

26.8.2015

Copyright © 2013 by Committee of Sponsoring Organizations of the Treadway Commission, (“COSO”) strictly reserved. No parts of this material may be reproduced in any form without the written permission of COSO.

Permission has been obtained from the copyright holder, COSO, to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of COSO.

Kaikki tekijänoikeudet © 2013 Committee of Sponsoring Organizations of the Treadway Commissionillä (“COSO”). Tätä aineistoa ei miltään osin saa kopioida missään muodossa ilman COSOn kirjallista lupaa.

Oikeudenomistaja COSO on myöntänyt oikeuden julkaista tämä käännös, joka kaikilta olennaisilta osiltaan vastaa alkuperäistä aineistoa paitsi milloin muutos on erikseen hyväksytty. Tätä dokumenttia ei ilman COSOn kirjallista hyväksymistä saa miltään osin kopioida, säilyttää tiedonhakujärjestelmissä eikä välittää missään muodossa sähköisesti, mekaanisesti, kopioimalla, äänittämällä tai muullakaan tavalla.

## INTERNAL CONTROL - INTEGRATED FRAMEWORK EXECUTIVE SUMMARY

### SISÄISEN VALVONNAN KOKONAISVALTAINEN AJATUSMALLI TIIVISTELMÄ

#### EXECUTIVE SUMMARY

Internal control helps entities achieve important objectives and sustain and improve performance. COSO's *Internal Control – Integrated Framework* enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risk to acceptable levels, and support sound decision making and governance of the organization.

Designing and implementing an effective system of internal control can be challenging; operating that system effectively and efficiently every day can be daunting. New and rapidly changing business models, greater use and dependence on technology, increasing regulatory requirements and scrutiny, globalization, and other challenges demand any system of internal control to be agile in adapting to changes in business, operating and regulatory

#### TIIVISTELMÄ

Sisäinen valvonta auttaa organisaatioita saavuttamaan tärkeitä tavoitteitaan sekä ylläpitämään ja kehittämään suorituskykyään. COSO:n *Sisäinen valvonta – kokonaisvaltainen ajatusmalli* mahdollistaa organisaatioita tuloksellisesti ja tehokkaasti kehittämään sisäistä valvontaa siten, että se mukautuu muuttuviin toimintaympäristöihin, saattaa riskejä hyväksyttävälle tasolle ja tukee linjakasta päätöksentekoa sekä johtamis- ja hallintojärjestelmää.

Tuloksellisen sisäisen valvonnan suunnittelu ja käyttöönotto voi olla haastavaa; sen päivittäinen hyödyntäminen tuloksellisesti ja tehokkaasti voi olla haasteellista. Uudet ja nopeasti muuttuvat liiketoimintamallit, teknologian lisääntyvä käyttö ja riippuvuus siitä, tiukentuva sääntely ja seuranta, kansainvälistyminen sekä muut haasteet vaativat jokaista sisäisen valvonnan järjestelmää olemaan ketterä omaksuakseen

26.8.2015

environments.

An effective system of internal control demands more than rigorous adherence to policies and procedures; it requires the use of judgment. Management and boards of directors<sup>1</sup> use judgment every day to select, develop, and deploy controls across the entity. Management and internal auditors, among other personnel, apply judgment as they monitor and assess the effectiveness of the system of internal control.

The *Framework* assists management, boards of directors, external stakeholders, and others interacting with the entity in their respective duties regarding internal control without being overly prescriptive. It does so by providing both understanding of what constitutes a system of internal control and insight into when internal control is being applied effectively.

For management and boards of directors, the *Framework* provides:

- A means to apply internal control to any type of entity, regardless of industry or legal structure, at the levels of entity, operating unit, or function
- A principles-based approach that provides flexibility and allows for judgment in designing, implementing, and conducting internal control – principles that can be applied at the entity, operating and functional levels
- Requirements for an effective system of internal control by considering how components and principles are present and functioning and how components operate together
- A means to identify and analyse risks, and to develop and manage appropriate responses to risks within acceptable levels and with a greater focus on anti-fraud measures
- An opportunity to expand the application of internal control beyond financial reporting to other forms of reporting, operations, and compliance objective
- An opportunity to eliminate ineffective, redundant, or inefficient controls that provide minimal value in reducing risks to the

muutokset toimintaympäristöissä.

Tulokellinen sisäinen valvonta vaatii enemmän kuin tiukkaa toimintaperiaatteiden ja menettelytapojen noudattamista; se vaatii arviointikyvyn hyödyntämistä. Johto ja hallitus<sup>2</sup> käyttävät arviointikykyään päivittäin valitessaan, kehittäessään ja käyttöönottaessaan valvontatoimenpiteitä koko organisaatiossa. Johto ja sisäiset tarkastajat, muun henkilöstön ohella, käyttävät arviointikykyään seurattessaan ja arvioidessaan sisäisen valvonnan tuloksellisuutta.

Ajatusmalli auttaa johtoa, hallitusta, ulkoisia sidosryhmiä ja muita organisaation vaikutuspiirissä olevia tahoja toteuttamaan sisäisen valvonnan tehtäviään olematta liian ohjaileva. Malli tarjoaa sekä ymmärryksen sisäisen valvonnan osa-alueista että näkemyksen siitä, milloin sisäinen valvonta toimii tuloksellisesti.

