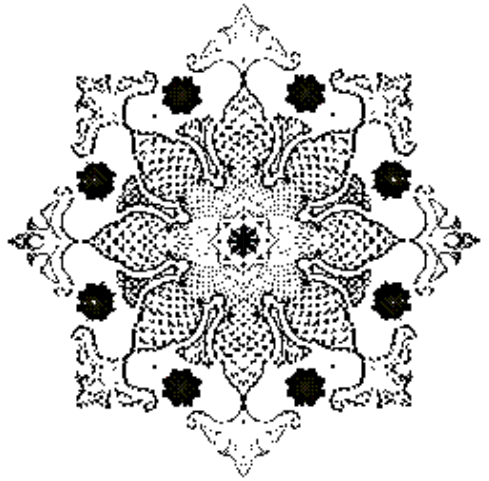
مدیریت تداوم در پسا بحران سایبری

راهکارهای عملی برای تداوم (BCP) و بازیابی از فاجعه (DRP)

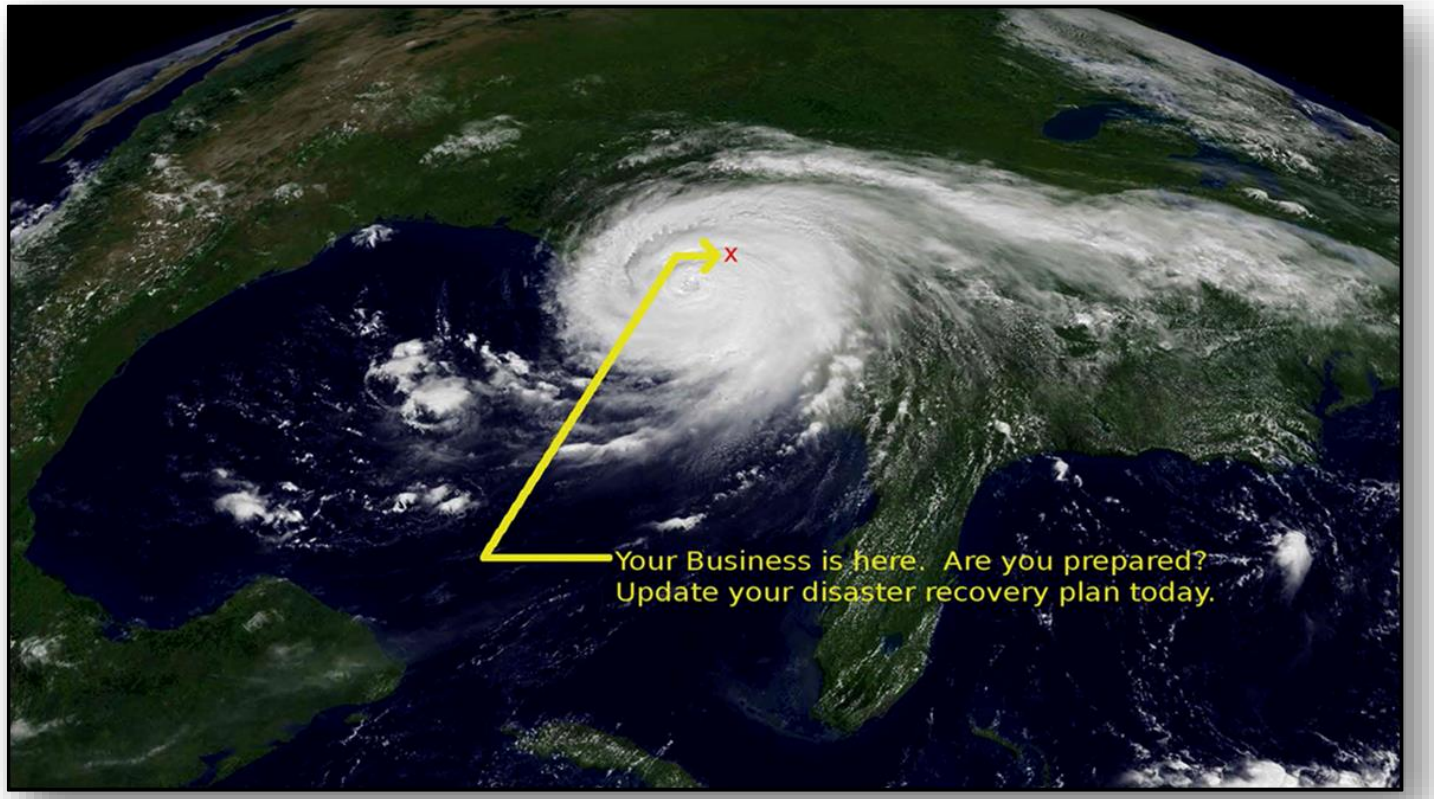
به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید؛ از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.



