باسمه تعالی

کارگاه نسل نوین مدیریت امنیت سازمانی
دانشگاه بیرجند، مرکز آپا

نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری

پایش مستمر و ارزیابی بلوغ امنیتی سازمان‌ها و زیرساخت های حیاتی

دکتر شهریار بیژنی

مدیر گروه علوم کامپیوتر دانشگاه شاهد

مدیر عامل شرکت فراکنش

۱۲ اسفند ۱۳۹۶

مقدمه ای بر مدیریت امنیت

نسل نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری

مدیریت امنیت

- استانداردهای مدیریت امنیت
  - ISMS
  - SOC2
  - PCI DSS
  - Infosec

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”

مقدمه ای بر مدل های بلوغ سازمانی

نسل نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری

چرا مدل بلوغ امنیت سایبری؟

- نفوذهای مکرر در فضای سایبری به سازمان و زیرساخت های 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 متفاوتی به روش‌های امن‌سازی رایج
- نیاز به نگاهی نو و پیشرفته به امنیت فضای 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:
۱- ارزیابی عملکرد داخلی
۲- تسریع بهبود عملکرد
۳- تسریع بهبود در عملکرد زیر بخش های سازمان
۴- ایجاد و تکمیل یک زبان مشترک بین ذینفعان
۵- برقراری توازن بین انتظارات و سطح سازمان

مدل بلوغ

انواع مدل‌های بلوغ:

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

مثال مدل بلوغ پیشرفت(۱)

Progression for Human Mobility
Fly
Sprint
Run
Jog
Walk
Crawl

مثال مدل بلوغ پیشرفت(۲): 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

مثال 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

مقایسه مدل‌های بلوغ پیشرفت و قابلیت

بلوغ پیشرفت

- ارائه نقشه راه
- کمّی تر: سنجش ساده تر
- اثر کمتر دیدگاه ارزیاب (objectivity)

- دیدگاه فنی به امنیت
- پیاده سازی کنترلهای بیشتر، لزوما به معنای امنیت کامل تر نیست

بلوغ قابلیت

- رویکرد فرایندی و سیستمی
- نگاه سطح کلان، مدیریتی و حاکمیتی

- اثر بیشتر نظر ارزیاب (subjectivity)

مدل بلوغ ترکیبی

ترکیب برخی ویژگی‌های مدل‌های بلوغ قابلیت و پیشرفت

- مثال: Cybersecurity Capability Maturity Model

معرفی برخی مدل‌های بلوغ امنیت

نسل نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری

برخی از مدل‌های بلوغ امنیت

- NIST SP 800-53
- CERT-RMM
- CERT-CRR
- C2M2
- OISM3
- COBIT 5 for Information Security
- OpenSAMM
- IAMM
- BSIMM
- CySAFE

پدیدآورنده COBIT

ISACA (Information System Audit and Control Association)

https://en.wikipedia.org/wiki/COBIT

Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
العربية
Čeština
Dansk
Deutsch
Español
فارسی
Français
Galego
Bahasa Indonesia
Italiano
Nederlands
日本語
Norsk bokmål
Polski
Português
Русский
Svenska
Türkçe
Українська
中文
Edit links

History [edit]

ISACA first released COBIT in 1996, originally as a set of control objectives to help the financial audit community better maneuver in IT-related environments.[1][2] Seeing value in expanding the framework beyond just the auditing realm, ISACA released a broader version 2 in 1998 and expanded it even further by adding management guidelines in 2000's version 3. The development of both the AS 8015: *Australian Standard for Corporate Governance of Information and Communication Technology* in January 2005[3] and the more international draft standard ISO/IEC DIS 29382 (which soon after became ISO/IEC 38500) in January 2007[4] increased awareness of the need for more information and communication technology (ICT) governance components. ISACA inevitably added related components/frameworks with versions 4 and 4.1 in 2005 and 2007 respectively, "addressing the IT-related business processes and responsibilities in value creation (Val IT) and risk management (Risk IT)."[1][2]

In April 2012, COBIT 5 was released. Several drivers were responsible for the transition from 4.1 to 5:[5]

- need for a more coherent understanding of how existing standards, best practices, and other tools relate and augment each other;
- need for a more end-to-end business/organization scope that covers all business and IT functions;
- need for improved guidance on hot-topic items such as enterprise architecture and emerging technologies;
- need for tighter integration among COBIT and other ISACA research, recommendations, and frameworks;
- need for tighter integration with external standards, recommendations, and frameworks; and
- need for improved information organization and dissemination concerning the framework.

An add-on for COBIT 5 related to information security was released on December 2012, and one related to assurance was released in June 2013.[6][7]

The COBIT framework [edit]

COBIT was initially "Control Objectives for Information and Related Technologies," though before the release of the framework people talked of "CobiT" as "Control Objectives for IT"[8] or "Control Objectives for Information and Related Technology."[9] The framework defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model. COBIT also provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. COBIT 5 consolidates COBIT 4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with other frameworks and standards.[1]

تسل نو ین مدیر یت امنیت ساز مانی: بلو ع امنیت سایبری

نسخه های Cobit

https://en.wikipedia.org/wiki/COBIT

Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
العربية
Čeština
Dansk
Deutsch
Español
فارسی
Français
Galego
Bahasa Indonesia
Italiano
Nederlands
日本語
Norsk bokmål
Polski
Português
Русский
Svenska
Türkçe
Українська
中文
Edit links

History [edit]

ISACA first released COBIT in 1996, originally as a set of control objectives to help the financial audit community better maneuver in IT-related environments.[1][2] Seeing value in expanding the framework beyond just the auditing realm, ISACA released a broader version 2 in 1998 and expanded it even further by adding management guidelines in 2000's version 3. The development of both the AS 8015: *Australian Standard for Corporate Governance of Information and Communication Technology* in January 2005[3] and the more international draft standard ISO/IEC DIS 29382 (which soon after became ISO/IEC 38500) in January 2007[4] increased awareness of the need for more information and communication technology (ICT) governance components. ISACA inevitably added related components/frameworks with versions 4 and 4.1 in 2005 and 2007 respectively, "addressing the IT-related business processes and responsibilities in value creation (Val IT) and risk management (Risk IT)."[1][2]

In April 2012, COBIT 5 was released. Several drivers were responsible for the transition from 4.1 to 5:[5]

- need for a more coherent understanding of how existing standards, best practices, and other tools relate and augment each other;
- need for a more end-to-end business/organization scope that covers all business and IT functions;
- need for improved guidance on hot-topic items such as enterprise architecture and emerging technologies;
- need for tighter integration among COBIT and other ISACA research, recommendations, and frameworks;
- need for tighter integration with external standards, recommendations, and frameworks; and
- need for improved information organization and dissemination concerning the framework.

An add-on for COBIT 5 related to information security was released on December 2012, and one related to assurance was released in June 2013.[6][7]

The COBIT framework [edit]

COBIT was initially "Control Objectives for Information and Related Technologies," though before the release of the framework people talked of "CobiT" as "Control Objectives for IT"[8] or "Control Objectives for Information and Related Technology."[9] The framework defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model. COBIT also provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. COBIT 5 consolidates COBIT 4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with other frameworks and standards.[1]

نسل نوین مدیریت امنیت سازمانی بر پایه امنیت سایبری

نسخه ۱.۰
۱۹۹۶

نسخه ۲.۰
۱۹۹۸

نسخه ۳.۰
۲۰۰۰

نسخه ۴.۰
۲۰۰۵

نسخه ۴.۱
۲۰۰۷

نسخه ۵.۰
۲۰۱۲

تفاوت Cobit 5 و Cobit 5 for Info. Sec.

Cobit 5 for Information Security

examines each of the processes from an information security perspective.

