TALLINNA ÜLIKOOL
Informaatika Instituut

Marily Visnapuu

IT auditi metoodikatest tulenevad soovitused IT juhtidele

Magistritöö

juhendaja: Andro Kull

Autor: ……..... „ … “ …….. 2008.a.
Juhendaja: …… „ … “ …….. 2008.a.
Instituudi juhataja: ……..... „ … “ …….. 2008.a.

Tallinn 2008

Autorideklaratsioon

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud. Käesolevat tööd ei ole varem esitatud kaitsmisele kusagil mujal.

Kuupäev:

Autor: Allkiri:

Annotatsioon

Käesoleva töö eesmärk on IT auditite metoodikate analüüsist tulenevalt sõnastada IT juhtidele suunatud parimatest praktikatest koosnev juhend. Juhend sisaldab IT audiitorite poolt kasutatavate IT auditi metoodikate lähtepunkte ja soovitusi, millele IT juhid peaksid oma töökohal suuremat tähelepanu osutama. Töö põhirõhk on suunatud erinevate metoodikate analüüsile ning tulenevatest soovitustest ja tähelepanekutest juhendi koostamiseks IT juhtidele.

Lõputöö on kirjutatud eesti keeles, koosneb 74 leheküljest, sisaldades 4 peatükki ja 5 joonist.

Annotation

The aim of this study is to formulate an instruction to IT managers based on IT audit methodologies and best practises. An instruction consists of the basis and recommendations from IT audit methodologies used by IT auditors to which IT managers should pay more intention. The main objective is to analyse different IT audit methodologies and based on those recommendations and observations create an instruction to IT managers.

The thesis is written in Estonian, contains 74 pages of text, 4 chapters and 5 figures.

Jooniste nimekiri

Sisukord

Sissejuhatus

Parimad praktikad on kasutusel erinevatel erialadel, erinevates töölõikudes. Samuti ka auditeerimisel ning IT auditite vallas. Suuremad ettevõtted peavad ja ka lasevad perioodiliselt audiitoritel enda töid ja tegemisi hinnata. Kuid nii mõnedki ettevõtted ei tee seda, olgu põhjuseks mis iganes. Seega paljud IT juhid ei teagi, mis IT audiitorit huvitaks, millele audiitor pööraks suuremat tähelepanu ehk mida täpselt auditeeritaks ning kuidas see välja näeks.

Üritades kokku ühendada neid kahte põhjust, on antud magistritöö eesmärgiks tuua IT audit lähemale IT juhtidele – koostades nimekirja nendest toimingutest, millele nad võiksid igapäevaselt oma töös tähelepanu pöörata. Nagu arvata võibki on suur osa auditeerimisest seotud turvariskide hindamise ja analüüsiga, kuid kindlasti ei tasu ära unustada ka seda, et audiitorid hindavad veel paljut muudki – strateegia elluviimist, visiooni, eesmärke jms. Kõike, mille läbi ettevõtte viib ellu oma nägemust millegi poolest parimast firmast.

Töö lisaeesmärgiks on aidata IT juhtidel näha „pilti suuremalt“. Suunata neid mõtlema erinevatele valdkondadele – turvalisus, IT meetodid, hetkel maailmas parimateks tunnistatud praktikad, meeskond ja nende intelligentsipagas ning palju muudki.

Töö eesmärgid

Käesoleva magistritöö eesmärgid:

1) erinevate IT auditi metoodikate võrdlus
2) analüüsist tulenevatest tulemustest järelduste tegemine
3) IT juhtidele suunatud IT auditite metoodikatest tulenevad soovitused

Töö aktuaalsus

Töö on aktuaalne, kuna ülemaailmselt on välja kujunenud erinevad standardid ja parimad praktikad erinevatele IT rakendustele. Iga IT juht võiks teada nende olemasolust, ning mis veelgi tähtsam, ta peaks olema valmis enda praktikaid ka teistega jagama ning olema valmis, et tema tööd hinnatakse – auditeeritakse. Ning ka nende ettevõtete IT juhid, kelle ettevõte peab mingi standardi saamiseks laskma ennast auditeerida, ka neile võiks huvi pakkuda, mis neid ees võib oodata.
Eestikeelset materjali antud teema kohta on praktiliselt võimatu leida sest seda vähemasti avalikult ei leia.
Magistritöö tulemused on suunatud ennekõike IT juhtidele, kuid üht-teist huvitavat võivad sellest leida kõik IT huvilised või auditeerimisest huvitatud osapooled.

Töö koostamiseks kasutatud meetodid

1) teoreetiline uurimus elektrooniliste teabeallikate põhjal – kuna analüüsimiseks on kasutatud ülemaailmselt tunnustatud standardeid ja metoodikaid, siis enamus neist on leitavad ametlikel veebilehtedel
2) teoreetiline uurimus IT auditeerimist käsitlevate raamatute alusel

Töö ülesehitus

Magistritöö jaguneb 4 peatükiks.

Esimeses peatükis antakse ülevaade IT auditist ja auditeerimisest.

Teises peatükis antakse ülevaade laiemalt levinud IT auditi metoodikatest.

Kolmas peatükk annab ülevaate metoodikate tööpõhimõtetest ning soovitustest ning lisaks autori poolsed järeldused kajastatud metoodikatest ja nende vastavusest IT juhtide töö eesmärkidele.

Neljas peatükk on suunatud neist parimate soovituste leidmisele ja analüüsimisele, ning selle kõige põhjal ülevaatliku nimekirja koostamine IT juhtidele teemadest, millele nad võiks oma töös suuremat tähelepanu pöörata.

IT juht

IT juhi kutsestandardi järgi on Infotehnoloogia juhi töö eesmärgiks ettevõtte infotehnoloogilise ja sidekontseptsiooni loomine ning konkurentsivõimet tagavate ja toetavate IT- ja sidealaste lahenduste väljatöötamise ning juurutamise juhtimine pidevalt muutuvas ja kõrge konkurentsiga keskkonnas.

Vastutus ja tegevused

IT juht vastutab ettevõtte IT strateegia ja äristrateegia kooskõlla viimise, infosüsteemi talitluspidevuse, informatsiooni õigsuse ja turbe ning järgnevate tööülesannete tulemusliku täitmise eest:

Ettevõtte äristrateegia väljatöötamisega seonduvad ülesanded:

1. ettevõtte arengukavade väljatöötamisel osalemine
2. IT vahendite parema rakendamise abil ettevõtte efektiivsuse suurendamise võimaluste selgitamine koostöös teiste juhtidega ja ettevõtte klientide ning partneritega. Juhtkonnale asjakohaste ettepanekute tegemine

IT strateegilise juhtimisega seonduvad ülesanded:

1. IT turul toimuvate muutuste ja trendide kohta info hankimine ja analüüsimine
2. IT strateegia väljatöötamine ja sõnastamine lähtuvalt IT võimalustest ja ettevõtte äristrateegiast tulenevatest vajadustest ning võimalustest
3. IT eelarve koostamine ja täitmise jälgimine

IT arendustegevusega seonduvad ülesanded:

1. IT-arendustegevuse planeerimine
2. IT valdkonna projektijuhtimise korraldamine
3. projektülesande püstitamise juhtimine koostöös vastava valdkonna ärijuhiga
4. projekteerimise ja rakenduse valiku juhtimine
5. uute IT-rakenduste koolituse organiseerimine
6. IT infrastruktuuri planeerimine

IT kasutamise ja ülalpidamisega seonduvad ülesanded:

1. arvuti- ja kommunikatsioonivõrgu administreerimise ja andmeturbe korraldamine
2. kasutajatoe olemasolu ja toimimise tagamine
3. riist- ja tarkvara ning IT-tarvikute ostusüsteemi korraldamine
4. IT ressursside haldus
5. tarkvara litsenseerituse tagamine

Meeskonna juhtimisega seonduvad ülesanded:

1. IT-organisatsiooni juhtimine
2. IT-organisatsiooni mehitamise juhtimine
3. IT osakonna töötajate motiveerituse tagamine
4. tööülesannete ja eesmärkide kokkuleppimine
5. töötulemuste ja töötajate hindamine
6. koostöö korraldamine teiste allüksustega. (Kutsekoda 2006)

IT audit

Audit – see on hinnang inimesele, organisatsioonile, süsteemile, protsessile, projektile või tootele. Auditeid sooritatakse veendumaks informatsiooni tõesuses ja usaldatavuses ning ühtlasi hinnangu andmises sisemistele kontrollidele. Auditi eesmärgiks on väljendada arvamust inimese/organisatsiooni/süsteemi jne kohta vastavalt sooritatud testide tulemustele. Audit otsib *mõistlikku kinnitust*, et süsteeme ei ohusta materiaalne kahju.

Traditsiooniliselt olid auditid seotud informatsiooni kogumiseks ettevõtte või äri finantssüsteemidest ja finantsandmetest.

Infotehnoloogia audit ehk IT audit on infotehnoloogia infrastruktuuri kontrollimine. IT audit on protsess, mille käigus kogutakse ning hinnatakse ettevõtte infosüsteemide, praktikate ja operatsioonide (tegevuste) tõestusmaterjali. Hinnangu käigus selgitatakse välja kas infosüsteemid kaitsevad ettevõtte varasid, hoiavad andmete täielikkust, opereerivad efektiivselt ja kasumlikult saavutamaks ettevõtte eesmärke ja sihte. Taolised ülevaatused võib läbi viia ka koos siseauditi või finantsauditiga.

Kõige enam on IT auditiga seotud informatsiooni turvalisuse hindamine sest see hõlmab ka üldisi riskide ja kontrollidega seotud tegevusi, mis on omakorda seotud arvutite ja telekommunikatsiooniga.

IT auditeid teati varem ka kui automatiseeritud andmete töötlemise auditeid (ADP[1] audit) või arvuti auditit, ning kutsuti neid elektroonseks andmete töötlemiseks. (Wikipedia (n.d))

IT auditite tüübid

Goodman ja Lawless (Goodman 1994) märgivad, et on olemas kolm süsteemilist lähenemist IT auditi läbiviimiseks:

- tehnoloogia-innovatsiooni protsessi audit

Eesmärk on olemasolevate ja uute projektide riski hindamine. Audit hindab ettevõtte kogemuse pikkust ja sügavust valitud tehnoloogiate osas, samuti nende olemasolu vastavatel turgudel

- innovatsiooni võrdlusaudit

Nagu ka nimi vihjab, on tegemist ettevõtte innovaatilisuse võrdlemisega teiste sarnaste ettevõtete omadega

- tehnoloogilise positsiooni audit

[1] ADP – Automated Data Processing

See audit vaatleb ettevõttes kasutusel olevaid tehnoloogiaid ning toob välja sealsed puudused e. soovitused, mida oleks mõistlik muuta/uuendada/lisada.

Mõned teised jaotavad auditeid jällegi viieks tüübiks:

- süsteemid ja rakendused. Auditi eesmärgiks on välja selgitada, kas süsteemid ja rakendused on sobivad, efektiivsed, ning kas on võimalik kontrollida sisendite tõesust, usaldatavust, ajakohasust ja turvalisust, töötlemist ning väljundeid kõigilt tasemetelt.
- informatsiooni töötlemise vahendid. Auditi eesmärgiks on kinnitada, et rakendused töötaksid normaalolukorras ning ka võimaliku segamise puhul vastavalt ajale, sobivusele ja efektiivsusele.
- süsteemide arendamine. Auditeeritakse, kinnitamaks, et arendamises olevad süsteemid vastavad ettevõtte eesmärkidele ning et süsteeme arendatakse vastavalt üldiselt tunnustatud standarditele.
- IT haldamine ja ettevõtte arhitektuur. Auditi eesmärgiks on kinnitada, et IT haldamine on arendanud organisatsiooni struktuuri ja protseduure nii, et need toetaksid kontrollitud ja efektiivset informatsiooni töötlemise keskkonda.
- Klient/Server, sisevõrk (ingl. k. Intranet), välisvõrk (ingl. k. Extranet). Auditeeritakse kinnitamaks, et andmete liiklemine võrgus on turvaline ning kontrollitav.

Samas on ka neid, kes väidavad, et auditeid on kahte sorti: üldine ülevaade juhtimisest või rakenduste juhtimise ülevaade. (Wikipedia (n.d))

IT audiitori tüüpilised tööülesanded

- **arvutisüsteemi/-võrgu töö audit:** ülevaade informatsiooni turvalisusest ja teistest kontrollidest seoses ümbritsevate arvutisüsteemide ja võrkudega;
- **IT installatsiooni audit:** ülevaade arvutite ehitusest, komplektidest, toast, või kapist, kaasa arvatud nende füüsiline turvalisus, keskkonnast olenevad ohud, arvuti ja võrgu protsessid ning juhtsüsteemid ja muidugi ka IT varustus üldiselt;
- **arendatavate süsteemide audit:** tüüpiliselt kajastatakse seal 2 aspekti: projekti/programmi juhtimise kontrollid; ja sobilike arendatud süsteemide turvalisuskontrollide rakendamine;

- **IT haldamise, juhtimise ja strateegia audit:** ülevaade organisatsioonist, struktuurist, strateegiast, tööplaneerimisest, vahendite planeerimisest, eelarvest, kulude kontrollist jne ning seal kus kohaldatav ka väljast sisse ostetud IT teenusepakkujatest. samuti ülevaade ka IT strateegiatest, visioonidest, plaanidest;
- **IT protsesside audit:** ülevaade IT-ga seotud protsessidest nagu nt rakenduste arendus, testimine, rakendamine, opereerimine, haldamine, majapidamine (varundamine, ennetav hooldus jne.), tugi, intsidentide haldamine;
- **muudatuste haldamise audit:** ülevaade muudatuste planeerimisest ja kontrollist süsteemides, võrkudes, rakendustes, protsessides, jne kaasa arvatud konfiguratsioonide haldamine ja kontrollid alustades koodist ja arendamisest kuni testimise ja tootmiseni;
- **Informatsiooni turvalisuse ja kontrollide audit:** ülevaade tehnilistest, protseduurilistest ja teistest kontrollidest, mis kaitsevad süsteemide ja andmete konfidentsiaalsust, terviklikkust ja kättesaadavust;
- **IT kooskõlastatuse audit:** ülevaade väliste nõuete järgimisest (nt IT-ga seotud seadused ja regulatsioonid nagu nt SOX[2], PCI[3], tarkvara autoriõigused ja personaalsed andmed) ja sisemiste/korporatsiooni nõudmistest (IT/informatsiooni turvalisuse poliitika, standardid, protseduurid ja juhised);
- **Võrdlev analüüs:** organisatsiooni võrdlemine teiste sarnaste organisatsioonide IT toimimise, efektiivsuse ja/või võimalustega, või suure organisatsiooni puhul erinevate osakondade võrdlemine või võrdlus üldiselt aktsepteeritud standardite suhtes;
- **sõltuvuste planeerimine:** ülevaade äri järjepidevusest ja IT katastroofidest taastumise plaanid ja sellega seotud protsessidest (nt testimine ja harjutused);
- **spetsiifilised uuringud:** sõltuvust ja mitte ette planeeritud töö nagu nt kahtlaste pettuste uurimine või informatsiooni turvalisuse lõhed, viies läbi IT varade nõuetekohast ülevaadet seoses liitumiste ja omandamistega;
- **muu:** IT audiitorid töötavad tihtipeale koos finants-, tegevus- jm mitte-IT audiitoritega täiendades meeskonda teadmistega IT valdkonnast. (Hinson 2007)

Infotehnoloogia turvalisuse auditeerimine on iga IT auditi osa. Infoturbe auditeerimine hõlmab andmekeskusi, võrke ja rakenduste turvalisust.

