

BEITRÄGE
DES INSTITUTS FÜR
RECHNUNGSWESEN
UND CONTROLLING
DER UNIVERSITÄT
ZÜRICH

EHEMALS «MITTEILUNGEN AUS DEM
HANDELSWISSENSCHAFTLICHEN
SEMINAR DER UNIVERSITÄT ZÜRICH»

HERAUSGEBER

PROF. DR. CONRAD MEYER
PROF. DR. DIETER PFAFF
PROF. FLEMMING RUUD, PHD

PATRICK K. FREI

LIC. OEC. PUBL.

IT-KONTROLLEN IN DER FINANZBERICHT- ERSTATTUNG

THEORETISCHE ANALYSE UND
PRAKTISCHE GESTALTUNG AM
FALLBEISPIEL DER CREALOGIX AG

Inhaltsverzeichnis

Dank	V
Inhaltsverzeichnis	VII
Abbildungsverzeichnis	XIII
Abkürzungsverzeichnis	XVII
Teil I: Grundlegung	1
1. Kapitel: Einleitung	1
1.1 Problemstellung	2
1.1.1 Vertrauenskrise	2
1.1.2 Bedeutung der IT im Unternehmen und deren Einfluss auf die Finanzberichterstattung	3
1.2 Stand der Forschung und Forschungsfrage	6
1.3 Untersuchungsobjekt	7
1.4 Zielsetzung	7
1.5 Aufbau	8
1.6 Beitrag der Arbeit	10
2. Kapitel: Interne Kontrolle und Informationstechnologie	11
2.1 Grundlagen der Internen Kontrolle	11
2.1.1 Ziel und Zweck	13
2.1.2 Abgrenzungen	16
2.1.2.1 Controlling	16
2.1.2.2 Revision	17
2.1.2.3 Risikomanagement	18
2.1.2.4 Gesamtübersicht	20
2.1.3 Aufgaben und Verantwortlichkeiten	21
2.1.3.1 Verwaltungsrat	21
2.1.3.2 Geschäftsleitung	22
2.1.3.3 Interne Revision	23
2.1.3.4 Externe Revisionsstelle	24
2.1.3.5 Mitarbeitende	26
2.2 Grundlagen der Informationstechnologie	26

2.2.1	Information	27
2.2.2	Kommunikation	29
2.2.3	Technologie	31
2.2.4	Informationstechnologie	32
2.2.5	Aufgaben und Verantwortlichkeiten	33
2.2.5.1	Chief Information Officer	33
2.2.5.2	Chief Security Officer und Chief Information Security Officer	34
3. Kapitel:	Regulatorische Rahmenbedingungen	37
3.1	Schweiz	37
3.1.1	Staatliche Regulierung	37
3.1.1.1	Obligationenrecht	37
3.1.1.2	Geschäftsbücherverordnung	42
3.1.1.3	Verordnung des EFD über elektronisch übermittelte Daten und Informationen	44
3.1.1.4	Strafgesetzbuch	45
3.1.1.5	Revisionsaufsichtsgesetz	49
3.1.2	Selbstregulierung	51
3.1.2.1	Schweizer Prüfungsstandards	51
3.1.2.2	Swiss Code of Best Practice for Corporate Governance	53
3.1.2.3	Corporate Governance-Richtlinie	54
3.2	Ausland	56
3.2.1	Sarbanes-Oxley Act	56
3.2.2	Abschlussprüferrichtlinie (8. EU-Richtlinie)	62
3.2.3	Basel II	64
3.2.4	Turnbull Report	67
Teil II: IT-Kontrollen in der Finanzberichterstattung		69
4. Kapitel:	Einfluss der IT auf die Finanzberichterstattung	69
4.1	Voraussetzungen der Finanzberichterstattung	70
4.1.1	Ordnungsmässige Buchführung	71
4.1.2	Ordnungsmässige Rechnungslegung	73
4.2	IT und Ordnungsmässigkeit	77
4.2.1	Besonderheiten bei der Buchführung mit IT	77

