# سیستم های اطلاعاتی حسابداری


نویسندگان:

دکتر مهدی مرادی

(دانشیار دانشگاه فردوسی مشهد)

نعیمه بیات


بسم الله الرحمن الرحیم

# فصل هشتم:

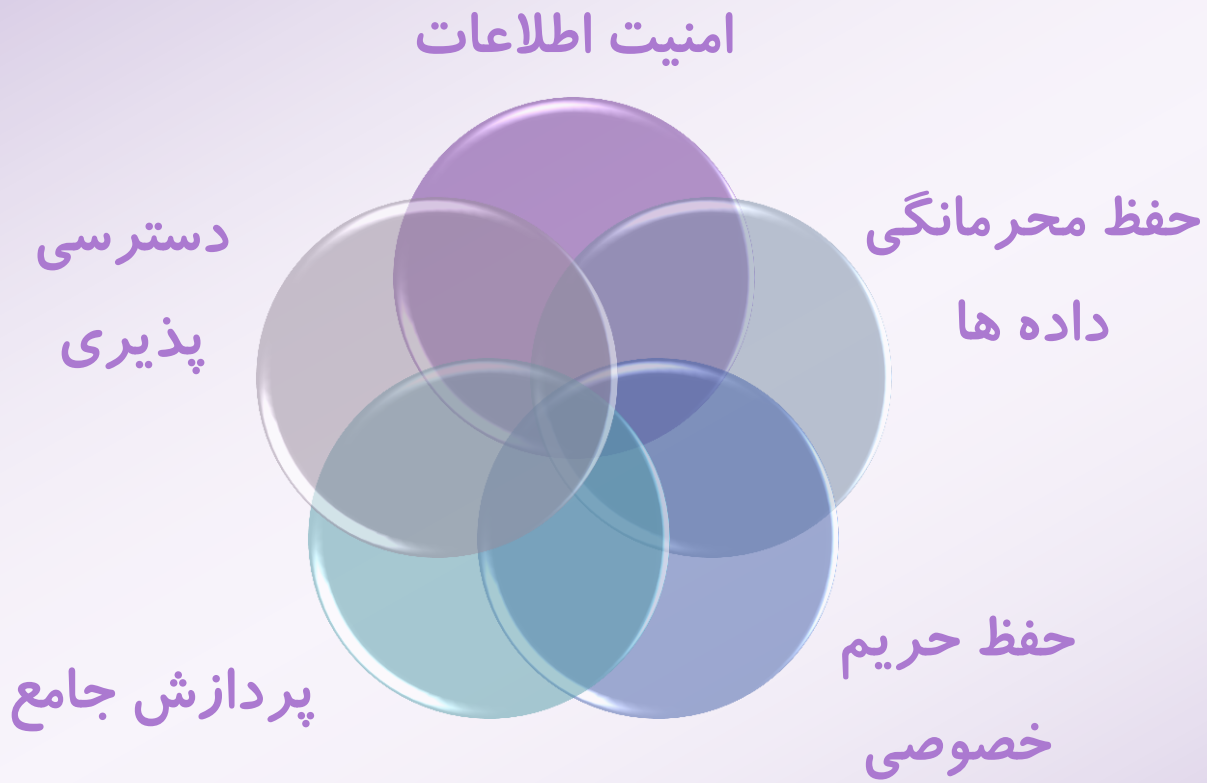
# کنترل در سیستم های اطلاعاتی رایانه ای

# امنیت اطلاعات

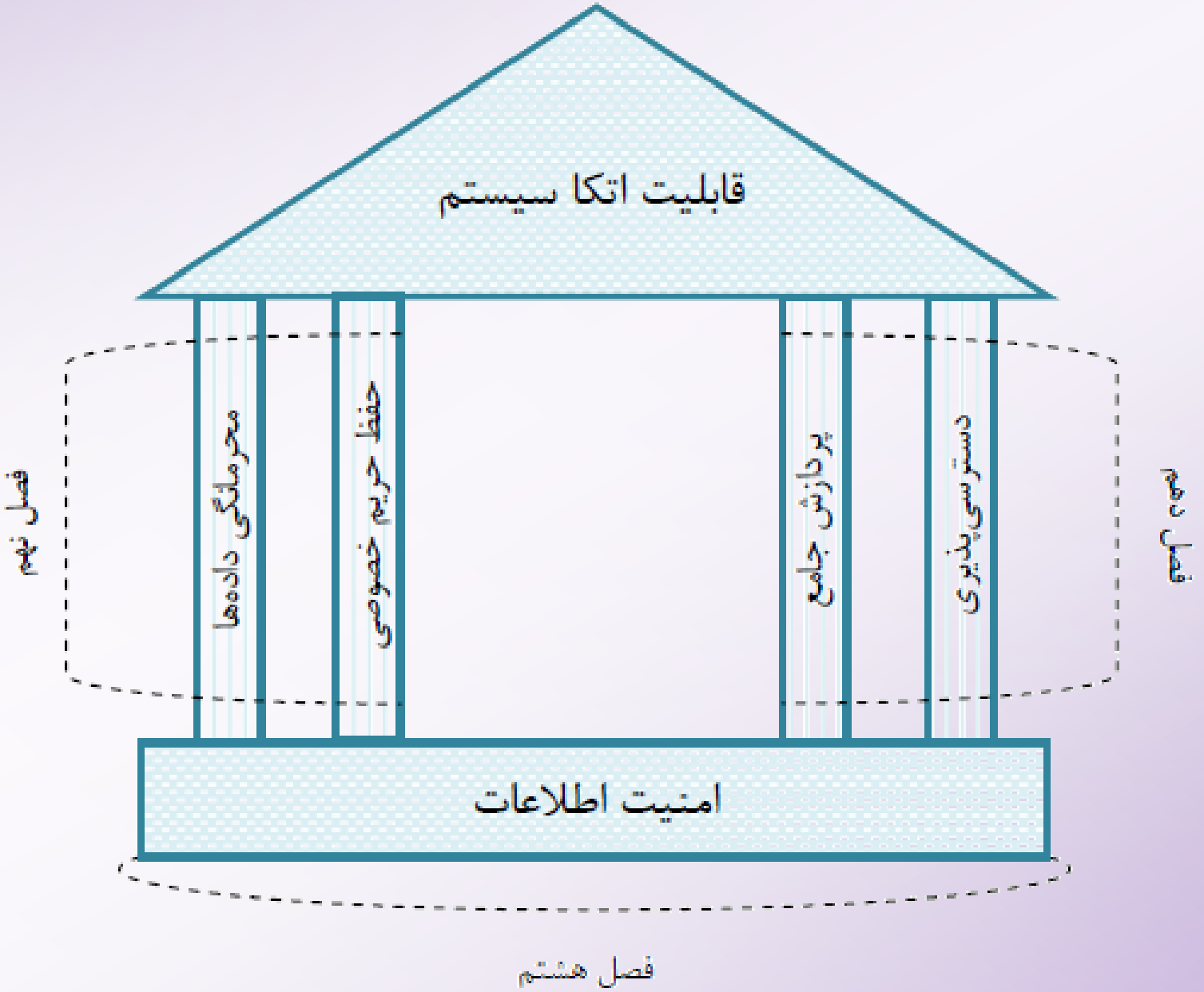
# پس از مطالعه این فصل، خواننده با مفاهیم ذیل آشنا می شود:

۱. آشنایی با مفهوم امنیت اطلاعات و اهداف آن
۲. آشنایی با انواع تهدیدات اطلاعات و سیستم‌های اطلاعاتی
۳. آشنایی با دستورالعمل ها، منابع و استانداردهای امنیت اطلاعات
۴. آشنایی با کنترل‌های داخلی و چارچوب یکپارچه کوزو
۵. آشنایی با چارچوب یکپارچه مدیریت ریسک
۶. آشنایی با چارچوب کوبیت
۷. آشنایی با انواع کنترل‌های کشف‌کننده، اصلاح‌کننده و کنترل‌های پیش‌گیرانه

یکی از ویژگی‌های اساسی که اطلاعات باید دارا باشند، قابلیت اتکا است. کنترل هایی که منجر به افزایش قابلیت اتکا می شود، عبارتند از:



# چارچوب خدمات اطمینان‌بخش برای رسیدن به قابلیت اتکا سیستم



# مفهوم امنیت اطلاعات

امنیت اطلاعات به مفهوم حفاظت و مراقبت از اطلاعات و سیستم‌های اطلاعاتی در مقابل مخاطرات و تهدیدهایی مانند دسترسی، افشا، تغییر و از بین بردن غیرمجاز است.

