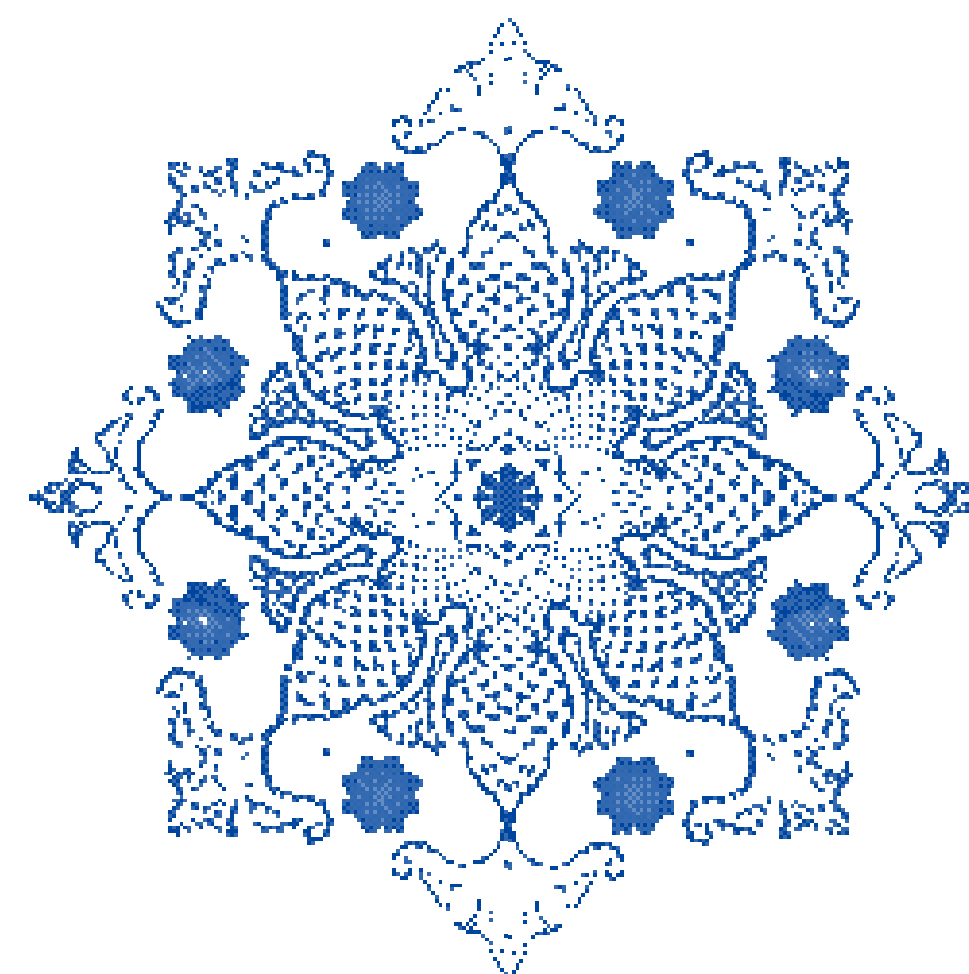




آشنایی با نحوه استقرار کنترل‌های نسخه ۸ چارچوب CIS

به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید. از روح خود در او
دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشکار فرو
فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.



محمد مهدی واعظی نژاد

مهندس امنیت فناوری اطلاعات
info@mvaezi.ir

فهرست مطالب

◀ مروری بر چالش‌ها و مسایل مرتبط با پیاده‌سازی چارچوب‌ها و استانداردهای امنیتی

◀ آشنایی با چارچوب CIS

◀ بررسی سطوح پیاده‌سازی ارایه شده و کنترل‌های هر کدام از سطوح

◀ نگاشت کنترل‌های پیشنهادی با استانداردهای امنیتی و اسناد بالادستی کشور

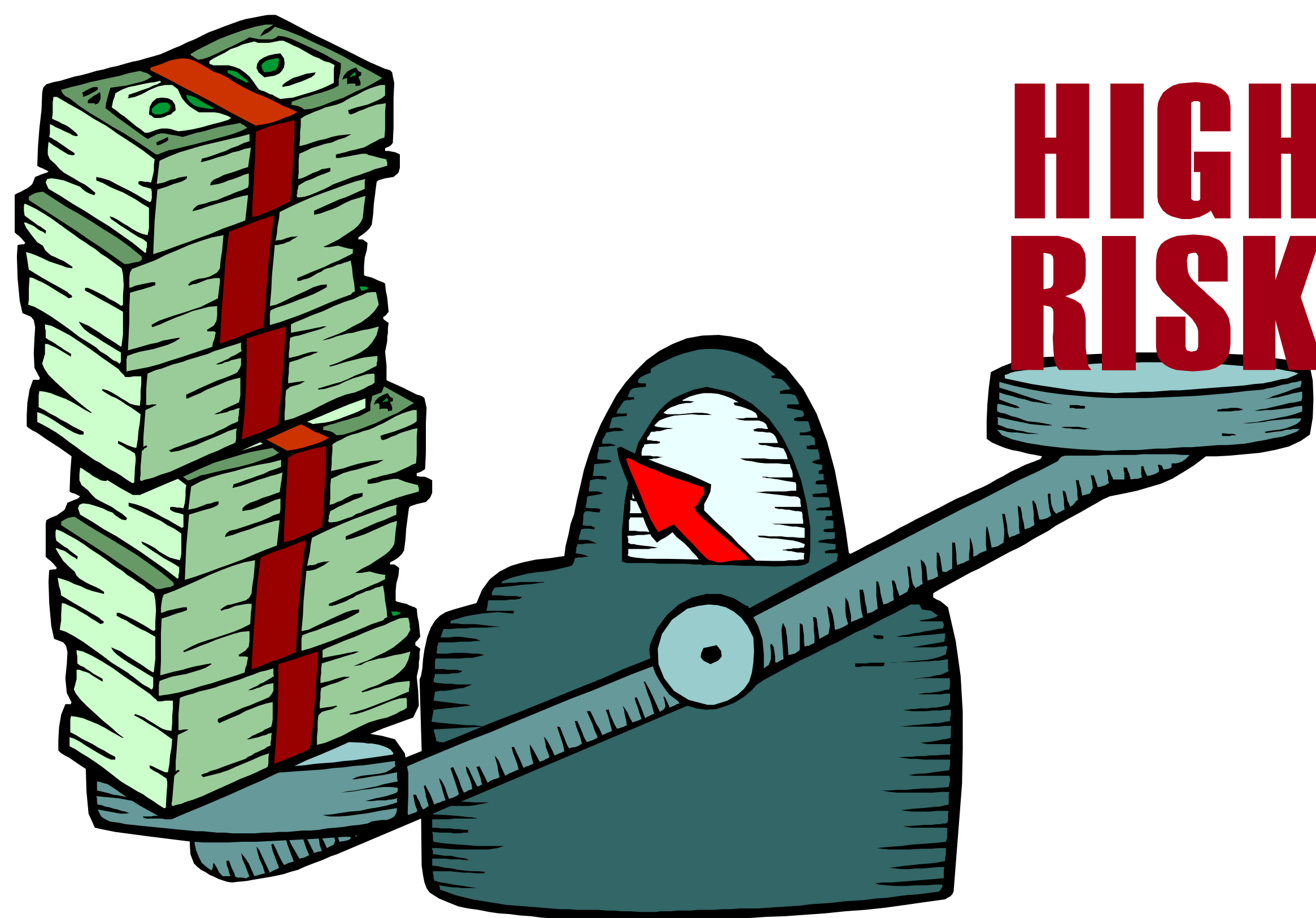
◀ بررسی ۱۸ سرفصل کنترلی و ساختار کنترل‌های پیشنهادی