Reference:

ISACA, 2012

& Wikipedia

Enabler: Processes

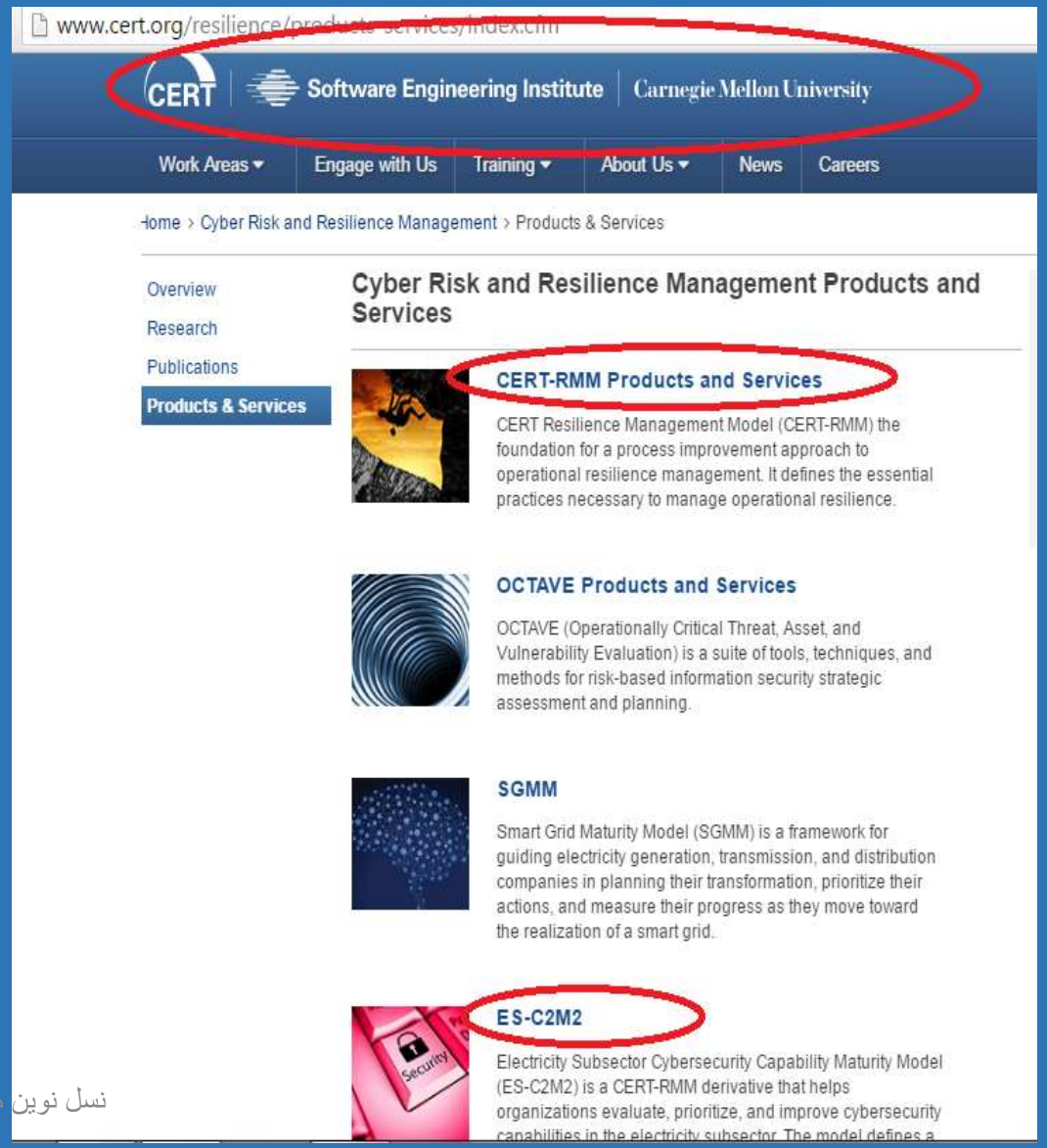
The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes:

- The Governance domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
- The four Management domains are in line with the responsibility areas of plan, build, run and monitor (PBRM).
- *COBIT 5 for Information Security* examines each of the processes from an information security perspective.

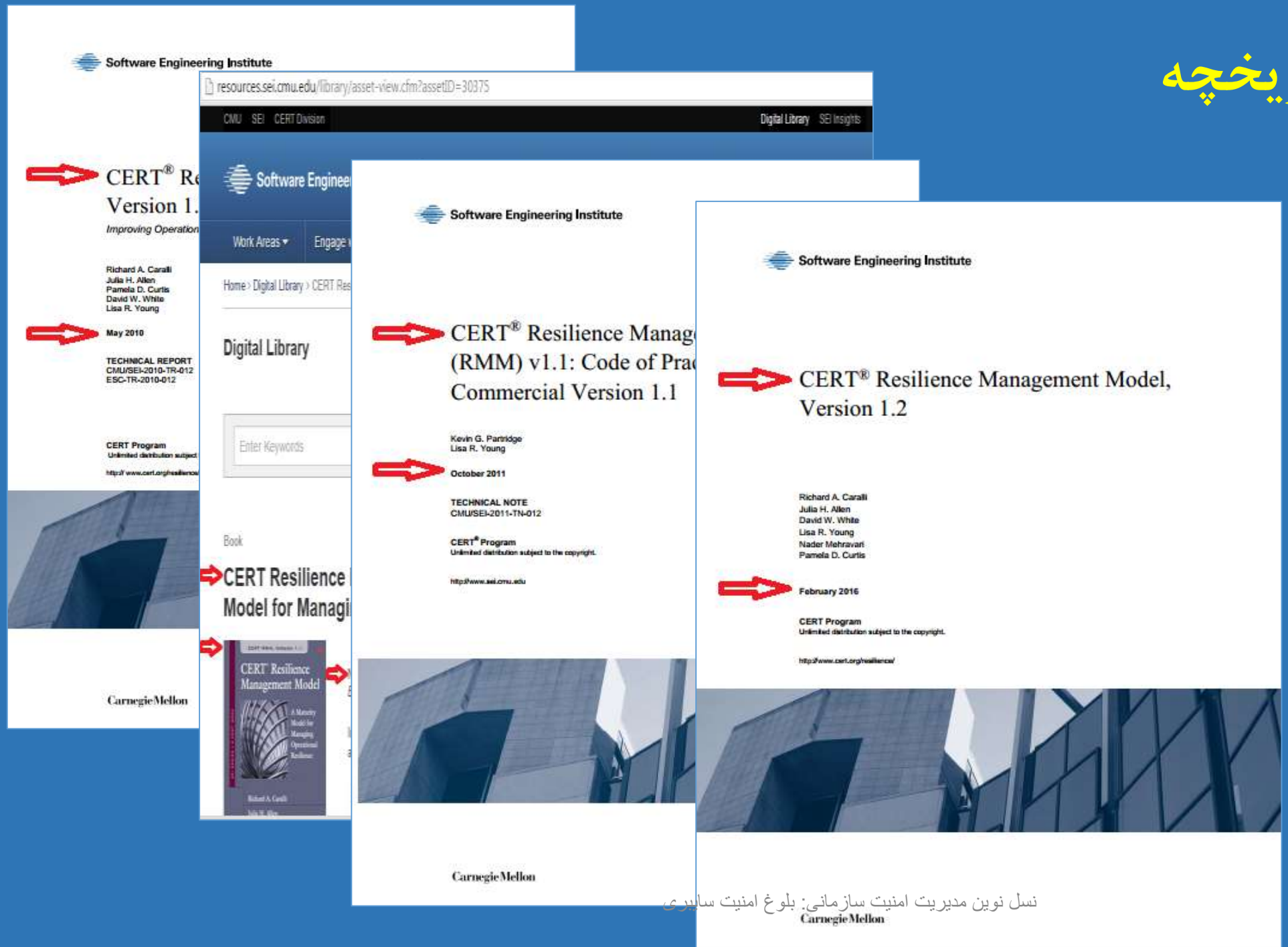
پدیدآورنده CERT-RMM

CMU-SEI-CERT:

- Carnegie Mellon University (CMU)
  - Software Engineering Institute (SEI)
    - CERT Division



CERT-RMM: تاریخچه



CERT-RMM

نسخه Draft

2008

نسخه ۱.۰

May 2010

نسخه ۱.۱

Nov. 2010

نسخه ۱.۱ Code of Practices

Oct. 2011

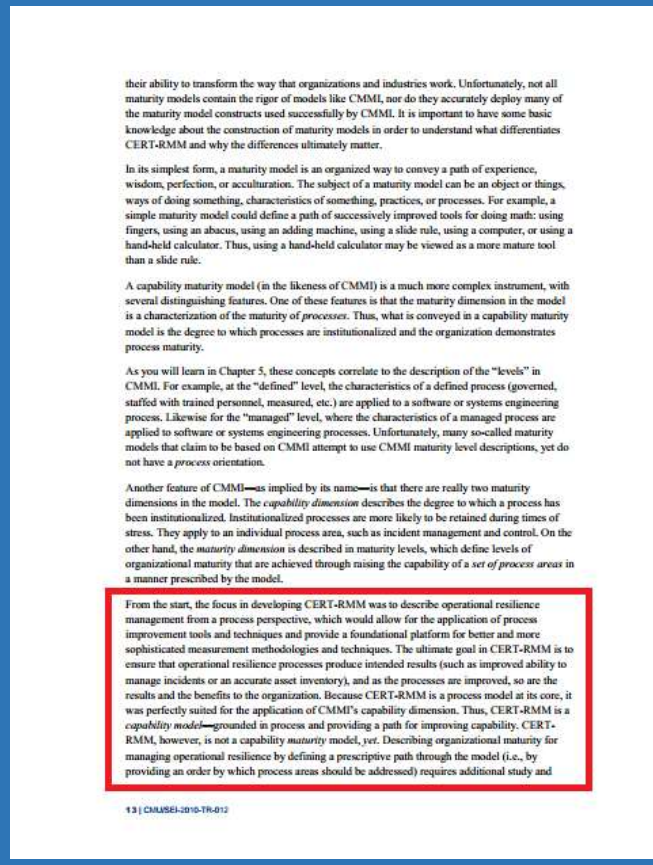
نسخه ۱.۲

Feb. 2016

CERT-RMM

Because CERT-RMM is a process model at its core, it was perfectly suited for the application of CMMI's capability dimension. Thus; CERT-RMM is a *capability model*—grounded in process and providing a path for improving capability. CERT-RMM, however, is not a capability *maturity* model, yet.

