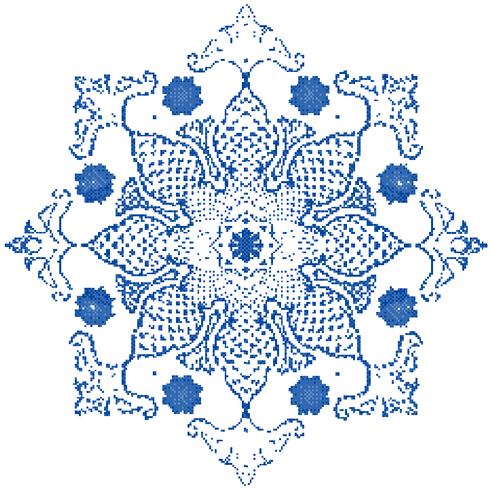
آشنایی با نحوه استقرار کنترل‌های نسخه ۸ چارچوب CIS

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



محمد مهدی واعظی نژاد

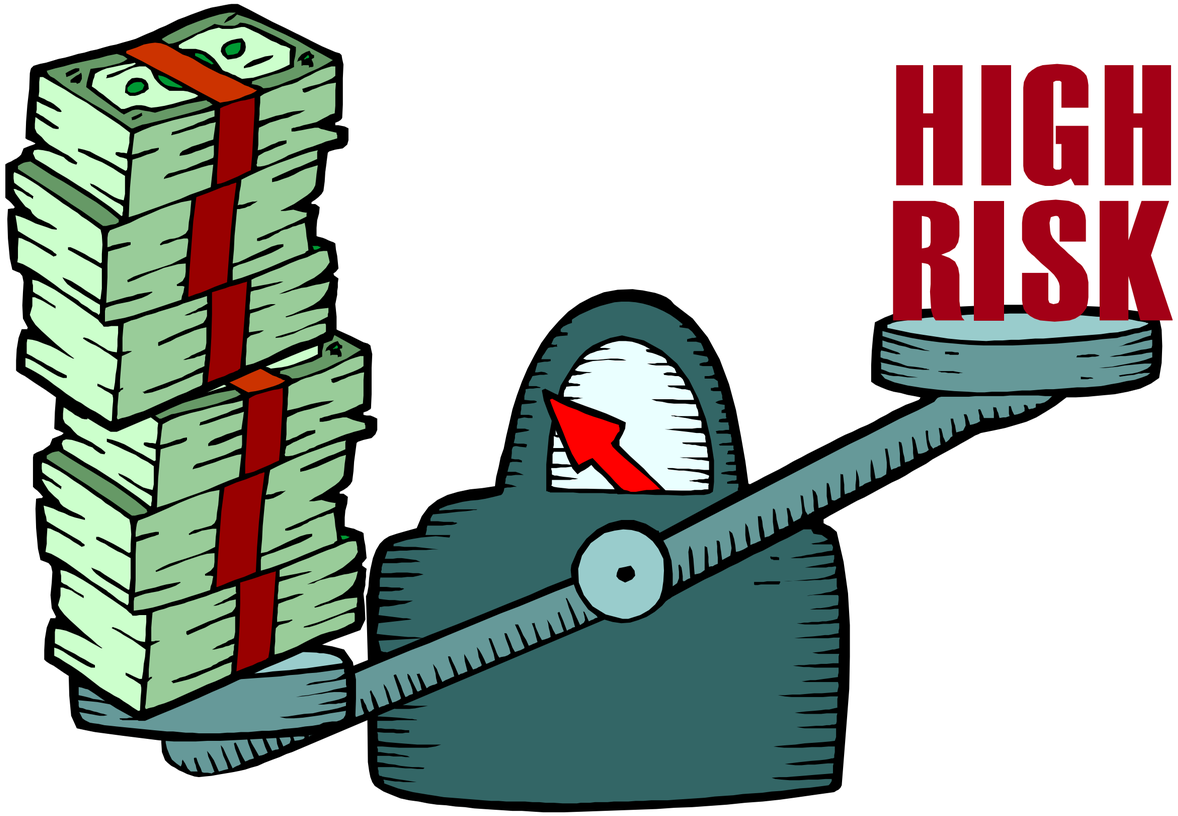
مهندس امنیت فناوری اطلاعات

info@mvaezi.ir

فهرست مطالب

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؟

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!

