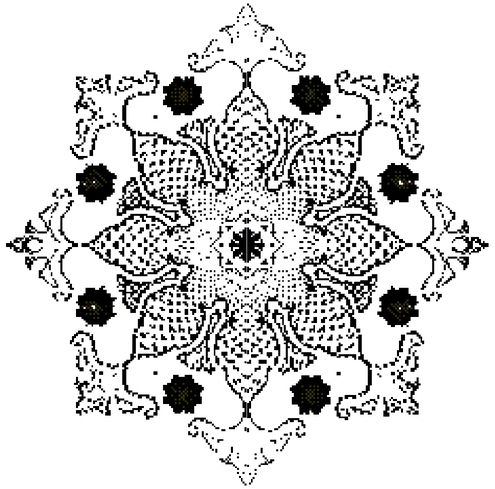
امنیت شبکه‌های صنعتی و فناوری عملیاتی (OT)

وبینار آشنایی با استاندارد امنیت شبکه‌های صنعتی (ISA/IEC 62443)

Ics Cyber Security (ICS2)

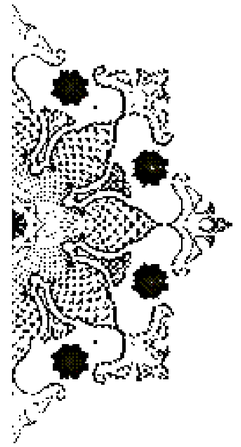


به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید؛
از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد
و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به
سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.

محمد مهدی واعظی نژاد

مهندس امنیت فناوری اطلاعات
info@mvaezi.ir

سرفصل مطالب



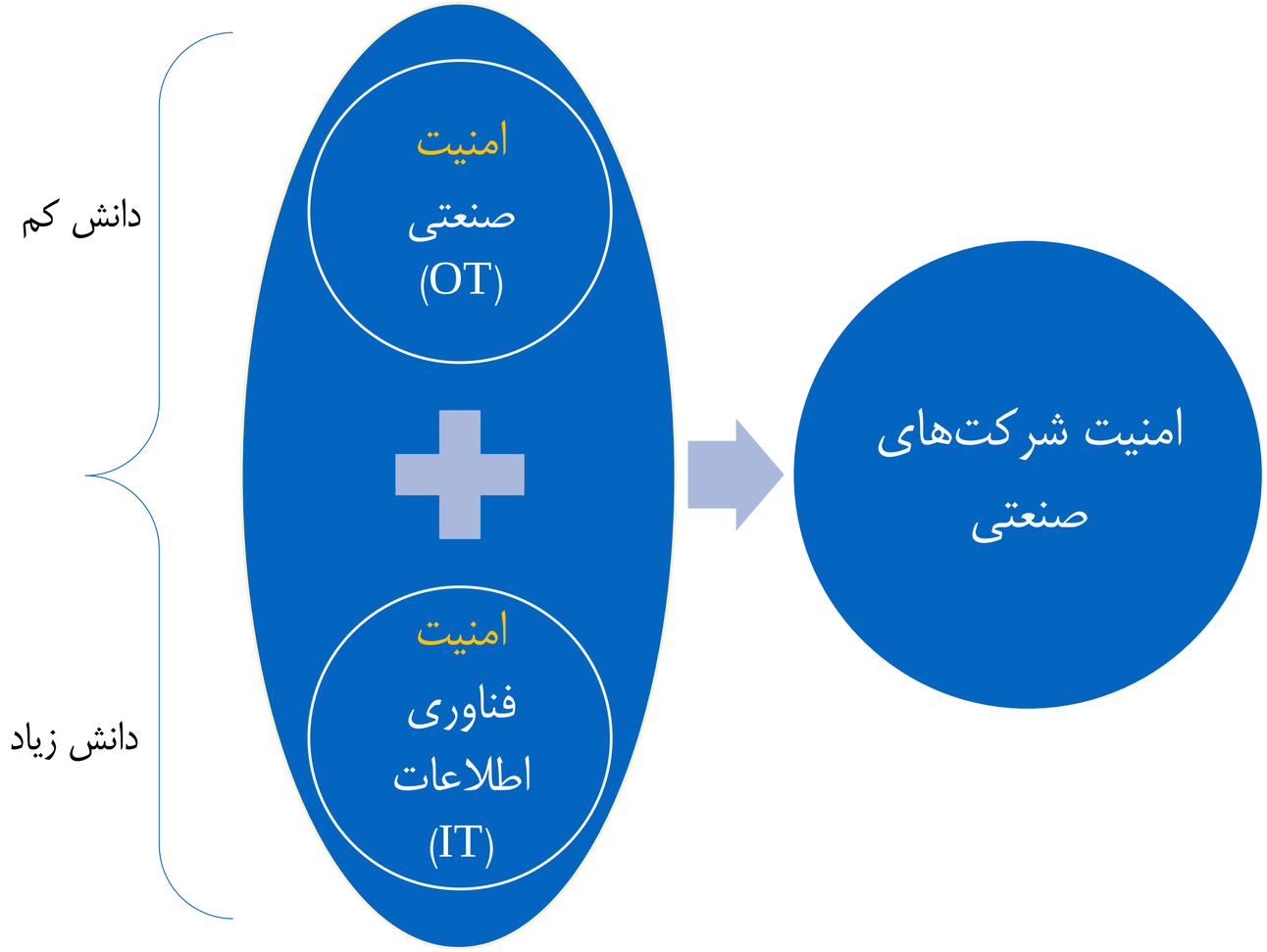
- بخش اول: امنیت اطلاعات صنعتی
- بخش دوم: آشنایی با استانداردهای سری ۶۲۴۴۳ و مقایسه آنها با سایر استانداردهای مشابه
- بخش سوم: تشریح کلی ساختار و الزامات استاندارد ۳-۳-۶۲۴۴۳