Ajatusmalli tarjoaa johdolle ja hallitukselle

- keinon soveltaa sisäistä valvontaa erilaisiin organisaatioihin, huolimatta niiden toimialasta tai laillisesta rakenteesta, organisaatio-, yksikkö- tai toimintotasoilla
- periaatteellisen lähestymistavan joka tarjoaa joustavuutta ja sallii arviointikyvyn hyödyntämisen sisäistä valvontaa suunniteltaessa, käyttöönotettaessa ja toteutettaessa – periaatteita, joita voidaan soveltaa organisaatio-, yksikkö- tai toimintotasoilla
- vaatimukset tulokselliseen sisäiseen valvontaan huomioimalla mitä elementtejä ja periaatteita on käytössä ja miten ne toimivat yhdessä ja erikseen
- keinon tunnistaa ja arvioida riskejä sekä kehittää ja hallita asianmukaisia hallintakeinoja riskien saattamiseksi hyväksyttävälle tasolle ja keskittymällä väärinkäytöksiä estäviin keinoihin
- mahdollisuuden laajentaa sisäisen valvonnan soveltamista taloudellisesta raportoinnista muihin raportoinnin, toiminnan ja vaatimustenmukaisuuden tavoitteisiin

<sup>1</sup> The *Framework* uses the term "board of directors", which encompasses the governing body, including the board, board of trustees, general partners, owner, or supervisory board.

<sup>2</sup> Ajatusmallissa sana "hallitus" viittaa organisaation ylimpään hallintoelimeen, joka voi olla hallituksen lisäksi säätiön hallitus, hallintoneuvosto, yhtiömielhet, omistaja tai johtokunta.

26.8.2015

achievement of the entity's objectives

- mahdollisuuden poistaa tuloksettomia, turhia tai tehostomia valvontakeinoja, jotka tuottavat hyvin vähän lisäarvoa organisaation tavoitteiden saavuttamista uhkaavien riskien pienentämiseksi.

For external stakeholders of an entity and others that interact with the entity, application of this *Framework* provides:

Ajatusmallin hyödyntäminen tarjoaa organisaation ulkoisille sidosryhmille ja muille organisaation vaikutuspiirissä oleville tahoille

- Greater confidence in the board of directors' oversight of internal control systems
- Greater confidence regarding the achievement of entity objectives
- Greater confidence in the organization's ability to identify, analyse, and respond to risk and changes in the business and operating environments
- Greater understanding of the requirement of an effective system of internal control
- Greater understanding that through the use of judgment, management may be able to eliminate ineffective, redundant, or inefficient controls
- vahvemman luottamuksen hallituksen sisäisen valvonnan ohjaukseen
- vahvemman luottamuksen organisaation tavoitteiden saavuttamiseen
- vahvemman luottamuksen organisaation kykyyn tunnistaa, arvioida ja vastata riskeihin sekä toimintaympäristöjen muutoksiin
- laajempaa ymmärrystä tehokkaan sisäisen valvonnan vaatimuksista
- laajempaa ymmärrystä siitä, että arviointikykyä hyödyntämällä johdolla on mahdollisuus poistaa tuloksettomia, turhia tai tehostomia valvontatoimenpiteitä.

Internal control is not a serial process but a dynamic and integrated process. The *Framework* applies to all entities: large, mid-size, small, for-profit and not-for-profit, and government bodies. However, each organization may choose to implement internal control differently. For instance, a smaller entity's system of internal control may be less formal and less structured, yet still have effective internal control.

Sisäinen valvonta on jatkuva ja kokonaisvaltainen prosessi. Ajatusmalli soveltuu kaikkiin organisaatioihin: suuriin, keskisuuriin, pieniin, voittoa tavoitteleviin tai yleishyödyllisiin sekä julkisiin organisaatioihin. Jokainen organisaatio voi kuitenkin valita erilaisen tavan soveltaa sisäistä valvontaa. Pienemmän organisaation sisäinen valvonta voi olla esimerkiksi vähemmän määrämuotoinen, mutta silti tehokas.

The remainder of this Executive Summary provides an overview of internal control, including a definition, categories of objective, description of the requisite components and associated principles, and requirement of an effective system of internal control. It also includes a discussion of limitations – the reasons why no system of internal control can be perfect. Finally, it offers considerations on how various parties may use the *Framework*.

Loppuosa tästä tiivistelmästä tarjoaa yleiskatsauksen sisäiseen valvontaan sisältäen määritelmän, tavoitteet, kuvauksen pakollisista osatekijöistä ja niitä tukevista periaatteista sekä tuloksellisen sisäisen valvonnan vaatimukset. Siinä käsitellään myös rajoituksia – syitä, miksi yksikään sisäisen valvonnan järjestelmä ei voi olla täydellinen. Lopulta se tarjoaa näkökohtia siihen, miten eri osapuolet voivat hyödyntää ajatusmallia.

