به نام خدا

حسابرسی فناوری اطلاعات با رویکرد

COBIT چارچوبی است که ابزارهایی را در اختیار صاحبان کسب و کار قرار می دهد که به راحتی مسئولیتهای خود در زمینه کنترل فناوری اطلاعات را انجام دهند.

COBIT از COSO و SAC به عنوان بخشی لاینفک از مستندات خود استفاده می کند. بدین معنی که تعریف کنترل را از COSO و تعریف اهداف کنترل فناوری اطلاعات را از SAC به امانت می گیرد.

COBIT برای اولین بار در سال ۱۹۹۶ به وسیله انجمن نظارت بر فناوری اطلاعات آمریکا (IT Governance institiute) مورد بررسی قرار گرفت.

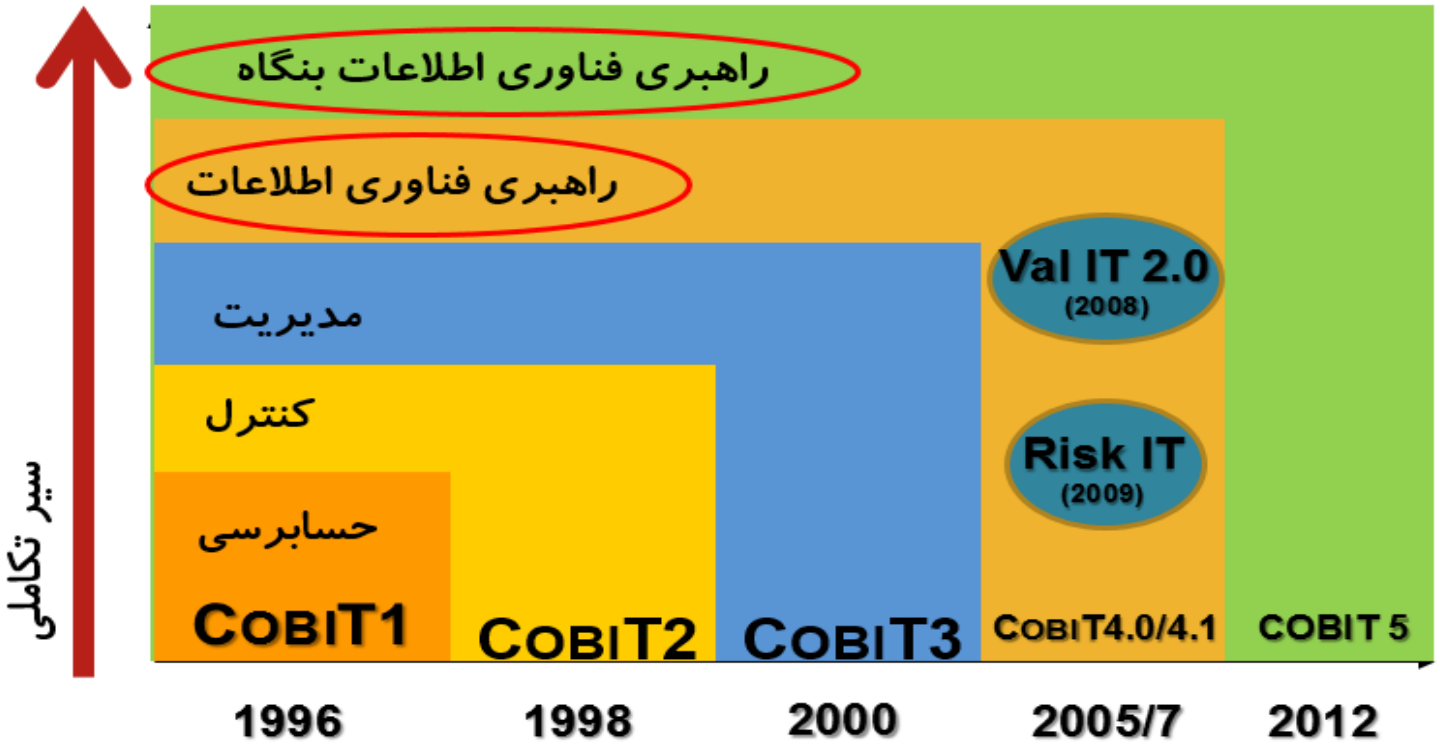
COBIT برای پاسخگویی و هماهنگ سازی منطقی نیازهای سه گروه عمده مدیران ارشد و اعضای هیات مدیره،مدیران فناوری اطلاعات و متخصصان کنترل سازماندهی شده است و نقش هریک را در فرآیندهای ۳۴ گانه فناوری اطلاعات که در الگوی COBIT به ۴ حوزه کلی زیر طبقه بندی شده اند مشخص می نمایند:

COBIT: Control Objectives for Information and Related Technology

COSO :Committee of Sponsoring Organizations of the Treadway Commission

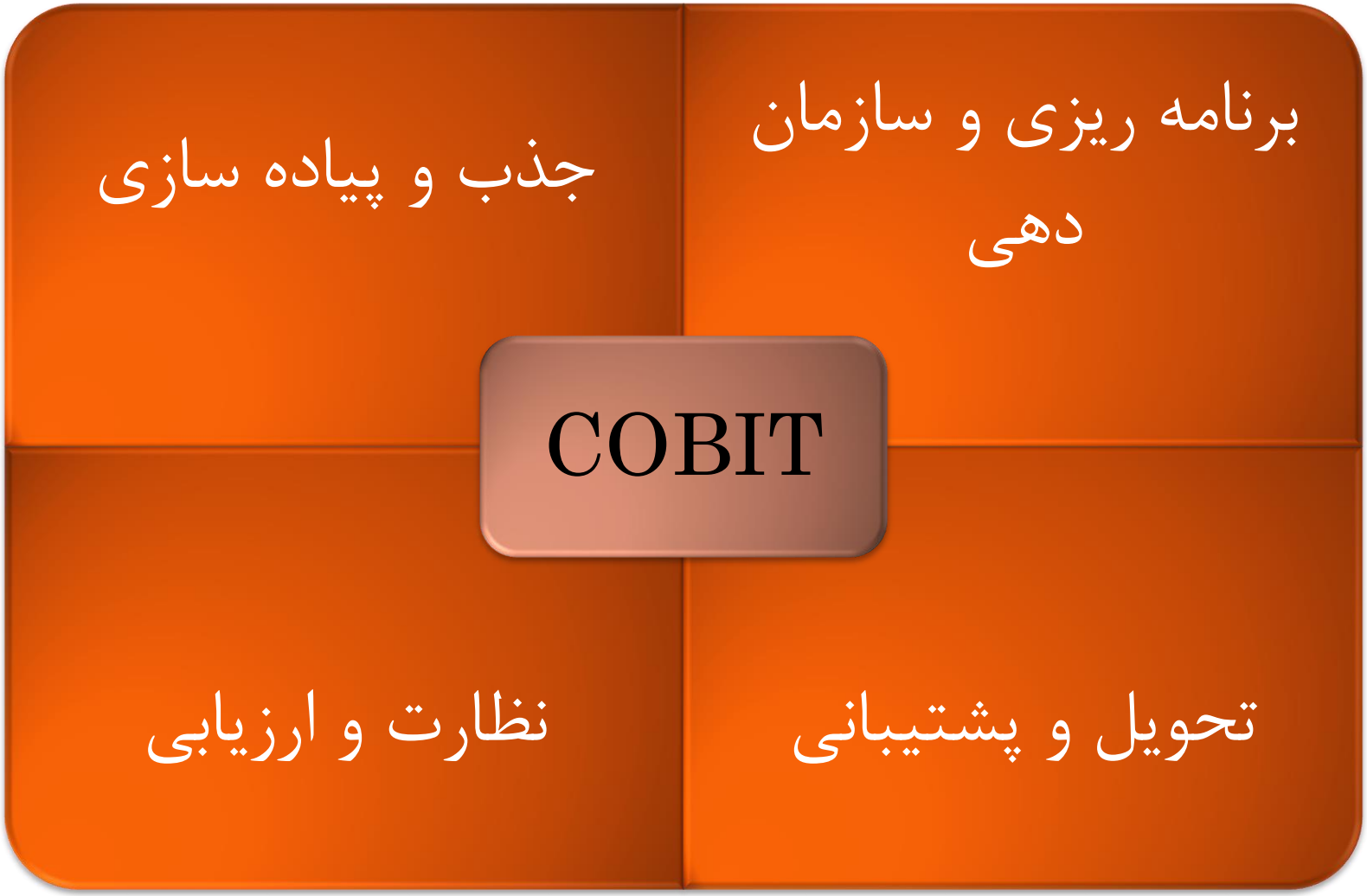
SAC :Systems Auditability and Control

سیر تکاملی کوبیت ۵



COBIT: Governance of Enterprise IT (GEIT)

کوبیت: راهبری فناوری اطلاعات بنگاه


برنامه ریزی و سازمان دهی
جذب و پیاده سازی
COBIT
تحویل و پشتیبانی
نظارت و ارزیابی

چارچوبCOBIT برای رفع نیازهای بنگاه های اقتصادی تمهیدات زیر را به کار می برد:

- برقراری ارتباط با نیازهای کسب و کار
- سازماندهی فعالیتهای فناوری اطلاعات در قالب یک مدل عمومی و قابل قبول در اجرای فرآیندها
- شناسایی منابع عمده و نیازمند بهبود فناوری اطلاعات
- تعریف اهداف کنترل مورد نیاز در سطح مدیریت

