بسم الله الرحمن الرحیم

به نام آنکه جان را فکرت آموخت

جایگاه حسابرسی IT
در حاکمیت فناوری اطلاعات

محمد هاشم بت شکن

بانک مسکن

بستر قانونی حاکمیت فناوری اطلاعات

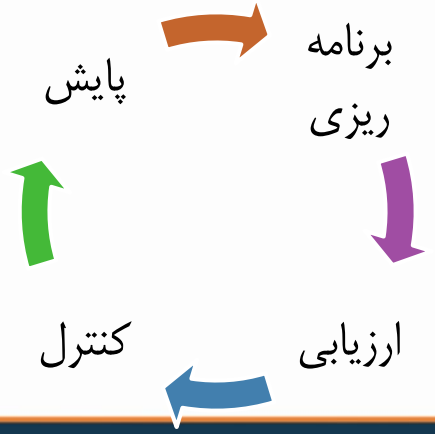
- بند ح ماده ۲ قانون تجارت الکترونیک: ویژگی های سیستم اطلاعاتی مطمئن را سیستمی می داند که به نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد، سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد، به نحوی معقول متناسب با اهمیت کاری که انجام می دهد پیکربندی و سازماندهی شده باشد.
- ماده ۲۹ لایحه قانون بانکداری: مسئولیت سیاستگذاری، مدیریت ریسک، نظارت و اداره کلیه امور بانک براساس قوانین و مقررات برعهده هیأت مدیره ای است که از میان اشخاص حقیقی توسط مجمع عمومی انتخاب می شوند. این هیأت مسئولیت حسن اجرای قوانین و مقررات ناظر بر بانک ها را برعهده دارد.
- ماده 73 لایحه قانون بانکداری: مؤسسه اعتباری موظف است اطلاعات مربوط به صورتهای مالی، مدیریت ریسک، حاکمیت شرکتی، کنترل داخلی، و همچنین گزارش عملکرد هیأت مدیره و رویدادهای با اهمیت طی هر دوره را مطابق با دستورالعملی که با پیشنهاد بانک مرکزی به تصویب هیأت نظارت م یرسد برای عموم منتشر نماید.
- تبصره ۳ ماده ۱۶ قانون رفع موانع تولید رقابت پذیر و ارتقای نظام مالی کشور: در اجرای این ماده وزارت امور اقتصادی و دارایی موظف است ظرف مدت سه سال مطابق دستورالعملی که به تصویب مجمع عمومی بانک ها می رسد، نسبت به بازسازی ساختار مالی و استقرار حاکمیت شرکتی در بانک های دولتی اقدام کند.

بستر مقرراتی حاکمیت فناوری اطلاعات

- بند ۱۰ بخشنامه شماره ۲۴۰۰/مب مورخ ۱۶/۱۲/۸۴ اداره مطالعات و مقررات بانکی بانک مرکزی با عنوان «حسابرسی داخلی در بانک ها و ارتباط بین ناظرین و حسابرسان» درخصوص بررسی و ارزیابی کفایت و کارایی سیستم های کنترل داخلی درحوزه سیستم اطلاعات الکترونیکی و خدمات بانکی الکترونیکی
- بند ۹-۲ از فصل چهارم بخشنامه ۱۱۷۲/مب مورخ ۳۱/۳/۸۶ اداره مطالعات و مقررات بانکی بانک مرکزی با عنوان «رهنمودهایی برای نظام موثر کنترل داخلی در موسسات اعتباری» درخصوص کنترل فرآیند داده پردازی
- اصل ۲۵ از اصول ۲۹ گانه برای نظارت بانکی موثر از انتشارات کمیته نظارت بانکداری بال درخصوص سیاست های و فرآیندهای مربوط به فناوری اطلاعات.

حاکمیت فناوری اطلاعات

- یکی از اجزا حاکمیت شرکتی، حاکمیت فناوری اطلاعات است که مسئولیت آن بعهده هیأت مدیره بانک است
- حاکمیت فن آوری اطلاعات به ساختار سازمانی وشرح وظایف آن اشاره دارد تا اطمینان حاصل شود که فناوری اطلاعات بانک، عملیات بانکی را به خوبی پشتیبانی و تسهیل می نماید. همچنین تضمین می نماید که منابع فناوری اطلاعات به طور موثر مورد استفاده قرار گرفته و ریسکهای مرتبط با فناوری به نحو احسن مدیریت می شوند.