## DEFINING INTERNAL CONTROL

## SISÄISEN VALVONNAN MÄÄRITELMÄ

Internal control is defined as follows:  
*Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable*

Sisäinen valvonta on määritelty seuraavasti:  
*Sisäinen valvonta on organisaation hallituksen, johdon ja muun henkilöstön toteuttama prosessi, jonka tarkoituksena on antaa kohtuullinen varmuus*

26.8.2015

*assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

*niiden tavoitteiden saavuttamisesta, jotka liittyvät toimintoihin, raportointiin ja vaatimustenmukaisuuteen.*

This definition reflects certain fundamental concepts. Internal control is:

Tämä määrittely kuvastaa tiettyjä peruskäsitteitä. Sisäinen valvonta

- *Geared to the achievement of objectives* in one or more categories – operations, reporting, and compliance
- *A process* consisting of ongoing tasks and activities – a means to an end, not an end in itself
- *Effected by people* – not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- *Able to provide reasonable assurance* – but not absolute assurance, to an entity's senior management and the board of directors
- *Adaptable to the entity structure* – flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

- *on suunnattu tavoitteiden saavuttamiseen*, koskivat ne sitten toimintoja, raportointia tai vaatimustenmukaisuutta
- *on prosessi*, joka koostuu jatkuvista tehtävistä ja toiminnoista - keinoista päästä tavoitteeseen, ei pelkästä lopputuloksesta
- *on ihmisten toteuttamaa* - kysymyksessä eivät ole ainoastaan periaatteet, ohjeistukset, järjestelmät ja mallit, vaan ihmiset ja heidän sisäiseen valvontaan liittyvät toimenpiteensä kaikilla organisaation tasolla
- *pystyy antamaan kohtuullisen varmuuden* - mutta ei täyttä varmuutta organisaation ylimmälle johdolle ja hallitukselle
- *soveltuu organisaation rakenteeseen* - voidaan joustavasti soveltaa koko organisaatiossa tai vain tietyssä tytäryhtiössä, toimialalla, liiketoimintayksikössä tai prosessissa.

This definition is intentionally broad. It captures important concepts that are fundamental to how organizations design, implement, and conduct internal control, providing a basis for application across organizations that operate in different entity structures, industries, and geographic regions.

Määritelmä on tarkoituksellisesti laaja. Se koostuu tärkeistä käsitteistä siitä, kuinka organisaatiot suunnittelevat, ohjaavat ja toteuttavat sisäistä valvontaa sekä siitä, kuinka ne tarjoavat perustan sisäisen valvonnan soveltamiselle kautta koko organisaation erilaisissa rakenteissa, eri toimialoilla ja eri maantieteellisillä alueilla.

## OBJECTIVES

## TAVOITTEET

The *Framework* provides for three categories of objectives, which allow organizations to focus on differing aspects of internal control:

Ajatusmallissa tavoitteet on luokiteltu kolmeen ryhmään, jotka heijastavat sisäisen valvonnan eri näkökulmia:

- *Operations Objectives* – These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
- *Reporting Objectives* – These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.

- *Toiminnan tavoitteet* liittyvät organisaation toiminnan tehokkuuteen ja tuloksellisuuteen mukaan lukien toiminnalliset ja taloudelliset tulostavoitteet ja omaisuuden turvaaminen.
- *Raportoinnin tavoitteet* liittyvät sisäiseen ja ulkoiseen laskentaan sekä toiminnalliseen raportointiin. Raportointi voi koskea viranomaisten, muiden normeja asettavien tahojen ja organisaation omien periaatteiden mukaista raportointia. Tavoitteet liittyvät

26.8.2015

- *Compliance Objectives* – These pertain to adherence to laws and regulations to which the entity is subject.

raportoinnin luotettavuuteen, ajantasaisuuteen, läpinäkyvyyteen tai muiden vaatimusten toteutumiseen.

- *Vaatimustenmukaisuuden tavoitteet* liittyvät organisaatiota koskevien lakien ja määräysten noudattamiseen.

## COMPONENTS OF INTERNAL CONTROL

Internal control consists of five integrated components.

### Control environment

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

### Risk assessment

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to estab-

## SISÄISEN VALVONNAN OSATEKIJÄT

Sisäinen valvonta koostuu viidestä toisiinsa linkittyvästä osatekijästä.

### Ohjausympäristö

Ohjausympäristö on joukko standardeja, prosesseja ja rakenteita, jotka muodostavat sisäisen valvonnan perustan koko organisaatiossa. Hallitus ja ylin johto osoittavat toiminnallaan, mikä merkitys sisäisellä valvonnalla on organisaatiossa ja miten organisaatiossa tulee toimia. Johto varmistaa, että nämä odotukset toteutuvat organisaation eri tasoilla. Ohjausympäristö käsittää

- organisaation eettiset arvot ja niiden mukaisen toiminnan
- keinot, joiden avulla hallitus toteuttaa valvontavelvollisuuttansa
- organisaatorakenteet sekä toimivaltuudet ja vastuut
- prosessin, jonka avulla palkataan pätevää henkilöstöä, kehitetään heidän osaamistaan ja sitoutetaan heidät
- monipuoliset ja kattavat suorituskyvyn mittarit, kannustimet ja palkitsemisen, joilla ohjataan vastuulliseen toimintaan.

Edellä kuvatut piirteet täyttävällä ohjausympäristöllä on kokonaisvaltainen vaikutus kaikkeen sisäiseen valvontaan.

### Riskien arviointi

Jokainen organisaatio kohtaa monenlaisia ulkoisia ja sisäisiä riskejä. Riski määritellään mahdolliseksi tapahtumaksi, joka vaikuttaa haitallisesti tavoitteiden saavuttamiseen. Riskinarviointi on dynaaminen ja jatkuva prosessi, jossa tunnistetaan ja arvioidaan tavoitteiden saavuttamiseen vaikuttavia riskejä. Tavoitteiden saavuttamista uhkaavat riskit arvioidaan suhteessa määriteltyyn riskinsietokykyyn.