# امنیت اطلاعات با کمک مولفه های زیر محقق می شود:

## محرمانگی داده یا سیستم

- عبارت است از حفاظت از اطلاعات در مقابل خوانده شدن یا نسخه‌برداری توسط اشخاصی که از جانب مالک آن اطلاعات مجوز دسترسی به آن را ندارند.

## حفظ حریم خصوصی

- عبارت است از اتخاذ تدابیری که از حریم شخصی افراد محافظت می کند.

## جامعیت و درستی

- عبارت است از محافظت از اطلاعات و برنامه‌ها در مقابل هرگونه حذف و تغییر غیرمجاز یا استفاده از آن توسط افراد غیرمجاز.

## دسترسی پذیری

- عبارت است از این که منابع سیستم مانند شبکه‌ها، دسترسی به اینترنت، برنامه‌های کاربردی و داده‌ها با کیفیت قابل قبولی در دسترس افراد مجاز قرار بگیرد.

## چرا امنیت اطلاعات مورد نیاز است؟

اطلاعات، سیستم‌ها، شبکه‌ها و سیستم‌های پشتیبان تصمیم، از دارایی‌های مهم سازمان‌ها هستند. محرمانه بودن، جامعیت و دقت و در دسترس بودن اطلاعات می‌تواند تاثیر فراوانی بر سودآوری، کارایی و اثربخشی سازمان داشته باشد.

# انواع تهدیدهای اطلاعات و سیستم‌های اطلاعاتی

- آتش سوزی، سیل، زلزله، افزایش دما، جنگ و غیره.

**حوادث طبیعی و سیاسی**

- خرابی سخت افزار، تغییرات و نوسان های برقی و خطا های انتقال داده ها.

**خطاها و خرابی‌های نرم‌افزاری و سخت‌افزاری**

- قصور در اجرای وظایف، عدم وجود آموزشهای مناسب، نبود سر پرستی مناسب و غیره.

**بی دقتی و سهل انگاری**

- خرابکاری در سیستم یا بعضی از عناصر آن توسط افراد، سرقت رایانه ای، اختلاس و غیره.

**اقدامات عمدی (جرایم رایانه ای)**

# استانداردها و آیین نامه های منتشر شده درباره امنیت اطلاعات




- موسسه بین‌المللی استاندارد و کمیسیون بین‌المللی الکتروتکنیک
  - *استاندارد مدیریت امنیت اطلاعات* ISO/IEC 27000
  - *استاندارد امنیت تبادل اطلاعات* ISO 27001
  - *استاندارد ارزیابی امنیت فناوری اطلاعات* ISO/IEC 15408
- کمیته سازمان‌های مسئول
  - *چارچوب کنترل های داخلی کوزو*
- انجمن ممیزی و کنترل سیستم‌های اطلاعاتی
  - *چارچوب کوبیت*


Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity Level
Division
Operating Unit
Function

# مكعب كوزو

# نحوه قرارگیری اجزای مختلف مکعب کوزو

ستون عمودی:

سه دسته اهداف (عملیاتی، گزارشگری و رعایت)

بعد سوم:

واحد های مستقل

ستون افقی:

پنج جزء کنترلهای داخلی

مکعب کوزو

# ۱-محیط کنترلی

اصل ۱- پایبندی سازمان به درستکاری و ارزش های اخلاقی

اصل ۲- عمل به مسئولیت های نظارتی

اصل ۳- استقرار ساختار سازمانی مناسب، اختیارات و مسئولیت ها

اصل ٤-تعهد و پایبندی به صلاحیت و شایستگی (شایسته سالاری)