اطلاعات، مهندسی و مدیریت امنیت صنعتی

چرا امنیت فناوری عملیات (OT) مهم است؟

- امروزه بیش از گذشته، بقای شرکت‌ها وابسته به **حفاظت کافی در برابر مخاطرات امنیتی و خرابکاری‌های صنعتی** است.

امنیت فناوری عملیات



Stuxnet

STATUS:	Inactive since 2012	TYPE:	Worm
DISCOVERY:	June 2010	TARGETED PLATFORMS:	Industrial SCADA systems
FIRST KNOWN SAMPLE:	2007	NUMBER OF TARGETS:	100,001-300,000

حملات سایبری؛
کم‌هزینه ولی پر
اثر، با امکان شناسایی
دیرهنگام و کم!

TOP TARGETED COUNTRIES:

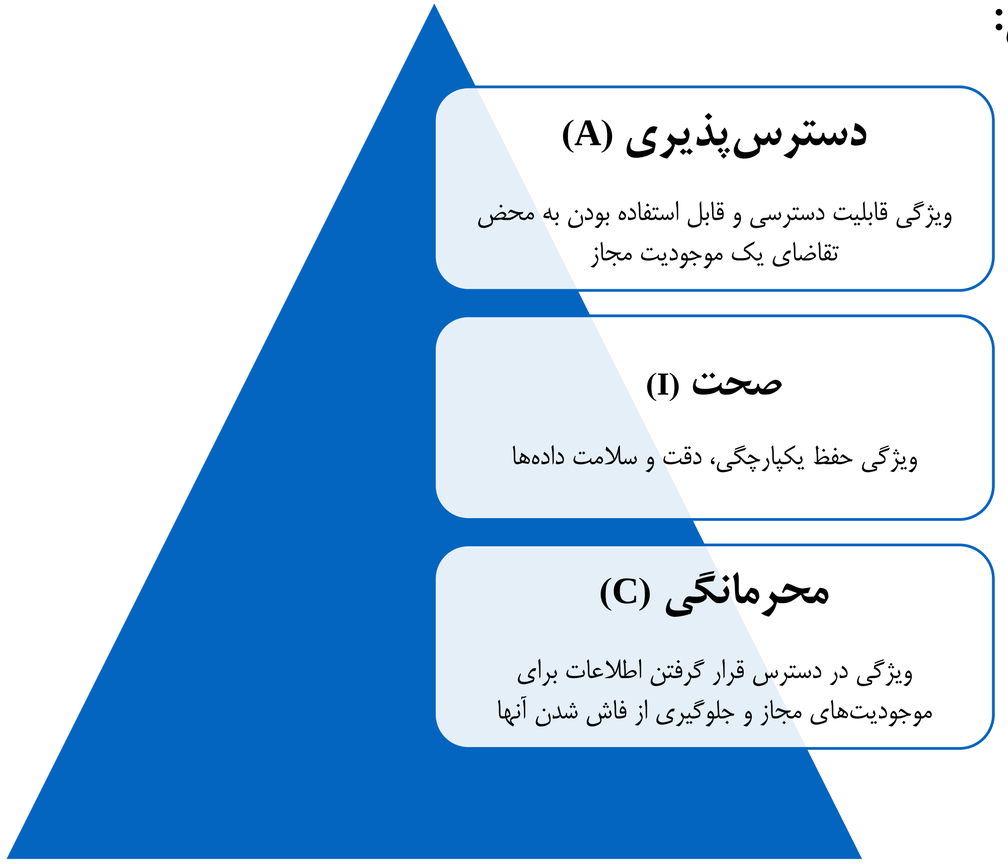
Iran

اطلاعات و دارایی‌های اطلاعاتی صنعتی

- دارایی (Asset): هر چیزی که برای سازمان دارای ارزش است.
- انواع مختلف دارایی‌ها:
  - **اطلاعات الکترونیکی یا کاغذی** (مانند داده‌های پایگاه‌های اطلاعاتی، مستندات سیستمی، پرونده‌ها، راهنماهای کاربری، طرح‌ها و قراردادها)
  - **نرم‌افزار** (مانند برنامه‌های کاربردی، نرم‌افزارها، ابزارهای توسعه سامانه‌ها و برنامه‌های کمکی)
  - **سخت‌افزار** (مانند تجهیزات رایانه‌ای (پردازشی، ذخیره‌سازی و ارتباطی)، تجهیزات امنیتی، تجهیزات سطح فیلد و امکانات ارتباطی)
  - **خدمات سازمانی** (مانند سرویس‌های شبکه صنعتی)
