

## SOMMARIO

Prefazione.....	III
Nota sugli autori .....	VII

## PRIVACY & AUDIT

### Capitolo 1 INTRODUZIONE

1.1 A chi ci rivolgiamo.....	4
1.2 Prerequisiti per la lettura .....	5
1.3 Ambito della trattazione.....	5
1.3.1 Esclusioni.....	6
1.4 Guida alla lettura .....	6
1.4.1 Sintesi dei contenuti e struttura.....	7
1.4.2 Note terminologiche .....	8

### Capitolo 2 LE PAROLE DELL'AUDIT

2.1 Termini e definizioni.....	11
2.2 Controllo e Verifica.....	21
2.3 Audit vs Assessment .....	22
2.3.1 L'Assessment dei sistemi informatici .....	23

### Capitolo 3 I CRITERI PER L'AUDIT DELLA PRIVACY

3.1 La Normativa in materia di Privacy.....	26
3.1.1 Codici deontologici e codici di condotta .....	26
3.2 Il Sistema di Gestione della Privacy.....	27
3.3 Le Linee Guida della famiglia ISO 27000 .....	31
3.3.1 Le Linee Guida ISO/IEC 27007: 2011 2017 .....	31
3.4 Protezione dei dati e Sicurezza delle informazioni: convergenze .....	32
3.4.1 Il rapporto tra SGP e Sistema di Gestione della Sicurezza delle Informazioni .....	32
3.4.2 Il ponte gettato dal Garante.....	33

## **Capitolo 4**

### **STANDARD E STRUMENTI PER LA CONDUZIONE DEGLI AUDIT**

4.1	Le Norme Tecniche.....	35
4.2	Le Linee Guida per condurre gli Audit: UNI EN ISO 19011 .....	36
4.3	Lo Standard o UNI CEI EN ISO/IEC 27001: 2017 come Criterio Ausiliario .....	39
4.4	L'Approccio basato sul Rischio .....	42
4.4.1	Analisi e gestione del Rischio: le Fonti.....	42
4.4.2	Una Classificazione dei Rischi .....	43
4.4.3	Il Risk Based Audit.....	46
4.5	Le tecniche: l'utilizzo degli indicatori .....	48
4.5.1	Definizione e Gestione degli Indicatori .....	49
4.5.2	Gli indicatori per l'audit della Privacy .....	50
4.5.3	Analisi della Customer Satisfaction.....	52

## **Capitolo 5**

### **L'AUDIT AI TEMPI DEL REGOLAMENTO EUROPEO**

5.1	Ruolo del Titolare nelle attività di Audit .....	56
5.2	Protezione dei dati dalla progettazione e per default .....	59
5.3	Ruolo del Responsabile del trattamento nelle attività di Audit .....	60
5.4	Ruolo del Data Protection Officer.....	63
5.5	Valutazioni sull'Audit alla funzione DPO.....	70
5.5.1	L'Audit alla funzione DPO: è opportuno? .....	70
5.5.2	L'Audit alla funzione DPO: quale criterio? .....	72
5.5.3	Quando il DPO dipende dal Titolare.....	73
5.6	Audit e sicurezza del trattamento .....	74
5.7	Codici di condotta e Certificazioni .....	76
5.7.1	I Codici di condotta.....	76
5.7.2	Certificazione e Marchio di protezione dei dati .....	80
5.8	L'Accreditamento degli Organismi di certificazione.....	82
5.9	Compiti dell'Autorità di controllo.....	85
5.10	L'Audit sul trasferimento con le Norme vincolanti d'impresa .....	88
5.11	Riflessioni sulle traduzioni del Regolamento .....	90

## Capitolo 6 LE TIPOLOGIE DI AUDIT

6.1	Audit di prima parte .....	93
6.2	Audit di seconda parte .....	93
6.2.1	Audit di pre-qualificazione .....	94
6.2.2	Audit di mantenimento.....	94
6.2.3	Audit di seconda parte: le Risultanze .....	95
6.2.4	Dalla parte del Fornitore Auditato: aspetti procedurali .....	96
6.2.5	Dalla parte del Fornitore Auditato: aspetti relazionali .....	97
6.3	Audit di terza parte .....	97
6.3.1	Non previsto nel Codice Privacy .....	97
6.3.2	Previsto nel Regolamento UE.....	98