هر کسی از ظن خود شد یار من از درون من نجست اسرار 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**

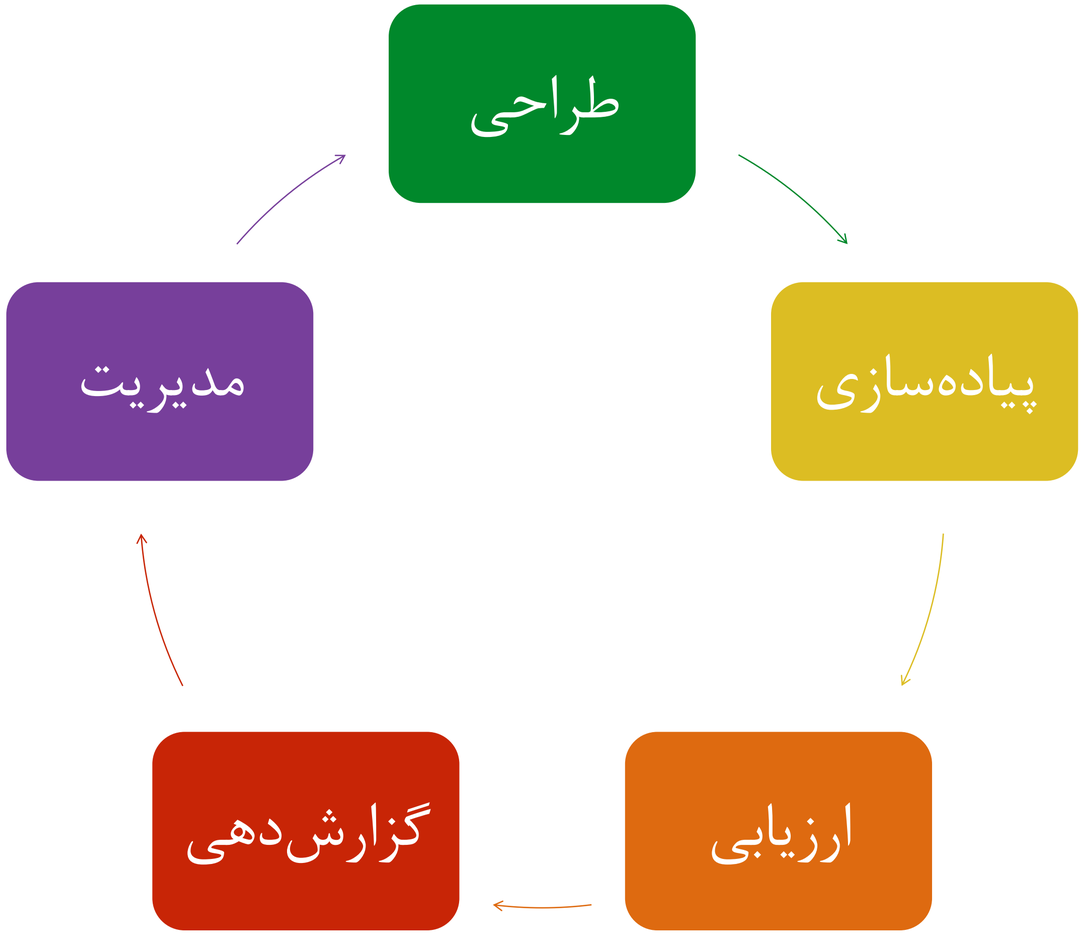
آشنایی با چارچوب CIS

◄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)

