معرفی سامانه بلوغ امنیت سایبری

جهت ارزیابی بلوغ امنیتی سازمان‌ها و زیرساخت
های حیاتی و ارائه راهکارهای مدیریت امنیت

تجربه جهانی: مدیریت

1. رییس جمهور کشور ایالات متحده، در سال 2013 فرمان اجرایی شماره EO 13636، جهت تقویت زیر ساخت‌های حیاتی در برابر حملات سایبری، را به امضاء رساند

2. موسسه NIST در سال 2014 اولین چارچوب محافظت زیرساخت‌های حیاتی از حملات سایبری را ارائه نمود

3. کلیه سازمان‌های دولتی ملزم به شناسایی زیرساخت‌های حیاتی، که می‌توانند توسط حملات سایبری مورد هجوم قرار بگیرند، شدند.

استانداردهای سنتی مدیریت امنیت

- ISMS (ISO/IEC 27001) استاندارد نیازمندی‌های فناوری اطلاعات، فناوری امنیت، سیستم‌های مدیریت امنیت اطلاعات که به طور مشترک توسط موسسه بین‌المللی استاندارد (ISO) و کمیسیون بین‌المللی الکتروتکنیکال (IEC) تدوین شده است.

- چارچوب بهبود امنیت سایبری زیرساخت‌های حیاتی، تدوین شده توسط موسسه ملی استاندارد و تکنولوژی ایالات متحده (NIST Framework).

- دیگر استانداردهای مشهور مدیریت امنیت عبارتند از SOC2، PCI DSS و Info-sec

استانداردهای سنتی مدیریت امنیت

- (ISMS) Information Security Management System
  - یکی از استانداردهای معروف مدیریت امنیت در دنیا
  - خوب است ولی کافی نیست!
- **Why ISO 27001 is not enough?**, BCS: The Chartered Institute for IT, UK, 2009.
  - “compliance or external certification to ISO 27001 does not mean you are secure”
  - “It is perfectly possible to implement an ISO 27001-compliant information security management system (ISMS) without adequately addressing information security”
  - “to actually be secure, it is necessary to develop a culture of valuing information and protecting it”

مشکل کجاست؟

- نفوذهای مکرر در فضای سایبری به سازمان و زیرساخت‌های حیاتی در کشور،
- تجربیات ناموفق و ناتمام در الزام استانداردها و نظام‌های امنیتی مانند ISMS،
- نیاز به درونی شدن امنیت و حاکم شدن فرهنگ امنیت در سازمان،
- نیاز به رویکردی متفاوت به روش‌های امن‌سازی رایج،
- نیاز به نگاهی نو و پیشرفته به امنیت سایبری.

مدل‌های سنتی خوب هستند ولی کافی نیستند

راهکار چیست؟

- امنیت یک فرهنگ است قبل از آنکه یک فناوری باشد
- پیش از آنکه تجهیزاتی خریداری شود یا سرمایه‌گذاری صورت پذیرد؛ می‌بایست راهبرد امنیتی مشخص شود
- امنیت تداوم می‌خواهد زیرا ناامنی تداوم دارد
- بنابراین؛ امن سازی و تفکر امنیت در همه شئون سازمان باید تداوم داشته

مدل بلوغ امنیت سایبری

مدل بلوغ امنیت سایبری

مدل بلوغ

بلوغ:

میزان توانایی یک سازمان برای توسعه دائمی در یک موضوع

مدل بلوغ:

مجموعه‌ای از صفات، ویژگی‌ها، شاخص‌ها و یا الگوها، نشان‌دهنده‌ی قابلیت و پیشرفت در یک نظام خاص

فواید استفاده از مدل بلوغ:

- ارزیابی عملکرد داخلی
- تسریع بهبود عملکرد
- تسریع بهبود در عملکرد زیر بخش های سازمان
- ایجاد و تکمیل یک زبان مشترک بین ذینفعان
- برقراری توازن بین انتظارات و سطح سازمان

مدل بلوغ

بلوغ:

میزان توانایی یک سازمان برای توسعه دائمی در یک موضوع

انواع مدل‌های بلوغ:

- مدل بلوغ پیشرفت (Progression)
- مدل بلوغ قابلیت (Capability)
- مدل بلوغ ترکیبی (Hybrid)

مدل بلوغ پیشرفت: حوزه امنیت

پیشرفت برای "تایید هویت"
تایید هویت چند عاملی
تایید هویت دو عاملی
استفاده از رمز عبور با پیچیدگی بالا
استفاده از رمز عبور اختصاصی
استفاده از رمز عبور مشترک

مدل بلوغ قابلیت

قابلیت برای انجام فعالیت های سازمانی
فعالیت ها به اشتراک گذاشته شده اند
فعالیت ها مدیریت شده اند
فعالیت ها انجام شده اند
فعالیت ها بصورت موردی انجام شده اند
فعالیت ها انجام نشده اند

برخی از مدل‌های بلوغ امنیت

- CERT-RMM
- CERT-CRR
- C2M2
- OISM3
- COBIT 5 for Information Security
- OpenSAMM
- IAMM
- BSIMM
- CySAFE

مدل بلوغ ترکیبی

ترکیب برخی ویژگی‌های مدل‌های بلوغ قابلیت و پیشرفت

- مثال: Cybersecurity Capability Maturity Model

مزایای مدل بلوغ امنیت سایبری

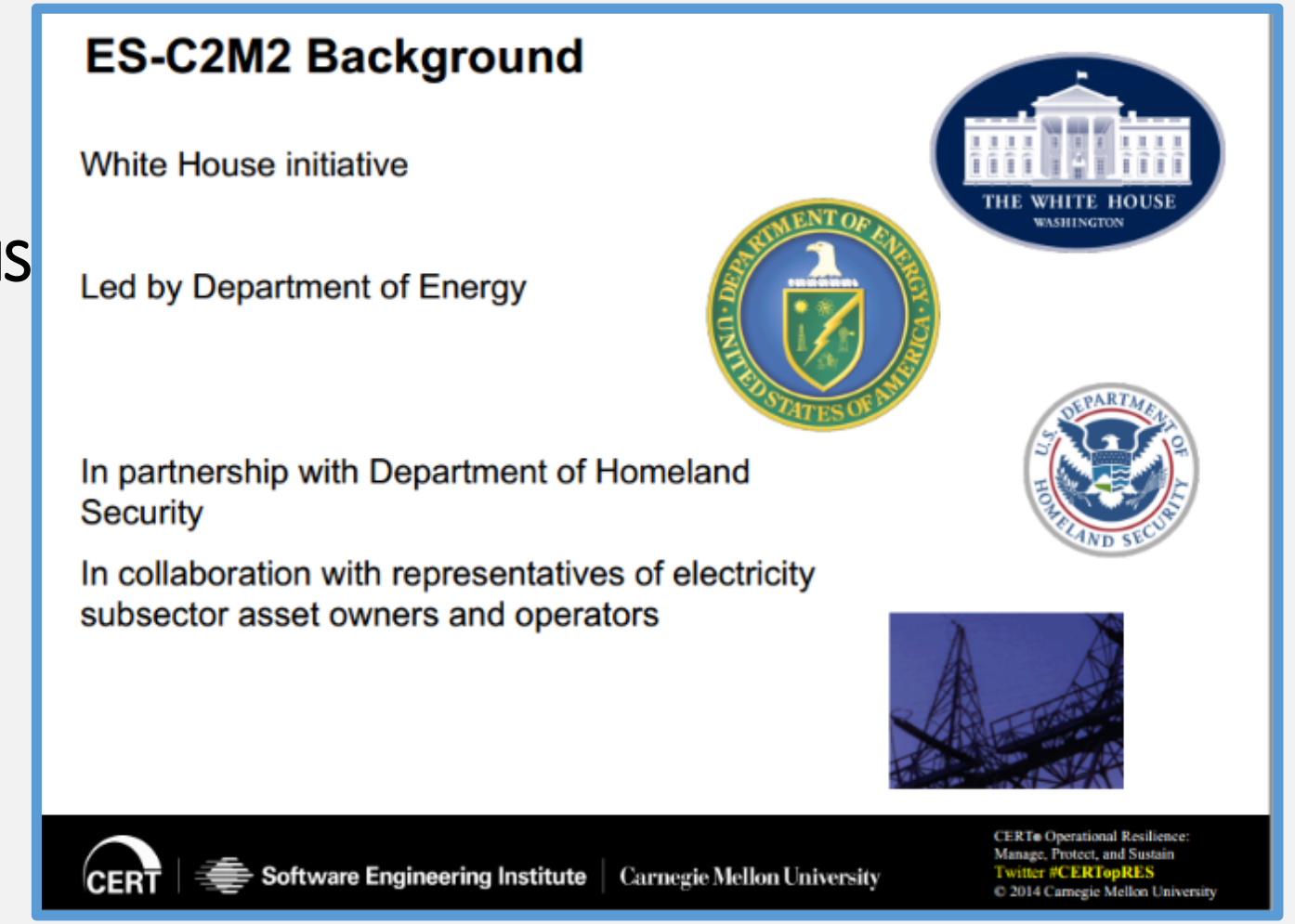
- تقویت امنیت فضای مجازی در سازمان‌ها
- مطابقت با نیازهای امنیتی زیرساخت های حیاتی
- کمک به ارتقاء فرهنگ امنیت سایبری در سازمان
- درونی سازی امنیت در سازمان به عنوان زیربنای فعالیت های امن سازی
- فراهم سازی امکان فعالیت های اولویت بندی شده و سرمایه گذاری بهینه در حوزه امنیت

