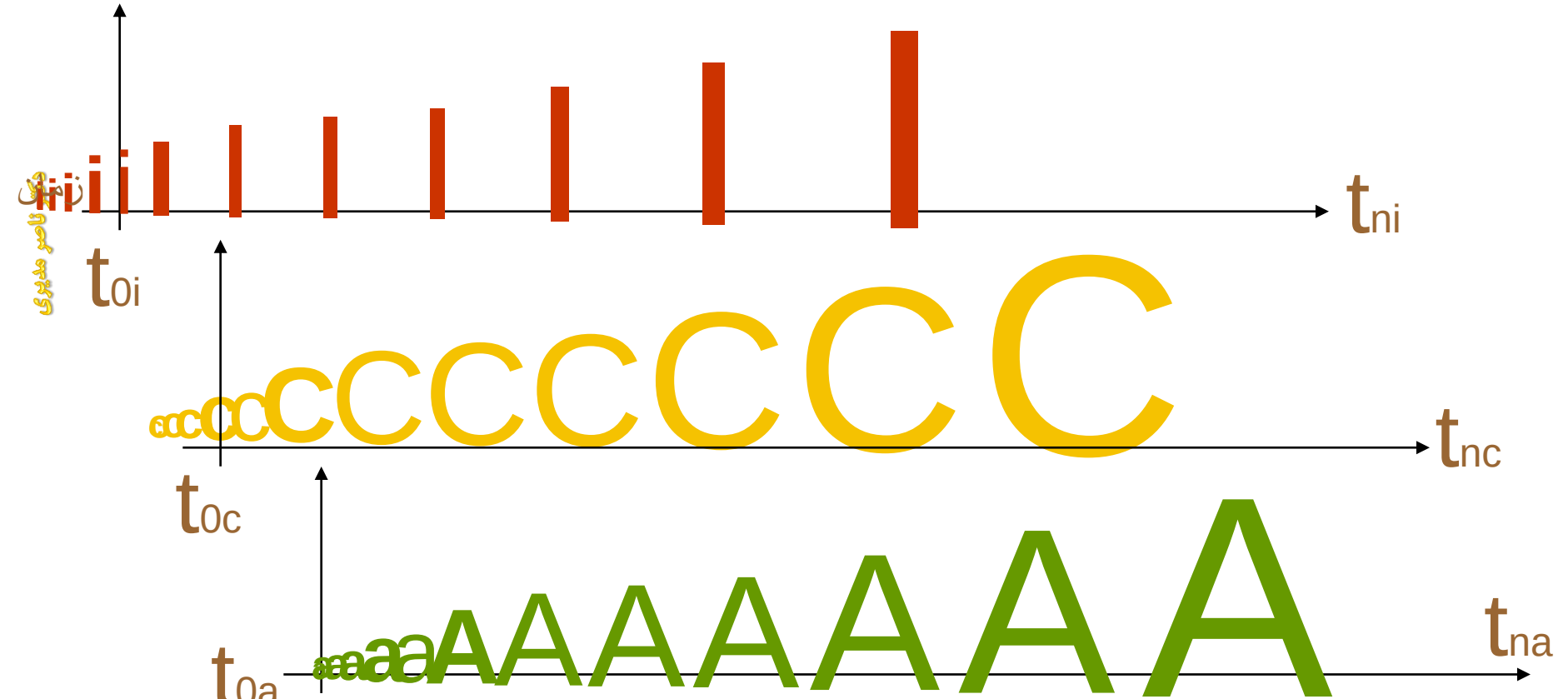
ریسک ها از دیدگاه Danger ، Hazard، Consequence، Endanger، و Expose بررسی خواهند شد.

تهدیدات – ریسک ها

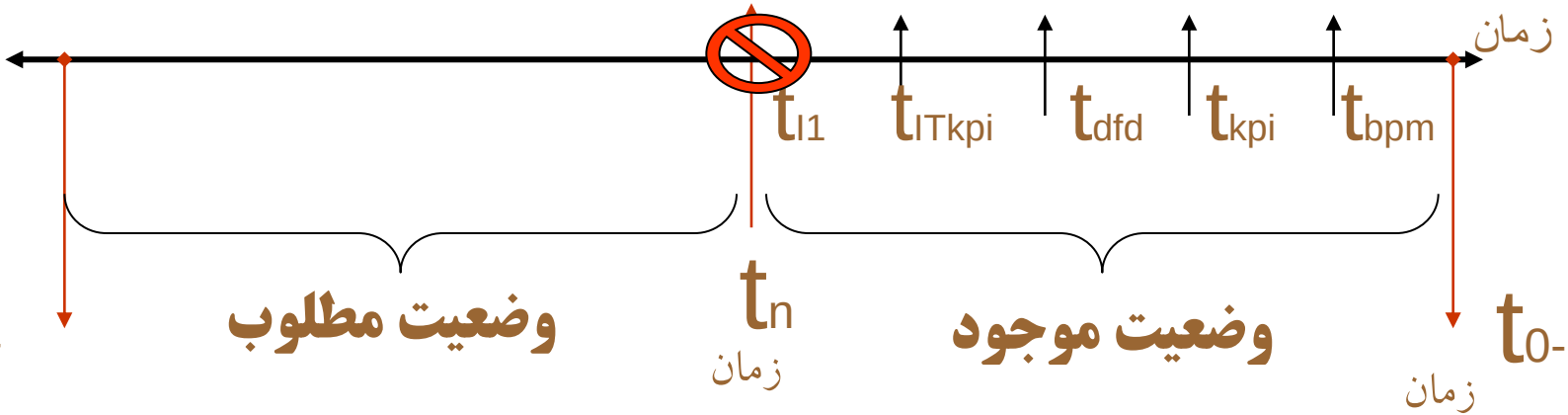
چرخه حیات تهدیدات



الزامات امنیت



الزامات امنیت – وضعیت موجود



t_{bpm} = Business Process Management First Time

t_{kpi} = Organization KPIs

t_{dfd} = DFD0, DFD1 and DFD2

t_{ITkpi} = ITIL KPIs First Time

t_{I1} = Integrity First Time

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

نقشه راه توسعه گستر ایمنی، امنیت و دفاع سایبری

CYBERSCAPE PATH

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

مدیریت سرمایه ها و دارایی ها سایبری
IT Asset Management (ITAM)

CONFIGURATION MANAGEMENT
مدیریت پیکربندی

مسیر فرآیندها

مدیریت خدمات فناوری اطلاعات

۷ نوع گواهینامه

متخصص حرفه ای مدیریت دارایی (CAMP)
مدیر دارایی نرم‌افزار (CSAM)
متخصص دارایی مدیریت سخت‌افزار ((CHAMP
مدیر دارایی موبایل (CMAM)
صدور گواهینامه در دارایی (CITAD)
کارشناس امنیتی خبره مدیریت دارایی (CAMSE)
مدیر دارایی IT (CITAM)

IT Service Management (ITSM)

مدیریت خدمات فناوری اطلاعات
ظارت و مدیریت رویدادها
مدیریت خطاها و مشکلات
مدیریت تغییر
مدیریت خدمات مشتریان
مدیریت درخواست‌های فناوری اطلاعات
مدیریت اطلاعات پیکربندی
مدیریت بهبود و بهینه سازی
مدیریت کارمندان

فواید ITAM بر ITSM

مدیریت رخداد: (Event Management)
مدیریت تغییر: (Change Management)
مدیریت مشکل: (Problem Management)

مسیر

سرمایه ها و آسیب پذیری ها
مخاطره ها
امنیت
جنگ آمادگی دفاع

سرمایه

ثابت
ملموس
تجهیزات
دیتا سنتر

دارائی

پویا
چه خدماتی
ارزش افزوده خدمات
چندین برابر سرمایه
وابستگی/همبستگی/هم راستایی/هم افزایی
تاثیر پذیری از یکدیگر
تاثیر گذاری بر همدیگر
رابطه ها
سرویس/خدمت
رویکرد/روش استفاده
اطلاعات/پیکره بندی/....

کتاب Vsحل مسئله

سرمایه و آسیب پذیری ها

عملیات
فرآیندهای ITIL
تدوین استراتژی سرویس ITIL
طراحی سرویس ITIL
انتقال سرویس ITIL
اجرای سرویس ITIL
توسعه سرویس ITIL

ITAM (Information Technology Asset Management)

مدیریت دارایی
هزینه‌های نگهداری را کاهش می‌دهد
دارایی‌های بلااستفاده را کاهش می‌دهد
خطرات امنیتی را محدود کرده و از نشت داده‌ها جلوگیری می‌کند
به شناسایی سریع‌تر مشکلات کمک می‌کند
به رعایت و آمادگی برای حسابرسی‌ها کمک می‌کند
به تصمیم گیری‌های بهتر کمک می‌کند
منجر به استفاده بیشتر از مجوزها (licenses)می‌شود

انجمن بین‌المللی مدیران دارایی فناوری اطلاعات (IAITAM)

نرم‌افزارهای ITAM

SysAid
Cherwell
Device42
ServiceNowS
olarWinds
AssetCloud
Asset Panda
BMC Track-It
LogMeIn Central
MMSoft Pulseway
GoCodes Asset Management
ManageEngine AssetExplorer
Ivanti IT Asset Management Suite

فرآیندهای زیرساختی

SMB

کوچک = ۱۵۰ – ۲۰۰
مستوسط = ۵۰۰ – ۷۰۰
بزرگ = ۱۰۰+۱۵۰۰
صنعتی های = ۱۵۰۰–۲۰۰۰

چارچوب

NIST
NIST-CSF
CRA
25 Architectures

کاهش صورت مسئله

18 CSCs
CIS Controls
OWASP (10)
CheatSheets
CWE (25)
ASVS 1..4
Eval 1..7

پشتیبانی و نگهداری مدیریتی شبکه (ITSM)

خدمات فناوری اطلاعات (APQC)
نظارت و مدیریت رویدادها
مدیریت خطاها و مشکلات
مدیریت تغییر
مدیریت خدمات مشتریان
مدیریت درخواست‌های فناوری اطلاعات
مدیریت اطلاعات پیکربندی
مدیریت بهبود و بهینه سازی
مدیریت کارمندان

برنامه ریزی فنی مدیریتی شبکه

IT Service Management (ITSM)

مدیریت شبکه
SNMP
NMS
FCAPS
مدیریت رخداد
Snort Rules
ارزیابی ایمنی (مغناطیسی، تشعشعات فرکانسی، جاسازی و ...)

NOC

مدیریت دارایی
رصد و پایش
مقاوم سازی (اجرا، عملیات)
جداسازی (اجرا، عملیات)

پشتیبانی و نگهداری و شبکه

Network Admin
(CISCO Admin, VM Admin, HelpDesk, Nodes)

مرکز عملیات شبکه

Network Operation Centre (NOC)

Network Manager

دارائی

CMDB
Configuration Management System (CMS)
Docker
Containers
Kubernetes
DevOps
DevOpsSec
IaaS Images

IaaS (Infrastructure as a Service)
PaaS (Platform as a Service)
SaaS (Software as a Service)

پشتیبانی و نگهداری فنی شبکه

عملیات
فرآیندهای ITIL
تدوین استراتژی سرویس ITIL
طراحی سرویس ITIL
انتقال سرویس ITIL
اجرای سرویس ITIL
توسعه سرویس ITIL

ایمنی سایبری

ایمنی سایبری مجموعه ای از مراحل و اقدامات به منظور ترویج استفاده ایمن از شبکه و جلوگیری از قرار گرفتن در معرض بدافزار اینترنتی، کلاهبرداری یا سرقت است. آگاه کرد /به روز نگه داشتن آنها در مورد خطرات و مشکلاتی

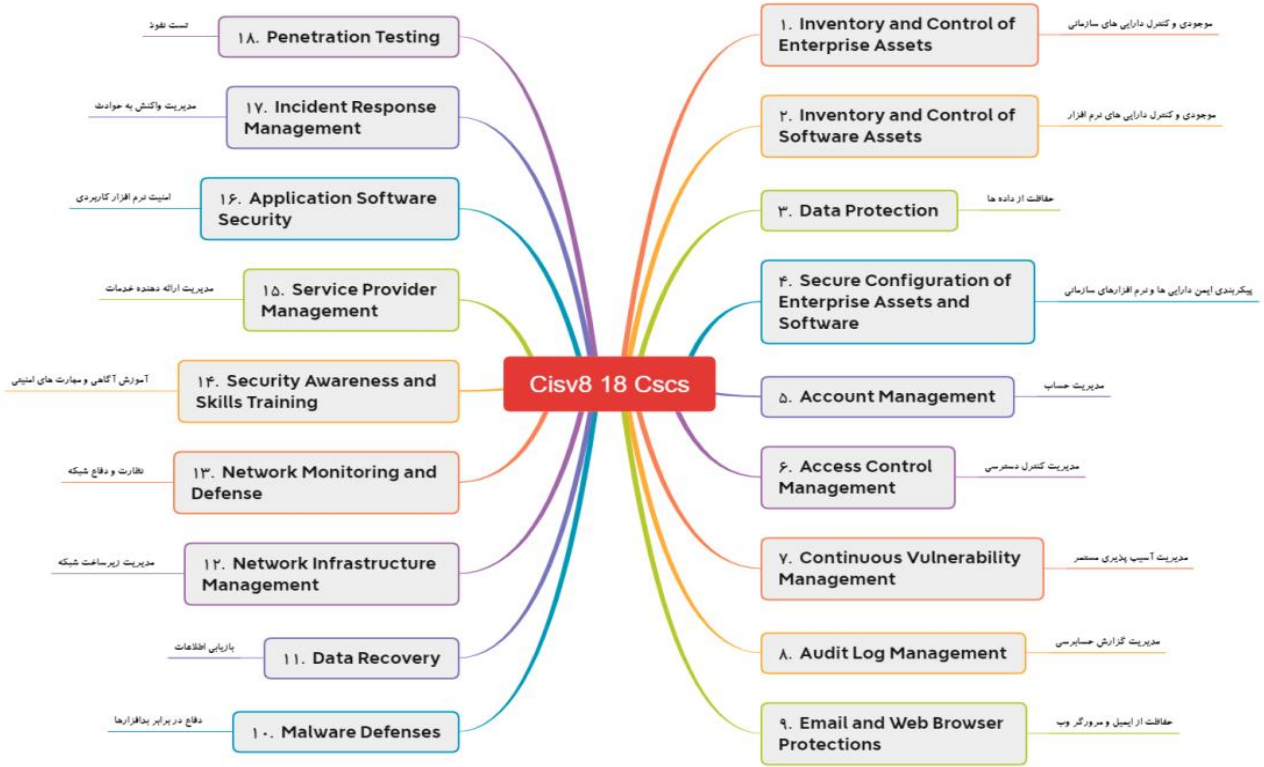
فعالیت های ایمن سازی:

- ❑ پیاده سازی احراز هویت چند عاملی در حسابها
- ❑ به روز رسانی خودکار نرم افزارهای امنیتی
- ❑ بررسی تمامی موارد قبل از کلیک برروی لینکهای مختلف
- ❑ استفاده از رمزهای عبور قوی

فرآیند های فنی ITSM

مدیریت رخداد: (Event Management)
مدیریت حوادث و رویداد ها: (Incident Management)
مدیریت بروزرسانی: (Update Management)
مدیریت پچ: (Patch Management)
مدیریت تغییر: (Change Management)
مدیریت مشکل: (Problem Management)

CISV8 18 CSCS



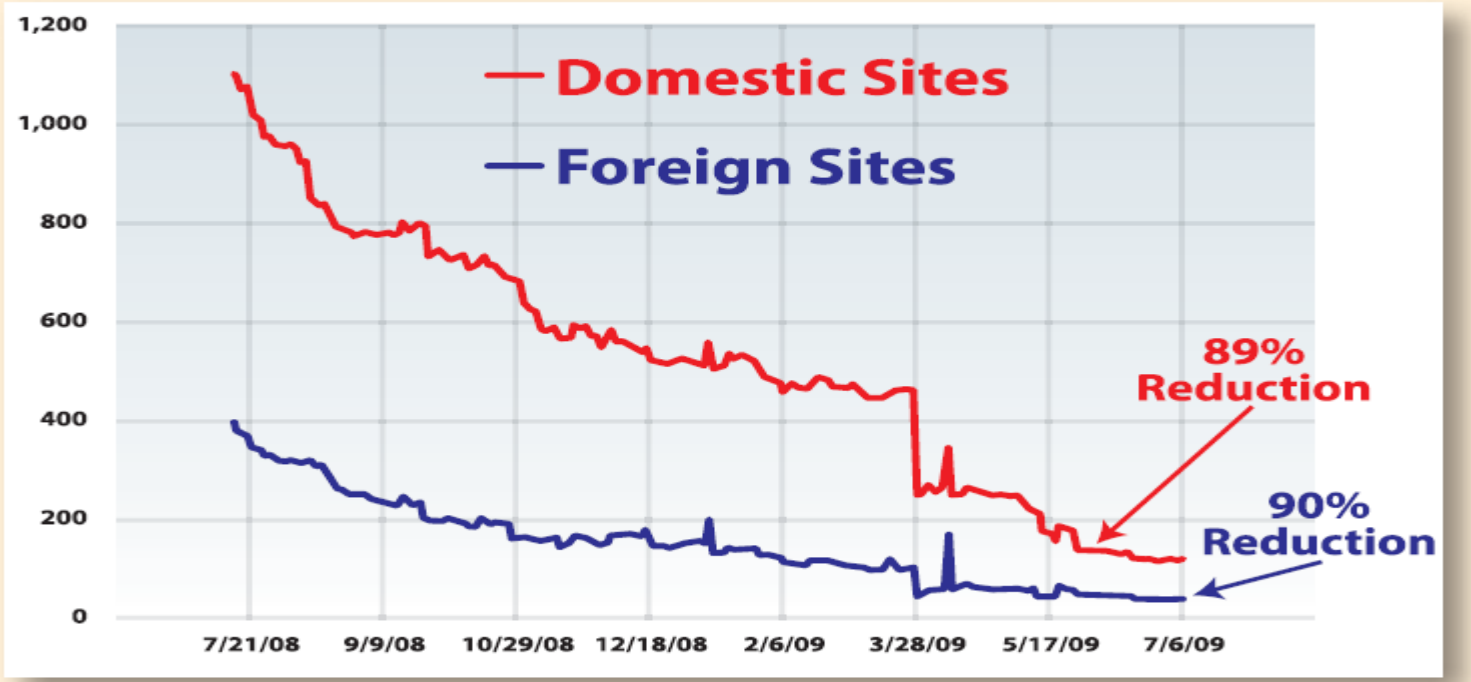
CISV8 18 CSCS

20 Critical Security Controls
for Effective Cyber Defense

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Security Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Incident Response Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Chart 1: 90% Risk Reduction In Less Than A Year

(U.S. State Department)



1
Inventory of Authorized and Unauthorized Devices

P PRIMARY:
Discovery, Vulnerability Assessment

S SECONDARY:
Network Access Control

SOLUTION = PROVIDER:

- P BSA Visibility = Insightix (McAfee)
- P IPSonar = Lumeta
- P CCM, IP360 = nCircle
- P Nmap = Open Source
- P QualysGuard = Qualys
- P Nexpose = Rapid7
- P CCS, RAS = Symantec
- P Nessus, Security Center = Tenable
- S Clear Pass = Aruba Networks
- S Network Sentry = Bradford Networks
- S Identity Services Engine (ISE) = Cisco
- S CounterAct = ForeScout Technologies

2
Inventory of Authorized and Unauthorized Software

P PRIMARY:
Software Change Management, Vulnerability Management

S SECONDARY:
Application Whitelisting

SOLUTION = PROVIDER:

- P Tivoli Endpoint Manager (BigFix) = IBM
- P Vulnerability Management = Lumension
- P System Center = Microsoft
- P CCM (primary), IP360 = nCircle
- P QualysGuard Policy Compliance Module = Qualys
- P Corporate Software Inspector = Secunia
- P Nessus, Security Center = Tenable
- P Enterprise, Log Center = Tripwire
- S Parity, Bit9 FileAdvisor = Bit9
- S Bouncer = CoreTrace
- S SolidCore = McAfee

3

Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

SOLUTION = PROVIDER:

Deep Freeze = Faronics

Tivoli Endpoint Manager (BigFix) = IBM

Vulnerability Management = Lumension

System Center, Steady State = Microsoft

CCM, IP360 = nCircle

QualysGuard = Qualys

CSP = Symantec

Nessus, Security Center = Tenable

Enterprise = Tripwire

Configuration Manager = VMware

4
Continuous Vulnerability Assessment and Remediation

P PRIMARY:
Vulnerability Assessment

SOLUTION = PROVIDER:

- P CORE IMPACT Pro = Core Security
- P Vulnerability Management Services = Dell SecureWorks
- P Retina = eEye Digital Security
- P Vulnerability Management = Infogressive
- P Vulnerability & Remediation Manager = McAfee
- P IP360 = nCircle
- P OpenVAS = Open Source
- P QualysGuard (VM Module) = Qualys
- P NexPose = Rapid7
- P SAINT & SAINTmanager = SAINT
- P CCS = Symantec
- P Nessus, Security Center = Tenable

5
Malware Defense

P PRIMARY:
Endpoint Protection Platforms

S SECONDARY:
Application Whitelisting

SOLUTION = PROVIDER:

P vSentry = Bromium
P Enterprise, Security Pro = Invincea
P Adminstration Kit = Kaspersky
P ePolicy Orchestrator = McAfee
P Forefront, System Center = Microsoft
P Endoint Protection = Sophos
P SEP=Symantec
P Control Manager = Trend Micro
S Bit9 = Bit9
S Bouncer = CoreTrace
S SolidCore = McAfee

6
Application Software Security

P PRIMARY:
Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST)

SOLUTION = PROVIDER:

- P Hailstorm Enterprise = Cenzic
- P Checkmarx = Checkmarx
- P Save = Coverity
- P Managed Web App Firewall, Web Application Testing = Dell SecureWorks
- P Fortify 360, Fortify on Demand, WebInspect = HP (Fortify)
- P Ounce Labs Core, Appscan = IBM
- P NTO Spider = NTObjectives
- P QualysGuard WAS = Qualys
- P Static/Dynamic = Veracode
- P Sentinel = WhiteHat

7

Wireless Device Control

P PRIMARY:

Wireless LAN Intrusion Prevention System (WIPS)

SOLUTION = PROVIDER:

- P WiFi Analyzer = AirMagnet (Fluke)
- P WLS Manager = AirPatrol
- P SpectraGuard = AirTight
- P RF Protect = Aruba
- P aWIPS, CleanAir = Cisco
- P AirDefense = Motorola
- P CCM = nCircle
- P Nessus, Security Center = Tenable

8

Data Recovery Capability

SOLUTION = PROVIDER:

AccessData FTK and PRTK = AccessData

ElcomSoft EFDD, Bitlocker, TruCrypt = Elcom

Encase Enterprise Edition = Guidance Software

Mandiant Platform = Mandiant

9

Security Skills Assessment and Appropriate Training to Fill Gaps

SOLUTION = PROVIDER:

Assessment

Cyber Simulators (Netwars) and Skills Validation - SANS Institute

Cyber Skills Assessment - GIAC (SANS)

Skills Development

Dakota State University

Naval Postgraduate School

Northeastern

SANS Institute (50 Hands-on Immersion Courses)

SANS Technology Institute (STI) (Masters Degrees)

University of Tulsa

Security Awareness Training = SANS Institute

Virginia Tech

10
Secure Configurations for Firewalls, Routers, and Switches

P PRIMARY:
Network Policy Management (NPM)

SOLUTION = PROVIDER:

- P Firewall Analyzer & FireFlow = AlgoSec
- P FirePAC = Athena Security
- P SecurityManager = FireMon
- P Network Advisor = RedSeal
- P Network Compliance Auditor = Skybox Security
- P Network Configuration Manager = Solarwinds
- P Enterprise = Tripwire
- P Tufin Appliance = Tufin

11
Limitation and Control of Network Ports, Protocols, and Services

P PRIMARY:
Discovery, Vulnerability Assessment

S SECONDARY:
Application Firewall

SOLUTION = PROVIDER:

P BSA Visibility = Insightix (McAfee)
P IPSonar = Lumeta
P FoundScan = McAfee
P CCM, IP360 = nCircle
P QualysGuard = Qualys
P Nexpose = Rapid7
P CCS = Symantec
P Nessus, Security Center = Tenable
S 2200 = Checkpoint
S ASA Series and virtual ASA = Cisco
S SonicWall = Dell Sonicwall
S FortiGate = Fortinet
S SRX and vGW = Juniper
S PaloAlto NGFW = Palo Alto Networks

12
Controlled Use of Administrative Privileges

SOLUTION = PROVIDER:

PowerBroker = BeyondTrust

PIM = Cyber-Ark

eDMZ = Dell

ArcSight ESM, ArcSight Identify View = HP

Security Manager = Intellitactics (Trustwave)

System Center, Active Directory = Microsoft

CCM = nCircle

sudo = Open Source

Access Auditor = Security Compliance Corporation (SCC)

CCS = Symantec

Enterprise, Log Center = Tripwire

Xsuite = Xceedium

13
Boundary Defense

P PRIMARY:
Firewall

S SECONDARY:
Intrusion Prevention System

SOLUTION = PROVIDER:

P 2200 = Checkpoint

P ASA Series and virtual ASA = Cisco

P SonicWall = Dell Sonicwall

P FortiGate = Fortinet

P SRX and vGW = Juniper

P PaloAlto NGFW = Palo Alto Networks

S Firewall Management, Managed NGFW, Managed IDS/IPS, Managed UTM, Security Monitoring = Dell SecureWorks

S XPS = Fidelis

S Fireeye Malware Protection System = FireEye

S TippingPoint = HP

S Network IPS = IBM (ISS)

S StealthWatch = Lancope

S Network Security Platform = McAfee

Snort = Open Source

S Firepower = Sourcefire

14

Maintenance, Monitoring, and Analysis of Audit Logs

P PRIMARY:
Security Information and Event Managemnt (SIEM)

SOLUTION = PROVIDER:

- P OSSIM = AlienVault
- P CorreLog Enterprise Server = Correlog
- P Security Monitoring, Log Management = Dell SecureWorks
- P ArcSight ESM, Logger = HP (ArcSight)
- P Q1 = IBM
- P Event Correlation = Infogressive
- P StealthWatch = Lancope
- P Open Log Management = LogLogic
- P SIEM 2.0 = LogRhythm
- P Snare = Open Source
- P Event Data Warehouse = SenSage
- P Enterprise = Splunk
- P Log Correlation Engine = Tenable
- P Security Information Management = TriGeo
- P Log Center = Tripwire

15
Controlled Access Based on Need to Know

P PRIMARY:
Enterprise Access Management

SOLUTION = PROVIDER:

- P IAM = Aveska
- P AAS = Courion
- P HyTrust = HyTrust
- P IAG = IBM
- P Active Directory = Microsoft
- P Identity Analytics = Oracle
- P Identity IQ = Sailpoint
- P Access Auditor = Security Compliance Corporation (SCC)
- P Enterprise, Log Center = Tripwire

16

Account Monitoring and Control

SOLUTION = PROVIDER:

Privileged Identity Management Suite = Cyber-Ark

Log Management = Dell SecureWorks

HyTrust = HyTrust

Security Manager = Intellitactics (Trustwave)

AD Reports = MaxPowerSoft

System Center = Microsoft

QualysGuard PC = Qualys

Enterprise Security Reporter = Quest

Enterprise, Log Center = Tripwire

17

Data Loss Prevention

SOLUTION = PROVIDER:

DLP Software Blade = Checkpoint

TrueDLP = Code Green

XPS = Fidelis

FortiGate = Fortinet

McAfee DLP = McAfee

Tablus DLP = RSA

DLP = Symantec

DLP = Trend Micro

Digital Guardian = Verdasys

18

Incident Response and Management

SOLUTION = PROVIDER:

FTK with Cerebrus = AccessData

CarBonBlack = CarbonBlack

UFED = Cellebrite

CorreLog Enterprise Server = Correlog

CyberSponse = CyberSponse

Essential Series, Incident Response Services, Security Monitoring = Dell SecureWorks

F-Response Enterprise = F-Response

EnCase Cybersecurity = Guidance Software

Incident Response & Forensics = Infogressive

StealthWatch = Lancope

Mandiant Intelligent Response (MIR) = Mandiant

19

Secure Network Engineering

SOLUTION = PROVIDER:

Firewall Analyzer & FireFlow = AlgoSec

FirePAC = Athena Security

CloudPassage = CloudPassage

SecurityManager = FireMon

Network Design Experts = Infogressive

StealthWatch = Lancope

Network Advisor = RedSeal

Network Compliance Auditor = Skybox Security

Network Configuration Manager = Solarwinds

Enterprise = Tripwire

Tufin Appliance = Tufin

20

Penetration Testing and Red Team Exercises

SOLUTION = PROVIDER:

CORE IMPACT Pro = Core Security

Penetration Testing, Incident Response Capabilities Testing = Dell SecureWorks

Immunity CANVAS = Immunity CANVAS

Penetration Testing = Infogressive

Metasploit Free and Pro = Rapid7

SAINT = SAINT

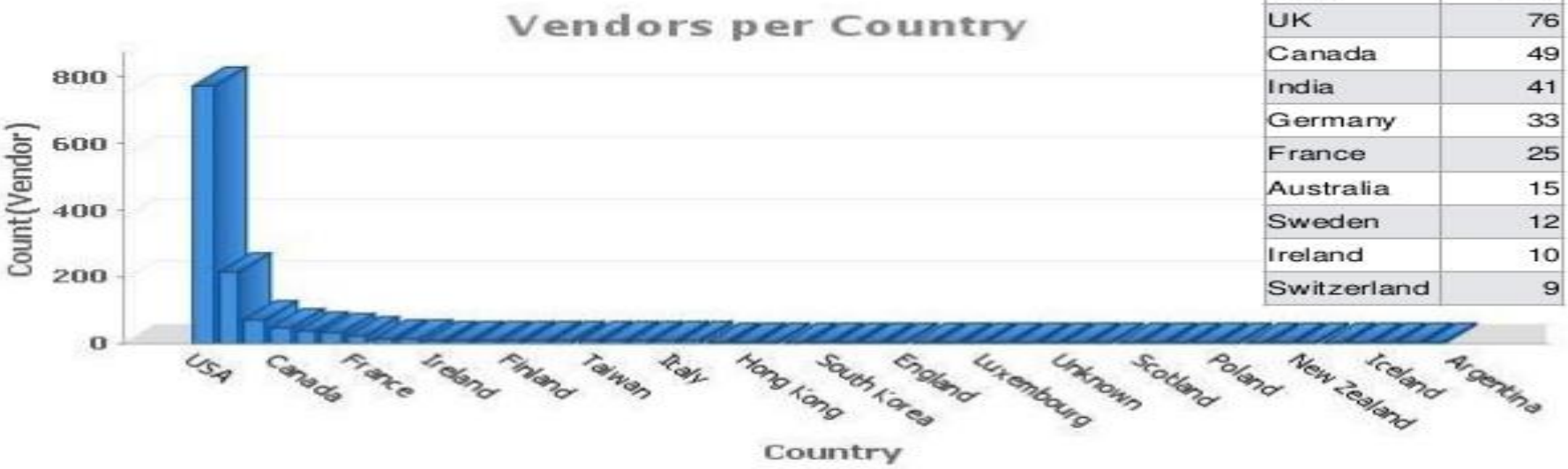
MySecurityScanner = Secure Ideas

Armitage / Cobalt Strike = Strategic Cyber LLC

CYBER SECURITY INDUSTRY TRENDS

By Country

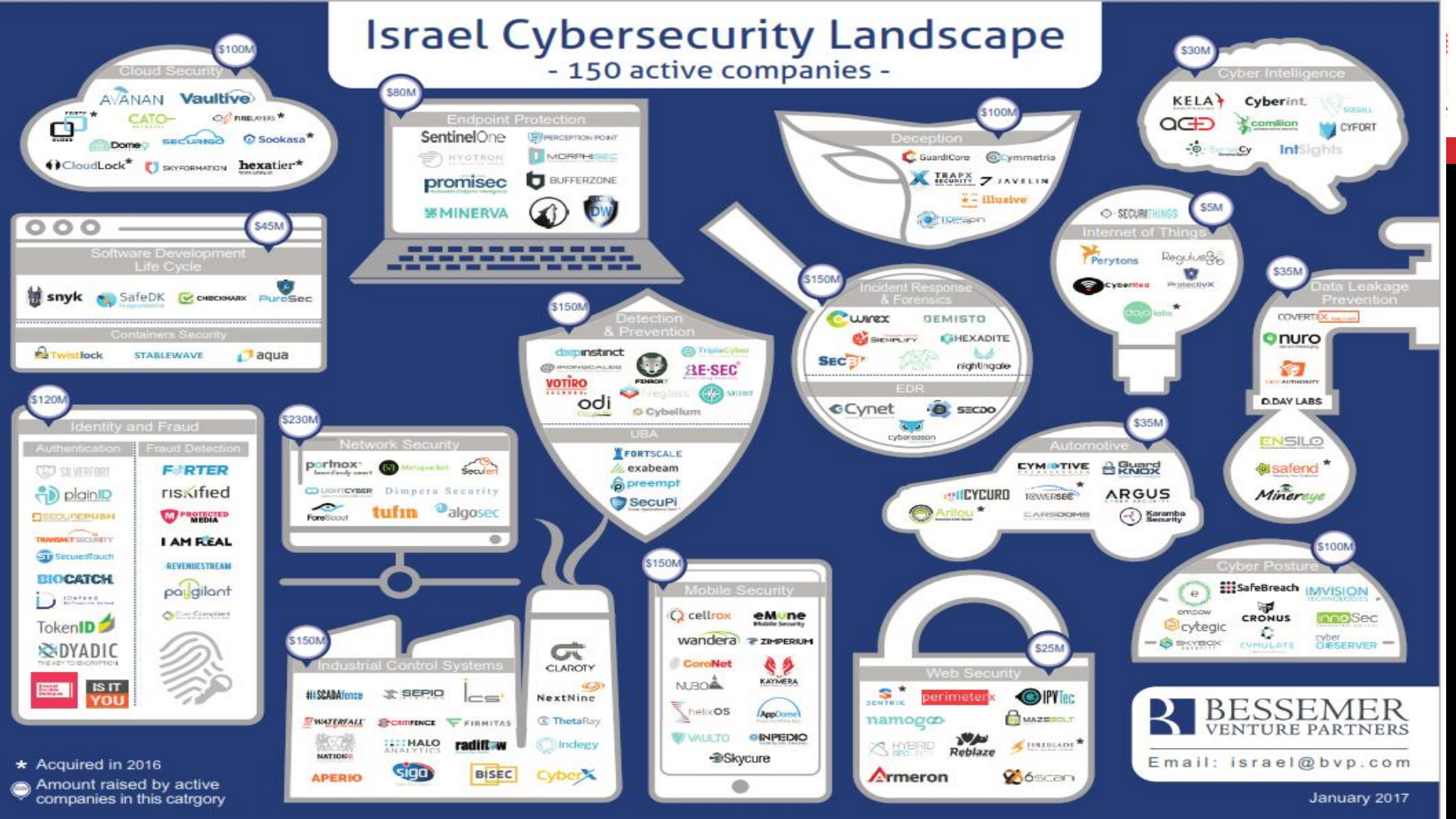
Country	Vendor Count
USA	827
Israel	228
UK	76
Canada	49
India	41
Germany	33
France	25
Australia	15
Sweden	12
Ireland	10
Switzerland	9



Source: www.ith-research.com

Israel Cybersecurity Landscape

- 150 active companies -



* Acquired in 2016

Amount raised by active companies in this catrgory

BESSEMER VENTURE PARTNERS

Email: israel@bvp.com

January 2017

APQC IT

طبقه ۸: مدیریت فناوری اطلاعات

گروه فرایند: مدیریت کسب و کار فناوری اطلاعات

فرایندها:

- ❑ توسعه استراتژی IT سازمان
- ❑ تعریف معماری سازمانی
- ❑ مدیریت پرتفولیوی IT
- ❑ اجرای تحقیقات و فناوری های IT
- ❑ ارزیابی و اطلاع رسانی ارزش و عملکرد کسب و کار IT

گروه فرایند: توسعه و مدیریت روابط مشتری IT

فرایندها:

- ❑ توسعه استراتژی خدمات و راه حل های IT
- ❑ توسعه و نگهداری سطوح خدمات IT
- ❑ انجام مدیریت سمت تقاضا (DSM) برای خدمات IT
- ❑ مدیریت رضایتمندی مشتریان IT
- ❑ عرضه کردن راه حل ها و خدمات IT

گروه فرایند: توسعه و اجرای کنترل های امنیتی، حریم خصوصی و حفاظت اطلاعات

فرایندها:

- تدوین استراتژی ها و سطوح امنیت اطلاعات، حریم خصوصی و حفاظت اطلاعات
- تست، ارزیابی و اجرای کنترل های امنیت اطلاعات و حریم خصوصی و حفاظت اطلاعات

گروه فرایند: مدیریت اطلاعات سازمانی

فرایندها:

- توسعه استراتژی های مدیریت محتوا و اطلاعات
- تعریف معماری اطلاعات سازمانی
- مدیریت منابع اطلاعاتی
- اجرای مدیریت محتوا و داده سازمان

گروه فرایند: توسعه و نگهداری راه حل های فناوری اطلاعات

فرایندها:

- تدوین استراتژی توسعه فناوری اطلاعات
- اجرای برنامه چرخه عمر خدمات و راه حل های فناوری اطلاعات
- توسعه و نگهداری معماری خدمات و راه حل های فناوری اطلاعات
- ایجاد راه حل ها و خدمات فناوری اطلاعات
- نگهداری از راه حل ها و خدمات فناوری اطلاعات

گروه فرایند: استقرار راه حل های فناوری اطلاعات

فرایندها:

- تدوین استراتژی استقرار فناوری اطلاعات
- برنامه ریزی و اجرای تغییرات
- برنامه ریزی و مدیریت انتشار

گروه فرایند: ارائه خدمات فناوری اطلاعات و پشتیبانی از آن

فرایندها:

- ❑ تدوین استراتژی ارائه خدمات و راه حل های فناوری اطلاعات
- ❑ توسعه استراتژی پشتیبانی فناوری اطلاعات
- ❑ مدیریت منابع زیرساخت فناوری اطلاعات
- ❑ مدیریت عملیات زیرساخت های فناوری اطلاعات
- ❑ پشتیبانی از راه حل ها و خدمات فناوری اطلاعات

فرآیندهای زیرساختی

مدیریت ریسک

Stage
Step 1: Prepare
Step 2: Categorize Information Systems
Step 3: Select Security Controls
Step 4: Implement Security Controls
Step 5: Assess Security Controls
Step 6: Authorize Information System
Step 7: Monitor Security Controls

NIST CSF Framework

CSF Areas:
- ❑ Identify
- ❑ Protect
- ❑ Detect
- ❑ Respond
- ❑ Recover

چارچوب تاب آوری

CERT Résilience Management Model (CERT-RMM)
Cyber Resilience Review (CRR) - 10 Areas

عناصر چارچوب تاب آوری (ادامه)
- ❑ مدیریت دارایی
- ❑ شناسایی و تشخیص
- ❑ پاسخ دهی و بازیابی
- ❑ حاکمیت و اطمینان

NIST SP800-160, Vol. 2.18

کنترل های عملیاتی

مدیریت اسیب پذیری ها و کاستی ها

Common Vulnerability Scoring System (CVSS)
Common Weakness Scoring System (CWSS)
Caveats:
- Conditions
- Limitations
- Caution

CVDDetails.Com
cve.mitre.org
NVD.NIST.Gov
First.org/cvss/calculator/3.0
Tools.Cisco.Com

کتابی

مدیریت ریسک
مدیریت آسیب پذیری ها و کاستی ها
مدیریت تهدیدات
اثرات ریسک

چارچوب مدیریت ریسک (RMF)

Controls
- Low - 125 controls
- Medium - 177 controls
- High - 188 controls

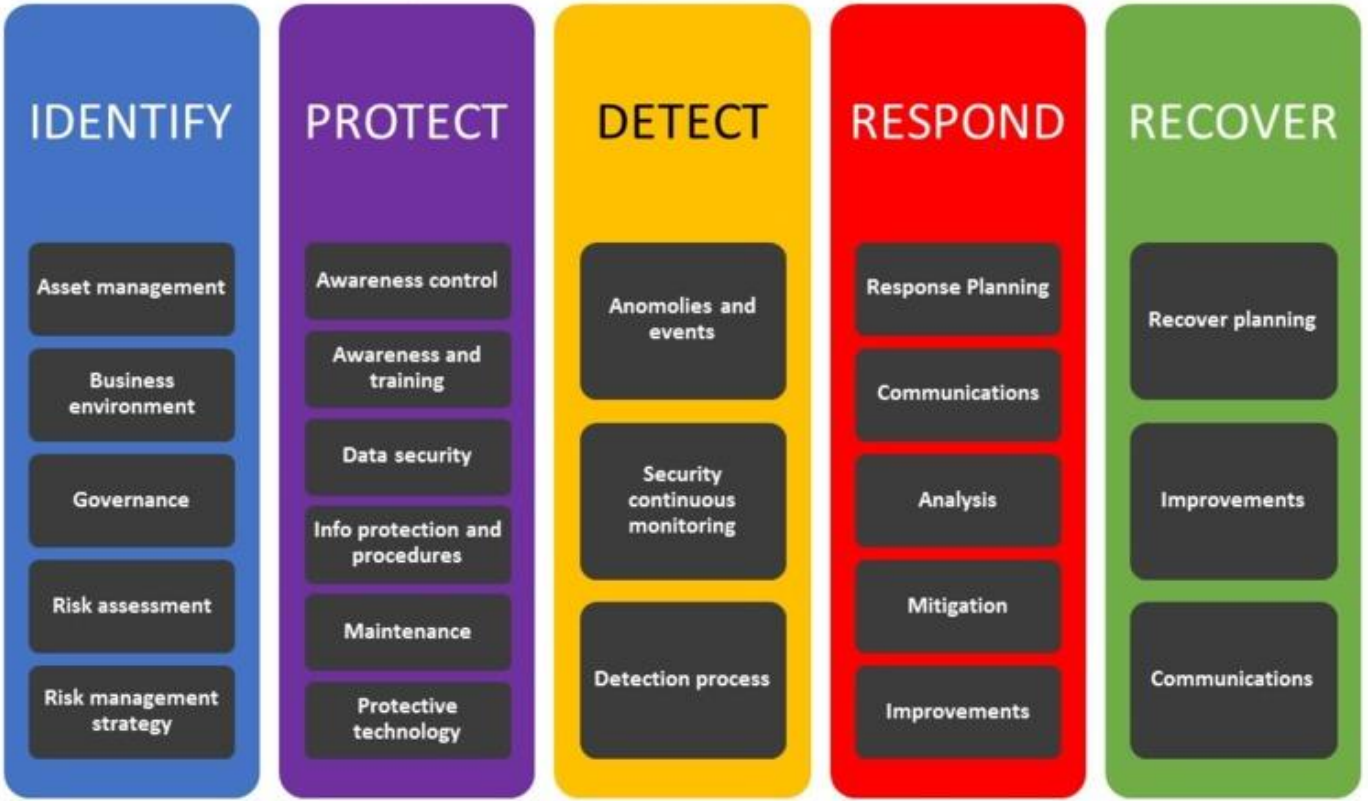
کنترل های پیشگیری

Cyber Resilience Review (CRR)

CRR, consisting of 299 questions
- ❑ Asset Management
- ❑ Controls Management
- ❑ Configuration and Change Management
- ❑ Vulnerability Management
- ❑ Incident Management
- ❑ Service Continuity Management
- ❑ Risk Management
- ❑ External Dependencies Management
- ❑ Training and Awareness
- ❑ Situational Awareness

NIST SPECIAL PUBLICATION 1800-5

NIST Cybersecurity Framework



جدول چارچوب امنیت NIST

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

چارچوب امنیت سایبری NIST بر چه کسانی تأثیر می‌گذارند

در ابتدا چارچوب امنیت سایبری **NIST** فقط به عنوان دستورالعمل‌های اجرایی تحت نظر رئیس جمهور باراک اوباما در نظر گرفته شد. این استانداردها اکنون در ادارات دولتی تحت دستورالعمل‌های اجرایی رئیس جمهور فعلی ایالات متحده، اجرا می‌شوند. اما، این دستورالعمل‌ها می‌توانند به نفع سازمان‌های غیردولتی و مشاغل نیز باشند. بنابراین، هر کسی که دغدغه حفظ امنیت سایبری سازمان خود را دارد، بهتر است چارچوب امنیت سایبری **NIST** را بشناسد.

در حقیقت می‌توان گفت، هر کسی که از رایانه استفاده می‌کند، لازم است در مورد چارچوب امنیت سایبری **NIST** تأمل کند. بخش فناوری اطلاعات هر سازمان باید اولین بخشی باشد که این دستورالعمل‌ها را پیاده‌سازی می‌کند، اما سایر بخش‌ها نیز باید از استانداردهای امنیتی پیروی کنند. هم‌چنین، مدیران کسب و کار مسئولیت اطمینان از صحت انجام این کار را بر عهده دارند.

هسته چارچوب امنیت سایبری NIST

به طور خاص، NIST CSF پنج عملکرد اصلی را برای مدیریت ریسک‌های موجود در امنیت داده‌ها و اطلاعات توصیه می‌کند. این عملکردها عبارت‌اند از شناسایی، محافظت، تشخیص، پاسخگویی و بازیابی.

عملکرد شناسایی(Identify) ، سازمان‌ها را در شناسایی خطرات امنیتی برای مدیریت دارایی‌ها، محیط کسب و کار و حاکمیت فناوری اطلاعات از طریق فرآیندهای جامع ارزیابی و مدیریت ریسک راهنمایی می‌کند.

عملکرد محافظت (Protect) نیز کنترل‌های امنیتی مورد نیاز برای حفاظت از سیستم‌های اطلاعاتی و داده‌ها تعریف می‌کند. این موارد شامل کنترل دسترسی، آموزش و آگاه سازی، امنیت داده‌ها، روش‌های حفاظت از اطلاعات و نگهداری از فناوری‌های محافظتی است.

عملکرد تشخیص (Detect) نیز دستورالعمل‌هایی برای تشخیص ناهنجاری‌ها در سیستم های امنیتی، سیستم‌های نظارتی و شبکه‌ها برای کشف حوادث امنیتی از بین اتفاقات دیگر ارائه می‌دهد.

عملکرد پاسخ (Response) شامل توصیه‌هایی برای برنامه‌ریزی جهت پاسخ به رویدادهای امنیتی، روش‌های کاهش ریسک، فرایندهای ارتباطی در جریان پاسخ به حوادث و فعالیت‌هایی برای بهبود انعطاف پذیری امنیت می‌باشد.

عملکرد بازیابی (Recovery) نیز دستورالعمل‌هایی را ارائه می‌دهد که سازمان‌ها می‌توانند از آنها برای بازگشت به حالت اولیه در حملات استفاده کند.

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management[1.1]
Protect	**Identity Management, Authentication and Access Control**[1.1]
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

پنج اقدام اصلی و پایه در چارچوب امنیت سایبری NIST عبارتند از: شناسایی، تشخیص، محافظت، واکنش و بهبود.

-دسته‌بندی‌ها

هریک از پنج اقدام اصلی دارای مجموعه مشخصی از وظایف هستند که لازم است صورت گیرد. به‌طور مثال اقدامات لازم برای محافظت از سیستم شامل به‌روزرسانی نرم‌افزارها، نصب نرم‌افزارهای آنتی‌ویروس و اعمال قوانین کنترل دسترسی می‌شود.

-زیرمجموعه‌ها

زیرمجموعه‌ها در واقع شامل وظایف مرتبط با هریک از دسته‌بندی‌ها هستند. برای مثال، جهت به‌روزرسانی نرم‌افزارها باید اطمینان حاصل شود در همه دستگاه‌های ویندوزی قابلیت به‌روزرسانی خودکار فعال است.

-منابع اطلاعاتی مفید

این منابع حاوی مستندات و راهنماهایی در رابطه با هریک از وظایف و اقدامات خاص هستند که به کاربران در نحوه انجام کارها کمک می‌کند

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

ASSET MANAGEMENT (ID.AM)

Asset Management (ID.AM):

- The data
- Personnel
- Devices
- Systems
- Facilities

That enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.

ASSET MANAGEMENT (ID.AM)

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
	ID.AM-2: Software platforms and applications within the organization are inventoried
	ID.AM-3: Organizational communication and data flows are mapped
	ID.AM-4: External information systems are catalogued
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

ASSET MANAGEMENT (ID.AM)

- **CIS CSC** 2
  - **COBIT 5** BAI09.01, BAI09.02, BAI09.05
  - **ISA 62443-2-1:2009** 4.2.3.4
  - **ISA 62443-3-3:2013** SR 7.8
  - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1
  - **NIST SP 800-53 Rev. 4** CM-8, PM-5
- **CIS CSC** 12
  - **COBIT 5** DSS05.02
  - **ISA 62443-2-1:2009** 4.2.3.4
  - **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2
  - **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
- **CIS CSC** 12
  - **COBIT 5** APO02.02, APO10.04, DSS01.02
  - **ISO/IEC 27001:2013** A.11.2.6
  - **NIST SP 800-53 Rev. 4** AC-20, SA-9
- **CIS CSC** 13, 14
  - **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02
  - **ISA 62443-2-1:2009** 4.2.3.6
  - **ISO/IEC 27001:2013** A.8.2.1
  - **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
- **CIS CSC** 17, 19
  - **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03
  - **ISA 62443-2-1:2009** 4.3.2.3.3
  - **ISO/IEC 27001:2013** A.6.1.1
  - **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6,
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	-1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PM-1, PM-2, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	-1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	PM-3, PM-7, PM-9, PM-10, PM-11, SA-2
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	PM-8, PM-9, PM-11, SA-14

IDENTIFY (ID)	**Asset Management (ID.AM):** داده ها، پرسنل، دستگاه ها، سیستم ها و امکاناتی که سازمان را قادر می سازد به اهداف تجاری دست یابد، مطابق با اهمیت نسبی آنها برای اهداف تجاری و استراتژی ریسک سازمان شناسایی و مدیریت می شوند.	**ID.AM-1:** دستگاه ها و سیستم های فیزیکی درون سازمان لیست هستند.	CM-8, PM-5
		ID.AM-2: پلتفرم‌های نرم‌افزاری و برنامه‌های کاربردی درون سازمان لیست هستند.	CM-8, PM-5
		ID.AM-3: ارتباطات سازمانی و جریان های داده نقشه برداری شده اند	AC-4, CA-3, CA-9, PL-8
		ID.AM-4: سیستم های اطلاعات خارجی فهرست بندی شده اند	AC-20, SA-9
		ID.AM-5: منابع (به عنوان مثال، سخت افزار، دستگاه ها، داده ها و نرم افزار) بر اساس طبقه بندی، اهمیت و ارزش تجاری آنها اولویت بندی می شوند.	CP-2, RA-2, SA-14, SC-6,
		ID.AM-6: نقش ها و مسئولیت های امنیت سایبری برای کل نیروی کار و ذینفعان شخص ثالث (به عنوان مثال، تامین کنندگان، مشتریان، شرکا) ایجاد شده است.	CP-2, PS-7, PM-11
	Business Environment (ID.BE): ماموریت، اهداف، ذینفعان و فعالیت های سازمان درک شده و اولویت بندی شده است. این اطلاعات برای اطلاع رسانی نقش ها، مسئولیت ها و تصمیمات مدیریت ریسک در امنیت سایبری استفاده می شود.	**ID.BE-1:** نقش سازمان در زنجیره تامین شناسایی و ابلاغ می شود	CP-2, SA-12
		ID.BE-2: جایگاه سازمان در زیرساخت های حیاتی و بخش صنعت آن شناسایی و ابلاغ می شود	PM-8
		ID.BE-3: اولویت‌ها برای مأموریت، اهداف و فعالیت‌های سازمانی تعیین و ابلاغ می‌شوند	PM-11, SA-14
		ID.BE-4: وابستگی ها و عملکردهای حیاتی برای ارائه خدمات حیاتی ایجاد می شود	CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: الزامات انعطاف پذیری برای پشتیبانی از ارائه خدمات حیاتی ایجاد شده است	CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): خط‌مشی‌ها، رویه‌ها و فرآیندهای مدیریت و نظارت بر الزامات نظارتی، قانونی، ریسک، زیست‌محیطی و عملیاتی سازمان درک شده و مدیریت ریسک امنیت سایبری را مطلع می‌کند.	**ID.GV-1:** خط مشی امنیت اطلاعات سازمانی ایجاد شده است	-1 controls from all families
		ID.GV-2: نقش ها و مسئولیت های امنیت اطلاعات با نقش های داخلی و شرکای خارجی هماهنگ و همسو هستند	PM-1, PM-2, PS-7
		ID.GV-3: الزامات قانونی و نظارتی در مورد امنیت سایبری، از جمله تعهدات حریم خصوصی و آزادی های مدنی، درک و مدیریت می شود	-1 controls from all families (except PM-1)
		ID.GV-4: فرآیندهای حکمرانی و مدیریت ریسک، خطرات امنیت سایبری را بررسی می‌کنند	PM-3, PM-7, PM-9, PM-10, PM-11, SA-2
	Risk Assessment (ID.RA): سازمان خطر امنیت سایبری برای عملیات سازمانی (شامل ماموریت، عملکرد، تصویر یا شهرت)، دارایی های سازمانی و افراد را درک می کند.	**ID.RA-1:** آسیب پذیری های دارایی شناسایی و مستندسازی می شوند	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: اطلاعات تهدید و آسیب پذیری از انجمن ها و منابع به اشتراک گذاری اطلاعات دریافت می شود	PM-15, PM-16, SI-5
		ID.RA-3: تهدیدها، چه داخلی و چه خارجی، شناسایی و مستند شده اند	RA-3, SI-5, PM-12, PM-16
		ID.RA-4: اثرات و احتمالات تجاری بالقوه شناسایی شده است	RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: تهدیدها، آسیب‌پذیری‌ها، احتمالات و تأثیرات برای تعیین ریسک استفاده می‌شوند	RA-2, RA-3, PM-16
		ID.RA-6: پاسخ های ریسک شناسایی و اولویت بندی می شوند	PM-4, PM-9
	Risk Management Strategy (ID.RM): اولویت ها، محدودیت ها، تحمل ریسک و مفروضات سازمان برای حمایت از تصمیمات ریسک عملیاتی ایجاد و استفاده می شود.	**ID.RM-1:** فرآیندهای مدیریت ریسک توسط ذینفعان سازمانی ایجاد، مدیریت و مورد توافق قرار می گیرند	PM-9
		ID.RM-2: تحمل ریسک سازمانی مشخص و به وضوح بیان می شود	PM-9
		ID.RM-3: تعیین تحمل ریسک توسط سازمان با نقش آن در زیرساخت های حیاتی و تجزیه و تحلیل ریسک خاص بخش مشخص می شود	PM-8, PM-9, PM-11, SA-14

PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	AC-2, AC-7, AC-8, AC-9, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, SC-17
		PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9
		PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20, PE-17, SC-15
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-10, AC-11, AC-12, AC-14, AC-16, AC-24, SC-2, SC-3, SC-4
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand roles & responsibilities	AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	SC-8, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	CM-2
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	MP-6
		PR.IP-7: Protection processes are continuously improved	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: A vulnerability management plan is developed and implemented	RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