[2] SOX – Sarbanes-Oxley Act
[3] PCI - Peripheral Component Interconnect

IT auditi sammud

IT auditid jälgivad samu protsesse nagu kõik auditid, täpsemalt:

1. **Audit kava või plaan** – juhtkond otsustab, mida ja millal auditeerida. Tulemuseks on tüüpiliselt kirjeldatud auditi skoop, ajakava ja ressursside jaotus igale auditile.
2. **Skoobi ja eel-auditi uuring** – audiitorid määravad kindlaks põhilise(d) valdkonna(d) ja ka need, mis jäävad skoobist välja, enamasti tehakse need valikud mingil riskipõhisel hindamisel. Informatsiooni allikad antud osas hõlmavad taustalugemist ja veebis surfamist, eelmisi auditi raporteid ja mõnikord ka subjektiivseid muljeid, mis on väärt edasist uurimist.
3. **Planeerimine ja valmistumine** – selle käigus jaotatakse skoop suurematekseks alamdetailideks – enamasti auditi tööplaaniks, kontrollnimekirjadeks ja riskikontrollmaatriksiks.
4. **Töö objektiga** – tõestusmaterjali kogumine töötajate ja juhtide intervjueerimise käigus, dokumentide, väljatrükkide ja andmete ülevaatamine, jne. Selles osas võidakse kasutada ka vastavaid tarkvarasid e. CAATs[4].
5. **Analüüs** varem kogutud materjalile. PEST[5] ja SWOT[6] tabelid võivad olla üheks võimalikuks analüüsimise tehnikaks.
6. **Raporteerimine** on auditi protsessi peamine fookus ja sellele pööratakse suurt tähelepanu nii audiitorite kui auditeeritavate poolt.
7. **Sulgemine** – lisaks auditi failide täiustamisele ja sulgemisele tehakse ka märkusi edaspidisteks audititeks uuendades riskimudeleid ja mõnedes ettevõtetes ka kinnitatakse kooskõlas juhatusega, et kõik kokkulepitud tegevused on läbi viidud ja lõpetatud. (Hinson 2007)

Ettevõtte eesmärkide saavutamiseks on oluline aru saada ärinõuetest. Järelikult peaksid IT teenused rahuldama ettevõtte nõudmisi, IT-ga seotud riskid peaks olema teada ja parimad praktikad peaksid olema kasutusele võetud. Laialdaselt on teada, et efektiivne riskihaldus on üldise haldamise võtmeelement.

[4] CAATs - Computer Aided Audit Techniques
[5] PEST - Political, Economic, Social, and Technological factors
[6] SWOT – Strenghts, Weakenesses, Opportunities, Threats analysis

Audiitorid peavad meeles pidama, et on loodud väga palju erinevaid IT metoodikaid, mis on kasutusel üle maailma. Audiitorid peavad määratlema, millised kohalikud IT meetodid, kui üldse, on klientidel kasutusel. Audiitorid peavad esialgu hindama kas kasutusel olevad meetodid on mõistlikud ning kas nad on korrektselt rakendatud.

Auditi metoodikate erinevad kasutusalad:

- IT auditid
- riskianalüüsid
- turvalisuse mõiste
- turvalisuseteemalised juhendid

Siseaudiitorid peaksid hindama IT plaane, strateegiaid, poliitikaid ja protseduure kinnitamaks adekvaatset juhtkonna tegemisi. Lisaks sellele peaksid nad hindama igapäevaseid IT kontrolle kindlustamaks, et tehingud on salvestatud ja protsessid on vastavuses raamatupidamismeetodite ja standarditega ning poliitikatega, mis on sätestatud juhtkonna poolt. (IIA 2008a)

Audiitorid viivad läbi ka tegevusauditeid, kaasa arvatud süsteemi arendamise auditeid, kindlustamaks, et kontrollid on paigas, et reeglid ja protseduurid on efektiivsed ning et töötajad käituvad vastavalt nendele. Audiitorid peavad hindama nõrkusi, üle vaatama juhtkonna plaane, et leida üles sealsed nõrkused, jälgima nende lahenduvust ning raporteerima juhatusele kui leidub materiaalseid nõrkusi.

Peamised riskifaktorid üldkasutatavates hindamissüsteemides:

- sisemiste kontrollide adekvaatsus
- tehingute iseloom
- süsteemi või rakenduste vanus
- operatsioonikeskkonna olemus
- informatsiooni, varustuse ja territooriumi füüsiline ja loogiline turvalisus
- juhtimise ülevaatus ja adekvaatne jälgimine
- juhtkonna suhtumine ellnevate regulatsioonide ja auditi tulemustesse
- inimressurss, kaasa arvatud juhatus ja meeskond, käive, tehniline kompetentsus, juhtkonna plaan ja delegeerimise tase

- vanemjuhatuse ülevaade (FFIEC (n.d))

Audiitorid peavad perioodiliselt vaatama üle sisemiste kontrollprotsesside tulemusi ning analüüsima finats- või tegevuslikke andmeid igasuguse riskiga seotud tegevuste suhtes. Juhtkond peab audiitorit teavitama kõigist suurematest muudatustest seoses muutustega meeskondades või erinevate funktsioonidega nagu nt uus toode, uue süsteemi implementeerimine, rakenduste konversioon või muutused organisatsioonis või töötajate seas.

- turvalisus – süsteem on turvatud valede isikute jaoks
- kättesaadavus – süsteem on tegevustele avatud ja kasutuses nagu kokku on lepitud
- käideldavuse integreeritus – süsteemi käideldavus on täielik, tõene, ajakohane ja kättesaadav volitatud isikutele
- konfidentsiaalsus – konfidentsiaalseks tunnistatud informatsioon on kaitstud vastavalt kokkulepitule

1. IT auditite metoodikad

Olles otsinud ja uurinud ülemaailmselt kasutusel olevaid metoodikaid, selgus et üldkasutatavaid ja üldiselt tunnustatud metoodikaid on vähe. Kindlasti on selles vallas vaieldamatuks liidriks ISACA[7] poolt koostatud CobiT metoodika, millele ka enamus teisi meetodeid kas otseselt või kaudselt viitavad. Kuna tegemist on niivõrd tunnustatud standardiga, ei ole teised organisatsioonid hakatud ratast uuesti leiutama ning tavaliselt viidatakse, et selle või teise punkti puhul soovitatakse tutvuda CobiT-ga.

Ja kui CobiT'i skoop on väga lai, siis teised meetodid pigem keskenduvad mingile konkreetsele valdkonnale – enim on muidugi erinevaid metoodikaid välja pakutud turvalisusega seotud teemadel, sellest sai valikusse ka BS7799 (või ISO/IEC [8]17799), kuna see oli taaskord üks nendest enim mainitutest, millele nii mõnegi teise standardi juures viidati sarnaselt CobiT'le.

Kolmandaks väljavalituks osutus GAIT, kuna see on loodud IIA (Insitute of Internal Auditors) poolt ning mõeldud IT auditites kasutamiseks ning selle loomisel on teadmisi ja kogemusi jaganud paljud suured ja tuntud ettevõtted.

[7] ISACA – Informations Systems and Control Association
[8] ISO/IEC – International Organisation of Standardisation/International Electrotechnical Commision

CobiT

CobiT[9] on IT valitsemise raamistik ja abivahend juhtidele, et ühendada puudujäägid juhtimisenõuete, tehniliste teemade ja äririski vahel.
CobiT põhineb enam kui 40 standardil ja parimal praktikal, mis on dokumenteeritud erinevate standardimisasutuste poolt üle maailma – Euroopast, Kanadast, Austraaliast, Jaapanist ja USA-st. Kuna CobiT koosneb asjakohastest ülemaailmsetest standarditest on see „kõik ühes“ tunnustus IT juhtstandarditele. Selle tulemusena saab CobiT'it kasutada usaldusväärse viitematerjalina kontrollkriteeriumitena (*ingl. k. controls criteria*) IT auditites.

CobiT-i esimene väljalase ilmus 1996. aastal. Eesmärgiks oli uurida, arendada, publitseerida ja tunnustada laialdaselt ühte autoriteetselt võetavat, ajakohast, rahvusvaheliselt üldiselt aktsepteeritavaid IT juhtimiseesmärke (*ingl. k. control objectives*) igapäevaseks kasutamiseks ärijuhtidele ja audiitoritele.

- CobiT 1 1996
    - 32 protsessi
    - 271 juhtimiseesmärki
- CobiT 2 1998
- CobiT 3 2000
- CobiT 4 2005
- CobiT 4.1 mai 2007
    - 34 protsessi
    - 210 juhtimiseesmärki jagatud 4 domeeniks

CobiT struktuuri 4 domeeni:

- Esimene domeen, *Planeerimine ja organiseerimine (ingl. k. Plan and Organize)*, viitab teemadele nagu IT strateegia ja taktika panustades ettevõtetele, tehes kindlaks, et nende ärieesmärgid on täidetud. Neid eesmärke on vaja planeerida, edastada ja juhtida ning ettevõtetes peab eksisteerima tehnoloogiline infrastruktuur ja kohane organisatsioon.

    - 11 protsessi

[9] CobiT – Control Objectives for Information and related Technology

Teine domeen, *Omandamine ja rakendamine (ingl. k. Acquire and Implement)*, viitab strateegia elluviimisele. Rakendused on identifitseeritud, arendatud või omandatud ja rakendatud. Lahendused peavad olema integreeritud äriprotsessidesse. Et veenduda elutsükli järjepidevuses süsteemide vahel on selles domeenis on ka muudatuste haldus ja süsteemide hooldus.

- 6 protsessi

Kolmas domeen on *Üleandmine ja toetus (ingl. k. Delivery and Support)*. Selles domeenis toimub tegelik süsteemide üleandmine turvalistest tegevustest, k.a. koolitamine. Need tegevused toetavad tegevusi, mis panevad organisatsioonis „vere tööle“. Antud domeen hõlmab ka tegelikku andmete töötlust rakendussüsteemide poolt üleandmine ja toetus

- 13 protsessi

Neljas domeen on *Seire (ingl. k. Monitoring).* See domeen tegeleb kõigi IT protsesside regulaarse hindamisega. Siin pööratakse tähelepanu selle, kui hästi organisatsiooni eesmärgid saavad tänu IT vahenditele ja protsessidele täidetud. Seega suunab see juhtkonna tähelepanu ettevõtte juhtprotsessidele ja sõltumatule kinnitusele sisemiste ja väliste audiitorite poolt.

- 4 protsessi

Kasulikkus CobiT'i rakendamisest IT valitsemise raamistikuna:

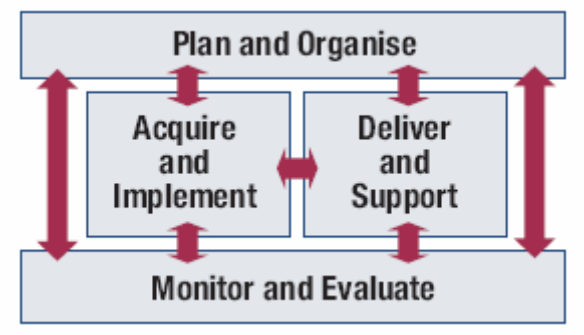
- parem joondamine äri ja IT vahel, vastavalt äri eesmärkidele
- selge ülevaade juhtkonnale, mida IT teeb
- selge omandus ja vastutused vastavalt protsesside omapärale
- üldine aktsepteeritavus kolmandate osapoolte ja regulaatorite poolt
- kõikide omanike jagatud teadmine vastavalt ühisele keelele
- COSO[10] nõuete täitmine IT juhtimise keskkonnas

CobiT'i kontrolleesmärgid (*ingl. k. control objective*) on miinimumnõuded igale efektiivsele kontrollile IT protsessis.

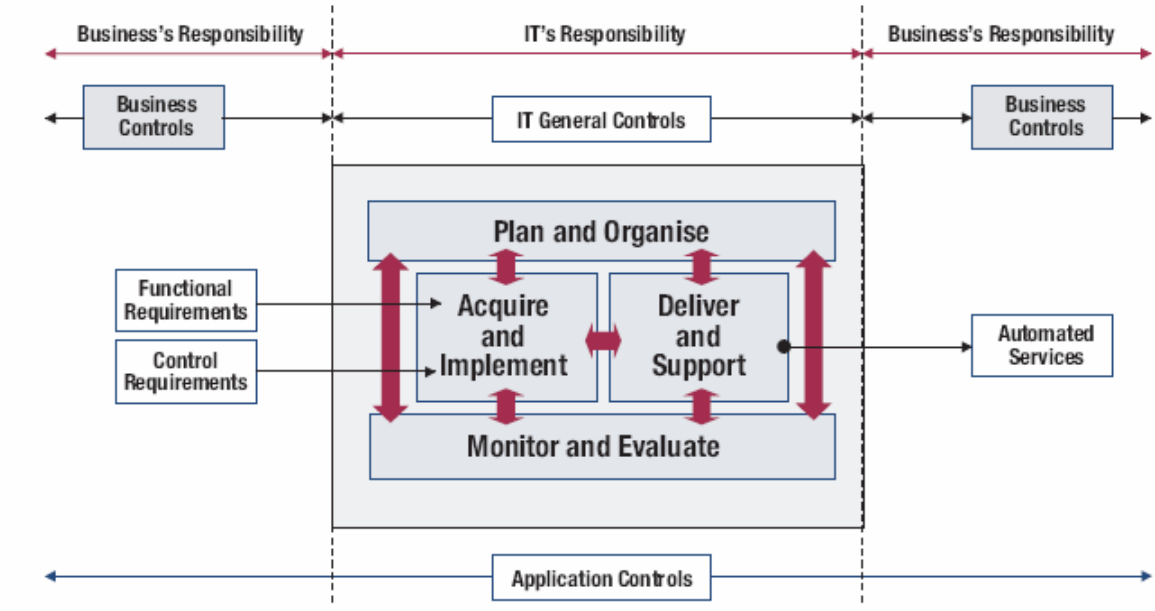
[10] COSO – Commitee of Sponsoring Organisations

Väljend kontroll/juhtimine (*ingl. k. control*) on defineeritud kui poliitikad, protseduurid, praktikad ja organisatoorsed struktuurid, mis on disainitud eesmärgil, et ettevõtte eesmärgid saavad saavutatud ja soovimatud tegevused hoitakse ära või avastatakse ja parandatakse.

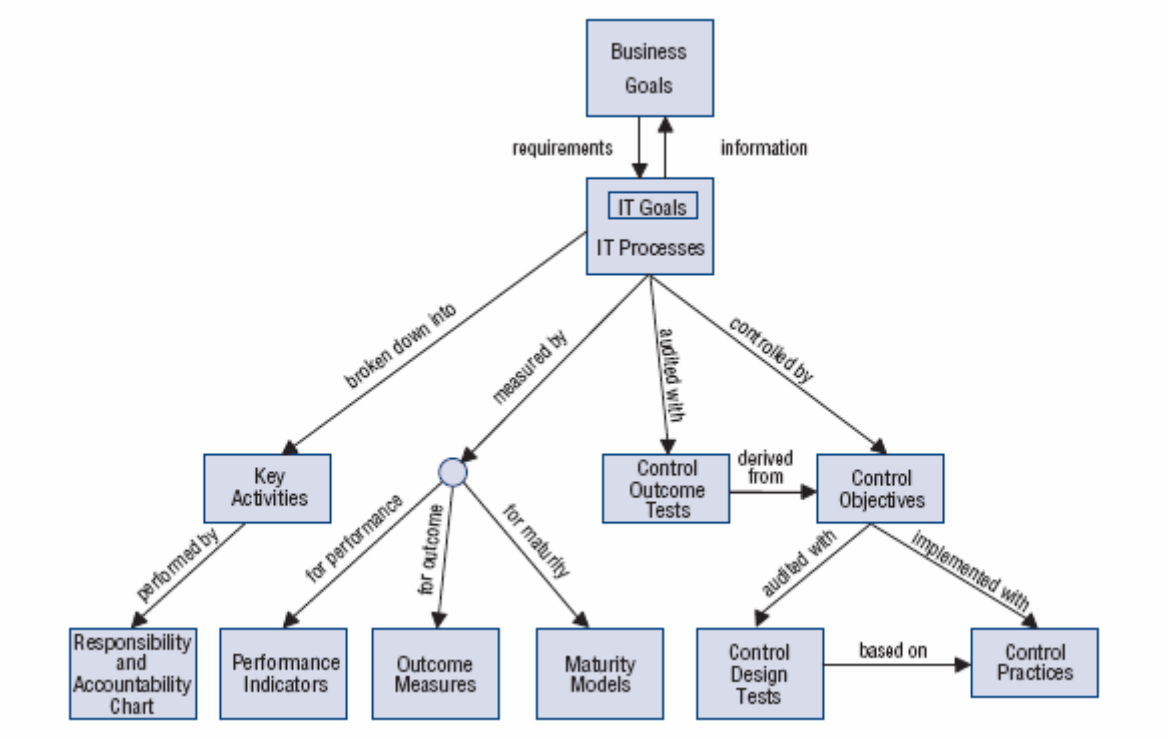
Joonis 1 CobiT'i 4 domeeni



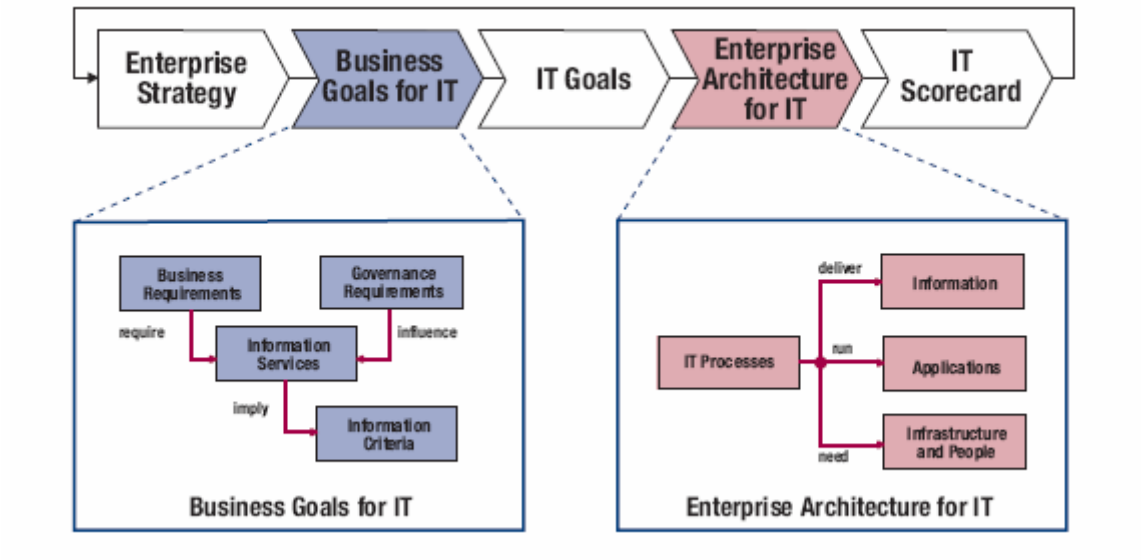
Joonis 2 Seosed äri-, üldiste- ja rakenduskontrollide vahel



