LAUREA

Organisaation tietojärjestelmän valvonta yleisellä tasolla

Martikainen, Mika

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Organisaation tietojärjestelmän valvonta yleisellä tasolla

Mika Martikainen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Mika Martikainen

Organisaation tietojärjestelmän valvonta yleisellä tasolla

Vuosi 2010 Sivumäärä 46

Tässä opinnäytetyössä keskitytään organisaation tietojärjestelmän valvontaan yleisellä tasolla. Opinnäytetyö käsittelee järjestelmäintegraatiota, joka liittyy kiinteästi järjestelmänvalvontaan. Järjestelmäintegraation toiminnallisuutta kuvataan yleisellä tasolla.

Opinnäytetyössä esitetään neljä keskeistä tutkimuskysymystä, jotka ovat:

- Mitä järjestelmistä yleensä tulisi valvoa?
- Miten valvonta tulisi toteuttaa?
- Mitä työkaluja on tarjolla ja mihin ne soveltuvat?
- Miten organisaation valvontakulttuuria tulisi kehittää ja organisoida)?

Tutkimustulokset on tarkoitus esittää opinnäytetyössä yleisellä tasolla. Tutkimustulokset pyrkivät antamaan yleisen käsityksen valvontaan liittyvistä huomioista. Näiden perusteella lukijalle hahmottuu perusajatus tietojärjestelmän valvonnasta. Opinnäytetyössä käytetään konstruktiivista tutkimusmenetelmää.

Asiasanat: järjestelmä, järjestelmäintegraatio, referenssimallinnus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Business information technology programme
Organization's IT Networks

Mika Martikainen

Organization's system monitoring in a common aspect

Year 2010 Pages 46

The thesis concentrates on systems monitoring, and the perspective to the subject, is on a general level. System integration which relates closely to system monitoring, is defined and presented with its functionalities. These are also presented in a common aspect and frame.

The following specified research questions are in focus in the thesis: what should be monitored in systems, how the monitoring should be carried out (e.g. reactive vs. proactive), what kind of tools are available and in what they are specified for and the development of the organization's monitoring culture (as a reference e.g. ITIL).

Theoretical reference models are often based on best practice thinking. This perspective often solves and simplifies the organization's decision-making, and therefore cuts down expenses. These models are presented in the thesis in an informative aspect. In addition to the one reference model presented in the research question, the thesis will present three other models and one standardization family.

The research results from the questions are presented from a general perspective, as well as the other observations regarding the case. The purpose of the thesis is to categorize systems monitoring, and other closely related fields. According to the presented facts and results, it is possible to draw indicative conclusions of the research question.

Key words: system, system integration, reference model

Sisällys

1 Johdanto

Järjestelmä voidaan yksinkertaistaen käsittää ohjelmistojen, laitteiston ja siihen kytkeytyvien oheislaitteiden yhtälöksi. Ne toimivat yhteistyössä keskenään. Järjestelmää hallinnoidaan käyttöjärjestelmän kautta. Järjestelmäintegraatiosta on kyse, kun järjestelmät yhdistyvät keskenään toimivaksi kokonaisuudeksi.

1960-lukua pidetään järjestelmäintegraation syntynä. Yhdysvaltojen puolustusvoimissa käynnistyi ARPANET-hanke. Tämä on kehittynyt maailmanlaajuiseksi järjestelmäintegraatioksi, Internetiksi. Samana vuosikymmenenä alkoi myös toinen suuri hanke American Airlinesin lippujenvarausjärjestelmä. Tätä voidaan pitää liikkeelle panevana voimana järjestelmäintegraation historiassa ja kehityksessä.

Tiedonmäärän kasvaessa ja monimutkaistuessa on samaan aikaa kehitetty teoreettisia mallinnuksia. Mallinnukset toimivat ohjaavina ja suuntaa-antavina tekijöinä yritysmaailmassa. Näitä käytetään yleisesti eri organisaatioissa. Mallinnukset perustuvat hyväksi havaittuihin toimintoihin (best practice). Nämä pyrkivät selkeyttämään ja tehostamaan organisaation toimintaa. Tunnetuin ja laajimmin käytössä oleva mallinnus on ITIL.

Opinnäytetyö pyrkii selventämään ja hahmottamaan yleisellä tasolla mitä tietojärjestelmän valvonta on. Laajana aiheena tutkimuskysymykset rajaavat opinnäytetyötä. Tutkimustulokset pyrkivät vastaamaan yleisiin kysymyksiin tietojärjestelmän valvonnasta.

2 Lähtötilanne, tavoitteet ja menetelmät

Opinnäytetyö käsittelee yleisellä tasolla järjestelmänvalvontaa sekä siihen läheisesti liittyvää järjestelmäintegraatiota. Tarkoituksena on selventää valvontaan liittyviä seikkoja ja mitä asioita tähän vaikuttaa. Opinnäytetyössä selvennetään teoreettisia referenssimallinnuksia valvonnan kannalta.

Opinnäytetyön tavoitteena on vastata tutkimuskysymyksiin ja selventää valvontaan liittyviä seikkoja. Tutkimustulokset pyrkivät selventämään tietojärjestelmävalvonnan periaatteita. Opinnäytetyössä käytetään konstruktiivista tutkimusmenetelmää.

3 Järjestelmän ja järjestelmänvalvonnan määritelmä

Järjestelmä voidaan selittää olevan ”joukko keskenään toimivia tai itsenäisiä kokonaisuuksia, jotka muodostavat integroidun kokonaisuuden” (System). Tietokonejärjestelmä puolestaan koostuu ohjelmistoista ja oheislaitteista, jotka toimivat keskenään tietokoneessa. Käyttöjärjestelmä ohjaa ja hallinnoi näiden toimivuutta. (Computer System) Tietojenkäsittelytieteen näkökulmasta järjestelmä on tietyntyyppinen alusta. Tämä on suunniteltu erilaisten ohjelmien ja sovellusten toimimiseksi. Alusta voi olla ohjelmisto- tai laitteistopohjainen. (System)

Informaatioteknologian näkökulmasta järjestelmän määrittyy myös alla mainittujen kohtien kautta:

- Ryhmä itsenäisiä osioita, jotka toimivat keskenään suorittaakseen jonkin toiminnon.
- On perustettu tai organisoitu proseduuri, metodi.
- Tietokonejärjestelmä kattaa yleensä kaksi määritystä: laitteisto- ja ohjelmistokokonaisuuden.
- Informaatiojärjestelmä kerää ja tallentaa dataa.
  (Computer System, 2009.)

Tietojärjestelmävalvonnan kahtena perustekijänä voidaan pitää asiantuntevaa henkilöstöä ja riittävän kehittyneitä järjestelmätyökaluja. Tietojärjestelmään asennettu valvontatyökalu valvoo järjestelmän toimivuutta. Valvontahenkilöstö seuraa järjestelmän toimivuutta ja reagoi mahdollisiin vikatilanteisiin järjestelmätyökalun kautta.

Järjestelmävalvontatyökalu tekee reaaliaikaista valvontaa tietojärjestelmän tilasta. Vikatilanteissa valvontatyökalu tallentaa lokitietoa tapahtuneesta. Tällöin vianselvitys mahdollistuu ja vastaava vikatilanne voidaan mahdollisesti tulevaisuudessa estää. Kehittyneet järjestelmätyökalut voivat tehdä itsenäistä viankorjausta vikatilanteissa tietyin rajoituksin. Valvontatyökalut voidaan kohdentaa tiettyihin resursseihin tietojärjestelmässä. Organisaation liiketoiminnalle keskeisiä toimintoja voidaan näin valvoa keskitetysti. (Ground Work Open Source Design principles for IT monitoring systems 2008, 2.)

4 Opinnäytetyössä käsiteltävät tutkimuskysymykset

Opinnäytetyössä tullaan esittämään neljä tutkimuskysymystä, jotka ovat:

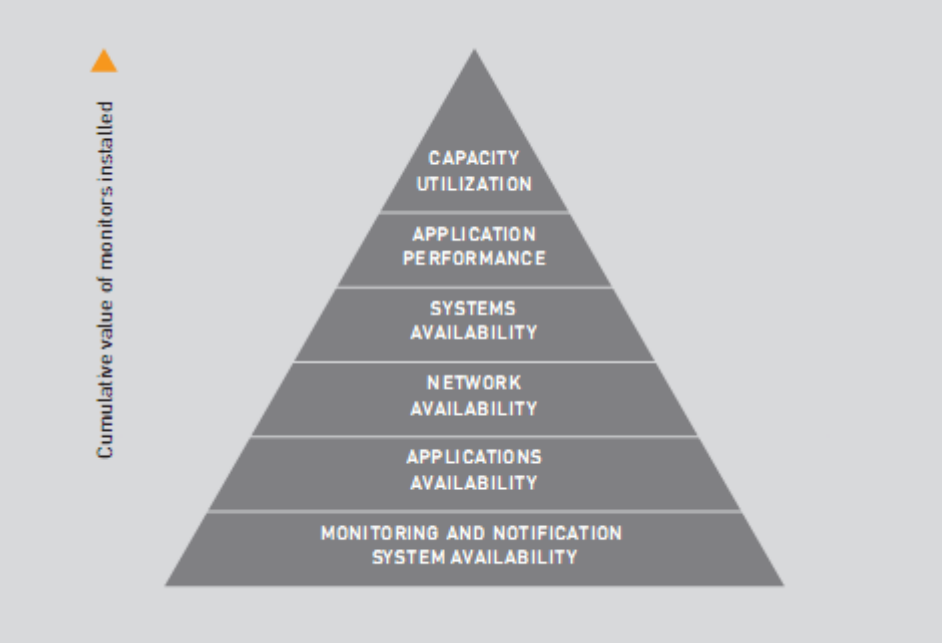
- Mitä järjestelmästä yleensä tulisi valvoa?
- Miten valvonta tulisi toteuttaa (esim. reaktiivinen vs. proaktiivinen)?
- Mitä työkaluja on tarjolla ja mihin ne soveltuvat?
- Miten organisaation valvontakulttuuria tulisi kehittää ja organisoida?

Tutkimustulosten käsittelyssä käytetään konstruktiivista tutkimusmenetelmää.

4.1 Mitä järjestelmistä yleensä tulisi valvoa?

Järjestelmänvalvonta on teknisestä näkökulmasta tarkasteltuna monimutkainen ja haasteellinen. Järjestelmään usein liittyy myös jonkin asteisen järjestelmäintegraation. Tämä puolestaan käsittää vielä monimutkaisemman hallintakokonaisuuden. Järjestelmäintegraatiosta on löydettävissä eri kriittisiä pisteitä. Nämä liittyvät suoraan tai epäsuorasti varsinaiseen liiketoimintaan. Perusajatuksena on toimintavarmuuden takaaminen ja ylläpito.

Valvonnan näkökulmasta organisaation tietojärjestelmästä on havaittavissa eri kriittisiä pisteitä. Nämä liittyvät yleensä suoraan liiketoimintaan. Tietojärjestelmän valvonta teknisestä näkökulmasta tarkasteltaessa tulisi pitää selkeänä ja yksinkertaisena. Tällöin sen hallinnointi ja ylläpito ovat yksinkertaisemmat. (Ground Work Open Source Design principles for IT monitoring systems 2008, 2.)



