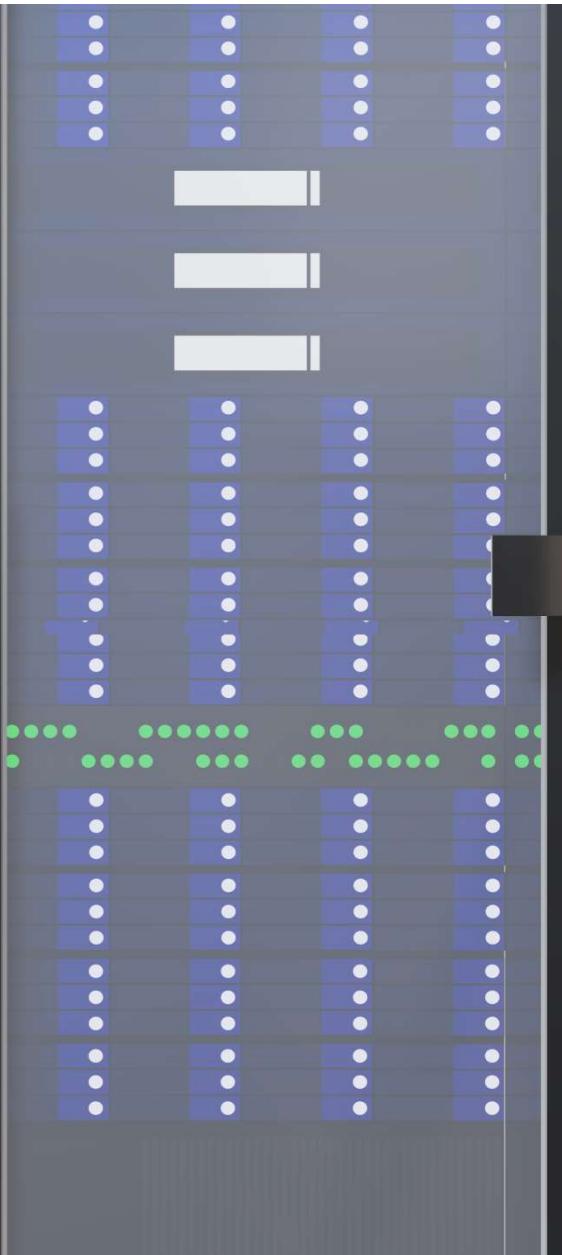




مدیریت امنیت اطلاعات در سازمان‌ها با رویکرد ISO/IEC 27001

علی رضایی، حامد محمدی



چرا امنیت اطلاعات مهم است؟

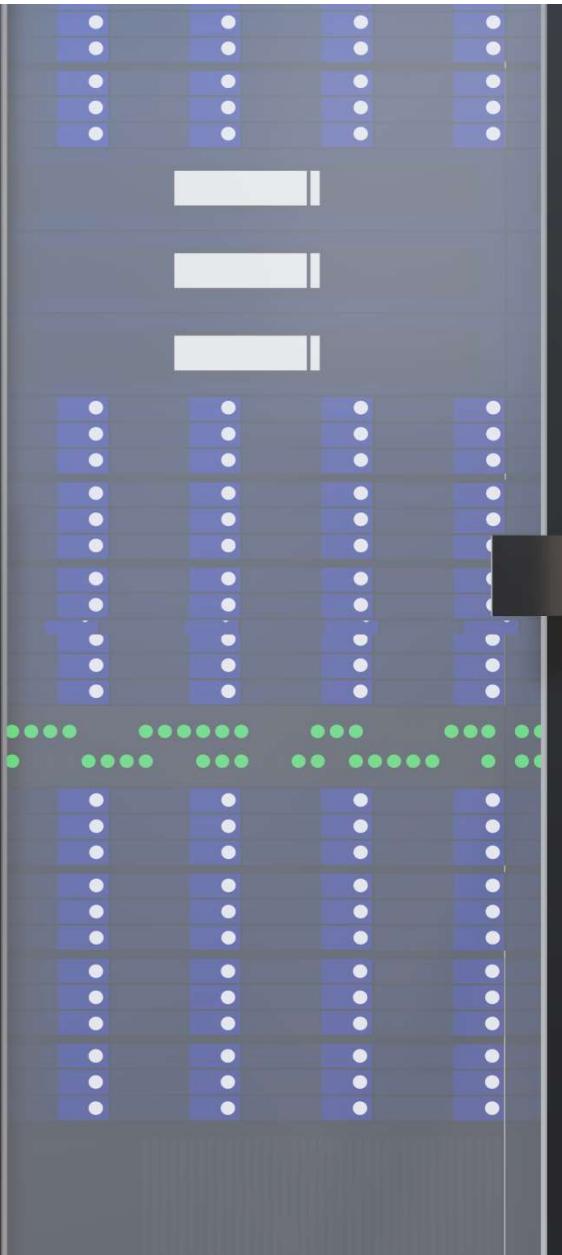
افزایش حملات سایبری به زیرساختها و سازمان‌ها در ایران:

حمله به سامانه هوشمند سوخت (1400): اختلال در پمپبنزین‌ها

حمله به راهآهن (1400): پیام‌های جعلی روی تابلوها

حمله به وزارت امور خارجه و زیرساخت‌های دیگر (2023)

حمله به سامانه‌های بانکی و آموزشی



چرا امنیت اطلاعات مهم است؟

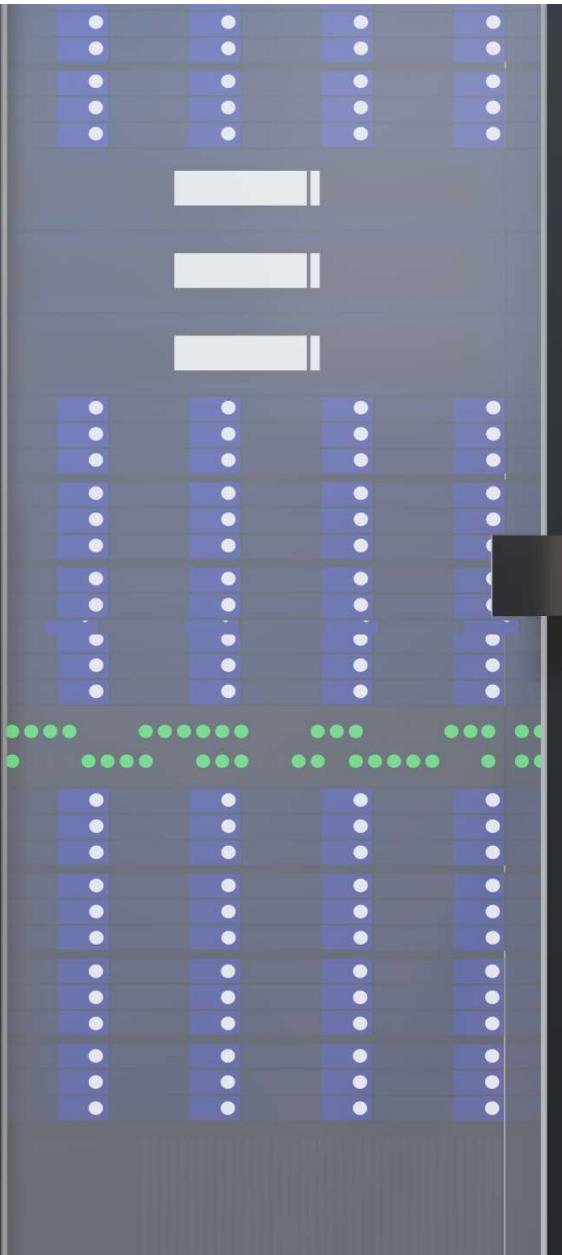
نشت اطلاعات حساس کاربران و سازمان‌ها

رایتل: اطلاعات 5 میلیون کاربر در دارکوب

سامانه ثنا: 15 میلیون رکورد هویتی فاش شد

سامانه شاد: اطلاعات معلمان و دانشآموزان منتشر شد

نشت اطلاعات سامانه ثبت‌نام واکسن کرونا(salamat.gov.ir)