  - **افراد** (صلاحیت‌ها، مهارت‌ها و تجربه‌های آنها)
  - **دارایی‌های نامشهود** (مانند وجهه (Image) و شهرت)

امنیت اطلاعات صنعتی

اجزای اصلی امنیت اطلاعات صنعتی:



آشنایی با استانداردهای سری ۶۲۴۴۳

آشنایی با استانداردهای ۶۲۴۴۳

- **استاندارد ISA/IEC 62443**
  - نام قبلی این استاندارد: ISA 99
  - ایجاد شده توسط انجمن بین‌المللی اتوماسیون (ISA)
  - مورد تأیید انجمن بین‌المللی الکتروتکنیک (IEC)
  - تغییر نام داده شده به استانداردهای سری ANSI/ISA-62443 توسط مؤسسه ملی استاندارد آمریکا (ANSI) در سال ۲۰۱۰ میلادی
  - مشتمل بر یکسری استانداردها، گزارش‌های فنی و اطلاعات مرتبط برای امنیت اتوماسیون صنعتی و سیستم‌های کنترل

ساختار استانداردهای سری ۶۲۴۴۳

- تقسیم‌بندی تمام استانداردهای ISA/IEC-62443 و گزارش‌های فنی آن به چهار دسته کلی به نام‌های:

1. **عمومی:**
   - ISA-62443-1-1 (IEC/TS 62443-1-1)
   - ISA-TR62443-1-2 (IEC 62443-1-2)
   - ISA-62443-1-3 (IEC 62443-1-3)
   - ISA-62443-1-4 (IEC/TS 62443-1-4)
2. **خط‌مشی‌ها و رویه‌ها:**
   - ISA-62443-2-1 (IEC 62443-2-1)
   - ISA-62443-2-2 (IEC 62443-2-2)

ساختار استانداردهای سری ۶۲۴۴۳

- ISA-TR62443-2-3 (IEC/TR 62443-2-3)
- ISA-62443-2-4 (IEC 62443-2-4)