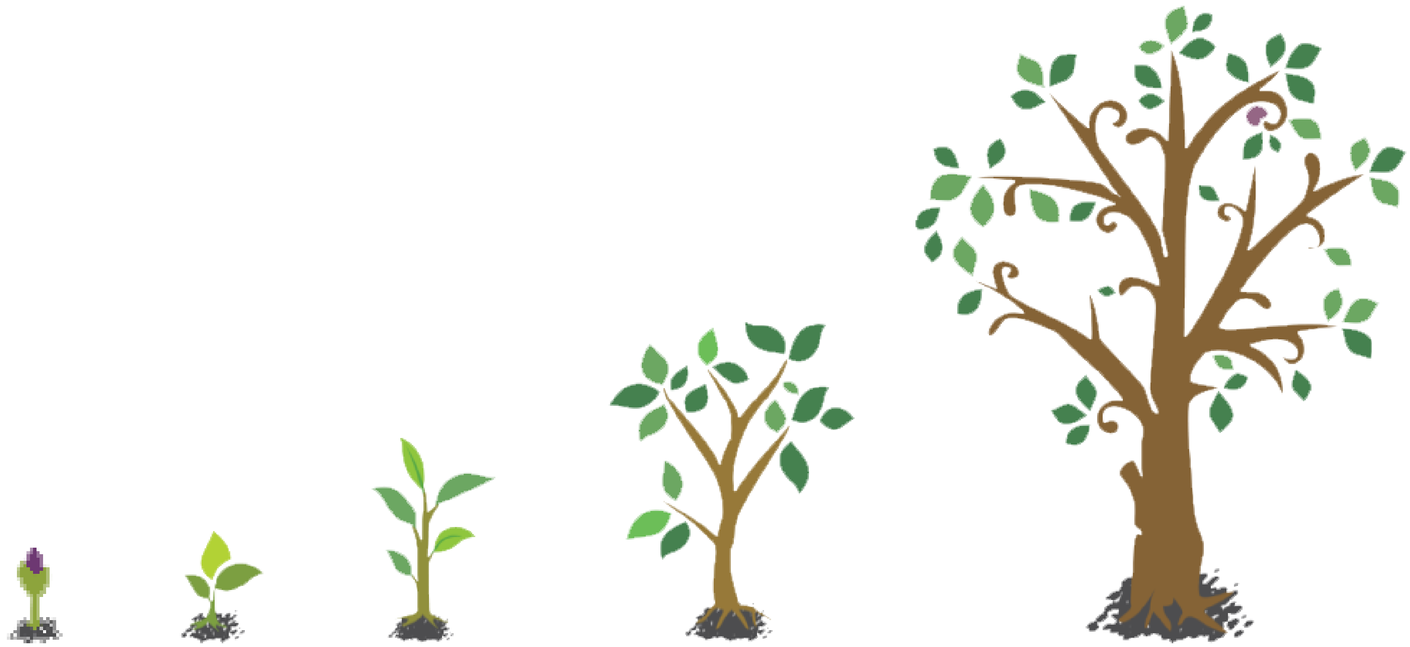
ساختار کنترلی CIS

- 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



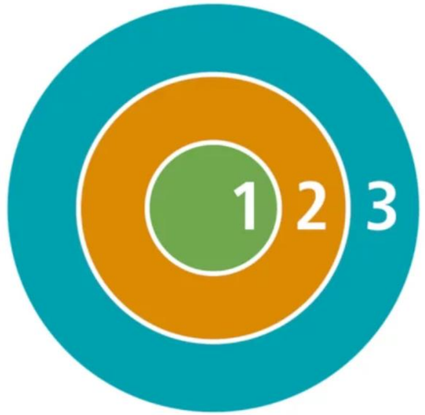
ساختار کنترلی CIS

- 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)

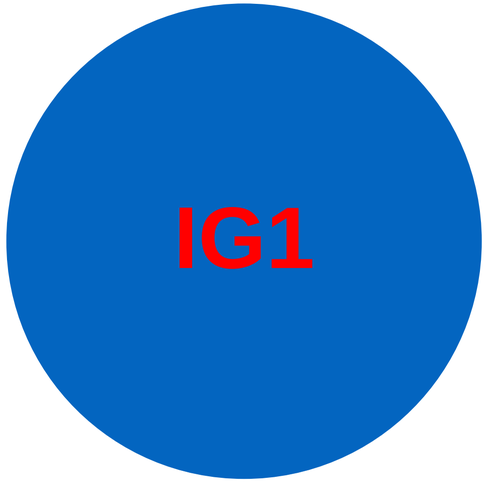


ساختار کنترلی CIS

- 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 شرکت ها
  - 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