مدل C2M2

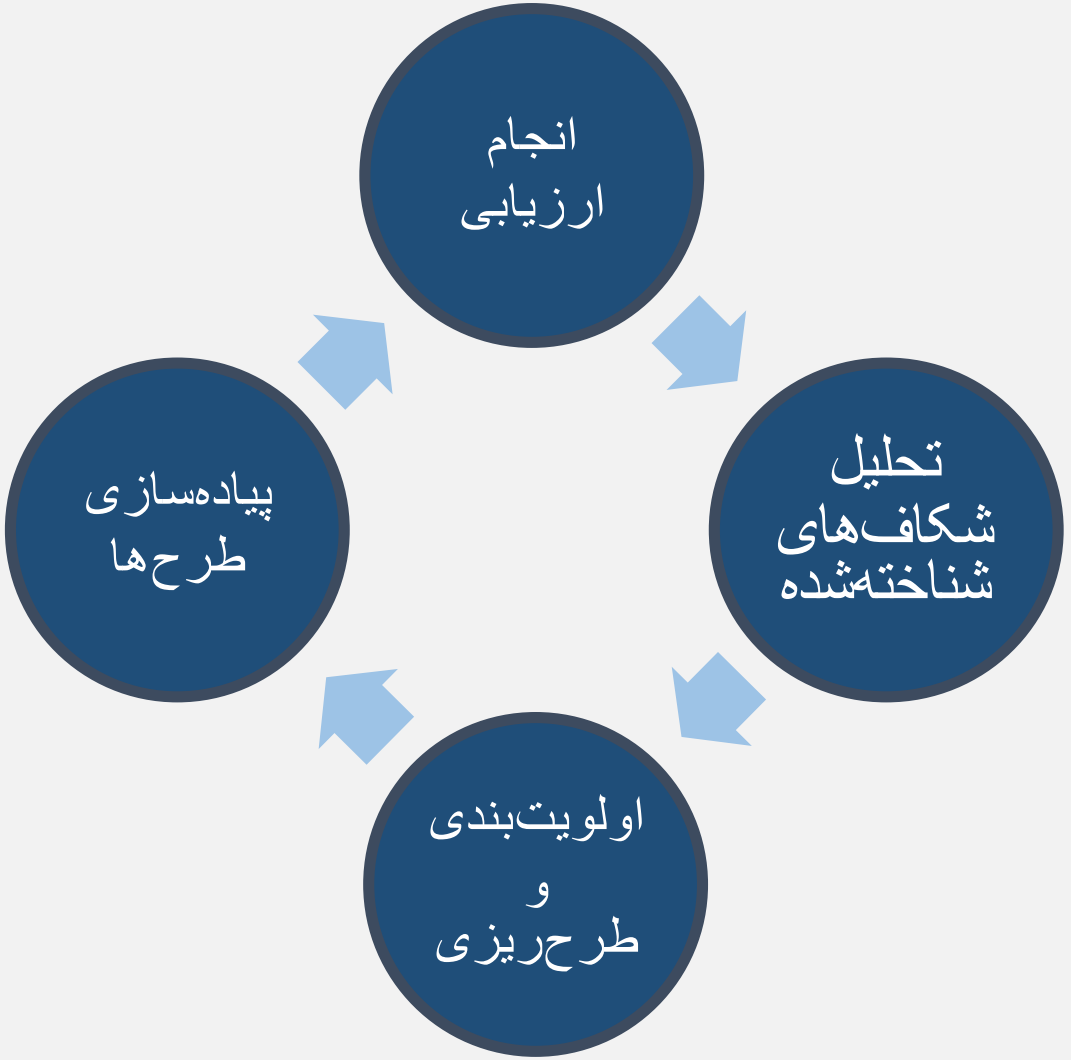
پدید آورندگان C2M2

Initiate by:
The White House
Led by:
U.S. Department of Energy (U.S. DOE)
Partnered with:
U.S. Department of Homeland Security (DHS
Model Architect:
CMU-SEI-CERT

Reference:
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (Case Study), CMU-SEI-CERT, 2014.