محمد مهدی واعظی نژاد

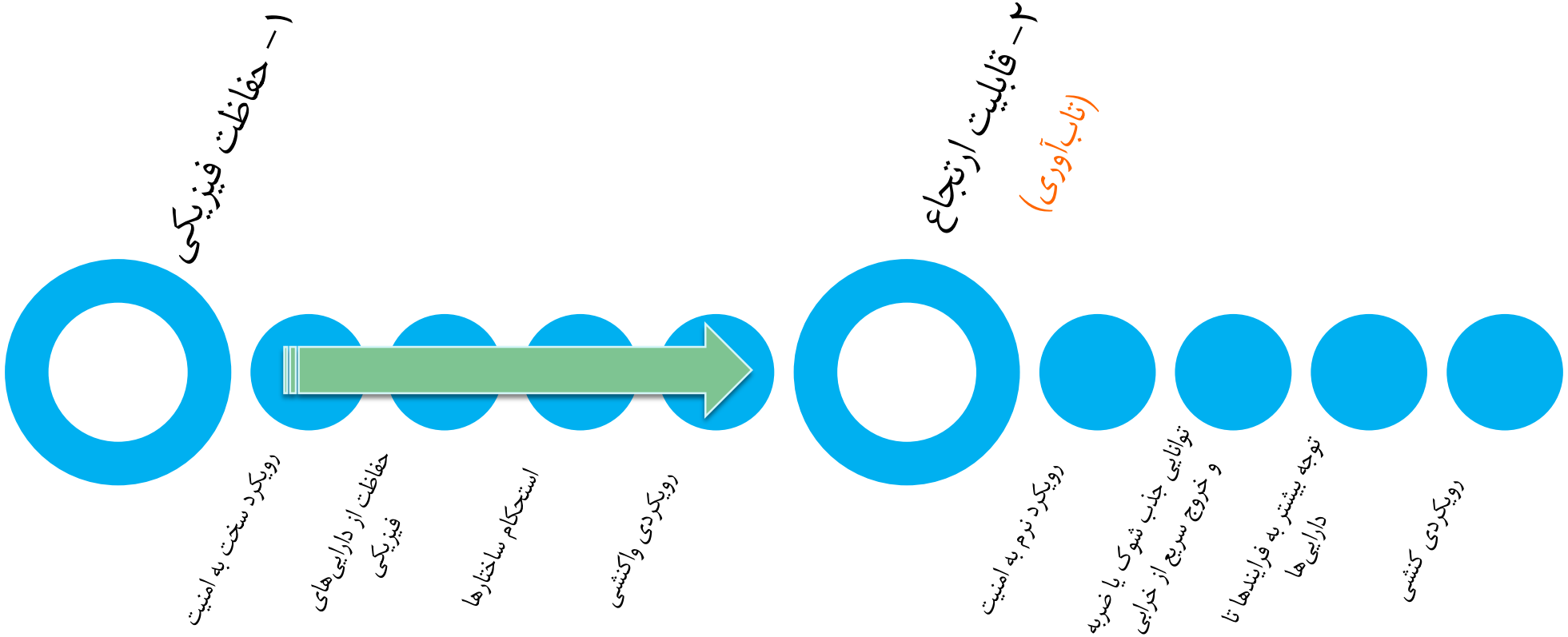
مهندس امنیت فناوری اطلاعات
info@mvaezi.ir

چرا تداوم سرویس‌های کسب‌وکاری مهم است؟



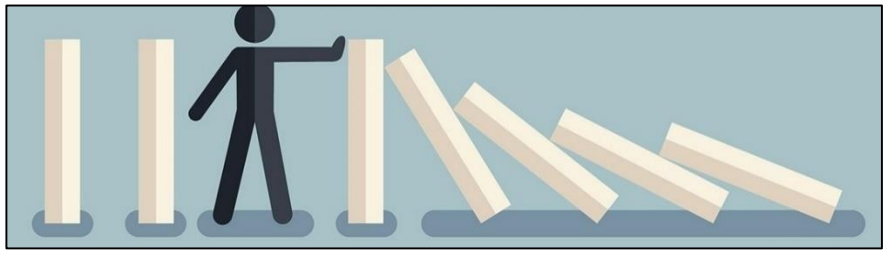
امروزه در بسیاری از موارد، بقا و تداوم شرکت‌ها و سازمان‌ها وابسته به **حفاظت کافی در برابر تهدیدها** است.