56+ 74

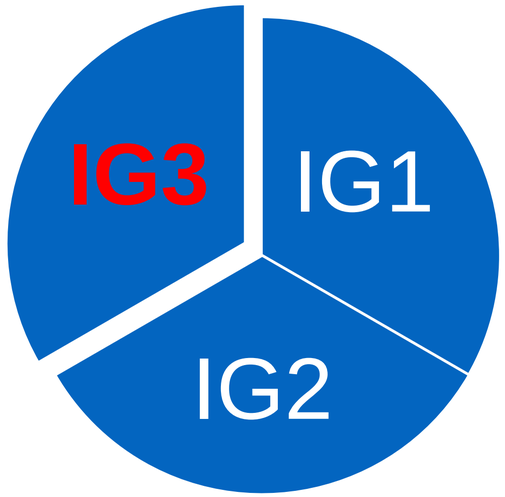
Control

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 دسترس‌پذیری 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

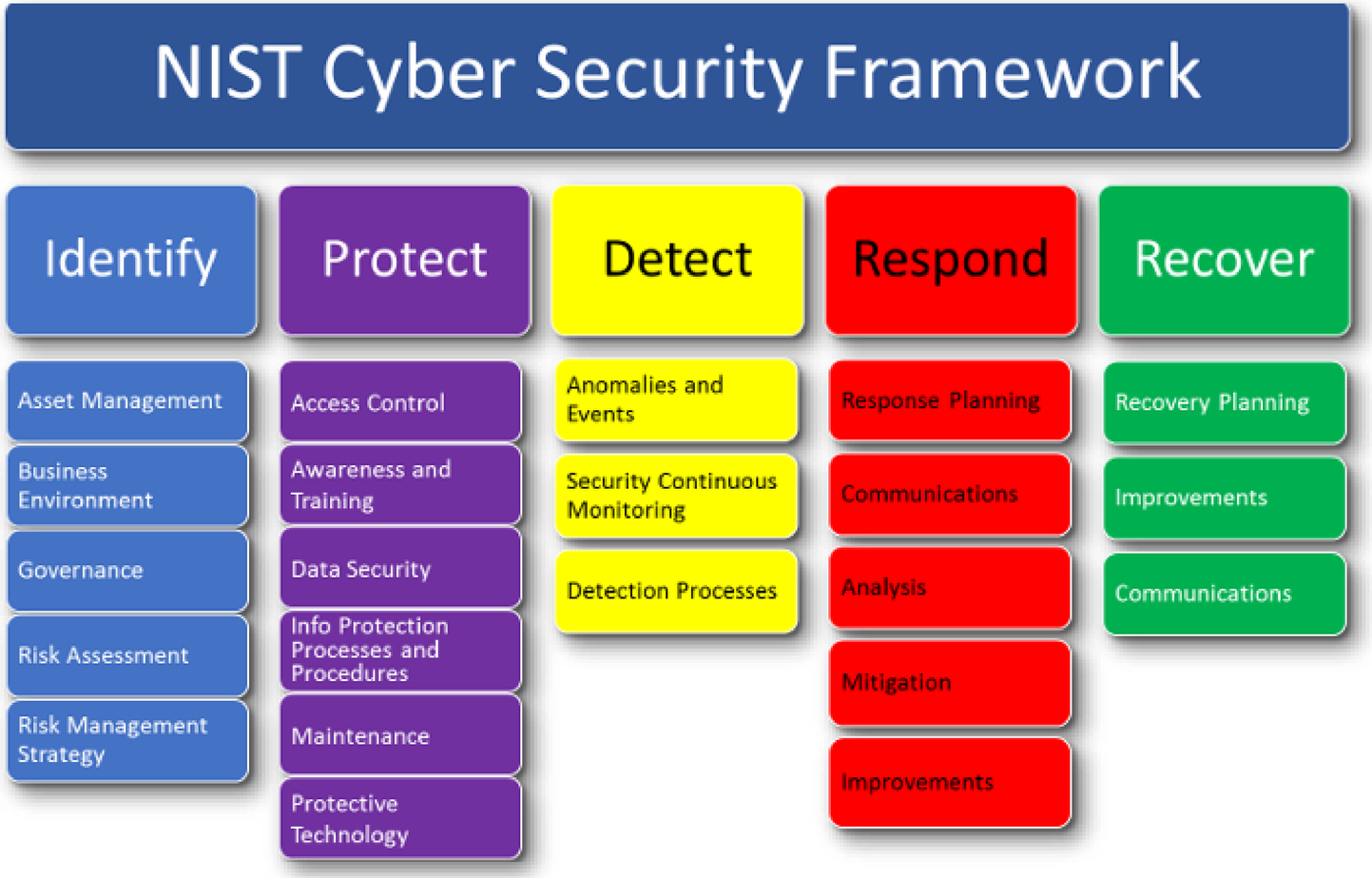
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Table of Contents