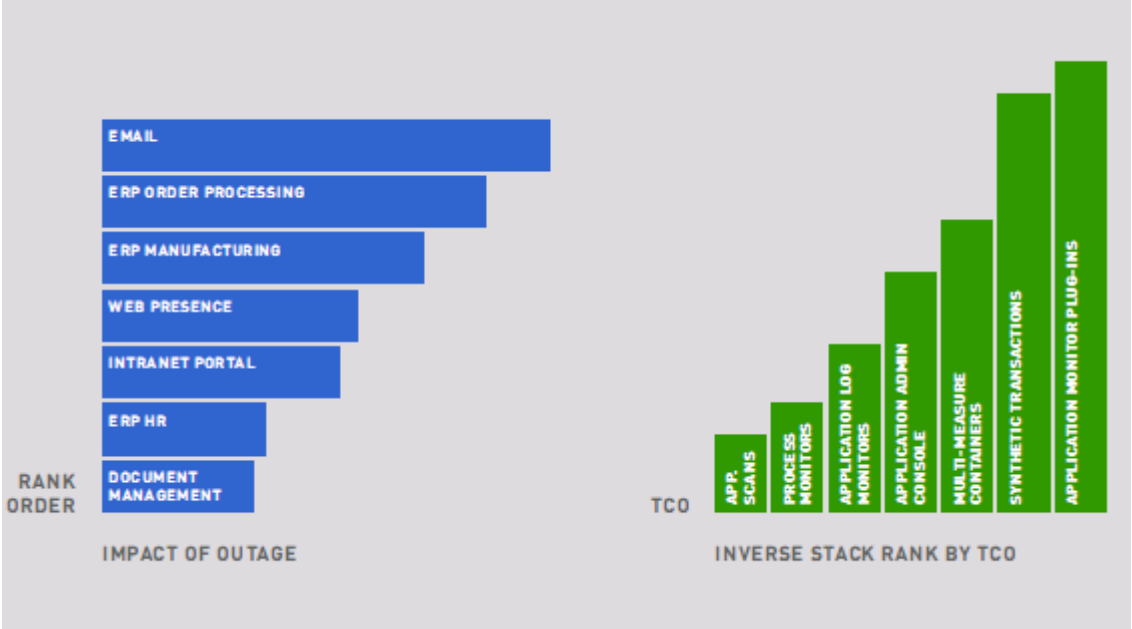
Kuva 1: Monitorointihierarkiakuvaus (Ground Work Open Source Design principles for IT monitoring systems, 2.)

Organisaation tietojärjestelmä voidaan kuvata ja priorisoida. Kuvaus antaa yleisellä tasolla olevan käsityksen tietojärjestelmän osa-alueiden tärkeydestä. Kuvassa 1 on ryhmitelty eri kokonaisuuksiin tietojärjestelmän valvonta. Osa-alueet kuvaavat valvonnan painoarvoa tietojärjestelmässä. Alin taso kuvaa koko organisaation tietoverkon toimivuutta. Liiketoiminnallisesti tämä on keskeisessä asemassa sekä siten myös valvonnan kannalta. Valvonnan näkökulmasta tietoverkon valvonta näyttelee suurinta osaa valvonnan rakenteessa.
(Ground Work Open Source Design principles for IT monitoring systems 2008, 3.)

4.2 Miten valvonta tulisi toteuttaa?

Tietojärjestelmävalvonnan toteuttaminen on aina organisaatiokohtainen. Organisaation omat sisäiset toiminnot ja toimintatavat määrittelevät pitkälle valvonnan toteuttamisen. Toteuttamisvaihtoehtoina esitetään proaktiivinen ja reaktiivinen näkökulma tietojärjestelmävalvontaan.

Alla oleva kuva esittää liiketoiminnan kriittisyys- ja toimintavarmuustason. Vasen kuvio kuvaa vaikuttuvuuden suuruusluokan vikatilanteen tapahtuessa eri IT-toiminnoissa. Oikea kuvio kuvaa organisaation järjestelmä- ja valvontatyökalujen kustannustekijää. Tämä voidaan suhteuttaa sen vaikuttuvuudella organisaation toimintaan IT:n näkökulmasta. (Ground Work Open Source Optimizing Application Monitoring 2008, 5.)



Kuva 2: Kriittiset järjestelmät sekä TCO-analyysi (Ground Work Open Source Optimizing Application Monitoring, 5.)

Total Cost of Ownership (TCO) on laskentamalli ja työkalu yritysten arvioimiseen IT-hankintojen kustannuksissa. Laskentamallia voidaan myös käyttää palvelutason määrittämiseen. TCO-analyysissä laskentamalli ottaa huomioon suorat ja epäsuorat kustannukset, kuten vaikutukset henkilöstön työmäärään. (Gartner TCO)

4.2.1 Proaktiivinen valvonta

Proaktiivinen, tai proaktiivisuus, käsittää toiminnan sekä toiminnallisuudet ennalta suunnitellulla toimintatavalla. Valvonnan näkökulmasta mahdolliset ongelma- ja vikatilanteet vältetään ennakoivasti. Tällöin ei tarvita henkilöä tai muun resurssin reagointia vikatilanteeseen. (Kuusio, A 2007, 10.)

4.2.2 Reaktiivinen valvonta

Reaktiivisuutta, tai reaktiivista toimintatapaa, voidaan tarkastella päinvastaisena toimintatapana proaktiiviselle. Tällöin jokin tapahtuma käynnistää tietyn toiminnon. Reaktiivinen toiminta tai tapahtuma on yhtäaikaisessa vaikutuksessa ainakin kahteen suuntaan. . Reaktiivinen tietojärjestelmä voidaan selittää tietojärjestelmänä, ”joka on jatkuvassa, vaikkei välttämättä tosiaikaisessa vuorovaikutuksessa ympäristönsä kanssa”. (Tietotekniikan liitto ry, 2008.)

4.2.3 Yhteenveto valvonnan toteuttamisesta

Järjestelmänvalvonnan muoto ja tapa on riippuvainen organisaation liiketoiminnan kriittisyydestä. Jos liiketoiminnalliset prosessit ovat kriittisiä, sen proaktiivisempaa tietojärjestelmävalvonta tulisi olla. Proaktiivisuus käsittää ennakoivan valmiuden ja virheenkorjauksen mahdollisiin virhetilanteisiin automatisoidusti tekniikkatasolla. Automaattista virheenkorjaamista järjestelmätyökalut pystyvät tekemään käyttäjälle huomaamattomasti tiettyyn tasoon asti. Tason saavutettua vaatii se käyttäjältä toimenpiteitä.

Proaktiivinen järjestelmänvalvonta on organisaatiolle kalliimpi ratkaisu toteuttaa. Valvontatyökalujen vaativuustaso ja toiminnallisuudet ovat eri luokkaa, kuin jos järjestelmänvalvonta suoritettaisiin reaktiivisesti. Organisaation liiketoiminta ja tietojärjestelmän kriittisyys ovat ratkaisevassa asemassa suunniteltaessa valvonnan toteuttamista.

4.3 Mitä työkaluja on tarjolla ja mihin ne soveltuvat?

Markkinoilla on suuri määrä erilaisia järjestelmänvalvontaan ja – ohjaukseen soveltuvia järjestelmätyökaluja. Työkaluina nämä ovat kattavia ja tehokkaita. Toimittajasta riippuen valvontatyökaluja on mahdollista saada muunneltuina (customize) kokonaisuuksina. Tällöin hankitaan erillisiä osia valvontatyökaluista, jotka käyttöönotetaan tietojärjestelmässä. Nämä hankinnat ovat yleensä melko suuria IT-projekteja, jotka toteutetaan eri vaiheissa. Ajallisesti projektit saattavat kestää kauan ja vaativat paljon resursseja.

4.3.1 CA Unicenter NSM

Unicenter Network and Systems Management on tarkoitettu hallinnoimaan suurten yritysten tietoteknisiä toimintoja sekä muita liiketoimintaan liittyvä tapahtumia.Työkalulla voi valvoa organisaation koko tietojärjestelmäkokonaisuutta. CA Unicenter NSM luo vakaan pohjan eri palveluiden saatavuudelle sekä datan automatisointiin. Valvontatyökalu parantaa järjestelmän tehokkuutta varmentamalla järjestelmässä olevien eri palveluihin ja toimintoihin pääsyn. Organisaatiolle tämä tuo kustannussäästöjä henkilötyötunneissa varsinaisen valvonnan minimoituessa. CA Unicenter NSM proaktiivisesti tarkentaa mahdolliset virhetilanteet ja pyrkii korjaamaan näitä. Tarvittaessa järjestelmätyökalu tekee hälytyksen käyttäjälle. Unicenter Network and Systems Management valvontatyökalu tukee perusalustoja kuten Linux, Unix ja Microsoft. Ominaisuuksiltaan CA Unicenter NSM pystyy toteuttamaan automatisoidun tapahtumahallinnan. Tällöin hakukelpoisen tapahtuman etsiminen ns. tapahtumamyrskystä on mahdollinen. Tapahtumamyrsky on samaan aikaan tapahtuvien tapahtumien sarja. Prosessointitehoa tarvitaan niin valvontatyökalulta kuin järjestelmältäkin. Keskitetty valvontakonsoli mahdollistaa näkyvyyden liiketoimintapuolen (business service) ja tukijärjestelmän (support service) välillä. Tämä on keskeistä hallittavuuden kannalta. (CA NSM, 2009.)

4.3.2 SAP R/3

SAP-toiminnanohjausjärjestelmä käsittää erilliset liiketoiminnalliset moduulit organisaation tavanomaisiin toimintoihin. Näitä moduuleita ovat mm. FICO (Financials and Controlling), HR (Human Resources), MM (Materials Management), SD (Sales & Distribution) sekä PP (Production Planning). SAP R/3 sisältää myös erillisen kehitysympäristön, jossa kehittäjät voivat muokata olemassa olevaa SAP-koodia. Tällä voidaan vaikuttaa sen hetkisiin toiminnallisuuksiin. SAP R/3 on client/server – perusteinen ratkaisu teknologialtaan ja käyttöperiaate muodostuu kolmesta tasosta. Nämä kerrokset ovat: esityskerros (presentation layer), sovelluskerros (application layer) ja tietokantakerros (database layer). Esityskerros on käyttäjälle näkyvä käyttöliittymä, jossa varsinaiset toiminnallisuudet tehdään. Sovelluskerros käsittää liiketoimintakeskeisen kokonaisuuden järjestelmään ja prosessointiin. Tietokantataso tallentaa kantaan kaiken järjestelmästä tulevan informaation. (SAPFANS R/3 All about SAP, 2008.)

4.3.3 Microsoft SMS 2003 R2 / SCCM

Microsoftin järjestelmätyökaluilla SMS (Systems Management Server 2003 R2) ja SMS:n seuraaja, SCCM (System Center Configuration Manager). Työkaluilla voidaan tehdä sisäverkon kautta työasemakohtaisia konfiguraatioita. Myös muutoksia Microsoftin alustoilla toimiville käyttöjärjestelmille on mahdollista tehdä muutoksia työkalun avulla.. Järjestelmätyökalun avulla sisäverkossa oleviin työasemiin voi asentaa esimerkiksi tietoturvapäivityksien lisäksi myös muiden ohjelmantoimittajien ohjelmistopäivityksiä. (Microsoft TechNet SMS, 2009.)