## Capitolo 7 I SOGGETTI DELL'AUDIT: DESIGNAZIONE - POSIZIONE E COMPITI

7.1	Gli Attori extra Team .....	99
7.1.1	La Direzione .....	99
7.1.2	Il Responsabile del Programma .....	99
7.2	Gli Attori nel Team .....	101
7.2.1	Il Responsabile del Team .....	101
7.2.2	L'Auditor.....	102
7.3	Il Team di Audit.....	102
7.3.1	La composizione del Team .....	102
7.3.2	La Valutazione dei Membri del Team .....	104
7.4	Programmare e Pianificare un audit con la Matrice RACI.....	105
7.5	L'impianto delle Procedure per l'Audit di un Sistema di Gestione ....	107

## Capitolo 8 LA PROGRAMMAZIONE DEGLI AUDIT

8.1	La Programmazione efficace.....	112
8.1.1	Audit di Processo.....	113
8.1.2	Audit di Funzione .....	113
8.1.3	Audit di Commessa.....	114
8.2	Una nota sulla pianificazione .....	114
8.3.	Programma di Audit - Output 1 .....	115

## **Capitolo 9**

### **IL CICLO DI VITA DELL'AUDIT**

9.1	Lo studio preliminare.....	119
9.2	Le Fasi del Ciclo di Vita.....	120

## **Capitolo 10**

### **LA PREPARAZIONE DELL'AUDIT**

10.1	La definizione della tempistica.....	123
10.1.1	L'incidenza dell'attività di back-office.....	124
10.2	Case study sulla tempistica.....	124

## **Capitolo 11**

### **L'ANALISI DOCUMENTALE**

11.1	L'Analisi documentale.....	128
11.2	Rapporto di analisi documentale - Output 2.....	129
11.3	Le attività dopo l'analisi documentale.....	131

## **Capitolo 12**

### **IL PIANO DI AUDIT**

12.1	Costituire il team di Audit.....	133
12.1.1	La determinazione dell'impegno del team.....	133
12.1.2	Audit completi, di processo o di commessa.....	137
12.2	Le Funzioni da intervistare.....	138
12.2.1	La Direzione e la funzione commerciale.....	140
12.2.2	L'ordine delle interviste per audit completi.....	140
12.3	Contenuti e Gestione del Piano.....	141
12.3.1	Contenuti del Piano di audit.....	141
12.3.2	L'invio del piano delle interviste.....	142
12.3.3	La Ricusazione di un auditor.....	142
12.4	Piano di Audit - Output 3.....	143

## **Capitolo 13**

### **LE LISTE DI CONTROLLO**

13.1	Tecniche di preparazione.....	156
------	-------------------------------	-----

13.1.1	La progettazione basata sul Criterio .....	156
13.1.2	Progettazione basata sui processi.....	158
13.1.3	Progettazione con tecnica rapida.....	160
13.2	Liste di Controllo - Output 4 .....	161
13.2.1	Lista di controllo per l'intera Organizzazione (approccio olistico) .....	161
13.2.2	Liste di controllo per un audit settoriale o mirato .....	164
13.2.3	Le domande trasversali .....	166

## **Capitolo 14**

### **L'AUDIT IN CAMPO**

14.1	La Riunione di apertura.....	169
14.1.1	Quali contenuti trattare.....	174
14.1.2	La Riunione di apertura: eccezioni .....	176
14.1.3	La Riunione di apertura in contesto Privacy .....	177
14.1.4	La prima mezz'ora di audit .....	178
14.2	Tecniche di Raccolta delle Evidenze .....	179
14.2.1	Evidenze qualitative e quantitative.....	182
14.2.2	Fotografie ed altri supporti di evidenze .....	182
14.3	Tecniche di Campionamento .....	183
14.3.1	Case study: piani di campionamento basati sul giudizio ....	184
14.3.2	Case study: i due sensi di marcia nel campionamento.....	187
14.4	L'Intervista di Audit .....	188
14.4.1	Le Fasi dell'intervista .....	188
14.4.2	L'intervista di audit: tecniche.....	193
14.4.3	Altri fattori da considerare .....	195
14.4.4	Due interviste a confronto.....	196
14.4.5	Case study: come ridurre gli errori in campo .....	208
14.5	L'audit in campo: altri spunti .....	210
14.5.1	La variazione del contesto.....	211
14.5.2	il settore dello sviluppo di applicativi gestionali .....	212
14.5.3	La verifica dell'efficacia delle Procedure .....	212
14.5.4	La verifica dei principi ispiratori del GDPR.....	213
14.5.5	Audit in situazione di tensione .....	214
14.6	La Sospensione dell'Audit .....	214
14.7	Il Rapporto sulle Risultanze di audit - Output 5 .....	215
14.7.1	Le Non Conformità .....	216
14.7.2	La classificazione delle Non Conformità.....	218