در واقع هدف اصلی COBIT پاسخ به سئوالاتی از جمله موارد زیر است:

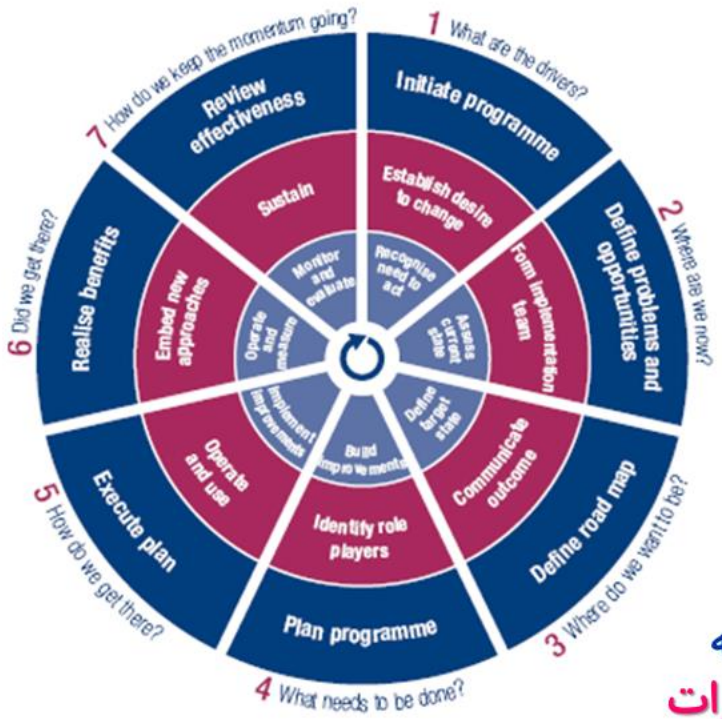
۱- یک بنگاه اقتصادی چگونه باید فناوری اطلاعات را تحت کنترل درآورد تا نیازهای اطلاعاتی بنگاه فراهم شود؟

۲- چگونه باید مخاطرات واحد فناوری اطلاعات را مدیریت کرد؟

۳- چگونه باید اطمینان حاصل نمود واحد فناوری اطلاعات به اهدافش رسیده است؟

۴- آیا واحد فناوری اطلاعات با ملاحظات منفعت- هزینه همراه می باشد؟

پیاده سازی کوبیت ۵



۱. الزامات؟

۲. وضعیت فعلی؟

۳. وضعیت مطلوب؟

۴. برنامه؟

۵. اجرا؟

۶. تحقق اهداف؟

۷. استمرار؟

برنامه

تغییرات

بهبود مستمر

اهمیت بخش امنیت اطلاعات در استاندارد "

۱– امنیت در کامپیوترهای شخصی: (چک لیست ۱۴ بندی)

کنترل های عمومی و کاربردی به نحو مناسب استقرار یافته است.

دستگاه ها و برنامه ها و اطلاعات از ایمنی لازم برخوردار هستند.

نرم افزارهای مورد استفاده مورد اتکا هستند.

گزارش ها و اطلاعات تهیه شده توسط سیستم قابل اعتماد هستند.

۲– امنیت در سیستم های اطلاعاتی و مراکز کامپیوتری : (چک لیست ۴۲ بندی)

امنیت داده ها

امنیت پایگاه های اطلاعاتی

امنیت سیستم های آنلاین

اهمیت بخش امنیت اطلاعات در استاندارد

۳– امنیت در ورود اطلاعات،پردازش اطلاعات و گزارشات خروجی: (چک لیست ۱۲ بندی)

امنیت طبقه بندی دسترسی های مجاز به اطلاعات

امنیت در مقوله اصلاح اشتباهات

کنترل جامعیت و تمامیت اطلاعات

۴– امنیت در حوزه های پیشگیرانه: (چک لیست ۱۲ بندی)

امنیت در بهنگام سازی سیستم ها

کنترل مستند سازی اطلاعات

اهمیت بخش امنیت اطلاعات در استاندارد

۱– کنترل جامع امنیتی سیستم: (چک لیست ۸۸ بندی)

کنترل وظایف استفاده کنندگان از سیستم و کنترل های دسترسی

کنترل آماده سازی اطلاعات

کنترل ورود اطلاعات

کنترل اصلاح اشتباهات

کنترل عملیات

کنترل نگهداری اطلاعات (فیزیکی)

کنترل نگهداری اطلاعات (سیستمی)

کنترل گزارشات خروجی

کنترل توزیع گزارشات

کنترل ملاحظات منفعت هزینه واحد فناوری اطلاعات

الگوی بلوغ COBIT