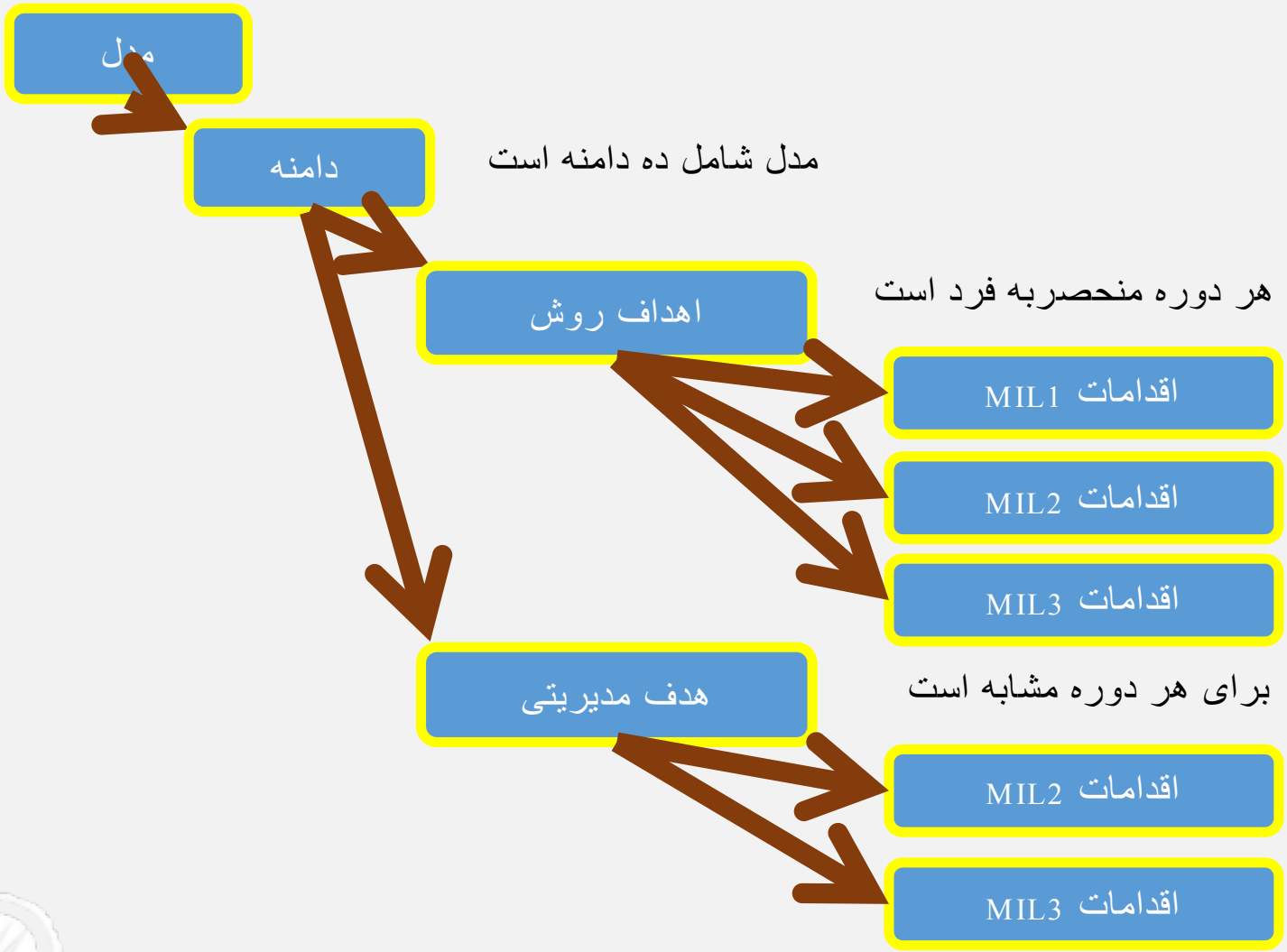
استفاده از مدل



نگاهی جامع به امنیت: 10 دامنه

TVM مدیریت تهدید و آسیب‌پذیری (**Threat** and Vulnerability Management)	IAM مدیریت دسترسی و هویت (Identity and **Access** Management)	ACM مدیریت دارایی، تغییرات و پیکربندی (**Asset**, Change, and Configuration Management)	RM مدیریت مخاطره (**Risk** Management)
EDM مدیریت زنجیره تأمین و وابستگی‌های خارجی (Supply Chain and External **Dependencies** Management)	IR واکنش به رویداد و حادثه، تداوم عملیات (Event and Incident **Response**, Continuity of Operations)	ISC ارتباطات و به اشتراک گذاری اطلاعات (Information **Sharing** and Communications)	SA آگاهی از موقعیت (**Situational** Awareness)
• **دامنه‌ها:** گروه‌بندی منطقی از فعالیت‌های امنیت فضای سایبری		CPM مدیریت برنامه امنیت فضای سایبری (**Cybersecurity** Program Management)	WM مدیریت نیروی کار (**Workforce** Management)

معماری مدل بلوغ



مدل شامل ده دامنه است

برای هر دوره منحصربه فرد است

اهداف روش توسط پیشرفت در فعالیت های منحصر به دامنه، پشتیبانی می شوند.

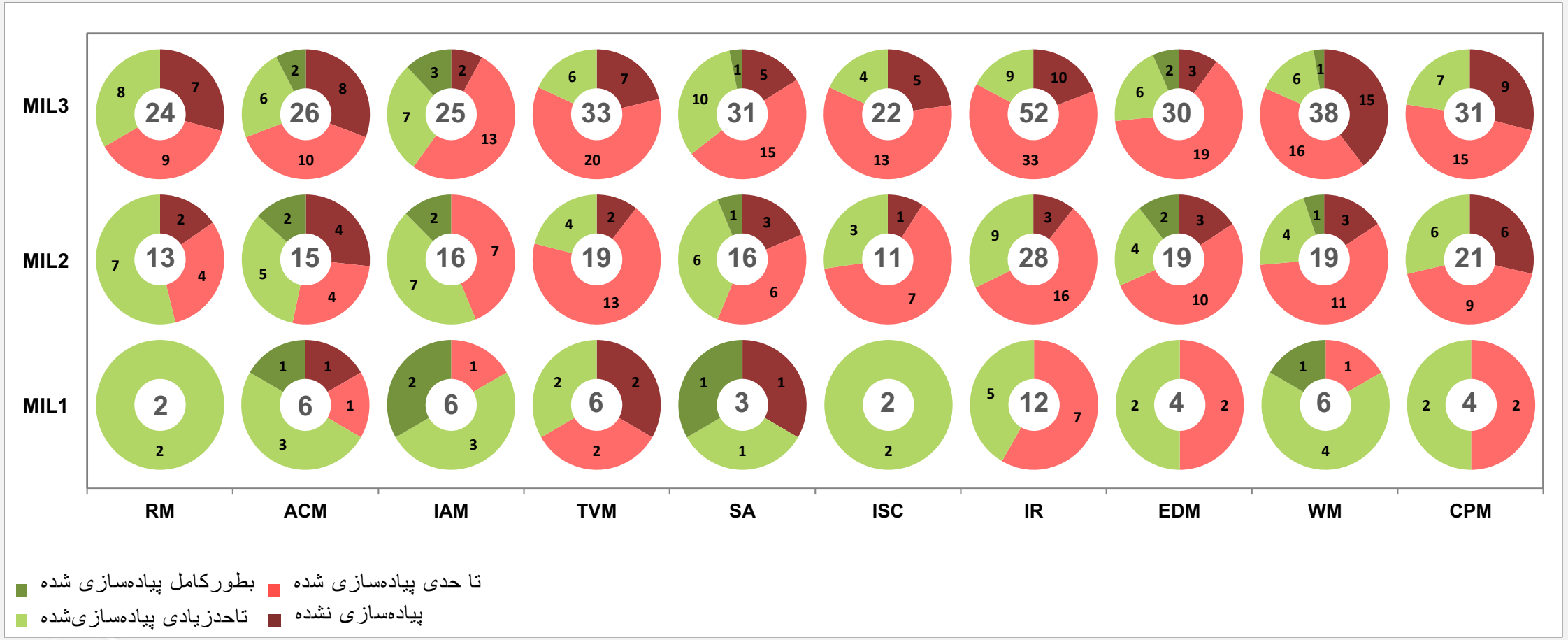
برای هر دوره مشابه است

هر هدف مدیریتی توسط پیشرفت در فعالیت های مشابه در هر دامنه پشتیبانی شده و فعالیت های نهادینه سازی را توضیح می دهد.

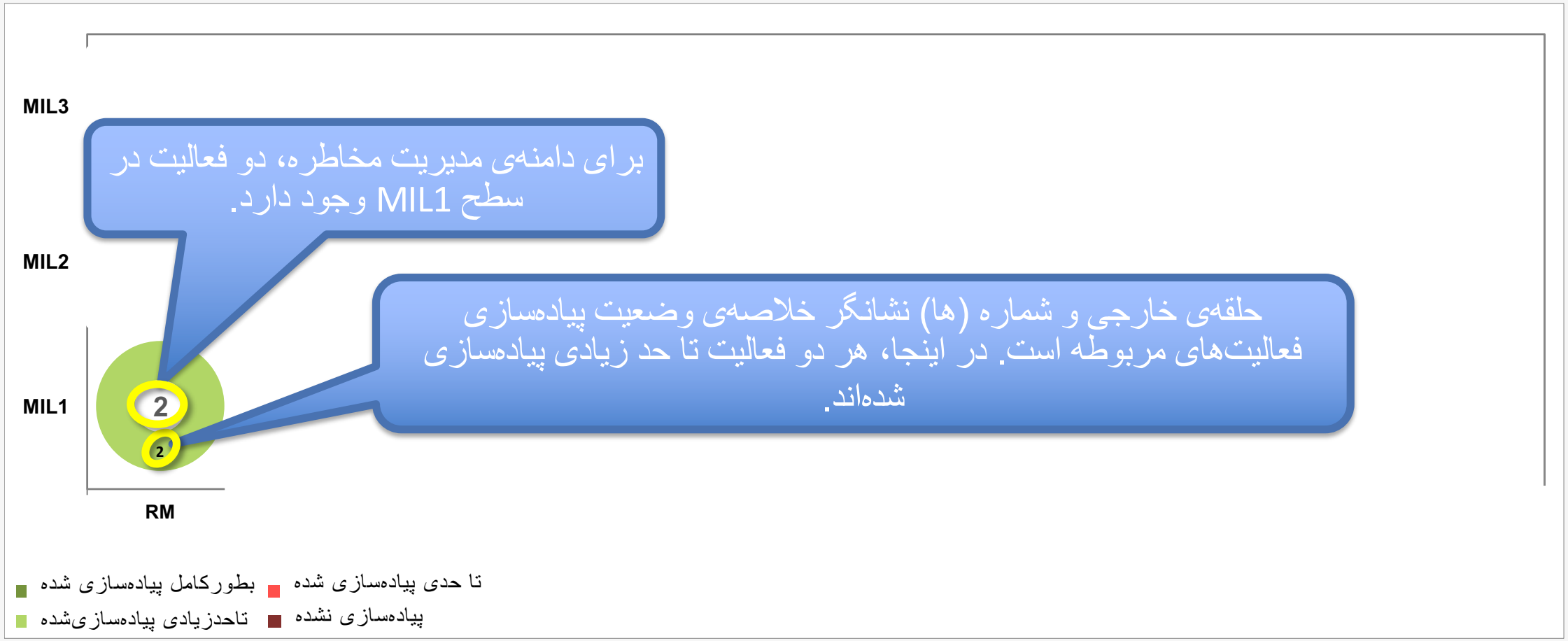
توضیحات سطوح شاخص بلوغ

سطح بلوغ	عنوان	توضیح
MIL0	انجام نشده	– فعالیت‌ها انجام نشده‌اند.
MIL1	آغاز شده	– فعالیت‌های اولیه انجام شده‌اند اما ممکن است بصورت موردی باشند.
MIL2	انجام شده	– فعالیت‌ها مستندسازی شده‌اند. – افراد ذیربط شناسایی شده و با پروژه درگیر شده‌اند. – منابع لازم برای پیشرفت پروسه تأمین شده‌اند. – استانداردها و راهنمایی‌ها برای هدایت مسیر پیاده‌سازی استفاده شده‌اند.
MIL3	مدیریت شده	– فعالیت‌ها به وسیله سیاست‌ها راهنمایی شده‌اند. – فعالیت‌ها به صورت منظم و دوره‌ای برای تطبیق با سیاست‌ها بررسی می‌شوند. – مسئولیت و اختیار لازم به پرسنل مناسب واگذار می‌شود. – در این مرحله تکنیک ها پیشرفته‌تر و کامل‌تر از MIL2 هستند.