◀ آشنایی با نحوه طراحی، پیاده‌سازی و استقرار کنترل‌ها در یک سازمان

چالش‌ها و مشکلات سازمانی

◀ چالش‌های مطرح در حوزه امنیت سایبری سازمانی

◀ بهترین راهکار امنیتی برای سازمان ما چیست؟



چالش‌ها و مشکلات سازمانی

◀ چالش‌های مطرح در حوزه امنیت سایبری سازمانی

◀ بهتر است کدام استاندارد یا چارچوب امنیتی را پیاده‌سازی کنیم؟



چالش‌ها و مشکلات سازمانی

◀ چالش‌های مطرح در حوزه امنیت سایبری سازمانی

◀ آیا استانداردهای امنیتی را پیاده‌سازی کنیم یا الزامات مراجع بالادستی کشور را؟



سازمان پدافند غیرعامل کشور



چالش‌ها و مشکلات سازمانی

◀ چالش‌های مطرح در حوزه امنیت سایبری سازمانی

◀ آیا با اجرای استانداردهای امنیتی و الزامات بالادستی، تمام مشکلات امنیتی ما برطرف می‌شود؟



شناخت؛ لازمه شروع هر اقدامی!

از درون من نجست اسرار من

هر کسی از ظن خود شد یار من



OOPS!

آشنایی با چارچوب CIS

◀ **ارایه چارچوب‌های کنترلی CIS با هدف: «کمک به سازمان‌ها برای تمرکز و شروع گام‌های حیاتی جهت دفاع از خودشان در برابر حملات واقعاً مهم»**

◀ **به اشتراک‌گذاری دیدگاه‌ها درباره حملات و مهاجمان**

◀ **شناسایی دلایل ریشه‌ای مشکلات و تبدیل این اطلاعات به توصیه‌های دفاعی کارآمد**

◀ **ایجاد و به اشتراک‌گذاری ابزارها، راهکارهای کمکی و روش‌های استفاده از این راهکارها برای حل مشکلات امنیتی**

◀ **نگاشت کنترل‌های CIS به چارچوب‌های قانونی و استاندارد، جهت اطمینان از همسو بودن با این استانداردهای قانونی و حفظ تمرکز و اولویت‌بخشی به آنها**

◀ **تشخیص موانع و مشکلات متداول (مثل ارزیابی‌های اولیه و نقشه راه پیاده‌سازی) و حل آنها به صورت گروهی**

آشنایی با چارچوب CIS

◀ چرا کنترل‌های CIS؟

1. استفاده از اطلاعات حمله برای دفاع و
وضع کنترل‌های امنیتی در این خصوص



آشنایی با چارچوب CIS

چرا کنترل‌های CIS؟

2. تمرکز بر مهمترین کنترل‌ها و اقدامات امنیتی



آشنایی با چارچوب CIS

چرا کنترل‌های CIS؟

3. عملی بودن و قابل اجرا بودن کنترل‌ها و اقدامات ذکر شده



آشنایی با چارچوب CIS

چرا کنترل‌های CIS؟

4. قابل ارزیابی بودن کنترل‌ها



آشنایی با چارچوب CIS

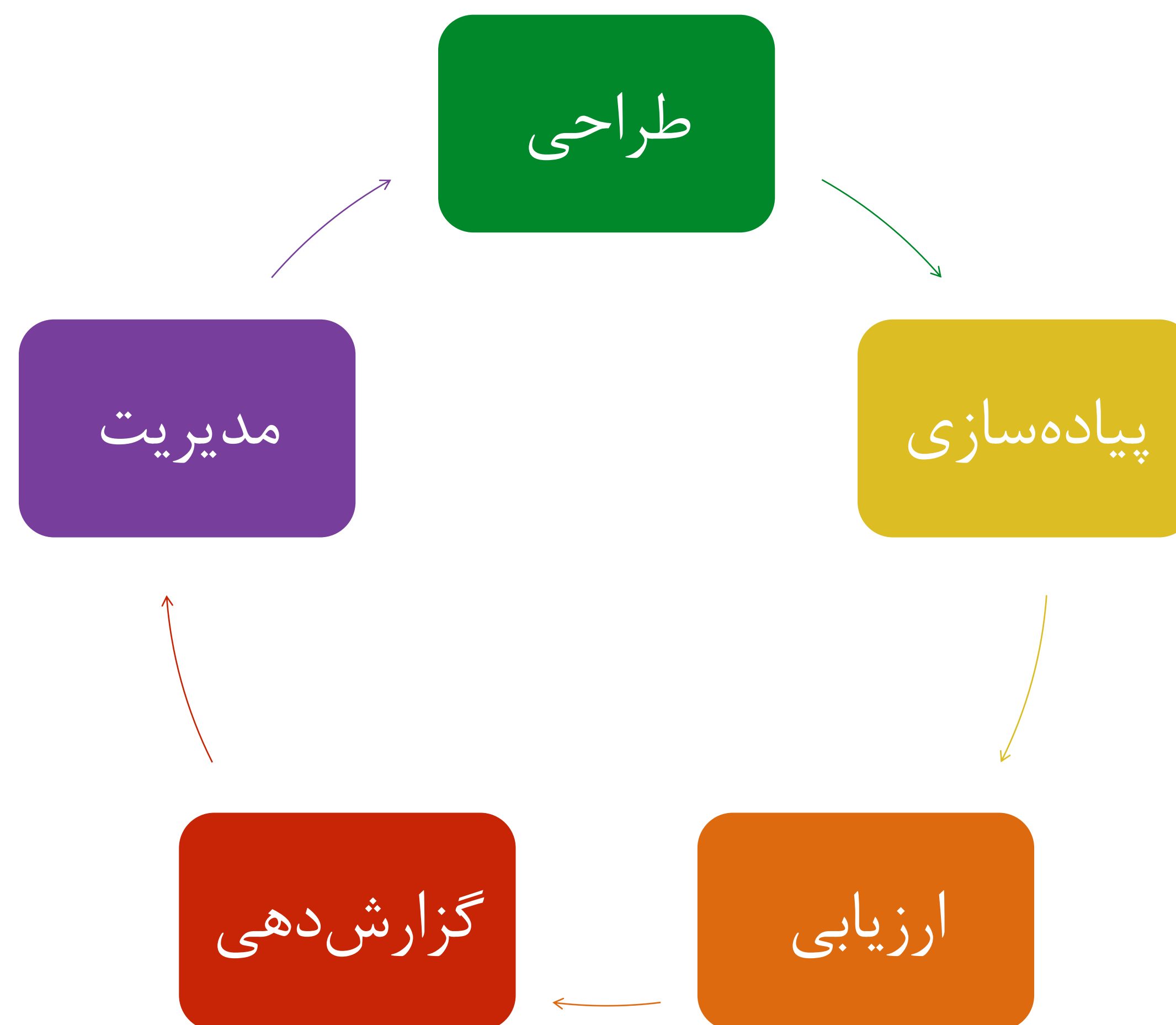
◀ چرا کنترل‌های CIS؟

5. هماهنگی با سایر استانداردهای امنیتی



آشنایی با چارچوب CIS

◀ مراحل اجرا و پیاده‌سازی کنترل‌های CIS:



ساختار کنترلی CIS

◀ دسته‌بندی تدابیر حفاظتی (۱۸ سرفصل کنترلی و ۱۵۳ کنترل امنیتی)

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7	CONTROL 03 Data Protection 14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12	CONTROL 05 Account Management 6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6	CONTROL 06 Access Control Management 8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7	CONTROL 08 Audit Log Management 12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7
CONTROL 10 Malware Defenses 7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7	CONTROL 11 Data Recovery 5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9	CONTROL 15 Service Provider Management 7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7
CONTROL 16 Applications Software Security 14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14	CONTROL 17 Incident Response Management 9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9	CONTROL 18 Penetration Testing 5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

ساختار کنترلی CIS



◀ ساختار سرفصل‌های کنترلی CIS:

1. مروری کوتاه بر هدف کنترلی
2. دلیل اهمیت کنترل ذکر شده
3. رویه‌ها و ابزارها اجرای آن کنترل
4. توضیح سازوکار حفاظتی

ساختار کنترلی CIS

◀ پیاده‌سازی کنترل‌های CIS بر اساس بلوغ امنیت سایبری هر سازمان



ساختار کنترلی CIS

◀ گروه‌های مختلف پیاده‌سازی (IMPLEMENTATION GROUP)

- ◀ مشتمل بر یکسری دسته‌بندی‌های ارزیابی شده برای سازمان‌ها
- ◀ امکان پیاده‌سازی آنها در سازمان‌های با شرایط ریسک و منابع مشابه
- ◀ ایجاد چشم‌انداز کلی بر کنترل‌های CIS، متناسب با هر نوع سازمانی

◀ طراحی هر IG بر اساس IG قبلی



گروه اول: بهداشت سایبری مقدماتی
(الزامی برای همه سازمان‌ها جهت مقابله با تهدیدات سایبری)



ساختار کنترلی CIS

◀ گروه اول (IG1)

- ◀ قابل پیاده‌سازی برای شرکت‌های کوچک تا متوسط، با سطح تخصص و منابع محدود افتا؛ به شدت آسیب‌پذیر در برابر وقفه‌های کسب‌وکاری
- ◀ تمرکز اصلی بر روی حفاظت از کارکنان سازمانی و دارایی‌های فاوا
- ◀ امکان اجرای کنترل‌ها با تخصص محدود امنیت سایبری این شرکت‌ها
- ◀ طراحی کنترل‌ها برای مقابله با حملات عمومی و غیرهدفمند
- ◀ تناسب کافی با سخت‌افزارها و نرم‌افزارهای تجاری مورد استفاده توسط این شرکت‌ها

56
Control



ساختار کنترلی CIS

◀ گروه دوم (IG2)

◀ قابلیت پیاده‌سازی کنترل‌ها برای سازمان‌های دارای:

◀ کارکنانی با مسئولیت مدیریت و حفاظت از زیرساخت فاوا؛ با توانایی کافی جهت حفظ تداوم کسب‌وکارهای عملیاتی خود

◀ بخش‌های سازمانی دارای سطوح ریسک متفاوت (بر اساس هدف و نوع عملکرد)

◀ طراحی کنترل‌ها بر اساس کمک به تیم‌های امنیتی جهت مقابله با پیچیدگی‌های روزافزون عملیاتی

◀ نیاز به فناوری سازمانی و تخصص ویژه برای پیاده‌سازی درست بعضی از این کنترل‌ها



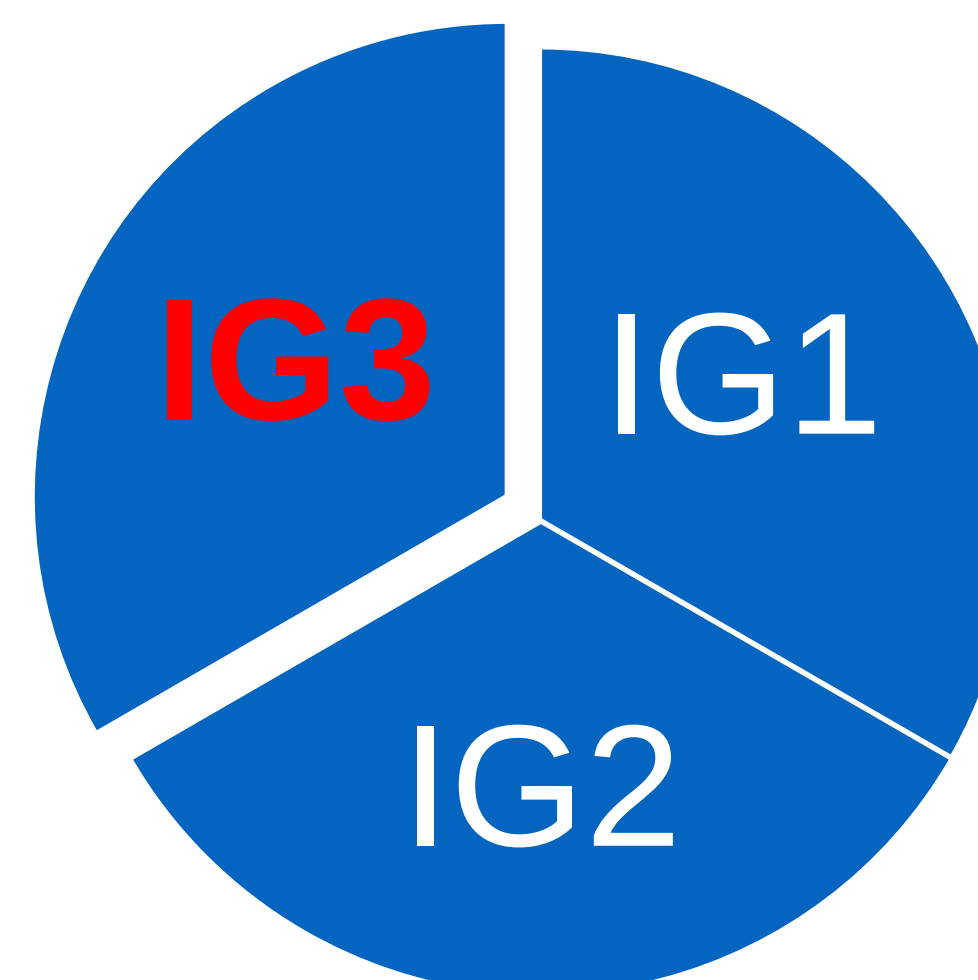
ساختار کنترلی CIS

◀ گروه سوم (IG3)