26.8.2015

lished risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

### **Control Activities**

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

### **Information and Communication**

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound com-

Riskien arviointi luo siten perustan sille, miten riskit hallitaan. Riskienarvioinnin edellytyksenä on tavoitteiden asettaminen ja niiden vieminen organisaation eri tasoille. Johto asettaa selkeät tavoitteet toiminnalle, raportoinnille ja vaatimustenmukaisuudelle voidakseen tunnistaa ja arvioida riskejä suhteessa näihin tavoitteisiin. Lisäksi johto arvioi, ovatko tavoitteet edelleen soveltuvia organisaatiolle. Riskien arviointi edellyttää myös, että johto ottaa huomioon ulkoisen toimintaympäristön ja sisäisen toimintamallin mahdollisten muutosten vaikutukset sisäisen valvonnan tuloksellisuuteen.

### **Valvontatoimenpiteet**

Valvontatoimenpiteet ovat politiikoissa ja ohjeissa määriteltyjä toimia, joilla varmistetaan, että johdon määräykset tavoitteiden saavuttamista uhkaavien riskien hallitsemiseksi toteutetaan. Valvontatoimenpiteitä toteutetaan organisaation kaikilla tasoilla, toimintaprosessien eri vaiheissa ja järjestelmäympäristöissä. Ne voivat olla luonteeltaan ennaltaehkäiseviä tai tunnistavia. Ne voivat rakentua erilaisista automaattisista ja manuaalisista valvontatoimenpiteistä, kuten esimerkiksi käyttöoikeuksista, hyväksymisistä, varmistuksista, täsmäytyksistä ja toiminnan tuloksellisuuden arvioinneista. Tehtävien eriyttäminen on tyypillinen tapa toteuttaa valvontatoimenpiteitä. Mikäli tehtävien eriyttäminen ei ole käytännössä mahdollista, johto kehittää korvaavia valvontatoimenpiteitä.

### **Tieto ja viestintä**

Tieto ja viestintä ovat välttämättömiä sille, että tavoitteiden saavuttamista tukevat organisaation sisäisen valvonnan vastuut toteutuvat. Johto käyttää tuottamaansa tai sisäisistä ja ulkoisista lähteistä hankkimaansa olennaista ja laadukasta tietoa, joka tukee sisäisen valvonnan muiden osa-alueiden toimivuutta. Viestintä on jatkuva prosessi, jossa tarvittavaa tietoa jaetaan ja vastaanotetaan. Sisäinen viestintä tarkoittaa tiedon jakamista organisaatiossa alhaalta ylös, ylhäältä alas ja sivusuunnassa. Viestinnän avulla ylin johto osoittaa henkilöstölle valvontavastuiden tärkeyden. Ulkoinen viestintä on kaksisuuntaista: se mahdollistaa olennaisen ulkoisen tiedon saamisen ja sen avulla viestitään ulkoisille sidosryhmille näiden vaatimusten ja odotusten

26.8.2015

munication of relevant external information, and it provides information to external parties in response to requirement and expectations.

mukaisesti.

### **Monitoring Activities**

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

### **Seurantatoimenpiteet**

Jatkuvia tai erillisiä arviointeja tai niiden yhdistelmiä käytetään varmistamaan kunkin viiden sisäisen valvonnan osatekijän – mukaan lukien niihin sisältyviin periaatteisiin vaikuttavien valvontatoimien - olemassa olo ja toimivuus. Jatkuvat arvioinnit, jotka sisältyvät toimintaprosesseihin organisaation eri tasoilla, tuottavat ajantasaista tietoa. Säännöllisesti tehtävät erilliset arvioinnit vaihtelevat laajuudeltaan ja toistumistiheydeltään riippuen riskien arvioinnista, jatkuvien arviointien tuloksellisuudesta ja muista johdon huomioista. Havaintoja arvioidaan lainsäätäjän ja viranomaisten, standardeja asettavien yleisesti tunnustettujen tahojen tai johdon ja hallituksen määrittämien kriteerien perusteella. Havaitut poikkeamat viestitään tarkoituksenmukaisella tavalla johdolle ja hallitukselle.

## **RELATIONSHIP OF OBJECTIVES AND COMPONENTS**

A direct relationship exists between *objectives*, which are what an entity strives to achieve, *components*, which represent what is required to achieve the objectives, and *organizational structure* of the entity (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube.

## **TAVOITTEIDEN JA OSATEKIJÖIDEN VÄLINEN SUHDE**

Tavoitteet (se, mitä organisaatio pyrkii saavuttamaan), osatekijät (ne, jotka vaaditaan tavoitteiden saavuttamiseksi) ja organisaation rakenne (toiminnalliset yksiköt, juridiset yksiköt ja muut) ovat suorassa suhteessa toisiinsa. Suhteita voidaan kuvata kuutiona.

26.8.2015



- The three categories of objectives – operations, reporting, and compliance – are represented by the columns.
- The five components are represented by the rows.
- An entity's organization structure is represented by the third dimension.
- Tavoitteiden kolme kategorialla (toiminta, raportointi ja vaatimusten mukaisuus) on kuvattu pylväinä
- Viisi osatekijää on kuvattu riveinä.
- Organisaation rakenne on kuvattu kolmantena ulottuvuutena.