Reference: CERT-Resilience Management Model, Version 1.0, May 2010, page 13.



their ability to transform the way that organizations and industries work. Unfortunately, not all maturity models contain the rigor of models like CMMI, nor do they accurately deploy many of the maturity model constructs used successfully by CMMI. It is important to have some basic knowledge about the construction of maturity models in order to understand what differentiates CERT-RMM and why the differences ultimately matter.

In its simplest form, a maturity model is an organized way to convey a path of experience, wisdom, perfection, or acculturation. The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes. For example, a simple maturity model could define a path of successively improved tools for doing math: using fingers, using an abacus, using an adding machine, using a slide rule, using a computer, or using a hand-held calculator. Thus, using a hand-held calculator may be viewed as a more mature tool than a slide rule.

A capability maturity model (in the likeness of CMMI) is a much more complex instrument, with several distinguishing features. One of these features is that the maturity dimension in the model is a characterization of the maturity of *processes*. Thus, what is conveyed in a capability maturity model is the degree to which processes are institutionalized and the organization demonstrates process maturity.

As you will learn in Chapter 5, these concepts correlate to the description of the "levels" in CMMI. For example, at the "defined" level, the characteristics of a defined process (governed, staffed with trained personnel, measured, etc.) are applied to a software or systems engineering process. Likewise for the "managed" level, where the characteristics of a managed process are applied to software or systems engineering processes. Unfortunately, many so-called maturity models that claim to be based on CMMI attempt to use CMMI maturity level descriptions, yet do not have a *process* orientation.

Another feature of CMMI—as implied by its name—is that there are really two maturity dimensions in the model. The *capability dimension* describes the degree to which a process has been institutionalized. Institutionalized processes are more likely to be retained during times of stress. They apply to an individual process area, such as incident management and control. On the other hand, the *maturity dimension* is described in maturity levels, which define levels of organizational maturity that are achieved through raising the capability of a *set of process areas* in a manner prescribed by the model.

From the start, the focus in developing CERT-RMM was to describe operational resilience management from a process perspective, which would allow for the application of process improvement tools and techniques and provide a foundational platform for better and more sophisticated measurement methodologies and techniques. The ultimate goal in CERT-RMM is to ensure that operational resilience processes produce intended results (such as improved ability to manage incidents or an accurate asset inventory), and as the processes are improved, so are the results and the benefits to the organization. Because CERT-RMM is a process model at its core, it was perfectly suited for the application of CMMI's capability dimension. Thus, CERT-RMM is a *capability model*—grounded in process and providing a path for improving capability. CERT-RMM, however, is not a capability *maturity* model, *yet*. Describing organizational maturity for managing operational resilience by defining a prescriptive path through the model (i.e., by providing an order by which process areas should be addressed) requires additional study and

13 | CMU/SEI-2010-TR-012

CERT-RMM

از نسخه ی ۱.۱ به بعد، سطوح Maturity به آن اضافه شده است.

The CERT-RMM v1.1 is a capability maturity model for managing operational resilience.

Reference: CERT- Resilience Management Model: Code of Practices, Version 1.1, 2011.

CERT-RMM

Building on the success of ES-C2M2, the MIL scale will form the basis for the maturity architecture of CERT-RMM v2.0.

CERT-RMM v2.0 is currently in development!

Reference: Advancing Cybersecurity Capability Measurement Using the CERT®-RMM Maturity Indicator Level Scale, CMU-SEI, page 13, Nov. 2013.

Executive Summary

In its simplest form, a *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. Architecturally, maturity models typically have levels arranged in an evolutionary scale that defines measurable transitions from one level of maturity to another. The current version of the CERT® Resilience Management Model (CERT®-RMM v1.2) utilizes the maturity architecture (levels and descriptions) as provided in the Capability Maturity Model Integration (CMMI) constellation models (Development, Acquisition, and Services) to ensure consistency with CMMI, particularly for CERT-RMM users who are already using one of the CMMI early lifecycle models. While the CMMI maturity levels and descriptions are a good fit for CERT-RMM, in practice the spacing between levels often causes CERT-RMM practitioners some difficulty. To address some of these issues, the CERT Division of the Software Engineering Institute, part of Carnegie Mellon University, did a comprehensive review of the existing specific and generic goals and practices in CERT-RMM to determine if a better scale could be developed to help users of the model show incremental improvement in maturity without breaking the original intent of the CMMI maturity levels. This resulted in the development of the maturity indicator level scale, or the CERT-RMM MIL scale.

Maturity indicator levels (MILs) are a specific representation of the capability levels currently instantiated in CERT-RMM. They describe attributes that would be *indicative* of these capabilities if the capabilities had been appraised through a formal appraisal process. In other words, achieving the MILs does not necessarily imply capability (as measured through formal CERT-RMM appraisal), but it does *indicate* capability.

While the MIL scale was originally prototyped in late 2011 as part of the planning for version 2.0 of CERT-RMM, the construct informed the development of hybrid maturity models—those that combine the progression of practices with the ability to measure increasing capability. The first application of the MIL scale was in the Cyber Resilience Review (CRR), a comprehensive review process based on CERT-RMM and developed in collaboration with the Department of Homeland Security to measure the effectiveness of resilience practices by owners and operators of critical infrastructure. Upon successful application in the CRR, the MIL scale was adapted for use in the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) developed collaboratively with the Department of Energy to comply with a White House initiative to examine and characterize the cybersecurity posture of the electric grid. The extensive piloting and use of the MIL scale in CRR and ES-C2M2 and the success of these models indicate that the MIL scale is not only a viable but accessible maturity architecture. Building on the success of ES-C2M2, the MIL scale is being incorporated into the Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2) and will form the basis for the maturity architecture of CERT-RMM v2.0.

* CERT® is a registered mark owned by Carnegie Mellon University.

نسل نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری

CERT-RMM از دیدگاه کمّی

آخرین بروزرسانی از نسخه ۱.۲ در تاریخ فوریه ۲۰۱۶:

# of Categories: 4

# of Process Areas: 26

# of Goals: 93 (Specific Goals)

# of Practices: 264

نمونه ای از خروجی CERT-RMM

SC: Service Continuity

S	**SG1**	**Prepare for service continuity**
LI	SG1.SP1	Plan for service continuity
LI	SG1.SP2	Establish standards and guidelines for service continuity
NS	**SG2**	**Identify and prioritize high-value services**
FI	SG2.SP1	Identify the organization's high-value services
PI	SG2.SP2	Identify internal and external dependencies and interdependencies
LI	SG2.SP3	Identify vital organizational records and databases
S	**SG3**	**Develop service continuity plans**
FI	SG3.SP1	Identify plans to be developed
FI	SG3.SP2	Develop and document service continuity plans
FI	SG3.SP3	Assign staff to service continuity plans
LI	SG3.SP4	Store and secure service continuity plans
LI	SG3.SP5	Develop service continuity plan training
NS	**SG4**	**Validate service continuity plans**
LI	SG4.SP1	Validate plans to requirements and standards
PI	SG4.SP2	Identify and resolve plan conflicts
S	**SG5**	**Exercise service continuity plans**
FI	SG5.SP1	Develop testing program and standards
FI	SG5.SP2	Develop and document test plans
FI	SG5.SP3	Exercise plans
FI	SG5.SP4	Evaluate plan test results
NS	**SG6**	**Execute service continuity plans**
FI	SG6.SP1	Execute plans
NI	SG6.SP2	Measure the effectiveness of the plans in operation
S	**SG7**	**Maintain service continuity plans**
LI	SG7.SP1	Establish change criteria
LI	SG7.SP2	Maintain changes to plans
NS	**GG2**	**Institutionalize a managed process**
PI	GG2.GP1	Establish process governance
LI	GG2.GP2	Plan the process
LI	GG2.GP3	Provide resources
FI	GG2.GP4	Assign responsibility
LI	GG2.GP5	Train people
LI	GG2.GP6	Manage work product configurations
PI	GG2.GP7	Identify and involve relevant stakeholders
FI	GG2.GP8	Monitor and control the process
PI	GG2.GP9	Objectively evlauate adherence
FI	GG2.GP10	Review status with higher-level managers
NS	**GG3**	**Institutionalize a defined process**
PI	GG3.GP1	Establish a defined process
NI	GG3.GP2	Collect improvement information