PROTECT (PR)	**Access Control (PR.AC):** دسترسی به دارایی‌ها و امکانات مرتبط به کاربران، فرآیندها یا دستگاه‌های مجاز و فعالیت‌ها و تراکنش‌های مجاز محدود می‌شود.	**PR.AC-1:** هویت‌ها و اعتبارنامه‌ها برای دستگاه‌ها و کاربران مجاز مدیریت می‌شوند	AC-2, AC-7, AC-8, AC-9, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, SC-17
		PR.AC-2: دسترسی فیزیکی به دارایی ها مدیریت و محافظت می شود	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9
		PR.AC-3: دسترسی از راه دور مدیریت می شود	AC-17, AC-19, AC-20, PE-17, SC-15
		PR.AC-4: مجوز های دسترسی مدیریت می شوند که اصول حداقل امتیاز و تفکیک وظایف را در بر می گیرد	AC-2, AC-3, AC-5, AC-6, AC-10, AC-11, AC-12, AC-14, AC-16, AC-24, SC-2, SC-3, SC-4
		PR.AC-5: یکپارچگی شبکه محافظت می شود و در صورت لزوم، جداسازی شبکه را نیز شامل می شود	AC-4, SC-7
	Awareness and Training (PR.AT): به پرسنل و شرکای سازمان آموزش آگاهی از امنیت سایبری ارائه می شود و به اندازه کافی آموزش دیده اند تا وظایف و مسئولیت های مرتبط با امنیت اطلاعات خود را مطابق با خط مشی ها، رویه ها و توافق نامه های مرتبط انجام دهند.	**PR.AT-1:** تمامی کاربران مطلع و آموزش دیده اند	AT-2, PM-13
		PR.AT-2: کاربران ممتاز نقش ها و مسئولیت ها را درک می کنند	AT-3, PM-13
		PR.AT-3: ذینفعان شخص ثالث (به عنوان مثال، تامین کنندگان، مشتریان، شرکا) نقش ها و مسئولیت ها را درک می کنند.	PS-7, SA-9, SA-16
		PR.AT-4: مدیران ارشد نقش ها و مسئولیت ها را درک می کنند	AT-3, PM-13
		PR.AT-5: پرسنل امنیت فیزیکی و اطلاعاتی نقش ها و مسئولیت ها را درک می کنند	AT-3, IR-2, PM-13
	Data Security (PR.DS): اطلاعات و سوابق (داده ها) مطابق با استراتژی ریسک سازمان برای محافظت از محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات مدیریت می شوند.	**PR.DS-1:** داده در حالت استراحت محافظت می شود	MP-8, SC-12, SC-28
		PR.DS-2: انتقال داده ها محافظت می شود	SC-8, SC-11, SC-12
		PR.DS-3: دارایی ها به طور رسمی در طول حذف، انتقال و واگذاری مدیریت می شوند	CM-8, MP-6, PE-16
		PR.DS-4: ظرفیت کافی برای اطمینان از در دسترس بودن حفظ می شود	AU-4, CP-2, SC-5
		PR.DS-5: حفاظت در برابر نشت داده ها اجرا شده است	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: مکانیسم های بررسی یکپارچگی برای تأیید صحت نرم افزار، سیستم عامل و یکپارچگی اطلاعات استفاده می شود	SC-16, SI-7
		PR.DS-7: محیط(های) توسعه و آزمایش جدا از محیط تولید است	CM-2
	Information Protection Processes and Procedures (PR.IP): سیاست‌های امنیتی (که به هدف، دامنه، نقش‌ها، مسئولیت‌ها، تعهد مدیریت و هماهنگی بین نهادهای سازمانی می‌پردازد)، فرآیندها و رویه‌ها حفظ شده و برای مدیریت حفاظت از سیستم‌های اطلاعاتی و دارایی‌ها استفاده می‌شوند.	**PR.IP-1:** یک پیکربندی پایه از فناوری اطلاعات / سیستم های کنترل صنعتی ایجاد و نگهداری می شود	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: چرخه عمر توسعه سیستم برای مدیریت سیستم ها پیاده سازی شده است	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: فرآیندهای کنترل تغییر پیکربندی وجود دارد	CM-3, CM-4, SA-10
		PR.IP-4: پشتیبان گیری از اطلاعات به صورت دوره ای انجام، نگهداری و آزمایش می شود	CP-4, CP-6, CP-9
		PR.IP-5: سیاست ها و مقررات مربوط به محیط عملیاتی فیزیکی برای دارایی های سازمانی رعایت می شود	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: داده ها طبق سیاست از بین می روند	MP-6
		PR.IP-7: فرآیندهای حفاظتی به طور مداوم بهبود می یابند	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: اثربخشی فن آوری های حفاظتی با طرف های مناسب به اشتراک گذاشته می شود	AC-21, CA-7, SI-4
		PR.IP-9: طرح‌های واکنش (واکنش به حادثه و تداوم کسب‌وکار) و طرح‌های بازیابی (بازیابی حادثه و بازیابی فاجعه) وجود دارند و مدیریت می‌شوند.	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: طرح های پاسخ و بازیابی آزمایش می شوند	CP-4, IR-3, PM-14
		PR.IP-11: امنیت سایبری در شیوه های منابع انسانی گنجانده شده است (به عنوان مثال، محروم کردن از امکانات، غربالگری پرسنل)	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: یک طرح مدیریت آسیب پذیری تدوین و اجرا می شود	RA-3, RA-5, SI-2
	Maintenance (PR.MA): نگهداری و تعمیرات اجزای سیستم اطلاعاتی و کنترل صنعتی مطابق با سیاست ها و رویه ها انجام می شود.	**PR.MA-1:** نگهداری و تعمیر دارایی های سازمانی به موقع و با ابزار تأیید شده و کنترل شده انجام و ثبت می شود.	MA-2, MA-3, MA-5, MA-6
		PR.MA-2: نگهداری از راه دور دارایی های سازمانی به گونه ای تأیید، ثبت و انجام می شود که از دسترسی غیرمجاز جلوگیری می کند.	MA-4
	Protective Technology (PR.PT): راه‌حل‌های امنیتی فنی برای تضمین امنیت و انعطاف‌پذیری سیستم‌ها و دارایی‌ها، مطابق با سیاست‌ها، رویه‌ها و توافق‌نامه‌های مرتبط مدیریت می‌شوند.	**PR.PT-1:** سوابق حسابرسی/ ثبت گزارش مطابق با خط مشی تعیین، مستند، اجرا و بررسی می شوند	AU Family
		PR.PT-2: رسانه قابل جابجایی محافظت شده است و استفاده از آن طبق خطمشی محدود شده است	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: دسترسی به سیستم‌ها و دارایی‌ها کنترل می‌شود و اصل کمترین عملکرد را در بر می‌گیرد	AC-3, CM-7
		PR.PT-4: ارتباطات و شبکه های کنترل محافظت می شوند	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	SI-3, SI-8
		DE.CM-5: Unauthorized mobile code is detected	SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	AC-25, CA-2, CA-7, PM-14, SA-18, SI-4
		DE.DP-3: Detection processes are tested	CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

DETECT (DE)	**Anomalies and Events (DE.AE):** فعالیت غیرعادی به موقع تشخیص داده می شود و تأثیر بالقوه رویدادها درک می شود.	**DE.AE-1:** یک خط پایه از عملیات شبکه و جریان های داده مورد انتظار برای کاربران و سیستم ها ایجاد و مدیریت می شود	AC-4, CA-3, CM-2, SI-4
		DE.AE-2: رویدادهای شناسایی شده برای درک اهداف و روش های حمله تجزیه و تحلیل می شوند	AU-6, CA-7, IR-4, SI-4
		DE.AE-3: داده‌های رویداد از منابع و حسگرهای متعدد تجمیع و مرتبط می‌شوند	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: تأثیر رویدادها مشخص می شود	CP-2, IR-4, RA-3, SI -4
		DE.AE-5: آستانه های هشدار حادثه ایجاد شده است	IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): سیستم اطلاعاتی و دارایی‌ها در فواصل زمانی مشخص برای شناسایی رویدادهای امنیت سایبری و تأیید اثربخشی اقدامات حفاظتی نظارت می‌شوند.	**DE.CM-1:** این شبکه برای شناسایی رویدادهای احتمالی امنیت سایبری نظارت می شود	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: محیط فیزیکی برای شناسایی رویدادهای بالقوه امنیت سایبری نظارت می شود	CA-7, PE-3, PE-6, PE-20
		DE.CM-3: فعالیت پرسنل برای شناسایی رویدادهای بالقوه امنیت سایبری نظارت می شود	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: کد مخرب شناسایی شد	SI-3, SI-8
		DE.CM-5: کد تلفن همراه غیرمجاز شناسایی شد	SC-18, SI-4. SC-44
		DE.CM-6: فعالیت ارائه‌دهنده خدمات خارجی برای شناسایی رویدادهای بالقوه امنیت سایبری نظارت می‌شود	CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: نظارت بر پرسنل، اتصالات، دستگاه ها و نرم افزارهای غیرمجاز انجام می شود	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: اسکن آسیب پذیری انجام می شود	RA-5
	Detection Processes (DE.DP): فرآیندها و روش‌های تشخیص برای اطمینان از آگاهی به موقع و کافی از رویدادهای غیرعادی حفظ و آزمایش می‌شوند.	**DE.DP-1:** نقش ها و مسئولیت های شناسایی برای اطمینان از پاسخگویی به خوبی تعریف شده است	CA-2, CA-7, PM-14
		DE.DP-2: فعالیت های تشخیص با تمام الزامات قابل اجرا مطابقت دارد	AC-25, CA-2, CA-7, PM-14, SA-18, SI-4
		DE.DP-3: فرآیندهای تشخیص آزمایش می شوند	CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: اطلاعات تشخیص رویداد به طرف های مربوطه مخابره می شود	AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: فرآیندهای تشخیص به طور مداوم بهبود می یابد	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

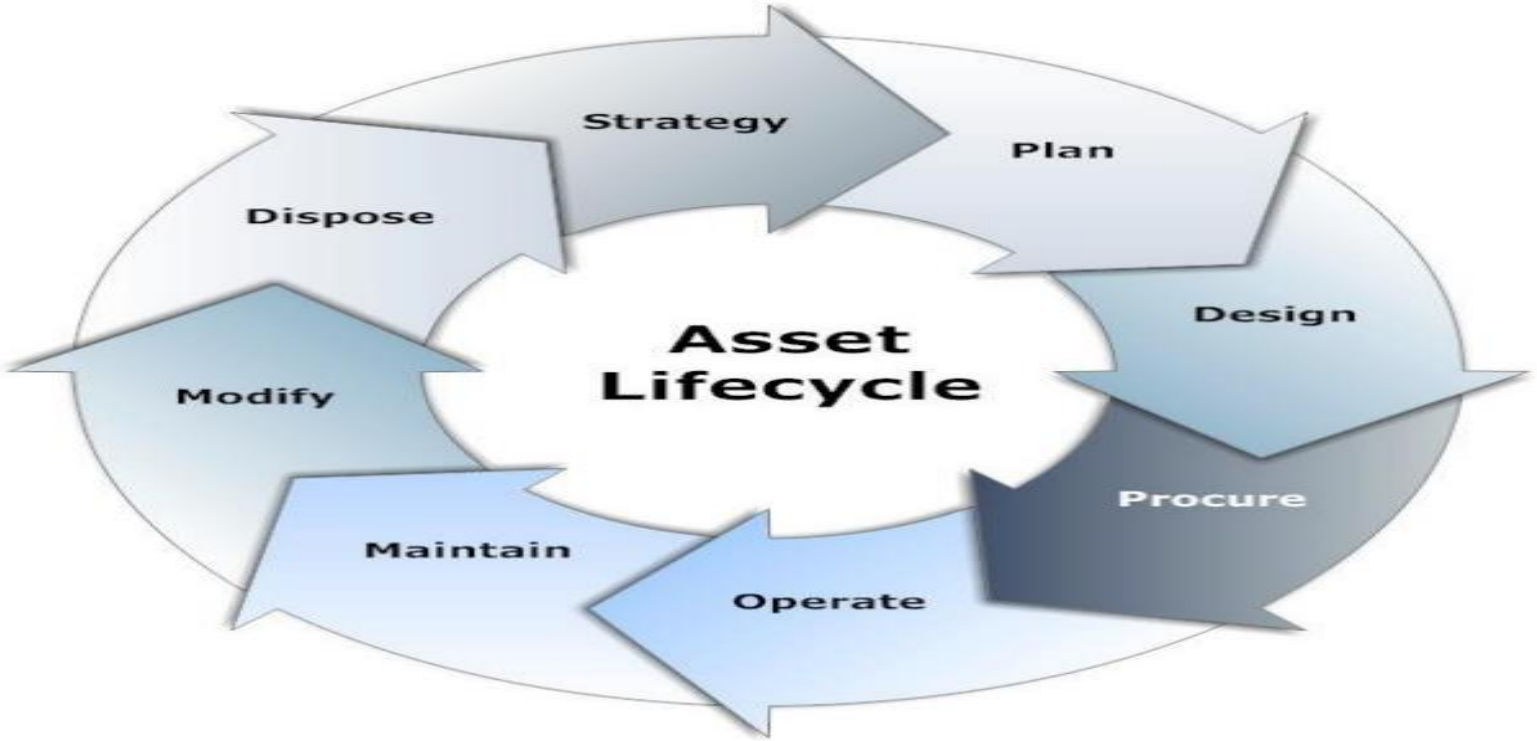
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	CP-2, IR-4
		RS.AN-3: Forensics are performed	AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	IR-4
		RS.MI-2: Incidents are mitigated	IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	CP-2, IR-4, IR-8

RESPOND (RS)	**Response Planning (RS.RP):** فرآیندها و رویه‌های پاسخ برای اطمینان از پاسخ به موقع به رویدادهای امنیت سایبری شناسایی شده اجرا و نگهداری می‌شوند..	**RS.RP-1:** طرح پاسخ در حین یا بعد از یک رویداد اجرا می شود	CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): فعالیت‌های واکنش با ذینفعان داخلی و خارجی هماهنگ می‌شوند تا در صورت لزوم شامل حمایت خارجی از سوی سازمان‌های مجری قانون شود.	**RS.CO-1:** پرسنل نقش و ترتیب عملیات خود را در مواقعی که نیاز به پاسخ است می دانند	CP-2, CP-3, IR-3, IR-8
		RS.CO-2: رویدادها مطابق با معیارهای تعیین شده گزارش می شوند	AU-6, IR-6, IR-8
		RS.CO-3: اطلاعات مطابق با طرح های پاسخ به اشتراک گذاشته می شود	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: هماهنگی با ذینفعان مطابق با طرح‌های واکنش صورت می‌گیرد	CP-2, IR-4, IR-8
		RS.CO-5: به اشتراک گذاری اطلاعات داوطلبانه با ذینفعان خارجی برای دستیابی به آگاهی موقعیتی گسترده تر از امنیت سایبری رخ می دهد.	PM-15, SI-5
	Analysis (RS.AN): تجزیه و تحلیل برای اطمینان از پاسخ کافی و حمایت از فعالیت های بازیابی انجام می شود.	**RS.AN-1:** اعلان‌های سیستم‌های تشخیص بررسی می‌شوند	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: تاثیر حادثه قابل درک است	CP-2, IR-4
		RS.AN-3: جرم شناسی انجام می شود	AU-7, IR-4
		RS.AN-4: حوادث مطابق با طرح های واکنش طبقه بندی می شوند	CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): فعالیت هایی برای جلوگیری از گسترش یک رویداد، کاهش اثرات آن و ریشه کن کردن حادثه انجام می شود.	**RS.MI-1:** حوادث مهار شده است	IR-4
		RS.MI-2: حوادث کاهش می یابد	IR-4
		RS.MI-3: آسیب پذیری های تازه شناسایی شده کاهش یافته یا به عنوان ریسک پذیرفته شده ثبت می شوند	CA-7, RA-3, RA-5
	Improvements (RS.IM): فعالیت های واکنش سازمانی با ترکیب درس های آموخته شده از فعالیت های شناسایی/پاسخ قبلی و فعلی بهبود می یابد.	**RS.IM-1:** طرح های پاسخ شامل درس های آموخته شده است	CP-2, IR-4, IR-8
		RS.IM-2: استراتژی های پاسخگویی به روز می شوند	CP-2, IR-4, IR-8

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	
		RC.CO-2: Reputation after an event is repaired	
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	CP-2, IR-4

RECOVER (RC)	**Recovery Planning (RC.RP):** فرآیندها و رویه‌های بازیابی برای اطمینان از بازیابی به موقع سیستم‌ها یا دارایی‌های متاثر از رویدادهای امنیت سایبری اجرا و نگهداری می‌شوند.	**RC.RP-1:** طرح بازیابی در طول یا بعد از یک رویداد اجرا می شود	CP-10, IR-4, IR-8
	Improvements (RC.IM): برنامه ریزی و فرآیندهای بازیابی با گنجاندن درس های آموخته شده در فعالیت های آینده بهبود می یابند.	**RC.IM-1:** برنامه های بهبودی شامل درس های آموخته شده است	CP-2, IR-4, IR-8
		RC.IM-2: استراتژی های بازیابی به روز می شوند	CP-2, IR-4, IR-8
	Communications (RC.CO): فعالیت های بازسازی با طرف های داخلی و خارجی، مانند مراکز هماهنگ کننده، ارائه دهندگان خدمات اینترنتی، صاحبان CSIRTسیستم های حمله کننده، قربانیان، سایر ها و فروشندگان هماهنگ می شوند.	**RC.CO-1:** روابط عمومی مدیریت می شود	
		RC.CO-2: اعتبار پس از یک رویداد ترمیم می شود	
		RC.CO-3: فعالیت های بازیابی به ذینفعان داخلی و تیم های اجرایی و مدیریتی اطلاع رسانی می شود	CP-2, IR-4

ASSET ENROLLMENT, OPERATION, AND END-OF-LIFE PHASES



ASSET ENROLLMENT

Enrollment:

- Manual activities performed by IT staff such as assigning and tagging the asset with a serial number and barcode
- Loading a baseline IT image
- Assigning the asset to an owner
- Recording the serial number and other attributes into a database.
- The attributes might also include primary location, hardware model, baseline IT image, and owner.

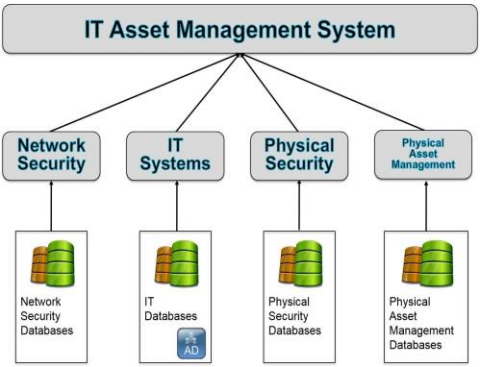
NIST SPECIAL PUBLICATION 1800-5

- **Reference Architecture Description ITAM refers to a set of policies and procedures that an organization uses to track, audit, and monitor the state of its IT assets, and maintain system configurations.**
- **Assets:**
  - computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards)” .
- **The cybersecurity value of ITAM is derived from some key aspects of the Risk Management Framework and the NIST Framework for Improving Critical Infrastructure Cybersecurity:**
  - selection and application of baseline security controls
  - continuous monitoring and reporting of asset status to a data store
  - implementation of anomaly detection mechanisms

ITAM (Information Technology Asset Management)

ارزش امنیت سایبری ITAM از برخی جنبه های کلیدی چارچوب مدیریت ریسک و چارچوب NIST برای بهبود امنیت سایبری زیرساخت حیاتی مشتق شده است، از جمله:

- ❖ انتخاب و بکارگیری کنترل های امنیتی پایه
- ❖ نظارت مستمر و گزارش وضعیت دارایی
- ❖ اجرای مکانیسم های تشخیص ناهنجاری. به عنوان مثال می توان به انحراف از ترافیک شبکه عادی یا انحراف از خطوط پایه پیکربندی تعیین شده اشاره کرد
- ❖ فراهم کردن زمینه برای ناهنجاری های شناسایی شده و رویدادهای امنیت سایبری در موتور گزارش دهی و تحلیلی



ITAM (Information Technology Asset Management)

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

قابلیت های موجود در ساخت ITAM بدین شرح می باشد:

1. **جمع آوری داده ها و گزارش نرم افزار و پیکربندی سیستمی منحصر به فرد هر دارایی و انتقال آن اطلاعات به محل های ذخیره سازی داده.**
2. **تجزیه و تحلیل داده ها که عملکردهای تحلیلی را بر روی داده های ذخیره شده انجام می دهد.**
3. **اعمال سیاست های سازمانی که بر دارایی های فناوری اطلاعات اعمال می شوند. این قوانین می تواند شامل شبکه/وب سایت هایی باشد که کارمندان می توانند از آنها بازدید کنند، چه نرم افزارهایی را می توان نصب کرد و چه خدمات شبکه ای مجاز است.**
4. **سیستم‌های مدیریت پیکربندی، حاکمیت و خط‌مشی‌های سازمانی را از طریق اقداماتی مانند اعمال وصله‌ها و به‌روزرسانی‌های نرم‌افزار، حذف نرم‌افزارهای لیست سیاه، و به‌روزرسانی خودکار پیکربندی‌ها اعمال می‌کند.**
5. **تهیه گزارش و نمایش جداول گرافیکی و عددی قابل خواندن توسط انسان که توسط قابلیت Data Analytics ارائه می شود.**

هر پنج قابلیت «زمان اجرا» هستند، زیرا به صورت دوره‌ای به صورت خودکار اتفاق می‌افتند.

پس از انجام تنظیمات اولیه و وارد کردن دستی دارایی در پایگاه داده دارایی، اکثر کارها به صورت خودکار انجام می شوند.

تحلیلگران ملزم به بررسی دوره ای گزارش های ذخیره شده در موتور تحلیلی برای تعیین ناهنجاری ها و انجام اصلاح هستند.

معیارهای مهم ارزیابی ابزارهای مدیریت دارایی:

- **تجربه تثبیت شده در مدیریت دارایی فناوری اطلاعات و توسعه نرم افزار.**
- **قابلیت به روز شدن در آینده.**
- **شواهد موفقیت و تخصص، مانند جوایز، اعتبارنامه ها و گواهینامه ها.**
- **اولویت شرکت و تمرکز بر توسعه نرم افزار مدیریت دارایی فناوری اطلاعات (بر خلاف خدمات حرفه ای، تمرکز توسعه بر سایر محصولات نرم افزاری و غیره).**
- **تاریخچه معرفی محصول و نوآوری تثبیت شده.**

ITAM (Information Technology Asset Management)

چالش ها:

- **نشان دادن و حس کردن مزایای ITAM بسیار وقت گیر است، به ویژه با استفاده از روشی که در سراسر سازمان پذیرفته شده است. با این حال، این عمل باعث اعتبار بخشی هموار نمودن راه برای افزایش بلوغ برنامه های ITAM می باشد.**
- **مدیران دارایی IT اغلب مطمئن نیستند که از چه نوع معیارهایی برای نشان دادن ارزش ITAM که برای کسب و کار معنادار است استفاده کنند.**

توصیه ها

این مراحل را دنبال کنند:

۱. مشخص کنید که چه چیزی برای کسب و کار و فناوری اطلاعات شما از نظر اهداف و نتایج مطلوب مهم است.

۲. فرآیندهای ITAM موجود خود را برای فعالیت هایی که به این نتایج دلخواه مرتبط می شوند، استخراج کنید.

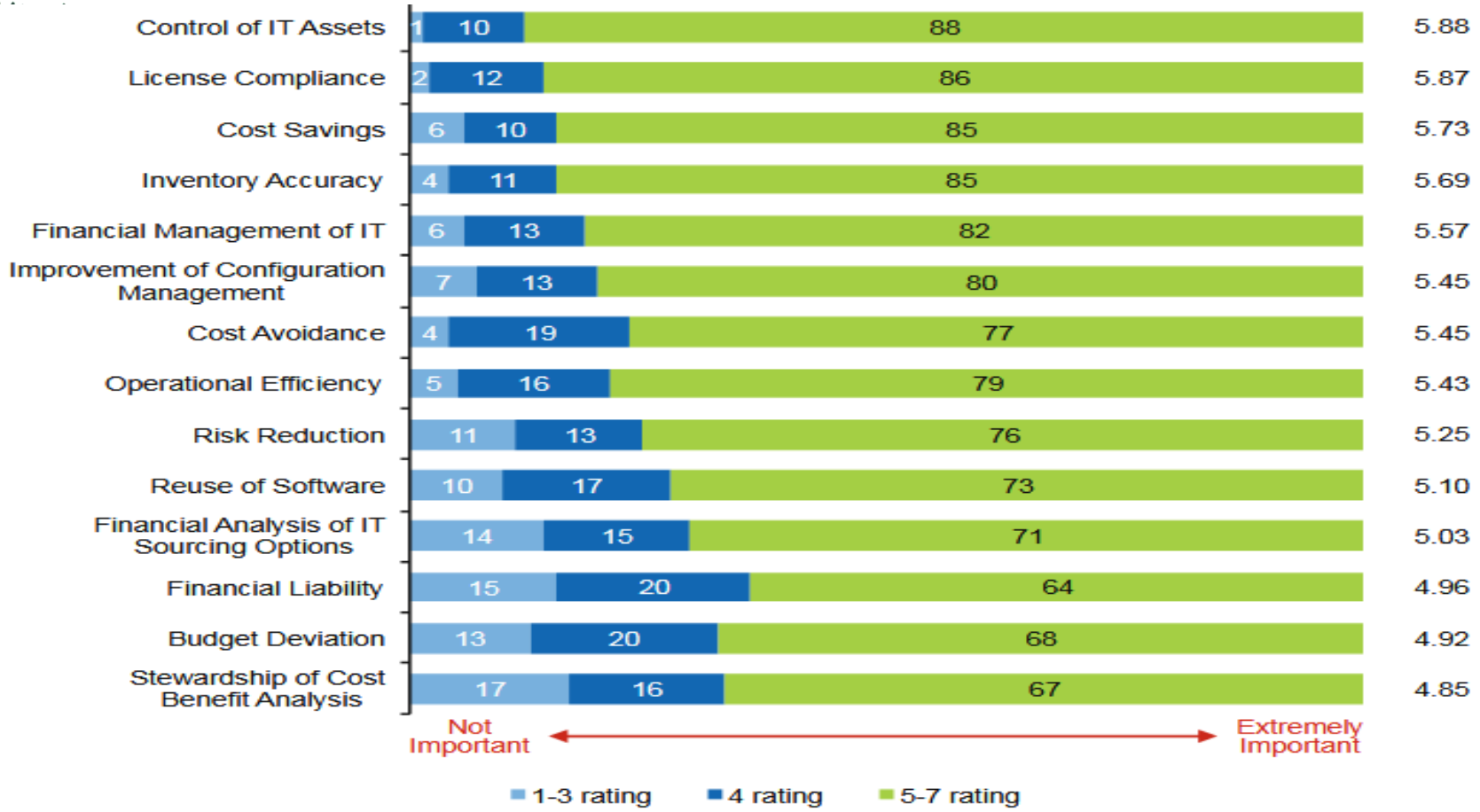
۳. تعیین کنید که چه نتایجی را می توان به طور موثر اندازه گیری و ردیابی کرد.

۴. یک نظم و انضباط مداوم برای ردیابی مزایای ITAM ایجاد کنید که شامل اعتبارسنجی اندازه گیری و ارتباطات نتایج است.

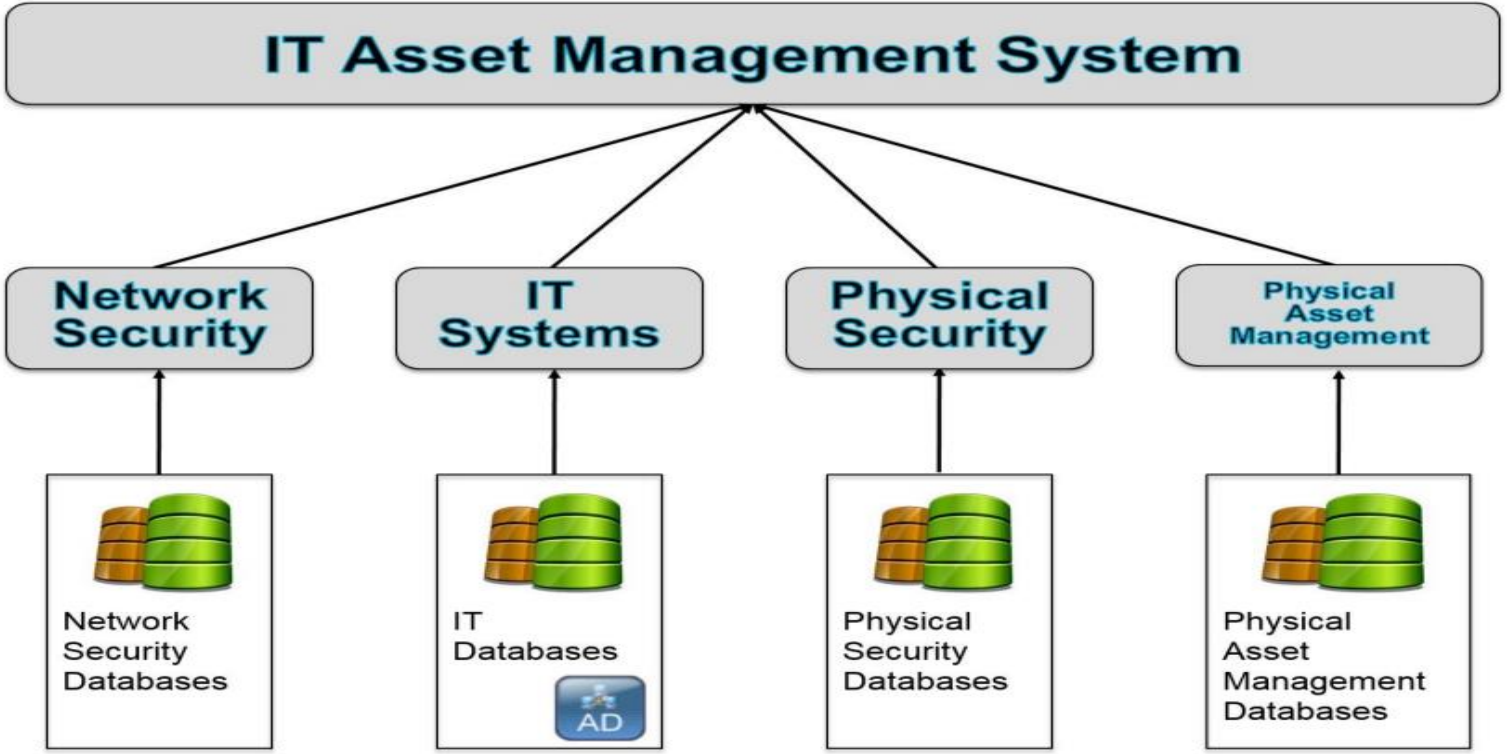
توصیه ها

- معیارهای ارزش ITAM خود را با ابتکارات تجاری مهم تراز کنید تا تأثیر نتایج را به حداکثر برسانید.
- اگر کسب و کار شما اطلاعات بسیار حساسی را حفظ می کند، در نقاط پایانی مانند رایانه های شخصی یا تلفن های همراه نگران کننده است، در این صورت معیارهای ریسک امنیتی نیز برای ردیابی بسیار سودمند خواهند بود.
- به عنوان مثال، تعداد دفعاتی که فرآیند ITAM توانست با موفقیت داده‌ها را از دستگاه‌های گم شده یا دزدیده شده پاک کند. در برخی موارد، برای جلوگیری از از دست دادن داده ها، ممکن است ارزش پولی تعیین شود، یا حداقل تخمین زده شود.