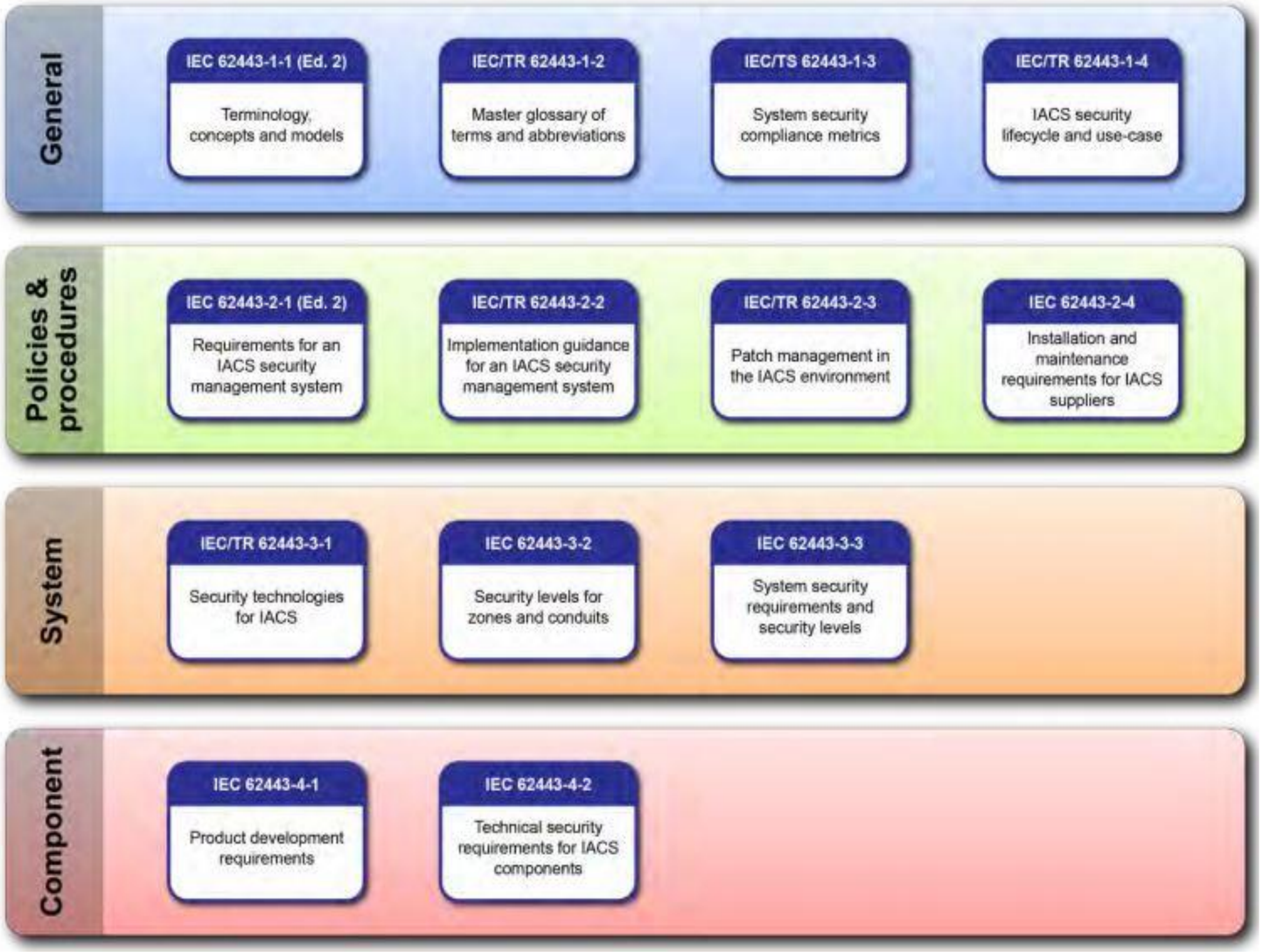
3. **سیستم‌ها:**

- ISA-TR62443-3-1 (IEC/TR 62443-3-1)
- ISA-62443-3-2 (IEC 62443-3-2)
- **ISA-62443-3-3 (IEC 62443-3-3)**