Keskeisiä toiminnallisuuksia ovat mm.

- Inventaariotyökalu ohjelmistopäivityksille, mikä sisältää kaksi erillistä komponenttia: integroitu skanneri arvioi kohdetyöaseman (client) päivitystarpeen. Julkaisutyökalu luo erillisen päivitysluettelon clientin päivitystarpeesta ja jakaa nämä verkon kautta.

- Työkalu haavoittuvuuksien havaitsemiseen: ohjelmistojen asennusvirheiden ja väärin konfiguroidut työasemien listaus sekä niistä raportointi.

Näiden edellä mainittujen ominaisuuksien lisäksi, SCCM sisältää:

- Käyttöjärjestelmien, ohjelmistojen ja ohjelmistopäivitysten jakamisen
- Ohjelmistokäytön mittaamisen
- Laitteisto- ja ohjelmistoinventaario raportoinnin
- Työasemien etähallinnan

(Microsoft TechNet SCCM, 2009.)

Järjestelmänvalvonnan kannalta valvontatyökalut ovat keskeisessä asemassa määrittämään järjestelmään kohdistuvia ongelmatilanteita. Järjestelmäintegraation kannalta on keskeistä, että valvontatyökalut ovat riittävän kehittyneet estämään ongelmatilanteet. Tärkeimpinä ominaisuuksina valvontatyökaluissa ovat: lokin ja virhelokin tuottaminen, valvontaohjelmiston vikasietotila, hälytysraportointi, ongelmatilanteiden korjaaminen ja järjestelmänpalautus. Valvontatyökalulla on rajalliset toiminnalliset mahdollisuudet korjata tulevaa tai olemassa olevaa vikatilannetta. Henkilötasolla järjestelmävastaavilla ja järjestelmävalvojilla on oltava riittävä tietotaito kuinka toimia vikatilanteissa.

4.4 Miten organisaation valvontakulttuuria tulisi kehittää ja organisoida?

Valvontakulttuurin kehittäminen on jatkuvaa organisaation muiden liiketoiminnallisten prosessien ohella. Teoreettiset referenssimallinnukset ovat yksi työkalu, jolla organisaation toimintaa ja tuottavuutta voidaan kehittää.

4.4.1 CMM

Capability Maturity Model–referenssimallinnus (CMM) keskittyy yksittäisten osa- ja erillisprosessien kypsyystasoihin. Prosessin saavutettua maksimitason, se joko valmistuu tai se on valmis siirtymään seuraavaan vaiheeseen. Prosessien kypsyystasomittaukset antavat arvokasta ja havainnollistavaa informaatiota sen eri toiminnoista. Referenssimallinnus sopii työkaluksi projekteihin, joissa aikasidonnaisuus on keskeinen. Tämä osaltaan vaikuttaa budjetissa pysymistä.
Mallinnus ei ota kantaa organisaation toimintojen tehokkuuteen suoranaisesti. Se ei myöskään anna tarkkaa tietoa tekijästä tai toiminnosta jos tiettyä kypsyystasoa ei saavuteta aikaraamissa.

4.4.2 COBIT

Control Objectives for Information and Related Technology –mallinnus (COBIT) tarjoaa best practices–toimintatavat organisaation johdolle prosessien toimivuudesta. Saatu informaatio on jalostettavissa toiminnallisiin ratkaisuihin, joiden perusteella organisaation tehokkuutta ja tuottavuutta on mahdollista parantaa. COBIT–malli kokoaa muita referenssi- ja standardimallinnuksia. COBIT tuottaa näin kattavan informaatiotyökalun organisaation johdon käyttöön.

Laajuudessaan teoriamallinnus saattaa tuottaa suuren määrän informaatiota. Tämän informaation prosessointi ja analysointi saattaa olla ongelmallista. Esimerkiksi ratkaisuvaihtoehto huonoksi todettuun toimintaan voi tuottaa haasteita. Mallinnus ei tarjoa toiminnallisessa mielessä yksiselitteistä ratkaisua huonoksi todettuun toimintaan.

Organisaation johdon asiantuntemus mallinnuksen käyttöön on ratkaisevassa tekijässä. Myös mahdollisena hankaloittavana tekijänä voidaan huomioida COBITin järkälemäisyys työkaluna. Sen tarjoamat best pracitce–toiminnallisuudet eivät välttämättä sovellu sellaisenaan organisaation sisäiseen toimintatapaan.

4.4.3 COSO

Commitee of Sponsoring Organizations (COSO) on organisaation johdon työkalu. Tällä tarkennetaan ja monitoroidaan organisaation sisäisiä prosesseja ja niiden toimivuutta. Työkalu tuottaa informaatiota eri prosessien tehokkuudesta. Mallinnus esittää myös ne kohteet, jotka mahdollisesti tarvitsevat lisähuomiota ja resursseja.

Mallinnuksen tuottama informaation tehokas hyödyntäminen voi tuottaa ongelmatilanteita organisaation johdolle. Mallinnus ei anna varsinaista ratkaisua heikosti toimivaan prosessiin. Mallinnus esittää vain huomionarvoisen osa-alueen organisaation sisällä. Johdolla tulee olla selkeä tulkinta ja toimintatapa kuinka reagoida heikosti toimivaan prosessiin.

Organisaation johdon ymmärtäminen mallinnuksen käyttöön on keskeistä. Myös informaation suodattaminen ja tämän oikeanlainen kanavointi toivottuun ratkaisuun, on keskiössä. Mallinnus saattaa näin olla sen varsinaisessa muodossa ongelmallista käyttää. Kysymykseen voi tulla eräänlainen muokattu (ns. kustomoitu) versio mallinnuksesta.

4.4.4 ISO/IEC 27001/27002

Standardi tietoturvahallinnoinnin parantamiseen syntyi yhteistyönä International Organization of Stadardization (ISO) ja International Electrotechnical Commission (IEC) tahojen välillä. Työkalu kokoaa organisaation sisäiset tietoturvakäytänteet standardin alle, joka yhdenmukaistaa hallinnointia. Yhdenmukaistaminen helpottaa ja tuo läpinäkyvyyttä, joissa tietoturvakäytänteet ovat hajautettu.

Haasteena standardiluokituksen saamiseksi saattaa olla organisaation sisäisten prosessien muokkaaminen vaadituksi. Investointi henkilöstön koulutukseen sekä mahdolliset ohjelmisto- ja laitteistokannan uusiminen voi viedä liikaa organisaation resursseja.

4.4.5 ITIL

Laajimmin käytössä oleva referenssimallinnus on Infromation Technology for Infrastructure Library (ITIL). Mallinnus kattaa ja ohjeistaa hyväksi havaittujen käytänteiden kautta laajimmin organisaation prosesseja. ITIL tuo selkeyttä ja läpinäkyvyyttä organisaation toimintoihin. Hallinnoinnin ja johtamisen kannalta mallinnus tarjoaa kontrolloitua informaatiota päätöksentekoon. Asiakasnäkökulmasta tarkasteltaessa ITIL tuo asiakaslähtöisempää näkökulmaa organisaation tuottamiin palveluihin.

Referenssimallinnuksen käyttöönotto organisaatiossa voi olla haasteellista, kun määritellään tarvittavat prosessit ja osaprosessit. Henkilöstön sitouttaminen on keskiössä mallinnuksen käyttöönotossa. Tämä puolestaan vaatii riittävää kouluttamista ja perehdyttämistä mallinnuksen käyttöön. ITIL sellaisenaan ei välttämättä sovellu jokaisen organisaation käyttöön. Tällöin voi tulla kyseeseen kustomoitu ratkaisu, jossa käytetään vain mallinnuksen eri osia. Onnistunut käyttöönotto tuo kustannussäästöjä sekä parantaa ja tehostaa tuottavuutta.

4.4.6 Mallinnusten yhteenveto

Referenssimallinnukset ovat toimivia informaatioita silloin, kun ne ovat oikein käyttöönotettuja ja niitä noudatetaan. Projektinäkökulmasta tarkasteltaessa sopivinta mallinnusta esitetyistä voinee pitää CMM-mallinnusta. Mallinnus antaa selkeää informaatiota projektin eri osista sekä niiden valmistumisesta. Tehokkain ja perustavanlaatuisin oleva mallinnus lienee ITIL. Päätyminen tähän johtopäätökseen perustuu ITILin läpileikkaavasta näkökulmasta organisaation eri toiminnallisuuksiin ja prosesseihin, tuottaen näistä selkeää ja informatiivista tietoa organisaation sen hetkisestä tilanteesta.

5 Tutkimustulosten esittely ja johtopäätökset

Referenssimallinnukset osaltaan ohjaavat ja tehostavat organisaation tuotannollisia, taloudellisia ja toiminnallisia ratkaisuja. Mallinnusten tuottama informaatio on käytettävissä organisaation johdolle. Tämän perusteella voidaan edelleen kehittää ja tehostaa prosesseja. Nykyään enenevässä määrin tarvitaan raportointia organisaation sen hetkisestä taloudellisesta ja tuotannollisesta tilasta. Referenssimallinnukset mahdollistavat tätä osittain. Tämän tueksi tietojärjestelmätyökalujen riittävä tehokkuus luo vakaan perustan tarvittavalle analyysille.

Opinnäytetyössä esitetyt mallinnukset ovat perusteellisia ja kattavia. Organisaation sijoittaminen mallinnukseen tuottaa selkeää informaatiota sen hetkisestä tilasta. Mallinnukset mahdollistaa siedettävällä reaaliaikaisuudella sekä vasteajalla vastaamaan johdon tarvitsemiin informaatioihin.

Haasteena on havaittavissa mallinnuksen käyttöönotto organisaatiossa. Ryhdyttäessä noudattamaan tiettyä mallinnusta, on organisaation mahdollisesti tehtävä mittaviakin muutoksia. Sisäiset toiminnot ja toiminnallisuudet tulee tarkentaa uudesta näkökulmasta. Näiden muokkaaminen mallinnusta vastaavaksi voi olla ongelmallista. Toimintojen muuttaminen ja nimeäminen prosesseja vastaavaksi saattaa vaatia radikaalejakin rakennemuutoksia organisaation sisällä.

Käyttöönotettaessa mallinnusta osaksi organisaatiokulttuuria, on huomioitava sen kokonaisvaltainen vaikuttavuus. Keskiössä on henkilöstö. Henkilöstön tulee olla selvillä ja tietoisia tehtävistä muutoksista. Tällöin pienentyy muutosvastarinta. Tällä on suora vaikutus työmotivaatioon ja työn laadukkaaseen suorittamiseen. Valvontakulttuurin kehittäminen ja tehostaminen on mahdollista silloin, kun päätöksenteko ja noudatettavat muutokset toiminnassa, ovat läpinäkyviä.

