

Sisällys

Esipuhe	VIII
1 Johdanto	1
1.1 Miksi jokaisen organisaation tulisi olla kiinnostunut sisäisestä valvonnasta?	1
1.2 Mitä on sisäinen valvonta?	3
1.2.1 Sisäisen valvonnan määritelmiä	3
1.2.2 Sisäisen valvonnan ja sisäisen tarkastuksen suhde	8
1.2.3 Tulokellinen sisäinen valvonta	9
1.2.4 Kontrollien testaus	11
1.2.5 Vastuu sisäisestä valvonnasta	12
1.2.6 Miksi sisäiseen valvontaan kannattaa investoida?	16
1.2.7 Sisäiseen valvontaan liittyvät rajoitteet	18
1.2.8 Merkkejä puutteellisesta valvonnasta	19
1.3 Sisäistä valvontaa koskeva lainsäädäntö ja ohjeistukset	21
1.3.1 Osakeyhtiölaki	21
1.3.2 Finanssivalvonnan standardi sisäisen valvonnan järjestämisestä	23
1.3.3 Sisäinen valvonta kuntasektorilla	24
1.3.4 Sisäinen valvonta valtion virastoissa ja laitoksissa	25
1.3.5 Suomen listayhtiöiden hallinnointikoodi	27
1.3.6 Listaamattomat yhtiöt	31
1.3.7 Sarbanes-Oxley-lainsäädäntö	33
1.4 Sisäisen valvonnan malleja ja viitekehyksiä	42
1.4.1 Kolmen linjan malli – Three Lines Model	42
1.4.2 COSO-malli	49
1.4.3 COSO-ERM-malli	56

2	Roolit ja vastuut sisäisessä valvonnassa – Kolmen linjan malli	61
2.1	Ylin johto, hallitus ja tarkastusvaliokunta	62
2.1.1	Ylimmän johdon rooli	63
2.1.2	Tarkastusvaliokunta	66
2.2	Ensimmäinen linja	71
2.2.1	Operatiivisen johdon vastuu	71
2.2.2	Esihenkilön vastuu	72
2.2.3	Työntekijän vastuu	73
2.3	Toinen linja	76
2.3.1	Riskienhallinta-toiminto	76
2.3.2	Compliance-toiminto	78
2.3.3	Muut toisen linjan toimijat	82
2.3.4	Kolmas linja - sisäinen tarkastus	83
2.4	Tilintarkastus	92
2.4.1	Tilintarkastuksen tehtävät ja vastuut	92
2.4.2	Tilintarkastuksen riippumattomuus ja raportointi	93
2.4.3	Tilintarkastuksen ja sisäisen tarkastuksen yhteistyö	94
3	Sisäisen valvonnan osa-alueet	97
3.1	Ohjausympäristö – johtamistapa ja valvontakulttuuri	97
3.1.1	Periaate 1: Sitoutuminen integriteettiin ja eettisiin arvoihin	99
3.1.2	Periaate 2: Hallituksen riippumattomuus ja valvontavastuu	105
3.1.3	Periaate 3: Organisaation rakenteet, raportointi- linjat ja tarkoituksenmukaiset toimivaltuudet	107
3.1.4	Periaate 4: Sitoutuminen kompetenssiin	110
3.1.5	Periaate 5: Tilivelvollisuus	112
3.2	Riskien arviointi	117
3.2.1	Periaate 6: Selkeät tavoitteet	118
3.2.2	Periaate 7: Riskien tunnistaminen ja analysointi	119
3.2.3	Periaate 8: Väärinkäytösrisikin arviointi	126
3.2.4	Periaate 9: Muutosten tunnistaminen ja arviointi	133

3.3	Valvontatoimenpiteet – toimintaohjeet ja menettelytavat	135
3.3.1	Periaate 10: Valvontatoimenpiteiden valinta ja kehittäminen	137
3.3.2	Periaate 11: Tietojärjestelmäkontrollien valinta ja kehittäminen	143
3.3.3	Periaate 12: Toimintaohjeet ja menettelytavat	145
3.4	Informaatio ja viestintä	150
3.4.1	Periaate 13: Relevantin tiedon käyttäminen	151
3.4.2	Periaate 14: Sisäinen viestintä	153
3.4.3	Periaate 15: Ulkoinen viestintä	159
3.5	Seurantatoimenpiteet	162
3.5.1	Periaate 16: Jatkuva seuranta ja erilliset arvioinnit	162
3.5.2	Periaate 17: Puutteiden arviointi ja kommunikointi	165
4	Sisäisen valvonnan kehittäminen organisaatiossa	169
4.1	Motivaatio organisaation sisäisen valvonnan kehittämiseksi	169
4.1.1	Miksi sisäistä valvontaa halutaan kehittää?	170
4.1.2	Mitä sisäinen valvonta organisaatiossa tarkoittaa?	172
4.2	Askel 1: Ohjausympäristön ja yritystason kontrollien määrittely	175
4.3	Askel 2: Avainprosessien tunnistaminen ja dokumentointi	178
4.4	Askel 3: Avainkontrollien tunnistaminen ja dokumentointi	181
4.4.1	Kontrollikatalogit dokumentoinnin työkaluksi	183
4.4.2	Miksi dokumentoida?	183
4.4.3	Kontrollien omistajat	184
4.5	Askel 4: Sisäisen valvonnan jalkauttaminen	185
4.6	Askel 5: Sisäisen valvonnan tuloksellisuuden arviointi	186
4.6.1	Tilintarkastus	187
4.6.2	Sisäinen tarkastus	188
4.6.3	Vertaisarviointi	190
4.6.4	Itsearviointi	191