Joonis 3 CobiT'i komponentide suhted üksteisesse



Joonis 4 IT eesmärkide defineerimine ja IT-le ettevõtte arhitektuur



Auditeerimise eesmärkideks, mis on defineerinud CobiT'is, on pakkuda ettevõtte juhatusele kinnitust, et juhteesmärgid on täidetud; kus on olulised puudujäägid (mis võivad põhjustada

põhjendamatuid riske) eesmärkide täitmiseks ning mida soovitada ettevõttele parendamistegevusteks. (ITGI 2005)

Auditi juhised kasutavad kose lähenemist – väites, et protsess on auditeeritud saavutamaks arusaamist äri nõudmistest, seotud riskidest ja vastavatest kontrollivahenditest; hinnates kontrollide sobilikkust; hinnates vastutulelikkust testides kas vastavad kontrollid töötavad järjepidevalt ja terviklikult nii nagu kirjeldatud ja lõpuks põhjendades kontrolleesmärkide riski mitte saavutada kasutades analüütilisi tehnikaid ja/või konsulteerides alternatiivsete allikatega. Auditi juhised on üles ehitatud neile neljale eeldusele.

Auditi sammud, mis läbi viiakse, hõlmavad alusteks olevate kontrolleesmärkide dokumenteerimist, veendudes, et vastavad kontrollmeetmed või protseduurid on ellu viidud, intervjueerides juhtkonda ja töötajaid aru saamaks protsessidest, dokumenteerides protsessiga seotud IT vahendid on protsessisõltuvad; ja kinnitama arusaamist protsessist ja selle kontrolli järelmist. Need auditi sammud lubavad audiitoril saavutada arusaam protsessist, mis iganes see ka ei ole, üldises mõttes.

Auditi juhised suunavad audiitori kaaluma kas infoteenused toimivad või ettevõtte poliitikad ja protseduurid viitavad struktureeritud planeerimise lähenemisele; plaanide formuleerimiseks ja modifitseerimiseks on metoodika paigas; lühi- ja pikaajalised IT plaanid eksisteerivad, on ajakohased ja adekvaatselt viitavad ettevõttele üldiselt, tema missioonile ja võtmefunktsioonidele; kontrollpunktid eksisteerivad, et kindlustada IT eesmärgid ja pika- ning lühiajalised plaanid jätkuvalt vastavad ettevõtte pika- ja lühiajalistele eesmärkidele.

Lõpuks, auditi juhised põhjendavad riski viies läbi analüüsi strateegiliste IT plaanide võrdlemiseks sarnaste ettevõtetega või vastavate rahvusvaheliste standardite/parimate praktikatega; detailne ülevaade IT plaanidest kinnitamaks, et IT peegeldab ettevõtte missiooni ja eesmärke; ning detailne vaade IT plaanidest saamaks kinnitust, et ettevõtte nõrgad kohad on üles leitud ja nende parendamisega tegeletakse ühe osana planeeritud IT tegevustest.

CobiT saavutab üha laiemat tuntust IT kontrolleesmärkide ja IT auditi vallas. CobiT’it leiab üha sagedamini erinevate ettevõtete auditi juhendites. Ka raamatupidamisettevõtted kasutavad seda osana auditi protseduuridest, kui auditeeritakse IT-d. IT juhid ühendavad CobiT’i põhimõtteid oma protseduuride ja reeglistikega IT vahendite haldamiseks. Turvajuhid kasutavad CobiT’i turvareeglistikke ja protseduure.

CobiT'i Kuldne Reegel on, et IT vahendid peavad olema hallatud loomulikult grupeerunud protsesside poolt, et pakkuda informatsiooni, mida ettevõte vajab oma eesmärkide saavutamiseks.
See on otsustav koht saavutamaks kontrolleesmärke ja see on otsustav koht auditis – teha kindlaks, et ettevõte saavutab oma missiooni ja eesmärgid.

IT protsessimaatriks:

Informatsioon

- efektiivsus
- jõudlus
- konfidentsiaalsus
- integreeritus
- kättesaadavus
- kuuletumine
- usaldusväärsus

IT vahendid

- inimesed
- rakendused
- tehnoloogia
- abivahendid
- andmed

IT protsessid

CobiT-st on kasu juhtidele, IT spetsialistidele ja audiitoritele. Juhtidel aitab see selgusele jõuda, milliseid IT otsuseid ja investeeringuid võib usaldada. Otsuste langetamine on efektiivsem sest CobiT aitab juhatusel defineerida strateegilise IT plaani, defineerides infotehnoloogia arhitektuuri, soovitab vajaliku IT raudvara ja tarkvara, millega strateegilist plaani teostada, kindlustades järjepideva teenuse osutamise ja IT süsteemide käitluse seire. IT kasutajad saavad CobiT'ist tuge defineeritud juhtimisest, turvamisest ja protsessi haldusest. Audiitorid saavad kasu sest see aitab neil identifitseerida IT juhtimisega seotud valdkondi ettevõtte infrastruktuuris. Ühtlasi aitab see neil tõestada oma auditi leide. (ITGI 2007)

BS7799

BS 7799 avaldati esmakordselt 1995 aastal Briti Standardite Instituudi (BSI) poolt. Peale mitmeid muudatusi võttis ISO[11] ta enda standardite hulka kui ISO/IEC 17799, Infotehnoloogia – parima praktika (Code of Practise) infoturbe haldamiseks. BS ISO/IEC 27001:2005 sobib igat tüüpi ettevõtetele ja selles on täpsustatud nõudmised ISMS-i (Information Security Management System) loomiseks, juurutamiseks, opereerimiseks, seireks, vaatlemiseks, haldamiseks ja parendamiseks/arendamiseks ettevõtte üldiste riskide kontekstis.

ISO/IEC 27001:2005 (BS 7799-2:2005) on uus rahvusvaheline standard, mis pakub spetsifikatsioone ISMS-le ja põhineb kolmanda-osapoole auditile ja sertifitseerimisele. Standard on täienduseks standardile BS ISO/IEC 17799:2005 (BS 7799-1:2005).

BS7799 – turvalisuse aluskontrollid

- 10 kontrolli kategooriat (ingl. k. control category)
- 32 kontrolli gruppi
- 109 turvalisuse kontrolli
- 10 turvalisuse põhikontrolli

BS7799 – kontrollikategooriad

- informatsiooni turvalisuse poliitika
- turvaosakond
- varade klassifitseerimine ja kontroll
- töötajate turvalisus
- füüsiline ja keskkondlik turvalisus
- arvutite ja võrgu haldus

BS7799 – kontrollikategooriad

- süsteemi juurdepääsu kontroll
- süsteemide arendamine ja hooldamine
- äri järjepidevuse planeerimine
- järgimine

[11] ISO – International Organisation for Standardisation

BS7799 10 võtmekontrolli (*ingl. k. key controls*)

- informatsiooni turvalisuse poliitika
- informatsiooni turvalisuse vastutuse hajutamine
- turvalisusealane koolitus
- turvajuhtude raporteerimine
- viiruste kontroll
- äri järjepidevuse planeerimise protsess
- kontroll tarkvara kopeerimise üle
- ettevõte infomaterjalide turvamine
- andmekaitse
- turvareeglistike järgimine. (BS 7799.BIZ 2007)

Peamine standardi eesmärk on aidata luua ja hallata informatsiooni haldamissüsteemi kasutades järjepidevat arendamise lähenemist. Uus standard asendab BS 7799-2:2002.
Informatsiooni riskide haldamise võtmeprotsessideks, kui ettevõte tahab hoida oma informatsiooni salajas ja turvaliselt, on nende tuvastamine, hindamine, käitlemine ja haldamine.

ISO/IEC 27001 standard viitab sellele, et erinevate osapoolte informatsiooni konfidentsiaalsuse, terviklikkuse ja kättesaadavuse osas on nõuded täidetud.

ISO/IEC 17799 koosneb kahest osast – esimene standardi osas koosneb enam kui sajast turvalisusega seotud kontrollist, mis aitavad ettevõtetel hinnata oma äris informatsiooni turvalisusega seotud valdkondi; teine osa on spetsifikatsioon, mille alusel neid saab hinnata ja registreerida.

BS7799 põhineb infovarade kättesaadavuse, konfidentsiaalsuse ja integreerituse kindlustamisel. See saavutatakse läbi kontrollide, mille ettevõtte juhtkond organisatsiooni sees loob ja haldab. 10 võtmekontrolli eduka informatsiooni turvalisuse loomiseks on:

- informatsiooni turvalisusreeglid on dokumenteeritud
- informatsiooni turvalisusega seotud vastutuste jagamine ettevõtte sees
- informatsiooni turvalisusega seotud informatsiooni jagamine ja koolitamine
- turvaintsidentide raporteerimine

- viiruse avastamise ja vältimise kontrollid
- äri järjepidevuse planeerimine
- kontroll firmasisese tarkvara kopeerimise üle
- kriitiliste andmete haldamise protsessid
- personaalsete andmete kaitse
- perioodilised vastavus-ülevaated

ISO 17799 kaudselt tunnistab, et informatsiooni turvalisus ja ISMS peaksid olema integreeritud osa igast sisekontrolli süsteemist, mis on loodud osana ettevõtte valitsemise protseduuridest.

BS7799 koosneb 10 erinevast osast:

- turvalisusega seotud reeglid: selle osa eesmärk on pakkuda juhiseid ja väljavaateid informatsiooni turvalisuse osas
- vahendite ja varade organiseerimine: selle osa eesmärk on hallata ettevõtte infosüsteeme
- varade kontroll ja klassifitseerimine: selle osa eesmärk on valmistada nimekiri ettevõtte varadest, kaasa arvatud infovarad ja nendele vastav turvalisus
- personaliga seotud turvalisus: selle osa peamine eesmärk on vähendada riski, mis võib tekkida seoses inimlike vigadega, pettustega, varastamisega või ettevõtte varade vale kasutamisega
- keskkondlik ja füüsiline turvalisus: eesmärgid on peaaegu samad, mis personaliga seotud teemade, kuid siinkohal on ohuks keskkonnast tulenevad ohud ja füüsilise asukohaga seotud ohud
- kommunikatsiooni ja tegevuste haldus: eesmärkideks on turvalise tegutsemise tagamine ettevõtte informatsiooni töötlemisel; süsteemi maasoleku aja vähenemisel jms
- juurdepääsukontroll: selle osa eesmärgiks on kontrollida igat sorti juurdepääsetavusi
- süsteemide arendamine ja haldamine: see osa on seotud reeglitega süsteemi maas oleku ajaks ja regulaarsete varundamistega
- äri järjepidevuse haldus: selle osa eesmärgiks on kindlustada äri protsesside toimimine

- vastavus: selle osa eemärgiks on standardite rakendamine, seadusandluse jälgimine ja auditi protsessist tuleneda võivate häirete vähendamine.

Turvamata süsteemid on haavatavad igasugustele ohtudele, nagu nt arvutipettused, viirused ja väljapressimised. Sellised ohud võivad olla nii sisemised kui välised ning nii juhuslikud kui pahatahtlikud. Augud informatsiooni turvalisuse osas võivad saada pääseteeks andmetele juurdepääsuks, varastamiseks, korruptsiooniks või kadumiseks.

Informatsiooni turvahaldussüsteem vastavuses ISO/IEC 27001 võib aidata näidata oma partneritele, et antud ettevõttes võetakse informatsiooni turvalisust tõsiselt.

ISO/IEC 27001 sertifikaat on suurepäraseks vahendiks tõestamaks ettevõtte pühendumust hallata informatsiooni turvaliselt.

Kuna paljud ettevõtted nõuavad enne koostöö alustamist ISO/IEC 27001 sertifikaati, on see ühtlasi ka konkurentsivõime näitajaks. Ettevõttel on võimalik teha avalikke seisukohavõtte ilma oma turvaprotsesse paljastamata ning ettevõtlusrisk on minimiseeritud kui riskivähenduskontrollid on paigas ja turvaohud ega süsteemi nõrkused ei ole ekspluateeritavad.

Sertifitseerimine on võimalik erinevate asutuste poolt üle maailma. Sertifikaadi auditeid viivad enamasti läbi ISO/IEC 27001 juhtivaudiitorid.

ISO/IEC 27001 sertifitseerimine hõlmab enamasti kolmetasemelist protsessi:

1) ülevaade põhidokumentatsioonist nagu ettevõtte turvanõuded, riskikäideldavuse plaan
2) detailne audit kaasates informatsiooni turvalisuskontrollide kättesaadavuse testimist, ühtlasi ka toetusmaterjali
3) kontrollimine, et eelnevalt sertifitseeritud organisatsioon ka säilitab standardi jälgimise. Sertifitseerimine hõlmab perioodilisi ülevaatusi ja hindamisi veendumaks, et ISMS on jätkuvalt töös nagu planeeritud. (ISO 17799 2008)

GAIT

GAIT (Guide to the assessment of IT risks) kirjeldab suhteid finantsaruannete, äriprotsesside võtmekontrollide, automaatsete kontrollide ja muude IT kriitiliste funktsionaalsuste ning IT üldiste kontrollide võtmekontrollide vahel. GAIT metoodika on juhend hindamaks IT üldiseid kontrolle kasutades ülalt-alla ja riskipõhist lähenemist. Seda võivad kasutada nii juhid kui siseaudiitorid IT üldiste kontrollide identifitseerimiseks ja finantsandmete raporteerimiseks. See on loodud aitamaks identifitseerida võtmekontrolle, mis võivad läbi kukkudes kaudselt põhjustada materiaalse vea finantsaruandes.

IIA (The Institute of internal auditors) arendas selle juhise, et aidata ettevõtetel identifitseerida võtme- IT üldisi kontrolle, kus tõrge võib põhjustada materiaalset kahju finantsaruandes. Veel enam, see metoodika laseb juhtkonnal ja audiitoritel identifitseerida võtme-IT üldised kontrollid osana ja järjepidevana ettevõtte ülalt-alla, riskipõhise SOX 404 (Rittenberg 2005) järgimise.
Kui tõrge on tõenäoline, siis metoodika identifitseerib IT üldised kontrollprotsesside riskid detailselt ja kui IT üldised kontrolleesmärgid on saavutatud, riski hajutada.