Järjestelmäintegraatioratkaisuissa ja teknillisessä puolessa on havaittavissa muutosta tulevaisuudessa. Esimerkiksi tällä hetkellä ns. rautapalvelimet ovat jäämässä historiaan ja tilalle tulossa enemmän virtualisoitu palvelinympäristö. Arkkitehtonisesti tämä ei sinänsä tee juurikaan muutoksia rautapalvelinarkkitehtuuriin. Hallittavuus, vianselvitys ja palautusmahdollisuudet paranevat huomattavasti virtuaalisoinnissa. (Tietokone – Virtualisointi, 2009.)

Kustannussäästötekijä on oleellinen vaikuttava tekijä infrastruktuurimuutoksessa. Ennustettavuus järjestelmävalvontatyökaluissa on vaikeaa. Havaittavissa kuitenkin on, että on pilvimalli – ajattelu valtaa alaa. Tällöin palvelut ja toiminnot eivät fyysisesti sijaitse organisaation omilla palvelimillaan. Tämän mahdollistaa palveluntarjoaja. Ajallisesti ja teknisesti ratkaisu saattaa nopeuttaa eri toimintoja ja läpivientejä. Esimerkkinä voidaan pitää virustorjuntaohjelmiston ja käyttöjärjestelmän teknistä toteutusta pilviratkaisussa. (Tietokone – Pilviratkaisu, 2009.)

6 Opinnäytetyössä käytetyt referenssimallinnukset

IT (Information Technology) on irrottamattomasti mukana organisaation varsinaisen toiminnan mahdollistajana. Jatkuvasti kasvava tietomäärä, nopeusvaatimukset informaation käsittelyyn ja laskentatoimen monimutkaisuudet ovat nykypäivää. Osaltaan näistä lähtökohdista ovat eri mallinnuskäsitteet ohjaaviksi tekijöiksi saaneet alkunsa. (Reference model, 2009.)

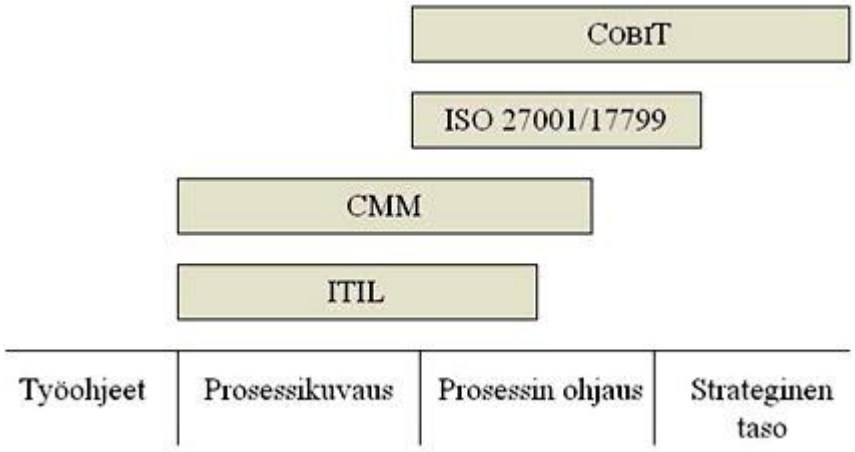
Tietojärjestelmäriippuvuus on ilmeinen vaatimusten kasvaessa ja monimutkaistuessa. Näistä lähtökohdista on syntynyt IT Governance – käsite. IT Governance toimintatapa on organisaation johdon käytössä. Tähän sisältyy johtajuutta, organisointia ja prosessointia. Näillä varmistetaan strategioiden ja tavoitteiden saavuttamiseen on IT:n täysi tuki ja osallistuminen. Tätä tukevat mm. teoriamallinnukset ITIL (Information Technology Infrastructure Library) ja COBIT (Control Objectives for Information and Related Technology). Muita vastaavia referenssimallinnuksia ovat mm. CMM (Capability Maturity Model), COSO (Committee of Sponsoring Organizations) ja standardit ISO/IEC 27001, ISO/IEC 27002. (Pohjola, K., 2007.)

6.1 COBIT-malli

COBIT-mallinnuksen tarkoituksena on tarjota best practices–toimintatavat. Nämä esitetään helposti käsiteltävässä muodossa ja etenevät loogisessa järjestyksessä. Näillä toimintatapamalleilla pyritään vastaamaan organisaation johdon IT:lle asettamiin vaatimuksiin. Tämä mahdollistuu yhdistämällä aukot liiketoimintariskien, teknisten osa-alueiden, kontrolloitavuuden sekä tuottavuusvaatimusten välillä. (Bita Center, 2008.)

6.1.1 COBIT–mallinnuksen historia ja tausta

COBIT –mallinnuskäsite syntyi vuonna 1996 ISACAn (Information Systems Audit and Control Association) ja ITGIn (IT Governance Institute) yhteistyönä. Tällä hetkellä COBIT-malli on versiossa 4.1, joka julkistettiin toukokuussa vuonna 2005. (Cobit, 2009.)



Kuva 3: COBIT–mallinnus (Pohjola, K., 2007.)

COBIT–malli voidaan käsittää eri teoriamallinnusten ylätason kokoavana sateenvarjomallina. Malli pyrkii sisältämään johtamisen, hallinnoinnin ja valvonnan koko tietohallinnossa. COBIT-referenssimalli täydentää rajatuimpiin osa-alueisiin tai näkökulmiin keskittyviä muita referenssimalleja ja standardeja. Sinällään COBIT ei siis korvaa muita malleja vaan toimii täydentävänä referenssinä sen alapuolella oleville malleille. (Pohjola, K., 2007.)

COBITissa on johtamisen helpottamiseksi kuvattu suorituskykyindikaattorit, ongelmaindikaattorit, tavoiteindikaattorit sekä kriittiset menestystekijät. Näiden indikaattorien seuranta antaa johdolle arvokasta informaatiota. Nämä helpottavat myös pitämään liiketoimintaa oikeassa suunnassa. Mallinnus tuottaa informaatiota siitä, kuinka varsinaisen liiketoiminnan ja IT-tukitoiminnan välistä rajapintaa tulisi hallinnoida sekä johtaa. Palvelun hankkijan näkökulmasta tarkasteltaessa COBITin tuottama hyöty on palveluiden hankinnassa. Mallinnus selventää liiketoiminnalliset seikat, joita organisaation kannattaa vaatia ja ottaa huomioon. Palvelun tuottajalle mallinnus kuvaa miten palvelut kannattaa rakentaa ja toimittaa, jotta nämä olisivat laadullisesti hyviä. (Cobit, 2009.)

6.1.2 COBIT -mallinnuksen kattavuus

Valvontanäkökulmasta mallinnus pyrkii huomioimaan organisaatiossa seuraavat asiat: luottamuksellisuuden, käytettävyyden, luotettavuuden, vaikuttavuuden, tehokkuuden, taloudellisuuden ja vaatimuksenmukaisuuden. Keskeiset hallittavat resurssit ovat tietojenkäsittelyn infrastruktuuri, sovellukset, informaatio sen eri muodoissa ja palveluita tuottavat henkilöt. Tehtäväalueet ja tietotekniikkaprosessit ovat jaettu mallinnuksessa neljään kategoriaan: suunnittelu, rakentaminen, tuotanto ja arviointi. (Cobit, 2009.)

Suunnittelu ja organisointi–osuudessa malli tarkastelee otsikkotasolla seuraavia tehtäväalueita: henkilöresurssit, laatu, riskit, projektit, viestintä, investoinnit, organisointi, tekniset arkkitehtuurit, tietoarkkitehtuurit ja strategisen suunnittelun. Mallinnus esittää keinot ja ratkaisut liiketoiminnan ja IT:n yhteensovittamiseen, riskien ymmärtämiseen ja hallintaan sekä hyötyjen optimointiin. Organisaation strategian toteuttamiseksi tarvitsee se vaatimustason täyttävän järjestelmän. Rakentaminen ja toteutus–vaiheen prosessit keskittyy: sovellusten ja infrastruktuurin kehittämiseen ja ylläpitämiseen, esitutkimukseen, käyttöönoton edellytysten rakentamiseen, hallittuun muutokseen ja tuotantoon siirtoon sekä tarvittavien resurssien varmistamiseen. (Pohjola, K., 2007.)

Kolmanteen kategoriaan, tuotanto ja tuki, on koottu ITILin kaltaiset palveluprosessit ja toiminnot. Tässä kategoriassa käsitellään mm. suorituskyvyn ja kapasiteetin hallintaa, toiminnan jatkuvuutta ja turvallisuutta, koulutusta, konfiguraation hallintaa sekä käyttäjätukea ja palvelupyyntöjen hallintaa. Viimeisessä neljännessä kategoriassa, arviointi ja seuranta, käsitellään prosesseja seurannan ja arvioinnin sekä vaatimustenmukaisuuden varmistamisen näkökulmasta. Tällä pyritään selvittämään heijastuuko IT:n suorituskyky sekä tuki varsinaisen liiketoiminnan tavoitteiden saavuttamiseen. (Pohjola, K., 2007.)

Aikaisemmin mainitut kypsyystasot ovat määriteltyjä prosessien profiileja. Nämä kuvaavat prosessien kypsyyttä, kun asiaa tarkastellaan hallittavuusnäkökulmasta. Tässä vaiheessa ei oteta kantaa siihen onko kaikki kontrollit asiayhteydessä toteutunut. CMM (Capability Maturity Model), josta seuraavassa osuudessa enemmän, on ohjelmistokehitykseen kehitetty ja ideoima kypsyystasomalli, joka on myös COBITin perustana. Tässä mallissa eri asiakokonaisuudet pisteytetään skaalalla 1 – 5, COBITissa on vielä 0-taso mukana. Pisteytys tapahtuu seuraavasti: 0-tasolla prosessia ei ole, eikä tällaista ole tunnistettu tai sellaiseen ei ole tarvetta. 1-tasolla toiminta tapahtuu tapauskohtaisesti, tekeminen on reaktiivisella tasolla tilanteesta ja henkilöistä riippuen. 2-taso käsittää yhteisiä toimintamalleja, joiden kautta toiminta tapahtuu ja mahdollistuu. 3-taso käsittää menettelyt ja toiminnat ns. hyväksi havaittujen käytäntöjen (best practices) mukaisesti. Nämä käytännöt ovat dokumentoitu. Tällöin toimintatavat ovat helpompi tarkistaa, seurata sekä kouluttaa ja ohjeistaa muulle henkilöstölle tarvittaessa. 4-taso käsittää jatkuvan parantamisen edellytykset toimintaan, jota täsmennetään seurannan ja mittauksen kautta. 5-taso käsittää automatisoituja työkaluja, vertailupohjaa muihin organisaatioihin ja hyväksi havaittuja käytäntöjä. Tasojen välimatkat ovat melko karkeita sillä hienojakoisuudessaan mallin käyttäminen olisi sekavaa ja harhaanjohtavaa. Mallin ydintarkoituksena onkin tarjota tunnisteet heikkoihin kohtiin organisaatiossa. (Cobit, 2009.)