توصیه ها


Control of IT Assets 1 10 88 5.88
License Compliance 2 12 86 5.87
Cost Savings 6 10 85 5.73
Inventory Accuracy 4 11 85 5.69
Financial Management of IT 6 13 82 5.57
Improvement of Configuration Management 7 13 80 5.45
Cost Avoidance 4 19 77 5.45
Operational Efficiency 5 16 79 5.43
Risk Reduction 11 13 76 5.25
Reuse of Software 10 17 73 5.10
Financial Analysis of IT Sourcing Options 14 15 71 5.03
Financial Liability 15 20 64 4.96
Budget Deviation 13 20 68 4.92
Stewardship of Cost Benefit Analysis 17 16 67 4.85
Not Important
Extremely Important
1-3 rating
4 rating
5-7 rating

ITAM REFERENCE ARCHITECTURE



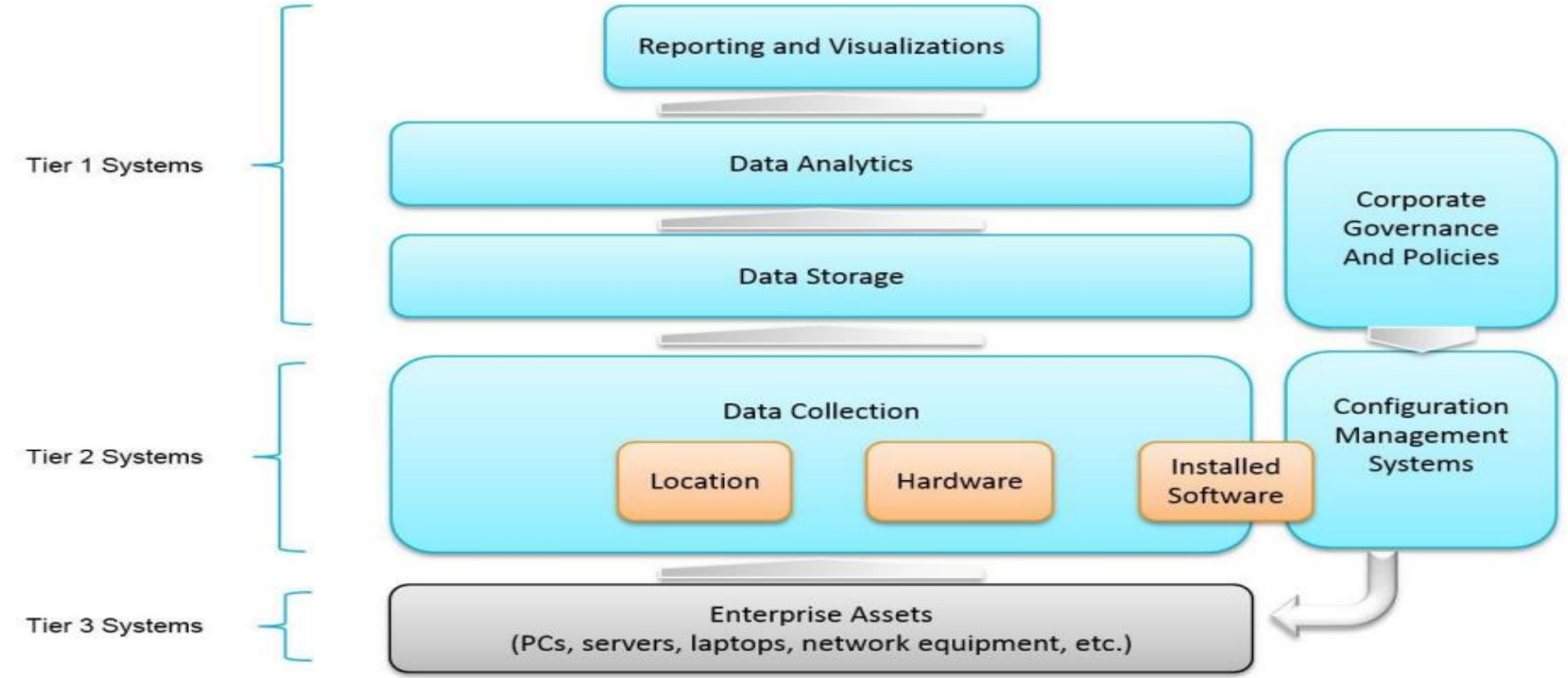
ITAM REFERENCE ARCHITECTURE

ITAM Reference Functionality, shows how data flows through the ITAM system.

- **Tier 3 is composed of enterprise assets themselves. Tier 3 is made up of all of the assets being tracked including hardware, software, and virtual machines.**
- **Tier 2 includes the sensors and independent systems that feed data into the enterprise ITAM system. Tier 2 systems include passive and active collection sensor and agents.**
- **Tier 1 is the enterprise ITAM system that provides the aggregation of data from all Tier 2 systems into business and security intelligence**

ITAM REFERENCE ARCHITECTURE

Figure 5-2 ITAM Reference Functionality



ITAM REFERENCE ARCHITECTURE

ITAM Reference Functionality, shows how data flows through the ITAM system.

- **Tier 3 is composed of enterprise assets themselves. Tier 3 is made up of all of the assets being tracked including hardware, software, and virtual machines.**
- **Tier 2 includes the sensors and independent systems that feed data into the enterprise ITAM system. Tier 2 systems include passive and active collection sensor and agents.**
- **Tier 1 is the enterprise ITAM system that provides the aggregation of data from all Tier 2 systems into business and security intelligence**

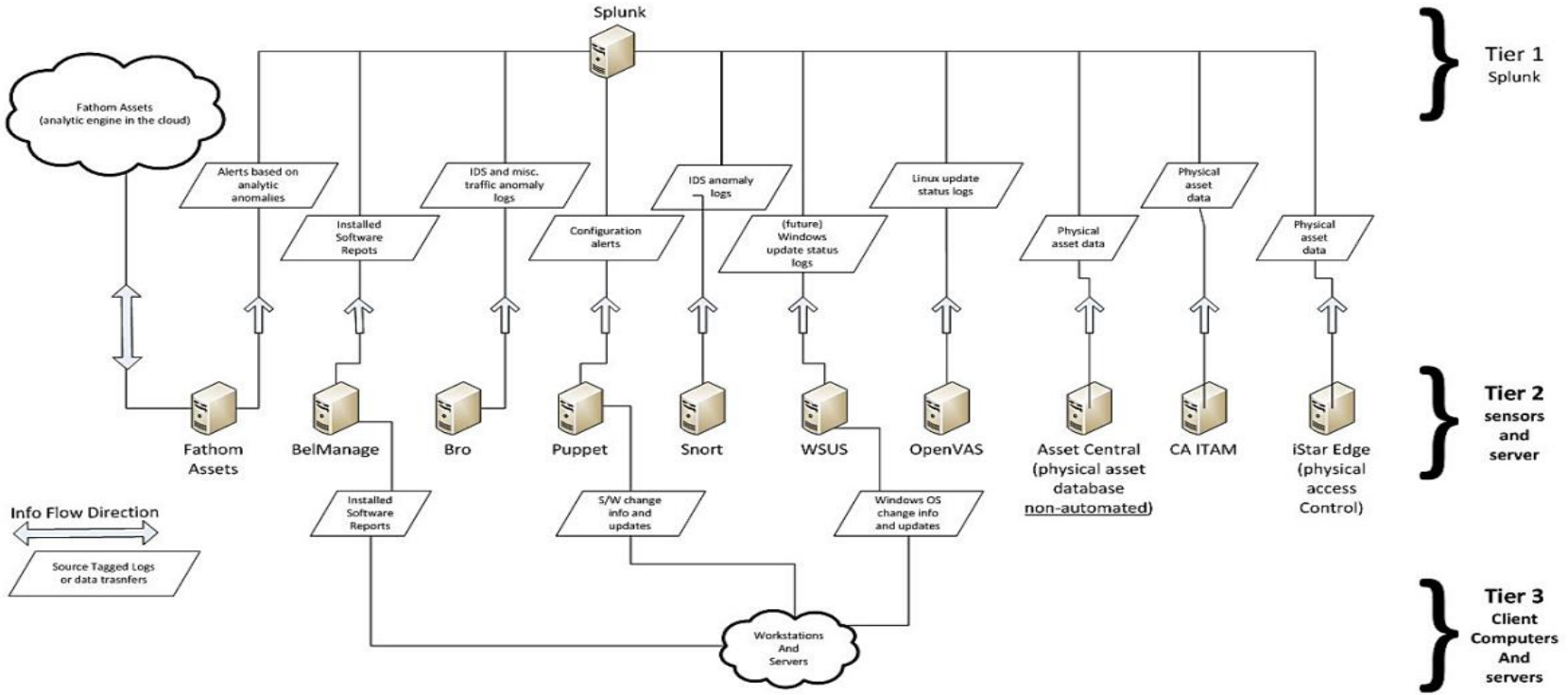
ITAM REFERENCE ARCHITECTURE

ITAM Reference Functionality

1. **Data Collection is the capability to enumerate and report the unique software and system configuration of each asset and transfer that information to the Data Storage capability.**
2. **Data Storage is the capability that receives data from the data collection capability, re-formats as needed, and stores the data in a storage system.**
3. **Data Analytics is the capability that performs analytic functions on the data made available by the Data Storage capability.**
4. **Corporate Governance and Policies are all of the rules that are placed upon the IT assets. These rules can include the network/web sites that employees can visit, what software can be installed, and what network services are allowed.**
5. **Configuration Management Systems enforce Corporate Governance and Policies through actions such as applying software patches and updates, removing blacklisted software, and automatically updating configurations.**
6. **Reporting and Visualizations is the capability that generates human-readable graphical and numerical tables of information provided by the Data Analytics capability.**

ACCESS AUTHORIZATION INFORMATION FLOW AND CONTROL POINTS

Figure 5-10 ITAM Data Flow



ACCESS AUTHORIZATION INFORMATION FLOW AND CONTROL POINTS

The ITAM solution deploys sensors throughout the enterprise that collect data from, or about, enterprise assets.

The sensors can be installed on the assets, collecting data about installed software, or they can be remote devices that monitor and scan the network, reporting on vulnerabilities, anomalies, and intrusions.

These sensors forward collected data to middle tier services that are responsible for storing, formatting, filtering, and forwarding the data to the analysis engine.

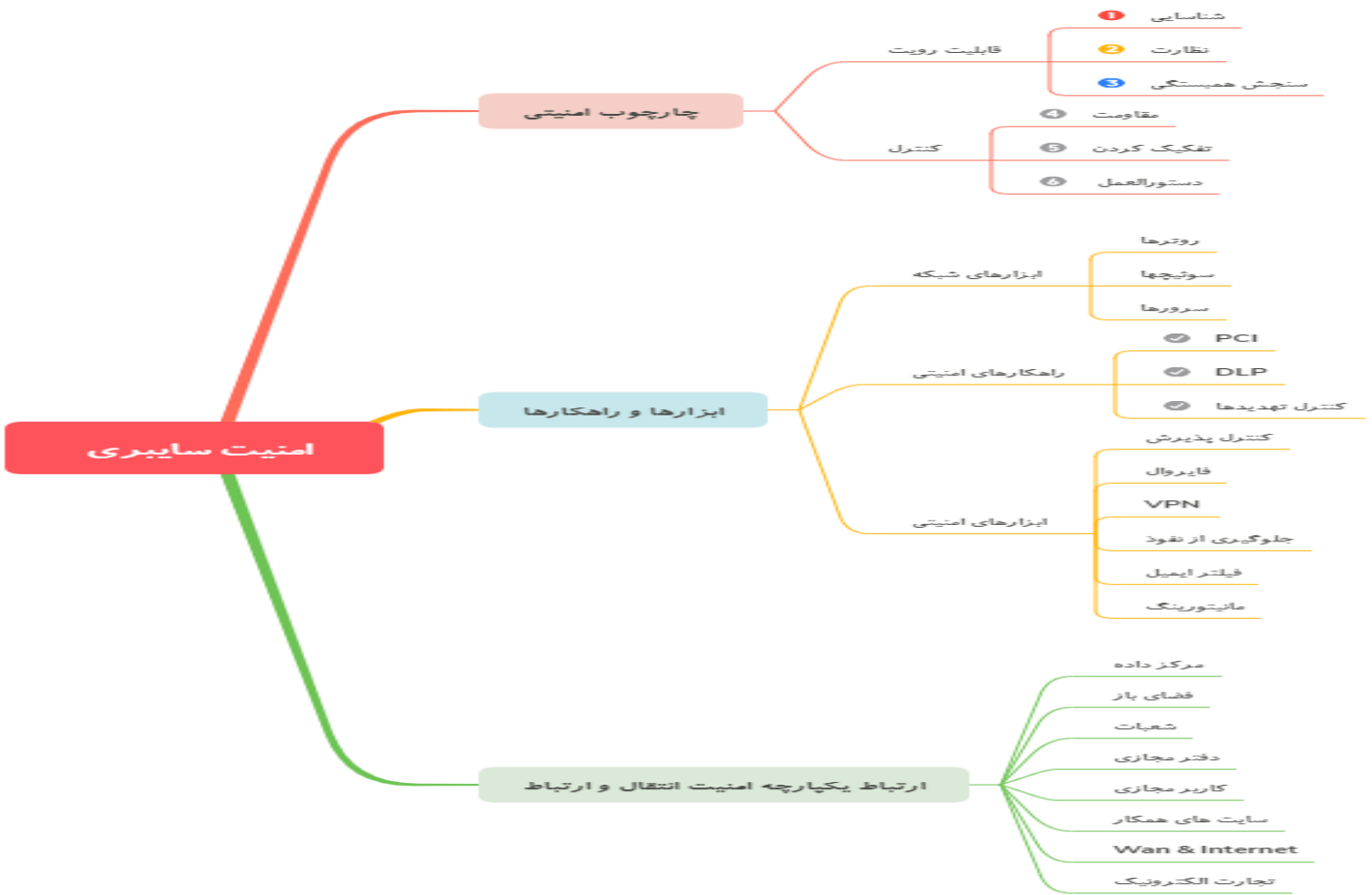
Further analysis of the data is performed on the analysis engine and involves running select queries to retrieve defined data using a visualization tool also installed on the analysis engine.

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

چارچوب تاب آوری سایبری

CYBER RESILIENCE FRAMEWORK


امنیت سایبری
چارچوب امنیتی
قابلیت رویت
1 شناسایی
2 نظارت
3 سنجش همبستگی
کنترل
4 مقاومت
5 تفکیک کردن
6 دستورالعمل
ابزارها و راهکارها
ابزارهای شبکه
روترها
سوئیچها
سرورها
راهکارهای امنیتی
PCI
DLP
کنترل تهدیدها
ابزارهای امنیتی
کنترل پذیرش
فایروال
VPN
جلوگیری از نفوذ
فیلتر ایمیل
مانیتورینگ
ارتباط یکپارچه امنیت انتقال و ارتباط
مرکز داده
فضای باز
شعبات
دفتر مجازی
کاربر مجازی
سایت های همکار
Wan & Internet
تجارت الکترونیک

تاب آوری سایبری

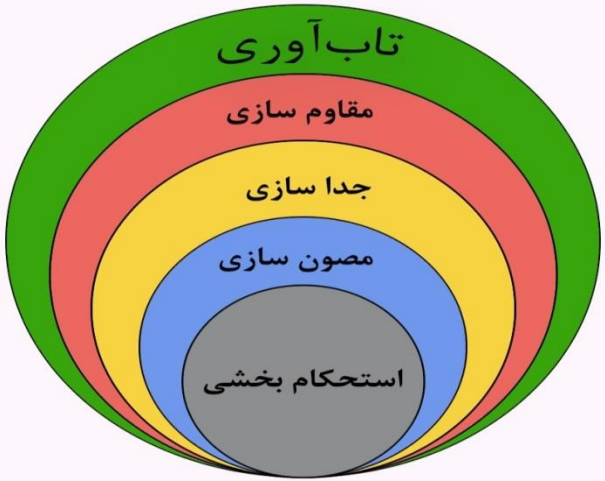
1. تاب آوری سایبری به عنوان «توانایی پیش‌بینی، مقاومت، بازیابی و انطباق با شرایط نامطلوب، استرس‌ها، حملات و...» تعریف می‌شود.
2. تاب آوری سایبری باعث می شود سازمان ها در برابر حملات سایبری، شکاف ها و شکست‌ها مقاومت کنند
3. و همچنین می‌توانند حتی در وضعیت تخریب شده یا ضعیف به کار خود ادامه دهند
4. و وظایف ضروری مأموریتی خود را انجام دهند
5. و اطمینان حاصل کنند که سایر جنبه‌های قابل اعتماد بودن (به ویژه ایمنی و امنیت اطلاعات حفظ می شوند.

تاب آوری سایبری

1. **تاب آوری سایبری توانایی آماده شدن، پاسخ به حملات سایبری و بازیابی از آن است.**
2. **این امر در چند سال گذشته پدیدار شده است زیرا اقدامات سنتی امنیت سایبری دیگر برای محافظت از سازمان ها در برابر موج حملات مداوم کافی نیست.**
3. **تاب آوری سایبری به سازمان کمک می‌کند تا در برابر خطرات سایبری محافظت کند.**
   - و در برابر حملات دفاع کند
   - و شدت آن را محدود کند
   - و از ادامه بقای خود با وجود حمله اطمینان حاصل کند
4. **منظور از تاب آوری سایبری؛ به توانایی یک سازمان، شرکت، یک واحد تجاری و ... برای ارائه خدمت (خدمات رسانی) علیرغم رویدادهای نامطلوب سایبری اشاره دارد.**

تاب آوری

- استحکام بخشی
  - حملات هدف گرا
  - آماده کردن /شناسایی، محافظت، شناسایی
  - امنیت اطلاعات
  - تداوم کسب و کار
  - تاب آوری سازمان
  - بقا
  - قابل اعتماد
  - رانش صفر
  - شکار تهدید
  - اطلاعات تهدید
- مصون سازی
  - مدیریت دارایی
  - مدیریت کنترل‌ها
  - برنامه اقدامات و نقاط عطف
  - پیکربندی و مدیریت تغییر
  - مدیریت تهدید
  - مدیریت آسیب پذیری
  - مدیریت حوادث
  - مدیریت تداوم خدمات
  - مدیریت ریسک و گزارش
  - مدیریت وابستگی خارجی
  - آموزش و آگاهی
  - برنامه ریزی احتمال
  - سیستم های بیمانکار
  - برنامه ریزی سرمایه امنیتی
  - آگاهی از موقعیت
- جدا سازی
  - معماری جداسازی
  - جداسازی شبکه ها
  - رصد و پایش شبکه و سنسورها
  - جداسازی منطقی زیرساخت، شبکه ها، کاربران و فرآیندها
- مقاوم سازی
  - مقاوم سازی رایانه ها
  - مقاوم سازی ابزارهای شبکه



تاب آوری سایبری

تاب آوری سایبری:

- قابلیت ارجاعی (elasticity)
- انعطاف پذیری (flexibility)
- برگشت پذیری – امن (safe)
- اطمینان – قابل تحمل (tolerable /bearable)
- و پایایی (survivability)

ویژگی های بهبود ارتقاء تاب آوری سیستم

مزیت هایی تاب آوری سایبری سازمان

1. حفظ تداوم کسب و کار
2. ایمن نگه داشتن اطلاعات مشتری
3. رعایت مقررات حفاظت از داده ها و انطباق
4. جلب اعتماد مشتری

پیشگیری

آیا مکانیزم مناسبی برای شناسایی یک تهدید سایبری قبل از اجرا دارید؟

آیا راه‌حل‌های نرم‌افزاری حفاظت از داده‌ها و امنیت شما به‌طور مرتب به‌روزرسانی می‌شوند تا از دسترسی عوامل تهدید از طریق سیستم‌های آسیب‌پذیر یا اصلاح‌نشده جلوگیری شود؟

آیا از شکاف هایی که باعث حمله سایبری به سایر شرکت های صنعت شما شده است آگاه هستید؟ آیا آن شکاف ها را مسدود کرده اید؟

حفاظت

در صورت وقوع یک حادثه امنیت سایبری، آیا میتوانید بدون تأثیرگذاری بر عملیات حیاتی تجاری، از گسترش حمله جلوگیری کنید؟

آیا می توانید منابع داده های آلوده (دستگاه ها و سرورها) را شناسایی کرده و آنها را قرنطینه یا ایزوله کنید تا آلودگی فراتر از سخت افزار آسیب دیده فراتر نرود؟

پاسخ دهی

آیا مدیران سطح ارشد سازمان شما از نحوه پاسخگویی به ذینفعان داخلی (اعضای هیئت مدیره) و خارجی (سهامداران) در حین و پس از یک تهدید سایبری آگاه هستند؟

آیا سازمان شما طرحی برای واکنش به حادثه دارد که مسئولیت های تیم های مختلف را در زمان وقوع حمله مشخص کند؟

آیا می توانید به طور خودکار (بدون مداخله فناوری اطلاعات) با استفاده از کتاب های بازی خودکار حوادث به یک حمله پاسخ دهید؟

بازیابی

آیا ابزارها و خدمات ارکستراسیون و اتوماسیون مناسبی برای بازگشت به مسیر پس از یک رویداد دارید؟

آیا مکانیزمی برای بازیابی اطلاعات از دست رفته دارید؟

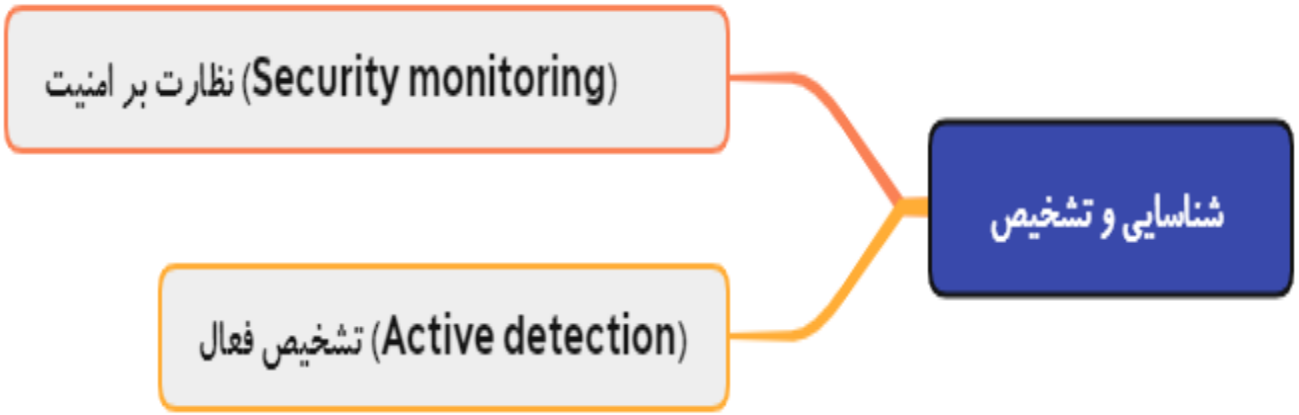
برنامه عملی برای پر کردن شکاف هایی که باعث حمله شده است چیست؟

چهار عنصر چارچوب تاب آوری سایبری

مدیریت و محافظت

1. اولین عنصر یک برنامه تاب آوری سایبری شامل توانایی شناسایی، ارزیابی و مدیریت ریسک های مرتبط با شبکه و سیستم های اطلاعاتی، از جمله خطرات در سراسر زنجیره تامین است.
2. همچنین مستلزم محافظت از اطلاعات و سیستم ها در برابر حملات سایبری، خرابی سیستم و دسترسی غیرمجاز است. این مرحله باید شامل سیزده آیتم هست

چهار عنصر چارچوب تاب آوری سایبری



مدیریت و محافظت

- (Malware protection)حفاظت از بدافزار
- (Information and security policies)سیاست های اطلاعاتی و امنیتی
- (The formal information security management program) برنامه رسمی مدیریت امنیت اطلاعات
- (Identity and access control) کنترل هویت و دسترسی
- (Security teams' competence and regular training) شایستگی تیم های امنیتی و آموزش منظم
- (Security staff awareness training) آموزش آگاهی کارکنان امنیتی
- (Encryption) رمزگذاری
- (Physical and environmental security)امنیت فیزیکی و محیطی
- (Patch management) مدیریت وصله
- (Network and communications security) امنیت شبکه و ارتباطات
- (Systems security) امنیت سیستم ها
- (Asset management) مدیریت دارایی
- (Supply chain risk management) مدیریت ریسک زنجیره تامین

چهار عنصر چارچوب تاب آوری سایبری

شناسایی و تشخیص

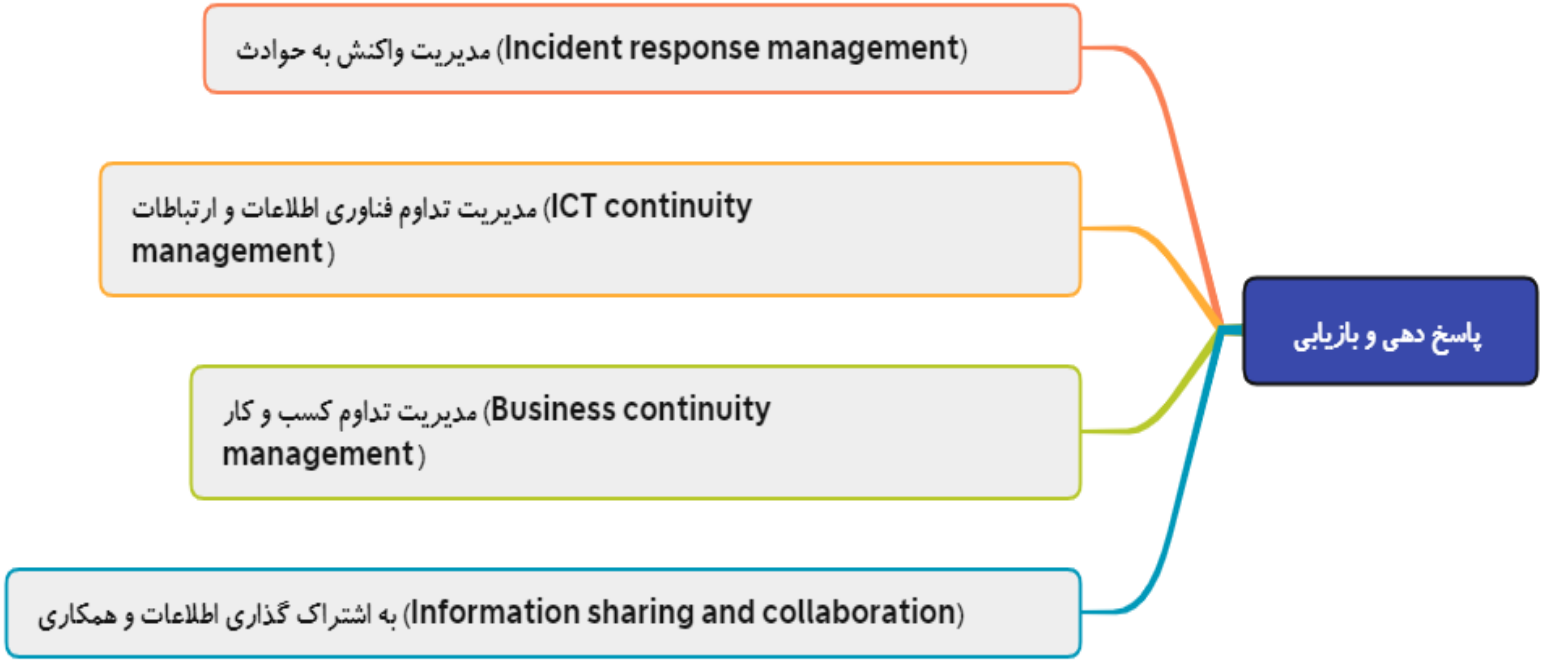
1. دومین عنصر یک برنامه انعطاف‌پذیری سایبری به نظارت مستمر شبکه و سیستم‌های اطلاعاتی برای شناسایی ناهنجاری‌ها و حوادث احتمالی امنیت سایبری قبل از اینکه آسیب قابل توجهی ایجاد کنند، بستگی دارد.
2. این مرحله باید شامل دو آیتم باشد

چهار عنصر چارچوب تاب آوری سایبری

پاسخ دهی و بازیابی

1. اجرای یک برنامه مدیریت واکنش به حادثه و اقداماتی برای اطمینان از تداوم کسب و کار به شما کمک می کند حتی اگر مورد حمله سایبری قرار گرفتید به فعالیت خود ادامه دهید و تا حد امکان سریع و کارآمد به تجارت عادی بازگردید.
2. این مرحله باید شامل چهار آیتم باشد