رویکردهای حفاظت در برابر تهدیدها



تداوم؛ مفاهیم و کارکردها

- تداوم و بازیابی از فاجعه شامل مجموعه فرایندهایی برای واکنش موفقیت‌آمیز در برابر حملات و تهدیدها
- ایجاد موانع لازم برای جلوگیری از دسترسی مهاجم به آسیب‌پذیرترین و مهمترین دارایی‌های سازمانی و توسعه راهکارهایی به منظور ارایه بدون وقفه سرویس
- رویکردی مبتنی بر سیاست‌های راهبردی جامع در حوزه فناوری اطلاعات، امنیت و لایه‌های مختلف کسب‌وکار



تداوم؛ مفاهیم و کارکردها

- کاملاً مخاطره‌محور و شروع آن با انجام فرایند تحلیل اثر ذینفعان (BIA) و ارزیابی مخاطرات شرکت
- توجه به سطح بلوغ امنیت شرکت در پیاده‌سازی راهکارهای امنیتی پیشنهادی جهت تداوم سرویس‌ها
- طراحی و پیاده‌سازی مجموعه دقیقی از کنترل‌های دنیای واقعی، به منظور حفاظت از دارایی‌های کلیدی
- فراهم کردن زمان بازیابی بهینه برای فعالیت‌های مهم شرکت در صورت ایجاد وقفه برای سرویس‌ها
- تأکید بر بازگرداندن سریع شرکت به حالت اولیه و مرحله قبل از وقوع حمله

تداوم؛ اصول، راهبردها و گام‌های اجرایی

- **اصول کلی تداوم:**

1. شناسایی و طبقه‌بندی سرویس‌ها

- شناسایی و تحلیل تمام سرویس‌های شرکت

2. ارزیابی و مدیریت مخاطرات سرویس‌ها

- تعیین تمام سناریوهای تهدید و مخاطره سرویس‌های سازمانی

تداوم؛ اصول، راهبردها و گام‌های اجرایی

3. اولویت‌بندی سرویس‌ها

- تعیین سرویس‌های حیاتی شرکت و تعیین پاسخ‌های مؤثر در برابر هر یک از تهدیدهای شناسایی شده

4. طراحی و استقرار برنامه تداوم

- تعیین یک معماری مناسب برای تداوم و بازیابی از فاجعه، به منظور تضمین پایداری سرویس‌های شرکت پس از وقوع حمله یا ایجاد بحران

تداوم؛ اصول، راهبردها و گام‌های اجرایی

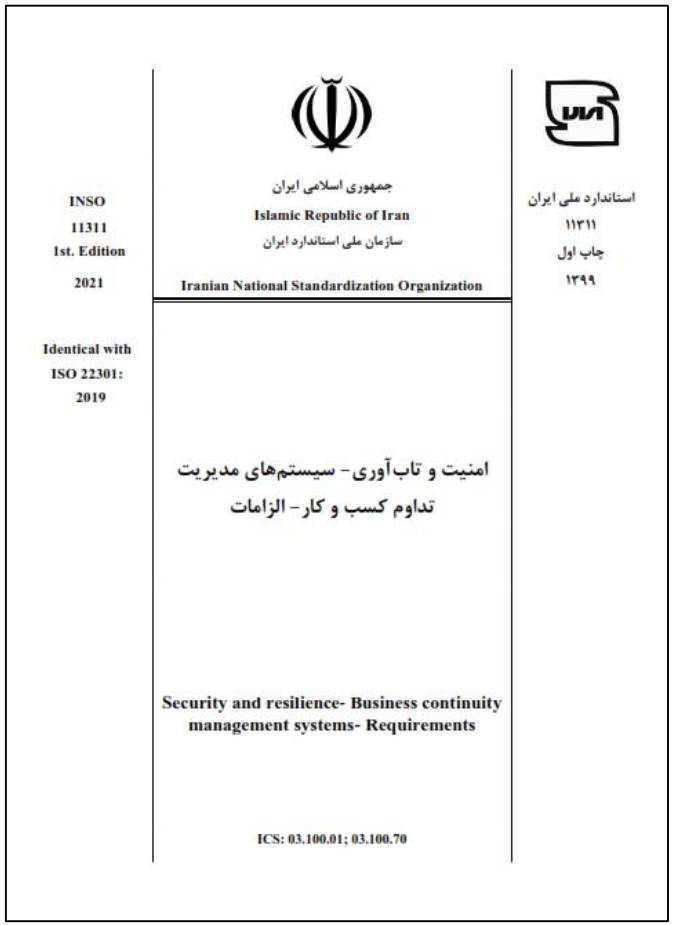
5. آزمون (تست) و بازیابی

- اطمینان از عملکرد مناسب و پایدار سرویس‌ها از طریق برگزاری منظم و دوره‌ای مانورها و نظارت دقیق بر انجام آنها

6. توسعه و بهبود راهکارهای تداوم

- توسعه مداوم معماری تداوم و بهبود راهکارهای اجرایی در نظر گرفته شده، بر اساس درس‌آموخته‌ها و بهین‌تجربه‌ها