COBIT–mallinnuksessa on kypsyystasojen lisäksi tasokriteerit. Nämä liittyvät erikseen mallissa kuvattuihin 34 tietotekniikkaprosessiin. COBIT esittää laajan kokoelman ehdotuksia mittareista, joiden avulla voi löytää oman organisaation toimintaan soveltuvia esimerkkejä. Vastaavasti voi myös syntyä uusia organisaation suorituskykyyn liittyviä mittareita. Malli esittää esimerkkejä tavoiteindikaattoreista (Key Goal Indicators, KGI) sekä suorituskykyindikaattoreista (Key Performance Indicators, KPI). Tavoiteindikaattori kuvaa prosessin tavoitteen saavuttamista lopputulosten kautta. Suorituskykyindikaattori käsittää prosessin toimintaa siten, minkälaiset mahdollisuudet tavoitteiden saavuttamiselle on. (Cobit, 2009.)

6.2 CMM

CMM (Capability Maturity Model) on mallinnuskäsite, joka kehitettiin ja ideoitiin ohjelmistokehityksessä. Tämä tarjoaa kypsyystasomallinnuksen organisaation ohjelmistokehitykseen. Tämä on yhtenä osana liiketoimintaprosessia. CMM keskittyy teoriamallina prosessien kypsyystasoihin, jotka eroavat muista yleisistä kypsyystasomalleista. Tämä tarjoaa kokoelman niitä osia, jotka kuvaavat tiettyjä kypsyystasoja organisaatiossa. CMM on käytännöllinen mallinnus, kun tarkoituksena on saada läpinäkyvyyttä organisaation prosesseihin ja näiden määrityksiin. (CMM, 2009.)

6.2.1 CMM:n historiaa ja taustaa

Alkujaan CMM–teoriamalli kehitettiin työkaluksi valtionjohdolle, jotta mahdollistuisi ohjelmistoprojektien objektiivinen seuranta. CMM pohjautuu Process Maturity Framework mallinnukseen, joka ensimmäisen kerran julkaistiin ja kuvattiin vuonna 1989. Myöhemmin tästä julkaistiin virallisempi raportti vuonna 1993. Vaikka CMM–malli tulee lähinnä ohjelmistokehityksen kuvaamisesta ja mallinnuksesta, käytetään sitä yleisenä mallinnuksena. Tällä pyritään helpottamaan, kehittämään ja tehostamaan organisaation liiketoimintaprosesseja. Mallinnusta käytetään mm.: ohjelmisto- ja järjestelmätekniikassa, ohjelmistokehityksessä, järjestelmähankinnoissa ja henkilöstöresurssien mittaamisessa. CMM–mallinnusta käytetään maailmanlaajuisesti laajalti hallinnossa, kaupankäynnissä, teollisuudessa ja ohjelmistokehityksessä yhteiskunnassa eri organisaatioissa. (CMM, 2009.)

6.2.2 CMM ja kypsyystasot

CMM–mallinnuksessa on tunnusomaista viisitasoinen kypsyysnäkökulma organisaation prosesseihin:

1. Lähtötilanne (kaoottinen, ad hoc): aloituspiste ja – hetki uudelle prosessille

2. Toistettavuus: prosessi voidaan toistaa useasti karkeilla toistuvilla lopputuloksilla

3. Määriteltävyys: prosessi määritellään tai todetaan standardiksi liiketoiminta-prosessiksi, joka luokitellaan tasojen 0, 1 ja 2 mukaisesti. Numero indikoi työohjeistuksen ja – ohjaamisen määrää, jossa maksimiluku on 2.

4. Hallittavuus: prosessi hallinnoidaan Määriteltävyys -tason metriikan mukaisesti. Painopiste työohjeistukselle ja ohjaamiselle määrittyy edellisen tason luvusta

5. Tehostettavuus: prosessinhallinta sisältää tarkoituksenmukaista tehostamista ja edistämistä.

Näiden edellä mainittujen kypsyystasojen sisällä on KPA (Key Process Area) ydinprosessialue, joka luonnehtii kyseessä olevaa tasoa. Jokaiselle KPA–määrittelylle on yksi identifioiva määritys:

1. Päämäärä

2. Sitoutuminen

3. Kykenevyys

4. Arviointi

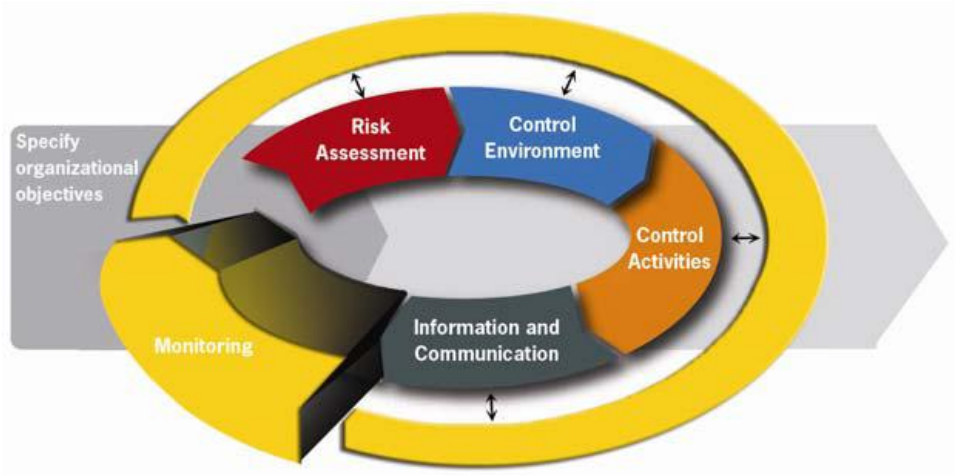
5. Vahvistus

KPA-määrittelyt eivät välttämättä ole ainutlaatuisia CMM-mallinnuksessa, mutta ovat suuntaa-antavia. Määrittely esittää ne tasot, jotka organisaation on käytävä läpi saavuttaakseen kypsyystason. Tasojen väliin jättäminen ei ole sallittua tai kannattavaa. CMM-mallinnus esittää teoreettisen jatkuvuuden kypsyystasojen väleillä. Näiden läpikäynti tulee tapahtua suuruusjärjestyksessä ensimmäisestä tasosta alkaen. (CMM, 2009.)

6.3 COSO

COSO (Committee of Sponsoring Organizations) tarjoaa monitorointi- ja seurantamallin organisaation sisäiseen tarkastukseen ja kontrollointiin. Mallinnuksessa on organisaation omat sisäiset prosessit ja niiden kontrollointi keskiössä. Tämä mahdollistaa saavuttamaan organisaation itselleen asetetut tavoitteet. Monitorointi ja seuranta ovat erottamattomat tekijät organisaation sisäisten prosessien mittaamisessa ja tarkentamisessa. Nämä tukevat informaation avoimuutta ja eheyttä yhteiskunnallisella tasolla. (Guidance on Monitoring Internal Control Systems, 2009.)

Eri hallinnoissa tunnistetaan ongelma, jossa sisäinen kontrollointi on aikaa vievä osa-alue. Tämän on tunnistanut myös COSO-mallinnuksen kehittänyt lautakunta. Tätä varten kehitettiin erityinen mallinnus. Mallinnuksessa on viisi erillistä komponenttia, jotka kuvaavat sisäisiä prosesseja.



Kuva 4: COSOn mallinnus (Guidance on Monitoring Internal Control Systems, 1.)

Malli kuvaa COSOn viisi ydinkomponenttia: Monitorointi, Riskin arviointi, Ympäristön hallinta, Kontrollitoiminnot, Informaatio ja kommunikointi. Ydinkomponentit ovat jatkuvassa vuorovaikutuksessa monitoroinnin kanssa. Jos tietty ydinkomponentti vie liian suuren osa-alueen mallinnuksesta, tulee tähän reagoida.

Organisaation sisäisten prosessien monitorointi ja toimintojen tehokas seuranta mahdollistaa organisaation: identifioimaan ja korjaamaan sisäiset kontrolliongelmat, tuottaa tarkempaa ja luotettavampaa informaatiota päätöksenteon tueksi, valmius tuottaa tarkkoja aikasidonnaisia tilinpäätöstietoja ja raportteja. Näiden tekijöiden huomioiminen mahdollistaa organisaation tehokkuuden lisäämisen sekä kustannusten alentamisen. Tällöin mahdolliset ongelmat ja vikatilanteet ovat tunnistettavissa ja hallittavissa. (Guidance on Monitoring Internal Control Systems, 2009.)

6.4 ISO/IEC 27001

ISO/IEC 20700–standardointiperhe muodostuu tietoturvastandardeista. Nämä ovat julkaissut ISO (International Organization for Standardization) yhteistyössä IEC:n (International Electrotechnical Comission) kanssa. Tietoturvaan liittyvä standardointiperhe tarjoaa hyväksi havaitut toiminnot (best practices) tietoturvahallinnoinnissa ja kokonaisriskienhallinnassa. ISO/IEC 207000–standardointiperhe laaja-alaisuudessaan kattaa IT:n ja muut tekniset turvallisuuskysymykset sekä luottamuksellisuuden ja yksityisyyden. Organisaatioita kannustetaan arvioimaan ja määrittämään oma tietoturvataso sekä tietoturvaan kohdistuvat riskit. Arvioinnin jälkeen organisaation tulisi päättää sille sopivan tietoturvakontrollien käyttöönottamista. (ISO/IEC 27000-series, 2009.)

ISO/IEC 27001 on osa edelleen kasvavaa ISO/IEC 27000–standardointiperhettä, joka on osana ISMS (Information Security Management System) standardia. Julkistaminen tapahtui elokuussa 2005 ISOn ja IEC:n yhteistyönä. Standardi esittää hallinnollisen toimintatavan, jonka tarkoituksena on liittää tietoturva suoraan hallinnolliseen kontrolliin. Tämä on virallinen määritelmä standardille, joka määrittää vaatimukset organisaatioille hallinnollisesti ja IT-infrastruktuurisesti. (ISO/IEC 27001, 2009.)

Standardin vaatimukset organisaatiolle

Standardin kolmitasoiseen vaatimusluokitukseen kuuluu:

- Tietoturvariskien tutkiminen ja havainnointi
- Tietoturvakontrollien johdonmukainen suunnittelu ja käyttöönotto
- Tietoturvavaatimusten käyttöönotto ja niiden noudattaminen organisaatiossa.

ISO/IEC 27001 ja ISO/IEC 27002–standardeja käytetään yhdessä, jotka täydentävät toisiaan. ISO/IEC 27001 listaa perusteellisesti tietoturvakontrollit ISO/IEC 27002–standardista. Vastaavasti ISO/IEC 27002 tarjoaa ajankohtaista informaatiota ja käyttöönotto-ohjeistusta kontrolleista ja niiden käytöstä. (ISO/IEC 27001, 2009.)

6.5 ISO/IEC 27002 (ISO/IEC 17799)

Kansainvälinen standardi ISO/IEC 17799 julkaistiin uudestaan heinäkuussa 2005 ISO/IEC 27002 nimellä. Ainoana teknisenä korjauksena oli tunnuksenmuutos (Suomen Standardisoimisliitto SFS ry). ISO/IEC 27002 käsittää hyväksi havaitut toiminnot (best practices) tietoturvahallinnoinnissa. Standardi on erityisesti henkilöille, jotka vastaavat organisaation ISMS (Information Security Managemet System) – politiikan perustamisesta, käyttöönotosta sekä ylläpidosta(ISO/IEC 27002, 2009.).