- ◀ امکان پیاده‌سازی کنترل‌ها برای سازمان‌های دارای کارشناسان امنیتی خبره و متخصص در حوزه‌های مختلف امنیت سایبری (مثل مدیریت مخاطره، آزمون نفوذپذیری و امنیت برنامه‌های کاربردی)
- ◀ طراحی کنترل‌ها برای سازمان‌های با اطلاعات یا عملکردهای حیاتی و تحت نظر نهادهای بالاسری و قانونی که حملات موفق بر ضد آنها می‌تواند آسیب جدی به رفاه عمومی وارد کند.
- ◀ گزینش کنترل‌ها جهت تضمین بالای دسترسی‌پذیری یکسری از خدمات و نیز حفظ محرمانگی و جامعیت داده‌های حساس سازمانی
- ◀ انتخاب کنترل‌ها جهت ممانعت از اجرای حملات هدفمند از سوی مهاجمان پیشرفته و کاهش شدت پیامد حملات روز صفر

56+74+23

Control



نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

SPECIAL PUBLICATION 800-171
REVISION 1

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN
NONFEDERAL SYSTEMS AND ORGANIZATIONS

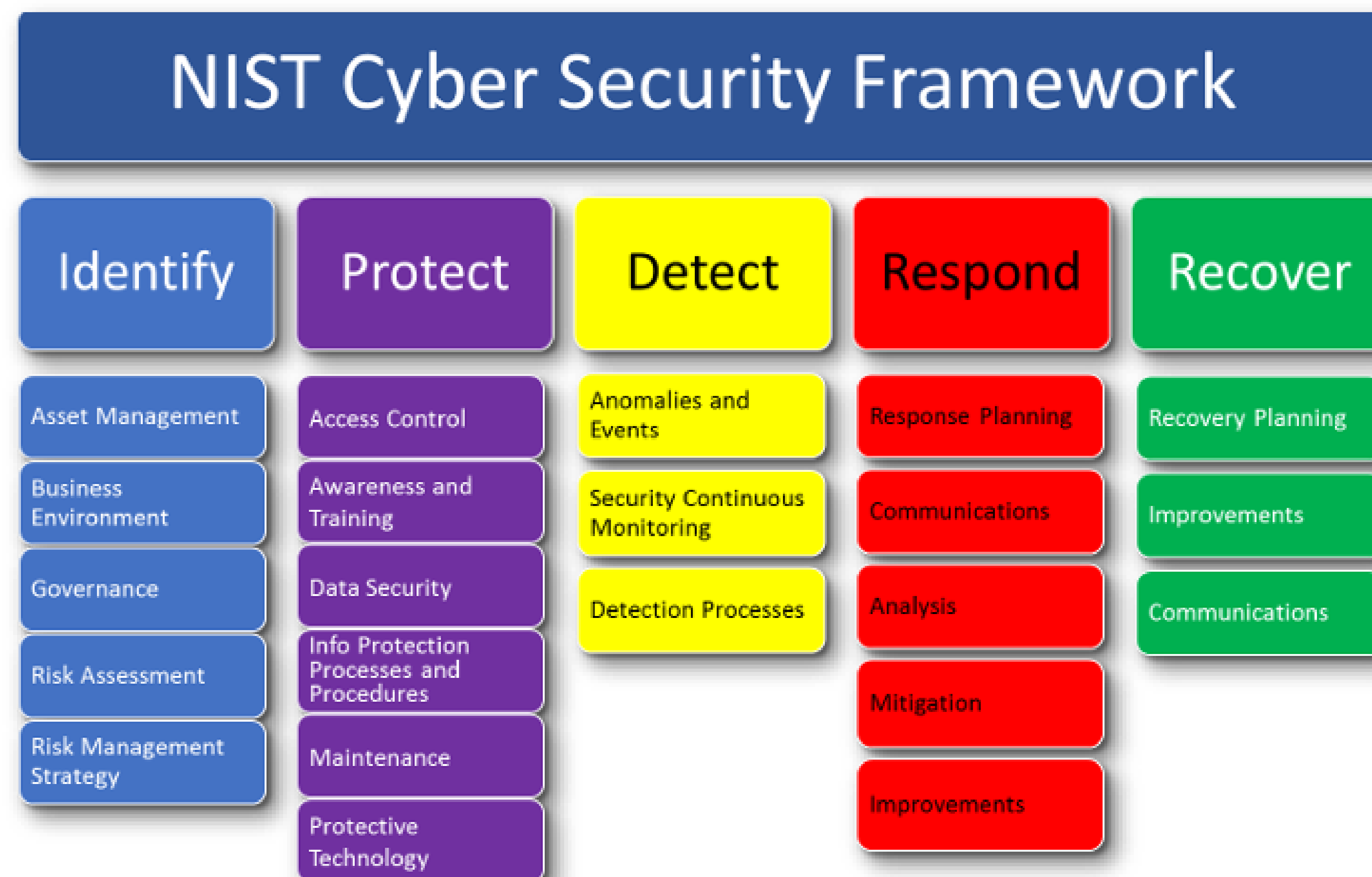
Table of Contents

CHAPTER ONE	INTRODUCTION	1
1.1	PURPOSE AND APPLICABILITY	2
1.2	TARGET AUDIENCE	4
1.3	ORGANIZATION OF THIS SPECIAL PUBLICATION	4
CHAPTER TWO	THE FUNDAMENTALS	5
2.1	BASIC ASSUMPTIONS	5
2.2	DEVELOPMENT OF SECURITY REQUIREMENTS	6
CHAPTER THREE	THE REQUIREMENTS	9
3.1	ACCESS CONTROL	9
3.2	AWARENESS AND TRAINING	10
3.3	AUDIT AND ACCOUNTABILITY	10
3.4	CONFIGURATION MANAGEMENT	11
3.5	IDENTIFICATION AND AUTHENTICATION	11
3.6	INCIDENT RESPONSE	12
3.7	MAINTENANCE	12
3.8	MEDIA PROTECTION	13
3.9	PERSONNEL SECURITY	13
3.10	PHYSICAL PROTECTION	13
3.11	RISK ASSESSMENT	14
3.12	SECURITY ASSESSMENT	14
3.13	SYSTEM AND COMMUNICATIONS PROTECTION	14
3.14	SYSTEM AND INFORMATION INTEGRITY	15
APPENDIX A	REFERENCES	17
APPENDIX B	GLOSSARY	19
APPENDIX C	ACRONYMS	27
APPENDIX D	MAPPING TABLES	28
APPENDIX E	TAILORING CRITERIA	51
APPENDIX F	DISCUSSION	69

نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

NIST CSF ◀

شناسه نقش	نقش	شناسه دسته‌بندی	دسته‌بندی
ID	شناسایی	ID.AM	مدیریت دارایی‌ها
		ID.BE	محیط کسب و کار
		ID.GV	وضع ضوابط
		ID.RA	ارزیابی مخاطرات
		ID.RM	مدیریت مخاطرات
PR	حفاظت	PR.AC	کنترل دسترسی
		PR.AT	آموزش و آگاهی‌رسانی
		PR.DS	امنیت داده‌ها
		PR.IP	فرایندها و سازوکارهای حفاظت از اطلاعات
		PR.MA	تعمیر و نگهداری
DE	کشف	PR.PT	فناوری‌های حفاظتی
		DE.AE	ناهنجاری‌ها و حوادث
		DE.CM	نظارت امنیتی پیوسته
		DE.DP	فرایندهای کشف
		RS.RP	برنامه‌ریزی پاسخ
RS	پاسخ	RS.CO	ارتباطات
		RS.AN	تجزیه و تحلیل
		RS.MI	کاهش اثرات
		RS.IM	بهبود و توسعه
		RC.RP	برنامه‌ریزی بازیابی
RC	بازیابی	RC.IM	بهبود و توسعه
		RC.CO	ارتباطات



نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

◀ سطوح پیاده‌سازی چارچوب NIST CSF:

- ◀ هر سطح، بیانگر نوع نگاه سازمان به **رخداد‌های افتا و فرایندهای مدیریت آنها** و همچنین یوندی تکاملی برای فعالیت‌های افتا در سازمان
- ◀ افزایش سخت‌گیری و پیچیدگی هر سطح نسبت به سطح قبلی در زمینه اقدامات **مدیریت مخاطرات افتا**
- ◀ انتخاب **سطح مطلوب** توسط خود سازمان‌ها
- ◀ حرکت به سطوح بالاتر تنها در صورت کاهش مخاطرات و توجیه اقتصادی
- ◀ موفقیت چارچوب بر اساس میزان **دستیابی به خروجی‌های تعیین شده در قالب هدف** و نه بر اساس سطوح پیاده‌سازی

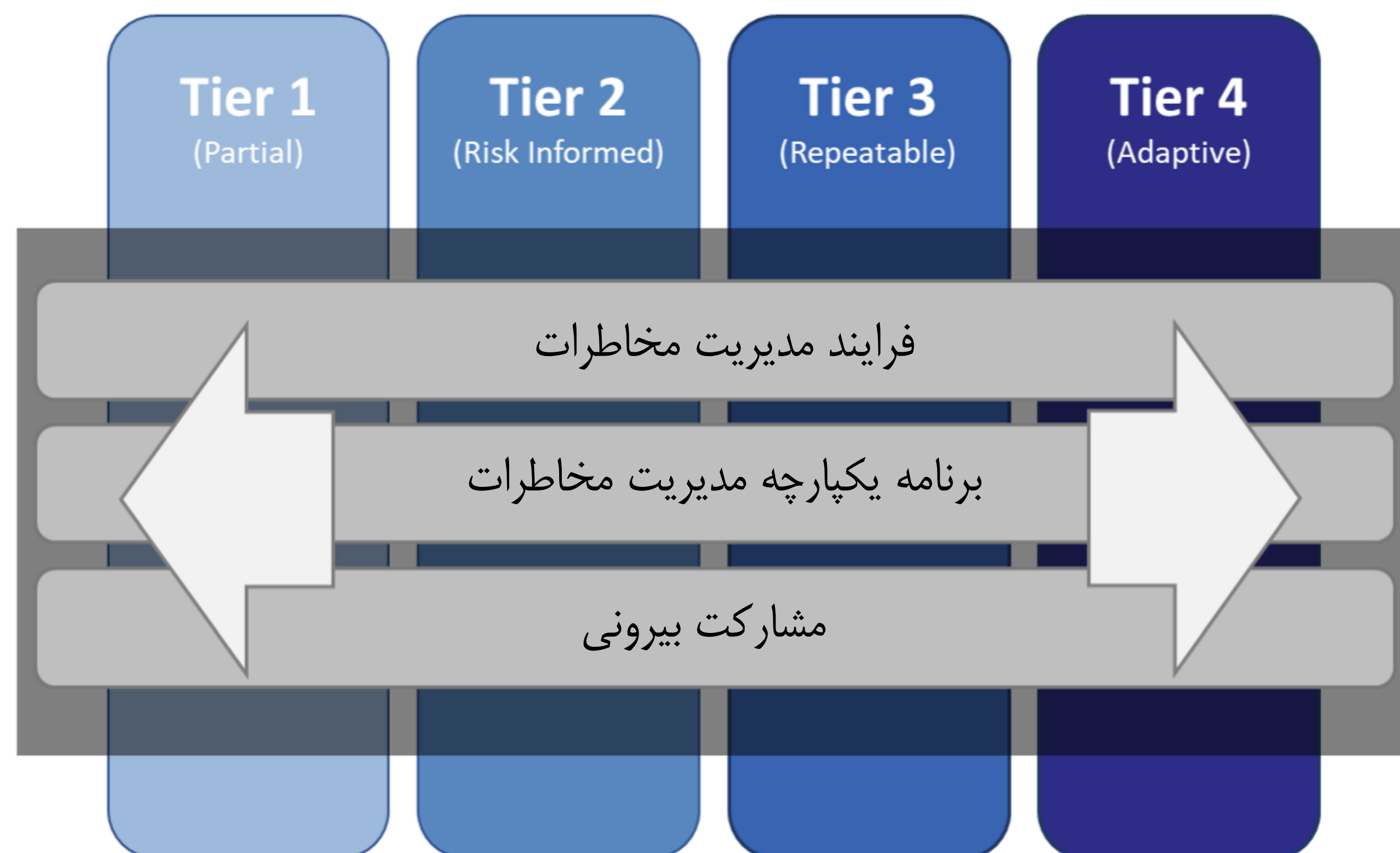
سطوح پیاده‌سازی، نمایش‌دهنده سطح بلوغ امنیتی سازمان نیستند!

نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

◀ سطوح پیاده‌سازی چارچوب NIST CSF:

◀ سطوح مختلف پیاده‌سازی:

1. نسبی (Partial)
2. آگاه از مخاطرات (Risk Informed)
3. تکرارپذیر (Repeatative)
4. انطباقی (Adaptive)



نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

◀ استاندارد ISO/IEC 27001:2022

◀ متشکل از بخش سیستمی (دارای ۷ بند، از بند ۴ تا ۱۰) و کنترل‌های امنیتی (دارای ۴ سرفصل کنترلی (فنی، فردی، فیزیکی و سازمانی) و ۹۳ کنترل امنیتی)

