ISACA
Gūstot vērtību no uzticamām informācijas sistēmām
Latvijas nodaļa

ISACA
Trust in, and value from, information systems

IT vadības sistēmas audits

19.03.2013

Ivo Ivanovs

Ernst&Young Baltic IT drošības projektu vadītājs

ISACA Latvijas nodaļas viceprezidents

Iekšējā audita padomes loceklis

ISACA Latvijā un pasaulē

ISACA
Trust in, and value from, information systems

IT Governance Forum

latin america cacs

ISACA e-Symposium
Trust in, and value from, information systems

international conference

Information Security and Risk Management Conference

euro cacs

ISACA Training Week

Information Security Management Forum

CISA Certified Information Systems Auditor
An ISACA Certification

CISM Certified Information Security Manager
An ISACA Certification

CGEIT Certified in the Governance of Enterprise IT
An ISACA Certification

CRISC Certified in Risk and Information Systems Control
An ISACA Certification

ISACA IT Governance, Risk & Compliance Conference

Val IT 2.0
Based on CobiT

CobiT
Governance, Control and Assurance for Information and Related Technology

Risk IT
Based on CobiT

ITAF
A Professional Practices Framework for IT Assurance

IT vadības sistēmas audits

- IT vadības sistēmas auditam jābūt
  - Risku bāzētam
  - Veiktam saskaņā ar IT audita standartiem
  - Plānotam
  - Izpildītam saskaņā ar audita programmu, sasniedzot audita mērķi
  - Sagatavots audita slēdziens
  - Veiktam pēc auditam (follow-up)