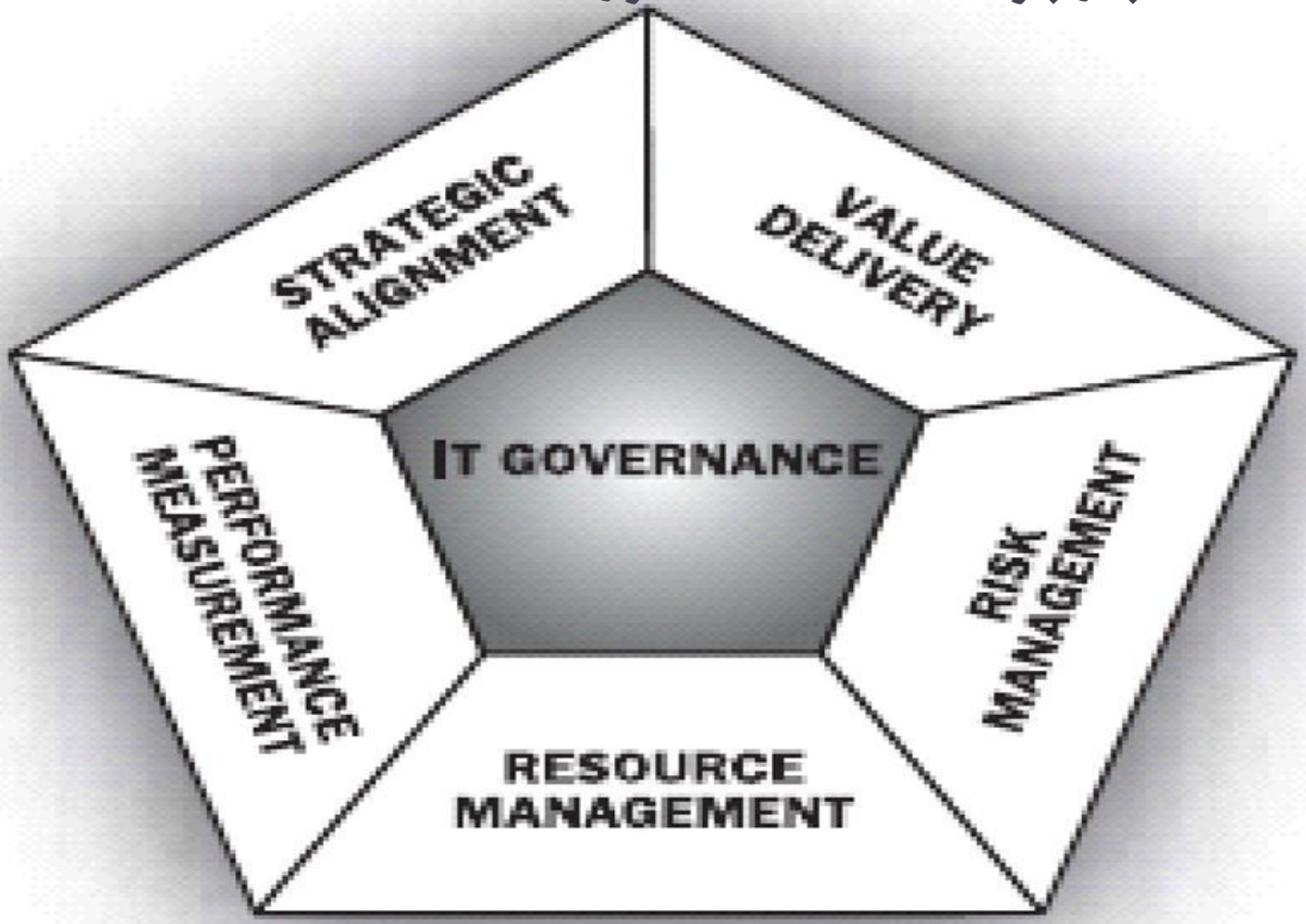


حاکمیت فناوری اطلاعات

- موسسه حاکمیت فناوری اطلاعات(IT Governance Institute) مدعی است که حاکمیت فناوری اطلاعات دارای معنای جداگانه ای نیست. حاکمیت فناوری اطلاعات می بایست یک عنصر پایه ای از عناصر حاکمیت شرکتی باشد و بنابراین نیازمند توجه سطح هیئت مدیره سازمان به منظور تضمین ریسکهای مربوط به فناوری اطلاعات است.