اصل ٥- تاکید بر حسابدهی و پاسخگویی

# ۲- ارزیابی ریسک

اصل ٦- تعیین اهداف موسسه

اصل ۷- شناسایی و تجزیه و تحلیل ریسک

اصل ۸- برآورد امکان وقوع تقلب

اصل ۹- شناسایی و تجزیه و تحلیل تغییرات مهم

# ۳- فعالیت های کنترلی

اصل ۱۰- انتخاب و توسعه فعالیت های کنترلی

اصل ۱۱- انتخاب و توسعه کنترل های عمومی حاکم بر فناوری

اصل ۱۲- گسترش فعالیت های کنترلی از طریق تدوین خط مشی ها و رویه های مناسب

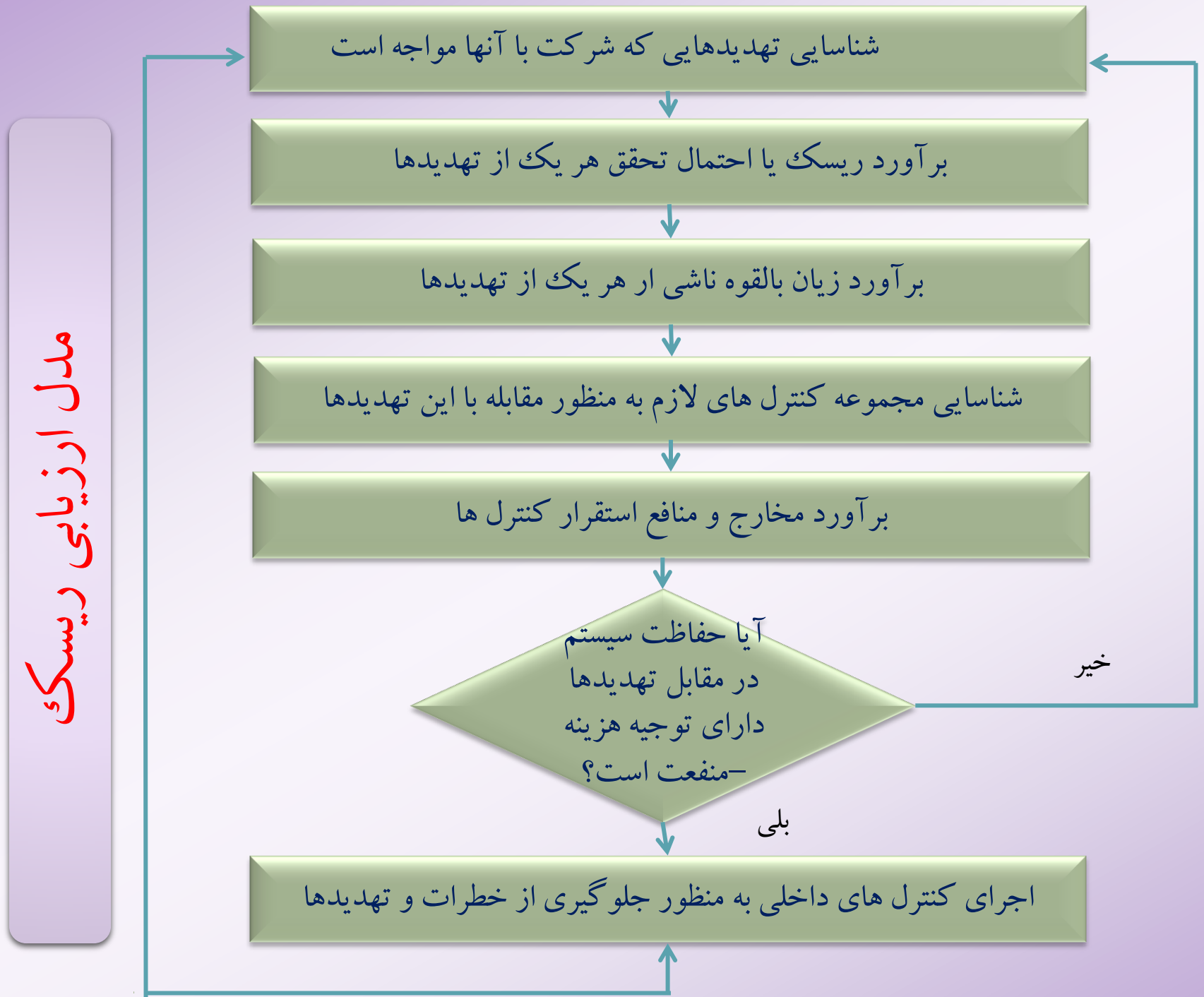