Key:

Goal Ratings

S	Satisfied
NS	Not Satisfied

Practice Characterizations

FI	Fully Implemented
LI	Largely Implemented
PI	Partially Implemented
NI	Not Implemented
NY	Not Yet

نسل نوین مدیریت امنیت سازمانی - طرح امنیت سایبری
© 2011 Carnegie Mellon University

مدل C2M2

نسل نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری

پدیدآورندگان 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.

ES-C2M2 Background

White House initiative

Led by Department of Energy

In partnership with Department of Homeland Security

In collaboration with representatives of electricity subsector asset owners and operators

CERT | Software Engineering Institute | Carnegie Mellon University

CERT® Operational Resilience: Manage, Protect, and Sustain
Twitter #CERTopRES
© 2014 Carnegie Mellon University

پدیدآورندگان C2M2

ES-C2M2 is derived from the CERT-RMM

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

© 2014 Carnegie Mellon University

پدیدآورندگان C2M2

C2M2 is based on ES-C2M2

-by removing sector-specific references and terminology.

Reference:

Cybersecurity Capability Maturity Model, Version 1.1, U.S. DOE, 2014.

ACKNOWLEDGMENTS

The Department of Energy (DOE) developed the Cybersecurity Capability Maturity Model (C2M2) from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.0 by removing sector-specific references and terminology. The ES-C2M2 was developed in support of a White House initiative led by the DOE, in partnership with the Department of Homeland Security (DHS), and in collaboration with private- and public-sector experts.

The DOE acknowledges the dedication and technical expertise of all the organizations and individuals who participated in the development of ES-C2M2 as well as the organizations and individuals from different sectors who have provided the critiques, evaluations, and modifications in order to produce this first release of the C2M2.

Program Technical Lead
Jason D. Christopher
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Program Team
Fowad Muneer, ICF International
John Fry, ICF International

Model Architect
Carnegie Mellon University Software Engineering Institute – CERT Division

مطالعه و ترجمه امنیت سازمانی: بلوغ امنیت سایبری

C2M2 & Critical Infrastructure Objectives

2.2 Critical Infrastructure Objectives

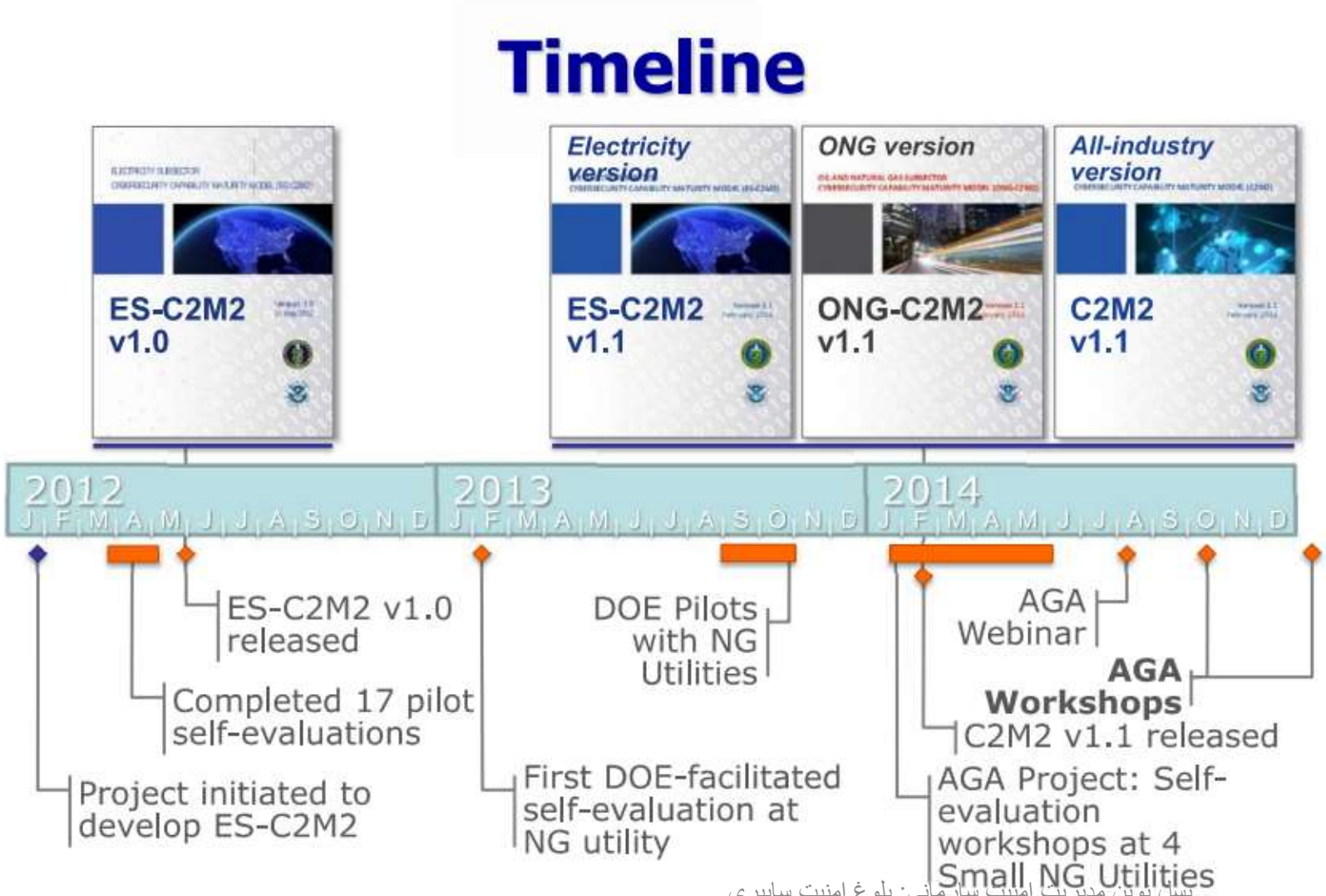
The model makes regular reference to *critical infrastructure objectives*. These are objectives found in the sector-specific infrastructure protection plans[5] of the 16 United States critical infrastructure sectors defined in Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience."[6] The referenced objectives serve as a reminder that many of the functions provided by potential adopters of the model support the Nation's critical infrastructure and that the broader cybersecurity objectives of the sector-specific plans should be considered.

Critical infrastructure objectives often transcend the business or operational objectives for an individual organization. Some organizations using the model may not be affiliated with any of the defined critical infrastructure sectors. For such organizations, the term *critical infrastructure objectives* can be interpreted to mean industry objectives, community objectives, or any other

[5] http://www.dhs.gov/sector-specific-plans
[6] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Reference: Cybersecurity Capability Maturity Model Version 1.1, Page:.3