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 کسب‌وکار
		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
		PR.PT	فناوری‌های حفاظتی
DE	کشف	DE.AE	ناهنجاری‌ها و حوادث
		DE.CM	نظارت امنیتی پیوسته
		DE.DP	فرایندهای کشف
RS	پاسخ	RS.RP	برنامه‌ریزی پاسخ
		RS.CO	ارتباطات
		RS.AN	تجزیه و تحلیل
		RS.MI	کاهش اثرات
		RS.IM	بهبود و توسعه
RC	بازیابی	RC.RP	برنامه‌ریزی بازیابی
		RC.IM	بهبود و توسعه
		RC.CO	ارتباطات



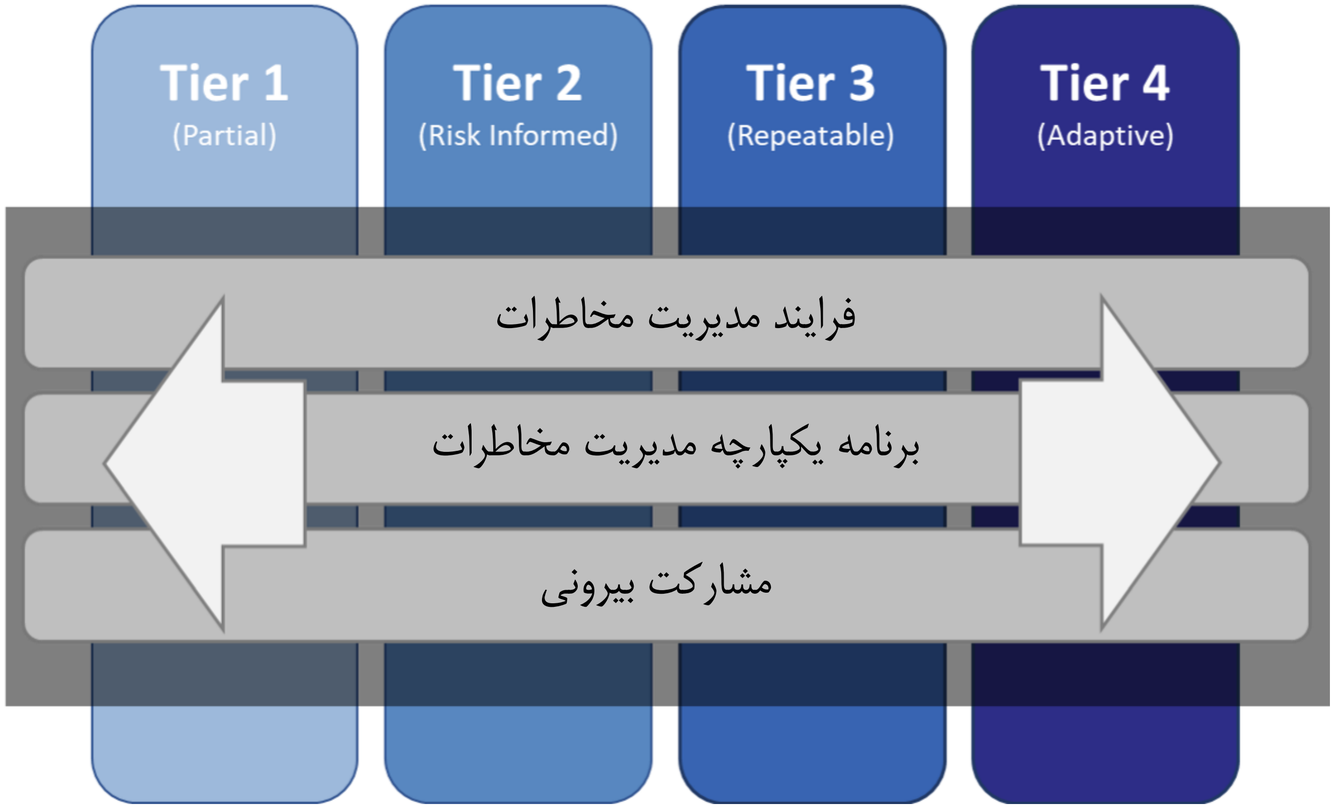
نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

