

*Martin Brogaard Nielsen &  
Isabella Ørgaard Jensen*

# it-revision og it-styring

– en håndbog

 KARNOV  
GROUP

Martin Brogaard Nielsen, Isabella Ørgaard Jensen og Mie Olsen  
*it-revision og it-styring – en håndbog*  
1. udgave/1. oplag  
© Karnov Group Denmark A/S, København 2023

ISBN 978-87-619-4411-5

Omslag: Torben Lundsted, Korsør  
Sats: Integra, Indien  
Tryk: Sowa Sp. z o.o., Polen

Denne bog er beskyttet i medfør af gældende dansk lov om ophavsret. Kopiering må kun ske i overensstemmelse med loven. Det betyder f.eks., at kopiering til undervisningsbrug kun må ske efter aftale med Copydan Tekst og Node. Alle rettigheder forbeholdes.

# Indholdsfortegnelse

<b>Forord</b> .....	9
<b>1. En proaktiv tilgang til styring af it.</b> .....	11
1.1. It: Virksomhedens “Black Box-problem” .....	12
1.2. Udviklingen er gået stærkt .....	14
1.3. Hvad er it-styring? .....	15
1.4. Risikoanalyse og inddragelse af ledelsen .....	18
1.5. En proaktiv tilgang til compliance .....	20
1.6. Hvorfor it-revision? .....	22
<b>2. Rammeværktøjer til styring af it-processer</b> .....	25
2.1. GRC: Governance, risk og compliance .....	26
2.2. Planlægning og almene standarder .....	28
2.3. Kortlægning af risici .....	31
2.4. Lovgivningsmæssige krav .....	35
2.5. Informationssikkerhedspolitik .....	37
2.6. Organisatorisk ansvarsfordeling .....	39
2.7. ISO: Et meget anvendt governance-rammeverk inden for it .....	40
2.8. Introduktion til ISO 27001/27002 .....	43
2.9. Implementering af et ISMS-system .....	45
<b>3. It-revision som disciplin</b> .....	49
3.1. Udviklingen fra EDB-revision .....	50
3.2. Regnskabsunderstøttende it-revision versus selvstændige erklæringer .....	52
3.2.1. Roller og yderligere specialisering som it-revisor ..	53
3.2.2. Erklæringsafgivende it-revisor (godkendt revisor) ..	54
3.2.3. It-infrastruktur .....	55
3.2.4. Baggrund og uddannelse .....	55
3.3. Et specielt kundeforhold .....	57
3.3.1. Underlagt revisorlov og opdagelsespligt .....	58
3.3.2. Intern og ekstern revision .....	59
3.3.3. It-revisors reaktive opgavetyper .....	60

3.3.4.	Dataanalyse . . . . .	60
3.3.5.	Assistance omkring risikovurdering . . . . .	61
3.3.6.	Assistance ifm. implementering af ISO/ISMS . . . . .	61
3.3.7.	Assistance ifm. implementering af databeskyttelsesforanstaltninger . . . . .	62
3.3.8.	Test og beredskab . . . . .	62
3.3.9.	Due diligence inden for it . . . . .	63
<b>4.</b>	<b>Tilrettelæggelse af it-revision . . . . .</b>	<b>65</b>
4.1.	Hvad er (it-) revision? . . . . .	66
4.2.	At påtage sig et kundeforhold som ekstern revisor. . . . .	67
4.3.	ISA 315: Forståelse for virksomheden og dens risici . . . . .	69
4.4.	Scope og grad af sikkerhed . . . . .	70
4.5.	Revisionsplanlægning og arbejdsplan . . . . .	72
4.6.	Partiel- og helhedsmetode . . . . .	76
4.6.1.	Helhedsmetoden . . . . .	76
4.6.2.	Partielmetoden. . . . .	77
4.7.	Brug af intern revisions arbejde . . . . .	77
4.8.	It-revision: Definition af kontrolbegreber. . . . .	78
4.9.	Samarbejde med den interne revision . . . . .	82
4.10.	It-revisors rapportering . . . . .	83
<b>5.</b>	<b>It-revision: Udførelse og metode . . . . .</b>	<b>87</b>
5.1.	Definition af kontroller og kontrolmål . . . . .	88
5.2.	I dybden med CIA-modellen . . . . .	89
5.3.	Revisionshandlinger og revisionsbevis . . . . .	91
5.4.	Dokumentation produceret af kunden (IPE) . . . . .	94
5.5.	Tests og metoder . . . . .	96
5.6.	Test af den resterende del af revisionsperioden . . . . .	100
5.7.	De 14 ISO-kontrolområder . . . . .	101
5.8.	Tidsramme og interaktion med kunden . . . . .	114
<b>6.</b>	<b>It-revision som led i den finansielle revision . . . . .</b>	<b>119</b>
6.1.	En regnskabsunderstøttende opgave . . . . .	120
6.2.	Den indledende vurdering af kundens it-afhængighed. . . . .	122
6.3.	Finansiel revisors valg af revisionsstrategi . . . . .	126
6.4.	It-revisors valg af revisionsstrategi . . . . .	129
6.5.	Værdi og samarbejde . . . . .	129
6.6.	Konklusion og rapportering ved GIK-rapport. . . . .	132
6.7.	Modtagelse af revisorerklæring. . . . .	134

