1- ISO 27001چیست؟

ISO/IEC 27001استاندارد بین‌المللی برای ایجاد، پیاده‌سازی، نگهداری و بهبود:

ISMS = Information Security Management System یا: سیستم مدیریت امنیت اطلاعات است.

هدف اصلی: حفاظت از اطلاعات سازمان از طریق مدیریت ریسک‌های امنیت اطلاعات.

2- سه اصل اساسی امنیت اطلاعاتCIA

محرمانگی C — Confidentiality : اطلاعات فقط در اختیار افراد مجاز باشد.

مثال:فایل حقوق کارکنان فقط برای واحد منابع انسانی قابل مشاهده باشد.

تمامیت / یکپارچگی I — Integrity : اطلاعات بدون مجوز تغییر نکند.

مثال: مبلغ تراکنش بانکی نباید توسط فرد غیرمجاز تغییر کند.

دسترس‌پذیری A — Availability : اطلاعات و سیستم هنگام نیاز در دسترس باشد.

مثال: سامانه بانکداری باید در زمان موردنیاز مشتری قابل استفاده باشد.

خلاصه:

Confidentiality = چه کسی ببیند؟
Integrity = چه کسی تغییر دهد؟
Availability = چه زمانی در دسترس باشد؟

3- خانواده ISO 27000

مهم‌ترین استانداردها:

موضوع	استاندارد
مفاهیم و واژگان	ISO/IEC 27000
الزامات ISMS	ISO/IEC 27001
راهنمای کنترل‌های امنیتی	ISO/IEC 27002
مدیریت ریسک امنیت اطلاعات	ISO/IEC 27005
مدیریت اطلاعات حریم خصوصی	ISO/IEC 27701

نکته ⭐

ISO 27001 استاندارد اصلی قابل صدور گواهینامه در خانواده 27000 است.

4- ساختار ISO 27001:2022

استاندارد از بندهای زیر تشکیل شده است:

Clause 1 — Scope دامنه کاربرد

Clause 2 — Normative References مراجع الزامی

Clause 3 — Terms and Definitions اصطلاحات و تعاریف

Clause 4 — Context of the Organization زمینه سازمان

Clause 5 — Leadership رهبری

Clause 6 — Planning برنامه‌ریزی

Clause 7 — Support پشتیبانی

Clause 8 — Operation عملیات

Clause 9 — Performance Evaluation ارزیابی عملکرد

Clause 10 — Improvement بهبود

نکته بسیار مهم ⭐⭐⭐

بندهای 4 تا 10 الزامات اصلی سیستم مدیریت هستند.

این ترتیب را حفظ کنید:

Context → Leadership → Planning → Support → Operation → Evaluation → Improvement

---

5- Clause 4 — Context زمینه سازمان

سازمان باید شرایط داخلی و خارجی مؤثر بر ISMS را شناسایی کند.

عوامل داخلی:

- ساختار سازمان
- منابع انسانی
- فناوری
- فرهنگ سازمانی

عوامل خارجی:

- قوانین
- رقبا
- تهدیدهای سایبری
- شرایط اقتصادی

Interested Parties – طرف‌های ذی‌نفع

باید مشخص شود:چه کسانی چه الزامات امنیتی دارند؟ مثلاً:

- مشتریان
- کارکنان
- سهامداران
- نهادهای قانونی
- تأمین‌کنندگان

ISMS Scope – دامنهISMS

باید مشخص شود ISMS دقیقاً چه بخش‌هایی را پوشش می‌دهد. مثلاً: سامانه بانکداری اینترنتی و زیرساخت‌های مرتبط

6- Clause 5 — Leadership رهبری

مدیریت ارشد باید:

- تعهد خود را نشان دهد .
- سیاست امنیت اطلاعات را ایجاد کند .
- مسئولیت‌ها را مشخص کند .
- منابع لازم را تأمین کند .

Information Security Policy – خط‌مشی امنیت اطلاعات

باید جهت‌گیری سازمان در حوزه امنیت اطلاعات را مشخص کند.

نکته ⭐

مسئول اصلی تعهد به:ISMS — Top Managementمدیریت ارشد

امنیت اطلاعات فقط وظیفه واحد IT نیست.

7- Clause 6 — Planning

این قسمت بسیار مهم است. شامل:

- مدیریت ریسک
- اهداف امنیت اطلاعات
- برنامه‌ریزی برای دستیابی به اهداف

Risk Assessment سازمان باید ریسک‌های امنیت اطلاعات را شناسایی و ارزیابی کند.

فرمول ساده: Risk = Likelihood × Impact

مثال: تهدید: Ransomware (احتمال: زیاد اثر: بسیار زیاد ⟶ریسک بالا)

Risk Treatment پس از ارزیابی، سازمان تصمیم می‌گیرد با ریسک چه کند.