# ٤- اطلاعات و ارتباطات

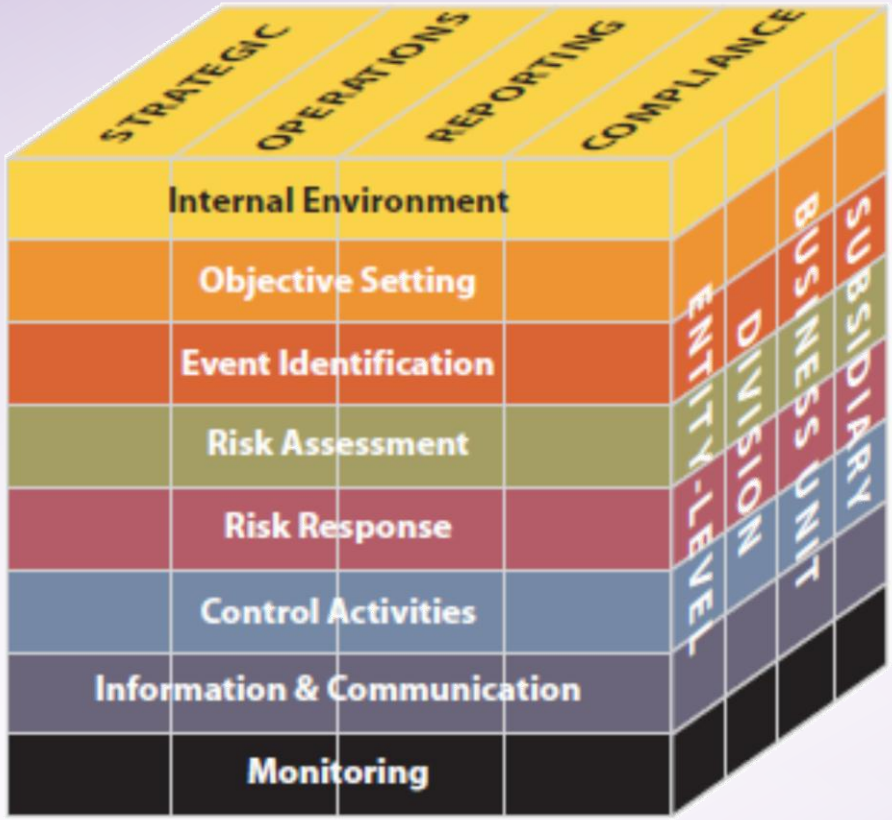
اصل ١٣- استفاده از اطلاعات مربوط

اصل ١٤- ارتباطات داخلی

اصل ١٥- ارتباطات خارجی

# مدل ارزیابی ریسک






# مکعب چارچوب مدیریت ریسک کوزو

# نحوه قرارگیری اجزای مختلف مکعب کوزو

ستون عمودی:

چهار دسته اهداف (استراتژیک،عملیاتی، گزارشگری و رعایت)

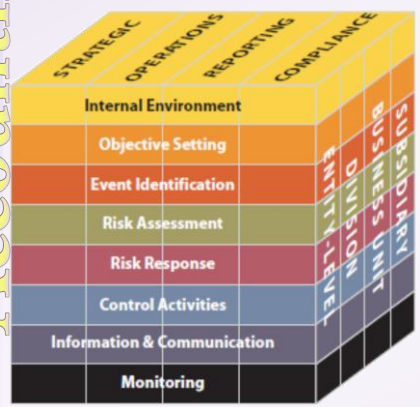
بعد سوم:

واحد های مستقل

ستون افقی:

هشت جزء کنترلهای داخلی

مکعب چارچوب یکپارچه ریسک



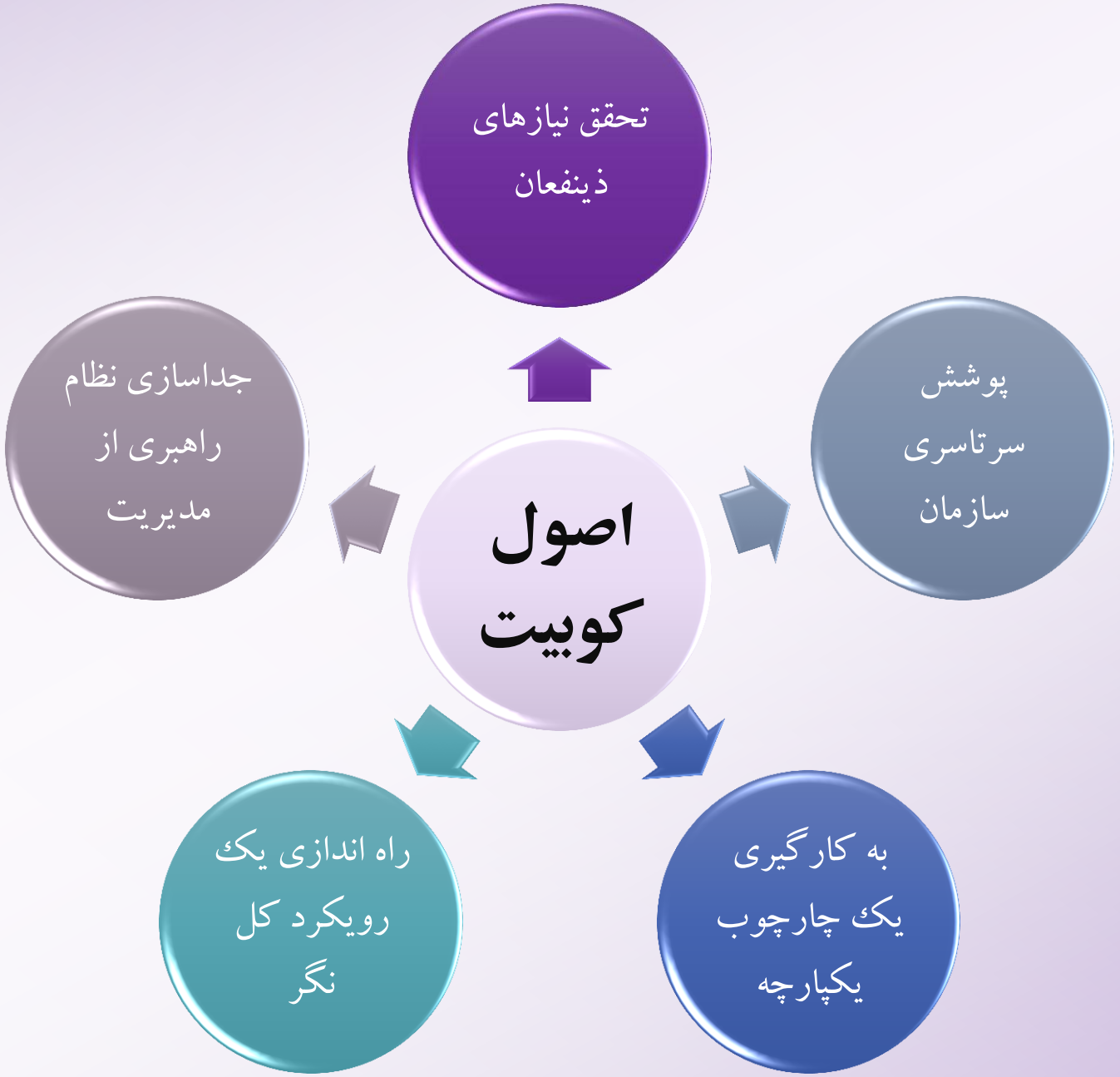

مولفه های
چارچوب یکپارچه
مدیریت ریسک
محیط داخلی
تنظیم
هدف
شناسایی
رویداد
ارزیابی
ریسک
واکنش به
ریسک
فعالیت
های کنترلی
اطلاعات و
ارتباطات
نظارت


## چارچوب کوبیت

چارچوبی که بر اساس آن کنترل های داخلی و کنترل های فناوری اطلاعات به صورت یکپارچه مورد استفاده قرار می گیرند.