Põhimõtted
Metoodika 4 põhimõtet:

1) IT üldiste protsesside riskide identifitseerimine peaks olema järjepidev ülalt-alla ja riskipõhine lähenemine, mis on mõeldud tähtsate kontode, nende kontode riski ja võtmekontrollide protsessides.
2) IT üldiste kontrollprotsesside riskid on need, mida on vaja leida ja mis mõjutavad kriitilisi IT funktsionaalsusega seotud finantsvahendeid ja nendega seotud andmeid.
3) IT kontrollprotsesside riskid, mida on vaja identifitseerida, leiduvad erinevates protsessides ja mitmetes IT kihtides: rakendusprogrammide koodides, andmebaasides, operatsioonisüsteemides ja võrgus
4) Riskid IT üldistes protsessides leevendavad kontrolleesmärkide saavutamist, mitte eraldiseisvaid kontrolle

GAIT metoodika võimaldab ettevõtetel need põhimõtted rakendada ning annab juhtkonnale ja audiitoritele juhised IT üldiste kontrollide skoobi määratlemisel ning vahendid ka nende otsuste kaitsmiseks. (IIA 2006)

GAIT2 e. GAIT IT üldiste kontrollide puudujääkide hindamine laseb hinnata iga-aastase sisekontrolli raames finantsraporteerimise jooksul selguvaid IT üldiste kontrollide puudujääke.
See juhend on mõeldud audiitoritele või juhtkonnale hindamaks kas neil on materiaalseid nõrkusi või silmapaistvaid puudujääke.
GAIT2 hindamisprotsess koosneb 10st sammust, mis põhinevad 6 põhimõttel, milleks on:

1) et hinnata ITGC[12] puudujääke on oluline mõista sõltuvusahelat finantsaruannete ja võtme ITGC-de vahel, mis on läbi kukkunud
2) materiaalse nõrkuse tunnuseks tuleb teha 2 testi: a) tõenäosus b) mõju
3) kuna ITGC puudujäägid ei mõjuta otse finantsaruandeid, ei ole hinnang samuti ühene. Hinnang on erinevates etappides või sammudes, ning tõenäosus- ja sõltuvustestid on kohaldatud ümber erinevate sammukombinatsioonide.
4) kõik ITGC puudujäägid, mis on seotud samade ITGC eesmärkidega tuleb hinnata grupina
5) kõik ITGC eesmärgid, mida ei ole saavutatud ja mis ei ühildu samade automaatsete võtmekontrollidega, võtmeraportitega, või teiste kriitiliste funktsionaalsustega, tuleb hinnata kui gruppi
6) liitmise põhimõte nõuab, et igat tüübi kontrollpuudujäägid, k.a. manuaalsed ja automaatsed kontrollpuudujäägid, mis on seotud samade kontode või avalikustamisega tuleb lugeda ühte gruppi. (IIA 2008b)

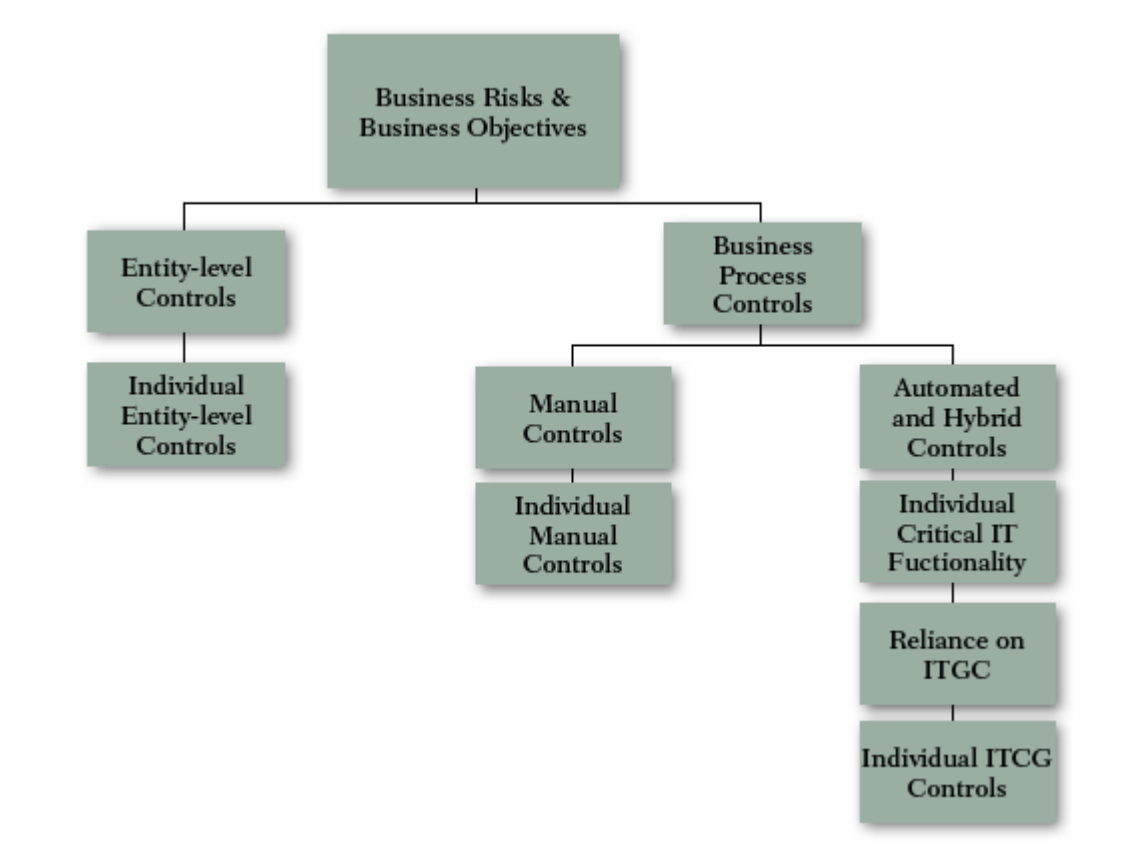
GAIT-R [13](GAIT IT ja äri riskideks) metoodika on üles ehitatud järgmistele põhimõtetele:

1) tehnoloogia äpardumine on ainult risk, mida tuleb hinnata, hallata ja auditeerida kui see kujutab endast ohtu ettevõttele
2) võtmekontrollid tuleb identifitseerida ülalt-alla ettevõtte riskide, riskitaluvuse ja kontrollide hindamise tulemusena – kaasa arvatud automaatsed kontrollid ja IT üldised kontrollid

[12] ITGC – Information Technology General Controls
[13] GAIT-R – GAIT for Business and IT Risk

3) äririskid on maandatud kombineerides automaatseid ja käsitsi kontrolle. Et hinnata sisemiste kontrollsüsteemide haldamist või hajutada äririske tuleb automatiseeritud kontrolle hinnata
4) IT üldised kontrollid võivad toetuda automatiseeritud kontrollide õigele käitumisele
    a. ITGC protsessi riskid, mida on vaja identifitseerida, on need, mis mõjutavad kriitilist IT funktsionaalsust olulistes rakendustes ja andmetes
    b. ITGC protsessiriskid eksisteerivad erinevates protsessides ja IT kihtides
    c. IT kontrolleesmärkide saavutamine kergendab ITGC protsessiriski

Joonis 5 GAIT-R kontrollide identifitseerimine



IT kontrollid jagunevad kaheks: üldised kontrollid ja rakenduste kontrollid.

Üldised kontrollid (ühtlasi ka infrastruktuuri kontrollid) seonduvad kõigi süsteemi komponentidega, protsessidega ja andmetega. Üldised kontrollid hõlmavad infoturbe poliitikat, administreerimist, sissepääse ja autentimist; varukoopiaid, taastust ja järjepidevust.

Rakenduste kontrollid on seotud individuaalsete äriprotsessidega või rakendussüsteemidega. Need hõlmavad selliseid kontrolle nagu andmete haldamine, toimingute logid ja vigade raporteerimine.
Kontrolle võib klassifitseerida kui vältivad, avastavad ja parendavad.
Vältivad kontrollid väldivad vigu või turvalisust puudutavaid tegevusi juhtumast.
Avastavad kontrollid avastavad vigu või juhtumeid, mis on suutnud vältida vältivaid kontrolle.
Parandavad kontrollid parandavad vigu või juhtumeid kui nad on juba leitud.

Ülalt-alla lähenemine koosneb erinevatest võtmekontrollidest (nt olemi tase ja tegevustase, manuaale, automatiseeritud, ITGC) sõltub ära hoidmisest või materiaalsete valeandmete avastamises finantsaruandluses.

Kui üks või mitu nendest kontrollidest peaks läbi kukkuma, siis kontrollide kogu ei suuda enam pakkuda nõutaval tasemel kindlustunnet ega vigade vältimist või leidmist.

Kontrollid võivad läbi kukkuda mitmel põhjusel ning selle ulatust tuleb mõista ja tähele panna hindamise jooksul. (IIA 2008c)

2. IT auditi metoodikatest tulenevad soovitused

CobiT

Et IT oleks võimeline edukalt ärinõudeid täitma, peab juhtkond panema paika sisekontrolli süsteemi või vastava raamistiku.
CobiT toetab IT valitsemist raamistikuga, mis kindlustab, et:

- IT on joondatud äriga
- IT järgib äri ning suurendab kasumit
- IT vahendeid on kasutatud vastutustundlikult
- IT riske hallatakse asjakohaselt

IT valitsemine

IS audiitor peab üle vaatama ja hindama kas IS funktsioonid on joondatud ettevõtte missiooni, visiooni, väärtuste, eesmärkide ja strateegiatega.
IS audiitor peab üle vaatama kas IS funktsioonidel on selge väljund, mida eeldab äripool ning lisaks peab audiitor hindama ka selle saavutusi.
IS audiitor peab vaatlema ja hindama IS ressursside efektiivsust ning nende talitlusprotsesse.
IS audiitor peab vaatlema ja hindama kooskõlastatust seaduste, keskkonna ja informatsiooni kvaliteedi ning hooldus- ja turvanõuetega.
IS audiitor peab hindama IS käitumist riskipõhise lähenemisega.
IS audiitor peaks vaatlema ja hindama riske, mis võivad ebasoodsalt mõjutada IS keskkonda.

IT kontrollid

IS audiitor peaks hindama ja jälgima IT kontrolle, mis on üks integreeritud osa sisemisest kontrollkeskkonnast organisatsioonis.
IS audiitor peaks juhendama juhatust IT kontrollide disainimise, rakendamise, käitlemise ja arendamise osas.

Erinevat tüüpi auditi tõendusmaterjale, mida IS audiitor peaks arvesse võtma, koosnevad:

- jälgitavad protsessid ja füüsiliste esemete olemasolu
- dokumenteeritud auditi tõendusmaterjal
- uuesti presenteerimine
- analüüsimine

IS audiitor peaks skoobi ja eesmärkide arvestamisel arvesse võtma rahvusvahelisi sertifikaate või raamistikke ning ISO nõudeid, mis võivad rakenduda välistele teenustele.

Lepingud väliste teenusepakkujatega

IT audiitor peaks arvesse võtma järgnevat:

- formaalse lepingu olemasolu teenuse pakkuja ja teenuse kasutaja vahel
- lepingus peab kajastuma, et teenuse pakkuja kohustub järgima kõiki seadusega määratud sätteid oma tegevuses ja täitma kõiki funktsioone teenuse kasutaja ees
- teenusepakkuja peab järgima kooskõlastust SLA[14]-ga ning ennetavalt raporteerima kõik turvajuhtumid või –kontrollide puudujäägid
- käitlemisseire protsessidega SLA olemasolu
- teenusepakkuja valmisolekut jätkata tegutsemist ka katastroofiolukorras
- teenuse kasutaja turvapoliitikatest kinnipidamist
- kontrollima teenuse pakkuja personalipoliitika ja protseduuride adekvaatsust

Sisseostetud teenuste haldamine

IS audiitor peab kindlustama, et:

- Äriprotsessid informatsiooni loomiseks, mis on mõeldud SLA-de täitmise monitoorimiseks on korrektselt kontrollitavad. Teenuse kasutaja peab olema kas teatud standardi teenuse taseme informatsiooni võimaldamiseks aktsepteerinud või on kooskõlas teenuse kasutajaga lisanud lisa raporteerimise võimalused
- kui SLA ei ole täidetud, on teenuse kasutaja nõudnud selle heastamist ja parandustegevusi, et saavutada taas kokkulepitud teenuste tase

[14] SLA – Service Level Agreement

- teenuse kasutajal on võimalusi ja oskusi kuidas jälgida ja vaadelda pakutavaid teenuseid

Riskide hindamine

IS audiitor peab hindama riski tekkimise tõenäosust ja sellest tekkida võivaid ebaregulaarsust. Enne hindamist peab audiitor arvesse võtma järgmisi faktoreid:

- organisatsiooni karakteristikud: nt eetika, ettevõtte struktuur, juhtimise adekvaatsus, kompenseerimise ja tasustamise põhimõtted tulenevalt korporatsiooni tegevustest
- ettevõtte ajalugu
- hiljutised muudatused juhatuses, tegevuses, IT süsteemides
- varade tüübid, pakutavad teenused
- vastavate kontrollide tugevused
- vastavad regulatsioonid või seaduslikud nõuded
- eelnevate auditite leiud
- tööstus ja konkurentsikeskkond
- auditiväliste osapoolte hinnangud, nt konsultantidelt, kvalifikatsiooni meeskondadelt või muudelt spetsiifilistelt juhatuse leidudelt
- igapäevatöös välja tulnud avastused
- majasiseselt arendatud/hallatud rakendussüsteemide olemasolu võrreldes „paki“-tarkvaraga

Detailsed IS kontrollid

Detailsed kontrollid koosnevad rakenduskontrollidest ja üldisest kontrollist välja jäävad IS kontrollid. CobiT’i järgi on detailsed kontrollid IS süsteemide ja teenuste rakendamise, üleandmise ja toetamise kontrollid. Nt:

- tarkvarapakettide juurutamine
- süsteemi turvalisuse parameetrid
- katastroofist taastumise planeerimine
- sisendandmete valideerimine

- erandite raportite tootmine
- kasutajakontode sulgemine peale ebaõnnestunud sisselogimist

Informatsiooni kogumine

Oma iseseisvuse säilitamiseks peavad audiitorid muu hulgas saama ülevaate organisatsioonist. Selleks tuleb vaadelda:

- organisatsiooni reegleid ja protseduure seoses iseseisvate protsessidega
- missiooni, poliitikaid, protseduure ja standardeid ning auditi plaane
- organisatsiooni mudel

Igal IS kontrollitasemel peab audiitor arvestama vastava taseme auditi valdkonna küsimustega:

- IS juhtimise terviklikkus, IS juhtimise kogemus ja teadmised
- muudatused IS juhtimises
- IS juhtimises ettetulevad pinged, mis võivad põhjustada ebaõige informatsiooni esitamist (nt üle-aja läinud projektid, häkkerirünnakud jne)
- ettevõtte äri ja süsteemide olemus (nt elektroonilise äri plaanid, süsteemide keerukus jne.)
- faktorid, mis mõjutavad ettevõtet kui tervikut (nt muutused tehnoloogias ja IS personali kättesaadavus)
- auditeeritavate süsteemide sõltuvus kolmandatest osapooltest (sisse ostetud IS protsessid ja klientide otsene juurdepääs jms)
- leiud eelnevatest auditit est

Rakendustaseme riskid süsteemis ja andmete tasemel hõlmavad:

- süsteemi kättesaadavuse risk tulenevalt süsteemi töövõimest
- süsteemi turvalisuse risk tulenevalt andmetele ja/või süsteemidele autoriseerimata juurdepääsust
- süsteemi käideldavuse risk tulenevalt võimetusest mitte süsteemi uuendada vastavalt nõudmistele, mis tagavad süsteemi kättesaadavuse, turvalisuse ja täiuslikkuse
- andmete täielikkuse, integreerituse, konfidentsiaalsuse ja õigsusega seotud riskid

IS audiitor peab saama infot ettevõtte infosüsteemide strateegiast, k.a.:

- lühi- ja pikaajalised plaanid ettevõtte missiooni ja eesmärkide täitmiseks
- lühi- ja pikaajalised strateegia ja plaanid IT ja süsteemide plaanide toetamiseks
- IT strateegia, arendusplaanide ja jälgimise progress vastavalt nendele plaanidele
- IT strateegia ja plaanide kontrolli muutmine
- IT missiooni sõnastamine ja kokkulepitud eesmärgid ning eesmärgid IT tegevustele
- hinnang kasutuses olevatele IT tegevustele ja protsessidele

Ülevaade tippjuhtkonna tegevustest

IT valitsemine, olles osa ettevõtte valitsemisest peaks juhinduma ettevõtte eesmärkidest. Audiitor peab hindama kas äristrateegia planeerimise protsess on olemas, arvestades:

- eksisteerib selge ärivisioon ja missioon
- kasutusel on äristrateegia planeerimise metoodika
- protsessi hõlmatud isikute arv on sobiv
- plaani uuendatakse perioodiliselt

IT strateegilise planeerimise protsesse vaadates tuleb audiitoril arvesse võtta, et:

- olemas selgelt defineeritud IT missioon ja visioon
- strateegiline IT planeerimise meetod on kasutuses
- metoodikas on seoses ärieesmärgid ja IT ärieesmärgid
- seda plaani uuendatakse perioodiliselt
- plaan määrab ära peamised IT vajatavad initsiatiivid ja ressursid
- protsessi hõlmatud isikute arv on sobiv