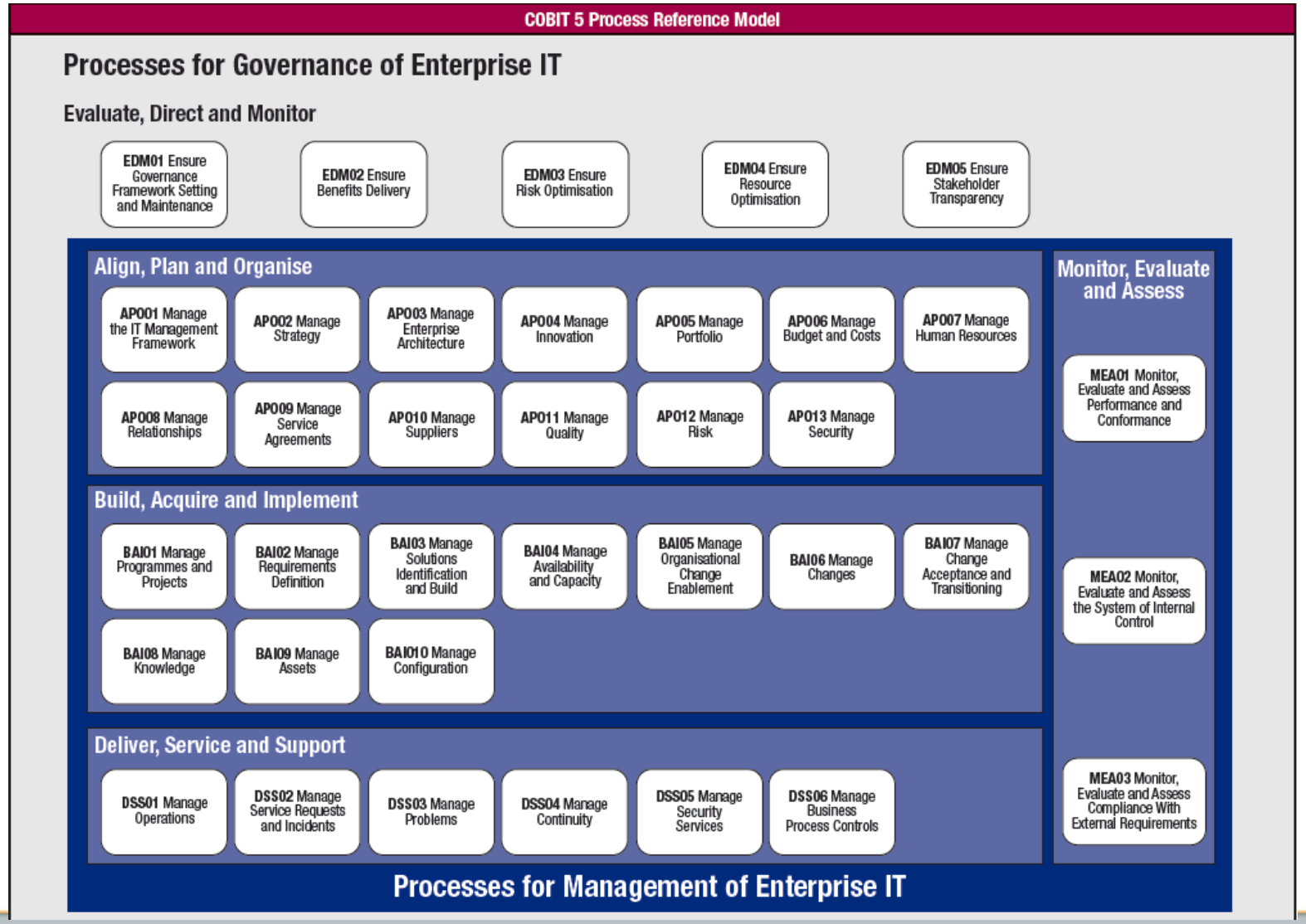
IT audita procedūras

- Izpratnes iegūšana par auditējamo objektu
- Risku plānošana un vispārējā audita plāna sagatavošana
- Detalizēto pārbaužu plānošana
- Sākotnējā audita objekta apskate (dokumentācija)
- Audita objekta novērtējums
- Pastāvošo kontroļu identifikācija
- Atbilstības testēšana (procesa walkthrough)
- Substances testi
- Audita ziņojums (rezultātu prezentēšana)
- Follow-up

IT vadības sistēmas audita jomas

- IT pārvaldības procesu(a) audits
  - Procesu grupas
    - Plānošana un organizācija
    - Sistēmu ieviešana
    - Sistēmu ekspluatācija un darbināšanas atbalsts
    - Pārraudzība un monitorings
  - Kritiskie procesi valsts iestādēm
    - Plānošana un stratēģija
    - IT drošības pārvaldība
    - Atbilstība likumdošanai
    - Izmaiņu pārvaldība un loģiskās pieejas kontrole