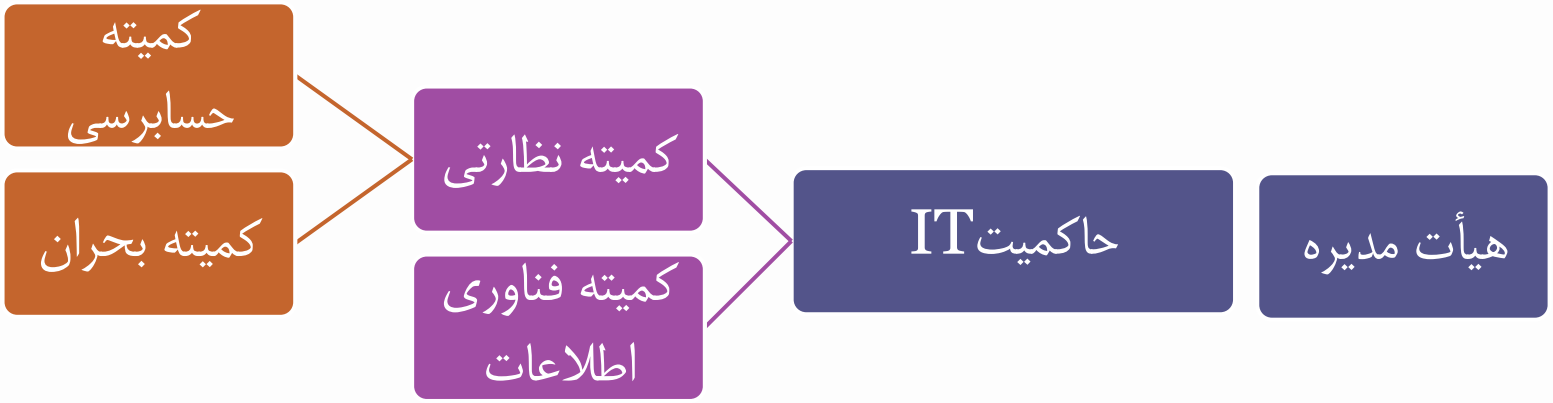
- سیستم مدیریت ریسک فناوری اطلاعات مناسب شامل
  - حاکمیت فناوری اطلاعات
  - فرایند مستمر مدیریت ریسک فناوری اطلاعات
  - اجرای شیوه های صحیح با توجه به کنترل های فناوری اطلاعات

چارچوب حاکمیت فناوری اطلاعات



هیأت مدیره و حاکمیت فناوری اطلاعات

- هیأت مدیره مسئولیت نهایی شناسایی ریسک های فناوری اطلاعات و نظارت بر طراحی و پیاده سازی یک سیستم مدیریت ریسک مناسب را به عهده دارد.
- هیأت مدیره باید طرح های فناوری اطلاعات سیاست ها و هزینه های عمده مربوطه را به تصویب برساند. هدف هیات مدیره حصول اطمینان از انجام فعالیت ها به نحو مطلوب، اتخاذ برنامه های راهبردی مؤثر فناوری اطلاعات و نظارت کارا بر عملکرد فناوری اطلاعات می باشد. برای انجام این مهم، اعضای هیأت مدیره باید با مفاهیم فناوری اطلاعات و مرکز داده ها و فعالیتهای آن آشنا باشد.



نقش کمیته حسابرسی در پیاده سازی حاکمیت فناوری اطلاعات

- هدف از تشکیل کمیته حسابرسی، کمک به ایفای مسئولیت نظارتی هیئت‌مدیره و بهبود آن جهت کسب اطمینان معقول از موارد زیر می باشد:

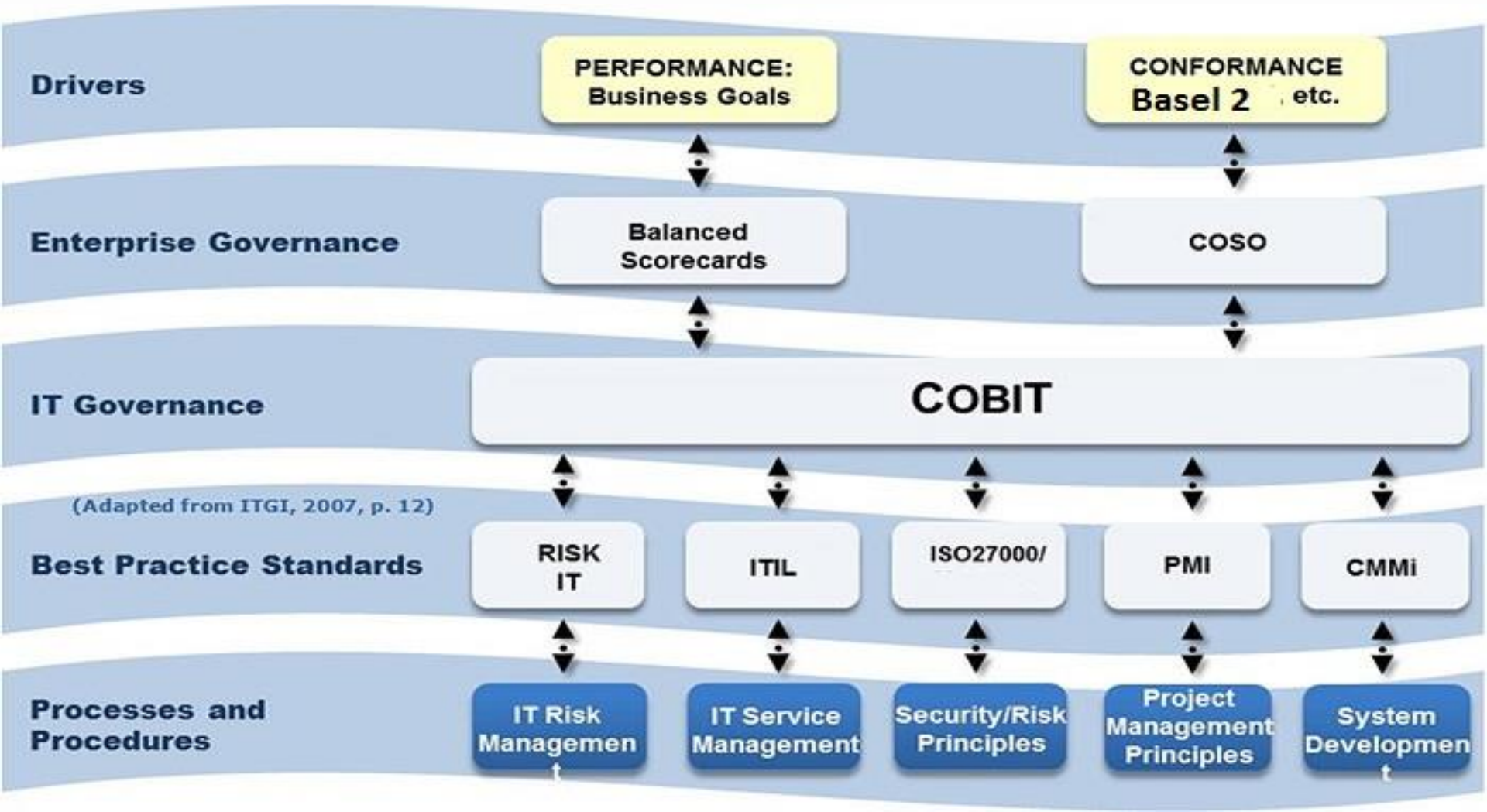
اثربخشی فرآیندهای نظام راهبری، مدیریت ریسک و کنترل‌های داخلی،

سلامت گزارشگری مالی

اثربخشی حسابرسی داخلی و مستقل

رعایت قوانین، مقررات و الزامات.

استاندارد و چارچوب های حسابرسی فناوری اطلاعات



حسابرسی فناوری اطلاعات

- حسابرسی فناوری اطلاعات: فرآیند سیستماتیک جمع‌آوری و ارزیابی بی طرفانه شواهد برای معین کردن اینکه
  - آیا سیستمهای اطلاعاتی از دارایی ها محافظت می کند؟
  - یکپارچگی داده ها را حفظ می کند؟
  - دستیابی به اهداف سازمانی را به صورت موثری محقق می کند؟
  - از منابع، استفاده بهینه می کند؟
- حسابرسی فناوری اطلاعات نمود عینی اتخاذ تدابیر مدیریتی در ریسک های عملیاتی، استراتژیک و شهرت است.
- بهترین روش انجام حسابرسی فناوری اطلاعات اجرای حسابرسی فناوری اطلاعات مبتنی بر ریسک است.
- حسابرسی فناوری اطلاعات باید دو فاکتور زیر را مد نظر قرار دهد:
- ارزیابی کنترل های عمومی
- کنترل برنامه های کاربردی

برنامه حسابرسی فناوری اطلاعات

- ارزیابی اثربخشی برنامه ریزی های مدیریتی و نظارتی فعالیت های IT
- ارزیابی اثربخشی فرآیندهای عملیاتی و کنترل های داخلی
- سنجش کفایت تطابق اقدامات بعمل آمده و روش های کنترل داخلی با سیاست های فناوری اطلاعات
- شناسایی نارسایی ها و ارائه پیشنهادات

شرح وظایف واحد حسابرسی فناوری اطلاعات بانک مسکن

۱. تهیه واجرای یک برنامه (طرح کلی) حسابرسی فناوری اطلاعات قابل انعطاف با بکارگیری متدولوژی مناسب و رویکردی مبتنی بر ریسک .

