

# 1. Innehållsförteckning

<b>1.</b>	<b>Förord</b>	<b>7</b>
<b>2.</b>	<b>Introduktion</b>	<b>9</b>
2.1	Syfte	11
2.2	Målgrupp	12
2.3	Varför säkerhetsarbete?	12
<b>3.</b>	<b>Omvärlden</b>	<b>14</b>
3.1	Hotbilden	14
3.2	Hur gör andra?	16
3.2.1	Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen	16
3.2.2	Enkät – “Get Ready for ISO 27000”	18
3.3	Trender	19
3.3.1	Riskstyrt säkerhetsarbete	22
3.4	Säkerhetsåtgärder	23
3.5	Direktiv, lagar, normer, standarder och ramverk – men vad är vad?	23
3.6	Verksamhetssystemets innehåll	26
3.7	OECD:s riktlinjer för säkerheten i informationssystem och nät	26
3.7.1	På väg mot en säkerhetskultur	26
3.7.2	Mål	27
3.7.3	Principer	27
<b>4.</b>	<b>Krav på ledning, styrning och kontroll</b>	<b>31</b>
4.1	Krav på säkerhetsarbetet	31
4.2	Den strategiska inriktningen för säkerhetsarbetet	32
4.3	Mål och målstyrning	33
4.4	Ekonomisk styrning	34
4.5	Säkerhetsprocessen	35
<b>5.</b>	<b>SS-ISO/IEC 27002:2005-standardens som verktyg</b>	<b>36</b>
5.1	Kapitel	36
5.2	Huvudområden för säkerhet	36
5.3	Att arbeta med säkerhet utifrån VAD till HUR och inte tvärtom!	37
5.4	Arbetsättet P-D-C-A	39
5.4.1	Processinriktning	39
5.5	Standarden SS-ISO/IEC 27002:2005 krav på säkerhetsorganisationen	42

<b>6.</b>	<b>Principer för en effektiv säkerhetsorganisation</b>	<b>49</b>
6.1	Säkerhetsfunktionens uppdrag	50
6.2	Övergripande beskrivning av säkerhetsprocessen	51
6.3	Säkerhetsaspekter	52
6.3.1	Vilka aspekter ska man arbeta efter?	52
6.4	Tillräckligt bra säkerhetsnivå	53
<b>7.</b>	<b>Vem är ansvarig</b>	<b>55</b>
7.1	Ledningens ansvar	57
7.2	Avdelningschefernas ansvar	58
7.3	Säkerhetsfunktionens ansvar	61
7.4	Enheter eller funktioner med utökade säkerhetsuppgifter	62
7.5	Krisledningsgruppen	63
7.6	Säkerhetskommitté/-råd	63
7.7	Medarbetares ansvar	64
<b>8.</b>	<b>Att mäta säkerhet eller säkerhetsorganisationen</b>	<b>65</b>
8.1	Vad är det som ska mätas inom säkerhetsområdet?	65
8.2	Verktyg för att mäta säkerhetsfunktionens arbete	71
8.2.1	Inledning	71
8.2.2	Säkerhetsfunktionens organisation och bedrivande	71
8.2.3	Oberoende och objektivitet	71
8.2.4	Kompetens och vederbörlig yrkesskicklighet	72
8.2.5	Kvalitetssäkring och kvalitetsförbättring	73
8.2.6	Leda säkerhetsfunktionen	73
8.2.7	Arbetets beskaffenhet	74
8.2.8	Planera uppdrag	74
8.2.9	Utföra åtagandet	75
8.2.10	Kommunicera resultat	76
8.2.11	Övervaka framsteg	76
<b>9.</b>	<b>Förankring av säkerhetsarbetet</b>	<b>78</b>
<b>10.</b>	<b>Säkerhetsfunktionens organisationsstruktur</b>	<b>80</b>
10.1	Säkerhetsentreprenör som organisationsbyggare	81
10.2	Rollen säkerhets- informationssäkerhetschef	81
10.3	Var ska säkerhetschefen organisatoriskt placeras?	82
10.4	Vad ska säkerhets- infosäkerhetschef heta?	82