چهار روش معروف:

1. Avoidاجتناب	2. Reduceکاهش	3. انتقال یا اشتراک Transfer/Share	4. Acceptپذیرش

Residual Risk ریسک باقی‌مانده : بعد از اعمال کنترل‌ها همچنان مقداری ریسک باقی می‌ماند.

مثال:

قبل از کنترل:	بعد از:
ریسک حمله = بالا	• Firewall • MFA • EDR ریسک = متوسط
	این ریسک متوسط: Residual Risk است.

8- Statement of Applicability — SoA

یکی از مهم‌ترین نکات آزمونی ISO 27001 ☆☆☆

SoAچیست؟ Statement of Applicability =بیانیه کاربردپذیری

سندی که مشخص می‌کند:

- چه کنترل‌هایی انتخاب شده‌اند؟
- چرا انتخاب شده‌اند؟
- کدام کنترل‌ها اجرا شده‌اند؟
- چرا کنترل‌هایی ممکن است اعمال نشوند؟

ارتباط SoA با Annex A

در ISO 27001:2022 ، Annex A شامل 93 کنترل است.

اما:	بلکه:
❌ سازمان الزاماً نباید هر 93 کنترل را اجرا کند.	✅ براساس ریسک و نیاز سازمان، کنترل‌های مناسب انتخاب می‌شوند. و در SoA مستند می‌شوند.

9- Annex A کنترل‌های امنیتی

در نسخه 2022: 93کنترل در چهار گروه:

A.8	A.7	A.6	A.5
Technological Controls کنترل‌های فناوری	Physical Controls کنترل‌های فیزیکی	People Controls کنترل‌های مرتبط با افراد	Organizational Controls کنترل‌های سازمانی
34کنترل	14کنترل	8کنترل	37کنترل
مثال: • کنترل دسترسی • رمزنگاری • Backup • Logging • امنیت شبکه	مثال: • کنترل ورود به اتاق سرور • حفاظت تجهیزات • نظارت فیزیکی	مثال: • آموزش امنیت • مسئولیت کارکنان • شرایط استخدام • آگاهی امنیتی	مثال: • سیاست امنیت اطلاعات • مدیریت دارایی‌ها • مدیریت تأمین‌کنندگان • مدیریت رخدادهای امنیتی

جمع: 93 = 34 + 14 + 8 + 37

⭐⭐⭐این عدد را حتماً حفظ کنید.

10- Clause 7 — Support پشتیبانی.ISMS

شامل:

Resources منابع

Competence شایستگی

Awareness آگاهی

Communication ارتباطات

Documented Information اطلاعات مستند

نکته آزمونی:

کارکنان باید نسبت به موارد زیر آگاه باشند :

- سیاست امنیت
- نقش خود
- پیامد عدم رعایت

11- Clause 8 — Operation عملیات

سازمان باید فرآیندهای لازم برای اجرای ISMS را برنامه‌ریزی و کنترل کند.

شامل:

- اجرای ارزیابی ریسک
- اجرای Risk Treatment
- کنترل فرآیندها
- مدیریت تغییرات

12- Clause 9 — Performance Evaluation ارزیابی عملکرد

یکی از بخش‌های مهم: Monitoring & Measurement

باید مشخص شود:

- چه چیزی اندازه‌گیری شود؟
- چگونه؟
- چه زمانی؟
- چه کسی؟

Internal Audit ممیزی داخلی

سازمان باید به‌صورت دوره‌ای بررسی کند: آیا ISMS مطابق الزامات استاندارد و الزامات خود سازمان اجرا شده است؟

Management Review بازنگری مدیریت

مدیریت ارشد عملکرد ISMS را بررسی می‌کند.

مثلاً:

- نتایج ممیزی
- وضعیت ریسک
- رخدادهای امنیتی
- فرصت‌های بهبود

13- Clause 10 — Improvement بهبود

شامل:

Continual Improvement بهبود مستمر.ISMS	Corrective Action اقدام اصلاحی یعنی: • علت را پیدا کنیم . • مشکل را اصلاح کنیم . • از تکرار جلوگیری کنیم .	Nonconformity عدم انطباق مثال:کنترل دسترسی طبق سیاست سازمان اجرا نشده است.

14- Internal Audit وManagement Review

این دو را اشتباه نگیرید:

Management Review	Internal Audit
بازنگری مدیریت	ممیزی داخلی
بررسی عملکرد کلی	بررسی انطباق
توسط مدیریت ارشد	معمولاً توسط ممیز داخلی
تصمیم‌گیری و جهت‌دهی	شواهد و عدم انطباق

15- ISO 27001 وISO 27002

ISO 27001 می‌گوید: چه الزاماتی باید وجود داشته باشد؟

ISO 27002 می‌گوید: برای کنترل‌های امنیتی چگونه راهنمایی عملی داشته باشیم؟

حفظ کنید:

27001 = Requirements
27002 = Guidance

16- تفاوت ISO 27001 وISO 27005

ISO 27001 استانداردISMS

ISO 27005 راهنمای مدیریت ریسک امنیت اطلاعات

پس: 27005بیشتر روی Risk Managementتمرکز دارد.