C2M2: تاریخچه



ES-C2M2

نسخه ۱.۰

May 2012

نسخه ۱.۱

Feb. 2014

C2M2

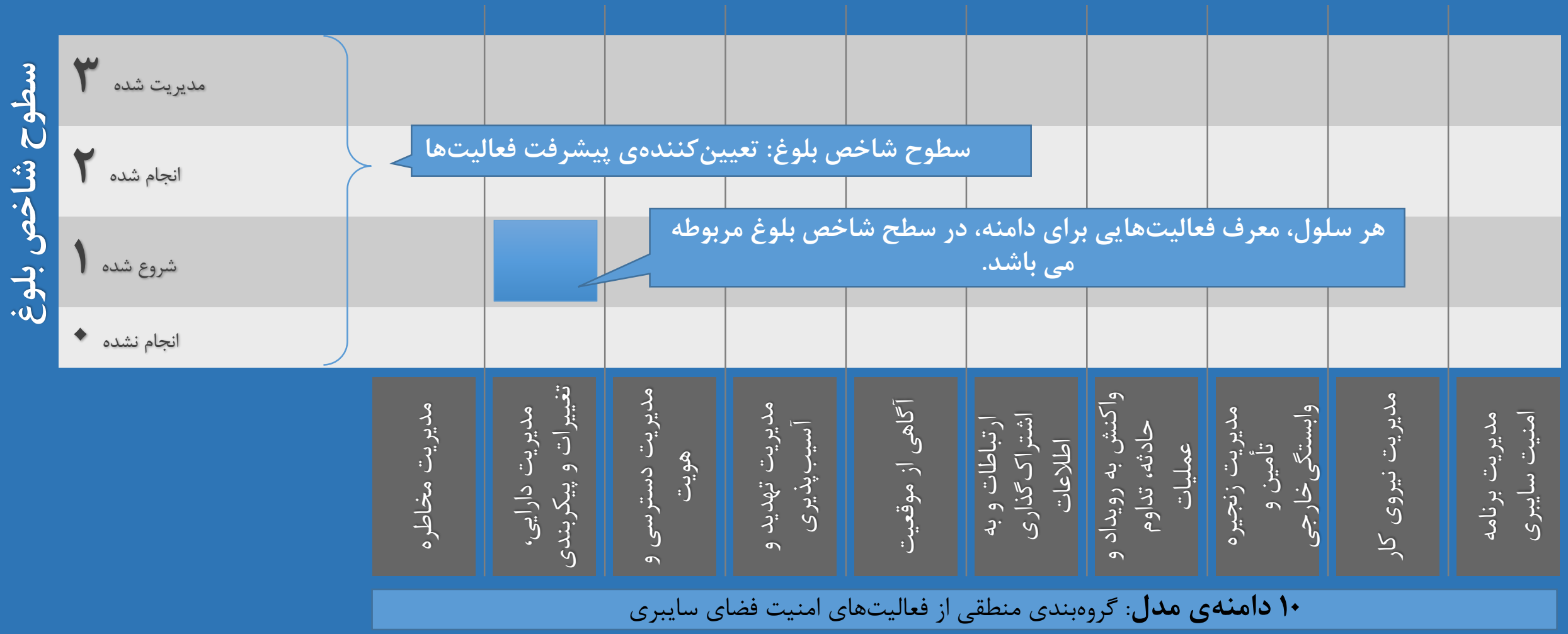
نسخه ۱.۱

Feb. 2014

نگاهی جامع به امنیت: ۱۰ 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)

مدل در یک نگاه



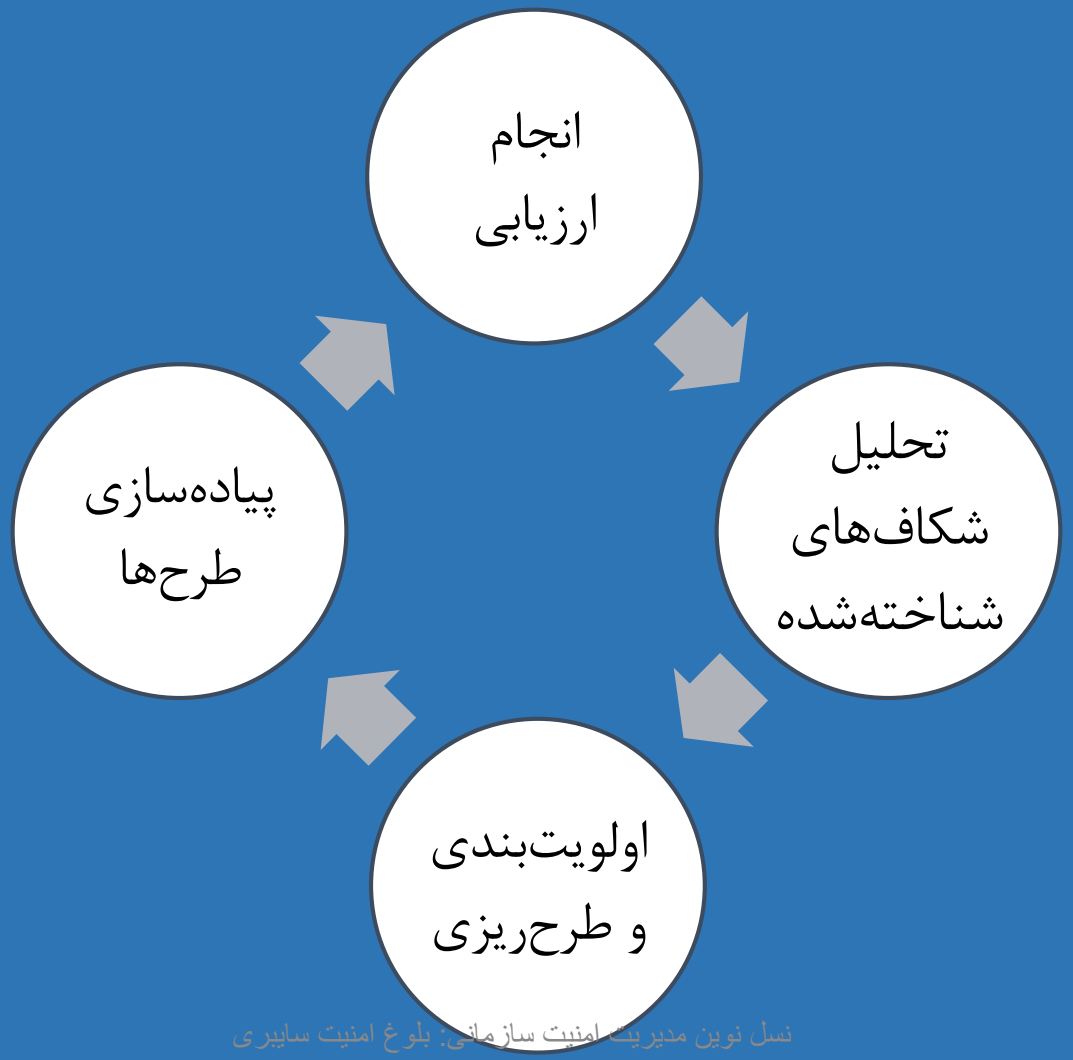
۱۰ دامنه‌ی مدل: گروه‌بندی منطقی از فعالیت‌های امنیت فضای سایبری

معماری مدل بلوغ

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.

استفاده از مدل



مزایای مدل بلوغ امنیت سایبری در این پروژه

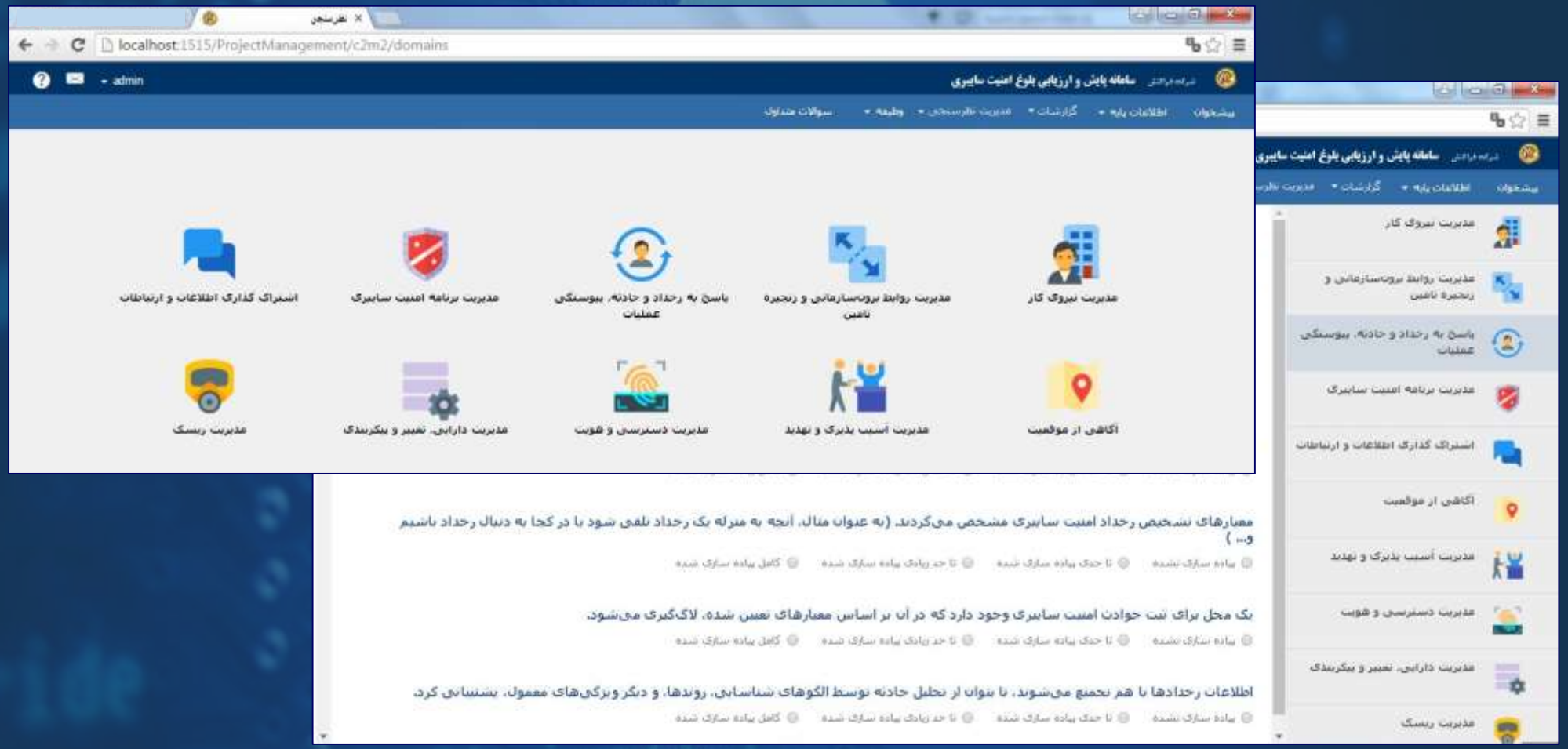
- تقویت امنیت فضای مجازی در سازمان‌ها
- مطابقت با نیازهای امنیتی زیرساخت های حیاتی
- کمک به ارتقاء فرهنگ امنیت سایبری در سازمان
- درونی سازی امنیت در سازمان به عنوان زیربنای فعالیت های امن سازی
- فراهم سازی امکان فعالیت های اولویت بندی شده و سرمایه گذاری بهینه در حوزه امنیت