چهار عنصر چارچوب تاب آوری سایبری

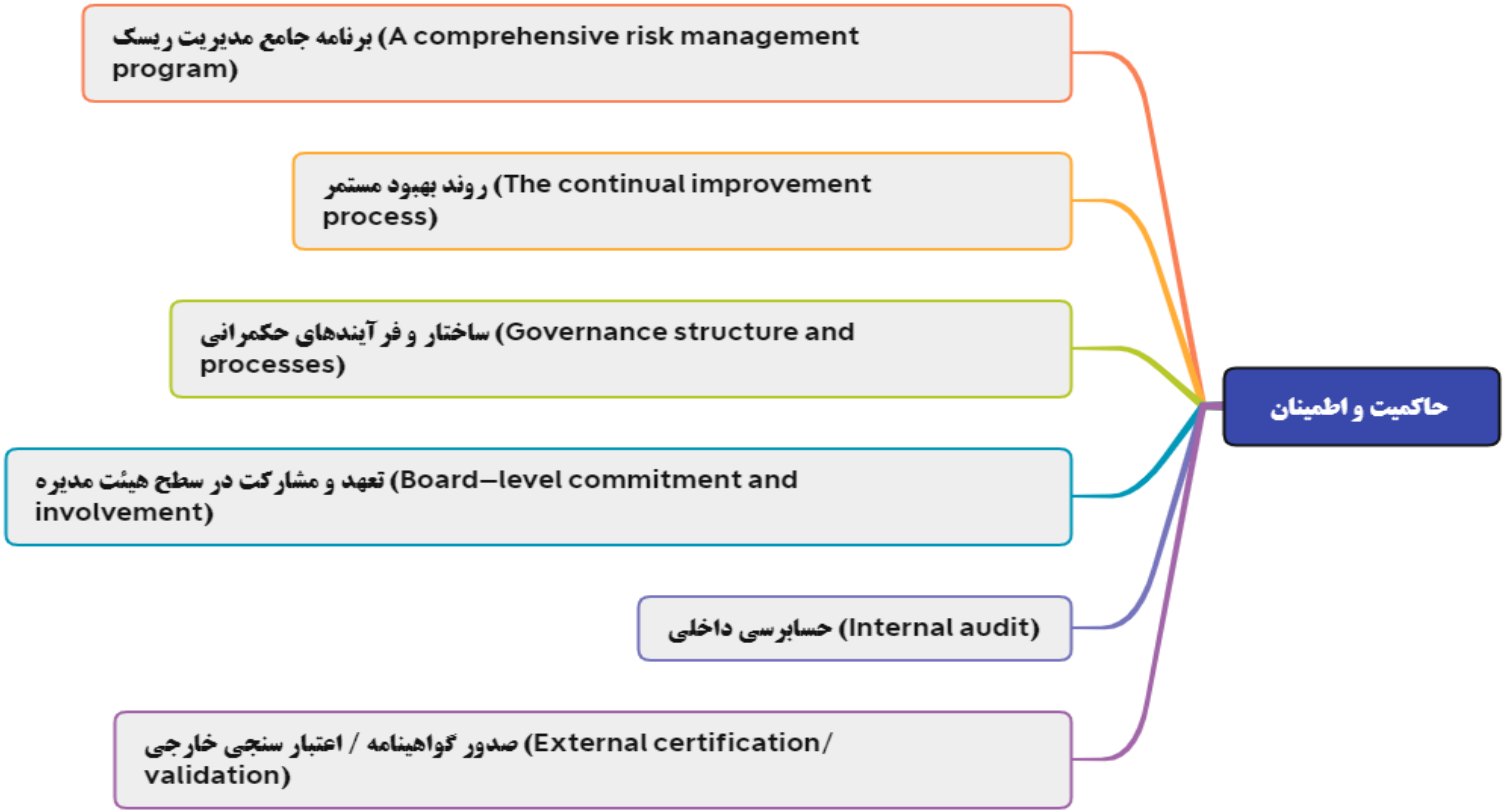


چهار عنصر چارچوب تاب آوری سایبری

حاکمیت و اطمینان

1. عنصر نهایی این است که اطمینان حاصل کنید که برنامه شما از بالای سازمان نظارت می شود و طبق معمول در تجارت ایجاد می شود. با گذشت زمان، باید بیشتر و بیشتر با اهداف تجاری شما هماهنگ باشد
2. این مرحله باید شامل شش آیتم باشد

چهار عنصر چارچوب تاب آوری سایبری



چارچوب تاب آوری ارائه شده توسط NIST

1. یک نمونه از چارچوب‌های انعطاف‌پذیری سایبری اخیراً توسعه‌یافته بر اساس NIST Special Publication 800-160, Vol. 2.18 می باشد که بر پایه این چهار عنصر است
2. استراتژی مدیریت ریسک– اهداف – اهداف– تکنیک

Risk management strategy	Goals
• Organizational level • Mission/business process level • System level	• Anticipate • Withstand • Recover • Adapt

Objectives		Techniques	
• Understand	• Constrain	• Deception	• Unpredictability
• Prevent/avoid	• Reconstitute	• Diversity	• Realignment
• Prepare	• Transform	• Redundancy	• Coordinated protection
• Continue	• Re-architect	• Segmentation	• . . .

بومی سازی متناسب با سازمان

یک واحد یا سازمان باید یک استراتژی و چارچوب شفاف تاب آوری سایبری متناسب با آسیب پذیری ها و تهدیدات در معرض اتخاذ نماید.یک استراتژی تاب آور سایبری باید موارد زیر را برای یک نهاد پوشش دهد:

- ☑اهمیت تاب آوری سایبری برای نهاد.
- ☑الزامات سطح بالای ذینفعان آن نهاد.
- ☑ چشم انداز و ماموریت نهاد در مورد تاب آوری سایبری.
- ☑ اهداف تاب آوری سایبری .
- ☑ تمایل به ریسک سایبری .
- ☑اهداف و طرح اجرای تاب آوری سایبری .
- ☑دامنه سطح بالای فناوری و دارایی هایی که برای مدیریت انعطاف پذیری سایبری استفاده خواهد شد.

بومی سازی متناسب با سازمان

☑ابتکارات تاب آوری سایبری چگونه ارائه، مدیریت و تامین مالی خواهد شد.

☑ ادغام تاب آوری سایبری با افراد، فرآیندها، فناوری و ابتکارات تجاری جدید یا موجود.

☑ با استفاده از استانداردها و دستورالعمل های پیشرو بین المللی و ملی به عنوان معیار طراحی شود.

☑ با چارچوب مدیریت ریسک نهاد سازگار باشد.

☑نهاد باید اطمینان حاصل کند که استراتژی و چارچوب انعطاف‌پذیری سایبری آن با اهداف تجاری، الزامات ذینفعان، استراتژی شرکت، چارچوب مدیریت ریسک و سایر استراتژی‌ها و چارچوب‌های مرتبط همسو است.

☑واحد باید اطمینان حاصل کند که استراتژی و چارچوب تاب‌آوری سایبری آن متناسب با تحمل ریسک و اهداف آن است.

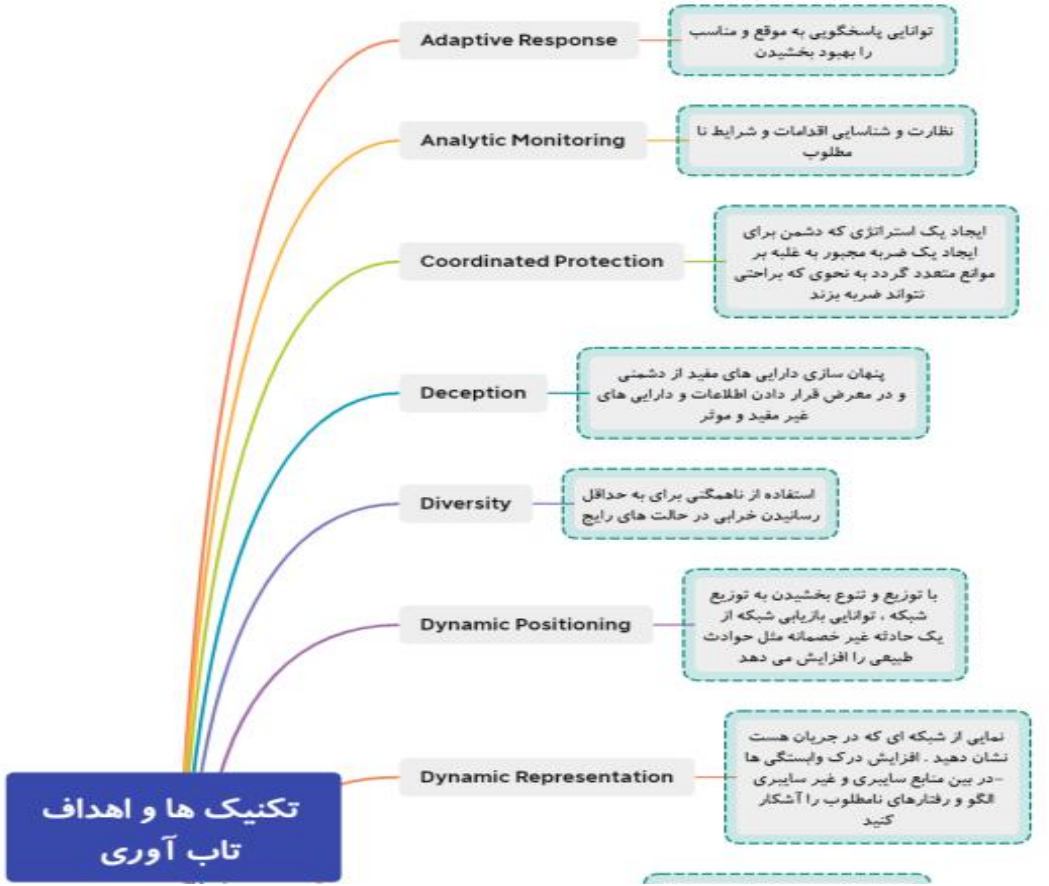
بومی سازی متناسب با سازمان

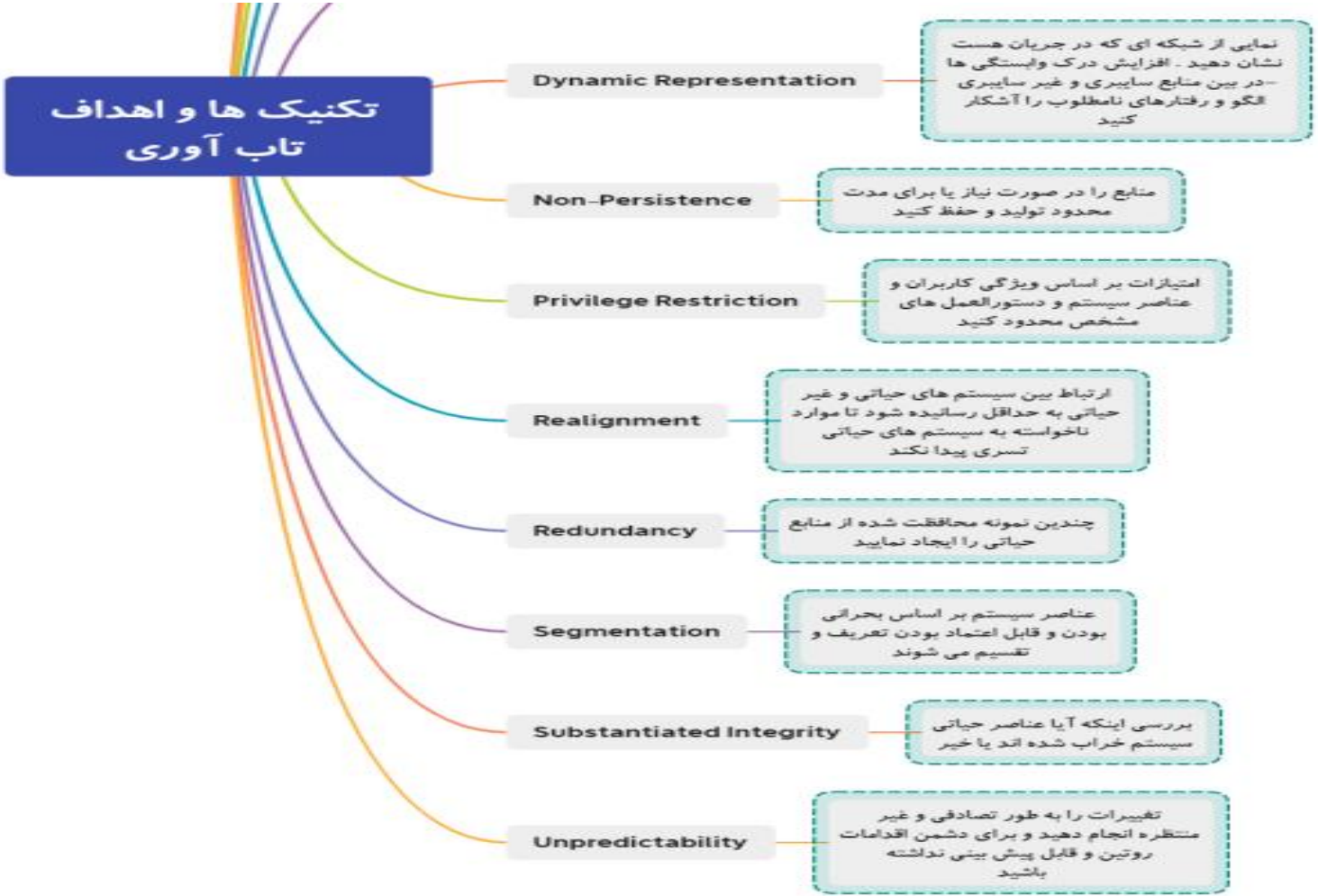
☑ واحد باید اطمینان حاصل کند که همه نقش‌ها و مسئولیت‌های مرتبط با تاب‌آوری سایبری به وضوح در چارچوب تاب‌آوری سایبری تعریف شده‌اند و با استراتژی تاب‌آوری سایبری همسو هستند.

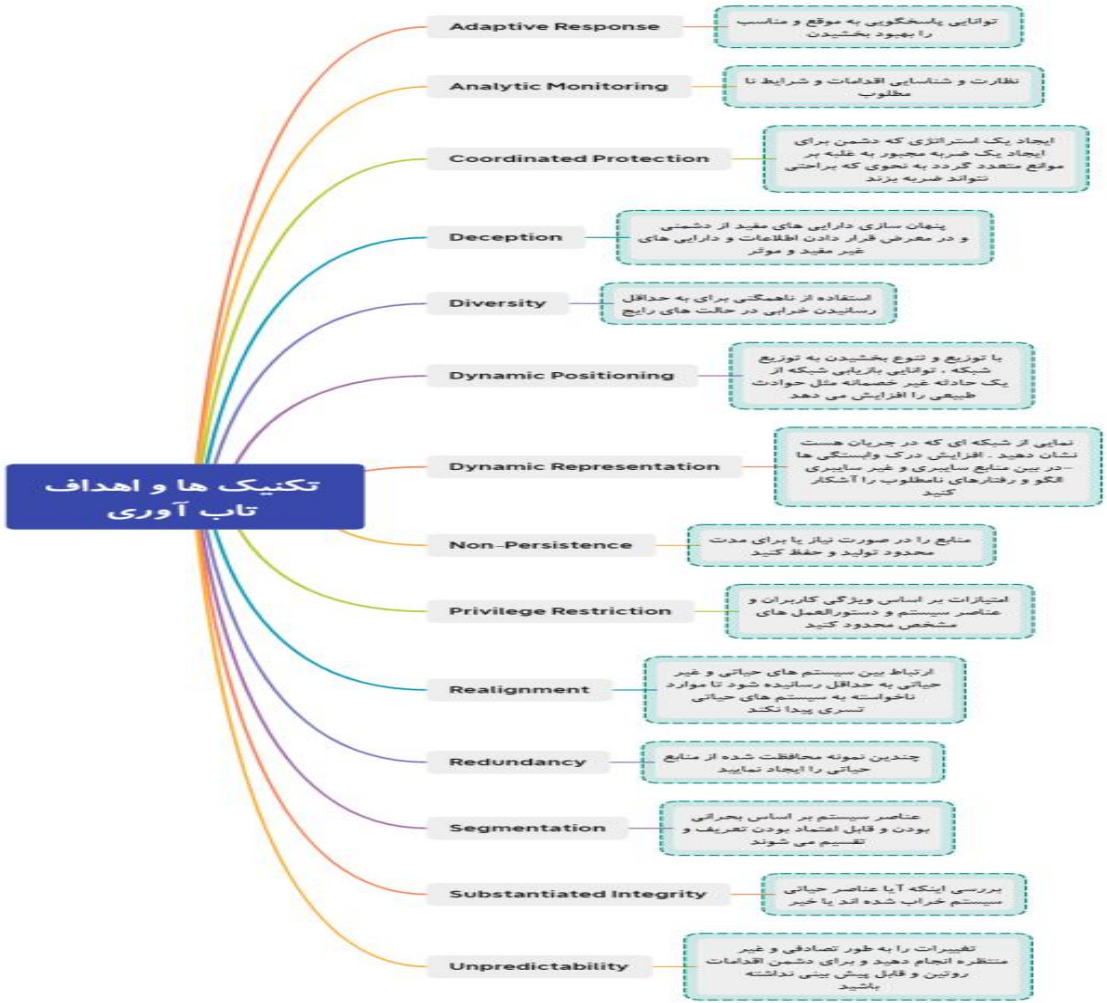
☑ واحد باید یک فرآیند حسابرسی داخلی برای کمک به نظارت و سنجش پیشرفت اجرا، کفایت و اثربخشی استراتژی و چارچوب تاب آوری سایبری خود داشته باشد. نهاد باید از استقلال تیم حسابرسی داخلی خود با استفاده از قابلیت حسابرسی داخلی درون سازمانی یا منابع خارجی خود اطمینان حاصل کند.

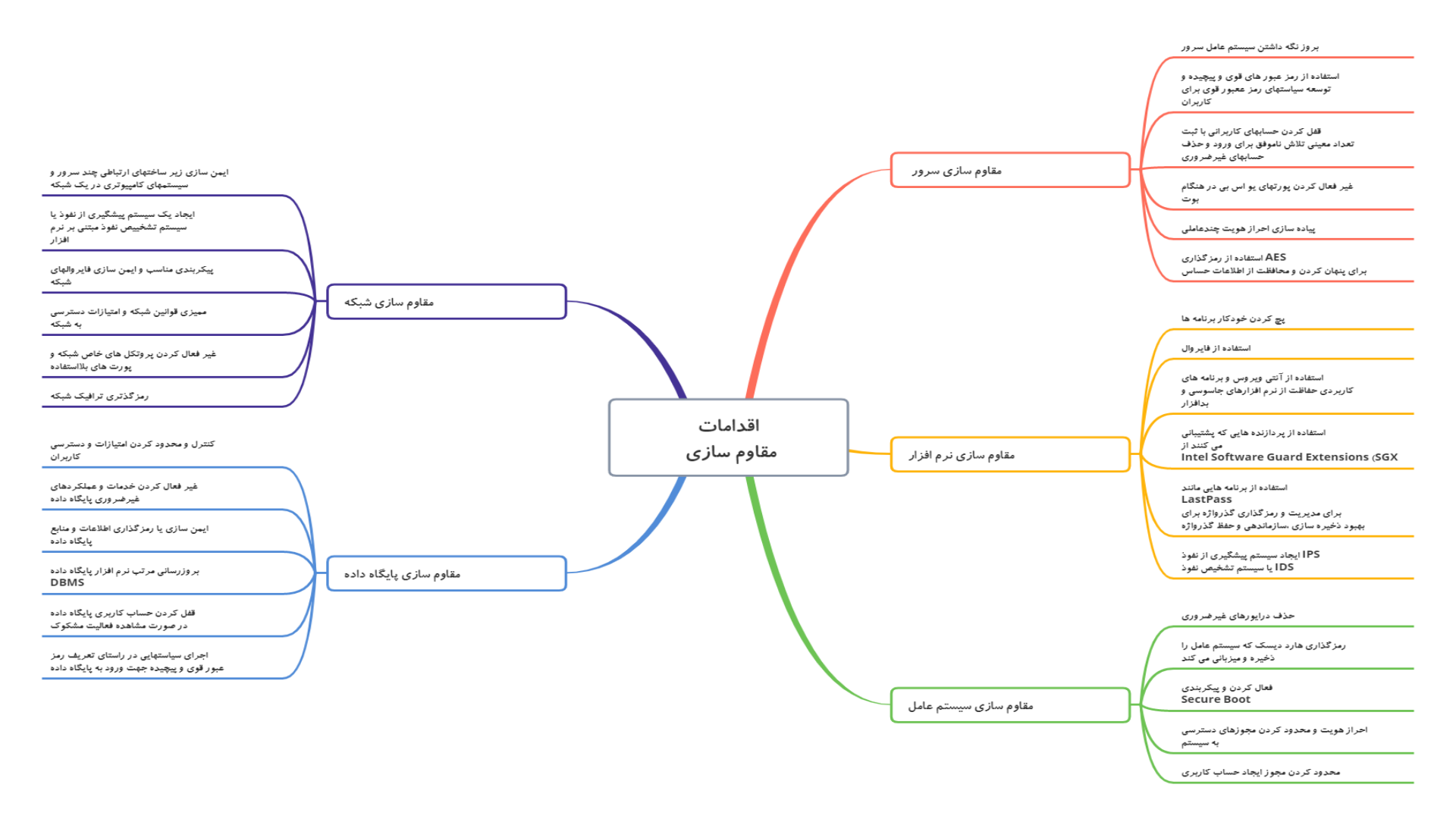
☑ استراتژی و چارچوب تاب‌آوری سایبری باید مرتباً مورد بازبینی و به‌روزرسانی قرار گیرد تا اطمینان حاصل شود که واحد تجاری می‌تواند در میان هرگونه تغییر در محیط ریسک سایبری به عملیات تجاری سالم ادامه دهد.