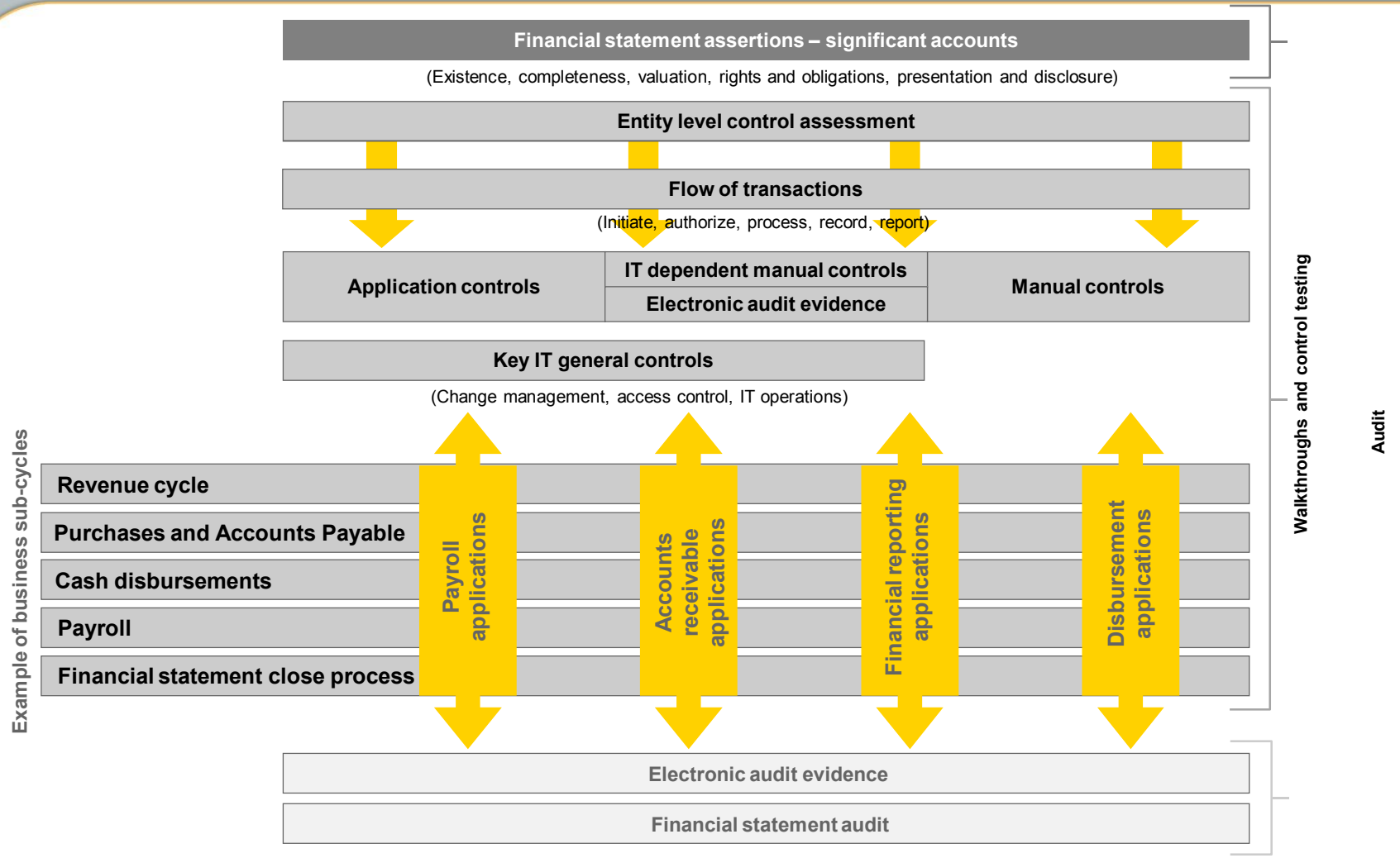
Cobit procesu modelis



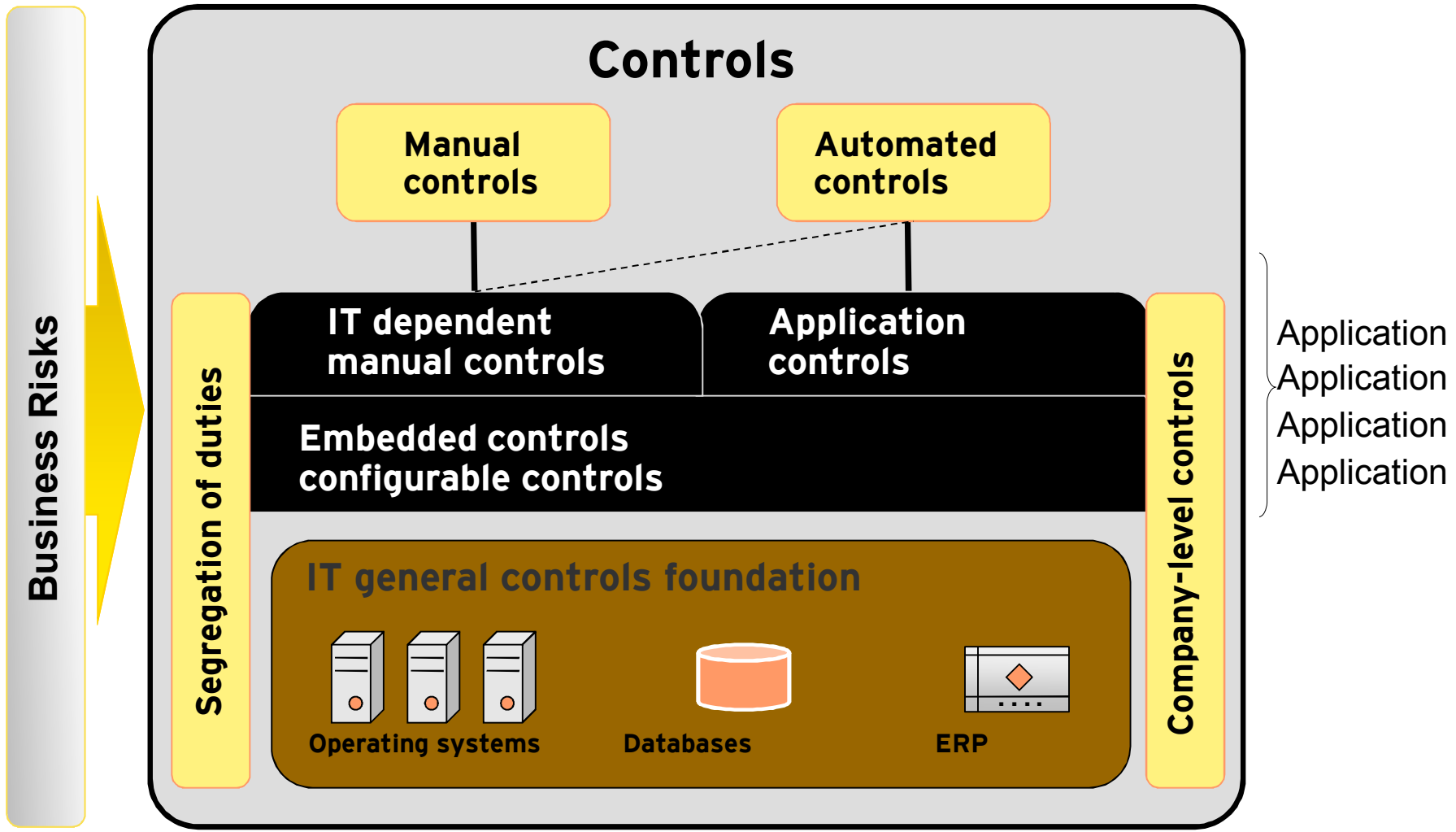
Ārējo auditoru izmantošana

- Ārējam auditoram jādarbojas IA uzdevumā
- Drīkst paļauties uz citu auditoru veikto darbu (S13 Using the Work of Other Experts)
- Audita plānošana un audita programma