استانداردها و بهروش‌های تداوم



INSO
11311
1st. Edition
2021

Identical with
ISO 22301:
2019

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۱۳۱۱
چاپ اول
۱۳۹۹

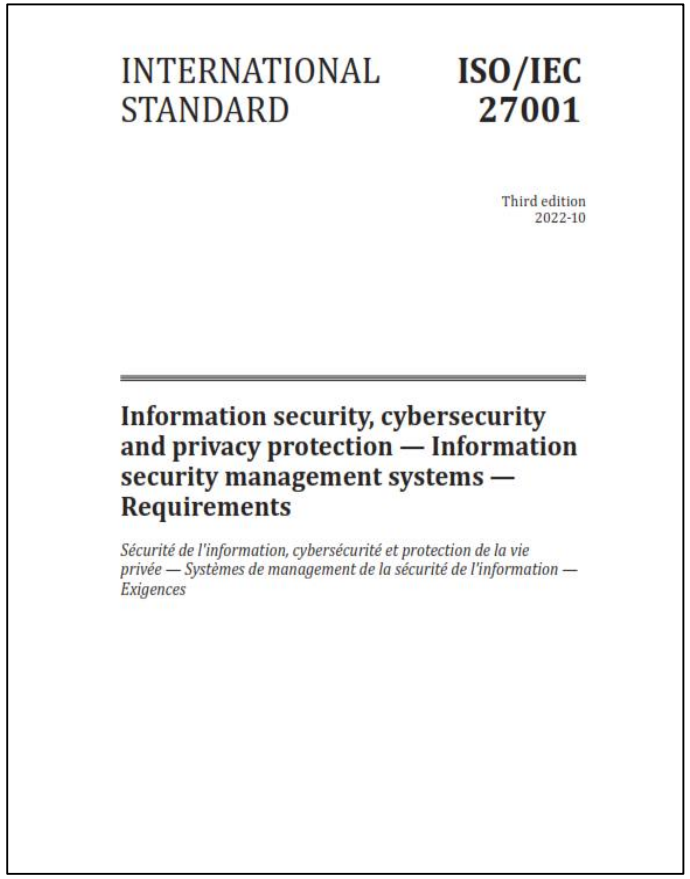
امنیت و تاب‌آوری- سیستم‌های مدیریت
تداوم کسب و کار- الزامات

Security and resilience- Business continuity management systems- Requirements

ICS: 03.100.01; 03.100.70

◄ استاندارد ISO 22301:2019

استانداردها و بهروش‌های تداوم


INTERNATIONAL STANDARD

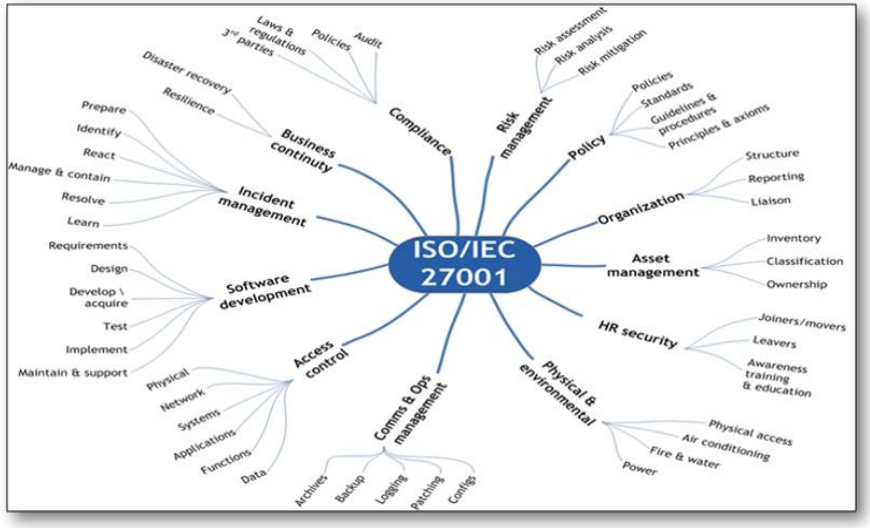
ISO/IEC 27001

Third edition
2022-10

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

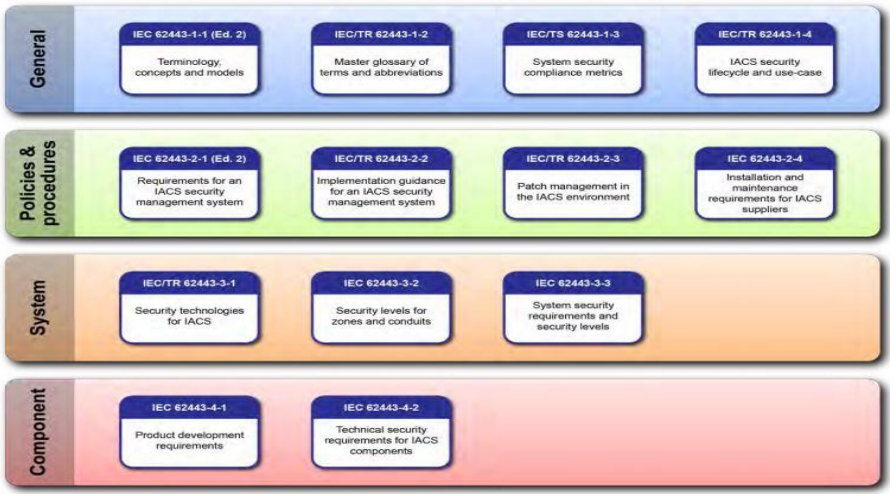
Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