4.2.2	Zusammenhang zwischen IT und Ordnungsmässigkeit	82
4.3	Risiken für die Finanzberichterstattung aus der Nutzung von IT	84
4.3.1	Grundbedrohungen	87
4.3.2	Spezifische Bedrohungen und Risikoszenarien	90
4.3.2.1	Höhere Gewalt	91
4.3.2.2	Organisatorische Mängel	92
4.3.2.3	Menschliche Fehlhandlungen	94
4.3.2.4	Technisches Versagen	97
4.3.2.5	Vorsätzliche Handlungen	99
5. Kapitel:	Kontrollmassnahmen	103
5.1	Ausgangslage	103
5.2	Grundsätzliche Kontrollkategorien	106
5.2.1	Durchführungsart	106
5.2.2	Durchführungszeitpunkt	108
5.2.2.1	Präventive Kontrollen	110
5.2.2.2	Detektive Kontrollen	111
5.2.2.3	Korrektive Kontrollen	112
5.2.2.4	Direktive Kontrollen	112
5.2.2.5	Abhaltende Kontrollen	112
5.2.2.6	Wiederherstellungskontrollen	113
5.3	Spezifische IT-Kontrollen	113
5.3.1	IT-Kontrollen auf Unternehmensebene	115
5.3.2	Generelle IT-Kontrollen	116
5.3.2.1	Computerbetrieb	117
5.3.2.2	Zugriff auf Programme und Daten	119
5.3.2.3	Programmentwicklung und Programmänderung	121
5.3.3	Applikationskontrollen	126
5.3.3.1	Zugriffskontrollen	127
5.3.3.2	Eingabekontrollen	128
5.3.3.3	Verarbeitungskontrollen	130
5.3.3.4	Ausgabekontrollen	132
5.3.4	Zusammenhang zwischen generellen IT-Kontrollen und Applikationskontrollen	134
5.3.5	Besondere Kontrollen im Bereich «End-User Computing»	136

5.3.5.1	Verwendung von «Spreadsheets»	136
5.3.5.2	«Spreadsheet»-Kontrollen	139
5.4	Kontrollrahmenwerke	141
5.4.1	Grundsätzliche Ansätze	142
5.4.1.1	COSO	142
5.4.1.2	COSO-ERM	148
5.4.1.3	CoCo	150
5.4.1.4	Vergleich der Ansätze	154
5.4.2	IT-spezifische Ansätze	155
5.4.2.1	CobiT	155
5.4.2.2	CONCT	159
5.4.2.3	ISO/IEC 17799 (ISO/IEC 27002)	162
5.4.3	Summarischer Vergleich aller Ansätze	164
6. Kapitel:	Beurteilung von IT-Kontrollen	167
6.1	Ausgestaltung	167
6.1.1	Verfahren	169
6.1.2	Identifikation, Dokumentation und Bewertung von Kontrollschwächen	173
6.1.3	Beseitigung von Kontrollschwächen	173
6.2	Operative Effektivität	174
6.2.1	Testumfang, Zeitraum und Ressourcen	175
6.2.2	Testverfahren	176
6.2.3	Dokumentation und Behebung von Kontrollschwächen	177
6.3	Grenzen Interner Kontrollen	178
Teil III:	Konzept zur Gestaltung von IT-Kontrollen in der Finanzberichterstattung	181
7. Kapitel:	Fallstudie Crealogix AG	181
7.1	Überblick über die Crealogix Gruppe	182
7.2	Forschungskonzept	184
7.2.1	Forschungsmethode	185
7.2.1.1	Wahl der Forschungsmethode	185
7.2.1.2	Fallstudienmethode	186
7.2.2	Forschungsdesign	188
7.2.3	Datenerhebung, Datenanalyse und Selektion	189

7.2.4	Validität und Reliabilität	191
7.2.5	Grenzen des Forschungsansatzes	192
7.3	Untersuchungsablauf	193
7.3.1	Projektkonzeption	193
7.3.1.1	Etablierung Projektteam	194
7.3.1.2	Projektzeitplanung	194
7.3.2	Ermittlung der Gegebenheiten des Unternehmensumfelds	196
7.3.2.1	Organisationsstruktur	196
7.3.2.2	Inventarisierung der Finanzsysteme und Finanzapplikationen	197
7.3.2.3	Analyse der IT-Finanzprozessstruktur	199
7.3.3	Risikobeurteilung	202
7.3.3.1	Applikationen im Allgemeinen und Schnittstellen bei der Erstellung des Geschäftsberichts	204
7.3.3.2	Applikationen im Allgemeinen und Schnittstellen bei der Datenaufbereitung	206
7.3.3.3	Applikationen im Besonderen	209
7.3.3.4	IT- und generelle Infrastruktur	211
7.3.4	Gestaltung und Beurteilung der IT-Kontrollen	212
7.3.4.1	IT-Kontrollen auf Unternehmensebene	217
7.3.4.2	IT-Kontrollen auf Dienstleistungsebene	220
7.3.4.3	Applikationskontrollen	228
7.4	Zusammenfassende Resultate und Optimierungsvorschläge	232
7.4.1	Unternehmensebene	233
7.4.2	Dienstleistungsebene	235
7.4.3	Geschäftsprozessebene	237
7.4.4	Ergänzende Schlussfolgerungen	238
7.5	Konzeptillustration	240
8. Kapitel:	Hypothesen	245
9. Kapitel:	Schlussbetrachtung	251
9.1	Zusammenfassung und kritische Würdigung	251
9.2	Ausblick	253
Literaturverzeichnis		255
Anhang		275