چرا امنیت اطلاعات مهم است؟

دلایل اصلی آسیب‌پذیری عنوان: چرا سازمان‌ها هدف آسانی هستند؟

نبود سیاست مشخص امنیت اطلاعات

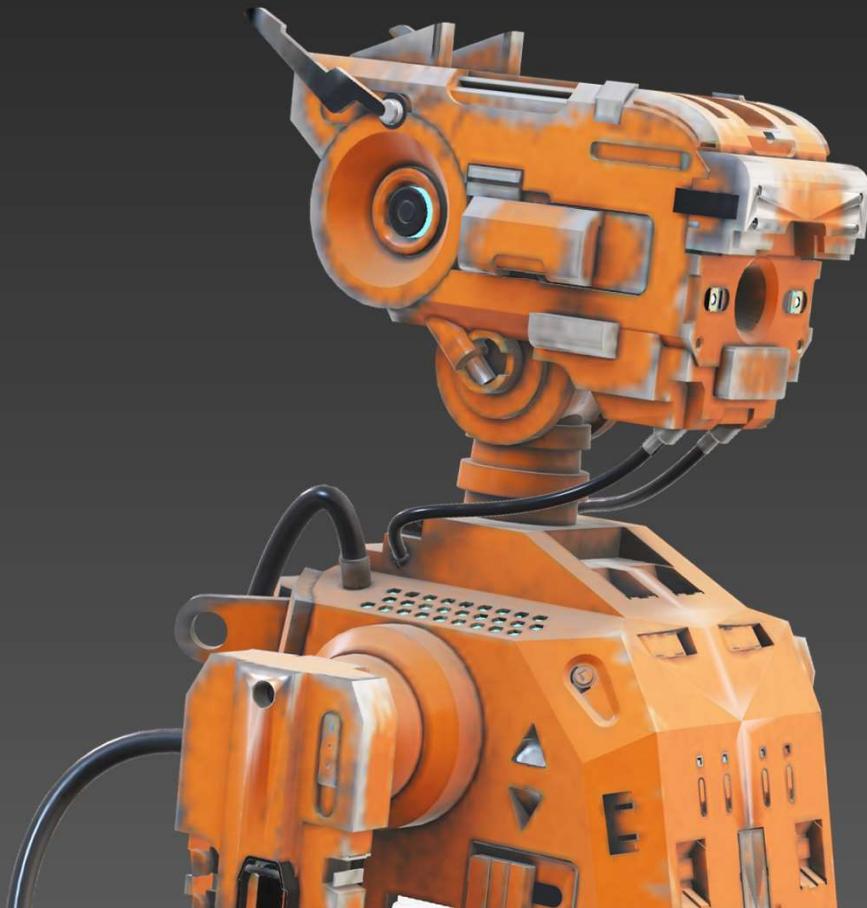
آموزش ناکافی کاربران و پرسنل

استفاده از سامانه‌های نایمن بدون تست

تعريف امنیت اطلاعات و مفاهیم پایه



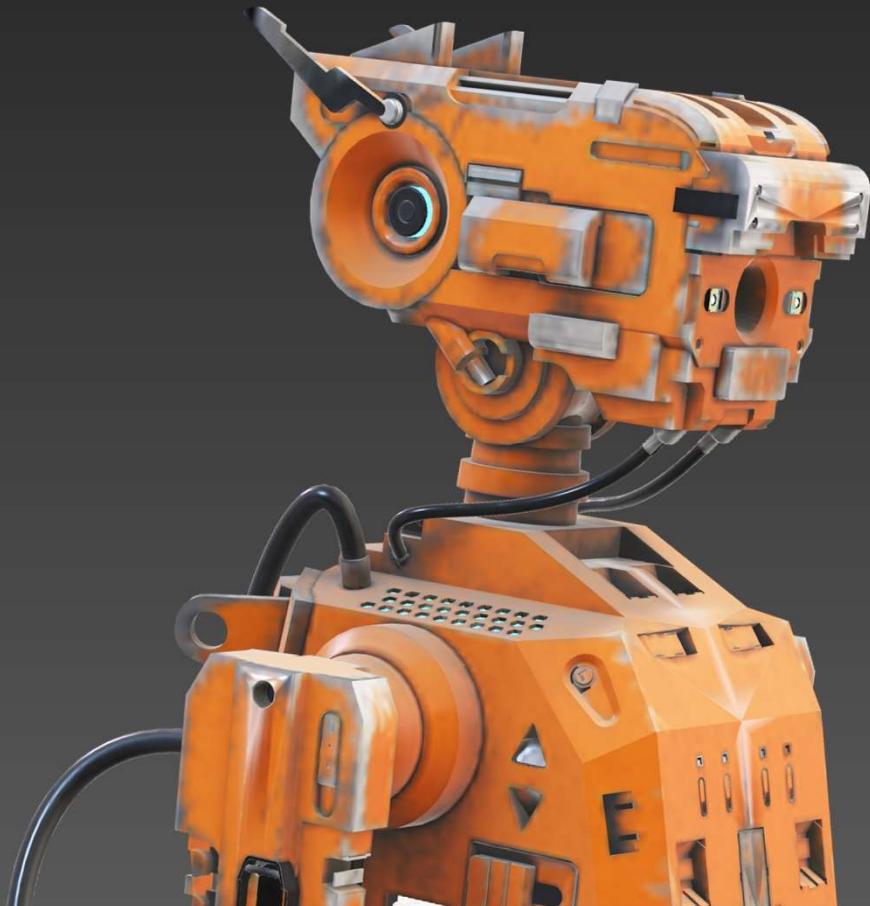
تعریف امنیت اطلاعات و مفاهیم پایه



محرمانگی

دسترسی فقط برای افراد مجاز