## COMPONENTS AND PRINCIPLES

The *Framework* sets out seventeen principles representing the fundamental concepts associated with each component. Because these principles are drawn directly from the components, an entity can achieve effective internal control by applying all principles. All principles apply to operations, reporting, and compliance objectives. The principles supporting the components are listed below.

### Control environment

1. The organization<sup>3</sup> demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal

## OSATEKIJÄT JA PERIAATTEET

Coso-ajatusmallissa on 17 periaatetta, jotka kuvaavat jokaiseen osatekijään liittyvät peruskäsitteet. Nämä periaatteet on johdettu suoraan ajatusmallin osatekijöistä, joten organisaation sisäinen valvonta on tuloksellista kun näitä kaikkia periaatteita sovelletaan. Kaikki periaatteet soveltuvat niin toiminnan, raportoinnin kuin vaatimustenmukaisuudenkin tavoitteisiin. Osatekijöitä tukevat periaatteet on lueteltu alla.

### Ohjausympäristö

1. Organisaatio<sup>4</sup> osoittaa sitoutumisensa rehellisyyteen, oikeudenmukaisuuteen ja eettisiin arvoihin.
2. Hallitus osoittaa toiminnallaan olevansa riippumaton toimivasta johdosta, ja se valvoo sisäisen valvonnan kehittymistä ja toimivuutta.

<sup>3</sup> For purposes of the *Framework*, the "organization" is used to collectively capture the board, management, and other personnel, as reflected in the definition of internal control.

<sup>4</sup> Ajatusmallissa sanaa "organisaatio" käytetään sisäistä valvontaa koskevan määritelmän mukaisesti viittaamaan hallituksen, johdon ja muun henkilökunnan muodostamaan kokonaisuuteen.



26.8.2015

control.

- |  |   |
|--|---|
| 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | 3. Toimiva johto järjestää hallituksen valvomana sellaiset rakenteet, raportointisuhteet sekä tarkoituksenmukaiset toimivaltuudet ja vastuut, jotka tukevat tavoitteiden saavuttamista. |
| 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.                            | 4. Organisaatio osoittaa sitoutumisensa tavoitteiden mukaisen, ammattitaitoisen henkilöstön palkkaamiseen, kehittämiseen ja säilyttämiseen.   |
| 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.                                  | 5. Organisaatio huolehtii siitä, että henkilöstö toteuttaa sisäisen valvonnan vastuutaan tavoitteiden saavuttamiseksi.  |

### **Risk Assessment**

- |  |  |
|--|--|
| 6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.                              | 6. Organisaatio määrittelee tavoitteensa riittävän selkeästi, jotta tavoitteisiin liittyvät riskit voidaan tunnistaa ja arvioida.  |
| 7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | 7. Organisaatio tunnistaa tavoitteiden saavuttamiseen liittyviä riskejä kaikilla organisaatiotasolla ja analysoi niitä, jotta riskien hallintakeinoista voidaan päättää. |
| 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.   | 8. Organisaatio ottaa huomioon väärinkäytösten mahdollisuuden arvioidessaan tavoitteiden saavuttamiseen liittyviä riskejä.   |
| 9. The organization identifies and assesses changes that could significantly impact the system of internal control.  | 9. Organisaatio tunnistaa ja arvioi muutoksia, jotka voivat vaikuttaa olennaisesti sisäiseen valvontaan.   |

### **Riskien arviointi**

### **Control Activities**

- |  |  |
|--|--|
| 10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | 10. Organisaatio valitsee ja kehittää valvontatoimenpiteitä, jotka auttavat hallitsemaan tavoitteiden saavuttamista uhkaavia riskejä ja saattamaan ne hyväksyttävälle tasolle. |
| 11. The organization selects and develops general control activities over technology to support the achievement of objectives.                                 | 11. Organisaatio valitsee ja kehittää yleisiä tieto- ja muihin teknologioihin kohdistuvia valvontatoimenpiteitä, jotka tukevat tavoitteiden saavuttamista.                     |
| 12. The organization deploys control activities through policies that establish what is expected   | 12. Organisaatio toteuttaa valvontatoimenpiteitä periaattein, jotka määrittelevät odotukset sekä   |

### **Valvontatoimenpiteet**

26.8.2015

and procedures that put policies into action.

menettelytavoin, joilla periaatteet pannaan toimeen.

### **Information and Communication**

### **Tieto ja viestintä**

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

13. Organisaatio hankkii tai tuottaa ja käyttää olennaista ja laadukasta tietoa tukeakseen sisäisen valvonnan toimivuutta.
14. Organisaatio viestii sisäisesti tietoa, mukaan lukien sisäisen valvonnan tavoitteet ja vastuut, joka on välttämätöntä sisäisen valvonnan toimivuuden tukemiseksi.
15. Organisaatio viestii ulkoisten sidosryhmien kanssa asioista, jotka vaikuttavat sisäisen valvonnan toimivuuteen.

### **Monitoring Activities**

### **Seurantatoimenpiteet**

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

16. Organisaatio valitsee, kehittää ja tekee jatkuvia ja/tai erillisiä arviointeja varmentaa sisäisen valvonnan osa-alueiden olemassaolon ja toimivuuden.
17. Organisaatio arvioi sisäistä valvontaa ajantasaisesti ja viestii siinä ilmenneistä puutteista ja/tai toimimattomuudesta osapuolille, jotka ovat vastuussa korjaavien toimenpiteiden toteuttamisesta sekä tarvittaessa ylimmälle johdolle ja hallitukselle.