مزایای سامانه پایش و ارزیابی امنیت سایبری

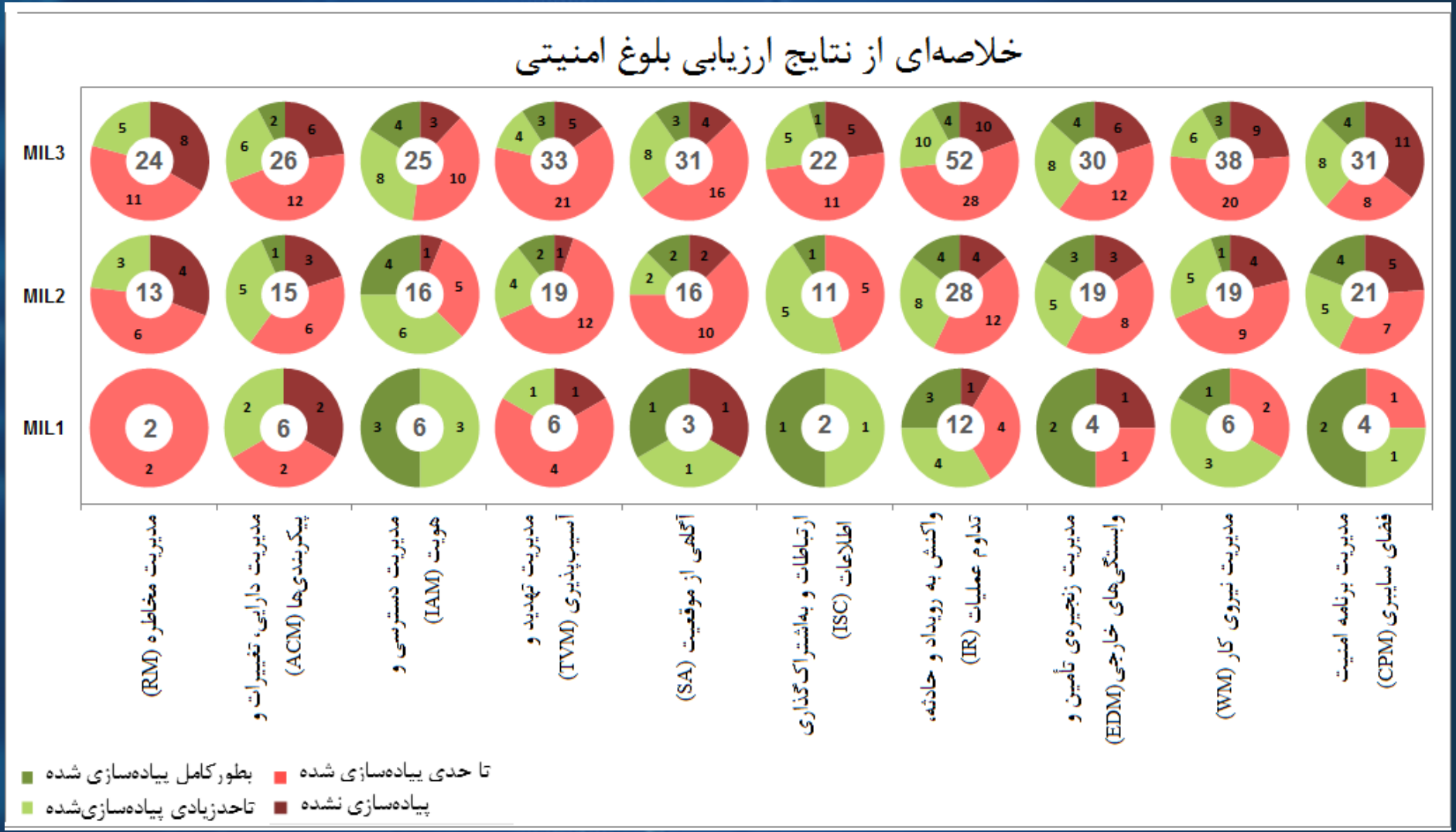
- نمایش جامع، یکپارچه و کلان وضعیت امنیت مبتنی بر بلوغ امنیتی
- داشبورد وضعیت امنیت سایبری جهت مدیران عالی سازمان
- مشاهده گزارش از بلوغ پیشرفت و قابلیت امنیت سایبری سازمان
- امکان مقایسه امنیتی واحدهای مختلف سازمان
- دسترسی دائمی به داده های اولیه، پردازش شده و گزارشات متنوع
- ارزیابی مستمر و جمع آوری سیستماتیک اطلاعات از وضعیت امنیت سایبری