- 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)



استانداردها و بهروش‌های تداوم

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



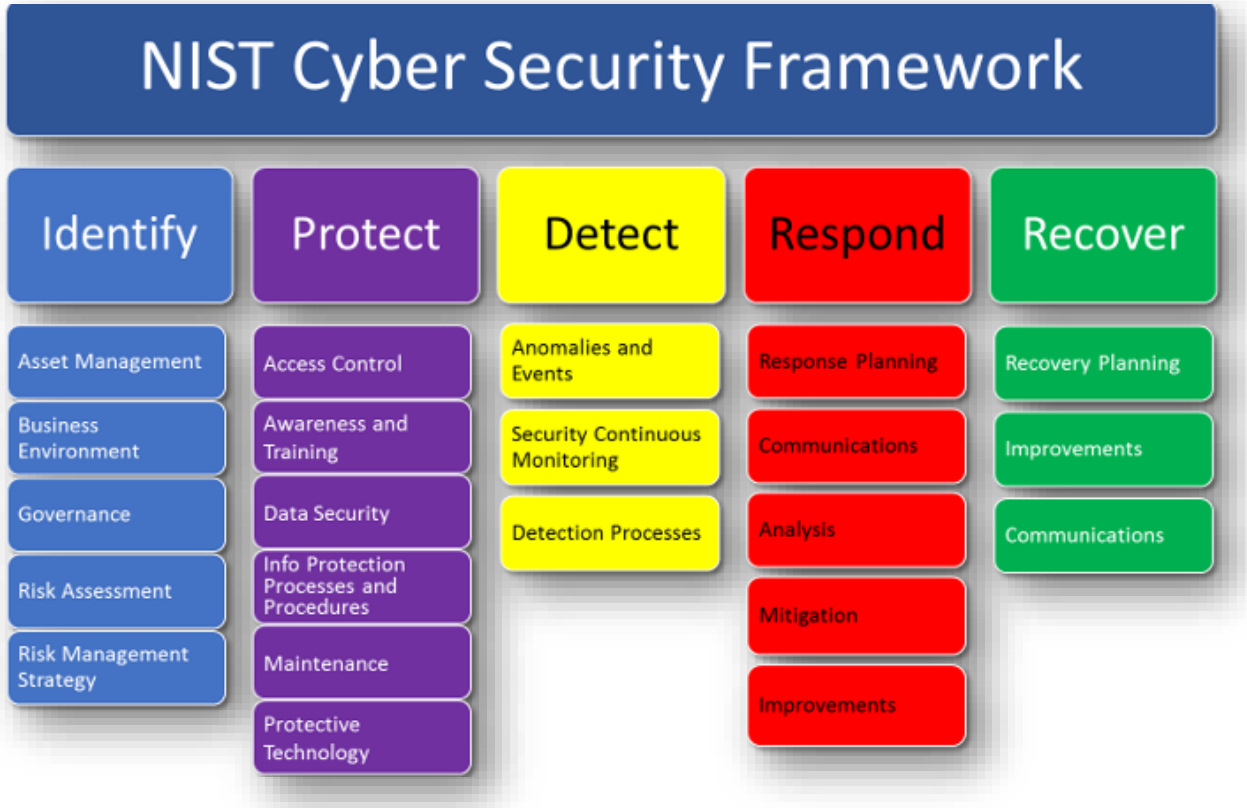
استانداردها و بهروش‌های تداوم

- چارچوب CIS نسخه ۸
- دسته‌بندی تدابیر حفاظتی (۱۸ سرفصل کنترلی و ۱۵۳ کنترل امنیتی)