4.6.5	Jatkuva poikkeamien raportointi	197
4.7	Askel 6: Valvonnan ja ohjauksen jatkuva kehittäminen	198
5	Riskit ja kontrollit organisaation eri toiminnoissa	201
5.1	Hankintaprosessi	201
5.1.1	Tyypilliset riskit ja kontrollitavoitteet	202
5.1.2	Hankintaprosessi ja keskeiset kontrollit	205
5.1.3	Hankintojen analyttinen tarkastelu	218
5.1.4	Työtehtävien eriyttäminen hankintaprosessissa	219
5.2	Myyntiprosessi	219
5.2.1	Tyypilliset riskit ja kontrollitavoitteet	220
5.2.2	Myyntiprosessi ja keskeiset kontrollit	222
5.2.3	Myyntin analyttinen tarkastelu	236
5.2.4	Työtehtävien eriyttäminen myyntiprosessissa	236
5.3	Valmistusprosessi ja varastonhallinta	237
5.3.1	Tyypilliset riskit ja kontrollitavoitteet	237
5.3.2	Valmistusprosessin ja varastonhallinnan keskeiset kontrollit	238
5.3.3	Valmistuksen ja varaston analyttinen tarkastelu	241
5.3.4	Työtehtävien eriyttäminen varastonhallinnassa	242
5.4	Henkilöstö- ja palkkahallinto	242
5.4.1	Tyypilliset riskit ja kontrollitavoitteet	243
5.4.2	Henkilöstö- ja palkkahallinnon keskeiset kontrollit	246
5.4.3	Työtehtävien eriyttäminen henkilöstöhallinnossa	263
5.5	Taloushallinto	264
5.5.1	Tyypilliset riskit ja kontrollitavoitteet	264
5.5.2	Keskeiset kontrollit taloushallinnossa	265
5.6	Tietohallinto	268
5.6.1	Yleiset IT-kontrollit	269
5.6.2	Sovelluskontrollit	272

6	Väärinkäytökset ja eettiset ilmoituskanavat	275
6.1	Taustaa ja tilastoja väärinkäytöksistä	275
6.1.1	Määritelmä	275
6.1.2	Väärinkäytöksistä aiheutuvat seuraukset organisaatioille	279
6.1.3	Kuka väärinkäytöksiä tekee?	279
6.1.4	Minkälaisia väärinkäytöksiä tehdään?	280
6.1.5	Miksi väärinkäytöksiä tehdään?	283
6.2	Kontrollit väärinkäytösriskin hallinnassa	285
6.2.1	Ehkäisevät kontrollit	286
6.2.2	Paljastavat kontrollit	294
6.3	Eettiset ilmoituskanavat	299
6.3.1	EU:n ilmoittajia suojaavan direktiivin vaikutukset organisaatioihin	300
6.3.2	Ilmoituskanavan suunnittelussa ja käytössä huomioitavia seikkoja	304
6.3.3	Ilmoitusten käsittely	309
6.3.4	Yhteenveto	311
6.4	Väärinkäytösten selvittäminen ja tutkinta	313
6.4.1	Väärinkäytöstutkinnan aloittaminen	314
6.4.2	Suunnittelu	315
6.4.3	Tiedon kerääminen ja faktojen arviointi	317
6.4.4	Raportointi	321
6.4.5	Seuraamukset ja korjaavat toimenpiteet	321
6.5	Roolit ja vastuut väärinkäytösriskin hallinnassa	324
6.5.1	Johto	324
6.5.2	Compliance-toiminnon rooli	324
6.5.3	Sisäisen tarkastuksen rooli	324
6.5.4	Tilintarkastajan rooli	326
6.5.5	Ulkoisen asiantuntijan rooli	328
6.5.6	Jokaisen työyhteisön jäsenen vastuu	329
7	Yhteenveto	331

Lähteet	333
----------------	-----

Liitteet

Liite 1: Esimerkki kontrollikatalogista (hankinnat)	338
Liite 2: Sisäisen valvonnan arviointilomake	342
Liite 3: Esimerkki poikkeamaraportoinnista	346
Liite 4: Tarkistuslista eettisten- ja väärinkäytösriskien arvioimiseksi	348