۲. حسابرسی فعالیتهای فناوری اطلاعات بانک مشتمل بر:

۱ -۲- بررسی و ارزیابی کفایت، کارایی و اثربخشی سیستمهای کنترل داخلی درحوزه فناوری اطلاعات

۲-۲- بررسی کلیه فعالیتهای مربوط به ساختار فناوری اطلاعات بانک و اسناد، قراردادها، معاملات، پروژه ها و گزارشهای تهیه شده به منظور حصول اطمینان از تطبیق آن با الزامات قانونی و مقرراتی، اهداف و اساسنامه بانک و دستورالعملها، آیین نامه ها، استانداردها، خط مشی ها و رویه های مربوطه.

۳-۲- بررسی و آزمون سیستمهای اطلاعاتی و نیز خدمات بانکداری نوین به لحاظ صحت و جامعیت، امنیت و قابل دسترس بودن داده های مالی و غیر مالی.

۴-۲- بررسی اجرای صحیح و مطلوب مصوبات هیات مدیره در حوزه فناوری اطلاعات، در زمان تعیین شده و میزان تحقق برنامه ها و اهداف راهبری بانک در زمینه های مربوط.

۵-۲- بررسی پیشنهادها و توصیه های حسابرسان مستقل در ارتباط با کنترل داخلی سیستمهای اطلاعاتی و پیگیری آنها.

۶-۲-نظارت بر رسیدگی ها و حسابرسی های فناوری اطلاعات برون سپاری شده.

۷-۲-انجام حسابرسی های خاص.

۳. کسب آموزش حرفه ای مستمر در زمینه حسابرسی فناوری اطلاعات.

چارچوب کوزو

اهداف:

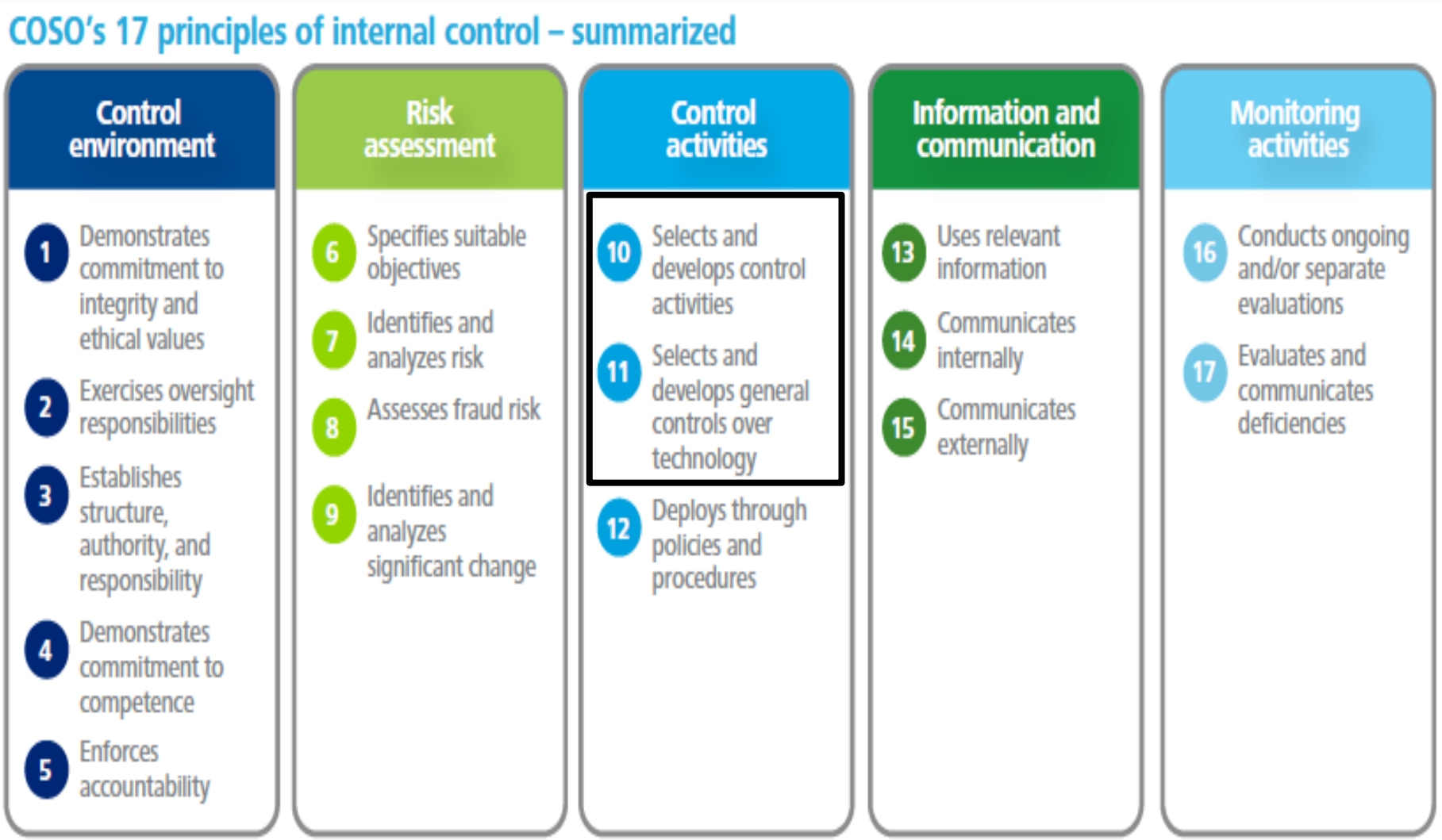
۱-اثربخشی و کارایی عملیات

۲-قابلیت اطمینان گزارشهای مالی

۳- انطباق با قوانین و مقررات

اجزا:

محیط کنترل، ارزیابی ریسک، فعالیتهای کنترلی، اطلاعات و ارتباطات، و نظارت

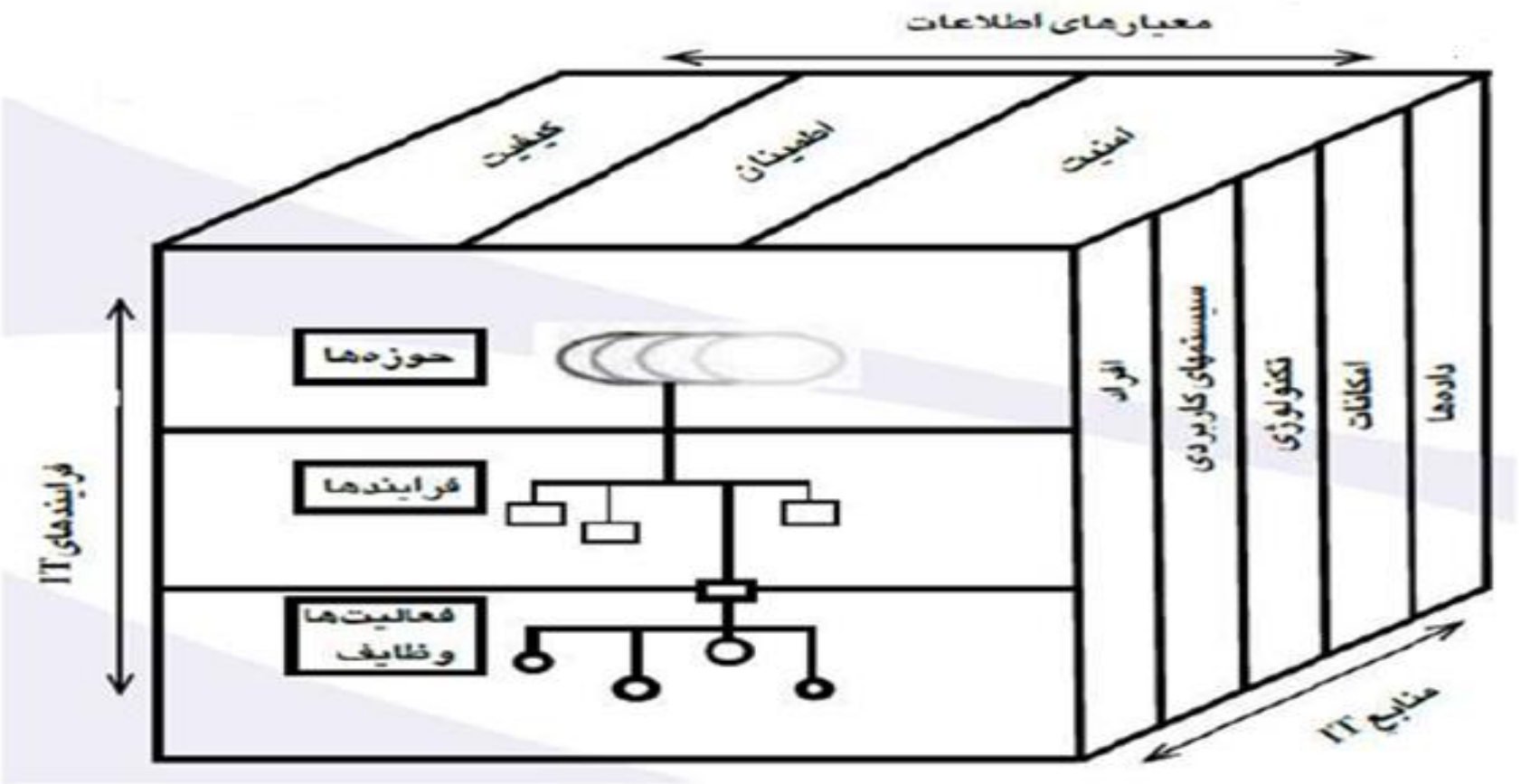

COSO's 17 principles of internal control – summarized
Control environment
1 Demonstrates commitment to integrity and ethical values
2 Exercises oversight responsibilities
3 Establishes structure, authority, and responsibility
4 Demonstrates commitment to competence
5 Enforces accountability
Risk assessment
6 Specifies suitable objectives
7 Identifies and analyzes risk
8 Assesses fraud risk
9 Identifies and analyzes significant change
Control activities
10 Selects and develops control activities
11 Selects and develops general controls over technology
12 Deploys through policies and procedures
Information and communication
13 Uses relevant information
14 Communicates internally
15 Communicates externally
Monitoring activities
16 Conducts ongoing and/or separate evaluations
17 Evaluates and communicates deficiencies
Source: Audit Committee Brief, March 2014. Deloitte Development Corporation. All rights reserved.

حسابرسی فناوری اطلاعات و چارچوب کوبیت

- کوبیت(COBIT)، چارچوبی ارائه شده توسط موسسه نظام حاکمیت فناوری اطلاعات(ITGI) و راه اندازی شده توسط انجمن حسابرسی و کنترل سیستمهای اطلاعاتی(ISACA) برای حسابرسی، کنترل و راهبری فناوری اطلاعات است. کوبیت چارچوب جامعی از هدفهای کنترلی است که به حسابرسان فناوری اطلاعات، مدیران عامل و مدیران فناوری اطلاعات کمک می کند که سیستمهای فناوری اطلاعات خود را درک کرده و از سطح امنیت، اطمینان و کیفیت آنها آگاهی یابند.

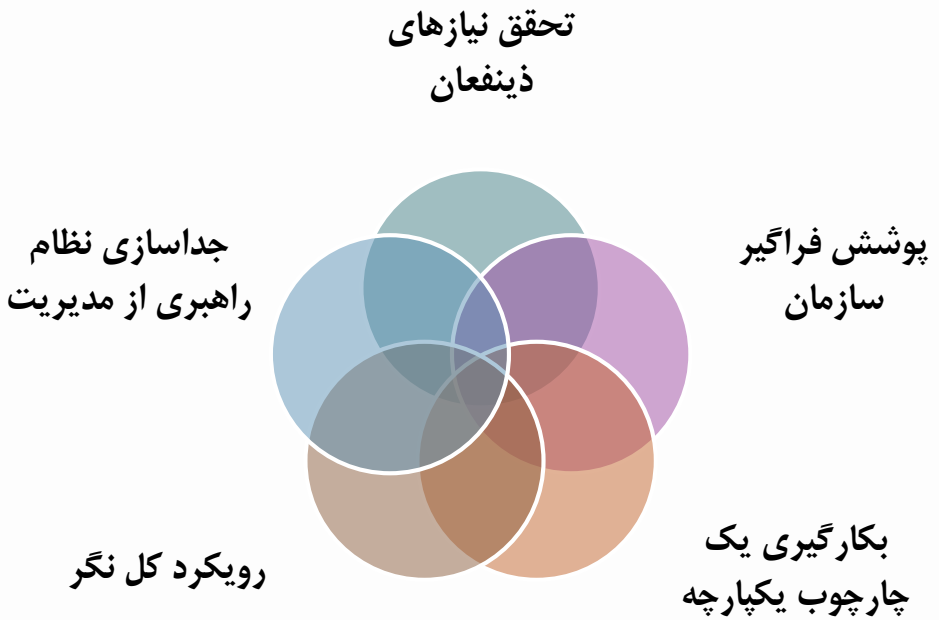
- Control Objectives for Information and Related Technology
- IT Governance Institute
- Information Systems Audit & Control Association

مکعب کوبیت



- کوبیت، تمامی فرآیندهای فناوری اطلاعات و منابع آن را با هـدف امنیـت، اطمینـان و کیفیت مورد ارزیابی قرار می دهد.