- سطوح پیاده‌سازی چارچوب NIST CSF:
  - هر سطح، بیانگر نوع نگاه سازمان به **رخدادهای افتا و و فرایندهای مدیریت آنها** و همچنین روندی 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

INTERNATIONAL STANDARD

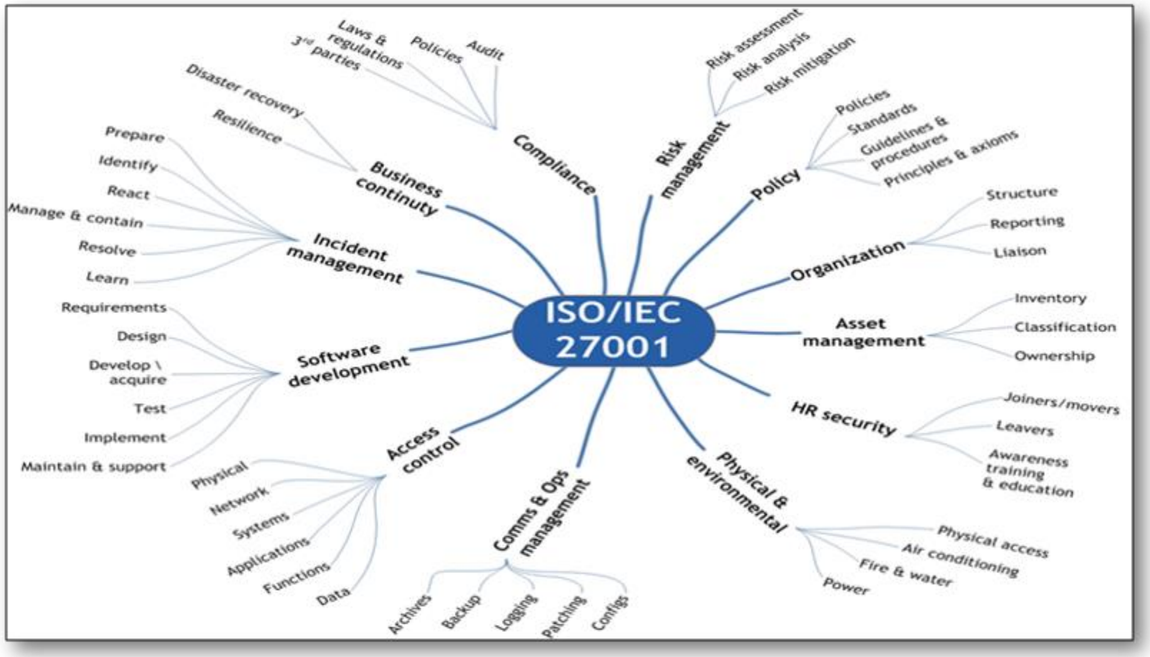
ISO/IEC 27001

Third edition
2022-10

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

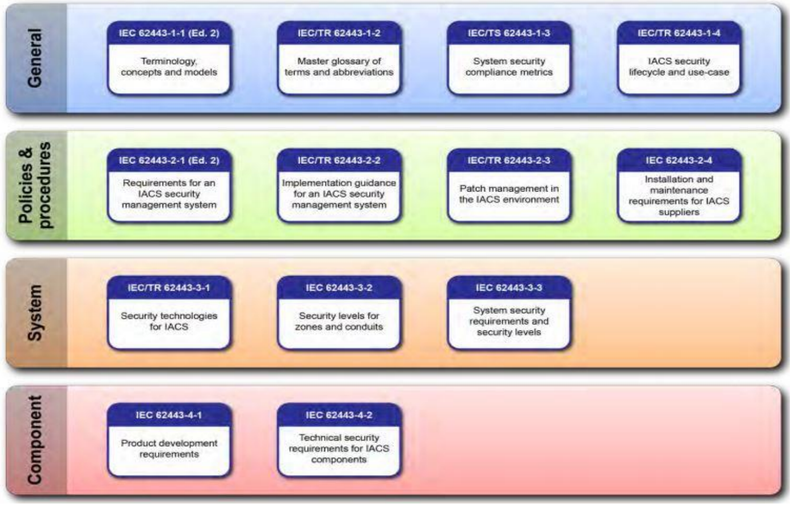
Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