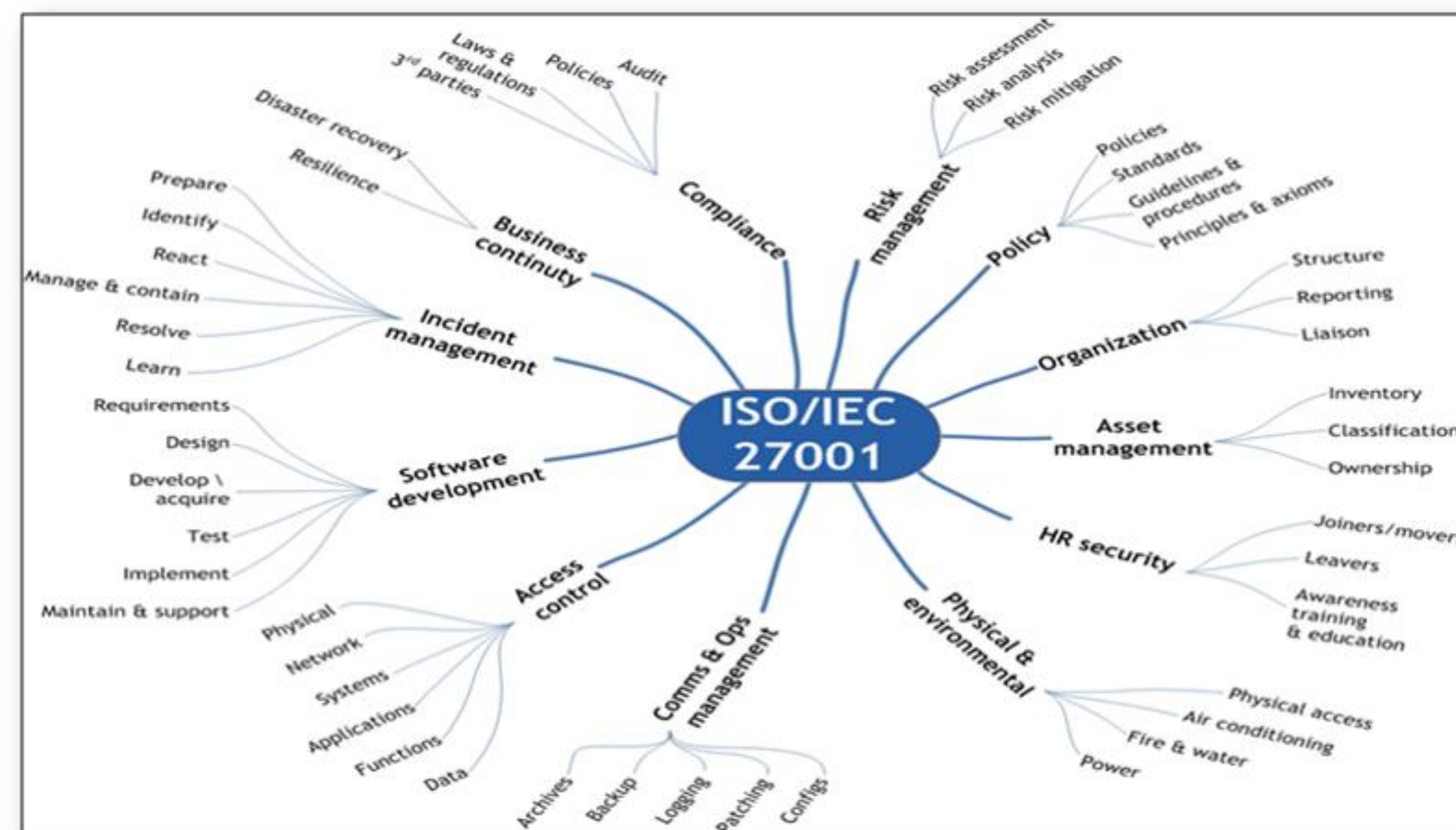
INTERNATIONAL
STANDARD

ISO/IEC
27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

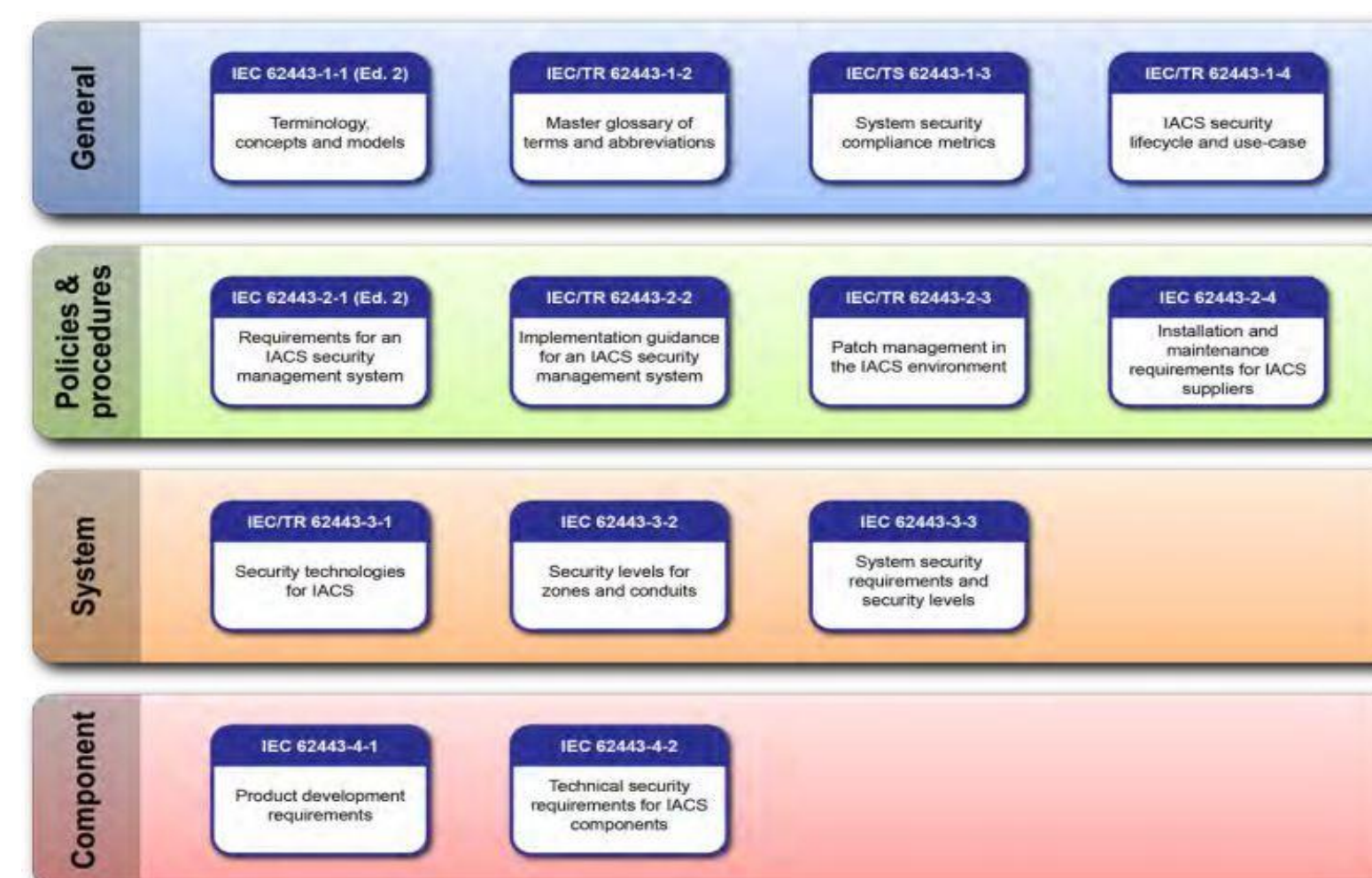


نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

◀ استاندارد ISA/IEC 62443

◀ شامل:

1. عمومی
2. خطامشی‌ها و رویه‌ها
3. سیستم‌ها
4. اجزای تشکیل‌دهنده سازمان‌یافته



مقایسه کنترل‌های CIS با اسناد بالاسری کشور

◀ طرح کلان امن‌سازی زیرساخت حیاتی مرکز افتای ریاست جمهوری

◀ کنترل‌های ۹ گانه افتا (الزامات طرح امن‌سازی):

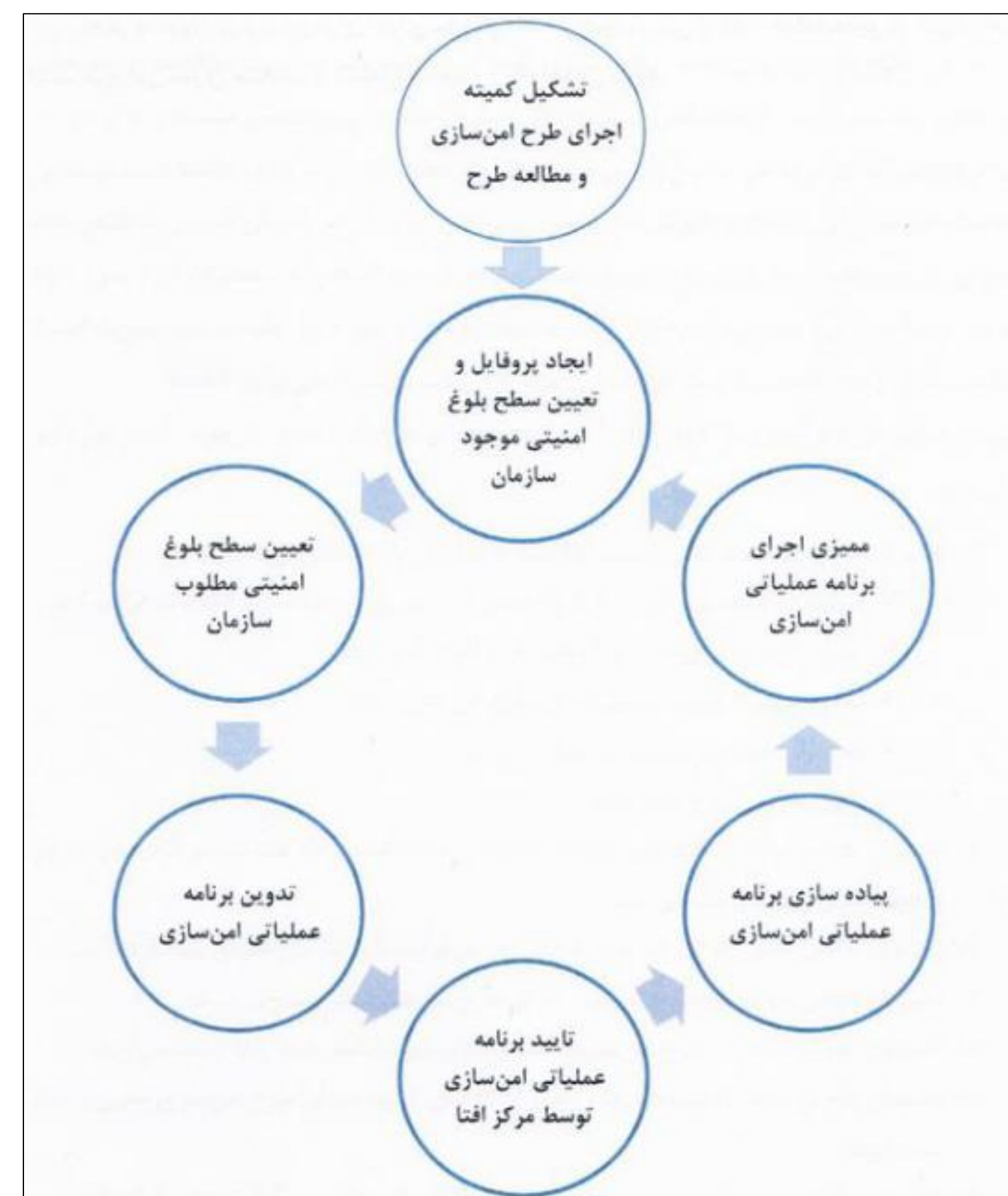
1. مدیریت مخاطرات
2. پایش و کنترل سایبری
3. مدیریت حوادث سایبری (IT و OT)
4. مدیریت تهدیدات بدافزاری
5. مدیریت تداوم کسب‌وکار
6. زیرساخت محرمانگی و استنادپذیری
7. مدیریت هویت و دسترسی
8. مدیریت زنجیره تأمین
9. آموزش و فرهنگ‌سازی



طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری

نسخه ۲۰ - اسفندماه ۹۷

نقشه راه و مدل بلوغ طرح کلان امن سازی زیرساخت حیاتی مرکز افتای ریاست جمهوری



مقایسه کنترل‌های CIS با اسناد بالاسری کشور

◀ سند راهبردی پدافند سایبری کشور

◀ اصول حاکم بر حوزه پدافند سایبری کشور:

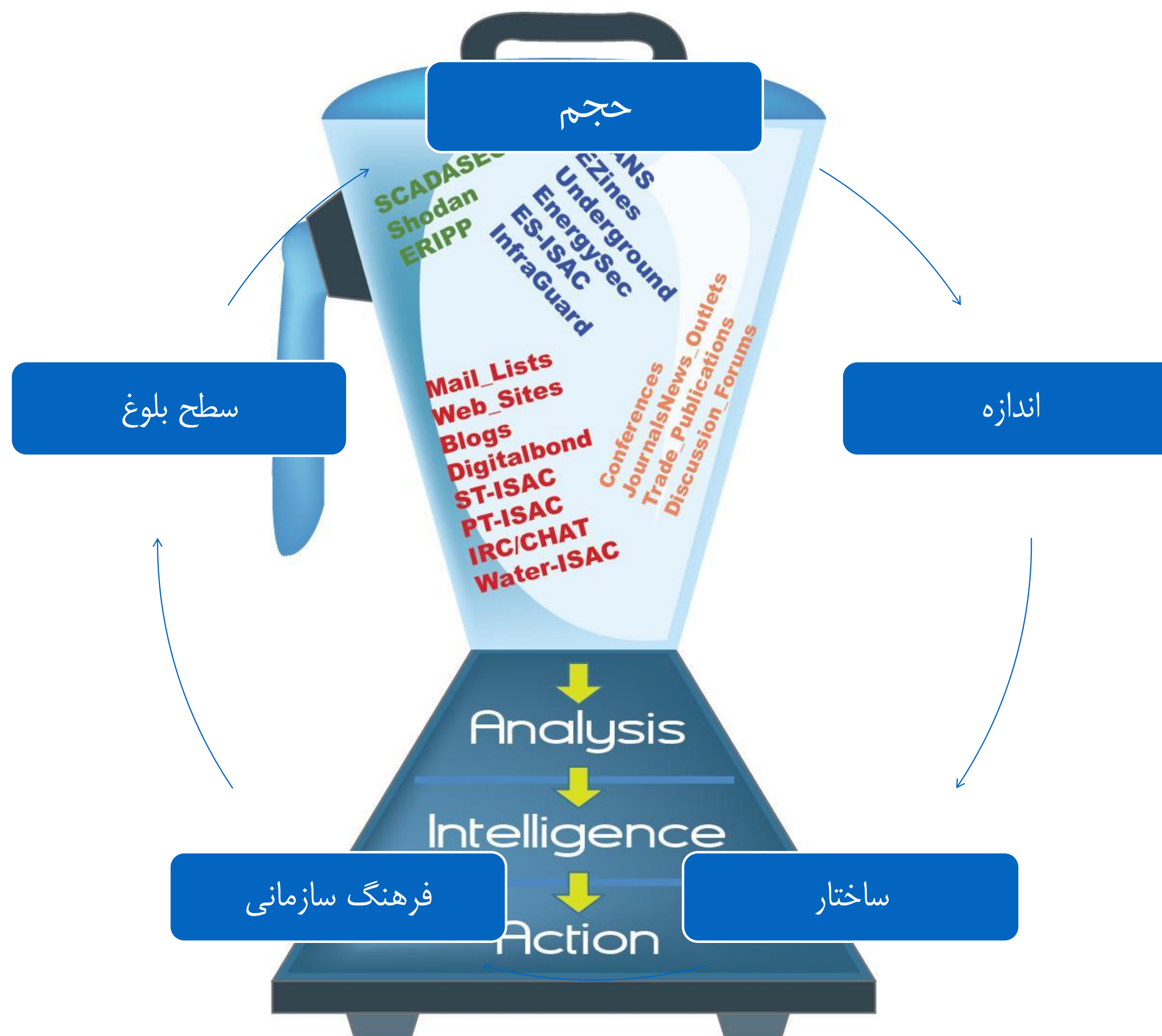
1. مصون سازی و پایداری
2. وحدت مدیریت
3. بازدارندگی
4. حفظ آمادگی
5. پیش بینی در تهدیدشناسی
6. اقتصادی سازی
7. اشراف اطلاعاتی
8. دیپلماسی فعال
9. اقتدار درون‌زا