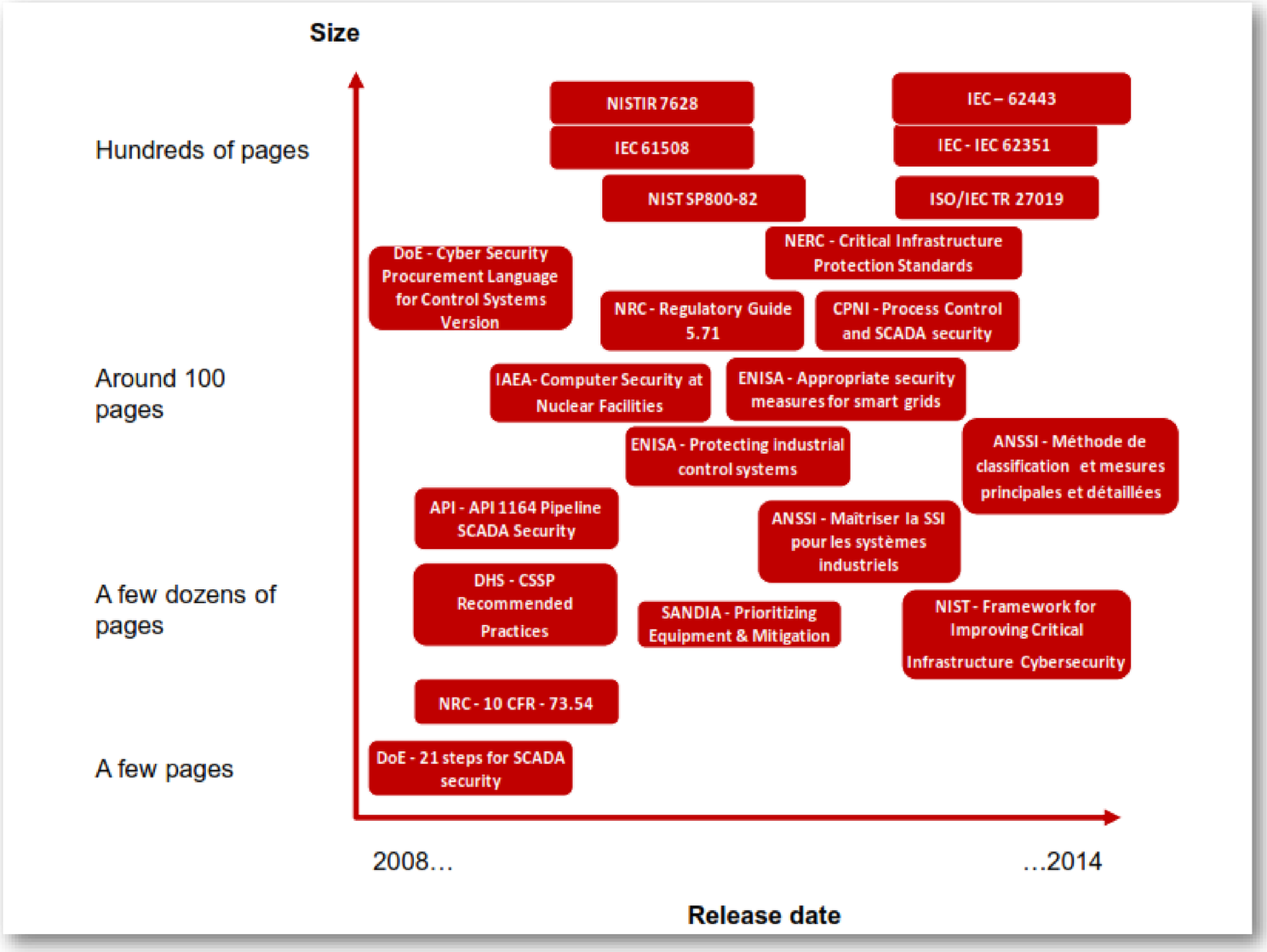
4. **اجزای تشکیل‌دهنده سازمان‌یافته:**

- ISA-62443-4-1 (IEC 62443-4-1)
- ISA-62443-4-2 (IEC 62443-4-2)