- 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)

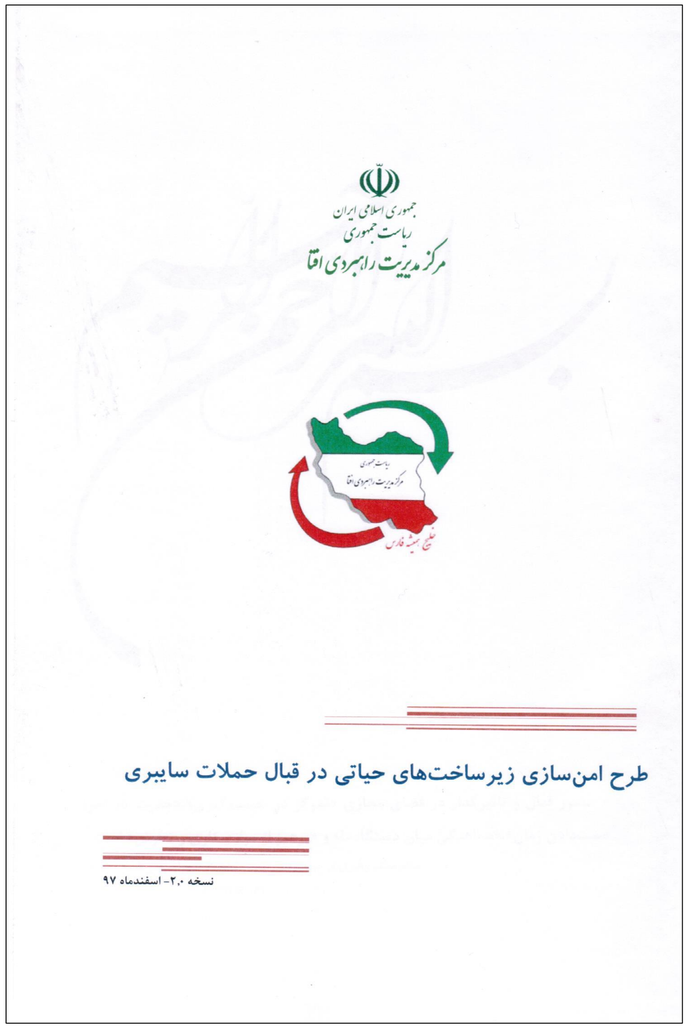


نقش و جایگاه CIS در بین راهکارهای مشابه مطرح

- استاندارد ISA/IEC 62443
- شامل:
  1. عمومی
  2. خطمشی‌ها و رویه‌ها
  3. سیستم‌ها
  4. اجزای تشکیل‌دهنده سازمان‌یافته