## **EFFECTIVE INTERNAL CONTROL**

## **TULOSELLINEN SISÄINEN VALVONTA**

The *Framework* sets forth the requirement for an effective system of internal control. An effective system provides reasonable assurance regarding achievement of an entity's objectives. An effective system of internal control reduces, to an acceptable level, the risk of not achieving an entity objective and may relate to one, two, or all three categories of objectives. It requires that:

Ajatusmalli esittää tuloksellisen sisäisen valvonnan edellytykset. Tuloksellinen valvonta tuottaa kohtuullisen varmuuden organisaation tavoitteiden saavuttamisesta. Tuloksellinen sisäinen valvonta saattaa organisaation tavoitteiden saavuttamista uhkaavat riskit hyväksyttävälle tasolle. Se voi liittyä johonkin tai useampiin edellä mainituista tavoiteryhmistä (toiminnan, raportoinnin ja vaatimustenmukaisuuden tavoitteet). Tuloksellinen sisäinen valvonta edellyttää seuraavaa:

26.8.2015

- Each of the five components and relevant principles is present and functioning. "Present" refers to the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives. "Functioning" refers to the determination that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objectives.
- The five components operate together in an integrated manner. "Operating together" refers to the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective. Components should not be considered discretely; instead, they operate together as an integrated system. Components are interdependent with a multitude of interrelationships and linkages among them, particularly the manner in which principles interact within and across components.
- Kaikki viisi osatekijää ja niihin kuuluvat periaatteet ovat käytössä ja toimivat. Ne ovat *käytössä* silloin, kun sisäisen valvonnan osatekijät ja niihin kuuluvat periaatteet on otettu huomioon määriteltyjen tavoitteiden saavuttamista tukevan sisäisen valvonnan suunnittelussa ja toimeenpanossa. Osatekijät ja periaatteet ovat *toimivia* silloin, kun käytössä olevat sisäisen valvonnan osatekijät ja niihin kuuluvat periaatteet sisältyvät toimintaan ja sen sisäiseen valvontaan.
- Kaikki viisi osatekijää toimivat yhdessä kokonaisuutena. 'Toimivat yhdessä' tarkoittaa, että kaikki viisi osatekijää yhdessä toimien vähentävät tavoitteiden saavuttamista uhkaavia riskejä hyväksyttävälle tasolle. Osatekijöitä ei pidä tarkastella erillisinä; sen sijaan ne toimivat kokonaisuutena. Osatekijöillä on moninaisia keskinäisiä riippuvuuksia, ja etenkin siinä, miten periaatteet vaikuttavat toisiinsa kunkin osatekijän sisällä ja niiden välillä.

When a major deficiency exists with respect to the presence and functioning of a component or relevant principle, or with respect to the components operating together in an integrated manner, the organization cannot conclude that it has met the requirements for an effective system of internal control.

Kun osatekijän tai asiaan kuuluvan periaatteen olemassa olossa tai toiminnassa ilmenee merkittäviä puutteita, organisaatio ei voi tehdä sellaista johtopäätöstä, että se täyttää tuloksellisen sisäisen valvonnan vaatimukset. Sama koskee osatekijöiden yhteistoiminnassa ilmeneviä merkittäviä puutteita.

When a system of internal control is determined to be effective, senior management and the board of directors have reasonable assurance, relative to the application within entity structure, that the organization:

Kun sisäinen valvonta todetaan tulokselliseksi, ylimmällä johdolla ja hallituksella on kohtuullinen varmuus - organisaation rakenne huomioon ottaen - seuraavista asioista:

- Achieves effective and efficient operations when external events are considered unlikely to have a significant impact on the achievement of objectives or where the organization can reasonably predict the nature and timing of external events and mitigate the impact to an acceptable level.
- Organisaation toiminta on tuloksellista ja tehokasta, kun ulkoisilla tapahtumilla ei todennäköisesti ole merkittävää vaikutusta tavoitteiden saavuttamiseen. Näin on myös silloin, kun organisaatio pystyy kohtuullisesti ennakoimaan ulkoisten tapahtumien luonteen ja ajoituksen sekä vähentämään niiden vaikutukset hyväksyttävälle tasolle.
- Understands the extent to which operations are managed effectively and efficiently when external events may have a significant impact on the achievement of objectives or where the organization can reasonably predict the nature and timing of external events and mitigate the impact to an acceptable level.
- Organisaatio ymmärtää, millaisia tuloksellisen ja tehokkaan hallinnan keinoja tarvitaan silloin, kun ulkoisilla tapahtumilla voi olla merkittävä vaikutus tavoitteiden saavuttamiseen. Näitä tarvitaan myös silloin, kun organisaatio pystyy kohtuullisesti ennakoimaan ulkoisten tapahtumien luonteen ja ajoituksen sekä

26.8.2015

vähentämään niiden vaikutukset hyväksyttävälle tasolle.

- Prepares reports in conformity with applicable rules, regulations, and standards or with the entity's specified reporting objectives.
- Organisaation raportointi on sääntöjen, säädösten, standardien ja organisaation määriteltyjen raportointitavoitteiden mukaista.
- Complies with applicable laws, rules, regulations, and external standards.
- Organisaatio noudattaa lakeja, sääntöjä, säädöksiä ja ulkoisia standardeja.