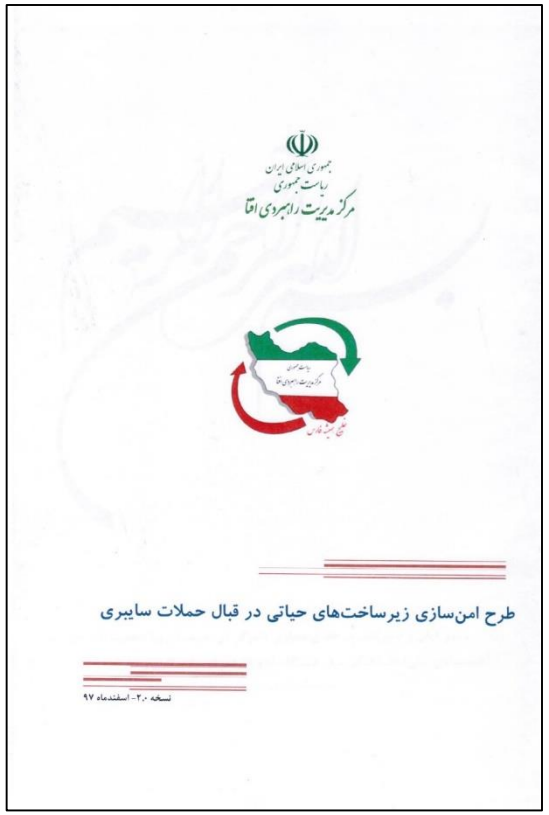
استانداردها و بهروش‌های تداوم

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

NIST CSF ◄



الزامات بالاسری کشور در حوزه مدیریت تداوم

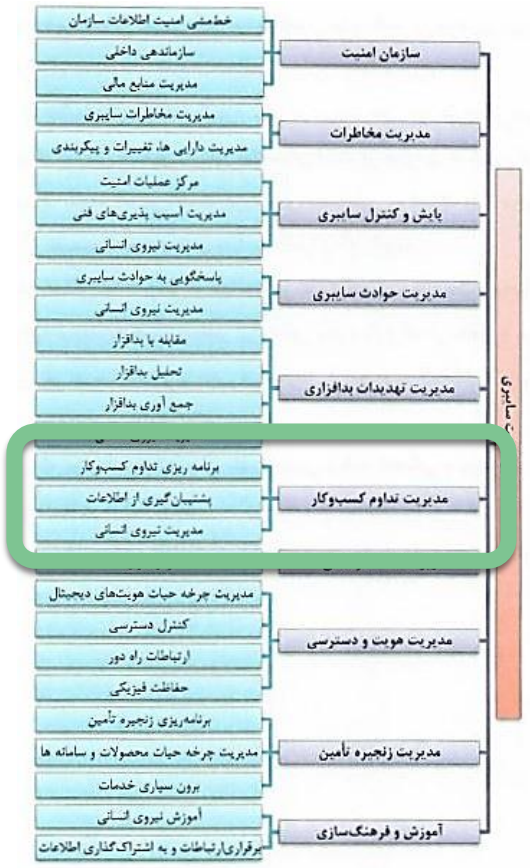


- **طرح کلان امن‌سازی زیرساخت حیاتی مرکز افتای ریاست جمهوری**
  - **کنترل‌های ۹ گانه افتا** (الزامات طرح امن‌سازی):

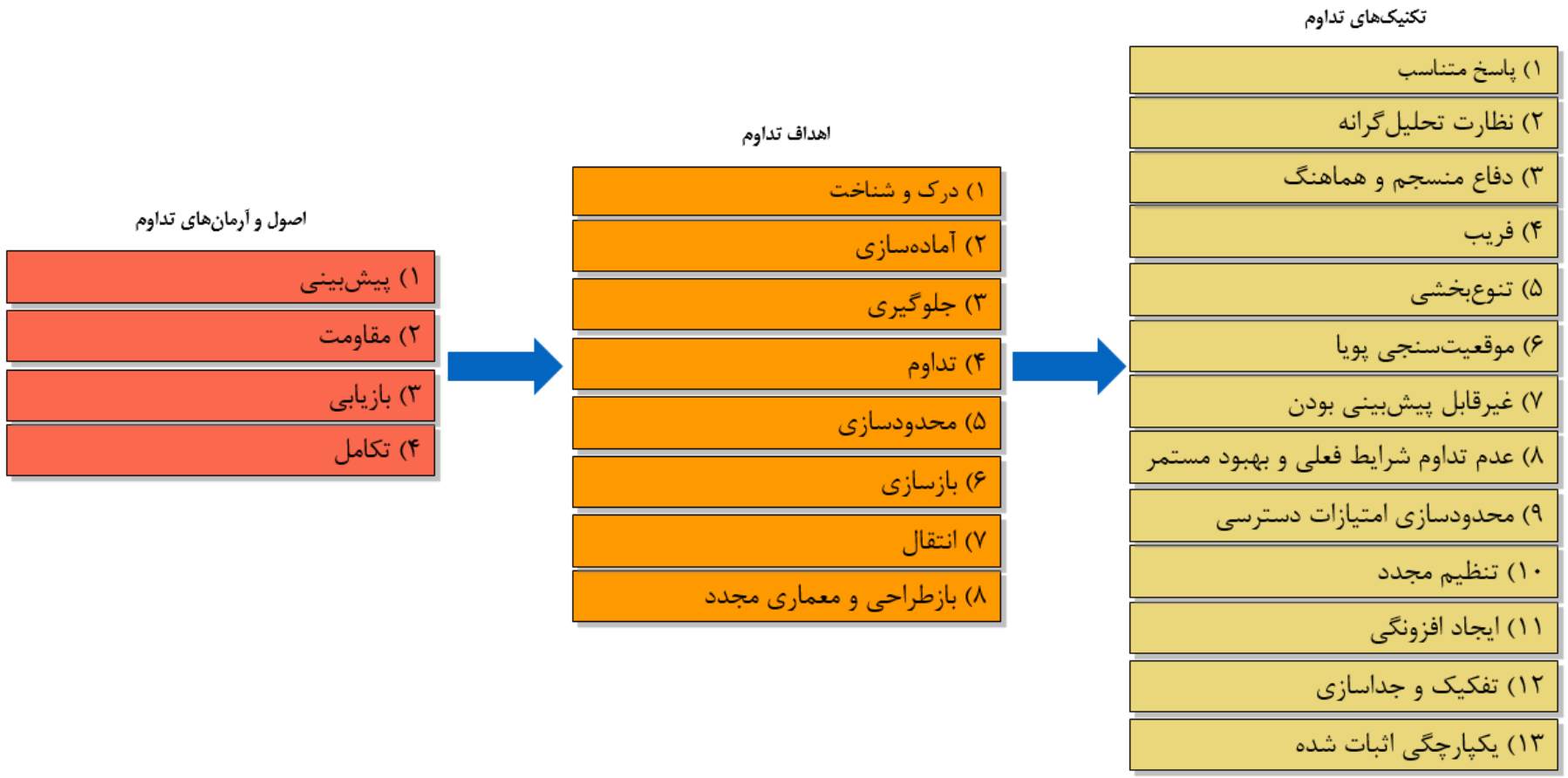
1. **مدیریت مخاطرات**
2. **پایش و کنترل سایبری**
3. **مدیریت حوادث سایبری (IT و OT)**
4. **مدیریت تهدیدات بدافزاری**
5. **مدیریت تداوم کسب‌وکار**
6. **زیرساخت محرمانگی و استنادپذیری**
7. **مدیریت هویت و دسترسی**
8. **مدیریت زنجیره تأمین**
9. **آموزش و فرهنگ‌سازی**