مقایسه کنترل‌های CIS با اسناد بالاسری کشور

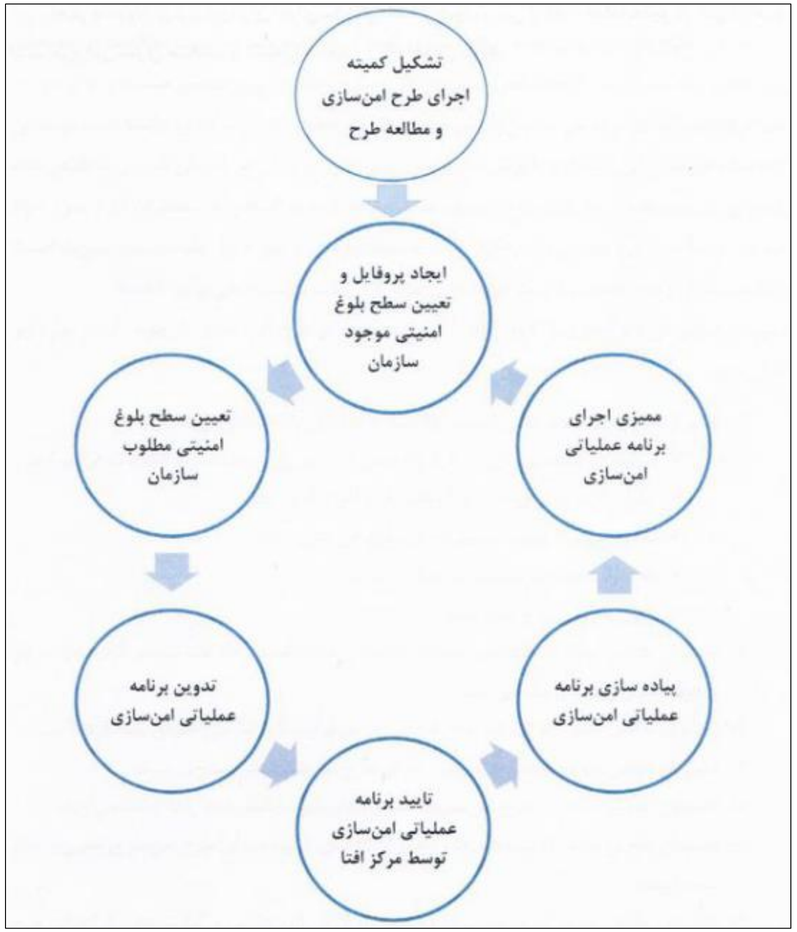


- طرح کلان امن‌سازی زیرساخت حیاتی مرکز افتای ریاست جمهوری
- کنترل‌های ۹ گانه افتا (الزامات طرح امن‌سازی):

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

مقایسه کنترل‌های CIS با اسناد بالاسری کشور

- نقشه راه و مدل بلوغ طرح کلان امن‌سازی 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. مصون‌سازی و پایداری
2. وحدت مدیریت
3. بازدارندگی
4. حفظ آمادگی
5. پیش‌بینی در تهدیدشناسی
6. اقتصادی سازی
7. اشراف اطلاعاتی
8. دیپلماسی فعال
9. اقتدار درون‌زا

بسمه تعالی
جمهوری اسلامی ایران
فرماندهی کل قوا
کمیته دائمی پدافند غیرعامل کشور

شماره: ۱۶۰/۱/۵۸۵
تاریخ: ۱۳۹۴/۰۳/۲۱
پیوست: ندارد

تصویب‌نامه

وزیر محترم کشور
وزیر محترم دفاع و پشتیبانی نیروهای مسلّح
معاون محترم رئیس جمهور و رئیس سازمان مدیریت و برنامه ریزی کشور
رئیس محترم کمیسیون امنیت ملّی و سیاست خارجی مجلس شورای اسلامی
سردار رئیس محترم ارکان و امور مسلّح مشترک نیروهای مسلح
سردار رئیس محترم سازمان پدافند غیرعامل کشور

سلام‌علیکم

باصلوات برمحمد وآل محمد احقاقی؛ کمیته دائمی **(شورای عالی)** پدافند غیرعامل کشور در جلسه مورخ ۱۳۹۴/۲/۲۹ به استناد **ماده(۸)** اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظم رهبری، فرماندهی کل قوا (مدظله العالی)، « **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

ماده۱ : تعاریف و اصطلاحات

۱) فضای سایبری: به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه های رایانه‌ای، پردازنده-های تعبیه‌شده(جا گذاری شده)، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه-های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه شده باشد.

۲) سرمایه ملی سایبری: بخشی از دارایی‌های کشور اعم از زیرساخت ها، سامانه ها، تجهیزات، نرم افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مستقیم و تعیین کننده داشته باشند، سرمایه ملی سایبری نامیده می‌شود.

۳) آسیب‌پذیری سایبری: به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی سایبری، رویه های امنیتی یا کنترل های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره برداری یا فعال شدن تهدیدات داخلی و خارجی به منظور تهاجم و یا جنگ سایبری را داشته باشد، اطلاق می گردد.

صفحه ۱ از ۸ صفحه

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

تهدیدها
منابع سازمانی
محدودیت های زمانی

با تشکر از توجه شما