Tietoturvan määritystä voidaan tarkastella ns. C – I - A–kolmion kautta. Kirjaimet tulevat englanninkielen sanoista: Confidentiality (luotettavuus), Integrity (eheys) ja Availability (saatavuus). Luotettavuus tarkoittaa informaatioon pääsyä vain niille henkilöille, joilla on tähän oikeus. Eheys viittaa tiedon virheettömyyteen ja täydellisyyteen. Saatavuus tarkoittaa pääsyä informaatioon, kun siihen on tarve. (CIA-triad, 2009.)

Standardi koostuu 12 osasta:

1. Riskinarviointi
2. Turvallisuuspolitiikka
3. Tietoturvan organisaatio: tietoturvahallinnointi
4. Voimavarojen hallinnointi: informaation koostaminen ja luokittelu
5. Henkilöstönturvallisuus: henkilöstön sitoumus turvallisuuspolitiikkaan
6. Ympäristönturvallisuus: tietoteknillisten tilojen suojaus
7. Kommunikaatio ja operatiivinen turvallisuus: järjestelmien ja tietoverkkojen teknisten turvallisuuskontrollien hallinnointi
8. Pääsykontrolli: pääsyn rajoittaminen tietoverkkoon, järjestelmiin, sovelluksiin ja dataan
9. IT-järjestelmien hankinta, kehittäminen ja huoltaminen: sovelluksiin rakennettava turvallisuustaso
10. Tietoturvatapaushallinta: ennakointi ja vastaaminen tietoturvauhkiin ja –rikkomuksiin riittävällä tasolla
11. Liiketoiminnallisen jatkuvuuden hallinnointi: suojaus, hallinnointi ja palautus liiketoimintakriittisille prosesseille ja järjestelmille
12. Standardin noudattaminen: standardin yhdenmukaistaminen ja lainsäädännön kanssa.(ISO/IEC 27002, 2009.).

6.6 ITIL-malli

ITIL (Information Technology Infrastructure Library) on kokoelma käytäntöjä, jotka perustuvat hyväksi havaittuihin käytäntöihin (best practices). ITIL–mallinnus on globaalisti yleisimmin käytössä oleva teoriamallinnus eri organisaatioissa. Teoriamalli antaa kehyksen kuinka organisaation sisällä eri prosessit ja toiminnallisuudet tulisi tapahtua. Mallinnus on ollut käytössä yli 20 vuotta ja tätä on kehitetty jatkuvasti. Tällä hetkellä ITIListä on käytössä versionumero 3. Tämän kehitys alkoi Englannissa 1980-luvulla OGC:n (Office of Government Commerce) hallinnolliseksi työkaluksi, joka on myös tuotemerkinnyt mallin itselleen. (ITIL, 2009)

6.6.1 IT-tukiprosessit

IT-tukiprosessi käsittää ITIL-mallinnuksen mukaisesti viisi erillistä osaprosessia. Prosessit ovat tapahtuma-, ongelma-, muutoksen-, version- ja konfiguraationhallinta. Nämä viisi osaprosessia ovat keskeisessä roolissa, kun organisaation toiminnallisuutta mallinnetaan esimerkiksi tuottavuuden tehostamisen näkökulmasta. IT-tukiprosesseihin kuuluu edellä mainittujen osaprosessien lisäksi yksi toiminnallisuus, joka on service desk. Service desk on loppukäyttäjien ensisijainen yhteydenottopiste (first point of contact), joka vastaa ensimmäisen asteen tuesta IT-vikatilanteissa. (ITIL, 2009)

6.6.2 Tapahtumanhallinta

Tapahtumanhallinnasta on kyse silloin, kun jokin tapahtuma keskeyttää muuten normaalina pidetyn toiminnan tai tapahtumaketjun. Tällöin tapahtumanhallinnan tavoitteena on palauttaa tilanne takaisin. Tällöin pyritään normalisoida palveluoperaatiot. Tähän pyritään vaikuttamaan ensisijaisesti minimoimalla vikatilanteen vaikuttuvuus työntekoon. (ITIL, 2009)

6.6.3 Ongelmanhallinta

Ensisijaisena tavoitteena ongelmanhallinnalla on minimoida virheistä johtuvien ja niistä aiheutuvat tapaukset ja ongelmat. Ennakoiva ja ennaltaehkäisevä toiminta tapausten ja ongelmien syntyyn ja esiintyvyyteen kuuluu ongelmanhallinnan toimenkuvaan. Ongelmahallinnan vastuualue kattaa vakavien tapausten hoitamisessa avustaminen, ongelmien ennakoiva estäminen, virheiden ja ongelmien kontrollointi, hallinnollisten ongelmatietojen saanti ja vakavien ongelmien tarkastelu. (ITIL, 2009)

6.6.4 Muutoksenhallinta

Muutoksenhallinnan pääasiallisena tavoitteena on varmistaa, että muutoksen toteuttaminen aiheuttaa minimoidun katkoksen työntekoon. Muutoksen aloitus ja toteuttaminen tapahtuu standardoituja menetelmiä käyttäen. Muutostarpeet yleensä ilmenevät, kun esimerkiksi jokin tietty ongelma toistuu. Muutoksenhallinnan vastuualueena on muutosten toimeenpanon hallinnointi ja koordinoiminen, ehdotetun muutoksen vaikutusten määrittäminen ja muutosten esiintuominen tallentaminen. (ITIL, 2009)

6.6.5 Versionhallinta

Versionhallinnalla tarkastelee ja varmentaa muutoksen toteutuksessa tapahtuvan teknisen ja liiketoiminnallisen puolen. Vastuualueenaan on myös organisaation itsensä hyväksymien ohjelmistojen ja laitteistojen käyttö sekä testaus. Versionhallinta vastaa tiiviistä yhteistyöstä muutoksenhallinnan kanssa ohjelmistojen jakeluversioiden turvallisuudesta ja suunnittelusta. (ITIL, 2009)

6.6.6 Konfiguraationhallinta

Konfiguraationhallinnan päämääränä on tuottaa ja järjestää looginen malli IT-infrastruktuurille. Tämä tapahtuu dokumentoinnin kautta. IT:n laitteistojen ja ohjelmistojen paikkaansa pitävyys ja ajantasaisuus mahdollistavat muiden prosessien hyödyntämisen. Konfiguraationhallinta vastaa konfiguraation rakenneosien yksilöimisestä ja merkitsemisestä sekä konfiguraation rakenneosien kontrolloimisesta ja näistä raportoimisesta. (ITIL, 2009)

6.6.7 IT-palvelujen toimittaminen

IT-palvelujen toimittamisella tarkoitetaan organisaation strategista näkymää, jonka avulla pyritään hallinnoimaan ja kontrolloimaan IT-resursseja. IT-palvelujen toimittaminen sisältää viisi hallintoprosessia. Nämä ovat: palvelutasohallinta, kapasiteettihallinta, saatavuuden hallinta, kustannushallinta ja IT Service Continuity management. (ITIL, 2009)

6.6.8 Palvelutasonhallinta

Palvelutasonhallinnan tavoitteena on kohdennettujen IT-palveluiden laatutasojen ylläpito ja parantaminen. Tämä tapahtuu IT-palveluista syntyvien saavutusten ja tulosten jatkuvalla seurannalla ja raportoinnilla. Vastuualueiksi tunnistetaan palvelutasojen ja kustannusten mittaaminen sekä raportointi. (ITIL, 2009)

6.6.9 Kapasiteetinhallinta

Kapasiteetinhallinnalla on tavoitteena ymmärtää ja tiedostaa tulevaisuuden vaatimuksia, jotka kohdentuvat liiketoimintaan. Vastuualueena on liiketoiminnan kapasiteetinhallinta. Tällä tarkoitetaan, että IT-palveluihin kohdistuvia liiketoiminnallisia vaatimuksia. (ITIL, 2009)

6.6.10 Saatavuuden ja käytettävyyden hallinta

Prosessialue vastaa IT-infrastruktuurin suorituskyvystä ja tuesta organisaatiota kohtaan. IT-palveluiden varmistaminen käyttäjille, kun he sitä tarvitsevat, on yksi tärkeimmistä vastuista. (ITIL, 2009)

6.6.11 Kustannustenhallinta

Vastuualueena on IT-omaisuudenhoidon järjestämisestä taloudellisesti kannatettavasti. Raportoinnilla taataan ja mahdollistetaan palveluiden tehokkuus sekä taloudellinen kannattavuus. Vastuisiin kuuluu myös IT-budjetin hallinnoiminen. (ITIL, 2009)

6.6.12 IT Service Continuity Management

IT Service Continuity Management pyrkii takaamaan tarvittavien tietoteknisten välineiden ja muiden IT-palveluiden korjaamisen vaaditussa aikaraamissa. Tällä pyritään takaamaan tuki varsinaiselle liiketoiminnalle. (ITIL, 2009)

7 Järjestelmäintegraatio

Järjestelmäintegraatio liittyy olennaisesti järjestelmään sekä sen toimintaan. Nykyään eri organisaatioiden tietojärjestelmät ovat yleensä ainakin osittain integroituja. Sovellukset, ohjelmistot ja tietokannat tulee integroida toimivaksi kokonaisuudeksi. Tällöin organisaation IT-toiminnot ovat yhtenäiset ja hallittavissa olevat. Tämä tuo nopeutta ja valmiutta vastata esimerkiksi liiketoiminnallisiin muutoksiin. Toimiva ja hallittava integraatio on vaativa ja haasteellinen kokonaisuus. Riittävä tietotaito on perusedellytys. Tämän jälkeen tulevat riittävän kehittyneet ja tehokkaat järjestelmätyökalut.

7.1 Historia

Järjestelmäintegraatio voidaan katsoa alkaneen kuutisenkymmentä vuotta sitten vuonna 1949. Yhdysvaltalain ilmavoimien alullepanema massiivinen projekti yhdistyi toisen vastaavan kanssa. Ensimmäinen näistä oli SAGE (Semi-Automatic Ground Environment), jonka tarkoituksena oli automatisoida huonossa kunnossa oleva ilmavalvontajärjestelmä. Toinen vastaavanlaista kokoluokkaa edusti siviilipuolen IBM:n SABRE–projekti (Semi-Automatic Business Environment Research). Tämä tosin myöhemmin muuttui muotoon SABER (suom. sapeli, jolla haluttiin luoda mielikuvaa nopeudesta ja osumatarkkuudesta). Tämä projekti oli suunniteltu American Airlinesille, jossa lentoyhtiö automatisoi paikanvaraukset sekä lipunmyynnin lennoillensa. Projektin tuotoksena oli hajautettu järjestelmä, jonka tekemiseen kesti kymmenen vuotta suunnittelu- ja kehitystyötä. Käyttöönottovuosi oli 1964. Tänä päivänäkin yli 200 lentoyhtiötä käyttää varausjärjestelmää. Tätä on edelleen kehitetty käyttöönottovuodesta. (Semi-Automatic Ground Environment (SAGE), 2010.)

Suurimpana järjestelmäintegraatioprojektina voidaan pitää 1960-luvulla eri Internet-tekniikoiden kehittämistä. Erityyppiset tietoliikenneverkot ja niihin kytketyt eri päätelaitteet kytkeytyvät keskenään yhdysverkon kautta. Tällöin mahdollistuu yhteen toimiminen toisten laitteiden kanssa maailmanlaajuisesti. Tätä kokonaisuutta kutsutaan Internetiksi. (Tähtinen 2005, 19.)