Vaadeldes IT taktikalist plaani peaks IT audiitor jälgima, et projektijuhtimise praktikad on kasutusel, arvestades:

- mis määral on projektijuhtimise metoodikad kasutusel
- projektijuhtimise kontrollid oleks rakendatud
- projektijuhtimise vahendid oleksid kasutuses

IT ja äriinimeste integreeritus erinevates projekti faasides

- muudatuste halduse metoodikad on kasutusel suurtes projektides, mis kaasavad suuri muutusi ettevõtetes

Vaadeldes olemasolevate süsteemide portfooliote haldamise protsesse peaks audiitor arvesse võtma käesolevate süsteemide strateegia ja toetusosa hõlmatust:

- kas protsessi hõlmatud inimestel on piisavalt oskusi ja teadmisi ning kogumusi oma rollide täitmiseks
- hinnata kas IT spetsialistide meeskond või funktsioonid on vastavad, et ettevõte saaks saavutada oma eesmärgid parimate IT lahendustega
- hinnata kas IT spetsialistide ja IT vastutusega mitte-spetsialistide juhid on võimelised hindama ettevõtte riske ohu, tegemata jätmiste või illegaalsete tegevuste korral

IS audiitor peab hindama ka teisi riskidega seotud faktoreid, mis võivad neid mõjutada:

- töötajate rahulolematus
- potentsiaalne vallandamine, sundlikvideerimine, sisse ostmine
- varade olemasolu, mis on lihtsalt plagieeritavad
- juhtkonna suhtumine eetikasse
- illegaalsed ja ebakorrapärased tegevused, mis on teatud tööstusele omased või mida on ette tulnud teistes taolistes ettevõtetes

Turvalisuse teemasid üle vaadates tuleb auditisse lisada:

- sidekanalid (nuuskijad, protokollid nt dekrüpteerimise tehnoloogiad jne)
- võrgu arhitektuur
- virtuaalsed võrgud
- rakenduste üleandmine
- turvateadlikkus
- kasutajate administreerimine
- kasutajate ja sessioonide administreerimine
- füüsiline turvalisus
- avaliku võtme infrastruktuur
- varukoopiad ja taastusprotseduurid
- toimingud (nt back-office töötlemine)

- tehnoloogia arhitektuur
- turvalisuse arhitektuur
- turvatarkvara (IDS, antiviirused, tulemüür)
- turvalisuse administreerimine
- pakktööde (batch'ide) haldamine
- äri järjepidevuse planeerimine

Personaalsete andmete kaitse

Digitaliseeritud ja „hard copy" andmete käitlemiseks peavad olema reeglid ja nõuded, et kaitsta personaalsete andmete turvalisust, terviklikkust ja kättesaadavust. Igas ettevõttes peab olema teatud lähenemine igat sorti personaalsete andmete kaitsmiseks ja need peaks arvestama:

- privaatsuse juhtimine – ettevõtte juht peab olema esmaselt vastutav privaatsuse eest. Personaalse informatsiooni kasutamiseks peab olema kirjeldatud turvalisuse/poliitika ja strateegia juhendis. Seal peab olema formaalselt kirjeldatud personaalse informatsiooni rutiinide sage hindamine toetudes avalikele seadustele ja regulatsioonidele.
- riski hindamine – ettevõttel peab olema ülevaade erineva personaalse informatsiooni kasutamisest. Ettevõttel peab olema paika pandud teatud riskikriteerium personaalse informatsiooni käitlemiseks. Vastutus personaalse info haldamise eest peaks minema andmekontrollerile. Riski hindamise tulemus peab olema dokumenteeritud.
- turvalisuse audit – turvalisuse audit seoses infosüsteemi kasutamisega peab olema läbi viidud regulaarselt. Tulemused peavad olema dokumenteeritud.
- kõrvalekalded – kõik infosüsteemide kasutamised, mis ei vasta formaalsetele rutiinidele ning mis võivad põhjustada turvalisuses lõhesid, peavad olema käsitletud kui kõrvalekalded. Kõrvalekallete käitlemise eesmärk on taastada normaalolukord, kõrvaldada põhjused, mis viisid kõrvalekaldumisele ja vältida nende kordumist. Kui kõrvalekalded on põhjustanud konfidentsiaalse informatsiooni jõudmise autoriseerimata isikuni, tuleb teavitada kohalikke võime. Tulemused peavad olema dokumenteeritud.

- organisatsioon – infosüsteemide kasutamise vastutus peab olema sisse viidud ja dokumenteeritud. Vastus peab olema muutumatu ilma vastava juhtkonna otsuseta. Infosüsteem peab olema seadistatud pakkumaks turvatunnet. Seadistus peab olema dokumenteeritud ning seda ei tohiks muuta ilma vastava juhtkonna loata.
- meeskond- töötajad peaks kasutama personaalset informatsiooni vastavalt oma ülesannetele ja vastavalt õigustele. Lisaks sellele peavad töötajatel olema vastavad teadmised, et kasutada infosüsteemi kooskõlas kehtivate rutiinidega. Autoriseeritu infosüsteemide kasutamine peab olema registreeritud.
- professionaalne salastatus – töötajad peaks allkirjastama formaalse lepingu mitte jagama konfidentsiaalset infot.
- füüsiline turvalisus – personaalse informatsiooni töötlemiseks peab ettevõte kasutusele võtma meetmed autoriseerimata juurdepääsu vältimiseks. Vahendid selleks tuleb installeerida nii, et nad ei põhjustaks personaalse info käitlemist.
- konfidentsiaalsus – ettevõte peaks võtma kasutusele meetmed, et vältida autoriseerimata juurdepääsu personaalsele informatsioonile. Konfidentsiaalne informatsiooni, mida edastatakse partneritele peaks olema krüpteeritud või turvatud muul moel. Salvestatud informatsioon, mis sisaldab konfidentsiaalset infot peab olema vastavalt märgistatud.
- täielikkus - personaalse informatsiooni autoriseerimata muudatuste vastu tuleb kasutusele võtta meetmed, mis tagaksid andmete terviklikkuse.
- turvalisuse meetmed – vältimaks autoriseerimata õigustega informatsiooni kasutamist tuleb kasutusele võtta meetmed, mis suudavad ka avastada vastavad katsetused. Kõik autoriseerimata õigustega sissepääsu katsed tuleb salvestada.
- dokumentatsioon – infosüsteemi kasutamise rutiinid ja teiste informatsiooni turvalisusega seotud informatsioon peab olema dokumenteeritud, mis peab olema ladustatud vastavalt kohalikele seadustele ja regulatsioonidele.
- koolitused teadlikkuse tõstmiseks – need tuleb läbi viia, et teadvustada neid töötajatele ja teenusepakkujatele, eriti neile, kes tegelevad kliendiinfo haldamisega (nt klienditeenindus)

OECD[15] poolt avaldatud andmete kaitse põhimõtted:

N°	põhimõte	selgitus

[15] OECD - Organization for Economic Co-operation and Development

1	Kogumise piirangud	Personaalsete andmete kogumine on võimalik, kui on teada andmete sisu.
2	Andmete kvaliteet	Personaalsed andmed on vastavuses eesmärgiga, milleks neid kasutatakse ja nad vastavad sellele määrale, on täpsed, täielikud ja ajakohased.
3	Eesmärgi spetsifikatsioon	Eesmärgid, milleks personaalseid andmeid kogutakse, on selgitatud hiljemalt andmete kogumise ajaks.
4	Kasutamise piiramine	Personaalseid andmeid ei tohi olla avalikustatud, kättesaadavaks teha või muul moel kasutada kui ülevalpool kirjeldatud juhtudel
5	Turvalisuse kindlustamine	Personaalseid andmeid tuleb kaitsta kindlustamaks nende turvalisust riskide vastu, nagu nt kadu või autoriseerimata juurdepääs, andmete muutmine või avaldamine
6	Avatus	Personaalsete andmete huvides peavad olemas olema avalikkuse reeglid arenduste, tavade ja reeglite kohta.
7	Individuaalne osavõtt 1	Indiviidil on õigus kinnitust selle kohta, kas andmekontrolleril on tema kohta infot õi mitte
8	Individuaalne osavõtt 2	Indiviidil on õigus saada andmeid enda kohta: • mõistliku ajaga • tasu eest, kui üldse, mis ei ole suur • mõistilikul moel • talle arusaadaval kujul
9	Individuaalne osavõtt 3	Indiviidil on õigus vaidlustada punktis 7 ja 8 toodud nõuete keeldumisel, see keeld
10	Individuaalne osavõtt 4	Indiviidil on õigus vaidlustada tema kohta olev informatsioon ning kui see on õigustatud, nõuda andmete kustutamist või korrastamist
11	Individuaalne osavõtt 5	Tuleb luua protseduurid selleks, et kui isik soovib andmete kasutamist ja avalikustamist

		muuta, peavad need muudatused toimuma kõigis süsteemides, kus tema andmeid on kasutatud
12	Andmekontrolleri aruandekohustus	Andmekontroller on vastutav mõõdikute vastavuse eest

IS audiitor peab välja selgitama kas ettevõttel on olemas:

- reeglid privaatsusele
- privaatsuse kontroller
- andmekontroller
- privaatsusega seotud koolitusplaan
- privaatsusega vastavuses juhtimisprotsess
- privaatsusnõuded töövõtjatele ja sisseostetud teenustele

ning kui on olemas, siis peab audiitor hindama nende vastavust seadustele ja regulatsioonidele.

IS audiitor peab hindama järgmisi administratiivseid tegevusi:

- juhatuse vastustus
- interneti juurdepääsu andmise põhjused
- kas ettevõttel on konfidentsiaalseid andmeid, mis tähendab, et ligipääs internetile peab olema piiratud või keelatud
- ühenduse tüüp
- kas juurdepääs on piiratud teatud tundidega või ajaga päevas/nädalas
- kas on piiranguid töötajatele surfamiseks/informatsiooni korjamiseks
- kas ettevõte müüb teenuseid/tooteid interneti vahendusel ning kas maksed on tehtud interneti vahendusel
- kas ettevõttel on vajalikud teadmised, aega ja võimalusi installeerida, jälgida ja hallata internetti

Interneti kasutusjuhend peab sisaldama vähemalt:

- ühendust turvameetmetega
- dokumentatsiooni teenustest, mis on lubatud
- reeglid nendele teenustele ja sanktsioonid, mida kasutatakse kui neid reeglid rikutakse
- eetilise suhtumise dokumentatsioon
- reeglid e-kirjade saatmises ja salvestamiseks
- nõuded kasutajate koolitamiseks

- lepingud, mille kõik töötajad peavad allkirjastama ning kus on sätestatud, et nad järgivad reegleid

Vastutused turvajuhtimises:

- informatsiooni turvamisega tegeleval isikul ei tohi olla lisafunktsioone nagu nt IT operaator, süsteemianalüütik või programmeerija
- turvajuhi üks peamiseid ülesandeid on välja töötada reeglistik interneti kasutamiseks ning jagada informatsiooni kasutajatele
- tulemüüride logide jälgimine
- turvasüsteemide raportite jälgimine
- kindlustada, et turvameetmeid testitakse regulaarselt
- kindlustada, et järjepidevuse ja katastroofiplaanid katavad ettevõtte tegevusi
- jälgida turvajuhtumeid ja katsetusi
- tõsiste intsidentide raporteerimine juhtkonnale

Tehnilised probleemid ja turvameetmed

Tehnilised teemad koosnevad:

- turvaalarmid ja autoriseerimata kasutajate katsetused tuleb aktiviseerida tarkvaras
- ühendus sisemise võrgu ja interneti vahel peab olema kaitstud tulemüüriga
- ainult juhtkonna poolt lubatud teenuseid saavad tulemüürist mööda
- tulemüür peaks peatama kõik lubamata võrguprotokollid
- tulemüür peaks peatama kõik sissepääsud kui tegevuses ilmnevad vead

Teenusega seotud meetmed sisaldavad:

- e-kiri
  - kriitilised kirjad peaks olema krüpteeritud
  - ajakriitilisi teateid tuleb jälgida manuaalselt
  - manused tuleb skaneerida vältimaks kahjustusi rikutud koodist
  - salasõnu ei tohi saata e-kirjaga
- WWW
  - internetti kasutades tuleb kasutusele võtta salasõnad ja kasutajanimed, mis oleksid teised, kui need, mida kasutatakse sisevõrgus

    - informatsiooni, mis on alla laetud internetist tuleb enne kasutamist kontrollida
    - kasutama peaks lubatud brauserit
    - kõik alla laetud failid tuleb kontrollida viiruste vastu
- FTP
    - kõik alla laetud failid tuleb kontrollida viiruste vastu
- uudised
    - kasutajad ei tohi kirjutada artikleid, mis võiksid ettevõttest, töötajatest, partneritest, tarnijatest vms jätta negatiivset muljet
    - uudistest kogutud informatsiooni tuleb kontrollida enne kasutamist
- otsesuhtlus (MSN/IRC)
    - kasutamisel ei tohi jagada ettevõttega seotud informatsiooni

Varade jälgimine ja vahendid

- varasid tuleb jälgida, et vältida nende varastamist, valeotstarbelist kasutamist
- tarkvara peab olema sildistatud, inventaris ja litsentseeritud. „Raamatukogu“ tarkvara (ingl. library software) peaks kasutama, et seda saaks kasutada auditites ja et hallata programmiversiooni numbreid, loomise kuupäeva ja koopiaid eelmistest versioonidest
- audiitor peaks saama nimekirja autoriseeritud tarkvarast ja kui võimalik automaatse vahendi, millega skaneerida sisse kõik seadmed, k.a. serverid ja lauaarvutid. Selline tarkvara pakub olulisi detaile, nagu nt:
    - raudvara tüüp ja mudeli nr
    - tarkvara elemendid
    - tarija tarkvara

IT audiitor peab saama ülevaate tarkvara omandamise kontrollidest, et kontrollida, et kogu tarkvara on salvestatud IT varade haldamise süsteemi.

Administreerimine

Juurdepääsu reeglid peaksid selgelt määrama ära vastutused, rollid ja protseduurid töötajate staatuse muutustes, nagu nt muutused ametikohal ja ülesannetes. On väga oluline saavutada

protseduurid haldamaks muutusi informatsiooni haldajate, kasutajate, super-kasutajate, juhendajate või iga isiku/osakonna vastutuses õiguste andmises/ära võtmises või õiguste/privileegide muutmises.

Kasutajakontrollid

Kasutajate aktiivsuse kontrollimiseks ja jälgimiseks tuleb sisse viia kontrollid, nt kasutaja blokeerimine peale mitmeid ebaõnnestunuid katseid sisse logida ja mitteaktiivsete kasutajate blokeerimine või kustutamine.

Preventiivsed kontrollid

Preventiivsed kontrollid koosnevad:

- süsteemile juurdepääs peaks olema kaitstud tugeva salasõnaga (reeglid salasõna pikkuse ja keerukuse kohta, muutmise kohta, jagamise kohta jne)
- enne õiguste andmist süsteemile juurde pääsemiseks peaks saama loa vastavalt isikult
- vastavalt regulatsioonidele tuleb kõiki kasutajad teavitada ning neil tuleb allkirjastada juurdepääsureeglid
- andmete õigeotstarbeliseks kasutamiseks tuleks anda samuti allkiri
- juurdepääsukontrolli vahendid, nagu auditi vahendid, tulemüür ja ID-d, peavad eksisteerima
- vahendite kasutamise reeglid, k.a. töötajate trahvid ebaotstarbeka (e-kiri, Internet) kasutamise eest peaks eksisteerima
- kolmanda osapoole juurdepääsu nõuded (SLA-d või lepingud)
- sildistamise protseduurid, sõltuvalt riski hindamisest
- piirangud ajutistele töötajatele
- vaikimise juurdepääs igale poole elimineerida

Juurdepääsu administreerimise protseduur

Sõltuvalt kohalikest protseduuridest, platvormidest jne võib see ülesanne varieeruda, kuid ta peab sisaldama:

- formaalselt dokumenteeritud juurdepääsu nõuded kõigile toimingutele (kustutamine, lisamine, jne) peavad olema omanikult saadud
- kui administreerimise protsess on manuaalne (mingi vorm või e-kiri) peab administraator, kes saab antud nõude kontrollima, et nõue on õige
- iga kasutaja administreerimisele peaks olema defineeritud ja kokku lepitud (nt SLA).
- protseduur, kuidas kasutajani toimetada parooli, peaks olema defineeritud
- kontroll peaks olema nende salasõnade üle, mida omanik ei ole mingi aja jooksul kätte saanud

Informatsiooni turvalisuse administreerimise kontrollid

Tegevused koosnevad:

- kõik tegevused peavad kajastuma auditi logis
- kõik kasutaja administreerimise funktsioonid peavad olema eraldatud muudest tegevustest (nt süsteemi administreerimine, tehingud jms), vastasel juhul võivad kohustuste eraldumise puudusel tekkida huvide konfliktid
- üks sõltumatu osapool peaks antud tegevuse eest vastutama 24 h või juurutama kontrolli, et ainult teatud tegevusi töödeldakse
- kõik privilegeeritud kasutajaid (nt administraatorid) peab jälgima ning õigustamiseks tihedam kontroll

IT juhtkomitee

IT juhtkomitee (või muu sarnane) koostatud juhtidest, äri ja IT juhtkondadest peab olema loodud:

- peab määrama prioriteedid IT investeeringute joondamiseks ettevõtte äristrateegiaga.
- jälgima teenuse taset ja teenuse arendamist

Tegevusprotseduurid ja ülesanded

Standardprotseduurid IT tegevustele peavad olema defineeritud, rakendatud ja hallatud ning personal peab olema teadlik neile määratud ülesannetest. Tegevusprotseduurid peavad hõlmama vahetuste vahetust, et järjepidev tegevus ei katkeks. Samuti peaksid olema defineeritud protsessid IT infrastruktuuri ja sellega seotud tegevustele.