ساختار سامانه پایش و ارزیابی امنیت سایبری

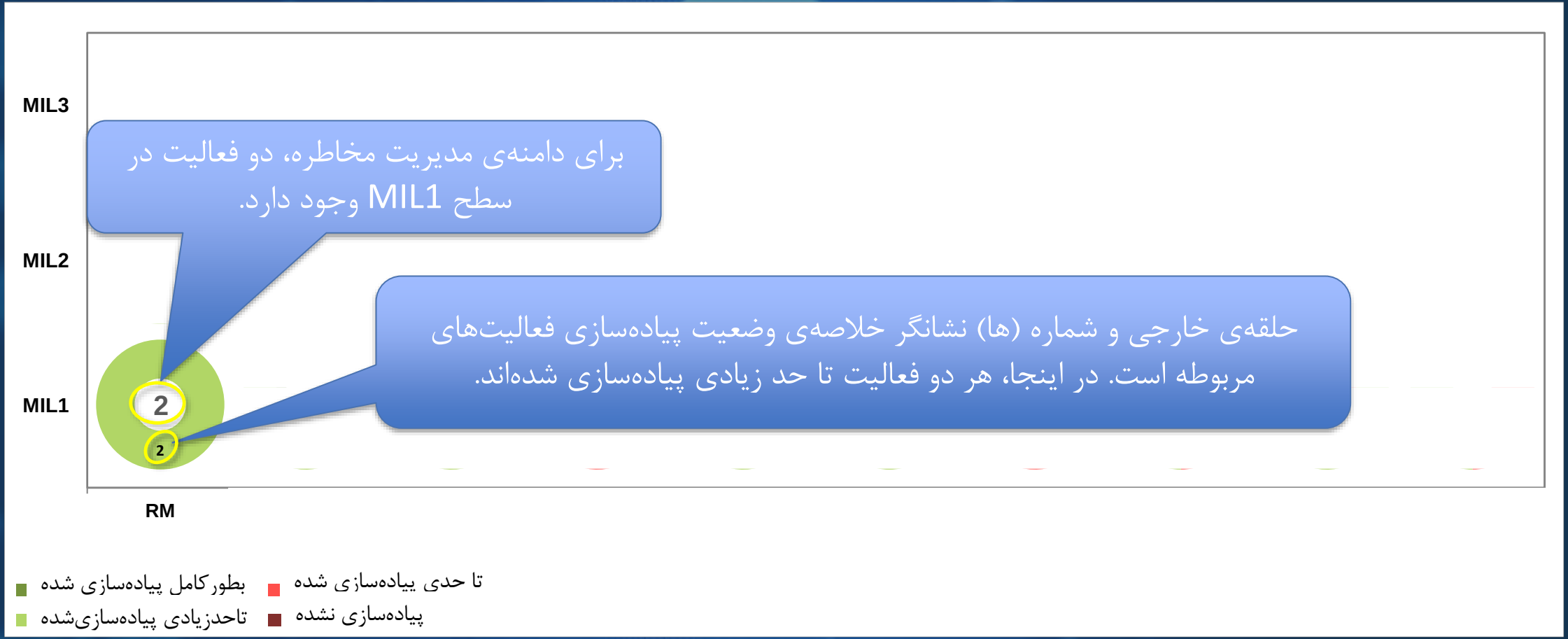
سامانه پایش و ارزیابی امنیت سایبری



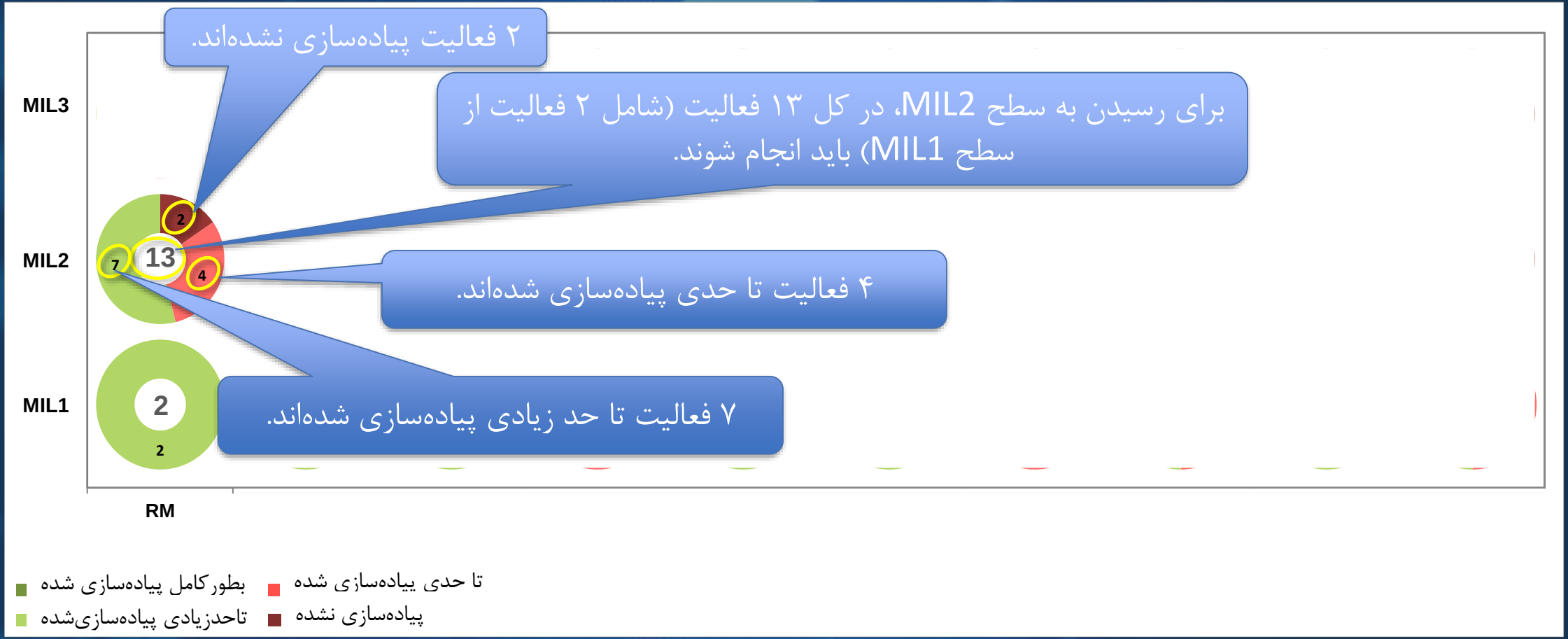
گزارش‌های متنوع مدیریتی



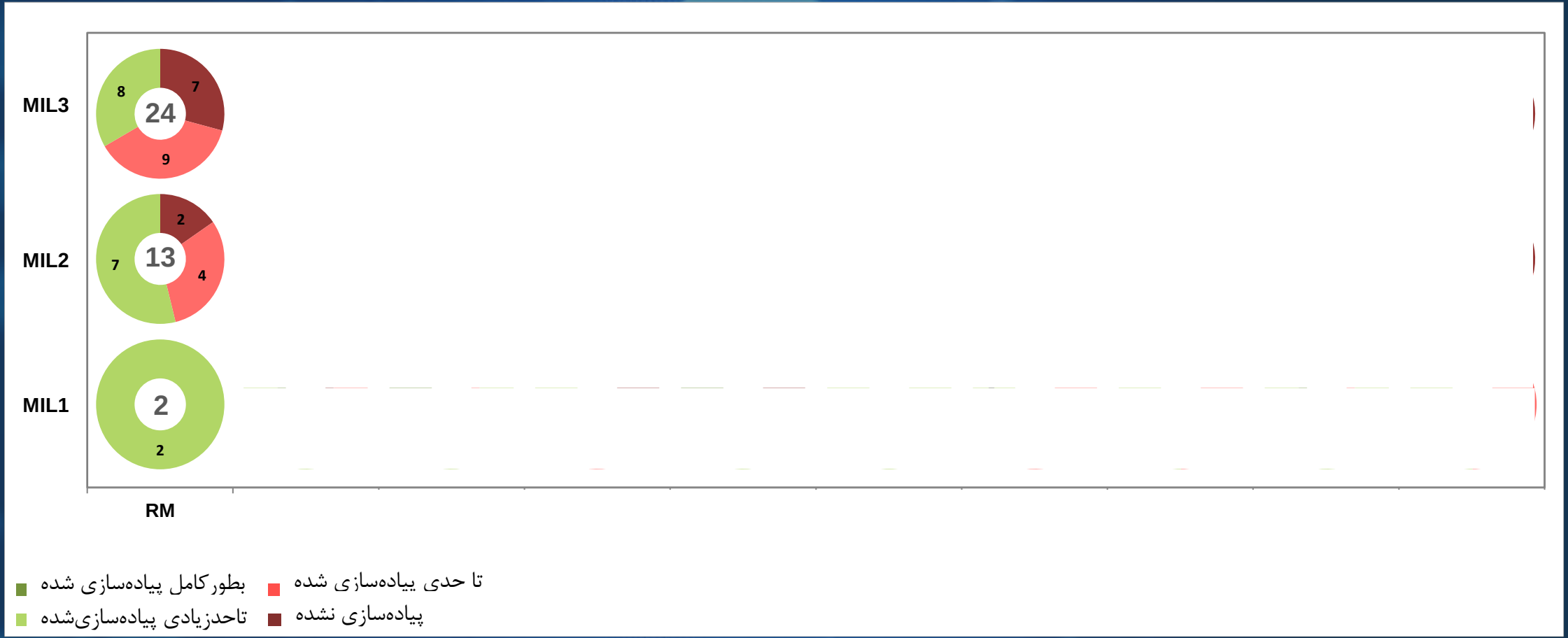
گزارش‌های متنوع مدیریتی



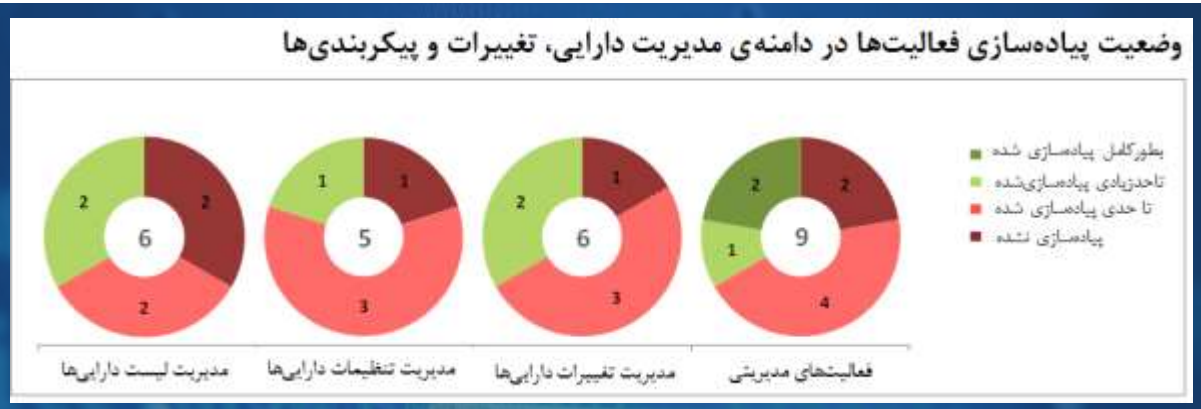
گزارش‌های متنوع مدیریتی

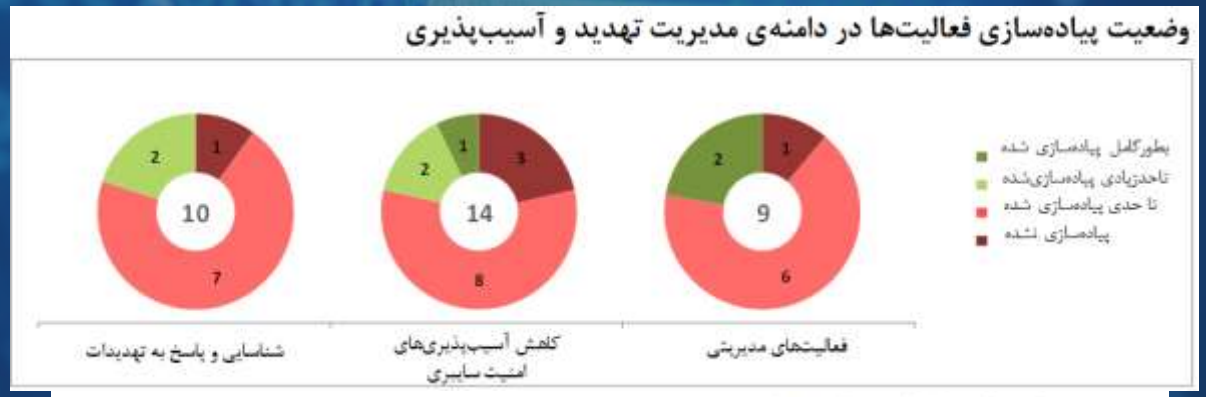