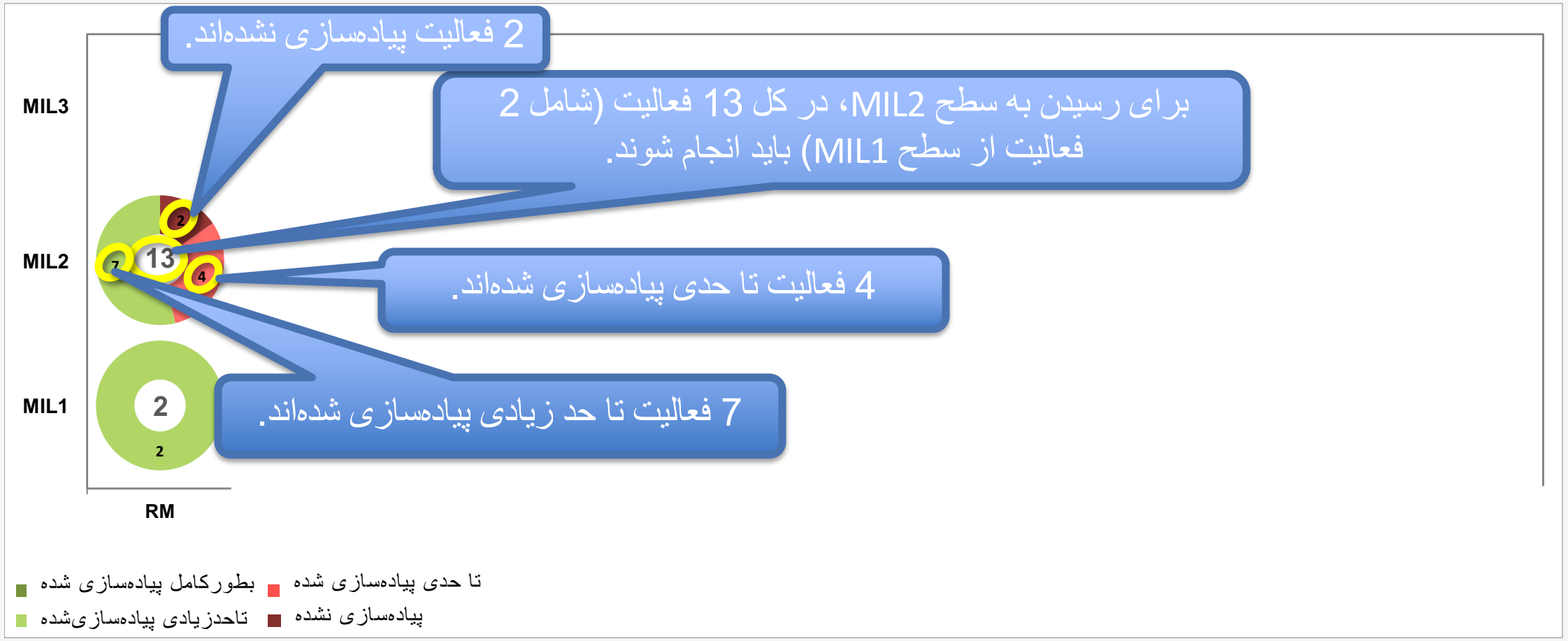
داشبورد امنیت سایبری



داشبورد امنیت سایبری



داشبورد امنیت سایبری



سامانه پایش و ارزیابی بلوغ امنیت سایبری

مزایای سامانه پایش و ارزیابی امنیت سایبری شرکت فراکنش

نمایش جامع، یکپارچه و کلان وضعیت امنیت مبتنی بر بلوغ امنیتی

مشاهده گزارش از بلوغ پیشرفت و قابلیت امنیت سایبری سازمان

داشبورد وضعیت امنیت سایبری جهت مدیران عالی سازمان

دسترسی دائمی به داده های اولیه، پردازش شده و گزارشات متنوع

امکان مقایسه امنیتی واحدهای مختلف سازمان

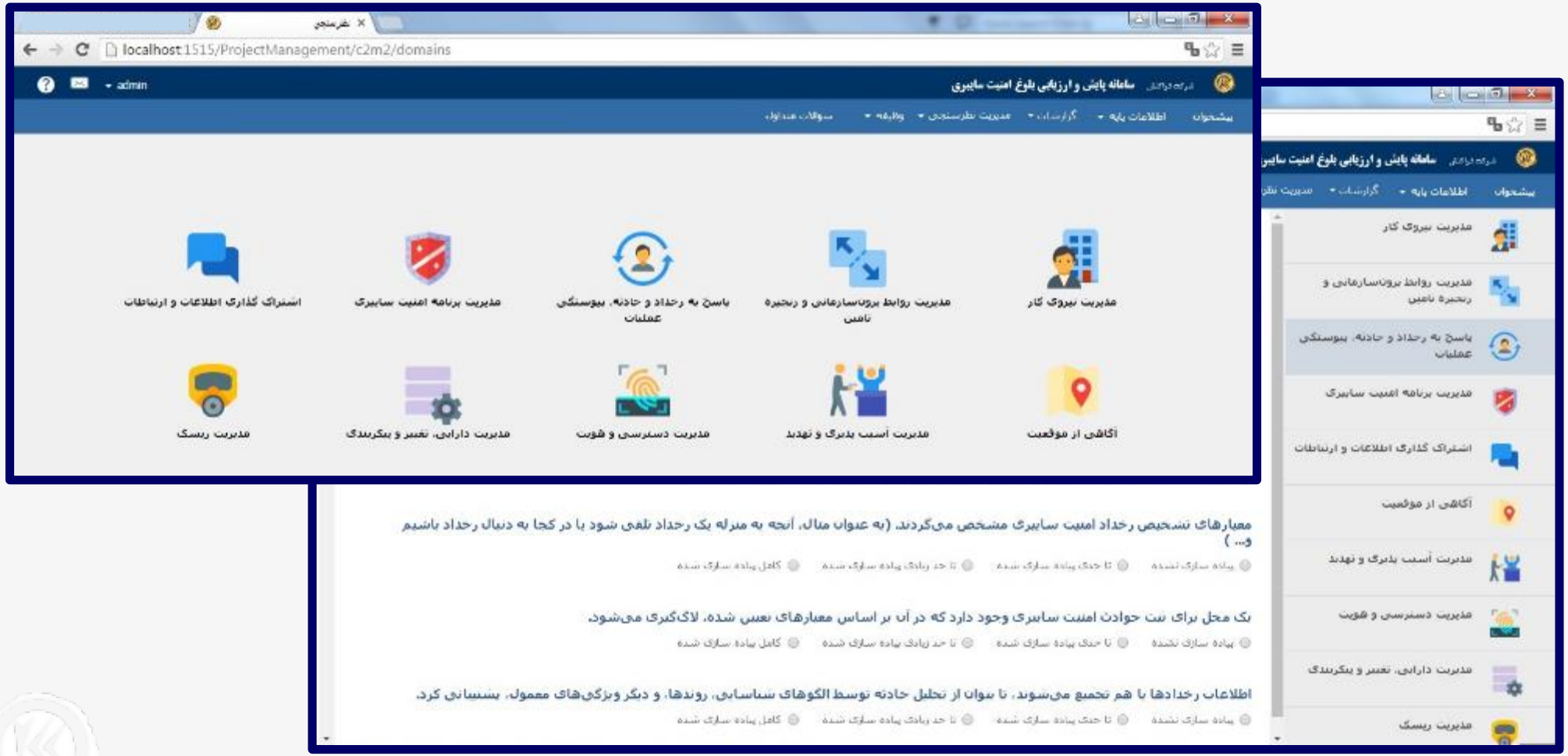
ارزیابی مستمر و جمع آوری سیستماتیک اطلاعات از وضعیت امنیت سایبری