الزامات بالاسری کشور در حوزه مدیریت تداوم

◄ طرح کلان امن‌سازی زیرساخت حیاتی مرکز افتای ریاست جمهوری



حرف اصلی استانداردها و بهروش‌های تداوم



شاخص‌های تداوم و تاب‌آوری سایبری

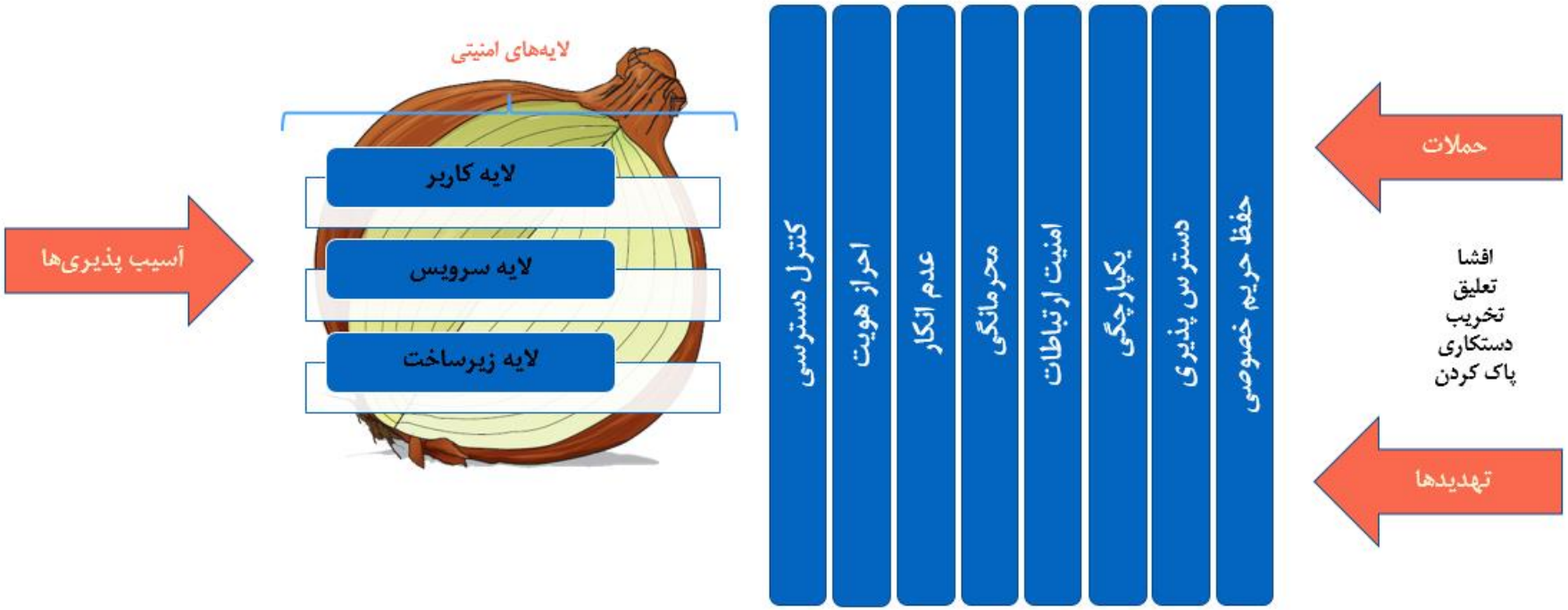
تمامی چارچوب‌ها و بهروش‌های تـداوم، دارای شاخص تاب‌آوری بوده و از طریق اجرا و کنترل مداوم ایـن شـاخص‌ها آن سـازمان را بـه سمت تاب‌آور شدن در مقابل تهدیدات هدایت می‌کنند.