Internetin alkuvaiheen kehityksen aikoihin 1960–70 luvulla tapahtui eräs käännekohta ohjelmistoteollisuudessa. Tällöin markkinoille tulivat paketoidut ohjelmistotuotteet, joissa ohjelmistot erotettiin erillisiksi lisensioiduiksi osiksi ratkaisutoimituksia. Tähän vaikutti suurelta osin IBM:n päätös sekä erinäiset antitrustioikeudenkäynnit. Aikaisemmin tietokonevalmistajat aiemmin näkivät ohjelmistojen toimituksen eräänlaisena pakollisena markkinointikuluna. Ohjelmistot katsottiin olevan myynnin tehostamisen selkärankana. Tämä johti maailman suurimman tietojärjestelmätoimittajan IBM:n päätös ohjelmisto- ja laitteistotoimituksen erityke-selle. Päätös mahdollisti monen muun pienemmän ohjelmistotoimittajan syntyyn ohjelmistoteollisuudessa. Tämän seurauksena räätälöidyt ja asiakaskohtaiseen tarpeeseen perustuvat ohjelmistot alkoivat saada markkinaosuutta tietotekniikkateollisuudessa. (Semi-Automatic Ground Environment (SAGE), 2010.)

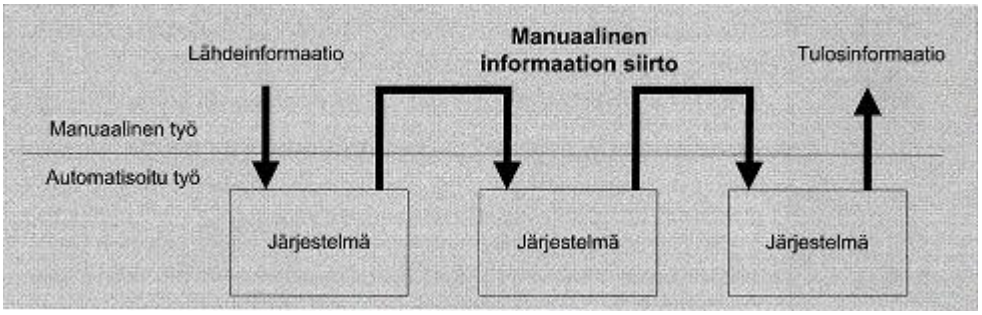
Ohjelmistot voidaan jakaa kolmeen ryhmään: räätälöidyt, paketoidut ja tuotteistutetut ohjelmistokokonaisuudet. Räätälöidyissä ohjelmistoissa pääpaino on yksittäisen asiakkaan tietty ongelma. Tämän ohjelmistontuottaja tuottaa asiakkaan tarpeisiin vaaditun ohjelman. Paketoidut ohjelmistot käsittävät suuren määrän valmista ja yleiskäyttöistä ohjelmakoodia. Järjestelmän käyttöönotossa paketoidut ohjelmistot nopeuttavat sen käyttöönottoa. Tuotteistettu ohjelmisto on erillinen ohjelmistopaketti. Yksittäinen henkilö tai yritys voi ottaa tämän käyttöön erittäin nopeasti ja vähällä vaivalla. (Tähtinen 2005, 20.)

7.2 Järjestelmäintegraation määritelmä

Järjestelmäintegraatiolla tällä tarkoitetaan niitä toimintatapoja ja tekniikoita, joilla mahdollistetaan yhtyeensopimattomat ja toimimattomat tietojärjestelmät toimimaan keskenään. Kommunikoimattomat järjestelmät pyritään saamaan keskustelemaan toistensa kanssa. (Tähtinen 2005, 47-48.) Integraatioratkaisussa on kysymys informaation siirtämisestä integroitavien järjestelmien välillä. Tämä tarkoittaa kokonaisprosessia, jossa on varsinainen tiedonsiirto ja tietomuunnokset, kontrollointi ja näihin liittyvä monitorointi sekä raportointi. (Jeffrey O., G. 1994, 3-4.)

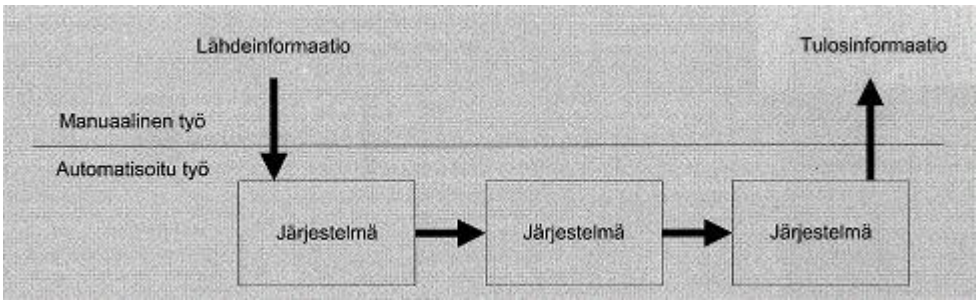
7.3 Järjestelmäintegraation hyödyt

Järjestelmäintegraatio esittää keskeistä roolia kustannussäästötekijänä. Laitehankinnat sekä tehtävät henkilötyötunnit minimoituvat automatisoinnin kautta. Manuaalisen ja automatisoidun työn eroa kuvaa seuraavat varsin yleisellä tasolla olevat kuvat. Lähde- ja tulosinformaation ääripäiden väliin jäävä manuaalinen työ jää seuraavassa kuvassa kokonaan pois.



Kuva 5: Informaation siirto ja kulku ilman integraatiota (Tähtinen, 23.)

Alla lähdeinformaation syöttö tapahtuu kerran integraation seurauksena.

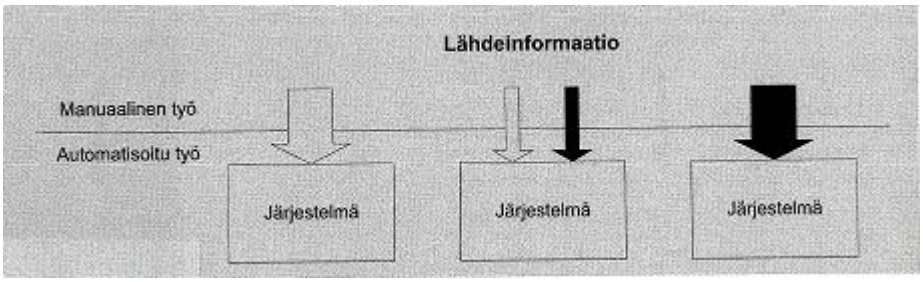


Kuva 6: Informaation kulku järjestelmäintegraatiossa (Tähtinen, 25.)

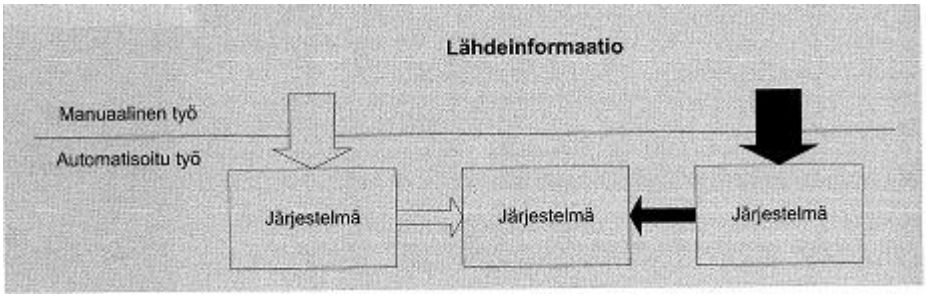
7.3.1 Kustannussäästöt organisaatiolle

Kokonaisjärjestelmässä erillisjärjestelmät ovat integroidut yhteen toimivaksi kokonaisuudeksi. Erillisjärjestelmien integrointi yhdeksi kokonaisjärjestelmäksi säästää organisaation IT-kustannusmenoissa pidemmällä aikavälillä. Aloituskustannukset voi järjestelmäintegraatiossa olla suuret. Yhden kokonaisjärjestelmän hallinnointiin käytettävät resurssit ovat pienemmät kuin useamman erillisjärjestelmän hallinnoinnissa. Selvin säästö tulee henkilötyötunneista ja IT-laitteistoista ja ohjelmistoista. (Tähtinen 2005, 22-27.)

Alla on kuvattuna syötteiden tekeminen järjestelmään manuaalisesti. Manuaalisen työn määrä on moninkertainen verrattaessa seuraavalla sivulla olevaan kuvaan (Kuva 4). Siinä järjestelmäintegraation seurauksena syöttö tapahtuu kerran.



Kuva 7: Informaation kulku integroimattomassa järjestelmässä (Tähtinen, 26.)

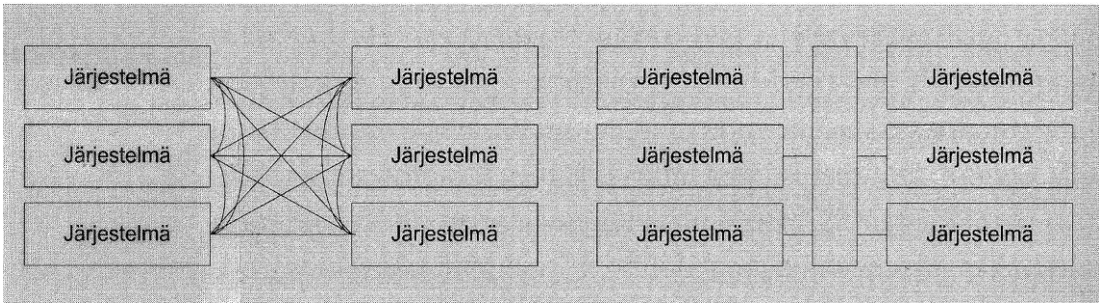


Kuva 8: Informaation kulku integroidussa järjestelmässä (Tähtinen, 26.)

7.3.2 Liiketoiminnan mukautuvuus

Organisaation vastaaminen uusiin liiketoiminnallisiin muutoksiin saattaa nopeutua integraation kautta. Mahdolliset muutokset tietojärjestelmään on tehtävissä hallitusti ja melko pienellä vasteajalla. Muutoksiin vastaaminen on yksinkertaisempaa ja nopeampaa, kun tiedetään yhden kokonaisjärjestelmän toiminnallisuudet. Usean erillisjärjestelmän hallinta ja muuttaminen lyhyellä vasteajalla on erittäin haasteellista, ellei mahdotonta.

Alla oleva kuva esittää edellisessä kappaleessa kuvattua tilannetta. Vasen kuvio kuvaa tietojärjestelmän hallintaa integraation kautta. Tässä hallinnointi on joustavampaa, kun vertaa oikeanpuoleiseen kuvioon. Järjestelmähallinnan näkökulmasta hallittavuus on jäykkää ja hidasta. Erillisjärjestelmien integroimattomuus hidastaa liiketoiminnalliseen muutokseen vastaamista. Tällöin tietojärjestelmään tehtävät muutokset on tehtävä yksi kerrallaan. Tämän jälkeenkin muutokset on saatava toimimaan kokonaisuutena.