سایرمزایای سامانه

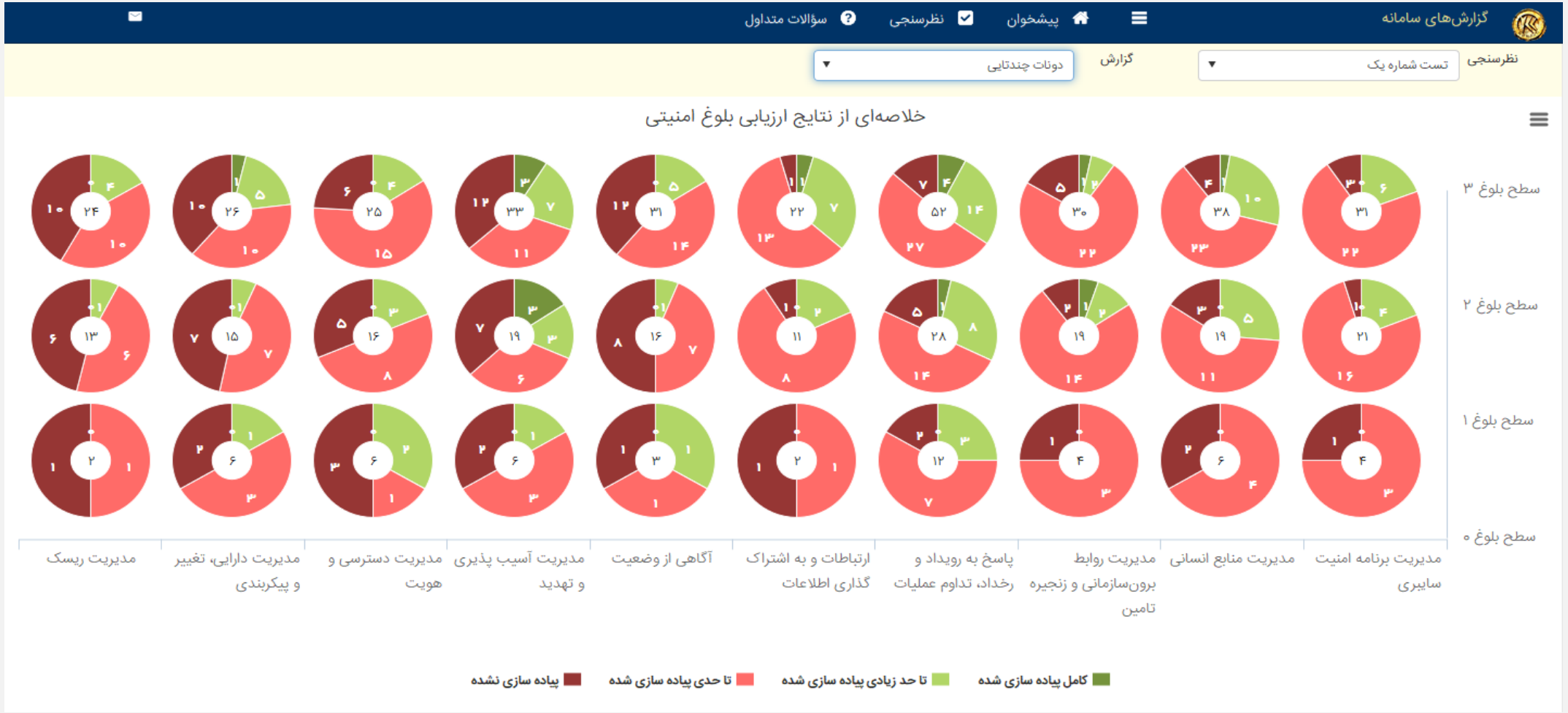
- قابلیت ارزیابی در سطح گسترده در یک سازمان یا گروهی از سازمان‌ها
- ارزیابی با امکان حذف پاسخ‌های غیرنرمال
- تشخیص پاسخ‌دهنده‌هایی که بدون توجه به مفهوم سئوالات صرفا بدنبال پر کردن فرم‌ها هستند
- امکان objective نمودن برخی سئوالات subjective