تعریف امنیت اطلاعات و مفاهیم پایه



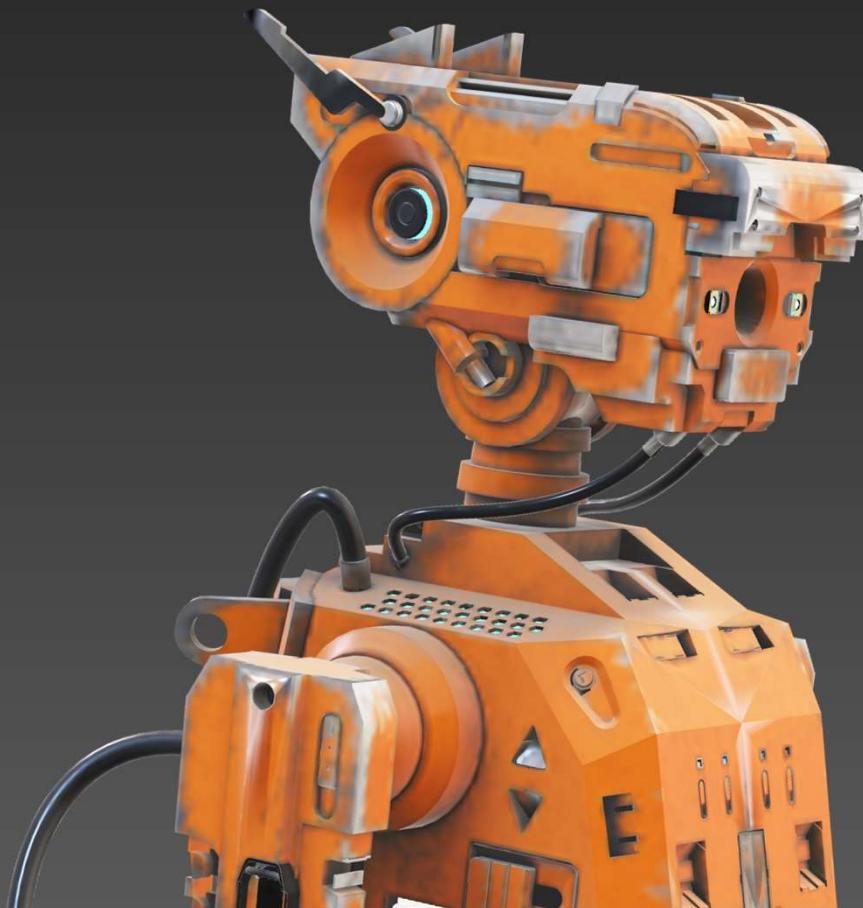
محرمانگی

دسترسی فقط برای افراد مجاز

یکپارچگی

اطلاعات کامل و دقیق باقی بمانند

تعریف امنیت اطلاعات و مفاهیم پایه



محرمانگی

دسترسی فقط برای افراد مجاز

یکپارچگی

اطلاعات کامل و دقیق باقی بمانند

دسترسی پذیری

اطلاعات در زمان نیاز در دسترس باشد





استاندارد ISO/IEC 27001 چیست؟

استاندارد ISO/IEC 27001 چیست؟

هدف اصلی :