10.5	Relation mellan CIO och säkerhetschef? Trend med att säkerhetschefen är ägare till komponenter i IT-infrastrukturen.	83
10.6	Något om budget för säkerhetsarbetet.	84
10.7	Evolutionen av hur säkerhetsarbetet är organiserat	85
10.8	Behovet av ett regelverk för säkerhetsarbetet?	86
10.8.1	Regelverkets uppbyggnad och dess fastställare	88
10.8.2	Exempel på regelverk	89
10.9	Efterlevnad	91
<b>11.</b>	<b>Rekrytering och löneläge</b>	<b>93</b>
11.1	Löneläge	93
11.2	Kompetenskrav	94
11.3	Chefsrollen	95
11.4	Synen på dig som säkerhetschef med ett chefsansvar	98
<b>12.</b>	<b>Beskrivning av en organisationsmodell för en säkerhetsorganisation</b>	<b>100</b>
<b>13.</b>	<b>Verksamhetsbeskrivning av en säkerhetsfunktion</b>	<b>103</b>
13.1	Inledning	103
13.1.1	Säkerhetsfunktionens ledningsfilosofi	103
13.2	Säkerhetsfunktionens mål för säkerhetsarbetet	104
13.3	Inhämtning/bearbetning/delgivning av information för att skapa kunskap	104
13.4	Organisationsstruktur	105
13.5	Fysisk placering och SÄKs utrustning	106
13.6	Strategiskt, taktiskt och operativt säkerhetsarbete	106
13.7	”Kunder”/Relationer internt	107
13.8	Våra ”kunders” behov	109
13.9	Sekretesskrav på säkerhetsfunktionens verksamhet	109
13.10	”Affärsidé” för säkerhetsfunktionen	109
13.11	Krav på säkerhetsfunktionen	110
13.12	Säkerhetskrav på funktionen	112
<b>14.</b>	<b>Exempel på en rollbeskrivning för säkerhetschefen</b>	<b>116</b>
14.1	Organisatorisk placering	116
14.2	Närmaste chef	116
14.3	Ansvar och befogenheter	116
14.3.1	Säkerhetsfunktionens ansvar	116
14.4	Säkerhetsfunktionens uppgift och grundläggande värderingar	118

14.5	Nödvändiga kunskaper och erfarenheter	119
14.6	Villkor	120
14.7	Säkerhetsfunktionens ansvar:	120
14.8	Rollschema inom säkerhetsfunktionen	122
<b>15.</b>	<b>P-D-C-A för att bygga upp säkerhetsorganisationen</b>	<b>123</b>
15.1	Planera	123
15.2	Genomföra	123
15.3	Följa upp	123
15.4	Förbättra	123
15.5	Resultatet – verksamhetens säkerhetsprocess	123
<b>16.</b>	<b>Bilaga: roller och ansvar för informationssäkerheten kopplat till olika målgrupper</b>	<b>125</b>
16.6	Roller och ansvar för informationssäkerhetsområdet – kopplat till olika målgrupper	125
16.7	Roller och ansvar sorterat per område	143
<b>17.</b>	<b>Bilaga: Checklista för att verifiera säkerhetsnivån</b>	<b>155</b>
17.1	Säkerhetsledning och organisation	155
17.1.1	Ledning	155
17.1.2	Organisation	160
17.1.3	Ansvar	163
17.1.4	Utbildning/medvetenhet	165
17.1.5	Central BKS-administration	167
17.1.6	Ekonomiskt skydd	168
17.1.7	Legala krav	170
17.1.8	Interna regler och avtal	173
17.1.9	Hantering av utrustning	175
17.1.10	Incidenthantering	176
17.1.11	Projektering/anskaffning	178
17.1.12	Kontroll	179
17.1.13	Hantering av tekniska sårbarheter	180
17.1.14	Identifiering av risker med utomstående parter	182
17.1.15	Hantering av säkerhet vid kundkontakter	185
17.1.16	Hantering av säkerhet i tredje partsavtal	187
17.1.17	Förteckning över tillgångar	192
17.1.18	Ägarskap för tillgångar	193
17.1.19	Godtagbar användning av tillgångar	194
<b>18.</b>	<b>Källor</b>	<b>195</b>
<b>19.</b>	<b>Bifogad Cd</b>	<b>195</b>