The *Framework* requires judgment in designing, implementing, and conducting internal control and assessing its effectiveness. The use of judgment, within boundaries established by laws, rules, regulations, and standards, enhances management's ability to make better decisions about internal control, but cannot guarantee perfect outcomes.

Ajattelumalli edellyttää harkintaa sisäisen valvonnan suunnittelussa, toimeenpanossa ja toteutuksessa sekä sen tuloksellisuuden arvioinnissa. Lakien, sääntöjen, säädösten ja standardien mahdollistama harkinta edistää johdon kykyä tehdä oikeita päätöksiä sisäisestä valvonnasta, joskaan ei takaa täydellistä lopputulosta.

## LIMITATIONS

The *Framework* recognizes that while internal control provides reasonable assurance of achieving the entity's objectives, limitations do exist. Internal control cannot prevent bad judgment or decisions, or external events than can cause an organization to fail to achieve its operational goals. In other words, even an effective system of internal control can experience a failure. Limitation may result from the:

- Suitability of objectives established as a precondition to internal control
- Reality that human judgment in decision making can be faulty and subject to bias
- Breakdowns that can occur because of human failures such as simple errors
- Ability of management, other personnel, and/or third parties to circumvent controls through collusion
- External events beyond the organization's control

These limitations preclude the board and management from having absolute assurance of the achievement of the entity's objectives – that is, internal control provides reasonable but not absolute assurance. Notwithstanding these inherent limitations, management should be aware of them when

## RAJOITUKSET

Vaikka ajattelumallin mukaan sisäinen valvonta antaa kohtuullisen varmuuden organisaation tavoitteiden saavuttamisesta, siihen sisältyy rajoituksia. Sisäinen valvonta ei voi estää virhearviointeja, huonoja päätöksiä eikä ulkoisia tapahtumia, jotka voivat estää organisaatiota saavuttamasta tavoitteitaan. Tuloksellisestikin järjestetty sisäinen valvonta voi osin epäonnistua. Rajoitukset voivat johtua seuraavista asioista:

- Asetetut tavoitteet eivät ole sisäisen valvonnan kannalta asianmukaisia.
- Inhimillinen päätöksenteko voi olla virheellistä ja ennakkoluuloihin perustuvaa.
- Epäonnistuminen voi aiheutua inhimillisistä, tahattomista virheistä.
- Johto, muu henkilöstö ja/tai kolmas osapuoli voivat tahallisesti kiertää sääntöjä.
- Ulkoiset tapahtumat, joita organisaatio ei pysty hallitsemaan.

Yllä mainituista rajoituksista johtuen hallituksen ja johdon on mahdotonta saavuttaa täydellistä varmuutta organisaation tavoitteiden saavuttamisesta. Sisäinen valvonta antaa siis kohtuullisen mutta ei täydellistä varmuutta. Johdon tulisi olla tietoinen näistä rajoituksista valitessaan,

26.8.2015

selecting, developing, and deploying controls that minimize, to the extent practical, these limitations.

kehittäessään ja toimeenpannessaan valvontakeinoja, jotka saattavat nämä rajoitukset siedettävälle tasolle.

## **USING THE INTERNAL CONTROL – INTEGRATED FRAMEWORK**

## **SISÄISEN VALVONNAN – KOKONAISVALTAISEN AJATUSMALLIN KÄYTTÖ**

How this report can be used depends on the roles of the interested parties:

Tämän ajatusmallin käyttötapa riippuu eri osapuolten rooleista:

- *The Board of Directors* – The board should discuss with senior management the state of the entity's system of internal control and provide oversight as needed. Senior management is accountable for internal control and to the board of directors, and the board needs to establish its policies and expectations of how members should provide oversight of the entity's internal control. The board should be apprised of the risks to the achievement of the entity's objectives, the assessments of internal control deficiencies, the management actions deployed to mitigate such risks and deficiencies, and how management assesses the effectiveness of the entity's system of internal control. The board should challenge management and ask the tough questions, as necessary, and seek input and support from internal auditors, external auditors, and others. Sub-committees of the board often can assist the board by addressing some of these oversight activities.
- *Senior Management* – Senior management should assess the entity's system of internal control in relation to the *Framework*, focusing on how the organization applies the seventeen principles in support of the components of internal control. Where management has applied the 1992 edition of the framework, it should first review the updates made to this version (as noted in Appendix F of the *Framework*), and consider implications of those updates to the entity's system of internal control. Management may consider using the *Illustrative Tools* as part of this initial comparison and as on ongoing evaluation of the overall effectiveness of the entity's system of internal control.
- *Hallitus* – Hallituksen tulee keskustella ylimmän johdon kanssa organisaation sisäisen valvonnan tilasta ja tarjota tarvittaessa ohjausta. Ylin johto vastaa sisäisestä valvonnasta hallitukselle. Hallituksen tulee luoda toimintaperiaatteita ja tavoitteita sille, miten se tarjoaa organisaation sisäisen valvonnan ohjausta. Hallitukselle tulee kertoa niistä riskeistä, jotka uhkaavat tavoitteiden saavuttamista sekä sisäisen valvonnan heikkouksien arvioinneista. Lisäksi hallitukselle tulee kertoa johdon toimenpiteistä, joilla tällaisia riskejä hallitaan ja heikkouksia parannetaan sekä miten tulokselliseksi johto arvioi organisaation sisäisen valvonnan. Hallituksen tulee haastaa johtoa ja esittää tarpeen vaatiessa kysymyksiä ja pyytää näkemystä ja tukea sisäisiltä tarkastajilta, tilintarkastajilta ja muilta tahoilta. Lisäksi hallituksen valiokunnat voivat avustaa hallitusta valmistelemalla ohjaukseen liittyviä toimenpiteitä.
- *Ylin johto* – Ylimmän johdon tulee arvioida organisaation sisäistä valvontaa ajatusmallin mukaisesti. Arvioinnissa tulee keskittyä siihen, miten organisaatio toteuttaa niitä ajatusmallin seitsemäätoista periaatetta, jotka tukevat sisäisen valvonnan osatekijöitä (ohjausympäristö, riskien arviointi, valvontatoimenpiteet, tieto ja viestintä ja seurantatoimenpiteet). Mikäli johto on soveltanut vuoden 1992 ajatusmallia, sen tulee ensin käydä läpi nykyisen ajatusmallin tuomat muutokset (ks. alkuperäiskielisen *ajatusmallin* liite F, *Summary of Changes to the COSO Internal Control - Integrated Framework*) ja harkita miten päivitykset vaikuttavat organisaation sisäiseen valvontaan. Johto voi harkita *Illustrative Tools* -ohjeen käyttöä osana tätä alustavaa vertailua sekä organisaation