ساختار سامانه پایش و ارزیابی امنیت سایبری شرکت فراکنش

سامانه پایش و ارزیابی بلوغ امنیت سایبری فراکنش



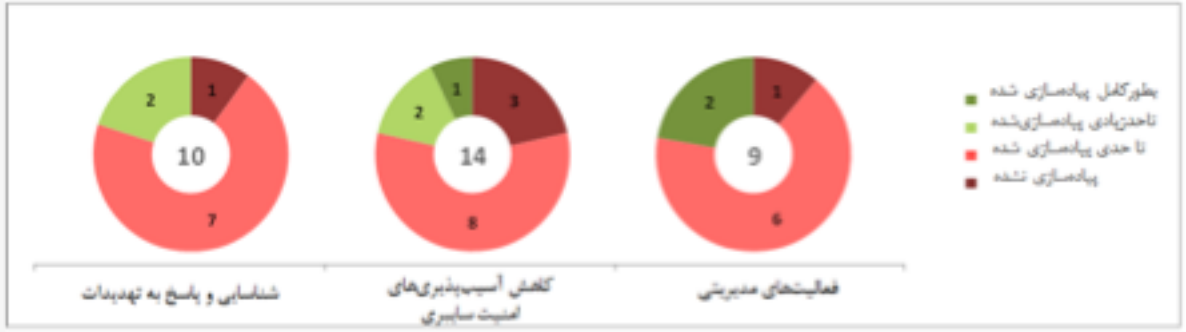
گزارش‌های متنوع مدیریتی



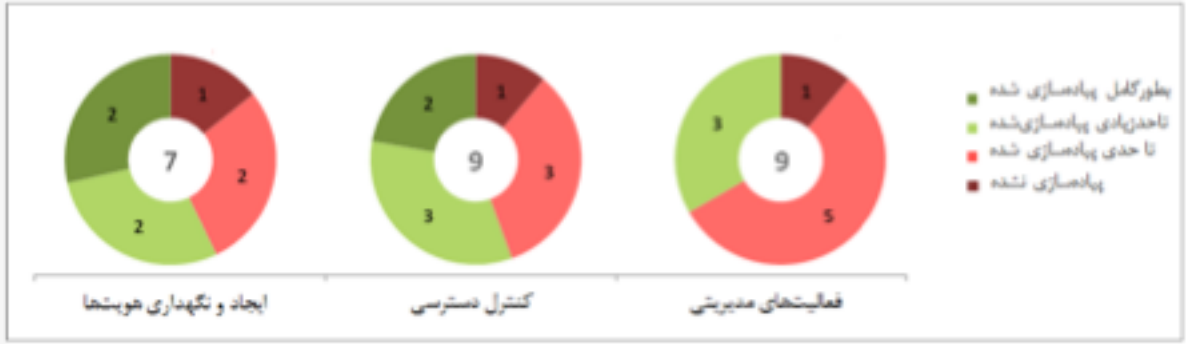
گزارش‌های متنوع مدیریتی

وضعیت پیاده‌سازی فعالیت‌ها در دامنه‌ی مدیریت دارایی، تغییرات و پیکربندی‌ها

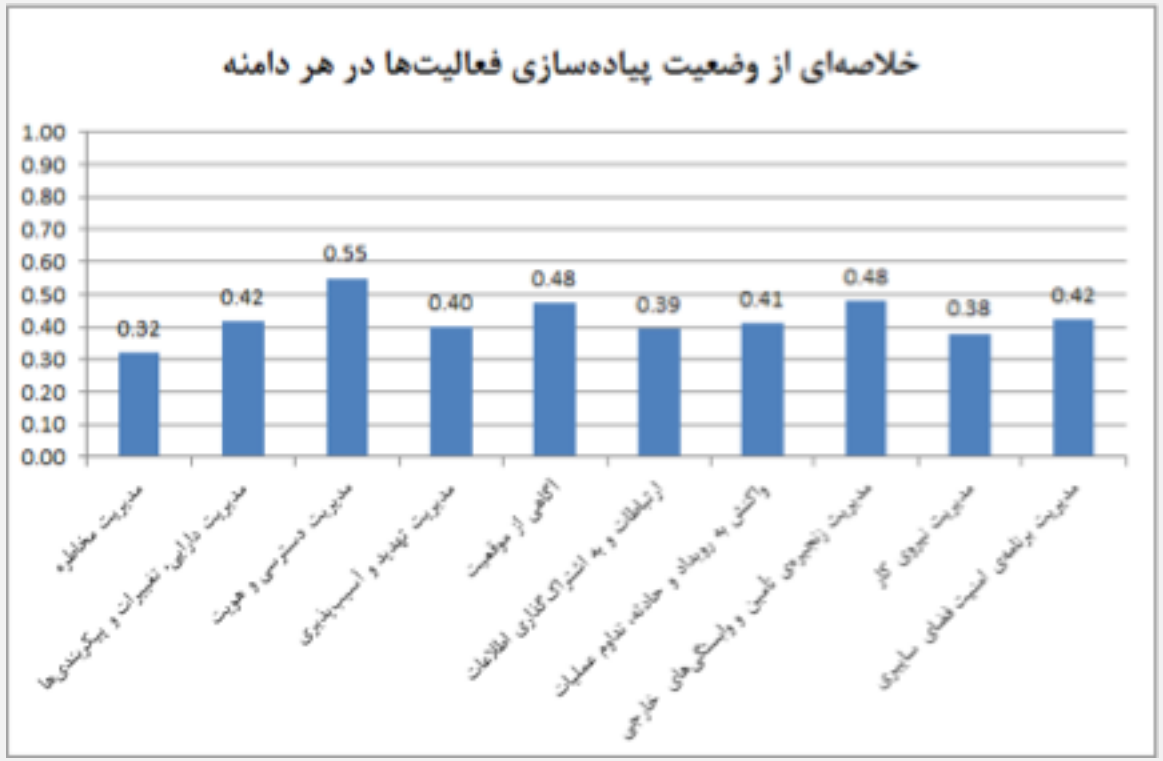
وضعیت پیاده‌سازی فعالیت‌ها در دامنه‌ی مدیریت تهدید و آسیب‌پذیری

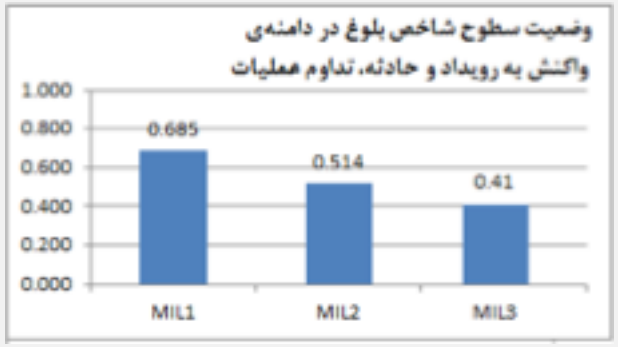


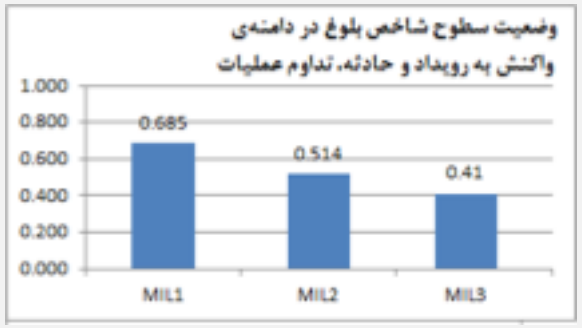
وضعیت پیاده‌سازی فعالیت‌ها در دامنه‌ی مدیریت دسترسی و هویت

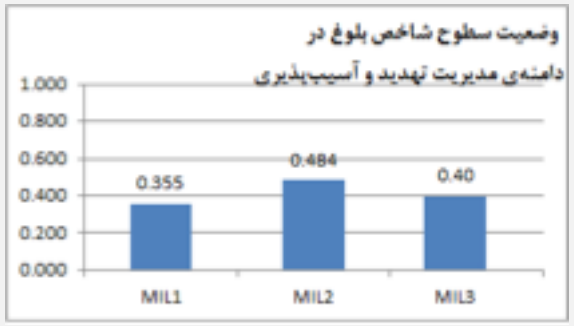


گزارش‌های متنوع مدیریتی









معرفی دامنه‌های C2M2

10 دامنه جامع امنیت

TVM مدیریت تهدید و آسیب‌پذیری (**Threat** and Vulnerability Management)	IAM مدیریت دسترسی و هویت (Identity and **Access** Management)	ACM مدیریت دارایی، تغییرات و پیکربندی (**Asset**, Change, and Configuration Management)	RM مدیریت مخاطره (**Risk** Management)
EDM مدیریت زنجیره تأمین و وابستگی‌های خارجی (Supply Chain and External **Dependencies** Management)	IR واکنش به رویداد و حادثه، تداوم عملیات (Event and Incident **Response**, Continuity of Operations)	ISC ارتباطات و به اشتراک گذاری اطلاعات (Information **Sharing** and Communications)	SA آگاهی از موقعیت (**Situational** Awareness)
• **دامنه‌ها:** گروه‌بندی منطقی از فعالیت‌های امنیت فضای سایبری		CPM مدیریت برنامه امنیت فضای سایبری (**Cybersecurity** Program Management)	WM مدیریت نیروی کار (**Workforce** Management)

مدیریت مخاطره

Risk Management(RM)

معرفی:

ایجاد و نگهداری برنامه‌ی مدیریت ریسک امنیت سایبری برای شناسایی، تحلیل و کاهش ریسک امنیت سایبری سازمان، شامل واحدهای کسب‌وکار، شرکت‌های تابعه، زیرساخت‌های مرتبط و ذینفعان.

اهداف:

1. ایجاد استراتژی مدیریت ریسک امنیت سایبری
2. مدیریت ریسک امنیت سایبری
3. فعالیت‌های مدیریتی

مدیریت دارایی، تغییرات و پیکربندی‌ها

Asset, Change, and Configuration Management(ACM)

معرفی:

مدیریت دارایی‌های IT و OT سازمان شامل سخت‌افزار و نرم‌افزار، متناسب با میزان ریسک بر زیرساخت حیاتی و اهداف سازمانی.

اهداف:

1. مدیریت لیست دارایی‌ها
2. مدیریت تنظیمات (پیکربندی) دارایی‌ها
3. مدیریت تغییرات دارایی‌ها
4. فعالیت‌های مدیریتی

مدیریت دسترسی و هویت

Identity and Access Management(IAM)

معرفی:

ایجاد و مدیریت هویت برای افراد و واحدهایی که ممکن است به‌صورت منطقی یا فیزیکی به دارایی‌های سازمان دسترسی یابند. کنترل دسترسی به دارایی‌های سازمان متناسب با میزان ریسک برای زیرساخت حیاتی و اهداف سازمانی.

اهداف:

1. ایجاد و نگهداری هویت‌ها
2. کنترل دسترسی
3. فعالیت‌های مدیریتی

مدیریت تهدید و آسیب‌پذیری

Threat and Vulnerability Management(TVM)

معرفی:

ایجاد و نگهداری برنامه، رویه و فناوری‌هایی برای تشخیص، شناسایی، تحلیل، مدیریت و پاسخ به تهدیدات و آسیب‌پذیری‌های امنیت سایبری متناسب با میزان ریسک برای زیرساخت حیاتی و اهداف سازمانی.

اهداف:

1. شناسایی و پاسخ به تهدیدات
2. کاهش آسیب‌پذیری‌های امنیت سایبری
3. فعالیت‌های مدیریتی

آگاهی از وضعیت

Situational Awareness(SA)

معرفی:

ایجاد و نگهداری فعالیت و فناوری‌هایی برای جمع‌آوری، تحلیل، هشدار، ارائه و استفاده از اطلاعات عملیاتی و امنیت سایبری شامل وضعیت و خلاصه‌ای از اطلاعات دامنه‌های دیگر برای ایجاد داشبورد عملیاتی (Common Operating Picture).

اهداف:

1. لاگ گیری
2. انجام نظارت
3. ایجاد و حفظ یک داشبورد عملیاتی
4. فعالیت‌های مدیریتی

ارتباطات و به اشتراک‌گذاری اطلاعات

Information Sharing and Communications(ISC)

معرفی:

ایجاد و نگهداری ارتباط با ادارات و نهادهای داخل و خارج سازمان به‌منظور جمع‌آوری اطلاعات امنیت سایبری، شامل تهدیدات و آسیب‌پذیری‌ها، به منظور کاهش ریسک و افزایش قابلیت بازگشت به عملیات نرمال متناسب با میزان ریسک برای زیرساخت حیاتی و اهداف سازمانی.