شاخص‌های تداوم و تاب‌آوری سایبری

- بعضی از مهمترین این شاخص‌ها عبارتند از:

1. تعداد حوادث سایبری شناسایی شده ناموفق/ موفق
2. تعداد راهکارهای تدوین شده BCP و DRP برای سرویس‌های مهم سازمانی به کل سرویس‌ها
3. تعداد مانورهای برگزار شده به کل مانورهای پیش‌بینی شده در سال

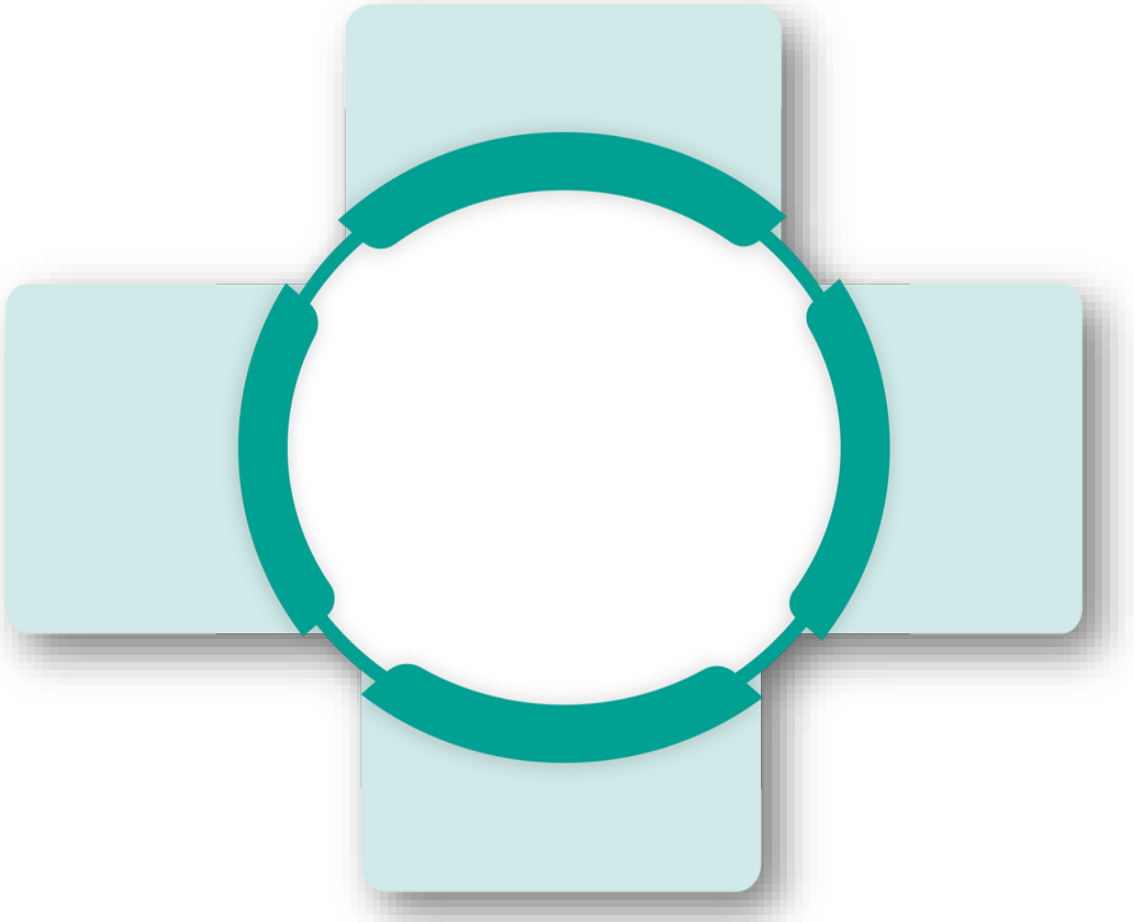
تداوم و تاب‌آوری؛ یعنی:



ایجاد قابلیت تداوم و تاب‌آوری؛ یعنی:

تهدیدها
منابع سازمانی
محدودیت‌های زمانی

راهکار تداوم و تاب‌آوری سازمانی شما؟



تاب‌آوری و تداوم از همین حالا!

با تشکر از توجه شما