26.8.2015

sisäisen valvonnan tuloksellisuutta jatkuvasti arvioitaessa.

- *Other Management and Personnel* – Managers and other personnel should review the changes made to this version and assess implications of those changes on the entity’s system of internal control. In addition, they should consider how they are conducting their responsibilities in light of the *Framework* and discuss with more senior personnel ideas for strengthening internal control. More specifically, they should consider how existing internal controls affect the relevant principles within the five components of internal control.
- *Internal Auditors* – Internal auditors should review their internal audit plans and how they applied the 1992 edition of the framework. Internal auditors also should review in detail the changes made to this version and consider possible implications of those changes on audit plans, evaluations, and any reporting on the entity’s system of internal control.
- *Independent Auditors* – In some jurisdictions, an independent auditor is engaged to audit or examine the effectiveness of the client’s internal control over financial reporting in addition to auditing the entity’s financial statements. Auditors can assess the entity’s system of internal control in relation to the *Framework*, focusing on how the organization has selected, developed, and deployed controls that affect the principles within the components of internal control. Auditors, similar to management, may use the *Illustrative Tools* as part of this evaluation of the overall effectiveness of the entity’s system of internal control.
- *Other Professional Organizations* – Other professional organizations providing guidance on operations, reporting, and compliance may consider their standards and guidance in comparison to the *Framework*. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- *Educators* – With the presumption that the *Framework* attains broad acceptance, its con-
- *Muu johto ja henkilöstö* – Johtajien ja muun henkilöstön tulisi tutustua nykyisen version tuomiin muutoksiin ja arvioida muutosten vaikutuksia organisaation sisäiseen valvontaan. Lisäksi heidän tulisi harkita *ajatusmallin* pohjalta, miten he toteuttavat sisäisen valvonnan velvollisuutensa ja keskustella kokeneemman henkilöstön kanssa siitä, miten sisäistä valvontaa voidaan parantaa. Heidän tulisi erityisesti harkita miten nykyiset valvontatoimenpiteet vastaavat niitä olennaisia periaatteita, jotka sisältyvät sisäisen valvonnan viiteen osatekijään.
- *Sisäinen tarkastus* – Sisäisen tarkastuksen tulisi käydä läpi tarkastussuunnittelunsa ja miten siinä on toteutettu vuoden 1992 ajatusmallia. Sisäisen tarkastuksen tulisi käydä läpi yksityiskohtaisesti nykyisen version tuomat muutokset ja harkita muutosten mahdolliset vaikutukset tarkastussuunnitteluun, arviointeihin ja kaikkeen organisaation sisäisen valvonnan raportointiin.
- *Tilintarkastus ja muu ulkopuolinen tarkastus* – Laki voi edellyttää, että tilintarkastaja on velvollinen tarkastamaan tai arvioimaan asiakkaan sisäisen valvonnan tuloksellisuutta liittyen taloudelliseen raportointiin sen lisäksi, että hän tarkastaa organisaation tilinpäätöksen oikeellisuutta. Tilintarkastajat ja muut ulkopuoliset tarkastajat voivat arvioida sisäistä valvontaa *ajatusmallin* avulla. Arvioinnissa he voivat keskittyä siihen, miten organisaatio on valinnut, kehittänyt ja ottanut käyttöön valvontatoimenpiteitä siten, että ne vastaavat sisäisen valvonnan osatekijöiden periaatteita. Ulkopuoliset tarkastajat voivat johdon tavoin käyttää *Illustrative Tools* -ohjetta arvioidessaan koko organisaation sisäisen valvonnan tuloksellisuutta.
- *Muut ammatilliset järjestöt* – Muut ammatilliset järjestöt, jotka ohjeistavat toimintaa, raportointia ja vaatimustenmukaisuutta, voivat arvioida, miten heidän standardinsa ja ohjeistuksensa vastaavat ajatusmallia. Kun käytetään samoja käsitteitä ja termejä, kaikki osapuolet hyötyvät.
- *Koulutuksen tarjoajat* – Olettaen, että *ajatusmalli* saa laajaa hyväksyntää, sen käsitteet

26.8.2015

cepts and terms should find their way into university curricula.

ja termit sisällytetään opetusohjelmiin.