شناسایی دارایی‌های اطلاعاتی

تحلیل ریسک‌های امنیتی

پیاده‌سازی کنترل‌های مناسب

حفظ امنیت اطلاعات و افزایش اعتماد



چرا سازمان‌ها باید ISO 27001 را اجرا کنند؟

چرا سازمان‌ها باید ISO 27001 را اجرا کنند؟

کاهش آسیب‌پذیری

محافظت در برابر حملات سایبری

انطباق قانونی

رعایت GDPR و قوانین حريم خصوصی

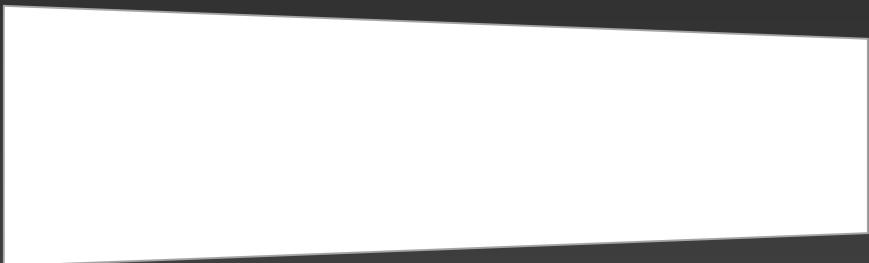
بهبود مستمر

چرخه PDCA برای امنیت پایدار

افزایش اعتماد

جلب رضایت مشتریان و شرکا

چرخه بهبود مستمر PDCA





چرخه بهبود مستمر

PDCA



چرخه بهبود مستمر

PDCA



چرخه بهبود مستمر PDCA

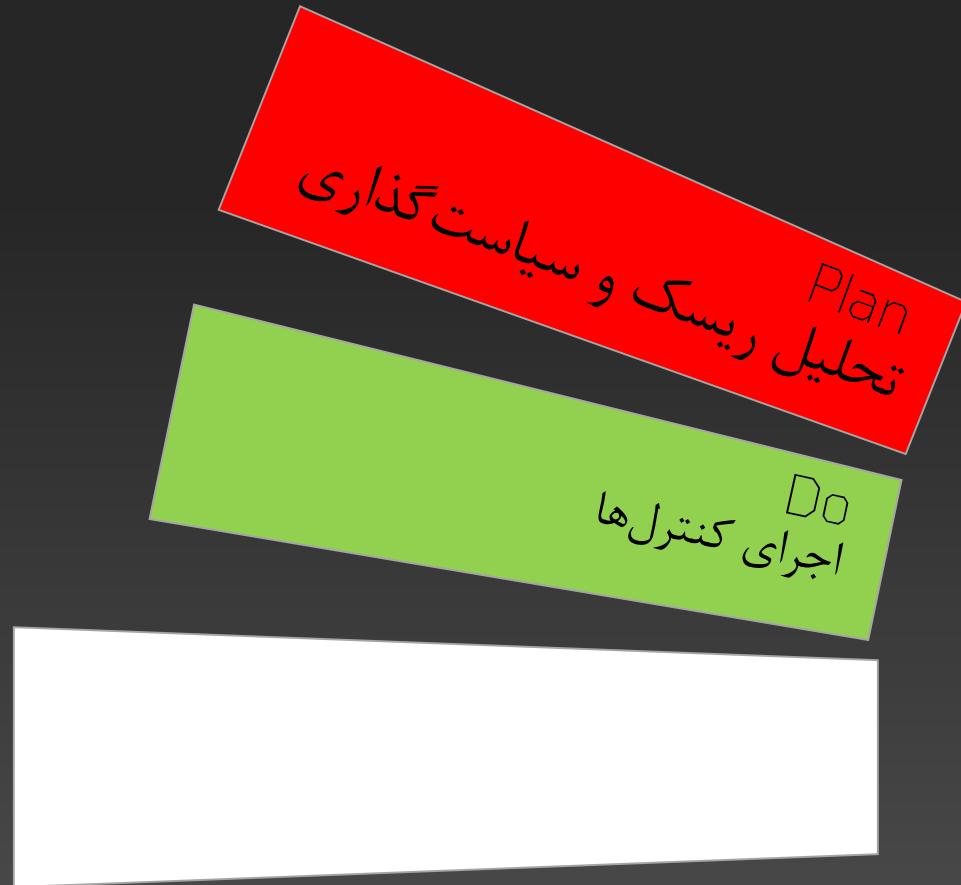


چرخه بهبود مستمر PDCA

چرخه بهبود مستمر PDCA



چرخه بهبود مستمر PDCA



چرخه بهبود مستمر PDCA



چرخه بهبود مستمر



چرخه بهبود مستمر PDCA



ساختار استاندارد ISO/IEC 27001:2022

بند 4	زمینه سازمان، دامنه ISMS
بند 5	رهبری و تعهد مدیریت
بند 6	برنامه‌ریزی و ارزیابی ریسک
بند 7	پشتیبانی و مستندسازی
بند 8	اجرای کنترل‌ها و مدیریت ریسک
بند 9	ارزیابی عملکرد و ممیزی
بند 10	اقدامات اصلاحی و بهبود مستمر