اصول COBIT



- کوبیت، شامل رهنمودهای مدیریتی و یک مجموعه ابزار پشتیبانی است که این امکان را به مدیران می دهد که شکاف بین نیازهای کنترلی، موضوعات فنی و ریسک های کسب وکار را پر کنند.

مراجع انجام حسابرسی فناوری اطلاعات

- امروزه شرکت های حسابدار رسمی(CPA) گروه های خاصی را طراحی کرده اند که در زمینه حسابرسی فناوری اطلاعات متخصص هستند. شرکت هایی نظیر PWC، Ernest & Young، KPMG،Deloitte دارای ستادهایی هستند که حسابرسی های فناوری اطلاعات را انجام می دهند. اکثر این گروه ها به حسابرسان مالی در تصدیق صحت صورت های مالی برای شرکت هایی که در آنها حسابرسی انجام می دهند، کمک می کنند.

- Certified Public Accountant

Deloitte.

IT System Audit, Review and Assessment

The goal of IT system audit	Deloitte Approach	Results
Identify risks and weaknesses	Testing logical and physical security controls	Reliable IT controls and risk management capability
Accelerate the business information collection process	Testing IT operations	Security information management enabled
Centralize the control system	Testing disaster recovery procedures	Improved data availability and integrity
Regulatory compliance	Testing business continuity	Improved ability to enter new markets
Reduce IT-related costs	Data integrity assessment	Enhanced reputation
Ensure information confidentiality, integrity and availability	IT strategy preview	Long-term savings
Align IT assessment and IT strategy	IT Process & organization review	Revenue growth

IT audit constitutes an **assessment** of IT system management, its **alignment** to **corporate management, vision, mission and organizational goals**.

IT Risk Management

Deloitte.

Key areas

- Security and Privacy (Information leakage prevention, Security of changes, Biometrics and identity management)
- Data (Data privacy, Data quality, Data access)
- Resilience and Continuity (Recovery after IS failure, Resilience and preparedness, Testing, drills and simulations)
- Fraud (IT forensics, Fraud risk management)
- Payments (Payment risk management, PSD/SEPA preparedness, Sanctions OFAC)
- Projects and Testing (Project risk management, Test management, Implementation of tests)
- Contracts (Contracting risk, Supplier risk management)
- IT Controls (Controlling changes, Technology risk management, Organization-level risk management, IT internal audit)

IT risk management enables measuring, managing and controlling IT-related risks, thus enhancing the reliability of processes and the entire information system.

Deloitte.

Key areas

- IT Due Diligence entails a comprehensive analysis of the organization's IT sector to ascertain its alignment with business goals and the extent to which it supports other parts of the organization.
- It is commonly performed when a potential investor/partner **wishes to gain insight into the level of IT support to business and IT resources**.

نقش مقام ناظر بانک ها در اجرای حسابرسی IT

- محیط کسب و کار بانکداری پویا و متناسب با توسعه فناوری دستخوش تغییر است. تا کنون اغلب اسناد بالادستی در قالب رهنمود به مقوله کنترل و نظارت بر واحدهای فناوری اطلاعات پرداخته اند.
- اسناد الزام آور نیز به طور مشخص به لزوم انجام حسابرسی فناوری اطلاعات تأکید ننموده اند و صرفا از طریق توصیه در زمینه مدیریت ریسک های مرتبط و یا استقرار کنترل های داخلی مربوط به این مسئله پرداخته اند.

پیشنهادات اجرایی برای نظام بانکی کشور

- تأکید مراجع بالادستی با توجه به درجه اهمیت و ریسک مترتب بر این حوزه بر ضرورت انجام حسابرسی فناوری اطلاعات.
- استفاده از تجربه جهانی در استقرار حسابرسی IT در بانکها و موسسات اعتباری.
- تدوین دستورالعملهای بومی شده متناسب با فناوری اطلاعات بانکها و موسسات اعتباری به منظور تسهیل در انجام حسابرسی فناوری اطلاعات .
- تقویت جایگاه حرفه ای و استقلال حرفه ای حسابرسان داخلی در بانک ها.
- نهادسازی به منظور برون سپاری خدمات فناوری اطلاعات