IT organisatsiooni ja strateegiliste planeerimisprotsesside ülevaade

IS audiitor peab hindama kas IT organisatsioonil on piisavalt oskusi ja töötajaid koos rollide ja vastustega, mis on joondatud äriga:

- juhtkond kinnitab, et IT tegevused on sõltumatud
- IT planeerimise/juhtivkomitee osalus ja funktsioonid on defineeritud ning vastutused on paigas
- IT juhtivkomitee põhikiri ühendab komitee eesmärgid ettevõtte eesmärgid ja pika- ning lühiajalised plaanid ning IT eesmärgid ja pika- ja lühiajalised eesmärgid
- IT juht raporteerib ettevõtte äritegevust vastavalt ja jälgib trende ettevõtte tegevusalal ning selle turul
- juhtkond kindlustab, et rollid ja vastutused on täidetud
- IT organisatsioonis eksisteerib kvaliteedi tagamise funktsioon
- kõikide peamiste andmete ja süsteemide vastutused on kaetud reeglite ja protseduuridega
- juhendamise reeglid ja protseduurid eksisteerivad kindlustamaks rollide ja vastutuste õppimist ning kogu personalil on vastavad õigused ja vahendid olemas, et oma tööd teha efektiivselt
- eksisteerib kohustuste eraldus süsteemi arendamise ja haldamise, süsteemi arendamise ja opereerimise, süsteemi arendamise/haldamise ja informatsiooni turvamise, tegutsemise ja andmete kontrolli, tegutsemiste ja kasutajate ning tegutsemise ja informatsiooni turvamise vahel
- IT koosseis ja kompetentsus on hallatud, et kindlustada selle võimet pakkuda efektiivseid IT lahendusi
- võtmeprotsesside jaoks eksisteerivad sobivad rollid ja vastutused, k.a. süsteemiarendamise elutsükli tegevused, informatsiooni turvalisus

- sobivad KPI[16] ja/või CSF[17] on kasutusel, et mõõta IT funktsioonide tulemusi eesmärkide saavutamiseks
- analüütikute ja teiste lepinguliste töötajate tegevuste jaoks on paigas IT reeglid ja protseduurid, mis kindlustavad ettevõtte varade puutumatuse
- protseduurid on rakendatavad lepingulistele IT teenustele adekvaatsuse ja vastavuses ettevõtte omandamisreeglitega
- garanteerimaks IT funktsioonidest tulenevate teenuste toimimist vastavalt õigustatud hinnale ja ettevõtte kuludele on kasutusel vastavad reeglid ja protseduurid
- ettevõttesse värbamise ja vabastamise protseduurid ning taustauuringu kontrollid

IT strateegilise planeerimise protsessi hinnates tuleb audiitoril hinnata kas:

- on olemas IT missiooni ja visiooni selge definitsioon
- strateegilise IT planeerimise metoodika on kasutusel
- metoodika korreleerub ettevõtte eesmärkidega ja IT ärieesmärkidega
- seda protseduuri uuendatakse perioodiliselt (vähemasti kord aastas)
- see plaan kajastab peamised IS initsiatiivid ja vajatavad vahendid
- sellesse protsessi hõlmatud isikute arv on sobiv. (ISACA 2008b)

[16] KPI – Key Performance Indicator
[17] CSF - Critical Success Factors

BS 7799

Turvareeglite haldus

- võta kasutusele üldised informatsiooni turvareeglid
  - arenda informatsiooni turvareeglite kogu
  - vaata üle oma informatsiooni turvareeglid

Korporatiivne turvareeglite haldus

- raja sisemine turvaorganisatsioon
  - pühendu aktiivselt informatsiooni turvalisusele
  - koordineeri informatsiooni turvalisuse rakendamist
  - jaga ära informatsiooni turvalisuse vastutused
  - loo uued vahendid autoriseerimisprotsessile
  - võta kasutusele konfidentsiaalsuslepingud informatsiooni kaitsmiseks
  - halda suhteid teiste organisatsioonidega
  - halda suhteid vastavate huvigruppidega
  - vii läbi sõltumatuid vaateid informatsioonisüsteemidest
- kontrolli väliste osapoolte poolt sinu informatsiooni kasutamist
  - identifitseeri riskid väliste osapoolte kasutamisest
  - viita turvalisusele enne kui kliendid saavad juurdepääsu
  - viita turvalisusele kasutades kolmanda osapoole lepinguid

Organisatsiooni varade haldus

- loo vastutused oma organisatsiooni varadele
  - koosta inventuur ettevõtte varadele
  - vali varadele ja informatsioonile omanikud
  - vii sisse informatsiooni ja varade kasutusreeglid
- kasuta informatsiooni klassifitseerimise süsteemi
  - arenda välja informatsiooni klassifitseerimise reeglid

- kasuta informatsiooni käsitlemise ja sildistamise protseduure

Inimressursi turvahaldus

- rõhuta turvalisusele enne positsioonidele paigutamist
  - defineeri turvarollid ja vastutused
  - kontrolli üle uute töötajate taust
  - kasuta lepinguid oma ettevõtte informatsiooni kaitsmiseks
- rõhuta turvalisusele töötamise käigus
  - eelda ülemustelt turvalisuse hindamist
  - vii läbi informatsiooni turvalisuse alaseid koolitusi
  - vii sisse turvalisuse lõhede jaoks distsiplinaarsed protsessid
- rõhuta turvalisuse töölt lahkumisel
  - töölt lahkumisel või ümber paigutamisel anna vastutus üle teistele
  - kindlusta, et töölt lahkumisel varad tagastatakse
  - töölt lahkumisel eemalda juurdepääsuõigused informatsioonile

Füüsiline ja keskkondlik turvahaldus

- kasuta valduste turvamiseks turvaalasid
  - kasuta füüsilisi turvapiiranguid alade kaitseks
  - kasuta füüsilisi turvakontrolle kaitsmaks turvaalasid
  - turva oma organisatsiooni kontorid, ruumid ja vahendid
  - kaitse oma vahendeid looduslike ja inimohtude eest
  - kasuta tööjuhendeid oma turvaalade kaitseks
  - eralda ja kontrolli avalikke sissepääsupunkte
- kaitse oma varustust
  - kasuta varustuse asumise ja kaitsestrateegiaid
  - tee kindlaks, et toetavad abivahendid on usaldusväärsed
  - kaitse telekommunikatsiooni kaableid
  - halda organisatsiooni varustust
  - kaitse organisatsiooni väljaspool asuvat varustust
  - kontrolli varustuse kasutamist väljaspool

Kommunikatsiooni ja tegevuste juhtimine

- vii sisse protseduurid ja vastutused
  - dokumenteeri tegevusprotseduurid
  - kontrolli muudatusi erinevates vahendites ja süsteemides
  - eralda kohutused ja vastutused
  - lahuta arendamine ja tegevused
- kontrolli kolmanda osapoole teenuste pakkumist
  - halda kolmanda osapoole teenuse lepinguid
  - jälgi kolmanda osapoole teenuste pakkumist
- teosta tulevikuks süsteemiplaneerimise tegevused
  - jälgi kasutamist ja teosta tootlikkuse planeerimist
  - kasuta vastuvõtukriteeriumi oma süsteemide testimisel
- kaitse pahatahtliku ja „mobile“ koodi vastu
  - vii sisse kontrollid pahatahtliku koodi käsitsemiseks
  - kontrolli „mobile“ koodi kasutamist
- vii sisse varundus (ingl. k. backup) protseduurid
  - tee koopiaid oma informatsioonist ja tarkvarast
- kaitse arvutivõrke
  - rakenda arvutivõrkude turvakontrollid
  - kontrolli võrguteenuse pakkujaid
- kontrolli meedia kasutamist
  - halda ettevõtte eemaldatavat meediat
  - halda oma ettevõtte kasutuses olevat meediat
  - kontrolli informatsiooni käsitlemist ja salvestamist
  - kaitse süsteemi dokumentatsiooni
- kaitse informatsiooni vahetamist
  - vii sisse informatsiooni vahetamise reeglid ja protseduurid
  - vii sisse informatsiooni ja tarkvara vahetamise lepingud
  - turva füüsilise meedia transportimist
  - kaitse elektroonilisi teateid ja teadete vahetamist
  - kaitse vastastikku seoses olevaid infosüsteeme

- kaitse elektroonilise äri teenuseid
    - kaitse e-äriga seotud informatsiooni
    - kaitse on-line tehingute informatsiooni
    - kaitse avalikes süsteemides kasutatavat informatsiooni
- jälgi infotöötlemisvahendeid
    - vii sisse ja halda auditi logisid
    - jälgi infotöötlemisvahendeid
    - kaitse sisselogimisvahendeid ja logimise informatsiooni
    - logi süsteemiadministraatori ja operaatori tegevusi
    - logi informatsiooni töötlemise ja kommunikatsiooni vead
    - sünkroniseeri süsteemi kellad

Informatsiooni juurdepääsukontrollide haldamine

- kontrolli informatsioonile juurdepääsetavust
    - loo reeglid informatsioonile juurdepääsuks
- halda kasutajate juurdepääsuõigusi
    - vii sisse kasutaja juurdepääsukontrolli protseduurid
    - kontrolli süsteemihaldus õigusi
    - vii sisse salasõnade haldamise protsess
    - jälgi kasutajate juurdepääsuõigusi
- võta kasutusele head juurdepääsu praktikad
    - eelda kasutajatelt oma salasõna kaitsmist
    - eelda kasutajatelt oma varustuse kaitsmist
    - vii sisse korras laua ja korras ekraani põhimõtted
- kontrolli internetiteenuste ligipääsetavust
    - formuleeri reeglid interneti kasutamiseks
    - kaugühenduse kasutamisel kasuta autentimist
    - kasuta automaatseid varustuse identifitseerimise meetodeid
    - kontrolli juurdepääsu diagnostilistele ja konfiguratsiooni portidele
    - kasuta segregatsioonimeetodit oma arvutivõrgu kaitsmiseks
    - piira ühendust jagatud võrkudele
    - rakenda võrgusuunamisprotokollid

- kontrolli juurdepääsu operatsioonisüsteemidele
  - vii sisse turvalise sisselogimise protseduurid
  - identifitseeri ja autendi kõik kasutajad
  - vii sisse salasõna haldamise süsteem
  - kontrolli kõikide süsteemivahendite kasutamist
  - kasuta sessiooni aegumist, et kaitsta informatsiooni
  - piira ühenduskorrad kõrge riskiga valdkondades
- kontrolli juurdepääsu rakendustele ja informatsioonile
  - piira juurdepääsu töötajate ja abipersonali poolt
  - eralda tundlikud rakendussüsteemid
- kaitse mobiili ja üle võrgu töötamise vahendeid
  - kaitse mobiilseid töövahendeid

Infosüsteemide turvahaldus

- tuvasta infosüsteemi turvanõuded
  - tuvasta turvakontrollid ja nõuded
- veendu, et rakendused töötlevad informatsiooni korrektselt
  - valideeri andmesisestus oma rakendustesse
  - töötlemise kontrollimiseks kasuta valideerimist
  - kaitse teadete täielikkust ja autentsust
  - valideeri rakendustest väljuvad andmed
- kasuta krüptokontrolle informatsiooni kaitsmiseks
  - koosta reeglid krüptograafilise kontrolli kasutamiseks
  - rakenda turvavõtme haldussüsteem
- kaitse ja kontrolli ettevõtte süsteemifaile
  - kontrolli tarkvara installeerimist
  - kontrolli süsteemi andmete kasutamist testimiseks
  - kontrolli juurdepääsu süsteemi koodile
- kontrolli arendus ja toetusprotsesse
  - vii sisse formaalsed muutuste kontrollimise protsessid
  - jälgi rakendusi peale operatsioonisüsteemi muudatusi
  - piira muudatused tarkvarapakettidele

    - väldi informatsiooni lekkimise võimalusi
    - kontrolli sisseostetud tarkvara arendamist
- vii sisse tehnika haavatavuse haldus
    - kontrolli tehniliste süsteemide haavatavust

Informatsiooni turvajuhtumite haldamine

- raporteeri informatsiooni turvalisust puudutavad sündmused ja nõrkused
    - raporteeri turvalisust puudutavad sündmused nii kiiresti kui võimalik
    - raporteeri süsteemi ja teenuste turvanõrkused
- halda informatsiooni turvalisust puuduvaid sündmusi ja arenguid
    - rakenda juhtumite vastutusvaldkonnad ja protseduurid
    - õpi oma informatsiooni turvalisusega seotud intsidentidest
    - korja tõendeid oma tegevuste toetamiseks

Äri järjepidevuse haldus

- kasuta oma informatsiooni kaitsmiseks pidevushaldussüsteeme
    - rakenda informatsioonile ärijärjepidevuse protsess
    - identifitseeri need sündmused, mis võivad segada äritegevust
    - arenda ja rakenda tegevused ärijärjepidevuse plaanid
    - rakenda raamistik äri järjepidevuse planeerimiseks
    - testi ja uuenda äri järjepidevuse plaane

Vastavushaldus (ingl. k. compliance)

- vasta seaduse nõuetele
    - uuri välja kõik vastavad seaduslikud nõuded
    - tunnusta intellektuaalset omandit
    - kaitse organisatsiooni kirjeid
    - kaitse personaalse informatsiooni turvalisust
    - väldi andmete töötlemise väärkasutust
    - kontrolli krüptograafiliste kontrollide kasutamist

- vii läbi ülevaateid turvavastavustest
    - jälgi vastavust turvareeglitele ja standarditele
    - jälgi vastavust tehnilisele turvalisusele
- vii läbi infosüsteemi auditeid
    - kontrolli infosüsteemi auditit
    - kaitse infosüsteemi auditi vahendeid

Kasutajal valed õigused infosüsteemile juurdepääsul,

- Konfidentsiaalse informatsiooni mittevolitatud avalikustamine
- IT rakenduste mitteusaldusväärne või kallis rakendamine,
- Ebasobiv IT süsteemide ja ärieesmärkide ühildamine
- Ebapiisavad süsteemid informatsiooni töötlemise ja tehingute jälgimiseks,
- Ebaefektiivsed treeningprogrammid töötajatele ja süsteemikasutajatele,
- Ebapiisavus nõuetekohase IT tarnija valimisel,
- Eba-adekvaatne kohustuste jagamine,
- Ebapiisavad või ebaadekvaatsed auditi jäljed,
- Lõpp-kasutaja süsteemide standardite ja kontrollide puudulikkus,
- Ebaefektiivne või ebaadekvaatne ärijärjepidevuse plaan
- Süsteemi katkestusest põhjustatud finantskaotus ja reputatsiooni kaotus. (Praxiom 2008)

GAIT

Allpool olevad soovitused näitavad samme ülalt-alla ja riskipõhisel protsessil võtme ITGC[18]-de määramiseks SOX[19] 404-le kasutades metoodikat:

- Identifitseerida, mõista ja hinnata ettevõtte taseme kontrollide efektiivsust
- Identifitseerida tähelepanuväärsed kontod ja asukohad ja vastavad väited
- Identifitseerida tähelepanuväärsed äriprotsessid ja peamised tehingute klassid
- Identifitseerida kohad, kust võivad protsessi jooksul tekkida vead või pettused
- Identifitseerida kontrollid, et testida mis väldivad või avastavad vigu või pettusi ajas
- Identifitseerida/valideerida kriitilised IT funktsionaalsused
- Identifitseerida rakendused, kus tuleb ITGC-d testida
- Identifitseerida ITGC protsessiriskid ja vastavad kontrolleesmärgid
- Identifitseerida ITGC testimaks kas see vastab kontrolleesmärkidele
- Viia läbi inimeste ülevaatus

Rakenduste kihi IT üldiste kontrollide protsessid

Muudatuste haldus - Hõlmab endas erinevaid riskivaldkondi:

- uus või muudetud funktsionaalsus on õigesti ehitatud ja kinnitatud
- muudatus on korralikult testitud kinnitamaks, et ta töötab korrektselt
- kasutaja aktsepteerib muudatuse, kinnitades, et see töötab nagu vaja
- autoriseerimata muudatusi hoitakse ära

Tegevused - Tegevuste võimalikud riskikohad:

- rakenduste töö korrapärasuse kinnitamiseks kasutatakse kontrolle
- vigade ja erandite töötlemisel on ajapiirang
- varukoopiad kriitilistest rakendustest ja andmefailidest
- töötlemise füüsiline turvalisus

[18] Information Technology General Controls e. IT üldised kontrollid
[19] Sarbanes-Oxley Act

Turvalisus - Turvalisusega kaasneb risk andmetele ja rakenduskoodile. Rakenduste turvalisus, juurdepääsuõiguste andmine ja ära võtmine ning rakenduskoodile juurdepääsu andmine on tüüpilised tegevused selles üldiste kontrollide osas.