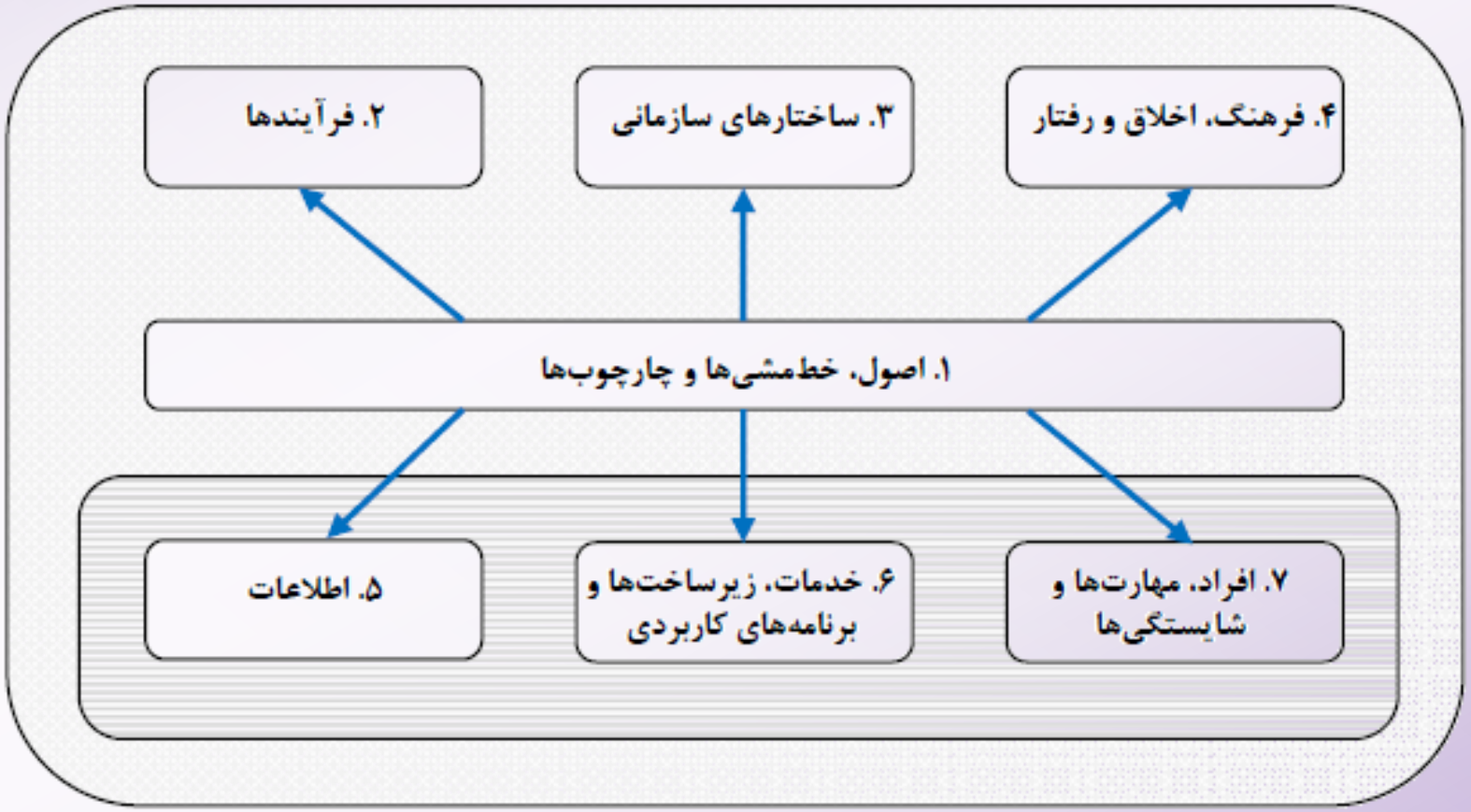
# چارچوب کوبیت

چارچوب کوبیت شامل پنج اصل کلیدی و هفت اصل توانمند ساز است

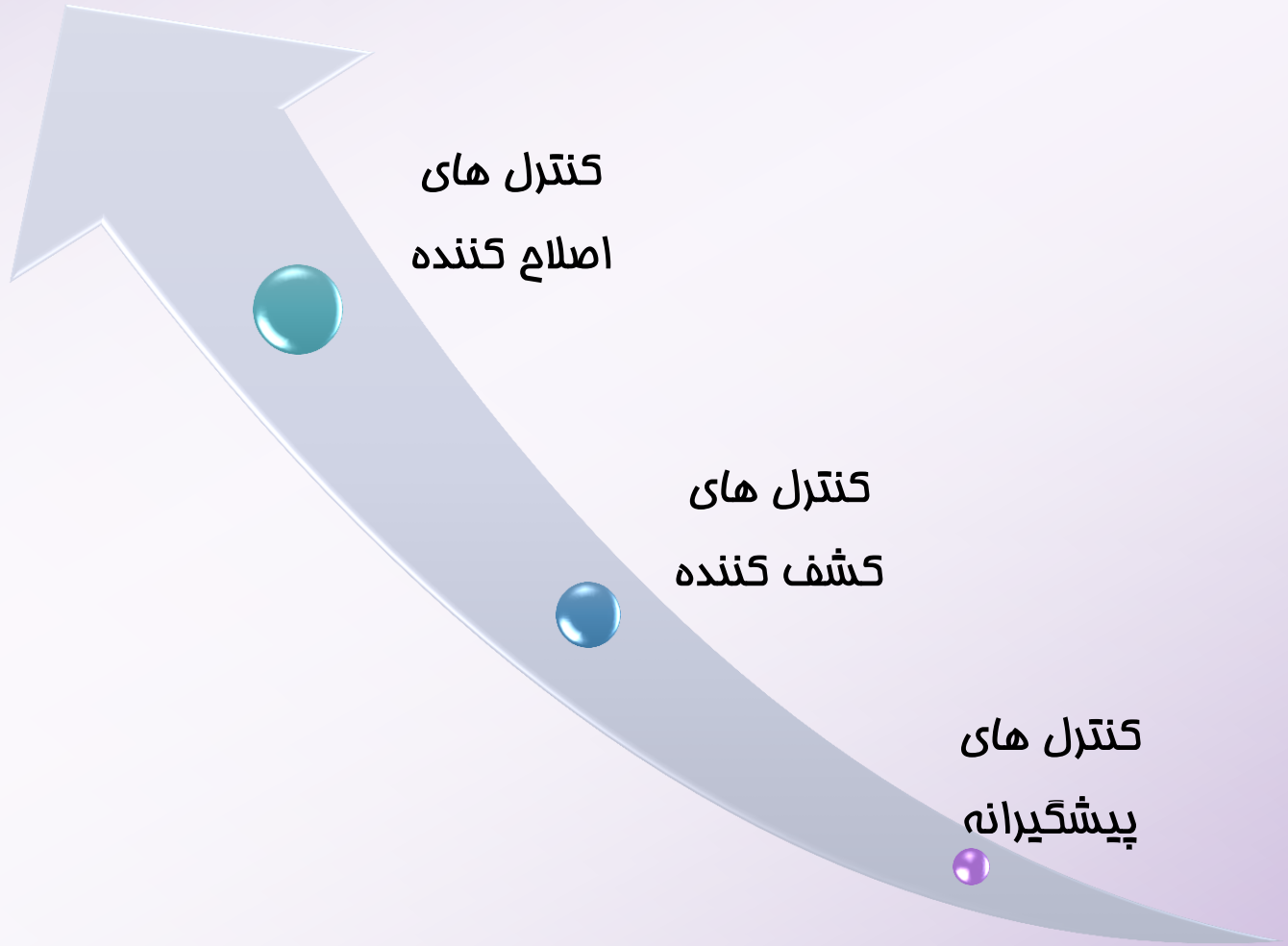


# توان‌مندسازهای کوبیت

برای دستیابی به اهداف اصلی بنگاه، مجموعه‌ای یکپارچه و مرتبط با هم شامل اصول و توانمندسازها در کوبیت درنظر گرفته شده است.



# کنترل های مورد استفاده برای کاهش تهدیدات امنیت اطلاعات




اللهم صل علی محمد و آل محمد