IT audita integrācija finanšu revīzijā

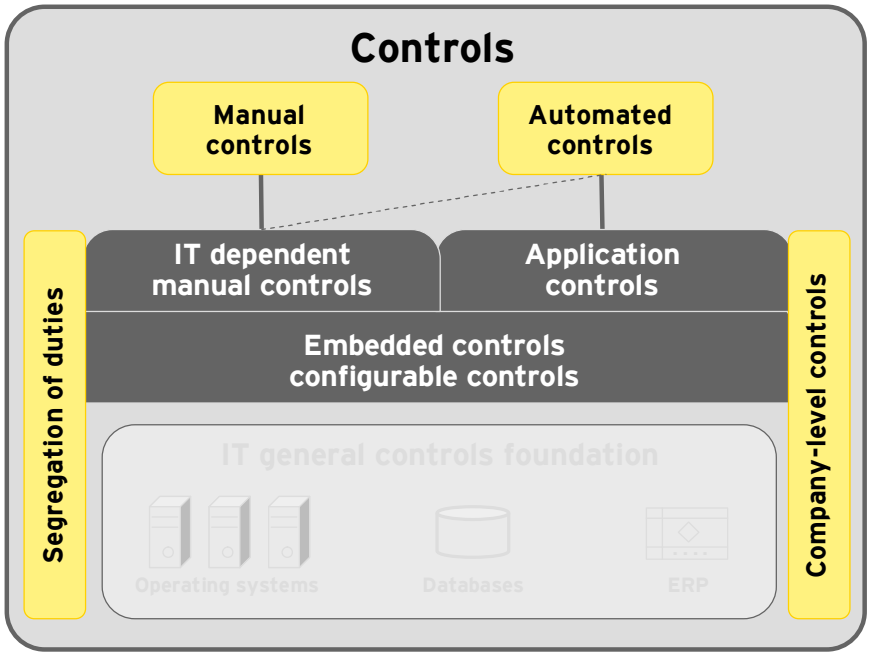


IT kontroles



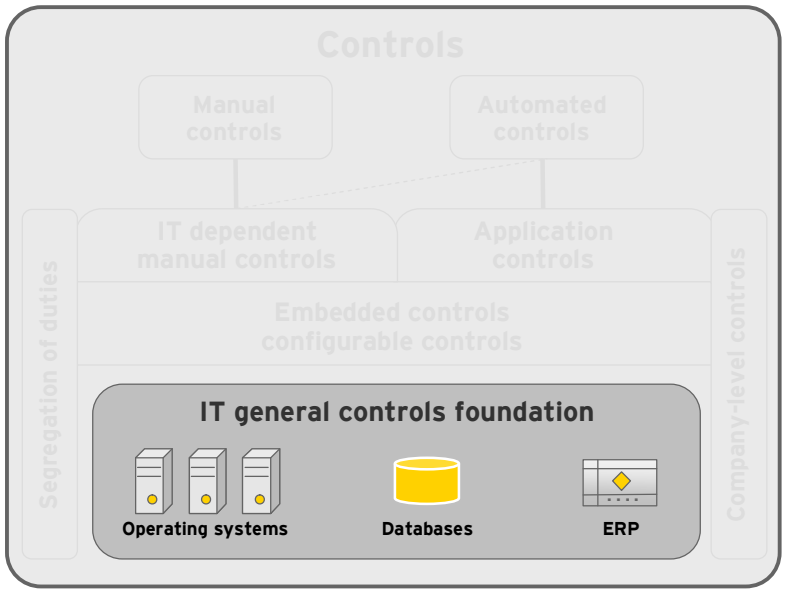
IT kontroļu veidi

- Automatizētās kontroles
  - IT sistēmā iebūvētās kontroles, kas notiek izpildot katru transakciju
  - Sniedz pārliecību, ka transakcijas ir pareizas (saskaņā ar prasībām), tās ir atbilstoši autorizētas un pilnībā izpildītas
  - Parasti ļoti svarīgas, ja jāpārliecinās par pareizu pienākumu sadali
- Veidi
  - Iebūvētas sistēmā (nav maināmas bez programmēšanas)
  - Konfigurējamas (maināmas, izmatojot sistēmā iebūvētus rīkus)
- Izpausmes
  - Datu lauku satura validācijas
  - Aprēķini
  - Interfeiss ar citām sistēmām
  - Autorizācijas pārbaudes
- IT atkarīgās manuālās kontroles
  - Manuālās kontroles, kas paļaujas uz IT sistēmas informāciju



IT vispārējās kontroles

- Kāpēc tās ir svarīgas revīzijas ietvaros?
  - IT vide ir viens no svarīgiem nosacījumiem, lai uzņēmums sasniegtu plānotos mērķus
  - No IT sistēmu pareizas darbības ir atkarīga vadības un finanšu informācijas precizitāte un savlaicīgums
  - IT vispārīgās kontroles nodrošina, ka sistēmās esošās automatizētās kontroles darbojas netraucēti visa pārskata periodā.
    - IT vispārējo kontroļu efektivitātes vērtējums ir priekšnosacījums, lai datus no sistēmām varētu izmantot revīzijas ietvaros bez papildus pārbaudēm



IT vispārējās kontroles

- Sistēmu izstrādes un izmaiņu pārvaldības kontroles
  - Mērķis: sistēmā tiek ieviestas izmaiņas kas ir
    - Atbilstoši autorizētas
    - Testētas un apstiprinātas
- Pieejas kontroles
  - Mērķis: sistēmā esošie dati ir pieejami tikai atbilstoši autorizētām personām konkrēto pienākumu izpildei (atbilstošā apjomā)
    - Attiecībā gan uz programmām, tabulām un eksportētajiem datiem
    - Pieejas veidi (iegūt informāciju, izmainīt informāciju, izpildīt operāciju)
- IT sistēmu darbības kontroles
  - Mērķi:
    - Elektroniskie finanšu dati ir aizsargāti pret iespējamu zaudēšanu vai sabojāšanu,
    - Regulārie un automātiskie sistēmas procesi tiek uzraudzīti
    - IT problēmas un incidenti tiek analizēti un savlaicīgi novērsti

Jautājumi

- Ivo Ivanovs
- E-pasts: ivo.ivanovs@isaca.lv
- Tālr: +37129294044