ساختار استانداردهای سری ۶۲۴۴۳



مقایسه استانداردهای سری ۶۲۴۴۳ با سایر استانداردها



فازهای اجرایی استاندارد ۶۲۴۴۳-۳-۳

- فاز اول: طراحی و مستندسازی (Plan)
  - هدف: برنامه‌ریزی و تدوین مستندات مورد نیاز برای اجرا و پیاده‌سازی الزامات استاندارد

- مستندات استاندارد:
  - خط‌مشی‌ها
  - روش‌های اجرایی
  - دستورالعمل‌ها
  - آیین‌نامه‌ها

فازهای اجرایی استاندارد ۶۲۴۴۳-۳-۳

- فاز دوم: اجرا و پیاده‌سازی (Do)
- هدف: اجرا و پیاده‌سازی طرح‌ها، خط‌مشی‌ها و روال‌های امنیتی تدوین شده، جهت دستیابی به اهداف کنترل‌های انتخاب شده از استاندارد

- تهیه تجهیزات مورد نیاز طرح‌های امنیتی سازمان
- تهیه LOM و خرید تجهیزات مورد نیاز در پیاده‌سازی طرح‌های برطرف‌سازی مخاطرات و طرح‌های امنیت شبکه صنعتی شرکت
- پیاده‌سازی و عملیاتی کردن کنترل‌ها، طرح‌ها، روال‌ها و سیاست‌های امنیتی تهیه شده در فاز یک
- نظارت بر اجرای مستندات تدوین شده و تکمیل سوابق استاندارد

فازهای اجرایی استاندارد ۶۲۴۴۳-۳-۳

- فاز سوم: بازنگری و بهبود (Check)
  - هدف: پایش و بازنگری الزامات اجرا شده در شرکت
- مدنظر قراردادن موارد زیر در این فاز:
  - انجام مراقبت و بازنگری در کنترل‌ها، روال‌ها و خط‌مشی‌ها به منظور:
    - شناسایی خطاهای احتمالی در شیوه پیاده‌سازی الزامات استاندارد
    - شناسایی سریع رخدادهای احتمالی امنیتی
    - ارزیابی افراد جهت نحوه انجام صحیح مسئولیت‌های امنیتی‌شان
    - کشف رویدادهای امنیتی و جلوگیری از وقوع حوادث، با استفاده از شاخص‌های ارزیابی
  - تعیین اثربخشی اقدام‌های انجام شده جهت رفع مسایل امنیتی
  - به‌روز کردن طرح‌های امنیتی، در صورت نیاز

فازهای اجرایی استاندارد ۳-۳-۶۲۴۴۳

- از جمله مهمترین اقدام‌های این فاز:

1. ممیزی داخلی

- انجام ممیزی داخلی، قبل از ممیزی نهایی؛ به منظور شناسایی انحراف‌های احتمالی در وضعیت امنیت صنعتی شرکت با الزامات استاندارد

2. اقدامات اصلاحی و رفع عدم انطباق‌ها

- رفع عدم انطباق‌ها و موارد انحرافی موجود، به منظور بهبود راهکارهای پیاده‌سازی شده

3. بازنگری مدیریت

- برگزاری جلسات بازنگری مدیریتی در شرکت

فازهای اجرایی استاندارد ۶۲۴۴۳-۳-۳

- فاز چهارم: بهبود (ACT)
- انتخاب شرکت گواهی‌کننده (CB)
- انجام ممیزی نهایی (ممیزی شخص سوم)
- انجام اقدامات لازم جهت ارتقا و بهبود راهکارهای امنیت صنعتی پیاده‌سازی شده در شرکت

امنیت صنعتی بر اساس استانداردهای ۶۲۴۴۳؛ یعنی:

آسیب‌پذیری‌ها

کنترل شناسایی و احراز هویت
کنترل استفاده
جامعیت سیستم
محرمانگی داده‌ها
جریان محدود داده‌ها
واکنش به موقع به رویدادها
دسترس‌پذیری منابع

حملات

افشا
تعلیق
تخریب
دستکاری
پاک کردن

تهدیدها

با تشکر از توجه شما