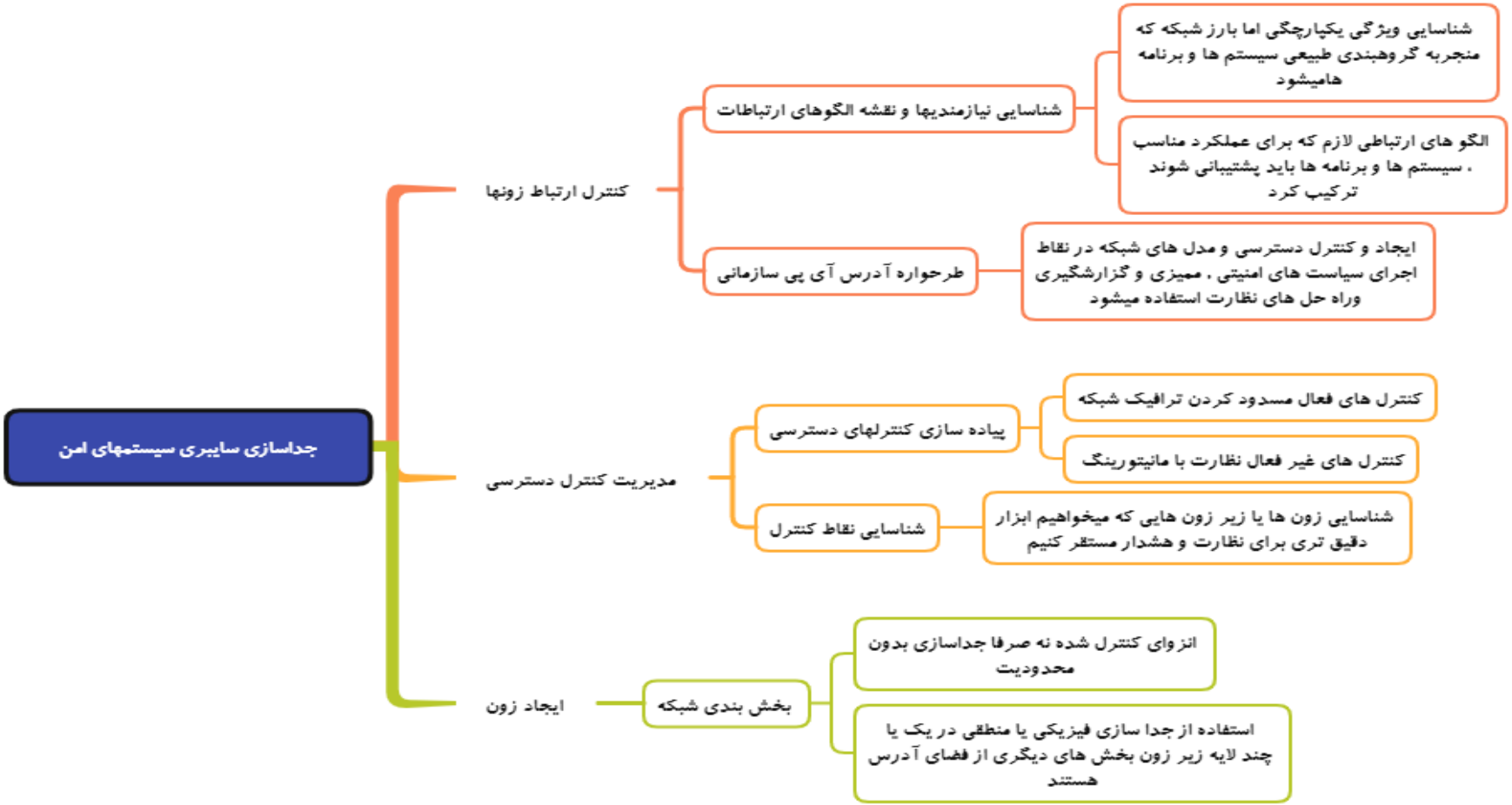
تکنیک های تاب آوری و اهداف آن

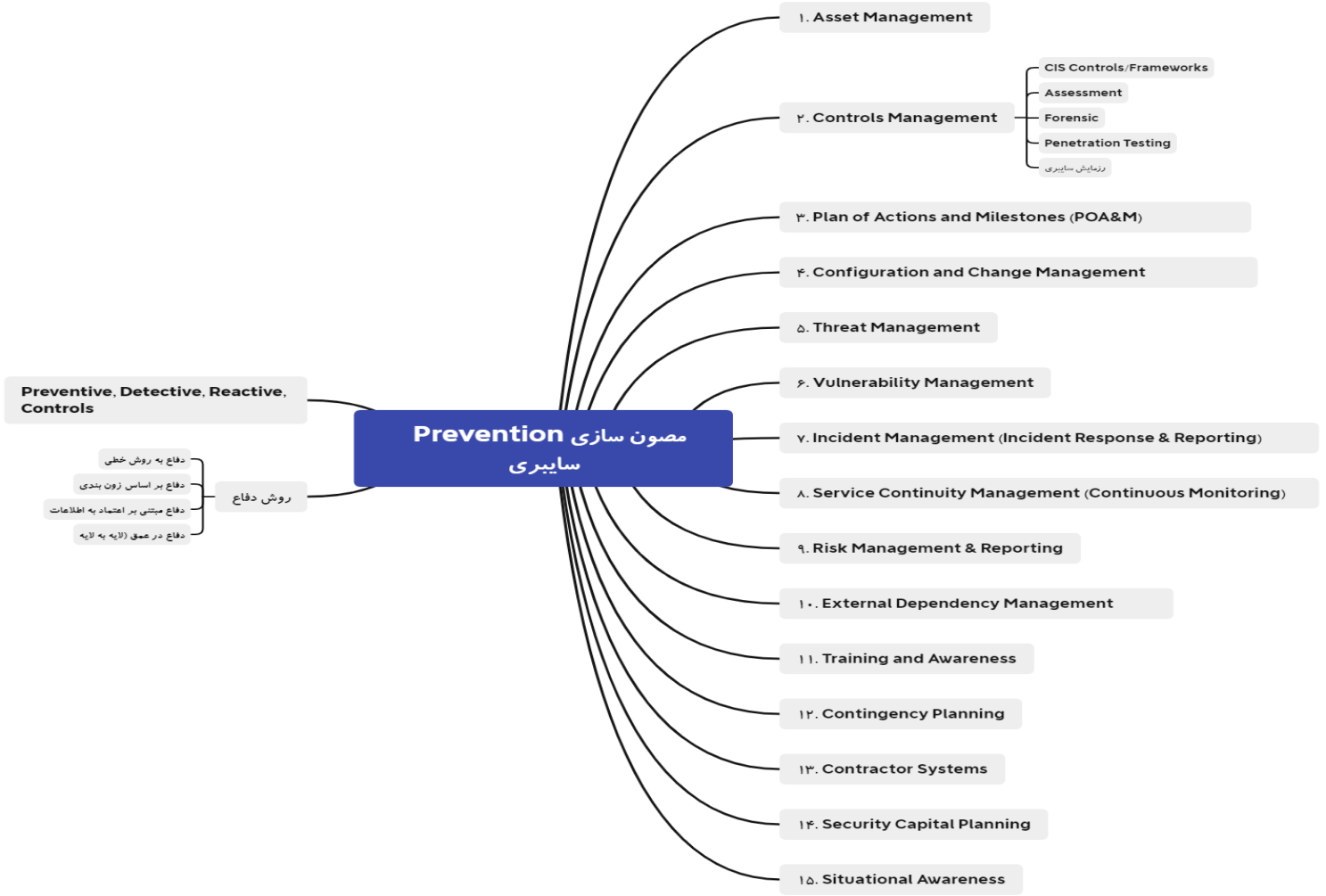


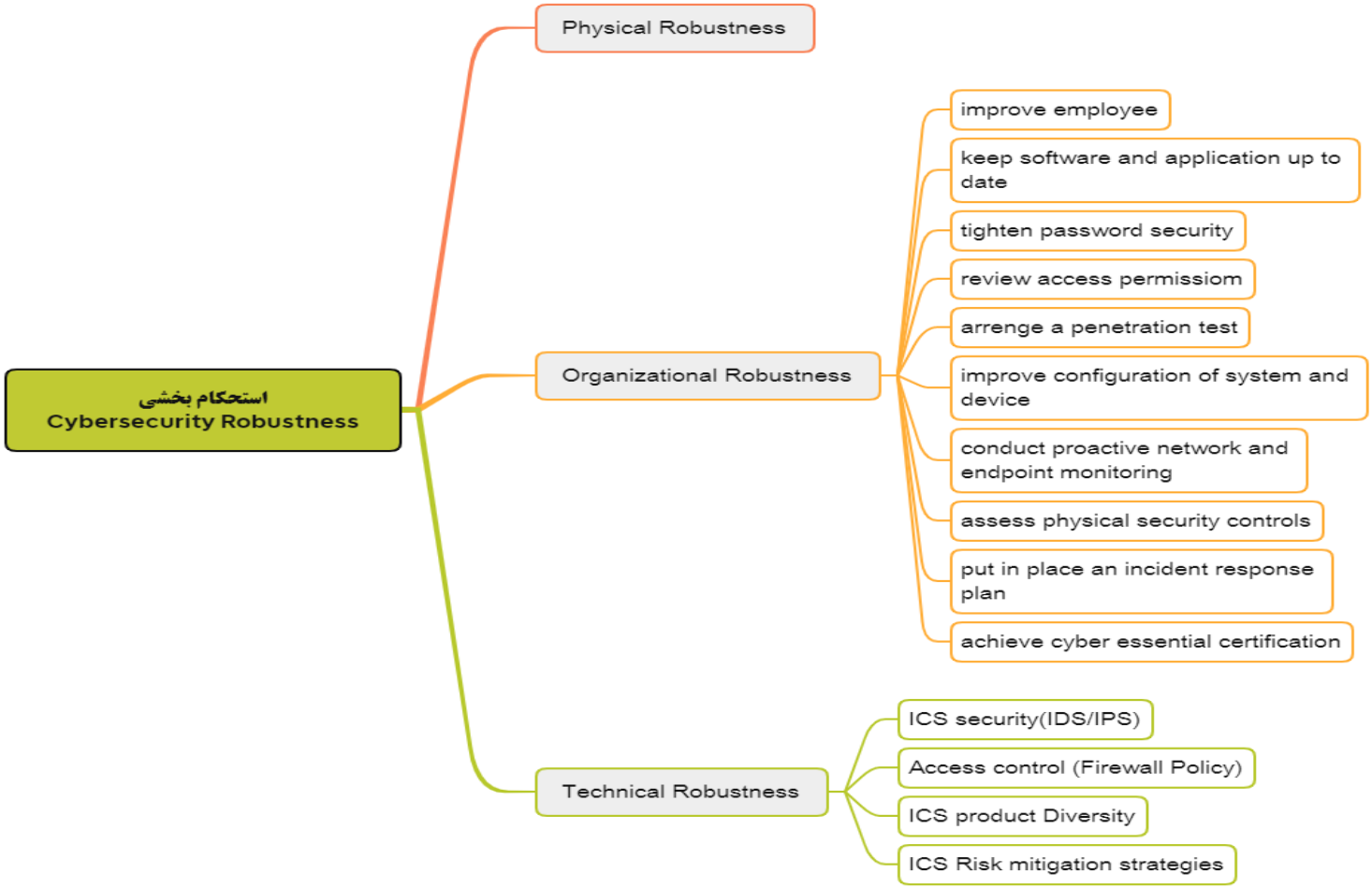


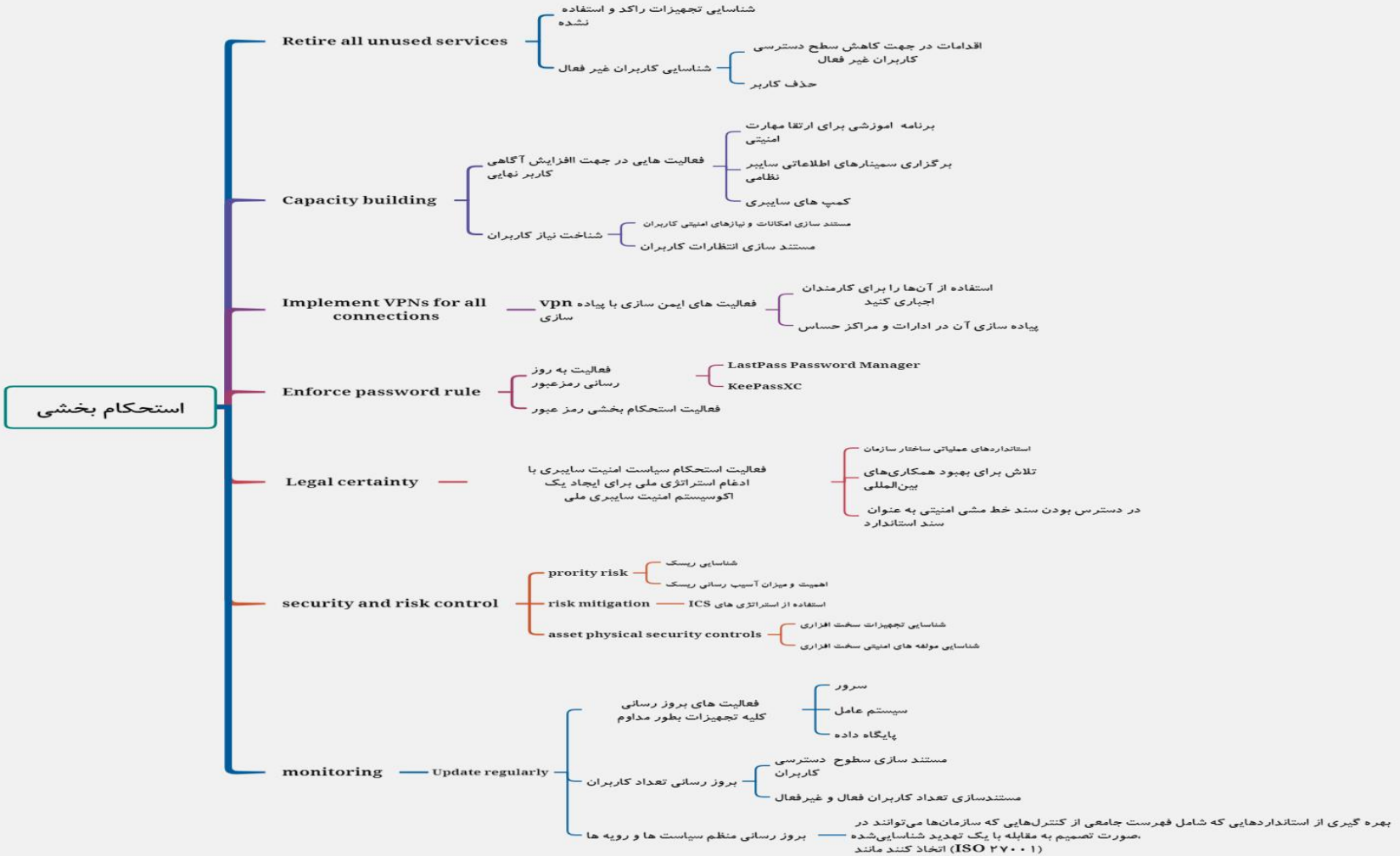


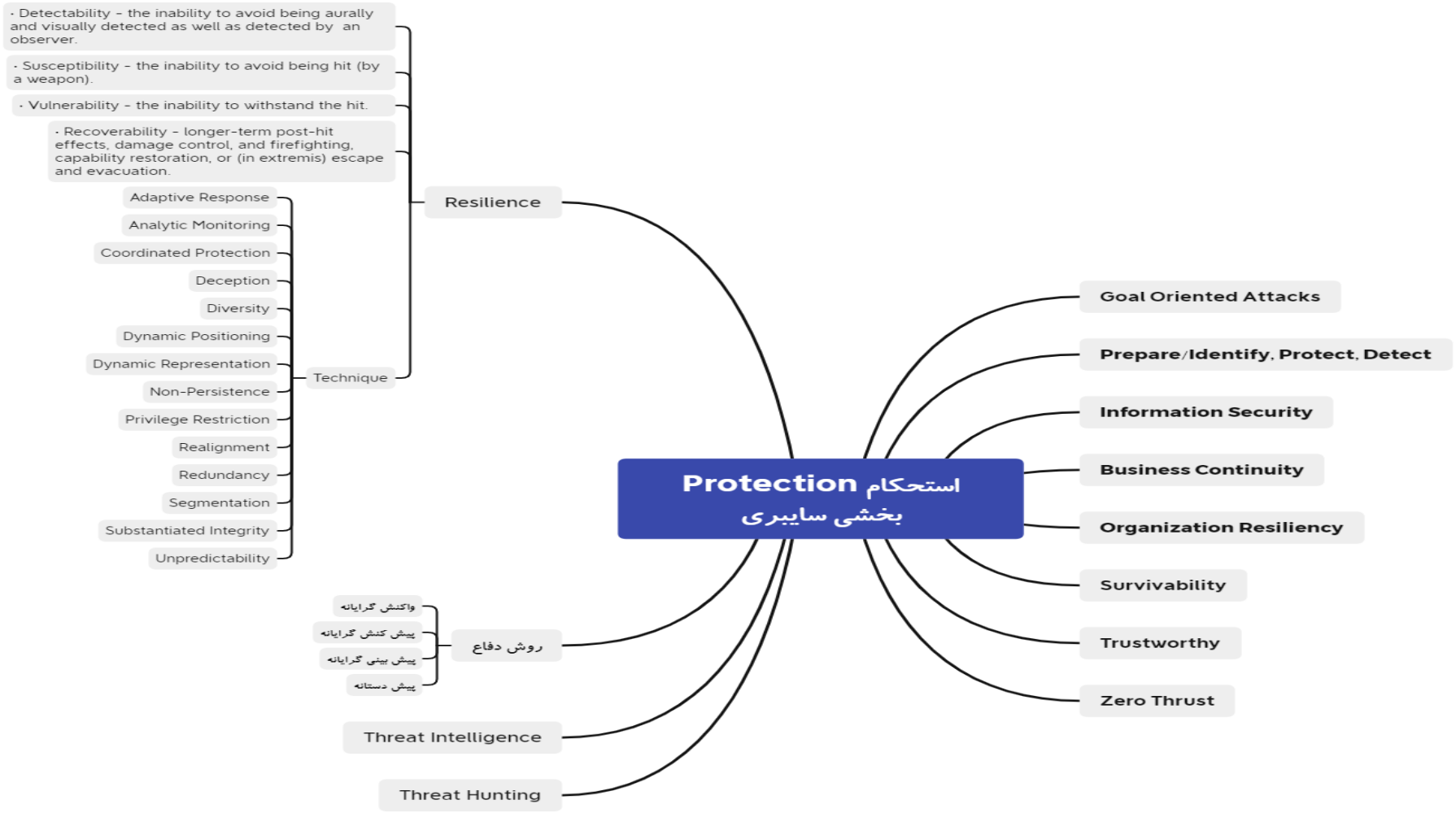

اقدامات
مقاوم سازی
مقاوم سازی سرور
بروز نگه داشتن سیستم عامل سرور
استفاده از رمز عبور های قوی و پیچیده و
توسعه سیاستهای رمز عبور قوی برای
کاربران
قفل کردن حسابهای کاربرانی با ثبت
تعداد معینی تلاش ناموفق برای ورود و حذف
حسابهای غیرضروری
غیر فعال کردن پورتهای یو اس بی در هنگام
بوت
پیاده سازی احراز هویت چندعاملی
AES استفاده از رمزگذاری
برای پنهان کردن و محافظت از اطلاعات حساس
مقاوم سازی نرم افزار
پچ کردن خودکار برنامه ها
استفاده از فایروال
استفاده از آنتی ویروس و برنامه های
کاربردی حفاظت از نرم افزارهای جاسوسی و
بدافزار
استفاده از پردازنده هایی که پشتیبانی
می کنند از
Intel Software Guard Extensions (SGX
استفاده از برنامه هایی مانند
LastPass
برای مدیریت و رمزگذاری گذرواژه برای
بهبود ذخیره سازی ،سازماندهی و حفظ گذرواژه
IPS ایجاد سیستم پیشگیری از نفوذ
IDS یا سیستم تشخیص نفوذ
مقاوم سازی سیستم عامل
حذف درایورهای غیرضروری
رمزگذاری هارد دیسک که سیستم عامل را
ذخیره و میزبانی می کند
فعال کردن و پیکربندی
Secure Boot
احراز هویت و محدود کردن مجوزهای دسترسی
به سیستم
محدود کردن مجوز ایجاد حساب کاربری
مقاوم سازی شبکه
ایمن سازی زیر ساختهای ارتباطی چند سرور و
سیستمهای کامپیوتری در یک شبکه
ایجاد یک سیستم پیشگیری از نفوذ یا
سیستم تشخییص نفوذ مبتنی بر نرم
افزار
پیکربندی مناسب و ایمن سازی فایروالهای
شبکه
ممیزی قوانین شبکه و امتیازات دسترسی
به شبکه
غیر فعال کردن پروتکل های خاص شبکه و
پورت های بلااستفاده
رمزگذتری ترافیک شبکه
مقاوم سازی پایگاه داده
کنترل و محدود کردن امتیازات و دسترسی
کاربران
غیر فعال کردن خدمات و عملکردهای
غیرضروری پایگاه داده
ایمن سازی یا رمزگذاری اطلاعات و منابع
پایگاه داده
بروزرسانی مرتب نرم افزار پایگاه داده
DBMS
قفل کردن حساب کاربری پایگاه داده
در صورت مشاهده فعالیت مشکوک
اجرای سیاستهایی در راستای تعریف رمز
عبور قوی و پیچیده جهت ورود به پایگاه داده


جداسازی سایبری سیستمهای امن
کنترل ارتباط زونها
شناسایی نیازمندیها و نقشه الگوهای ارتباطات
شناسایی ویژگی یکپارچگی اما بارز شبکه که منجربه گروهبندی طبیعی سیستم ها و برنامه هامیشود
الگو های ارتباطی لازم که برای عملکرد مناسب ، سیستم ها و برنامه ها باید پشتیبانی شوند ترکیب کرد
طرحواره آدرس آی پی سازمانی
ایجاد و کنترل دسترسی و مدل های شبکه در نقاط اجرای سیاست های امنیتی ، ممیزی و گزارشگیری وراه حل های نظارت استفاده میشود
مدیریت کنترل دسترسی
پیاده سازی کنترلهای دسترسی
کنترل های فعال مسدود کردن ترافیک شبکه
کنترل های غیر فعال نظارت با مانیتورینگ
شناسایی نقاط کنترل
شناسایی زون ها یا زیر زون هایی که میخواهیم ابزار دقیق تری برای نظارت و هشدار مستقر کنیم
ایجاد زون
بخش بندی شبکه
انزوای کنترل شده نه صرفا جداسازی بدون محدودیت
استفاده از جدا سازی فیزیکی یا منطقی در یک یا چند لایه زیر زون بخش های دیگری از فضای آدرس هستند






استحکام بخشی
Retire all unused services
شناسایی تجهیزات راکد و استفاده نشده
شناسایی کاربران غیر فعال
اقدامات در جهت کاهش سطح دسترسی کاربران غیر فعال
حذف کاربر
Capacity building
فعالیت هایی در جهت اافزایش آگاهی کاربر نهایی
برنامه اموزشی برای ارتقا مهارت امنیتی
برگزاری سمینارهای اطلاعاتی سایبر نظامی
کمپ های سایبری
شناخت نیاز کاربران
مستند سازی امکانات و نیازهای امنیتی کاربران
مستند سازی انتظارات کاربران
Implement VPNs for all connections
vpn فعالیت های ایمن سازی با پیاده سازی
استفاده از آن‌ها را برای کارمندان اجباری کنید
پیاده سازی آن در ادارات و مراکز حساس
Enforce password rule
فعالیت به روز رسانی رمزعبور
LastPass Password Manager
KeePassXC
فعالیت استحکام بخشی رمز عبور
Legal certainty
فعالیت استحکام سیاست امنیت سایبری با ادغام استراتژی ملی برای ایجاد یک اکوسیستم امنیت سایبری ملی
استانداردهای عملیاتی ساختار سازمان
تلاش برای بهبود همکاری‌های بین‌المللی
در دسترس بودن سند خط مشی امنیتی به عنوان سند استاندارد
security and risk control
prority risk
شناسایی ریسک
اهمیت و میزان آسیب رسانی ریسک
risk mitigation
استفاده از استراتژی های ICS
asset physical security controls
شناسایی تجهیزات سخت افزاری
شناسایی مولفه های امنیتی سخت افزاری
monitoring
Update regularly
فعالیت های بروز رسانی کلیه تجهیزات بطور مداوم
سرور
سیستم عامل
پایگاه داده
بروز رسانی تعداد کاربران
مستند سازی سطوح دسترسی کاربران
مستندسازی تعداد کاربران فعال و غیرفعال
بروز رسانی منظم سیاست ها و رویه ها
بهره گیری از استانداردهایی که شامل فهرست جامعی از کنترل‌هایی که سازمان‌ها می‌توانند در صورت تصمیم به مقابله با یک تهدید شناسایی‌شده، اتخاذ کنند مانند (ISO ۲۷۰۰۱)


Protection استحکام
بخشی سایبری
Resilience
· Detectability – the inability to avoid being aurally and visually detected as well as detected by an observer.
· Susceptibility – the inability to avoid being hit (by a weapon).
· Vulnerability – the inability to withstand the hit.
· Recoverability – longer-term post-hit effects, damage control, and firefighting, capability restoration, or (in extremis) escape and evacuation.
Technique
Adaptive Response
Analytic Monitoring
Coordinated Protection
Deception
Diversity
Dynamic Positioning
Dynamic Representation
Non-Persistence
Privilege Restriction
Realignment
Redundancy
Segmentation
Substantiated Integrity
Unpredictability
روش دفاع
واکنش گرایانه
پیش کنش گرایانه
پیش بینی گرایانه
پیش دستانه
Threat Intelligence
Threat Hunting
Goal Oriented Attacks
Prepare/Identify, Protect, Detect
Information Security
Business Continuity
Organization Resiliency
Survivability
Trustworthy
Zero Thrust

فرآیندهای زیرساختی

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

مدیریت آسیب پذیری ها و کاستی ها

Common Vulnerability Scoring System (CVSS)
Common Weakness Scoring System (CWSS)
Caveats:
- Conditions
- Limitations
- Caution

CVDDetails.Com
cve.mitre.org
NVD.NIST.Gov
First.org/cvss/calculator/3.0
Tools.Cisco.Com

ارزیابی امنیتی

Forensic
CyberSec Assessment
CyberSec Evaluation
ASVS 1..4
- Eval 1..7

Pen Test –Black/White/Gray
Internal/External
- CyberSec Exercises
- CyberSec Drills

Continuous Monitoring

تاب آوری سایبری

- Predictive
- Resistive
- Adaptive
- Method:
  - Segregate – جداسازی
  - Hardening – مقاوم سازی
  - Immunity – مصون سازی
  - Strengthening – استحکام بخشی

Mitigation Techniques
- Enterprise
- Mobile
- ICS

ASRR (Attack Surface Reduction Rules)
Security Target (ST)
Organizational Security Policies (OSP)
Security Objectives
Protection Profiles (PPs)
Target of Evaluation (TOE)

تهدیدات درون سازمانی

CyberSec Insider Threat

- **Initial Insider Threats Metrics**
- **Insider Threats Metrics**
- **Misusecases**
- **Abucases**

شناخت علمی آسیب پذیری ها و کاستی ها

Common Platform Enumeration (CPE)
Common Configuration Enumeration (CCE)
Security Content Automation Protocol (SCAP)

- Asset Identification
- Asset Reporting Format (ARF)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
  - Applicability
  - Language
  - Dictionary
  - Name Matching
  - Naming

Open Vulnerability Assessment Language (OVAL)
Open Checklist Interactive Language (OCIL)
Trust Model for Security Automation Data (TMSAD)
Extensible Configuration Checklist Description Format (XCCDF)
Software Identification (SWID)
Software Assurance Metrics and Tool Evaluation (SAMATE)

بهبود مستمر ارزیابی امنیتی

Audits – Internal/ External
Mitigation Techniques
- Enterprise
- Mobile
- ICS

Mitigation
- Policy
- Plan
- Programme
- Process
- Operation

Continuous Monitoring

چارچوب مدیریت ریسک (RMF)

Controls
- Low – 131 controls
- Medium - 177 controls
- High –188 controls

ASRR (Attack Surface Reduction Rules)

Block abuse of exploited vulnerable signed drivers
Block Adobe Reader from creating child processes
Block all Office applications from creating child processes
Block credential stealing from the Windows local security authority subsystem (lsass.exe)
Block executable content from email client and webmail
Block executable files from running unless they meet a prevalence, age, or trusted list criterion
Block execution of potentially obfuscated scripts
Block JavaScript or VBScript from launching downloaded executable content
Block Office applications from creating executable content
Block Office applications from injecting code into other processes
Block Office communication application from creating child processes
Block persistence through WMI event subscription
* File and folder exclusions not supported.
Block process creations originating from PSExec and WMI commands
Block untrusted and unsigned processes that run from USB
Block Win32 API calls from Office macros
Use advanced protection against ransomware

فرآیندهای زیرساختی

سرویس های فضای سایبری

Federal Information Security Management Act (FISMA)

Federal Risk and Authorization Management Program (FedRAMP):

- Marketplace
- Compliance
- Authorized
- **Controls:**
  - **Low-level -125**
  - **Moderate level - 325**
  - **High-level - 421.**

دانش حمله

- ATT&CK
  - 42 Evasion Techniques
- Red Teaming
- Offensive CheatSheets
- Drills
  - Enterprise
  - Mobile
  - ICS

- حل بحران سایبری
- حل مورد سایبری
- تجزیه و تحلیل مورد سایبری

شناخت الگوی حملات

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
Common Attack Pattern Enumeration and Classification (CAPEC)
Cyber Observable eXpression (CybOX™)
Malware Attribute Enumeration and Characterization (MAEC™)
Event Management Automation Protocol (EMAP)
Open Vulnerability Assessment Language (OVAL®)
Incident Object Description and Exchange Format (IODEF)
IETF Managed Incident Lightweight Exchange (MILE)
Making Security Measurable (MSM)

Defense D Models

Deter
Detect
Assess
- Based on Deter/Detect
- تنظیمی-خود

Delay
Deception
Dirty Tricks
Defeat
Deny

Defense Models

- Passive
- ReActive
- Active
- ProActive
- PreEmptive
- PreEmptive ProActive
- Offensive
- PreEmptive ProActive Offensive

Indigenous Defense Models

- Adaptive
- Adaptive Predictive
- Adaptive Resistive

شناخت های قبل حمله

Attack Surface (AS)
Attack Tactic (ATa)
Attack Technique (ATe)
Attack Procedure (ATp)
- Attack CPM (ATi)

Attack Modeled
- STRIDE/DREAD

Attacked Asset (AdA)
Attacked Service (AdS)
Attack Operation (AO)
- Covert
- Overt
- Deceptive
- Cheat/ گول زنی/فتنه انگیزی
- Fraud
- Dirty Tricks
- Deception/فتنه، گمراه سازی
- Seduction/فریبندگی/اغوا/فریب خوردگی

THREAT MODELING

Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.

STRIDE

STRIDE is a threat classification model developed by Microsoft for thinking about computer security threats.[1] It provides a mnemonic for security threats in six categories:

The threat categories are:

Spoofing of user identity

Tampering

Repudiation

Information disclosure (privacy breach or data leak)

Denial of service (D.o.S)

Elevation of privilege

DREAD (RISK ASSESSMENT MODEL)

DREAD is part of a system for risk-assessing computer security threats previously used at Microsoft and currently used by OpenStack and many other corporations[*citation needed*]. It provides a mnemonic for risk rating security threats using five categories.

The categories are:

Damage - how bad would an attack be?

Reproducibility - how easy is it to reproduce the attack?

Exploitability - how much work is it to launch the attack?

Affected users - how many people will be impacted?

Discoverability - how easy is it to discover the threat?

MICROSOFT THREAT MODELING TOOL 2016

Microsoft Threat Modeling Tool 2016 is a tool that helps in finding threats in the design phase of software projects. It's available as a free download from the Microsoft Download Center.

When you start a web application design, it is essential to apply threat modeling; otherwise you will squander resources, time, and money on useless controls that fail to focus on the real threats. There are multiple approaches to threat modeling, as listed below:

- Software centric threat modeling
- Security centric threat modeling
- Asset or risk centric threat modeling

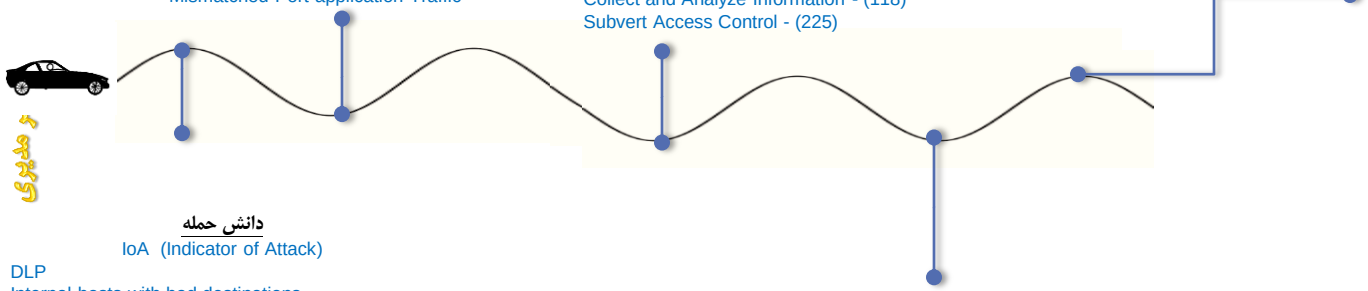
فرآیندهای زیرساختی

دانش نفوذ

IoC (Indicator of Compromise)
CIA
Unusual Outbound Network Traffic
Anomalies in Privileged User Account Activity. ...
Geographical Irregularities
Other Login Red Flags
Swells in Database Read Volume
HTML Response Sizes
Large Numbers of Requests for the Same File. ...
Mismatched Port-application Traffic

Mechanisms of Attack Categories

Engage in Deceptive Interactions - (156)
Abuse Existing Functionality - (210)
Manipulate Data Structures - (255)
Manipulate System Resources - (262)
Inject Unexpected Items - (152)
Employ Probabilistic Techniques - (223)
Manipulate Timing and State - (172)
Collect and Analyze Information - (118)
Subvert Access Control - (225)



دانش حمله

IoA (Indicator of Attack)

DLP
Internal hosts with bad destinations
Internal hosts with non-standard ports
Public Servers/DMZ to Internal hosts
Off-hour Malware Detection
Network scans by internal hosts
Multiple alarm events from a single host
The system is reinfected with malware
Multiple Login from different regions
Internal hosts use much SMTP
Internal hosts many queries to External/Internal DNS

Common Attack Pattern Enumeration and Classification (CAPEC™)

Well-Known Attack Patterns
HTTP Response Splitting (CAPEC-34)
Session Fixation (CAPEC-61)
Cross Site Request Forgery (CAPEC-62)
SQL Injection (CAPEC-66)
Cross-Site Scripting (CAPEC-63)
Buffer Overflow (CAPEC-100)
Clickjacking (CAPEC-103)
Relative Path Traversal (CAPEC-139)

Attack Vector (AV)

APT (Advanced Persistent Threat)
Advanced Evasion Technique (AET) - 42

- ❑ Abuse Elevation Control Mechanism (4)
- ❑ Access Token Manipulation (5)
- ❑ BITS Jobs
- ❑ Build Image on Host
- ❑ Debugger Evasion
- ❑ Deobfuscate/Decode Files or Information
- ❑ Deploy Container
- ❑ Direct Volume Access
- ❑ Domain Policy Modification (2)
- ❑ Execution Guardrails (1)
- ❑ Exploitation for Defense Evasion
- ❑ File and Directory Permissions Modification (2)
- ❑ Hide Artifacts (10)
- ❑ Hijack Execution Flow (12)
- ❑ Impair Defenses (9)
- ❑ Indicator Removal on Host (6)
- ❑ Indirect Command Execution
- ❑ Masquerading (7)
- ❑ Modify Authentication Process (5)
- ❑ Modify Cloud Compute Infrastructure (4)
- ❑ Modify Registry
- ❑ Modify System Image (2)
- ❑ Network Boundary Bridging (1)
- ❑ Obfuscated Files or Information (6)
- ❑ Plist File Modification
- ❑ Pre-OS Boot (5)
- ❑ Process Injection (12)
- ❑ Reflective Code Loading
- ❑ Rogue Domain Controller
- ❑ Rootkit
- ❑ Subvert Trust Controls (6)
- ❑ System Binary Proxy Execution (13)
- ❑ System Script Proxy Execution (1)
- ❑ Template Injection
- ❑ Traffic Signaling (1)
- ❑ Trusted Developer Utilities Proxy Execution (1)
- ❑ Unused/Unsupported Cloud Regions
- ❑ Use Alternate Authentication Material (4)
- ❑ Valid Accounts (4)
- ❑ Virtualization/Sandbox Evasion (3)
- ❑ Weaken Encryption (2)
- ❑ XSL Script Processing

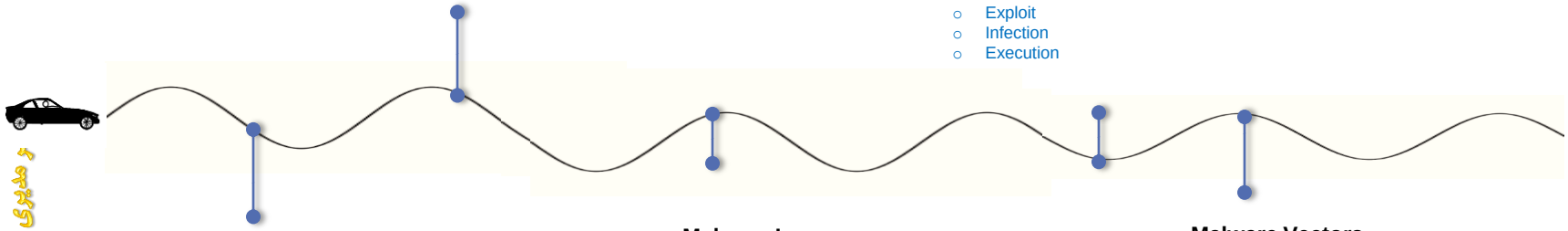
فرآیندهای زیرساختی

مدیریت تهدیدات

Advanced persistent threats (APT)
Advanced Evasion Techniques (AETs)
Threat Info - OSINT, STIX, TAXII
Threat Intelligence
Threat Hunting
Threat Intelligence Information
Threat Intelligence Feeds
Insider threats

Malware Five Stages

- Entry
- Traffic distribution
- Exploit
- Infection
- Execution



شناخت حمله

Attack Strategy (AS)
Attack Policy (APo
Attack Planning (APl)
Attack Programme (APr)
Attack Diligence (AD)
Attack Tactic Diligence (ATad)
Attack Technique Diligence (ATed)
Attack Procedure Diligence (ATpd)
Attack Operation Diligence (AOd)
Attack Report (AR)
Attack Information Intelligence (AII)
Attack Intelligence (AI)

Malware In

In (Malicious) Email Attachments
In (Malicious) Links Sent in Emails
In Traffic Redirects
In Software Downloads
In Online Ads
On (Infected) Websites
In Torrent Downloads

- Meta-info file
- Metadata
  - In Documents.
  - Bot
  - DDoS
  - SPAM
  - Financial fraud
  - Data theft
  - Extortion

Malware Vectors

- Characteristics
- Classification
- Malware Attributes
  - Capabilities
  - Subcapabilities
  - Behaviors
  - Behavior Instances
  - Obfuscation Methods
  - Attributes
- The Malware Behavior Catalog (MBC)

فرآیندهای زیرساختی

بازیابی-بازگرداندن عملیات به وضعیت عادی

استفاده از

Endpoint Detection and Response (EDR)
- Microsoft Defender Advanced Threat Protection (ATP)
- Kaspersky Endpoint Detection and Response (EDR)
- Cynet 360.
- MVISION Endpoint Security.
- Adaptive Defense 360 / WatchGuard EPDR.
- Huntress.
- CrowdSec.
- Cortex XDR.
- Bitdefender GravityZone.