Kuva 9: Integroidun ja point-to-point järjestelmien eroavuudet (Tähtinen, 30.)

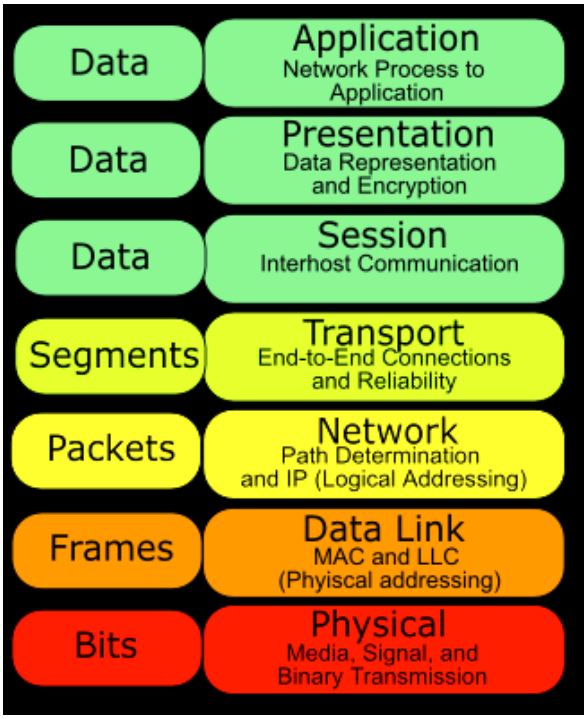
7.3.3 Valvottavuus

Järjestelmähallinta ja valvonta yksinkertaistuvat järjestelmäintegraation seurauksena. Tällöin valvottavana on yksi kokonaisuus, jolloin hallittavuus säilyy. Henkilöresurssien vapautuminen ja uudelleensijoitus tehostaa organisaation toimintaa ja tuo säästöjä. (System Monitoring)

7.4 Järjestelmäintegraation tekniikankuvaus

Yritysten välisessä tiedonsiirrossa verkkoarkkitehtuurina pidetään yleisesti LAN - lähiverkkoratkaisua (Local Area Network). Protokollatasolla dataliikenne siirtyy yleisimmin TCP/IP -perusteisesti (Transmission Control Protocol / Internet Protocol). Dataliikennöinti tapahtuu siirtomedian välityksellä. (Tähtinen 2005, 50-51.)

Dataliikennöinnin kuvaukseen ja protokollatason toimintoihin selventää OSI-malli (Open System Interconnection Referecne Model). OSI-malli kehitettiin kuvaamaan ja selventämään dataliikennöintiä. Riippuen datan liikennöinnistä, mallia luetaan ylhäältä alas tai päinvastoin. Perusperiaatteena on, että jokainen kerros tarjoaa tarvittavaa toimintoa seuraavalle kerrokselle. (OSI model, 2009.).



Kuva 10: OSI-malli (OSI model, 2009)

7.4.1 Rajapinnat

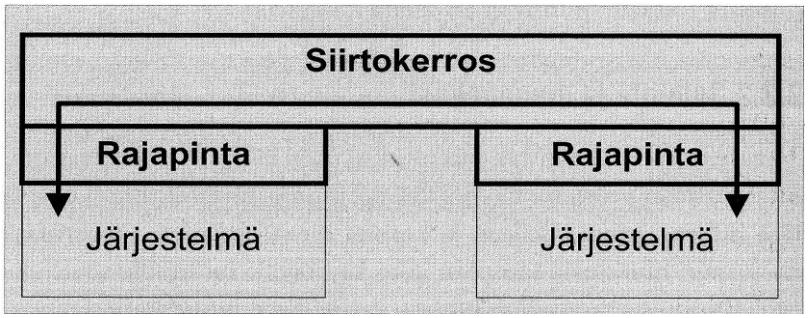
Rajapinta mahdollistaa eri järjestelmien välisen informaation siirron. Integroitavien järjestelmien tekniset ominaisuudet on mahdollistettava tämä. Rajapinnan välityksellä järjestelmien on mahdollista hakea ja syöttää informaatiota. Varsinaisen informaation siirtämiseen tarvitaan fyysinen siirtotie. Tällainen on esimerkiksi tietoverkko tai sen päällä toimiva sanomajärjestelmä. (Tähtinen 2005, 49.)

Rajapintaa voidaan kuvata tilanteessa, jossa kaksi itsenäistä järjestelmää kohtaavat rajan ylittävässä tarkoituksessa. Tällöin tapahtuu jokin toiminto, esimerkiksi yhteyden hylkäys, tai järjestelmien välinen kommunikointi. Rajanpintaa voidaan myös tarkastella käyttäjän näkökulmasta. Käyttöliittymiä ovat mm. tietokoneen näppäimistö, hiiri, käyttöjärjestelmän eri valikot. Toisaalta ohjelmassa tai ohjelmistossa rajapintana on ohjelmointikieli ja ohjelmakoodi. Nämä mahdollistavat kommunikoinnin laitteiston sekä ohjelmapuolen kanssa. Laitteiston näkökulmasta rajapintana ovat johdot, kaapelit ja erilaiset liitännät ja pistorasiat. (Interface, 2009.)

7.4.2 Siirtokerros

Verkkoarkkitehtuuri sekä etäkutsu- ja/tai sanoma-arkkitehtuuri yhdessä luovat määrityksen siirtokerrokselle. Verkkokerroksen päällä toimii etäkutsu- tai sanomansiirtoarkkitehtuuri. Tämä mahdollistaa järjestelmien välisen kommunikoinnin sekä informaationsiirron. Integraatioarkkitehtuurissa toimiva siirtokerros huolehtii informaation jakamisesta luotettavasti ja aikakriittisesti eri järjestelmien välillä.

Informaation kulku on toimittava mahdollisissa vikatilanteista huolimatta muuttumattomana. Alla oleva kuva hahmottaa siirtokerroksen toiminnallisuutta kahden eri järjestelmän tiedonsiirrossa ja kommunikoinnissa. (Tähtinen 2005, 50-53.)



Kuva 11: Tiedonsiirto kahden eri järjestelmän välillä (Tähtinen, 53.)

8 Arviointia

Aiheen käsittely ja rajaus tuotti aluksi hieman haastetta tämän ollessa aluksi kiteytettynä tutkimuskysymyksiin. Tekijän näkökulmasta tämä todettiin liian suppeaksi ja hankalasti käsiteltäväksi. Aihe laajentui käsittämään järjestelmäintegraatiota sekä teoreettisia referenssimallinnuksia. Vaarana tässä oli jälleen aiheen rajaus mallinnusten laaja-alaisuuden vuoksi.

Loppukaneettina voidaan todeta opinnäytetyön onnistuneen tavoitteessaan´. Tutkimusnäkökulma ja rajaus pysyvät opinnäytetyön raamissa. Aihetta käsitellään konstruktiivisen tutkimusnäkökulmasta. Samalla työ pyrkii olemaan informatiivinen ja antaa lukijalle perushahmotuksen järjestelmävalvonnan periaatteista.

Lähteet

Bita Center. 2008. Viitattu: 25.7.2009. http://www.bita-center.com/cobit

CA NSM. 2009. Viitattu: 25.9.2009.
http://www.ca.com/us/system-management.aspx

CIA-triad. 2009. The CIA Triad Viitattu: 5.6.2009.
http://blogs.techrepublic.com.com/security/?p=488

CMM. 2009. CMMI Viitattu:12.8.2009. http://www.sei.cmu.edu/cmmi/start/

Cobit. 2009. Cobit forums and information Viitattu:25.7.2009. http://www.controlit.org/

Computer System. 2009. Webopedia Viitattu: 25.5.2009.
http://www.webopedia.com/TERM/C/computer_system.html

Gartner TCO. 2009. Viitattu: 25.9.2009.
http://www.microsoft.com/finland/business/tco/default.mspx

Ground Work Open Source 2008a. Design principles for IT monitoring systems. Ground Work Open Source, Inc.: San Francisco.

Ground Work Open Source 2008b. Optimizing Application Monitoring. Ground Work Open Source, Inc.: San Francisco.

Guidance on Monitoring Internal Control Systems 2009.

Interface. 2009. Webopedia Viitattu: 23.7.2009.
http://www.webopedia.com/TERM/i/interface.html

ISO/IEC 27000-series. 2009. About ISO27k Viitattu:4.6.2009.
http://www.iso27001security.com/html/iso27000.html

ISO/IEC 27001. 2009. ISO/IEC 27001:2005 Viitattu:4.6.2009.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=42103

ISO/IEC 27002. 2009. Introduction to ISO 27002 Viitattu:4.6.2009.
http://www.27000.org/iso-27002.htm

ITIL. 2009. ITIL – The IT Infrastructure Library Viitattu: 23.7.2009.
http://itil.technorealism.org/

JZY Computers. 2009. Viitattu: 14.8.2009.
http://www.jzycomputers.net/12.html

Kuusio, A. 2007. HAMK:N JA HAMIN tietohallintostrategia.

Microsoft TechNet SCCM. 2009 Viitattu: 25.9.2009.
http://technet.microsoft.com/en-us/library/bb735860.aspx

Microsoft TechNet SMS. 2009. Viitattu: 25.9.2009.
http://technet.microsoft.com/en-us/sms/bb676790.aspx

OSI model. 2009. Webopedia Viitattu: 16.8.2009.
http://www.webopedia.com/quick_ref/OSI_Layers.asp

Pohjola, K. 2007. COBIT-malli tietohallinnon kehittämiseen. Viitattu: 23.7.2009.
http://www.yliopistojenit.fi/weblehti/nro1_07/cobit.html

Reference model. 2009. Viitattu 19.5.2009.
http://www.wfmc.org/reference-model.html#workflow_reference_model

SAPFANS R/3 All about SAP. 2008. Viitattu: 25.9.2009.
http://www.sapfans.com/?page_id=2

Semi-Automatic Ground Environment (SAGE). 2010. Viitattu 4.5.2009.
http://www.livinginternet.com/i/ii_sage.htm

Suomen Standardisoimisliitto SFS ry. 2007. Viitattu: 4.6.2009.
http://www.sfs.fi/ajankohtaista/tiedotteet/20070921152430.html

System. 2009. Definitions of Systems and Models. Viitattu: 23.7.2009.
http://www.physicalgeography.net/fundamentals/4b.html

System Monitoring. Viitattu 15.5.2009.
http://www.sys-net.it/LDP/LDP/sag/html/system-monitoring.html

Tietotekniikan liitto ry. 2008. Viitattu: 1.6.2009.
http://www.ttlry.fi/atk-sanakirja/su019.htm

Tietokone – Pilviratkaisu. 2009. Viitattu: 24.10.2009.
http://www.tietokone.fi/uutiset/ilmainen_pilvivirustorjunta_valmistui

Tietokone – Virtualisointi. 2009. Viitattu 24.10.2009.
http://www.tietokone.fi/uutiset/2009/suomi_on_virtualisoinnin_etulinjassa

Tähtinen, S. 2005. Järjestelmäintegraatio – Tarve, Vaihtoehdot, Toteutus. Gummerus Kirjapaino Oy Jyväskylä.

Kuvaotsikkoluettelot