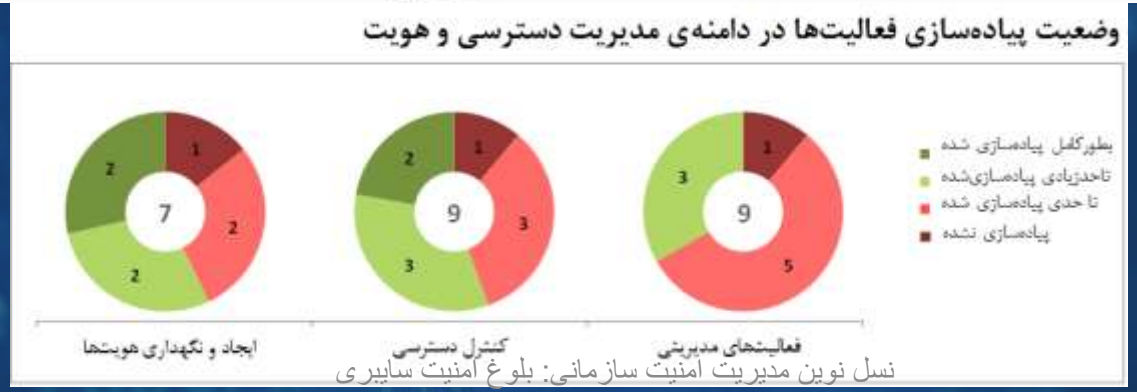
گزارش‌های متنوع مدیریتی



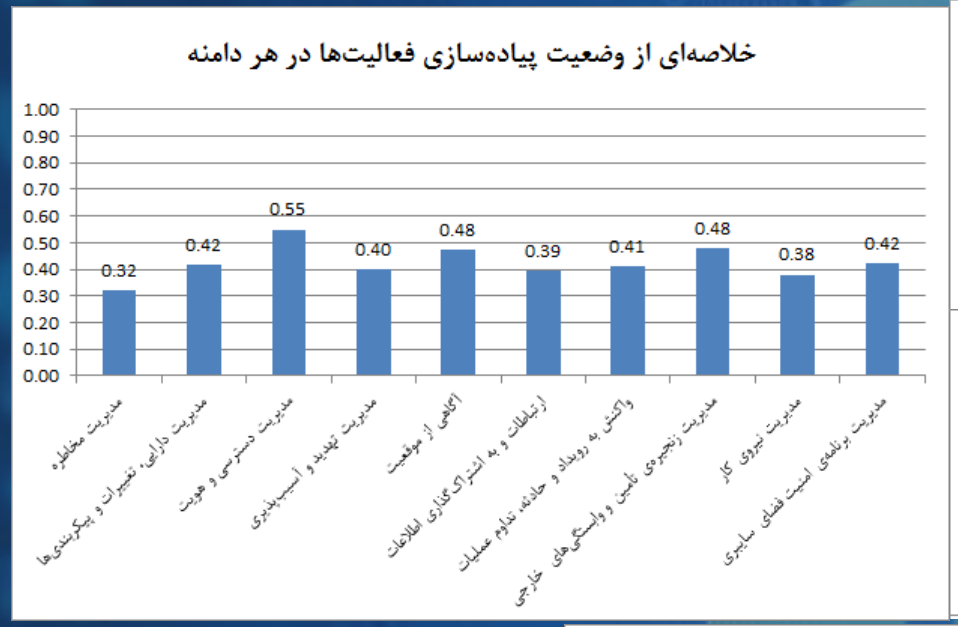
گزارش‌های متنوع مدیریتی

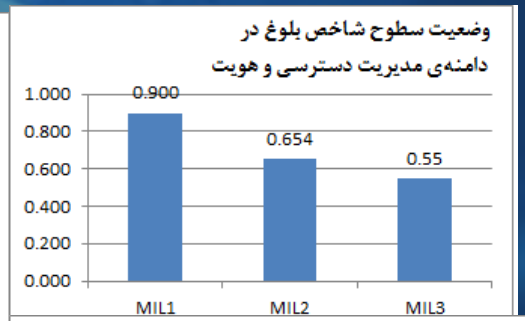


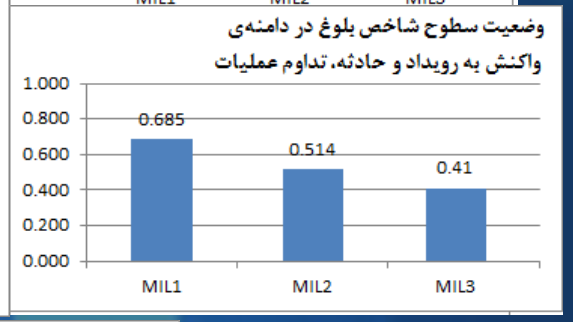


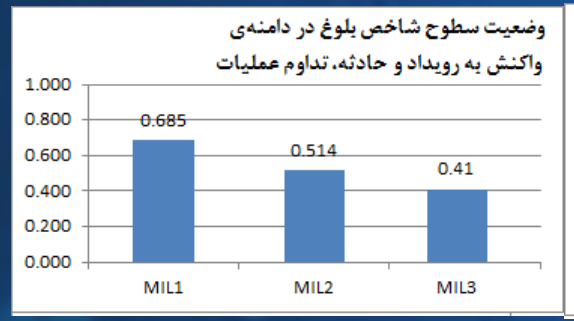


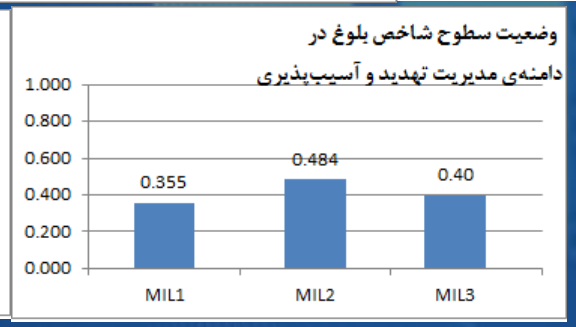
گزارش‌های متنوع مدیریتی











نسل نوین مدیریت امنیت سازمانی: بلوغ امنیت سایبری