ضمیمه A-کنترل‌های امنیتی

ضمیمه A-کنترل‌های امنیتی

کنترل‌های انسانی

- پاسخ به حادثه
- آموزش

کنترل‌های سازمانی

- سیاست امنیت
- مدیریت دسترسی
- آموزش و پاسخ به حادثه

کنترل‌های فیزیکی

- کنترل دسترسی فیزیکی
- تجهیزات امن

کنترل‌های فناوری

- رمزنگاری
- آنتیویروس

سازمان‌ها کنترل‌ها را بر اساس ریسک‌های شناسایی شده انتخاب می‌کنند

Risk-Based برای امنیت هدفمند و موثر رویکرد

چارچوب حاکمیت امنیت اطلاعات با استاندارد ISO/IEC 27001

چارچوب ISO/IEC 27001 به عنوان یک الگوی مدیریتی جامع برای امنیت اطلاعات مطرح است که گام‌های مشخصی را شامل می‌شود. این گام‌ها با تعیین دامنه، تعهد قوی مدیریت ارشد، تدوین سیاست‌های امنیت اطلاعات و ارزیابی دقیق ریسک آغاز می‌شود.

در مراحل بعدی، انتخاب کنترل‌های امنیتی مناسب، مستندسازی سامانه مدیریت امنیت اطلاعات، آموزش کارکنان، انجام ممیزی‌های داخلی و نهایتاً صدور گواهی‌نامه قرار دارد. ابزارهای تخصصی مانند Risk Register، Asset Register و Statement of Applicability (SoA) در این فرآیند کلیدی هستند.



مقایسه ISO 27001 با چارچوبهای امنیتی دیگر

NIST SP 800-53

COBIT

PCI-DSS

ISO 27701

مقایسه ISO 27001 با چارچوبهای امنیتی دیگر

NIST SP 800-53

چارچوب تخصصی دولت آمریکا با تمرکز دقیق‌تر بر امنیت ملی و دولتی است که جزئیات فنی بیشتری دارد.

COBIT

رویکردی جامع به حاکمیت فناوری اطلاعات که امنیت اطلاعات جزئی از آن است و تمرکز کمتری روی امنیت دارد.

PCI-DSS

چارچوبی محدود به حوزه پرداخت الکترونیک و اطلاعات مالی، کاربردی بسیار تخصصی و محدود دارد.

ISO 27701

مکمل ISO 27001 برای مدیریت حریم خصوصی و داده‌های شخصی، تقویت کننده حفاظت اطلاعات حساس مشتریان است.

نتیجه‌گیری ISO 27001: به عنوان بهترین گزینه برای سازمان‌هایی که به دنبال راهکار مدیریت جامع امنیت اطلاعات هستند، شناخته می‌شود.

نمونه‌هایی از پیاده‌سازی موفق ISO 27001 در شرکت‌ها

نمونه‌هایی از پیاده‌سازی موفق ISO 27001 در شرکت‌ها



Fujitsu

- دامنه: خدمات ابری
- نتیجه: افزایش اعتماد مشتریان بین‌المللی

نمونه‌هایی از پیاده‌سازی موفق ISO 27001 در شرکت‌ها

Vodafone UK

- دامنه: خدمات مخابراتی
- نتایج: کاهش شکایات امنیتی و
- موفقیت در مزایده‌های دولتی



نمونه هایی از پیاده سازی موفق ISO 27001 در شرکت ها



فناپ ایران

- دامنه: فناوری مالی
- نتایج: تطابق کامل با مقررات
بانک مرکزی و افزایش اعتماد
سازمانی

نتیجه‌گیری و اهمیت ISO/IEC 27001 در سازمان‌ها

فراتر از چارچوب

ISO/IEC 27001 تنها یک استاندارد نیست؛ بلکه تبدیل به فرهنگی در سازمان می‌شود که امنیت را در تمامی سطوح حکمرانی می‌کند.

1

افزایش شفافیت و انطباق

پیاده‌سازی مؤثر این چارچوب موجب بهبود شفافیت فرآیندها و انطباق با قوانین و مقررات می‌شود.

2

اعتماد سازمانی

با به‌کارگیری استاندارد، اعتماد ذینفعان و مشتریان به امنیت و صحت عملکرد سازمان افزایش چشمگیری می‌یابد.