Kokkuvõttes, mida vähem riske leitakse andmebaasi või rakenduste kihis, seda väiksem on tõenäosus leida neid madalamatelt kihtidelt.

Andmebaasikihi IT üldiste kontrollide protsessid ja tüüpilised riskid

Muudatuste haldus - Muudatuste haldus selles kihis võtab arvesse riske, mis on seotud mitte-andmete elementidega, nt skeemidega
Tegevused - Tegevuste riskid siin kihis on tihtipeale avastatud samade kontrollide poolt, mis olid rakenduskihis.
Turvalisus - See on koht, kus autoriseerimata juurdepääs andmetele on otse suunatud.
Defektid operatsioonisüsteemi tasemel põhjustavad väga väikese tõenäosusega materiaalseid vigu, kuna nende mõju on tihtipeale kohe märgatav – töötluse seiskumine või töötlemisvead.

Operatsioonisüsteemi kihi IT üldiste kontrollide protsessid ja tüüpilised vead

Muudatuste haldus – Muudatuste haldus selles kihis viitab muudatustele operatsioonisüsteemi keskkonnas.
Tegevused – Selle taseme riskid on tuvastatavad nende samade kontrollide poolt, mis rakenduskihiski.
Turvalisus – operatsioonisüsteemi kihi riskid on harva edasi ulatuvad „juure“ tasemele ja teistesse privilegeeritud juurdepääsudesse. (IIA 2006)

3. Metoodikate võrdlus

Vaatluse alla võetud metoodikad on oma olemustelt erinevad, kuid nendes kõigis on ühiseid jooni turvalisuse küsimustes.
IT juhi üheks eesmärgiks on infosüsteemi talitluspidevuse, informatsiooni õigsuse ja andmeturbe tulemuslik täitmine. Selleteemalisi soovitusi leiab kõigist kolmest vaatluse all olnud metoodikast, sest need teemad kõik viitavad ühele suurele valdkonnale – turvalisusele. Kõige spetsiifilisemalt on see osa lahti kirjutatud BS 7799-s, mis selle otstarbega on ju ettevõtetele turvastandardiks loodud. Aga samas on peamised audiitorile huvipakkuvad teemad CobiT's välja toodud. Ning on iga ettevõtte enda teha, millist meetodit ta oma IT turvalisuse haldamiseks kasutab. GAIT rõhutab ettevõttes kasutusel olevatele erinevatele kontrollidele ja nende otstarbekale kasutamisele. Kui kõik kontrollid on hallatud, siis järelikult võib väita, et ka turvalisusega ei peaks probleeme olema, kuna kontrollide efektiivse töö eesmärgiks on just nimelt välistada kõik kõrvalekalded.

IT juhtimise vaatenurgast ettevõtte äristrateegia väljatöötamisega seonduvad ülesanded on kõige paremini ära kirjeldatud CobiT'is, mis on suuresti välja töötatud just selle eesmärgi täitmise kontrollimiseks. CobiT annab selleks selgeks juhised. Kuid kuna IT vahendite parema rakendamise abil ettevõtte efektiivsuse suurendamise võimalused hõlmavad endas ka turvalisusega ja efektiivsete kontrollidega seonduvaid haldamistöid, siis täidavad tegelikult mingil määral ka teised kaks metoodikat selle eesmärgi.

IT strateegilise juhtimise (IT turul toimuvate muudatuste ja trendide kohta toimuva jälgimine, IT strateegia väljatöötamine, IT eelarve koostamine jne) kohta annab taaskord kõige täpsemaid näpunäiteid CobiT – IT valitsemine, lepingud väliste osapooltega, erinevad administreerimistegevused ning muidugi tihe koostöö ettevõtte juhtkonnaga.

IT arendustegevusega (IT arendustegevuse planeerimine, IT valdkonna projektijuhtimise korraldamine, IT rakenduste koolituste korraldamine, IT infrastruktuuri planeerimine jne) seonduvast räägib kõige laiemalt CobiT. Kuid üsna palju soovitusi sellel teemal saab ka BS7799-lt, eriti just infrastruktuuri vallas – nt on kirjeldatud organisatsiooni varade haldus, erinevad turvahaldused (inimeste, keskkonna, infosüsteemide jms), kommunikatsiooni ja tegevuste juhtimine, juurdepääsukontrollid, ärijärjepidevuse jälgimine, vastavushaldus.

GAIT on tihedalt seotud äriprotsessidega ja nende korrapärase toimimise kontrollimise ja jälgimisega.

IT kasutamise ja ülalpidamisega (arvuti- ja kommunikatsioonivõrgu administreerimine ja andmeturbe korraldamine, kasutajatoe olemasolu ja toimimine, riist- ja tarkvara ning IT tarvikute ostmine/haldamine, IT ressursside haldus, tarkvara litsentside haldamine) seonduvast – taaskord, oma sõna võtavad sellele teemal kõik metoodikad. Eriti BS 7799 ja CobiT. Tooks siinkohal kohe välja BS 7799 mõned peamised punktid, nagu nt vahendite ja varade organiseerimine, varade kontroll ja klassifitseerimine, kommunikatsiooni ja tegevuste haldus, süsteemi arendamine ja haldus ning äri järjepidevuse haldus.

4. IT metoodikatest tulenevad soovitused IT juhtidele

Toetudes kutsestandardis kirjeldatud IT juhi eesmärkidele, toon välja järgmised punktid:

Ettevõtte äristrateegia väljatöötamisega seonduvad ülesanded

- ettevõtte arengukavade väljatöötamisel osalemine
  - IS funktsioonid on joondatud ettevõtte missiooni, visiooni, väärtuste, eesmärkide ja strateegiatega
  - IS funktsioonidel on selge väljund, mida eeldab äripool
  - IS juhtimise terviklikkus, IS juhtimise kogemus ja teadmised
  - IS ressursside efektiivsus ning nende talitlusprotsessid
  - kooskõlastatus seaduste, keskkonna ja informatsiooni kvaliteedi ning hooldus- ja turvanõuetega
  - IT missiooni sõnastamine ja kokkulepitud eesmärgid ning eesmärgid IT tegevustele
  - vaadelda ja hinnata riske, mis võivad ebasoodsalt mõjutada IS keskkonda
- IT vahendite parema rakendamise abil ettevõtte efektiivsuse suurendamise võimaluste selgitamine koostöös teiste juhtidega ja ettevõtte klientide ning partneritega
  - kasutuses rahvusvahelised sertifikaadid või raamistikud ning ISO nõuded
  - lepingud väliste teenusepakkujatega
  - identifitseerida, mõista ja hinnata ettevõtte taseme-kontrollide efektiivsust

IT strateegilise juhtimisega seonduvad ülesanded

- IT turul toimuvate muutuste ja trendide kohta info hankimine ja analüüsimine
  - IT juht raporteerib ettevõtte äritegevust ja jälgib trende ettevõtte tegevusalal ning selle turul
  - analüüsida olemasolevaid ja tekkivaid tehnoloogiaid ning plaanida milline tehnoloogiline suund on sobiv realiseerimaks IT strateegiat ja ärisüsteemide arhitektuuri

- rajada protseduur jälgimaks äri sektori/tööstuse, tehnoloogia, infrastruktuuri, õiguslikke ja reguleerivaid keskkonna trende
- kirjeldada ja rakendada protseduur kindlustamaks õigeaegset teatamist kohalikest ja rahvusvahelistest õiguslikest, lepingulistest, poliitika ja regulatiivsete nõuete muutumisest informatsioonile, infoteenuse toimetamisele, k.a. kolmanda osapoole teenustele. Võtta arvesse seadusi ja regulatsioone elektroonilisele ärile, andmevoo, privaatsuse, sisekontrollide, finantsraporteerimise, valdkonna-spetsiifiliste regulatsioonide, intellektuaalse omandi ja autoriõiguse ning tervise ja ohutuse osas
- jälgida ja optimiseerida IT poliitikaid, standardeid ja protseduure kindlustamaks, et seadusandlikud ja regulatiivsed nõuded on täidetud

- IT strateegia väljatöötamine ja sõnastamine lähtuvalt IT võimalustest ja ettevõtte äristrateegiast tulenevatest vajadustest ning võimalustest
  - lühi- ja pikaajaline strateegia ning plaanid IT ja süsteemide plaanide toetamiseks
  - IT strateegia, arendusplaanide ja jälgimise progress vastavalt nendele plaanidele
  - IT strateegiline plaan peaks olema piisavalt detailne, et selle põhjal luua ka taktikaline plaan, mis kirjeldab lahti nõutavad IT initsiatiivid, vahendite nõuded ning kuidas vahendite kasutamist ja kasumisaamise saavutusi jälgida ja hallata
  - IT strateegia ja plaanide kontrolli muutmine
  - IT missiooni sõnastamine ja kokkulepitud eesmärgid ning eesmärgid IT tegevustele
  - strateegilise IT planeerimise metoodika on kasutusel ning metoodika korreleerub ettevõtte eesmärkidega ja IT ärieesmärkidega
- IT eelarve koostamine ja täitmise jälgimine
  - IT strateegiline plaan peaks kajastama investeeringute/haldamise eelarvet, rahastamisvahendeid, vahendite strateegiat, omandamise strateegiat ning õiguslikke ja regulatiivseid nõudmisi
  - garanteerimaks IT funktsioonidest tulenevate teenuste toimimist vastavalt õigustatud hinnale ja ettevõtte kuludele on kasutusel vastavad reeglid ja protseduurid

- hoida kinni ja jaotada tegelikud kulud vastavalt kirjeldatud kulude mudelile. Muutusi prognooside ja tegelike tulemuste vahel tuleb analüüsida ja raporteerida ettevõtte finantsmõõdikute süsteemi

IT arendustegevusega seonduvad ülesanded

- IT-arendustegevuse planeerimine
  - vastavate osanikega koos luua strateegiline plaan, mis kirjeldab, kuidas IT panustab ettevõtte eesmärkide täitmisesse ja nendega seotud kuludesse ning riskidesse.
  - ärijärjepidevuse haldus
  - identifitseerida kohad, kust võivad protsesside jooksul tekkida vead või pettused
  - kasutada küpsusmudeleid vajalike muudatuste hindamiseks
  - kirjeldada ja võtta kasutusele protseduurid, mis kindlustavad kõigi elektroonselt salvestatud andmete (nt andmebaasid, andmelaod ja andmearhiivid) terviklikkuse ja järjepidevuse
  - luua ja hallata tehnoloogilise infrastruktuuri plaan, mis vastab IT strateegilisele ja taktikalisele plaanile
- IT valdkonna projektijuhtimise korraldamine
  - projektijuhtimise kontrollid rakendatud
  - projektijuhtimise vahendid kasutuses
  - muudatuste halduse metoodikad on kasutusel suurtes projektides, mis kaasavad suuri muutusi ettevõtetes
  - hinnata, kas protsessi hõlmatud inimestel on piisavalt oskusi ja teadmisi ning kogumusi oma rollide täitmiseks
- projektülesande püstitamise juhtimine koostöös vastava valdkonna ärijuhiga
  - pidada meeles IT ja äripoole erinevaid teadmisi ja arusaamu
  - IT ja äriinimeste integreeritus erinevates projekti faasides
  - nõuded programmimuudatusteks, süsteemi muudatusteks ja haldamiseks (k.a. süsteemi tarkvara muudatused) on standardiseeritud, dokumenteeritud ning vastavad üldistele muudatushaldus protsessidele
  - IT juhtkond kindlustab, et kasutajad on kaasatud rakenduste disainimisse, pakett-tarkvara valimisse ja testimisse, et kindlustada usaldusväärne keskkond
- projekteerimise ja rakenduse valiku juhtimine

  - projektijuhtimise metoodikate kasutamine
  - testimise strateegia on välja arendatud ja kasutusel kõigi olulisemate rakenduste muutustega, kuhu on kaasatud süsteemi-, integratsiooni-, ja kasutajataseme testid kindlustamaks, et süsteemid töötavad nagu ette nähtud
  - liideseid teiste süsteemidega testitakse, veendumaks, et andmete ülekanne on täielik, vigadeta ja paikapidav
- uute IT-rakenduste koolituse organiseerimine
  - koolitada välja kõik asjasse puutuvad kasutajad vastavalt treeningplaanile ja materjalidele, osana igast infosüsteemi arendamise, rakendamise või modifikatsiooni projektist
  - erinevad poliitikad ja reeglistikud peavad olema viidud kasutajani ning vajadusel organiseeritud ka vastavasisulised koolitused (olenevalt materjali raskusastmest)
- IT infrastruktuuri planeerimine
  - koostada plaan tehnoloogilise infrastruktuuri omandamiseks, rakendamiseks ja haldamiseks, mis vastaks ettevõtte funktsionaalsetele ja tehnilistele nõudmistele ning oleks kooskõlas ettevõtte üldise tehnoloogilise suunaga
  - viia sisse sisekontrolli, turvalisuse ja auditeerimise mõõdikud tarkvara ja riistvara konfigureerimise, rakendamise ja haldamise ajaks, et kaitsta vahendeid ning tagada kättesaadavus ja täielikkus
  - eksisteerivad dokumenteeritud protseduurid, mida jälgitakse kindlustamaks, et infrastruktuuri süsteemid, k.a. võrguvahendid ja tarkvara, töötavad vastavalt finantsrakenduste nõudmistele, mida nad peavad toetama
  - kirjeldatud organisatsiooni varade haldus, erinevad turvahaldused (inimeste, keskkonna, infosüsteemide jms), kommunikatsiooni ja tegevuste juhtimine, juurdepääsukontrollid, ärijärjepidevuse jälgimine, vastavushaldus
  - IT juhtkond kindlustab, et tarkvara rakendamine ja seadistamine ei ohusta andmeid ega süsteemiga seotud programme
  - rakenda kokkulepped kindlustamaks, et äripoolelt oodatavad dokumendid on saadud, kõik äripoolelt saadud andmed on töödeldud, äripoolelt nõutav väljund valmistatud ja kohale toimetatud ning ümbertöötlemise vajadust toetatakse
  - valmistada ja rakendada protseduurid andmete hoidmiseks ja arhiveerimiseks, nii et andmed oleksid kättesaadavad ja kasutatavad
  - valmistada ja rakendada protseduurid varunduse- ja taastamissüsteemidele

- järjepidev seire IT kontrollikeskkonnale ja juhtraamistikule. Hindamisel kasutada parimaid praktikaid ja võrdlusanalüüsi, et neid arendada. Seirata ja raporteerida sisemiste kontrollide efektiivsust IT-s, nt vastavust poliitikatele ja standarditele, informatsiooni turvalisus, muudatuste kontrollid ja kontrollid teenustaseme lepingutes
- sisseostetud teenuste haldamine, nende staatuse hindamine
- kirjeldada raamistik, mis toetab formaalset teenustaseme juhtimisprotsesse kliendi ja teenuse pakkuja vahel. Raamistik hõlmab protsesse teenuste nõuete loomiseks, teenuse definitsioone, teenustaseme lepinguid (SLA[20]), ülalhoiu taseme lepinguid (OLA[21]) ning rahastamisvahendeid
- kirjelda ja lepi kokku teenustaseme lepingud kõigile kriitilistele IT teenustele vastavalt kliendi nõudmistele ja IT võimalustele. See hõlmab kliendi kohustusi, teenusetoe nõudmisi, kvantitatiivseid ja kvalitatiivseid mõõdikuid teenuse osas, kui vaja siis rahastamise ja kaubanduslikke kokkuleppeid ning rolle ja vastutusi, k.a ülevaadet SLA-st
- kindlustada, et OLA- s selgitatakse, kuidas teenuseid tehniliselt esitatakse, et toetada SLA-d optimaalselt
- rakendada protsess teenuse pakkumise seireks, kindlustamaks, et tarnija vastab praegustele ärinõuetele ja jätkuvalt täidab lepingus kirjeldatud kokkuleppeid ja teenuse taseme kokkuleppeid ning et pakutu on konkurentsivõimeline alternatiivsete tarnijatega ja antud turuolukorras
- KPI-de raamistik on kasutusel, et hallata teenustaseme lepinguid, nii sisemisi kui väliseid