Extended Detection and Response (XDR)
Trusted Automated Exchange of Intelligence Information (TAXII™)
STIX (Structured Threat Information eXpression)
- stix-visualization

OASIS Cyber Threat Intelligence (CTI) TC

فعالیت های بازیابی از حادثه:
- به محض بروز نشانه ها
- دریافت گزارش ها

تیم بازیابی از حادثه:
- بررسی ماهیت
- آگاهی از اتفاقات
- برنامه ریزی
- آماده سازی
- رویاروی با موضوع
- طرح بازیابی از حادثه
- مدیریت اختلال ها در عملیات
- غلبه بر حادثه

Recover – برگشت/بازیابی

Disaster Recovery Plan (DRP)
Recovery Point Objective (RPO)
- **Recovery Consistency Objective (RCO)**
- **Recovery Consistency Characteristics (RCC)**
- **Recovery Object Granularity (ROG)**

Recovery Time Objective (RTO)
- **Maximum Tolerable Period of Disruption (MTPoD)**
- **Maximum Tolerable Downtime (MTD)**
- **Maximum Tolerable Outage (MTO)**
- **Maximum Allowable Outage (MAO)**

Information Retrieval

جستجو اطلاعات در یک سند
جستجو برای خود سند
جستجو برای برای پایگاه داده متنی، عکسی/آوایی و ویدیو
بازیابی خودکار
قابلیت: دسترسی، ذخیره و مدیریت
کمک برای اطلاعات مورد نظر در انبوهی از اطلاعات
ساختار نایافته

Recover – بازیابی

بازیابی – Recover
ترمیم – Restore
بازسازی/دوباره گذاشتن/دوبار سالم کردن/برگرداندن/درمان کردن
بهبود بخشیدن
تعمیر کردن/مرمت کردن
اصلاح کردن/لحال اول برگرداندن
بازیابی بعد از حادثه

حادثه (اختلال در عملکرد):
- **طبیعی (ثاثیر منفی بر محیط عملکرد سازمان، وقایع ناگهانی – سیل، آتش سوزی، زلزله)**
- **انسانی (خطای انسانی – عدم دانش و آگاهی)**
- **تروریسم های سایبری، ویروس ها (دسترسی بر دسترسی پذیری، قابلیت اطمینان**

حوادث = عدم مدیریت موثر مخاطرات باعث گستگی کسب و کار:
- **علل و ریشه ها**
- **طبیعی/فجایع طبیعی**
- **شکست فنی**
- **عمدی/فعالیت های مخرب**
- **خطا/اشتباهات انسانی**

بازیابی از حادثه

فرآیندها/سیاست ها/رویه ها:
- **قابلیت بازیابی عملیات**
- **تداوم عملکردها پس از وقوع حادثه**
- **شرایط اضطراری**
- **حفظ وضعیت اجرایی سازمان**

- **DRP – Minimize Interruption to the Normal Operation:**
  1. Create your disaster recovery contingency planning team
  2. List all names and contact details
  3. Determine a chain of command
  4. Consider your risk assessment
  5. Do you have a 'Plan B'?
  6. Protect your company data
  7. Test, test and test again

Data Recovery

Physical Data Recovery
Logical Data Recovery
Backup = Protect the DB against data loss
Recovery = Reconstruct DB after Data loss
Data Lost
Data Accidentally Deleted
Data Corrupted
Data Inaccessible
Data Recovery Techniques:
- Synchronous
- Replication
- Asynchronous Replication
- Mixed

فرآیندهای زیرساختی

تداوم/استمرار کسب و کار
(Business Continuity Plan)

بعد یا در هنگام بروز فاجعه:

- به مدار برگردانند سرویس های حساس و حیاتی
- بازیابی به سطح عملیاتی قابل قبول

Data loss.
Cyberattacks.
Malware and viruses.
Network & internet disruptions.
Hardware/software failure.
Service Outages
Fire.
Natural disasters.
Severe weather.

اهداف BCP

- ❑ Risk Management processes and procedures to prevent interruptions to mission-critical services
- ❑ How to Operate During Unplanned Event Disruption
- ❑ Organization's System of Procedures To Restore Critical Business Functions in the Event of an Unplanned Disasters

BCP

- ❖ **Resilience**
- ❖ **Recovery**
- ❖ **Contingency**

Metrics:

- ❖ **Recovery Time Objective (RTO)**
- ❖ **Recovery Point Objective (RPO)**

Contingency Planning Steps

- ❑ فهرستی از خطرات تهیه کنید.
- ❑ خطرات را بر اساس شدت و احتمال سنجید خطرات مهم را شناسایی کنید
- ❑ برای بزرگترین خطرات برنامه های اضطراری ایجاد کنید
- ❑ برای طرح اضطراری خود تأییدیه بگیرید ب
- ❑ رنامه های احتمالی خود را توزیع کنید
- ❑ بر برنامه های احتمالی خود نظارت کنید
- ❑ در صورت لزوم برنامه های احتمالی جدید ایجاد کنید

Business Continuity Plan

- ❑ توابع حیاتی کسب و کار
- ❑ بازیابی فضای کاری
- ❑ تاب آوری سایبری
- ❑ پشتیبان گیری، تکرار و بازیابی اطلاعات
- ❑ پرسنل ا
- ❑ رائه دهندگان خدمات شخص ثالث.
- ❑ مخابرات.
- ❑ مدیریت تغییر.
- ❑ ارتباطات و اطلاعیه ها
- ❑ چابکی
- ❑ مدیریت بحران ا
- ❑ رتباطات بحران پ
- ❑ اسخ اضطرار ی
- ❑ IT Disaster Recovery
- ❑ تداوم کسب و کار
- ❑ بازیابی کسب و کار

BCP Phases

Business Continuity Proactive
- ❑ Prevent, Respond and Recover from a disaster

Disaster Recovery Reactive
Mitigation
Avoidance
BCP:
- ❑ Phase 1: Initiation
- ❑ Phase 2: Business Impact Analysis (BIA)
- ❑ Phase 3: Develop Recovery Strategies
- ❑ Phase 4: Implementation
- ❑ Phase 5: Test and Monitor

NIST's 7-Step Contingency Planning Process

- ❑ Develop the contingency planning policy statement.
- ❑ Conduct the business impact analysis (BIA)
- ❑ Identify preventive controls
- ❑ Create contingency strategies
- ❑ Develop an information system contingency plan
- ❑ Ensure plan testing, training, and exercises
- ❑ Ensure plan maintenance

Attack Intend (AI)

- ❑ Reconnaissance Attac — حملات شناسایی
- ❑ Access Attacks — دسترسی به حملات
- ❑ Denial of Service Atta — انکار حمله های سرویسی
- ❑ Snooping — جاسوسی تغییر
- ❑ Modification — ماسکه کردن
- ❑ Masquerading — سرقت اطلاعات
- ❑ Theft of data — خرابکاری تخریب منابع کامپیوتری
- ❑ Sabotage — جرایم سایبری
- ❑ Destruction of compu resources. — جاسوسی
- ❑ Cybercrime — تجاوز
- ❑ Espionage
- ❑ Trespass

بلوک های شبکه های کامپیوتری

2+20Hsec Blocks

شبکه های زیرساخت کامپیوتری

شبکه های محلی کامپیوتری

شبکه محوطه کامپیوتری

شبکه سایت های کامپیوتری

- شبکه دسترسی به شبکه اینترنت
- شبکه سرویس های عمومی DMZ
- شبکه دسترسی راه دور
- شبکه دسترسی راه دور VPN
- شبکه دسترسی به لبه شبکه گستر

شبکه دسترسی به مراکز اقماری

شبکه گسترده اینترانتی

شبکه گسترده اینترنتی

شبکه های بی سیم کامپیوتری

شبکه مرکز دیتا

شبکه تجهیزات مبتنی بر IP

کنترل دسترسی و ....

تجهیزات فعال شبکه

ردیف	نوع تجهیز	تعداد
۱	سرور	
۲	سوئیچ	
۳	روتر	
۴	تجهیزات ذخیره سازی	
۵	تجهیزات تهیه کننده نسخه پشتیبان از اطلاعات	
۷	فایروال	
۸	تجهیزات وایرلس	
۹	مودم	
۱۰	رک	

تجهیزات مور
- انواع فایر
- انواع سوی

این خصوص
- انواع سوی

و براساس نیاز
- انواع سرو
- انواع تجهی

بینی واعلام منا
- سرویس ه

عامل ها وسرو
- انواع تجهی
- تجهیزات

- طرف قرار

اعلام منابع آتی مورد نیاز در

دهای درگیر (غیرسیسکو)

HP Storage و پیش

و پشتیبانی کامل سیستم

وطه

هد شد

جام اقدامات لازم جهت ایجاد

Redundancy و Load Balancing و High Availability بر روی تجهیزات شبکه در هر نقطه ای که کارفرما صلاح بداند اقدام نماید. کلیه عملیات نصب، پیکربندی و کانفیگ، استقرار و رفع مشکلات احتمالی بر عهده طرف قرارداد است.

تخصص ها

مشاور اعلام و اقرار مینماید که دارای تخصص های ذیل میباشد:

- توان مستند سازی تجربه های عملیاتی و فنی
- تسلط کامل به تحلیل وضع موجود شبکه و طراحی وضع نوین در شبکه جهت افزایش کارآیی، اعتماد پذیری، رفع تهدیدات و تاب آوری سایبری
- مسلط به انواع تخصص های موجود در زمینه CCNA,CCNP,CCIE و MCSE
- مسلط به کار و مسلط به ارایه خدمات مشاوره تخصصی و نظارت فنی در زمینه نحوه نگهداری انواع سرورهای HP ، تجهیزات سیسکو (Switch, Router) و انواع فایروالهای بومی و غیر بومی و سخت افزارهای شبکه ای و همچنین مسلط به ارائه راه کارهای لازم در خصوص ارتقاء ، نصب و راه اندازی ، نگهداری و پیکربندی و حل مشکلات احتمالی
- تسلط بردانش روتینگ، سوییچینگ و تجهیزات روتر و سوییچ اعم از نصب ، راه اندازی ، ارتقاء، پیکربندی و حل مشکلات احتمالی
- مسلط به کار با CISCO ISE - CISCO ACS ASA Fire power Next Generation
- آشنایی کامل با شبکه های Wireless، توانایی و تسلط بر پیکربندی، ارتقا، رفع مشکلات و خطاها
- مسلط به انواع Tunnel های شبکه ای و امن
- تسلط کامل به VM Virtualization و آخرین تکنولوژیهای روز مجازی سازی VMWare ESXi
- مسلط به نصب، راه اندازی، پیکربندی و مدیریت و رفع مشکلات انواع تجهیزات و تکنولوژی NAS ,SAN و انواع تجهیزات ذخیره سازی اعم از: HP Storage,Eva,Tape , Emc2 Storage, blue ray, Tape Backup
- مسلط به سیستمهای عامل شبکه اعم از ویندور لینوکس (متن باز: Centos, Ubuntu... و غیره
- تسلط کامل به سیستم عامل ویندوز اعم از کلاینتی و سرورها
- تسلط کامل به سرویسهای شبکه ای اعم از پیکربندی، ارتقاء و حل مشکلات سیستمی و سرویس دهی سامانه ها اعم از اکتیو دایرکتوری، DHCP، DNS، WSUSو NTP
- مسلط به مدیریت بانکهای اطلاعاتی SQL Server، اوراکل، MSsql و بانکهای متن باز
- مسلط به Mail server های Exchange , Qmail, MDaemon و ...

۴۰ تخصص اصلی

دکتر ناصر مدیری

مهارت ها

۳۰ مهارت

- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه نحوه روتینگ، سوییچینگ ، تجهیزات روتر و سوییچ اعم از نصب ، راه اندازی ، ارتقاء، پیکربندی و حل مشکلات احتمالی
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه نحوه نگهداری و پشتیبانی از سرویس CISCO ISE -
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه نحوه نگهداری و پشتیبانی از تجهیزات Wireless، و توانایی ارایه راه حل های لازم در پیکربندی ، ارتقا و رفع مشکلات و خطاهای تجهیزات مورد نظر
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه انواع Tunnel های شبکه ای و امن
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه VM Virtualization و آخرین تکنولوژیهای روز مجازی سازی VMWare ESXiو VMWare Horizon
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه نحوه نصب ، راه اندازی ، پیکربندی و مدیریت و رفع مشکلات احتمالی تجهیزات و تکنولوژی SAN و انواع تجهیزات ذخیره سازی اعم از: HP Storage,Eva,Tape , Emc2 Storage, Tape Backup
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه نصب سیستمهای عامل شبکه اعم از ویندور لینوکس (متن باز: Centos, Ubuntu…) و غیره
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه رفع مشکلات احتمالی سیستم عامل ویندوز اعم از کلاینتی و سرورها
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه سرویسهای شبکه ای اعم از اکتیو دایرکتوری ، DHCP، DNS، WSUSو NTP
- مسلط به ارایه مشاوره تخصصی و نظارت فنی در زمینه راه اندازی ، رفع اشکال و نحوه مدیریت انواع نرم افزار های مانیتورینگ شبکه ای

فرآیندها

مشاوره لازم است آشنایی کامل با فرآیندها، عمل به فرآیندها و تدوین اسناد و گردش کار داشته باشد. فهرست فرآیند ها و بهروش ها بشرح ذیل است:

- فرآیند کمک و پاسخگویی به کاربران
- فرآیند مدیریت رخداد های رایانه ای
  - بکارگیری نرم افزار های مدیریت خرابی
  - ارایه گزارش های دوره ای از وضعیت کل شبکه
  - مقایسه مداوم نوع ها و فعالیت ها و بهره برداری ها از شبکه
  - رصد و پایش مداوم و بی درنگ تهدیدات، مخاطرات و حوادث
  - جمع آوری، مرتب کردن، سامانبندی کردن، منظم کردن اطلاعات
  - تجزیه و تحلیل تهدیدات مزاحمت‌دار و گزیری جهت ارتحصال، درک، استخراج، استنتاج و نتیجه گیری کردن،
- فرآیند مدیریت به روز رسانی (تهیه و تدوین برنامه ها، اقدامات و فعالیت های به روز رسانی سیستم عامل های کلیه تجهیزات فعال)
- فرآیند مدیریت مشکلات
- فرآیند مدیریت تغییرات
- فرآیند ایمن سازی، مقاوم سازی، جداسازی، مصون سازی و استحکام بخشی
- فرآیند مستند سازی و برآورد آسیب پذیری و کاستی ها (ارزش گذاری)
- فرآیند مدیریت کشف و پیدا کردن شهود وقایع سایبری (فارنزیک)
- فرآیند وضعیت شناسی و ادراک وضعیت بحران سایبری

برنامه و بهروش انجام کار

مشاوره لازم است بتواند برنامه های زیر را ارایه نماید:

- مشاوره لازم است بتواند ارایه برنامه برای استقرار CISCO ISC بنمائید.
- مشاوره لازم است بتواند ارایه برنامه برای راه اندازی سرویس IPAM بنمائید.

مشاوره لازم است توان، ارایه و مستند سازی:

- برنامه کلان مرکز بصورت CPM سالانه و برنامه های ماهانه فعالیت های مدیریتی
- تدوین شرح وظایف پرسنل مرکز، شرایط احزار، تدوین مسئولیت ها و وظایف
- کنترل عملکرد پرسنل و ارایه گزارش روزانه، هفتگی و ماهانه از فعالیت های انجام شده توسط پرسنل
- نقشه های شبکه (بروزرسانی)
- پیکربندی های شبکه و تشریح دلایل و جزئیات پیکره بندی ها
- رخدادها
- مشکلات
- روش های کاهش مشکلات
- ارایه گزارشات دوره ها
- ارایه برنامه برای:
- تست نفوذ شبکه
- تست نفوذ بی سیم
- تست نفوذ اپلیکیشن وب
- برگزاری رزمایش سایبری (در شش ماه نخست دو رزمایش برگزار شود)
- مستند سازی کامل شبکه موجود و ارایه مستندات کامل و حرفه ای
- طرح نوین شبکه (معماری، چارچوب، سرویس ها، سامانه ها، ... , Domains, Zones, VLANs) با رویکرد پدافندغیرعامل و تاب آوری مبتنی بر CRA.
- تهیه توصیه نامه و راه کارهای مصون سازی، احصائ آسیب پذیری، مدیریت ریسک و پیامد های حاصله

۱۲

بهروش

مسئولیت ها و وظایف (جاری روزانه)

پاسخگویی، پاسخ دهی و پیگیری نیاز های ذینفان شبکه و همکاری تا رفع مشکل و ارایه راه کارهای اجرایی و عملیاتی به موقع

رصد و پایش وضعیت شبکه:

بکارگیری روش های و تدابیر پیشگیرانه سایبری

بکارگیری روش های و تدابیر محدود سازی رخداد سایبری

ارتباط مستمر با مراکز ماهر، افتا و سازمان پدافندغیرعامل و پیگیری [illegible] روش ها

رصد و پایش روزانه مراکز اطلاع رسانی و هشدار دهی سایبری

اشتراک گذاری اطلاعات تهدیدات اقدامات خصمانه، مخاطرات، خطرات و پیامدها، کاهش ریسک و حوادث ناشی و راه حل های سریع به در زیر ساخت شبکه

هماهنگی، همکاری، ظرفیت سازی، توسعه قابلیت توان مقابله با رخداد ها سایبری

کشف، بهبود تشخیص (تجزیه و تحلیل و طبقه بندی)، کنترل و نظارت، مراقبت، تعقیب فعالیت های تهدیدات کننده و حملات دشمن سایبری

کشف و تشخیص آسیب پذیریهای سایبری (ارزش گذاری و اولویت بندی آسیب پذیری و ایجاد بانک اطلاعاتی آسیب پذیری ها)

هشدار اطلاعاتی، اعلام وضعیت سطح هشدار و آگاهی رسانی (هشدار تعیین وضعیت سایبری)

مدیریت برنامه ریزی، هماهنگی، سازماندهی و هدایت تیم عملیاتی و اقدام و هدایت عملیات سایبری

مسئولیت ها و وظایف (جاری روزانه)

پاسخگویی، پاسخ دهی و پیگیری نیاز های ذینفان شبکه و همکاری تا رفع مشکل و ارایه راه کارهای اجرایی و عملیاتی به موقع

رصد و پایش وضعیت شبکه:

- بکارگیری روش های و تدابیر پیشگیرانه سایبری
- بکارگیری روش های و تدابیر محدود سازی رخداد سایبری
- ارتباط مستمر با مراکز ماهر، افتا و سازمان پدافندغیرعامل پیگیری روش ها
- رصد و پایش روزانه مراکز اطلاع رسانی و هشدار دهی سایبری
- اشتراک گذاری اطلاعات تهدیدات اقدامات خصمانه، مخاطرات، خطرات و پیامدها، کاهش ریسک و حوادث ناشی و راه حل های سریع به در زیر ساخت شبکه
- هماهنگی، همکاری، ظرفیت سازی، توسعه قابلیت توان مقابله با رخداد ها سایبری
- کشف، بهبود تشخیص (تجزیه و تحلیل و طبقه بندی)، کنترل و نظارت، مراقبت، تعقیب فعالیت های تهدیدات کننده و حملات دشمن سایبری
- کشف و تشخیص آسیب پذیریهای سایبری (ارزش گذاری و اولویت بندی آسیب پذیری و ایجاد بانک اطلاعاتی آسیب پذیری ها)
- هشدار اطلاعاتی، اعلام وضعیت سطح هشدار و آگاهی رسانی (هشدار تعیین وضعیت سایبری)
- مدیریت برنامه ریزی، هماهنگی، سازماندهی و هدایت تیم عملیاتی و اقدام و هدایت عملیات سایبری

۱۰ مسولیت

فرآیندهای زیرساختی

Attack Intelligence Info. (AII)

Zero Date

توسعه تکنولوژی

Zero Trust
Zero Trust Security Model
- Zero Trust Architecture-ZTA
- SP 800-207
- •Zero Trust Network Architecture- ZTNA
- National Cyber Intelligence Platform
- Trust Worthy

ISAC
Cyber Situational Awareness
Cyber Alerts
ISAO
Fusion Centers

مرکز ائتلاف تصمیم گیری

مرکز مدیریت فرماندهی و کنترل (مفروک)

Malware Information Sharing Platform (MISP)

- Alert
- Multiple Attribute Decision making
- Multi-Objective Decision Making
  - وش تحلیل سلسله مراتبی (AHP)
- Analytic Hierarchy Process
- Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)

- فرآیند تصمیم گیری
- تصمیمات استراتژیک
- تصمیمات کنترلی مدیریت
- تصمیمات عملیاتی
- روش های تصمیم گیری
- تصمیم‌گیری چندمعیاره (MCDM)
- تصمیم‌گیری چندشاخصه(MADM)
- تصمیم‌گیری چندهدفه(MODM)

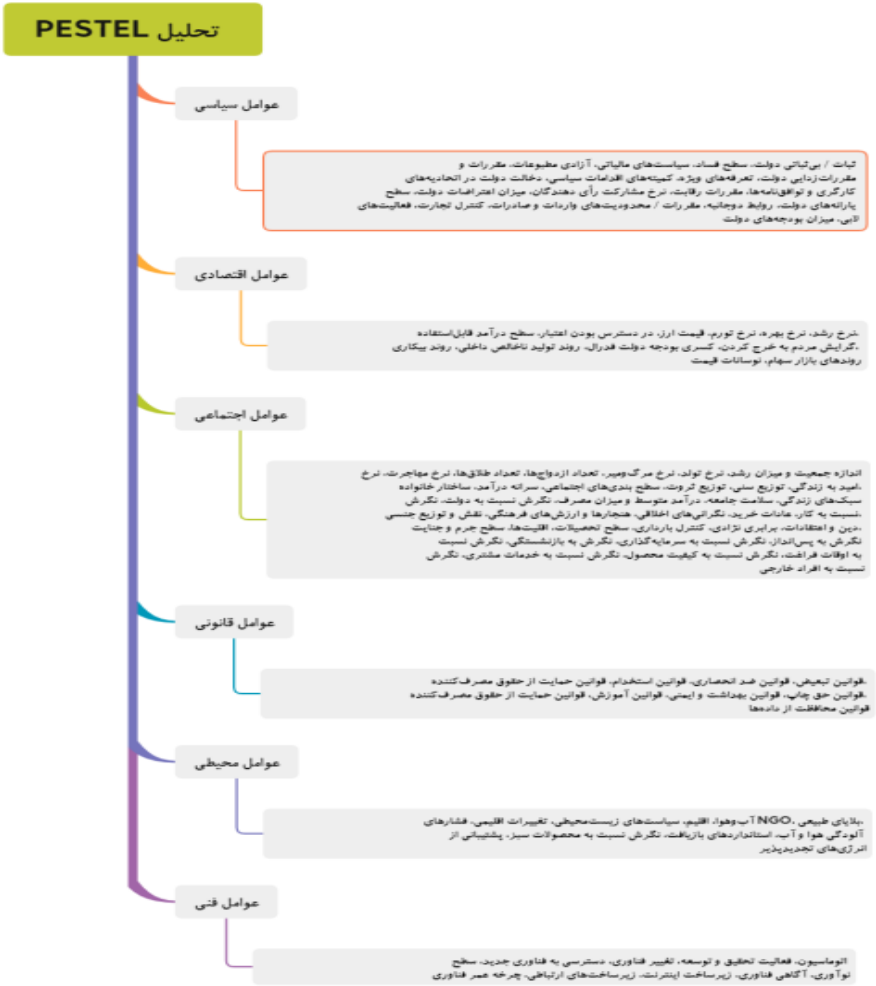
تحلیل PESTEL

- عوامل سیاسی
- عوامل اقتصادی
- عوامل اجتماعی
- عوامل قانونی
- عوامل محیطی
- عوامل فنی

تحلیل PESTEL

- **عوامل سیاسی** – ثبات / بی‌ثباتی دولت، سطح فساد، سیاست‌های مالیاتی، آزادی مطبوعات، مقررات و مقررات‌زدایی دولت، تعرفه‌های ویژه، کمیته‌های اقدامات سیاسی، دخالت دولت در اتحادیه‌های کارگری و توافق‌نامه‌ها، مقررات رقابت، نرخ مشارکت رأی دهندگان، میزان اعتراضات دولت، سطح یارانه‌های دولت، روابط دوجانبه، مقررات / محدودیت‌های واردات و صادرات، کنترل تجارت، فعالیت‌های لابی، میزان بودجه‌های دولت
- **عوامل اقتصادی** – نرخ رشد، نرخ بهره، نرخ تورم، قیمت ارز، در دسترس بودن اعتبار، سطح درآمد قابل‌استفاده، گرایش مردم به خرج کردن، کسری بودجه دولت فدرال، روند تولید ناخالص داخلی، روند بیکاری، روندهای بازار سهام، نوسانات قیمت
- **عوامل اجتماعی** – اندازه جمعیت و میزان رشد، نرخ تولد، نرخ مرگ‌ومیر، تعداد ازدواج‌ها، تعداد طلاق‌ها، نرخ مهاجرت، نرخ امید به زندگی، توزیع سنی، توزیع ثروت، سطح بندی‌های اجتماعی، سرانه درآمد، ساختار خانواده، سبک‌های زندگی، سلامت جامعه، درآمد متوسط و میزان مصرف، نگرش نسبت به دولت، نگرش نسبت به کار، عادات خرید، نگرانی‌های اخلاقی، هنجارها و ارزش‌های فرهنگی، نقش و توزیع جنسی، دین و اعتقادات، برابری نژادی، کنترل بارداری، سطح تحصیلات، اقلیت‌ها، سطح جرم و جنایت، نگرش به پس‌انداز، نگرش نسبت به سرمایه‌گذاری، نگرش به بازنشستگی، نگرش نسبت به اوقات فراغت، نگرش نسبت به کیفیت محصول، نگرش نسبت به خدمات مشتری، نگرش نسبت به افراد خارجی
- **عوامل قانونی** – قوانین تبعیض، قوانین ضد انحصاری، قوانین استخدام، قوانین حمایت از حقوق مصرف‌کننده، قوانین حق چاپ، قوانین بهداشت و ایمنی، قوانین آموزش، قوانین حمایت از حقوق مصرف‌کننده، قوانین محافظت از داده‌ها
- **عوامل محیطی** – آب‌وهوا، اقلیم، سیاست‌های زیست‌محیطی، تغییرات اقلیمی، فشارهای NGO، بلایای طبیعی، آلودگی هوا و آب، استانداردهای بازیافت، نگرش نسبت به محصولات سبز، پشتیبانی از انرژی‌های تجدیدپذیر
- **عوامل فنی** – اتوماسیون، فعالیت تحقیق و توسعه، تغییر فناوری، دسترسی به فناوری جدید، سطح نوآوری، آگاهی فناوری، زیرساخت اینترنت، زیرساخت‌های ارتباطی، چرخه عمر فناوری

تحلیل PESTEL



فرآیند مساله

یک مدل دقیقتر برای مسائل دنیای واقعی پیشنهاد شده است. در مدل مطرح شده هدف نقش مهمی در تعریف مسائل دنیای واقعی ایفا می کند. هدف، ارزش، نیاز، خواسته، منظور، انتها و مقصد (Value, Need, Desire, Purpose, End, or Objective) را بیان می کند.