3



مراحل پیاده‌سازی ISO/IEC 27001



پیاده‌سازی ISO/IEC 27001 یک مسیر ساختار یافته است. این مسیر شامل تحلیل، طراحی، اجرا و ارزیابی سیستم امنیت اطلاعات می‌شود.

[] - تعیین دامنه سیستم مدیریت امنیت اطلاعات



مستندسازی

شامل محل جغرافیایی، فرآیندها، سیستم‌ها و اطلاعات.

تعريف دامنه

مشخص کردن بخش‌های تحت پوشش استاندارد مانند واحد IT یا کل شرکت.

اهمیت دامنه

بدون دامنه مشخص، ارزیابی ریسک و کنترل‌ها ممکن نیست.

۲- جلب تعهد مدیریت ارشد

حمایت مدیران

حمایت صریح و فعال مدیران ارشد برای موفقیت پروژه ضروری است.

نماینده مدیریت

انتصاب نماینده مدیریت برای نظارت بر پروژه.

تخصیص منابع

مدیریت باید منابع، زمان، بودجه و اختیارات لازم را اختصاص دهد.



۳- تعریف سیاست امنیت اطلاعات



مبانی کنترل‌ها

پایه‌ای برای انتخاب کنترل‌ها و ارزیابی عملکرد.

تعهد به بهبود

پیشرفت مستمر در امنیت اطلاعات سازمان.

اهداف کلی

حفظ محramانگی داده‌ها و تعهد به انطباق با
قوانين.

4- ارزیابی ریسک امنیت اطلاعات



شناسایی دارایی‌ها

شامل سرورها، پایگاه داده‌ها و سیستم‌های حساس.

1

تحلیل تهدید
بررسی حملات سایبری، خطاهای انسانی و نقص فنی.

2

ارزیابی ریسک
سنجه احتمال و تاثیر تهدید برای هر دارایی.

3

5-انتخاب و پیاده‌سازی کنترل‌های امنیتی



نمونه کنترل‌ها:

- حدودسازی دسترسی
- رمزگاری داده‌ها
- مدیریت حادثه
- امنیت فیزیکی

ثبت کنترل‌ها

ثبت در سند Statement of Applicability (SoA).

انتخاب کنترل‌ها

بر اساس ضمیمه A استاندارد، کنترل‌های مرتبط با ریسک‌ها انتخاب می‌شوند.



6-طراحی ساختار مستندسازی

نمونه اسناد

Risk Treatment .ISMS Policy
Incident Report و Plan
Templates.

شواهد ممیزی

لاکهای سیستم و سوابق آموزش کارکنان.

مستندات کلیدی

شامل سیاست‌ها، رویه‌ها و دستورالعمل‌های اجرایی.

۷-آموزش و آگاهی‌رسانی به کارکنان

۷-آموزش و آگاهی‌رسانی به کارکنان

روش‌ها

نقش کارکنان

آموزش خطرات

کارگاه‌های آموزشی و آزمون‌های آگاهی امنیتی. درک مسئولیت‌ها و نحوه گزارش‌دهی.

8-ممیزی داخلی



- یک تیم مستقل وضعیت پیاده‌سازی را بررسی می‌کند و گزارش رسمی تهیه می‌کند.
- هدف: شناسایی نقاط ضعف، عدم انطباق و فرصت‌های بهبود
- نتایج این ممیزی در جلسه بازنگری مدیریت (Management Review) تحلیل می‌شود.

۹- دریافت گواهی نامه توسط مرجع معترض

سازمان پس از آمادگی کامل، از یک نهاد شخص ثالث (مثل TÜV، BSI، NQA) دعوت می‌کند.

این ارزیاب‌ها بازرسی می‌کنند که آیا ISMS مطابق IEC/ISO 27001 است یا نه.

در صورت موفقیت، گواهی نامه بین‌المللی دریافت می‌شود (معمولًاً با اعتبار ۳ ساله).