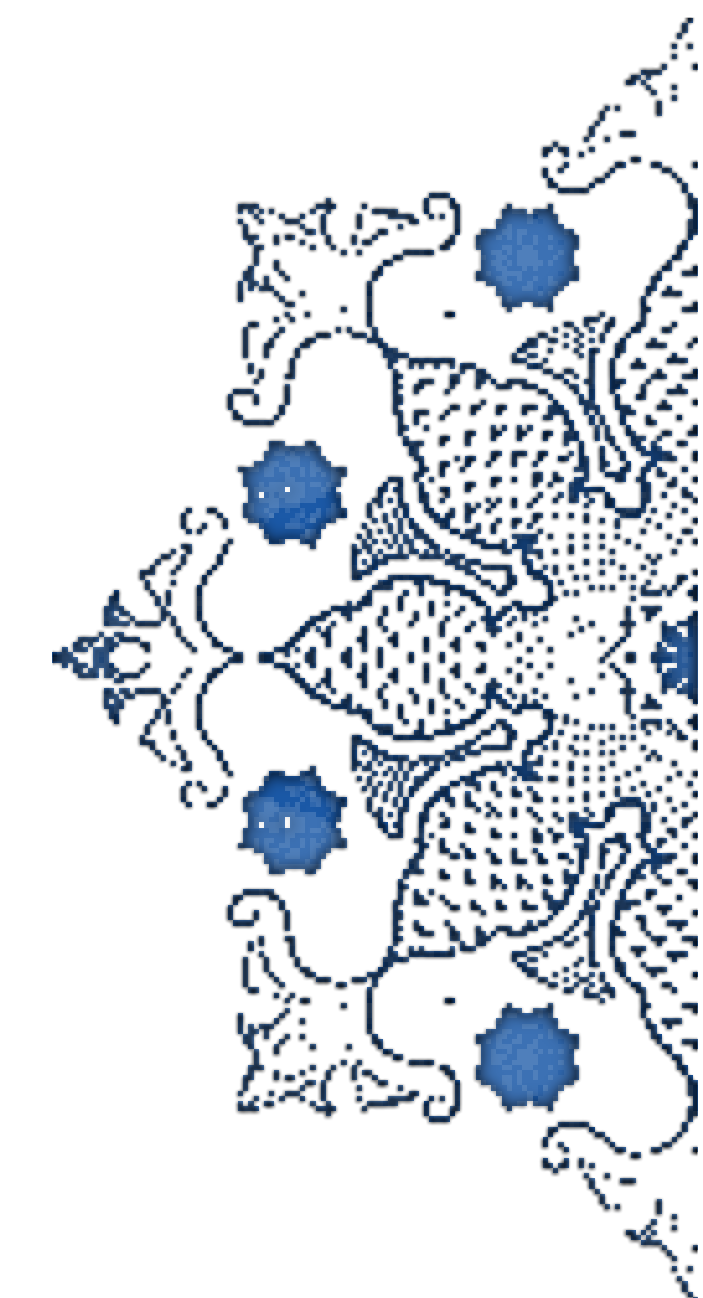
سازمان پدافند غیرعامل کشور

شماره: ۱۶۰/۱/۵۸۵ تاریخ: ۱۳۹۴/۰۳/۲۱ پوست: ندارد	فرماندهی کل قوا کمیته ملی پدافند غیرعامل کشور
تصویب نامه وزیر محترم کشور وزیر محترم دفاع و پشتیبانی نیروهای مسلح معاون محترم رئیس جمهور و رئیس سازمان مدیریت و برنامه ریزی کشور رئیس محترم کمیسیون امنیت ملی و سیاست خارجی مجلس شورای اسلامی سردار رئیس محترم ارکان و امور مسلح مشترک نیروهای مسلح سردار رئیس محترم سازمان پدافند غیرعامل کشور سلام علیکم با استحضار بر مبنای آراء و نظرات محترم و کمیته دائمی (شورای عالی) پدافند غیرعامل کشور در جلسه مورخ ۱۳۹۴/۲/۲۹ به استناد ماده (۸) اساسنامه سازمان پدافند غیرعامل کشور مصوب تمام محترم ریاست جمهوری و فرماندهی کل قوا و اعلامی، «سند راهبردی پدافند سایبری کشور» پیشنهادی سازمان پدافند غیرعامل کشور، موضوع بند ۱ ماده ۹ اساسنامه مذکور را بررسی و به شرح زیر تصویب نمود:	سند راهبردی پدافند سایبری کشور
ماده ۱: تعاریف و اصطلاحات (۱) فضای سایبری: به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تهیه‌شده (جاگذاری شده)، کنترل‌کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهربرداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تهیه شده باشد. (۲) سرمایه ملی سایبری: بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مهم و تعیین‌کننده داشته باشند، سرمایه ملی سایبری نامیده می‌شود. (۳) آسیب‌پذیری سایبری: به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی سایبری، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال شدن تهدیدات داخلی و خارجی به منظور تهاجم و یا جنگ سایبری را داشته باشد، اخلاق می‌گردد.	پیوسته ۱ از ۸ صفحه

و در نهایت؛ آنچه که باید انجام دهیم ...



تهدیدها
منابع سازمانی
محدودیت های زمانی



با تشکر از توجه شما