با یک هدف معین، یک مسأله بصورت نیاز به یک هدف یا شکست در رسیدن به آن هدف تعریف شود. علاوه بر اهداف و مسائل، زبان بر سایر جنبه‌های وضعیت مسأله شامل محدودیتها، دانش و اعمال متعدد احاطه دارد.

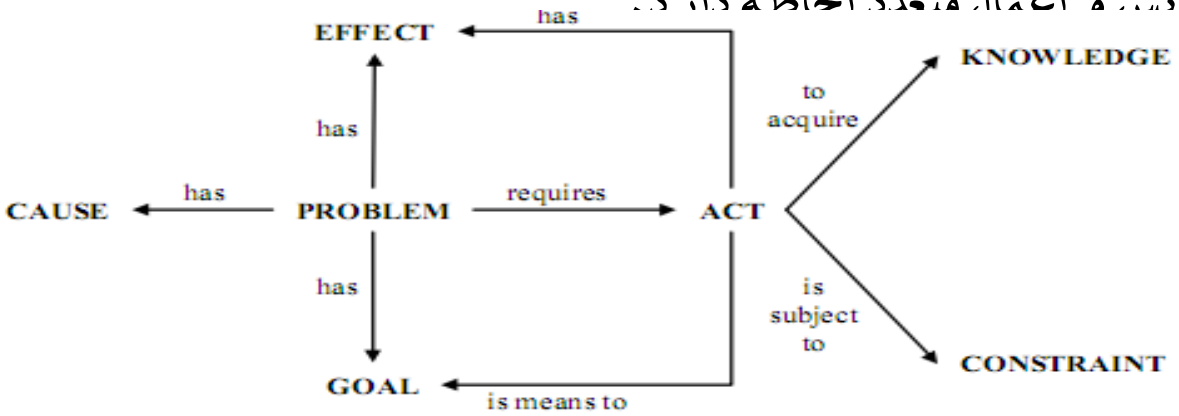
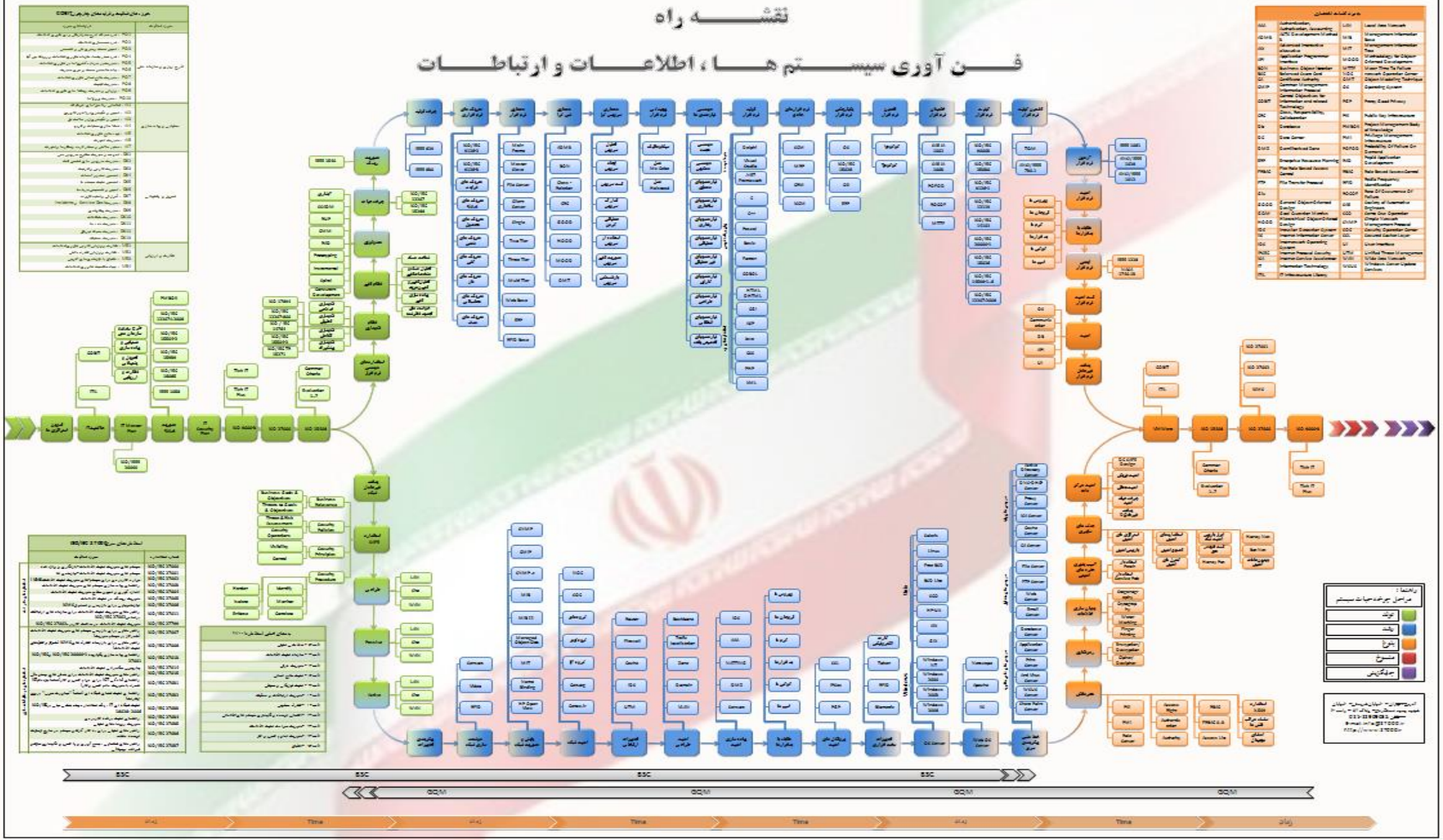
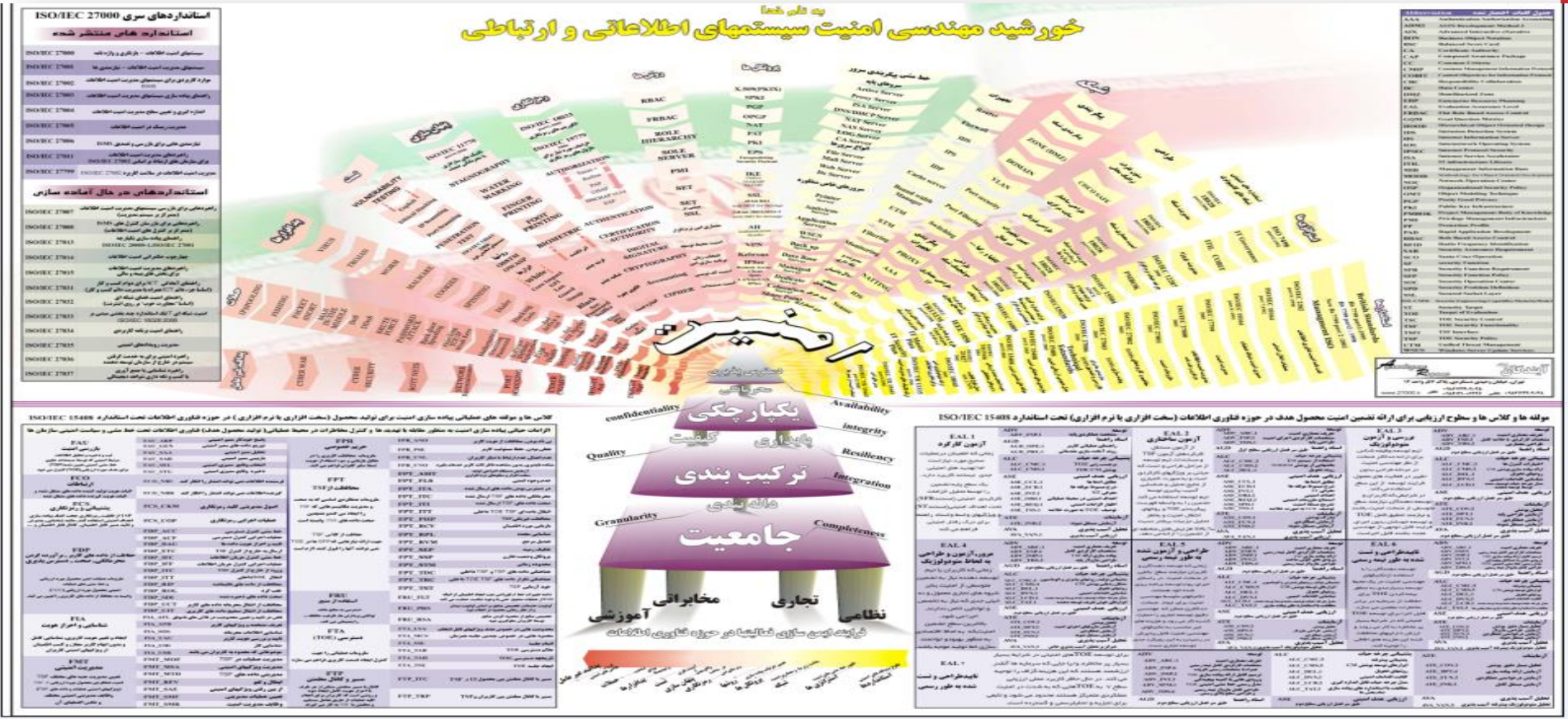
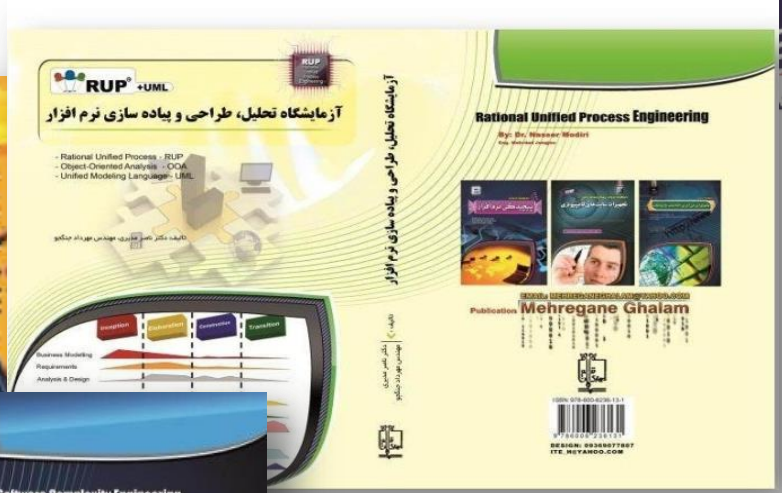


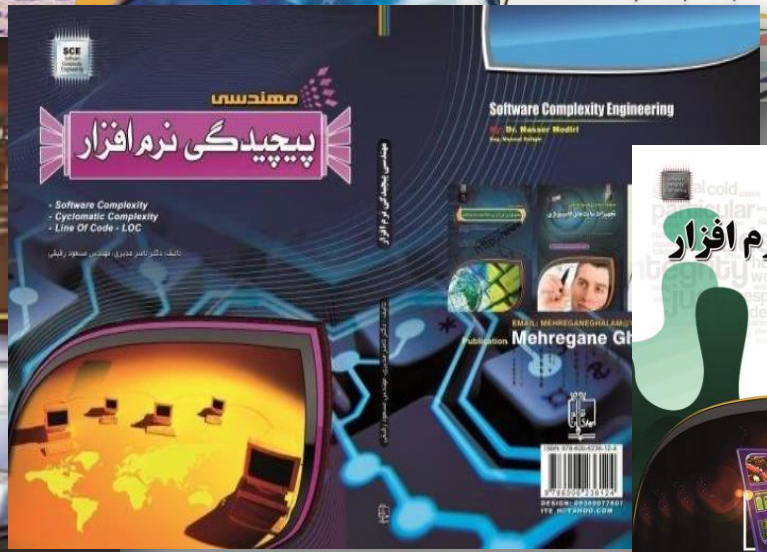
Figure 1.5: Components of problem situations [Smith 1993]


نقشه راه
فن آوری سیستم ها، اطلاعات و ارتباطات

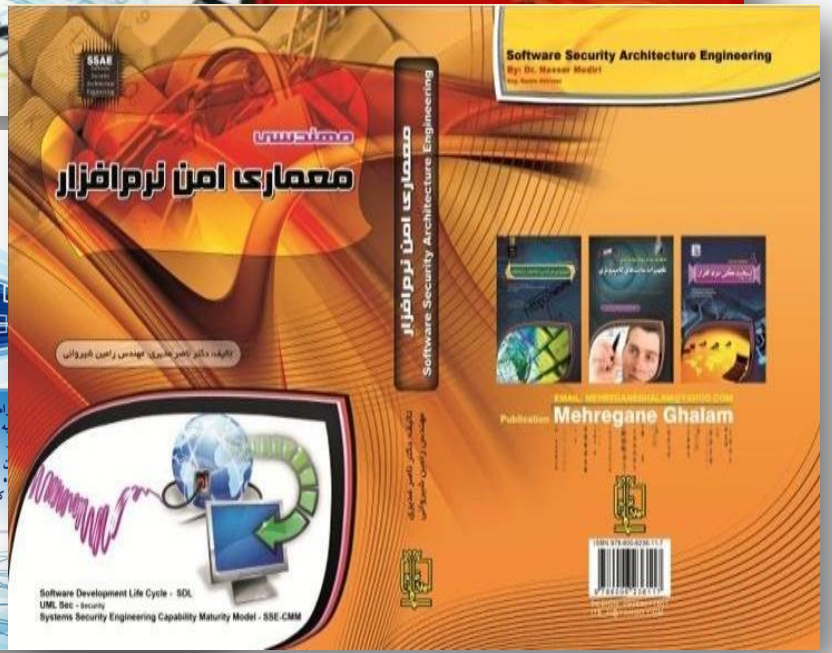
الزامات امنیت



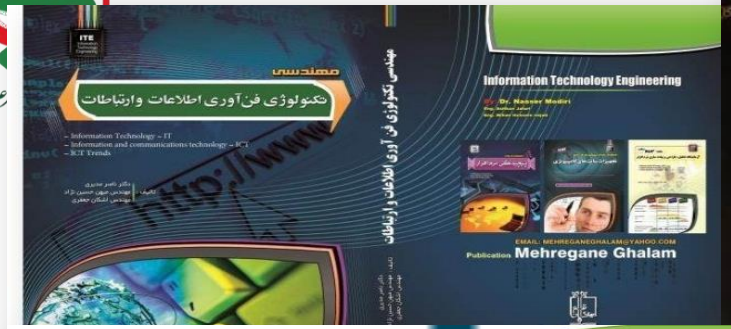




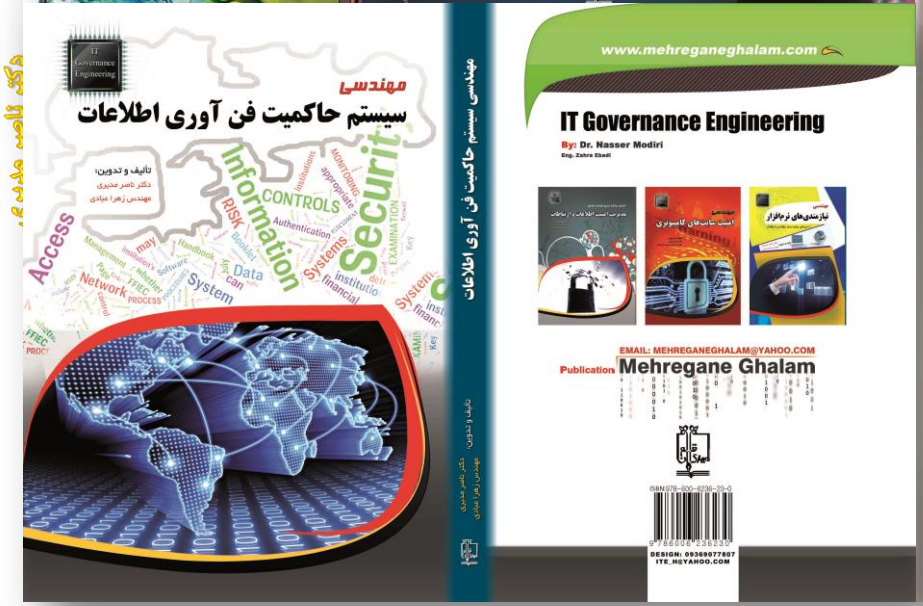
دکتر ناصر مدیری



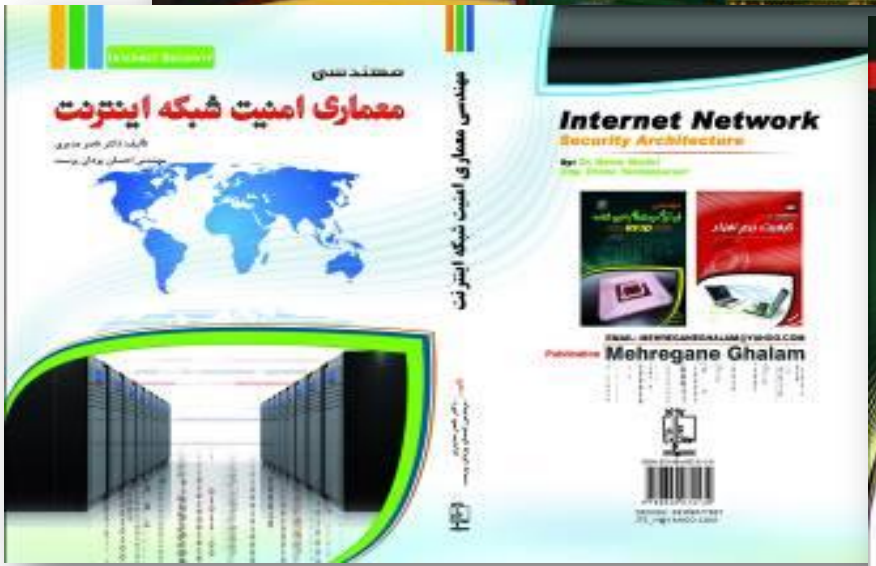
دکتر ناصر مدیری


مهندسی
تکنولوژی فن‌آوری اطلاعات وارتباطات
Information Technology Engineering
Dr. Nasser Modiri
EMAIL: MEHREGANEGHALAM@YAHOO.COM
Publication Mehregane Ghalam

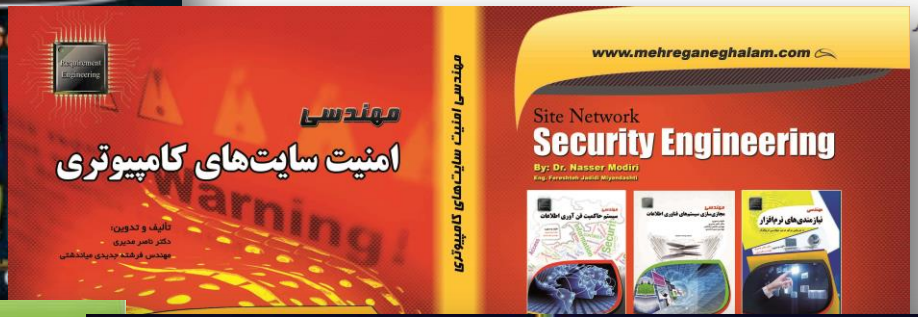

شبکه اینترنت
در ایران و جهان

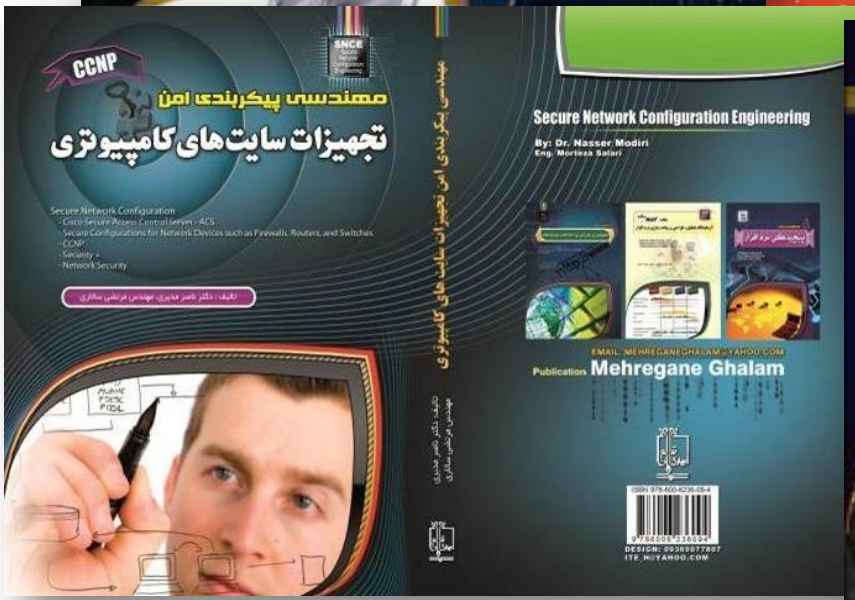

مهندسی
سیستم حاکمیت فن آوری اطلاعات
تالیف و تدوین:
دکتر ناصر مدیری
مهندس زهرا عبادی
مهندسی سیستم حاکمیت فن آوری اطلاعات
www.mehreganeghalam.com
IT Governance Engineering
By: Dr. Nasser Modiri
Eng. Zahra Ebadi
EMAIL: MEHREGANEGHALAM@YAHOO.COM
Publication Mehregane Ghalam

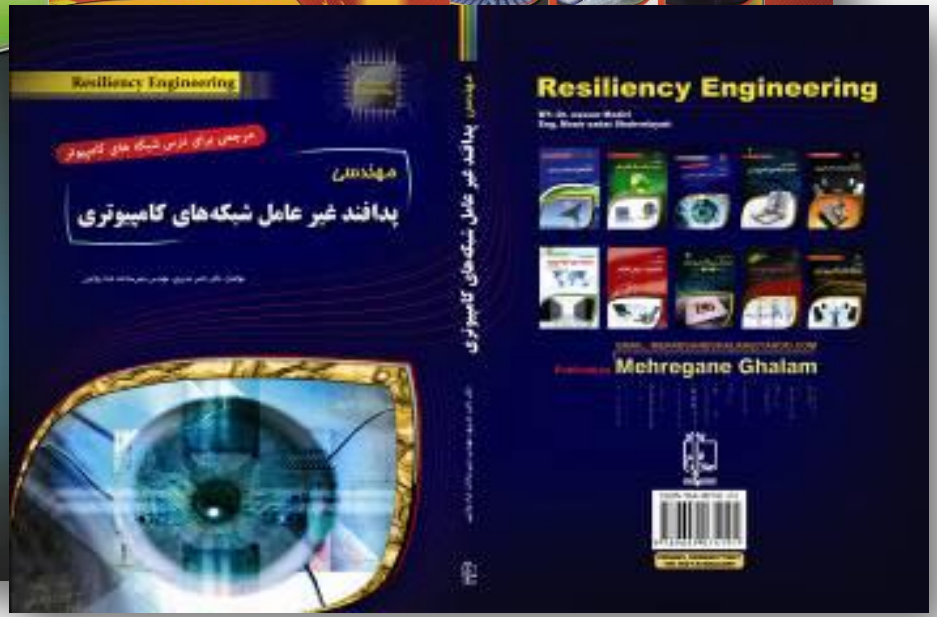

اصول شبکه‌های موردی



دکتر ناصر مدیری



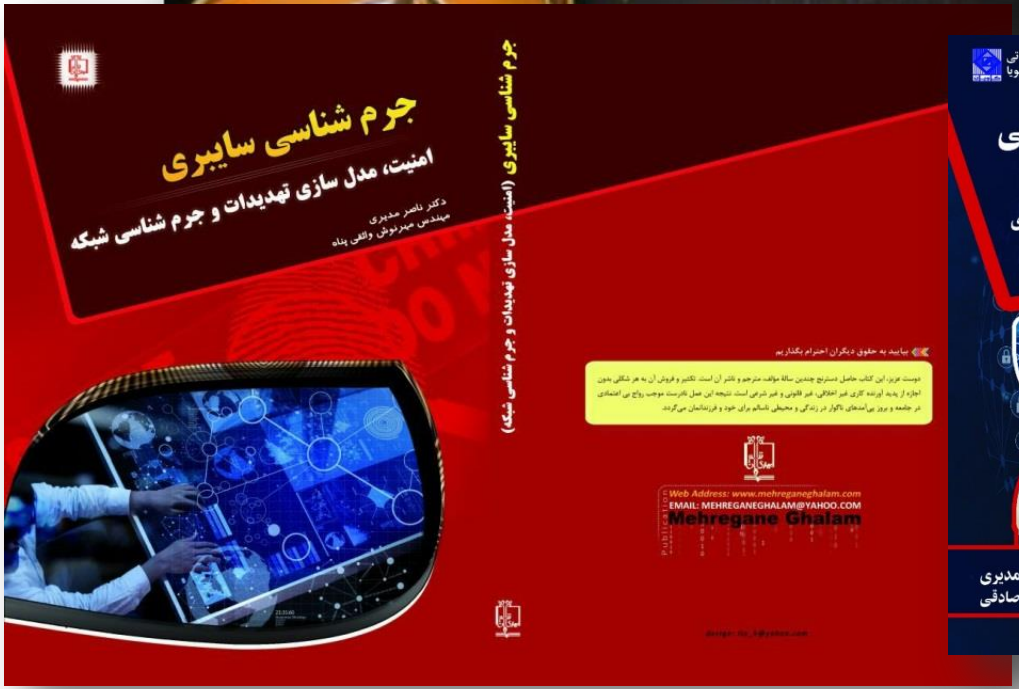




سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

دکتر ناصر مدیری



دکتر ناصر مدیری

دیکشنری
امنیت سایبری
CyberSecurity Dictionary

دیکشنری امنیت سایبری (CyberSecurity Dictionary)

دفاع سایبری
OSINT ISAC CTI
Threat Information ,Threat Intelligence
Preventive Discourage Barrier
Blockade Forbid STIX/TAXII
Threats Hunting ATT&CK
Fusion Centers

بقا سایبری
تداوم کسب و کار

تاب‌آوری سایبری
جداسازی مقاوم‌سازی
مصون‌سازی استحکام بخشی
مدیریت تهدیدها

واکنش،پاسخ سریع و فارنزیک
CERT CSIRT

ارزیابی امنیت
نرم افزار- سخت افزار
سامانه، پروتکل‌های رمز،
پروتکل و رمزنگاری
تست نفوذ و رزمایش

امنیت سایبری
مدیریت ریسک
مدیریت کاستی‌ها
SIEM

ایمن‌سازی
استفاده صحیح، محیط کاری
تندرستی، مغناطیسی و حریق

بازدارندگی و مجازات
Deter Deny
Degrade Disrupt
Defeat

مولفین :
دکتر ناصر مدیری
دکتر یاسمن پولادزاده

سال چاپ ۱۴۰۱

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

دکتر ناصر مدیری


D450B84CA
D55U
PASSWORD


سازمان پدافند غیرعامل کشور
قرارگاه پدافند سایبری کشور
حسین

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

با تشکر از توجه شما

اللهم صل علی محمد و آل محمد