17- چند مفهوم بسیار مهم امنیتی

Authentication	Authorization	Accounting / Auditing
احراز هویت تو چه کسی هستی؟ مثال: Username + Password	مجوزدهی چه کاری اجازه داری انجام دهی؟	ثبت و بررسی فعالیت‌ها. مثلاً: چه کسی وارد سیستم شد؟ چه فایلی را تغییر داد؟

نکته:

Authentication = Who are you?
Authorization = What can you do?

18- Least Privilege حداقل سطح دسترسی

هر کاربر فقط به اندازه نیاز کاری خود دسترسی داشته باشد.

مثال: کارمند منابع انسانی لازم نیست به Database واحد مالی دسترسی کامل داشته باشد.

19- Defense in Depth دفاع در عمق

به‌جای یک کنترل، چند لایه کنترل استفاده کنیم. اگر یک کنترل شکست خورد، کنترل دیگری وجود داشته باشد.

مثلاً:

```
Firewall
↓
Network Security
↓
MFA
↓
Endpoint Security
↓
Encryption
↓
Backup
```

20- Backup و امنیت اطلاعات

Backup برای Availabilityبسیار مهم است. اما: Backupبه‌تنهایی امنیت اطلاعات نیست.

باید موارد نیز در نظر گرفته شود.:

- رمزنگاری
- کنترل دسترسی
- تست بازیابی
- نگهداری نسخه‌های مناسب

21- Business Continuity

در امنیت اطلاعات، دسترس‌پذیری بسیار مهم است.

دو مفهوم را بشناسید:

BCP (Business Continuity Plan) برنامه تداوم کسب‌وکار

DR (Disaster Recovery) بازیابی پس از بحران

22- چند کنترل مهم Annex A که ارزش حفظ کردن دارند

برای آزمون، به‌جای حفظ 93 کنترل، این‌ها را بشناسید:

- Information Security Policies
- Asset Management
- Access Control
- Identity Management
- Authentication
- Information Backup
- Logging
- Monitoring
- Cryptography
- Supplier Security
- Incident Management
- Business Continuity
- Secure Coding
- Vulnerability Management
- Configuration Management
- Data Leakage Prevention

23- ارتباط ISO 27001 با COBIT وITIL

این جدول بسیار مهم است:

سؤال اصلی	چارچوب
آیا IT درست حاکمیت و مدیریت می‌شود؟	COBIT
آیا خدمات IT درست ارائه می‌شوند؟	ITIL
آیا امنیت اطلاعات به‌صورت نظام‌مند مدیریت می‌شود؟	ISO 27001

24- چند دام آزمونی مهم ⭐⭐⭐

دام 1

❌اجرای همه 93 کنترل Annex A الزامی است.

✅کنترل‌ها بر اساس فرآیند ارزیابی و درمان ریسک و نیاز سازمان انتخاب می‌شوند و در SoA ثبت می‌شوند.

دام 2

ISO 27001 ❌فقط درباره امنیت سایبری است.

✅دامنه آن Information Security Managementاست و جنبه‌های سازمانی، انسانی، فیزیکی و فناورانه را پوشش می‌دهد.

دام 3

❌امنیت اطلاعات فقط مسئولیت IT است.

✅مدیریت ارشد و کل سازمان در ISMS نقش دارند.

دام 4

ISO 27002 ❌استاندارد قابل صدور گواهینامه ISMS است.

ISO 27001 ✅استاندارد الزامات ISMS و مبنای گواهینامه است.

25- 15نکته‌ای که حتماً قبل از آزمون حفظ کنید ⭐⭐⭐

1. ISO 27001 = ISMS
2. هدف = مدیریت ریسک امنیت اطلاعات
3. CIA = Confidentiality + Integrity + Availability
4. بندهای اصلی 4 = تا 10
5. Clause 4 = Context
6. Clause 5 = Leadership
7. Clause 6 = Planning / Risk
8. Clause 7 = Support
9. Clause 8 = Operation
10. Clause 9 = Performance Evaluation
11. Clause 10 = Improvement
12. Annex A 2022 = 93 Controls
13. چهار گروه 34 + 14 + 8 + 37 =
14. SoA = Statement of Applicability
15. 27001 = Requirements / 27002 = Guidance

🧠نقشه ذهنی یک‌دقیقه‌ای ISO 27001