نکته نهایی درباره ساختار پیاده‌سازی

درگیر بودن کل سازمان

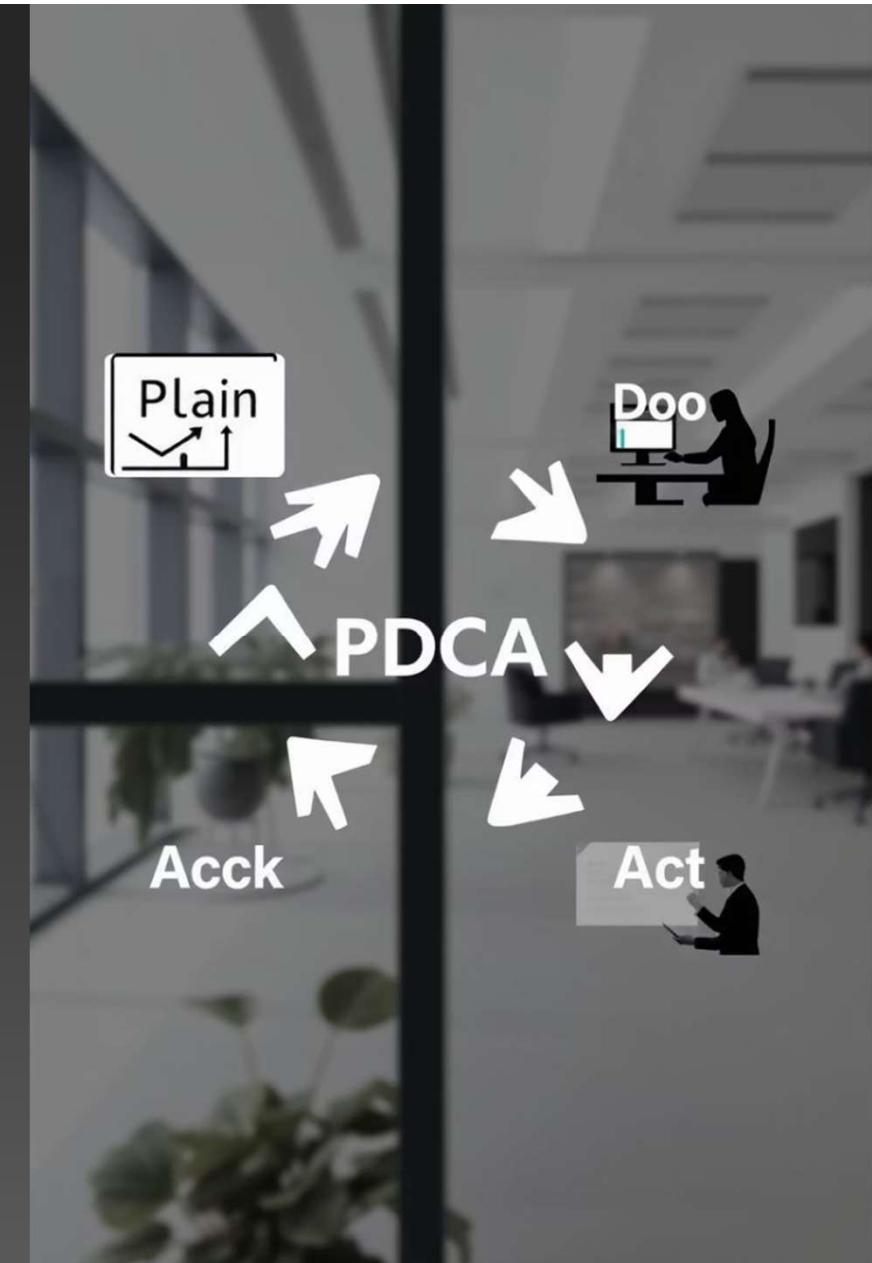
موفقیت نیازمند مشارکت همه بخش‌ها، نه
فقط IT.

سیستم مدیریتی بلندمدت

بر پایه چرخه PDCA و بهبود مستمر.

انطباق با تغییرات

هماهنگی مداوم با فناوری‌های نوین و تغییرات محیطی.



1. راهنمای پیاده‌سازی ISO 27001 از NQA

<https://www.nqa.com/getmedia/ae/fdp.ediuG-noitatnemelpml-27001af/NQA-ISO-540a996261-3e4a-73b4dbb-4-945c12https://www.nqa.com/getmedia/ae/fdp.ediuG-noitatnemelpml-27001af/NQA-ISO-540a996261>

2. راهنمای پیاده‌سازی ISO/IEC 27001:2022 از BSI

https://www.bsigroup.com/siteassets/pdf/en/insights-and-fdp.ediug_noitatnemelpmi_27001media/insights/brochures/

3. راهنمای جامع پیاده‌سازی ISO 27001 از ISMS.online

<https://www.isms.online/iso-27001https://www.isms.online/iso-27001>

ممنون از توجه شما