اهداف:

1. به اشتراک گذاری اطلاعات امنیت سایبری
2. فعالیت‌های مدیریتی

واکنش به رویداد و حادثه، تداوم عملیات

Event and Incident Response, Continuity of Operations(IR)

معرفی:

ایجاد و نگهداری برنامه، رویه و فناوری‌هایی برای شناسایی، تحلیل و پاسخ به رخدادهای امنیت سایبری و ادامه عملیات زمانی که رویدادی رخ می‌دهد.

اهداف:

1. شناسایی رخدادهای امنیت سایبری
2. رخدادهای اضطراری امنیت سایبری و اعلام حادثه‌ها
3. پاسخ به حوادث و رخدادهای اضطراری امنیت سایبری
4. برنامه‌ریزی برای تداوم
5. فعالیت‌های مدیریتی

مدیریت زنجیره‌ی تأمین و وابستگی‌های خارجی

Supply Chain and External Dependencies Management(EDM)

معرفی:

ایجاد و نگهداری کنترل‌هایی برای مدیریت ریسک‌های امنیت سایبری مرتبط با سرویس و دارایی‌هایی که به نهادهای خارجی مرتبط هستند.

اهداف:

1. شناسایی وابستگی‌ها
2. مدیریت ریسک وابستگی‌ها
3. فعالیت‌های مدیریتی

مدیریت نیروی کار

Workforce Management(WM)

معرفی:

تدوین و پایش برنامه، رویه، فناوری و کنترل‌هایی برای ایجاد فرهنگ امنیت سایبری و اطمینان از شایستگی مستمر و رقابت افراد مرتبط.

اهداف:

1. اختصاص مسئولیت‌های امنیت سایبری
2. کنترل چرخه‌ی حیات نیروی کار
3. توسعه نیروی کار امنیت سایبری
4. افزایش آگاهی امنیت سایبری
5. فعالیت‌های مدیریتی

مدیریت برنامه امنیت سایبری

Cybersecurity Program Management(CPM)

معرفی:

ایجاد و نگهداری یک برنامه امنیت سایبری در سازمان که نظارت، برنامه‌ریزی راهبردی و حمایت را برای فعالیت‌های امنیت سایبری سازمان فراهم می‌کند به طوری که اهداف امنیت سایبری با اهداف استراتژیک سازمان و ریسک زیرساخت حیاتی تطابق یابد.

اهداف:

1. ایجاد استراتژی برنامه امنیت سایبری
2. حمایت برنامه امنیت سایبری
3. ایجاد و حفظ معماری امنیت سایبری
4. اجرای توسعه نرم‌افزار با استانداردهای امنیتی
5. فعالیت‌های مدیریتی

تشریح دامنه نمونه

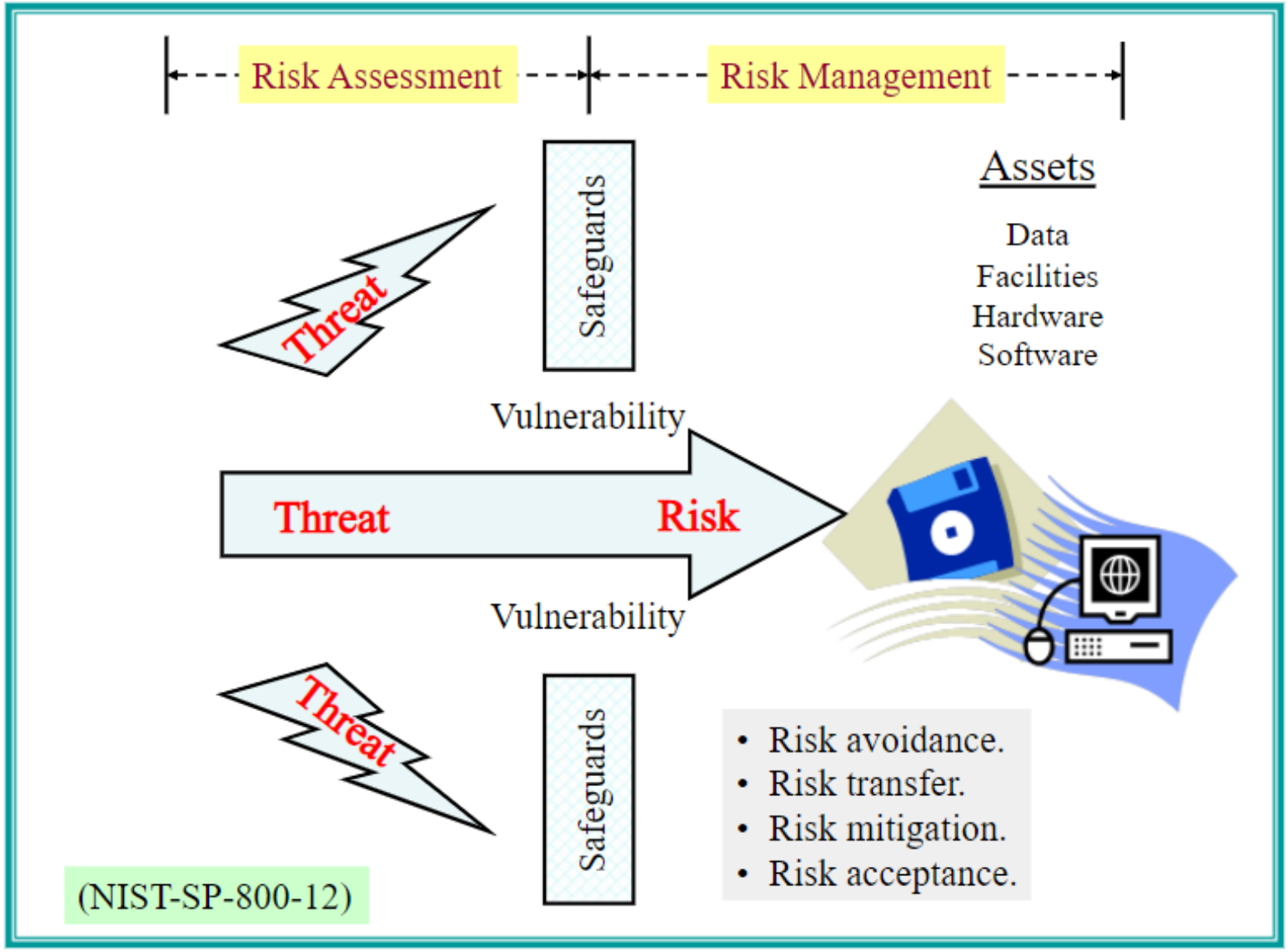
مدیریت تهدید و آسیب‌پذیری

Threat and Vulnerability Management(TVM)

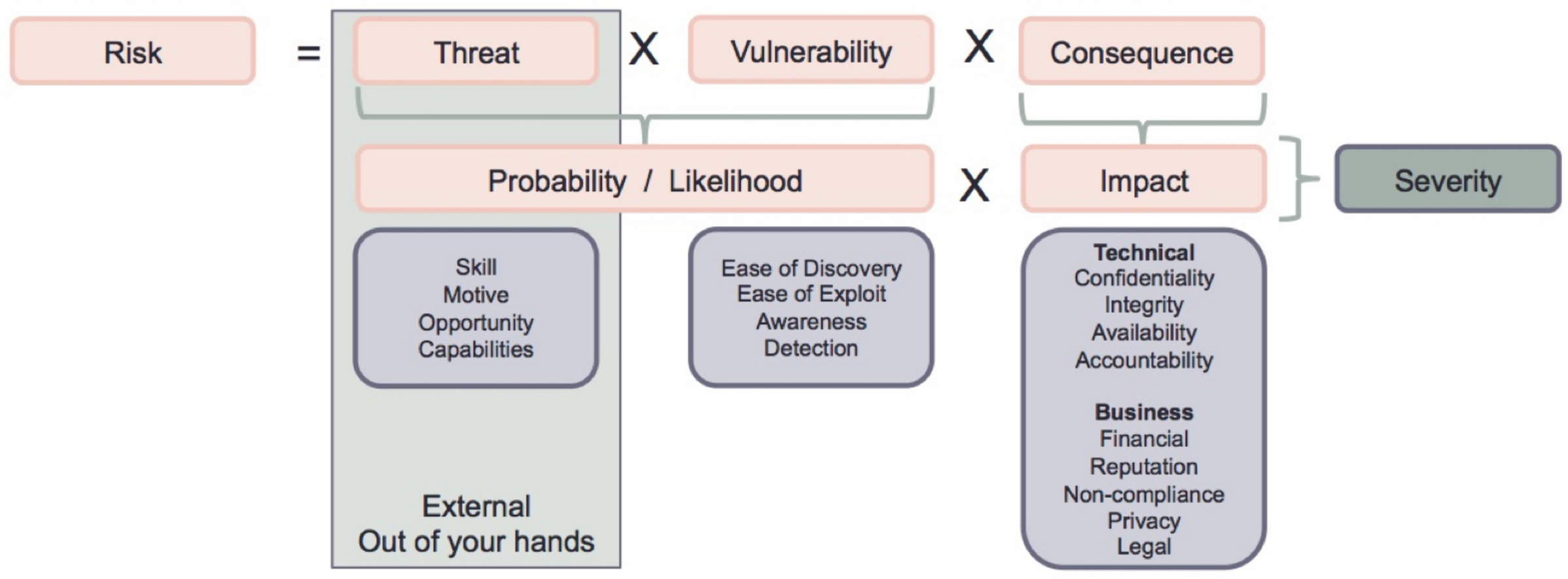
اهداف:

1. شناسایی و پاسخ به تهدیدات
2. کاهش آسیب‌پذیری‌های امنیت سایبری
3. فعالیت‌های مدیریتی

تعریف تهدید و آسیب‌پذیری



تعریف ریسک


Risk
=
Threat
X
Vulnerability
X
Consequence
Probability / Likelihood
X
Impact
Severity
Skill
Motive
Opportunity
Capabilities
Ease of Discovery
Ease of Exploit
Awareness
Detection
Technical
Confidentiality
Integrity
Availability
Accountability
Business
Financial
Reputation
Non-compliance
Privacy
Legal
External
Out of your hands

مدیریت تهدید و آسیب‌پذیری

Threat and Vulnerability Management(TVM)

اقدامات شناسایی و پاسخ به تهدیدات

- منابع اطلاعاتی برای انجام فعالیت‌های مدیریت تهدید مشخص می‌شوند (مانند تامین کنندگان و مراکز CERT و CSIRT)
- اطلاعات تهدیدات امنیت سایبری برای حوزه کاری ذیربط جمع‌آوری و تفسیر می‌شوند.
- به تهدیداتی که برای حوزه کاری ذیربط مهم تلقی می‌شوند، رسیدگی می‌شود (به عنوان مثال، پیاده سازی کنترل‌های بازدارنده، نظارت بر وضعیت تهدید).
- پروفایل تهدیدات برای حوزه کاری ذیربط ایجاد می‌شود که شامل مواردی مانند نیت احتمالی، ابعاد و اهداف تهدیداتی که به حوزه کاری ذیربط وارد می‌شوند، است.

اقدامات شناسایی و پاسخ به تهدیدات ۲

- منابع اطلاعاتی تهدیدات که شامل همه اجزای پروفایل تهدیدات هستند، اولویت‌بندی و نظارت می‌شوند.
- تهدیدات شناسایی شده تحلیل و اولویت‌بندی می‌شوند.
- به تهدیدات با توجه به اولویت اختصاص داده شده رسیدگی می‌شود.
- پروفایل تهدیدات برای حوزه کاری ذیربط باتوجه به تناوب تعریف شده در سطح سازمان بازبینی می‌شوند.

اقدامات شناسایی و پاسخ به تهدیدات ۳

- تحلیل و اولویت‌بندی تهدیدات براساس معیارهای ریسک حوزه کاری یا سازمانی (RM-1C) انجام می‌شوند.

- اطلاعات تهدید به پایگاه داده ریسک‌ها (RM-2J) اضافه می‌شوند.

اقدامات کاهش آسیب‌پذیری‌های امنیت سایبری

- منابع اطلاعاتی جهت کشف آسیب پذیری‌های امنیت سایبری مشخص می‌شوند (مانند تامین کنندگان و مراکز CERT و CSIRT)
- اطلاعات آسیب پذیری‌های امنیت سایبری برای حوزه کاری ذیربط جمع‌آوری و تفسیر می‌شوند.
- به آسیب پذیری‌های مهم امنیت سایبری در حوزه کاری ذیربط، رسیدگی می‌شود (به عنوان مثال، پیاده سازی کنترل‌های بازدارنده، اعمال patchهای امنیت سایبری).
- منابع اطلاعاتی آسیب پذیری‌های امنیت سایبری مرتبط با همه دارایی‌های مهم حوزه کاری رصد می‌شوند.
- ارزیابی‌های آسیب پذیری‌های امنیت سایبری انجام می‌شوند (به عنوان مثال، بازنگری معماری، آزمون نفوذ، مانورهای امنیت سایبری، ابزار شناسایی آسیب‌پذیری).

اقدامات کاهش آسیب‌پذیری‌های امنیت سایبری ۲

- آسیب پذیری‌های امنیت سایبری که شناسایی شده‌اند، تحلیل و اولویت‌بندی می‌شوند (مانند مراکز ثبت و ارزش‌گذاری آسیب‌پذیری‌ها (CVSS))
- به آسیب پذیری‌های امنیت سایبری با توجه به اولویت اختصاص داده شده رسیدگی می‌شود.
- تاثیر عملیاتی بر روی حوزه کاری ذیربط قبل از استقرار patchهای امنیت سایبری مورد ارزیابی قرار می‌گیرد.
- ارزیابی‌های آسیب‌پذیری‌های امنیت سایبری برای تمام دارایی‌های مهم حوزه کاری، به تناوب تعریف شده در سطح سازمان، انجام می‌شوند.

اقدامات کاهش آسیب‌پذیری‌های امنیت سایبری ۳

- ارزیابی آسیب پذیری‌های امینت سایبری بر اساس معیارهای ریسک حوزه کاری ذیربط (یا سازمانی) انجام می‌شوند (RM-1C)
- ارزیابی‌های آسیب پذیری‌های امنیت سایبری توسط بخش مستقل از عملیات حوزه کاری انجام می‌شوند.
- تحلیل و اولویت‌بندی آسیب پذیری‌ها توسط معیارهای ریسک حوزه کاری (یا سازمانی) انجام می‌شوند (RM-1C)
- اطلاعات آسیب پذیری‌های امنیت سایبری به پایگاه داده ریسک‌ها اضافه می‌گردند (RM-2J)
- درستی پاسخ به آسیب پذیری‌های امنیت سایبری توسط فعالیت‌های پایش ریسک بررسی می‌شود (به عنوان مثال، استقرار patchها یا دیگر فعالیت‌ها).

اقدامات فعالیت‌های مدیریتی

- برای انجام فعالیت‌های مدیریت تهدید و آسیب پذیری از روال‌های مستند استفاده می‌شود.
- برای انجام فعالیت‌های مدیریت تهدید و آسیب پذیری؛ ذینفعان شناسایی و وارد عمل می‌شوند.
- برای انجام فعالیت‌های مدیریت تهدید و آسیب پذیری؛ منابع کافی (افراد، بودجه، و ابزار) فراهم شده است.
- برای استفاده در فعالیت‌های مدیریت تهدید و آسیب پذیری؛ استانداردها و/یا دستورالعمل‌هایی مشخص شده است.
- فعالیت‌های مدیریت تهدید و آسیب پذیری در راستای سیاست‌های مستند یا دیگر اسناد بالادستی سازمان است.

اقدامات فعالیت‌های مدیریتی ۲

- سیاست‌های مدیریت تهدید و آسیب پذیری شامل الزامات اجرایی برای انطباق فعالیت‌ها با استانداردها یا دستورالعمل‌های مشخص شده، است.
- فعالیت‌های مدیریت تهدید و آسیب پذیری جهت اطمینان از انطباق با سیاست‌های سازمان به صورت دوره‌ای بازنگری می‌شوند.
- جهت انجام فعالیت‌های مدیریت تهدید و آسیب پذیری؛ مسئولیت‌ها و اختیاراتی به کارکنان واگذار می‌شود.
- کارکنانی که فعالیت‌های مدیریت تهدید و آسیب پذیری را انجام می‌دهند، مهارت‌ها و دانش مورد نیاز برای انجام وظایف اختصاص داده شده خود را دارند.

فرآنش

مدیریت امنیت – امنیت مدیریت