<b>7. Gennemgang af databehandler og serviceleverandør</b> . . . . .	137
7.1. Hvad er en it-serviceleverandør? . . . . .	138
7.2. I hvilke situationer bruges it-revisors erklæring? . . . . .	140
7.3. Stort behov for at dokumentere GDPR-overholdelse. . . . .	142
7.4. Databehandler og dataansvarlig . . . . .	143
7.5. FSR's rapporteringseksempel for GDPR-gennemgang. . . . .	145
7.6. Kontraktuel forpligtelse og fornyelse. . . . .	150
7.7. Erklæringer – variationer . . . . .	152
<b>8. It-revisors arbejde med selvstændige erklæringer</b> . . . . .	155
8.1. Tre forskellige erklæringsformater . . . . .	156
8.1.1. ISAE 3402 . . . . .	157
8.1.2. ISAE 3000 . . . . .	158
8.1.3. ISRS 4400 . . . . .	159
8.2. SOC og ISO-certificering . . . . .	160
8.3. Opbygning af en erklæringsrapport. . . . .	161
8.4. Den indledende fase . . . . .	164
8.5. Projektstyring og -udførelse . . . . .	166
8.6. Konklusion og udformning af erklæringsrapport . . . . .	169
8.7. Eksempel på en revisionsproces . . . . .	171
<b>9. Databeskyttelseslovgivningen</b> . . . . .	175
9.1. Databeskyttelsesforordningen og den danske databeskyttelseslov . . . . .	176
9.2. Almindeligt versus følsomt persondata . . . . .	178
9.3. Lovlig indhentning og behandling . . . . .	180
9.4. En specialistkompetence . . . . .	181
9.5. Den dataansvarlige fører tilsyn med databehandleren . . . . .	182
9.6. Overførsel til tredjelande eller internationale organisationer . . . . .	186
9.7. I tilfælde af databrud . . . . .	188
9.8. Finansiell revisors fokus på databeskyttelse . . . . .	190
<b>10. It-revision i praksis: Udvalgte cases</b> . . . . .	193
10.1. GIK-revision af B2B-salgsvirksomhed fra it-revisors synspunkt . . . . .	194
10.2. Kundens oplevelse af en GIK-revision . . . . .	201
10.3. Erklæringsforløb. . . . .	205

<b>11. It-revisorfagets transition over de næste ti år</b> . . . . .	213
11.1. Kigger ind i rivende udvikling på flere fronter . . . . .	213
11.2. Auditering af blockchain-platforme . . . . .	214
11.3. AI: Automatiserede beslutninger og potentielle bias. . .	217
11.4. Mere systemrevision og øget behov for it-revisor . . . . .	219
<b>Afslutning</b> . . . . .	221