IT kasutamise ja ülalpidamisega seonduvad ülesanded

- arvuti- ja kommunikatsioonivõrgu administreerimise ja andmeturbe korraldamine
  - informatsiooni turvalisuse poliitika on olemas ning see on kinnitatud vastava taseme tegevjuhtkonna poolt
  - turvastandardite raamistik on arendatud ning toetab turvapoliitika eesmärke
  - hinnata riski tekkimise tõenäosust ja sellest tekkida võivaid ebaregulaarsusi
  - kasutusel detailsed kontrollid e. IS süsteemide ja teenuste rakendamise, üleandmise ja toetamise kontrollid

[20] SLA – Service Level Agreement
[21] OLA – Operating Level Agreement

    - töötajad peaks allkirjastama formaalse lepingu mitte jagama konfidentsiaalset infot
    - infosüsteemi kasutamise rutiinid ja teiste informatsiooni turvalisusega seotud informatsioon peab olema dokumenteeritud, mis peab olema ladustatud vastavalt kohalikele seadustele ja regulatsioonidele
    - kasutusel üldised informatsiooni turvareeglid
    - selged vastutused turvajuhtimises
    - rajatud sisemine turvaorganisatsioon
    - infosüsteemide turvahaldus
- kasutajatoe olemasolu ja toimimise tagamine
    - asutada teenusetoe funktsioon, mis on kasutajaliides IT-ga, et registreerida, edastada, lahendada ja analüüsida kõnesid, raporteeritud juhtumeid, teenuse päringuid ja infovajadusi
    - mõõta lõppkasutaja rahulolu kasutajatoega ja IT teenustega
    - viia sisse süsteem, mis võimaldab jälgida/jälitada kõnesid, juhtumeid, teenusepäringuid ja infovajadusi
    - rakendada protsessid, mis võimaldavad raporteerida ja jagada/kategoriseerida probleeme (nt kategooria, mõju, kiirus ja prioriteet), mis on üks osa intsidendihaldusest
    - standardprotseduurid IT tegevustele peavad olema defineeritud, rakendatud ja hallatud ning personal peab olema teadlik neile määratud ülesannetest. Tegevusprotseduurid peavad hõlmama vahetuste vahetust, et järjepidev tegevus ei katkeks jne
- riist- ja tarkvara ning IT-tarvikute ostusüsteemi korraldamine
    - tarkvara peab olema sildistatud, inventaris ja litsentseeritud. Süsteemihaldus tarkvara (*ingl. library software*) võiks kasutada, et seda saaks kasutada auditites ja et hallata programmiversiooni numbreid, loomise kuupäeva ja koopiaid eelmistest versioonidest
- IT ressursside haldus
    - kirjeldada, rakendada ja hallata standardprotseduure IT ülalhoiule (*ingl. k. operations*) ning kindlustada, et ülalhoiu töötajad on teadlikud kõigist neile määratud ülesannetest. Tegevusprotseduurid peaksid hõlmama vahetuste üleandmist, et kindlustada järjepidev ülalhoid

- kirjeldada ja juurutada protseduurid IT infrastruktuuri ja sellega seotud tegevuste seireks
- kindlustada, et seireprotsess kasutab meetodit (nt tasakaalus tulemuskaart), mis pakub tabavat, üleüldist vaadet IT tegevustele ja ühtib ettevõtte seiresüsteemiga
- hallata IS juhtimises ettetulevaid pinged, mis võivad põhjustada ebaõige informatsiooni esitamist (nt üle-aja läinud projektid, häkkerirünnakud jne)
- luua vastutused oma organisatsiooni varadele
- informatsiooni juurdepääsukontrolli haldamine
- kirjeldada ja teavitada infosüsteemiga seotud ametikohad ja vastutused kõigile ettevõtte töötajatele, et oleks piisavalt õigusi täita ametikohustusi ja vastutusi
- luua töökirjeldused (mis sisaldavad õigusi ja vastutusi, teadmiste ja oskuste nõudeid vastavalt ametikohale ning need peavad kirjeldama ka vastutusi sisekontrolli jaoks) ja uuendada neid regulaarselt
- hinnata IT töötajate koosseisu regulaarselt või kui äri-, tegevuse- või IT keskkonnas toimuvad suured muudatused, kindlustamaks, et IT funktsioonid on hallatud piisava hulga kompetentsete IT töötajatega
- ohuolukorra juhtudeks peab olemas olema plaan võtmeisikutega kontakteerumiseks
- kindlustada, et äripool saaks aru IT taastusaegadest ja vajalikest tehnoloogilistest investeeringutest, et toetada äri taastumise ja uuesti alustamise vajadusi

- tarkvara litsentseerituse tagamine
  - IT varadega töötavad töötajad võivad kasutada ainult litsentseeritud tarkvara
  - vastavushaldus - vasta seaduse nõuetele
  - kontroll firmasisese tarkvara kopeerimise üle
  - ülevaade tarkvara omandamise kontrollidest - kogu tarkvara on salvestatud IT varade haldamise süsteemi

Meeskonna juhtimisega seonduvad ülesanded

- IT-organisatsiooni juhtimine
  - standardprotseduurid IT tegevustele peavad olema defineeritud, rakendatud ja hallatud ning personal peab olema teadlik neile määratud ülesannetest.

Tegevusprotseduurid peavad hõlmama vahetuste vahetust, et järjepidev tegevus ei katkeks

- IT-organisatsiooni mehitamise juhtimine
  - kindlustada, et IT töötajate tööle värbamine on vastavuses ettevõtte üldise personalipoliitika ja protseduuridega
  - IT koosseis ja kompetentsus on hallatud, et kindlustada selle võimet pakkuda efektiivseid IT lahendusi
  - juhendamise reeglid ja protseduurid eksisteerivad kindlustamaks rollide ja vastutuste õppimist ning kogu personalil on vastavad õigused ja vahendid olemas, et oma tööd teha efektiivselt
  - personaliga seotud turvalisus - peamine eesmärk on vähendada riski, mis võib tekkida seoses inimlike vigadega, pettustega, varastamisega või ettevõtte varade vale kasutamisega
  - minimiseeri sõltuvust võtmeisikutest läbi teadmiste dokumenteerimise, teadmiste jagamise ning asendajatega
  - tegeleda töö muudatustega, eriti töölt lahkumistega – tuleb organiseerida teadmiste edasiandmine, vastutuste ümbersuunamine ning juurdepääsuõigused tuleb eemaldada, et minimiseerida riske ja funktsioonide järjepidevus oleks kindlustatud
- IT osakonna töötajate motiveerituse tagamine
  - inimesed on oluline vara ning sisekontroll on tihedalt seotud personali motiveerimise ja kompetentsusega
- tööülesannete ja eesmärkide kokkuleppimine
  - juhendamise reeglid ja protseduurid eksisteerivad kindlustamaks rollide ja vastutuste õppimist ning kogu personalil on vastavad õigused ja vahendid olemas, et oma tööd teha efektiivselt
  - varadele ja informatsioonile määratud omanikud
  - kasutusel informatsiooni ja varade kasutusreeglid
  - regulaarselt tuleb hinnata töötajate kompetentsust vastavalt nende rollile
  - määratleda tuumik IT kompetentsuse nõuetest ning kindlustada, et neid hallatakse vastavate kvalifikatsiooni- ja sertifitseerimiseprogrammidega
- töötulemuste ja töötajate hindamine
- koostöö korraldamine teiste allüksustega

Kokkuvõte

Magistritöö eesmärkideks olnud erinevate IT auditi metoodikate võrdlus, analüüsist tulenevatest tulemustest järelduste tegemine ja IT juhtidele suunatud IT auditite metoodikatest tulenevad soovitused, said autori arvates täidetud.

Magistritöö esimeses osas anti ülevaade IT auditeerimisega seotud mõistetest, auditi tegevustest ja audiitori tööülesannetest. Selle osa eesmärgiks oli tekitada lugejatele taustinformatsiooni auditi kui sellise kohta – kes, kuidas, mida teeb; millised on auditeerimisel esinevad auditi sammud, mis on nende igaühe eesmärk ning kuidas üldse auditeid läbi viiakse.

Töö teises osas võeti vaatluse alla 3 erinevat ülemaailmselt levinumat standardit. Toodi välja nende põhilisemad omadused, otstarve. Auditeerimisel kasutatakse ülemaailmselt väga erinevaid meetodeid, kuid pigem võib neid jagada just konkreetse valdkonna auditeerimisele vastavalt – olenevalt, millist osa ettevõtte IT-st auditeeritakse ning millise suunitlusega ettevõttega on tegemist. Selliseid metoodikaid, mis kataks ära enamuse kogu IT-st on vähe, kui mitte üldse öelda et ainult CobiT. St. et on ka teisi erinevaid viise auditeerimaks IT-d, kuid need ei ole (veel) väljakujunenud standardid, vaid pigem lihtsalt erinevate audiitorite poolt kirja pandud nende endi parimad praktikad. Seega otsustas autor vaadelda juba eelpool mainitud CobiT'it ning lisaks sellele veel ülemaailmselt tunnustatud IT turvastandardit BS 7799 (e. ISO/IEC 17799) ning finantskontrollidele suunatud GAIT meetodit.

Magistritöö kolmandas osas andis autor ülevaate metoodikate tööpõhimõtetest ning soovitustest, mida need meetodid edastasid ning lisaks tegi autor järeldused kajastatud metoodikatest ja nende vastavusest IT juhtide tööeesmärkidega. See osa kirjeldab lahti erinevad metoodikate peamised sihid ja eesmärgid e. mis on need valdkonnad, millele antud metoodika tähelepanu pöörab. Selle põhjal tegi autor ka kokkuvõtte, kuidas need erinevad auditi metoodikad on kooskõlas IT juhtide tööülesannetega.

Neljandas osas koostas autor vastavalt Infotehnoloogia juhi kutsestandardile ning IT auditi metoodikatest tulevatele soovitustele lühiülevaate nendest teemadest, millele IT juht võiks suuremat tähelepanu pöörata ning mille vastu tunnevad audiitorid auditeerides enim huvi.

Kasutatud kirjandus

(BS 7799.BIZ 2007). BS 7799.BIZ. BS 7700 and ISMS (2007). Loetud marts 2008
URL: www.bs7799.biz/bs7799-and-isms.html

(BSI 2002). BSI, BS 7799 will not hurt a bit (n.d.). Loetud märts 2008
URL: www.bsi-global.com/en/About-BSI/News-Room/BSI-News-Content/Sectors/ICT--Telecommunications/BS-7799-will-not-hurt-a-bit/

(FFIEC (n.d)). FFIEC, IT Handbook InfoBase – Audit (n.d.). Loetud märts 2008
URL: www.ffiec.gov/ffiecinfobase/html_pages/audit_book_frame.htm

(Goodman 1994). Goodman & Lawless, 1994, §8. Loetud jaanuar 2008

(Hinson 2007).Gary Hinson, The State of IT Auditing in 2007 (2007). Loetud märts 2008
URL: www.informaworld.com/smpp/section?content=a781163986&fulltext=713240928

(IIA 2006). The Institute of Internal Auditors, GAIT Methodology (n.d.). Loetud märts 2008
URL: www.theiia.org/guidance/technology/gait/

(IIA 2008a). Institute of Internal Auditors, Frequently Asked Questions (n.d.). Loetud märts 2008
URL: www.theiia.org/theiia/about-the-profession/faqs/

(IIA 2008b). The Institute of Internal Auditors, GAIT2 (n.d.). Loetud märts 2008
URL: www.theiia.org/guidance/technology/gait/gait2/

(IIA 2008c). The Institute of Internal Auditors, GAIT-R (n.d.). Loetud märts 2008
URL: www.theiia.org/guidance/technology/gait/gait-r/

(INTOSAI (n.d.)). Information Technology Audit, General Principles (n.d.). Loetud veebruar 2008
URL: www.intosaiitaudit.org/India_GeneralPrinciples.pdf

(INTOSAI 2007). INTOSAI, Audit & Best Practise Guides (n.d.). Loetud märts 2008
URL: www.intosaiitaudit.org/auditguides.htm

(ISACA 2008a). ISACA. CobiT (2008). loetud veebruar 2008
URL: www.isaca.org/cobit

(ISACA 2008b). ISACA. IS Standards, Guidelines and Procedures for Auditing and Control Professionals (2008). Loetud märts 2008

(ISECT 2008). ISECT, Frequently Avoided Questions about IT Auditing (2008). Loetud veebruar 2008
URL: www.isect.com/html/ca_faq.html

(ISO 27001 2008). ISO 27001 Security, ISO/IEC 27002 (n.d.). Loetud märts 2008
URL: www.iso27001security.com/html/27002.html#Section0

(ISO 17799 2008). ISO 17799 Guide (n.d.). Loetud veebruar 2008
URL: http://iso-17799.safemode.org/

(ITGI 2004). ITGI, IT Control Objectives for Sarbanes-Oxley (2004). Loetud aprill 2008
URL:
www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27526

(ITGI 2005). ITGI. CobiT 4.0 (2005) Loetud märts 2008
URL:
www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27263

(ITGI 2006). ITGI, CobiT Mapping – Overview of International IT Guidance, 2nd Edition (2006). Loetud aprill 2008

(ITGI 2007). ITGI, Cobit 4.1 Excerpt (2007). Loetud veebruar 2008

(ITGI 2008). ITGI. About IT Governance (2008). Loetud märts 2008
URL:
www.itgi.org/template_ITGI.cfm?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657

(Kutsekoda 2006). Kutsekoda, Infotehnoloogia juht V (n.d.). Loetud aprill 2008
URL:
www.kutsekoda.ee/download.aspx/download/1012/Infotehnoloogia%20juht%20V%20'06.doc

(Praxiom 2008). Praxiom Research Group Limited, (2008). ISO/IEC 27002 2005. loetud aprill 2008
URL: www.praxiom.com/iso-17799-2005.htm

(Rittenberg 2005). Larry E. Rittenberg, Sarbanes-Oxley Section 404 Work Looking at the benefits (n.d.). Loetud märts 2008

(SecureIT (n.d.)). SecureIT (n.d.). loetud märts 2008
URL: www.secureit.com/knowledge_center/internal_it_audit.aspx

(Simpson (n.d.)). Barclay Simpson, An Introduction to Computer Auditing (n.d.). Loetud veebruar 2008
URL:
www.barclaysimpson.com/document_uploaded/Introduction%20to%20Computer%20Audit.pdf

(Wikipedia (n.d)). Wikipedia, Information Technology Audit (n.d.). Loetud jaanuar 2008
URL: http://en.wikipedia.org/wiki/Information_technology_audit

RESUME

Recommendations to IT Managers Regarding IT Audit Methodologies

Aim of this thesis was to give some recommendations to IT managers regarding IT audit. Author had three goals: analysis of different IT audit methodologies, make conlusions based on those methodologies and make a list of items about what IT managers should should be aware of regarding IT auditing.

At the first section author gave an overview of auditing – main ideas, audit types, audit steps.

At the second section author gave an overview of most commonly used IT auditing methodologies – CobiT, BS 7799 and GAIT (these three because they are in use as best practises all over world).

At the third section author made some conclusions based on the information given in previous sections and based on material that she has studied. She concluded that CobiT is definitely with the widest area – business/IT strategy, business and IT relationship, IT governance, etc. Security area is a bit weaker but CobiT has all kind of mappings with other standards and one of them is for BS 7799. BS 7799 is an IT security standard and therefore concentrates on security issues. This standard consists of different guidelines and framework of controls which organisations can use to benchmark their own practises and look forward to the establishment of their own Information Security Management System. Third methodology GAIT describes the relationships among risk to financial statements, key controls within business processes, automated controls and other critical IT functionality and key controls within IT general controls. They all concentrate on different issues but they all have at the same time some common areas – they all share best practices on security.

At the forth section author makes some recommendations to IT managers based on IT managers profession standard.

Authors' opinion is that all those goals were achieved.