14.7.3	La formulazione delle Non Conformità: l'approccio anglosassone .....	220
14.7.4	La Non Conformità su due criteri .....	223
14.7.5	Le Raccomandazioni per il Miglioramento .....	224
14.7.6	Le Buone Prassi .....	227
14.7.7	Risultanze e giudizi personali.....	228
14.7.8	Quando le Procedure sono ambigue .....	229
14.8	La Riunione di chiusura.....	229
14.8.1	Le Criticità nel corso della Riunione.....	230
14.8.2	La Riunione di chiusura in contesto Privacy .....	231
14.8.3	Una Riunione di chiusura simulata.....	231

## **Capitolo 15**

### **LE AZIONI SUCCESSIVE**

15.1	La preparazione del Rapporto di Audit .....	237
15.2	Rapporto finale di Audit - Output 6 .....	239
15.3	La Gestione delle Non Conformità.....	246
15.3.1	Casi particolari di Non Conformità.....	247
15.3.2	Documentazione delle Non Conformità: Output 7 .....	248
15.3.3	Case study - Non Conformità .....	251
15.4	Le Azioni Correttive e le Azioni di Miglioramento.....	260
15.4.1	Le azioni Correttive.....	262
15.4.2	La documentazione delle azioni Correttive .....	263
15.4.3	Case study: le azioni Correttive in campo .....	266
15.4.4	La verifica dell'efficacia.....	268
15.4.5	Report delle Azioni Correttive: Output 8 .....	272
15.4.5	Le Azioni di Mitigazione del Rischio .....	276
15.4.6	Le azioni di Miglioramento .....	277
15.5	Tecniche di problem solving .....	278
15.5.1	Il metodo dei "Cinque perché" .....	278
15.5.2	Il metodo delle 8 Discipline .....	280

## **Capitolo 16**

### **LA COMUNICAZIONE NELL'AUDITING**

16.1	L'Intervista: comunicazione e valutazione.....	283
16.1.1	Le fasi dell'intervista .....	283
16.2	Le Trappole della valutazione .....	285

16.2.1	I pregiudizi dell'auditor .....	285
16.2.2	Gli errori di valutazione.....	286
16.2.3	Suggerimenti all'auditor .....	288
16.3	La Comunicazione: teoria e pratica .....	289
16.3.1	Le costanti della Comunicazione .....	289
16.3.2	La Comunicazione interculturale.....	290
16.3.3	La Comunicazione non verbale .....	292
16.4	Le opportunità offerte dalla tecnologia.....	293
16.5	Dalla parte dell'auditato.....	293

## **Capitolo 17**

### **TIPOLOGIE PARTICOLARI DI AUDIT**

17.1	Il Perimetro dell'Audit .....	297
17.1.1	Gli Audit mirati .....	297
17.1.2	Gli Audit combinati .....	299
17.2	Modalità di svolgimento particolari.....	300
17.2.1	Audit all'estero .....	300
17.2.2	Audit senza preavviso .....	302
17.2.3	Audit in incognito.....	302
17.3	Audit e Situazioni eccezionali.....	303
17.4	Audit e Procedure di emergenza.....	304
17.5	Audit dei Piani di Disaster Recovery e di Continuità .....	305
17.5.1	Il Piano di Disaster Recovery.....	305
17.5.2	Il Piano di Continuità del Business.....	306

## **Capitolo 18**

### **IL PROFILO DELL'AUDITOR DELLA PRIVACY**

18.1	I principi etici dell'attività di audit.....	309
18.1.1	Il comportamento etico .....	312
18.2	Le conoscenze e le capacità.....	315
18.2.1	Il Bagaglio delle conoscenze.....	316
18.2.2	Il Bagaglio delle Capacità .....	317
18.2.3	Esempi - le Capacità personali.....	318
18.2.4	La consapevolezza del ruolo.....	319
18.3	Il Paradosso dell'auditor .....	320
18.3.1	La designazione ad Incaricato del trattamento .....	321

## Capitolo 19 CONCLUSIONI

19.1 L'audit è un'attività creativa... e non solo.....	327
19.2 Avremmo potuto anche parlare di... (e non siamo riuscite a farlo)..	328
19.3 Dialogo con un Auditor errante... ..	328
Appendice 1 - Il parere dell'accademia della crusca .....	333
Appendice 2 - Un modello di procedura per l'audit integrato .....	337
Appendice 3 - La Gestione del rischio - Principi e Linee Guida .....	348
Appendice 4 - La famiglia delle norme ISO 27000.....	357
Bibliografia.....	361



---

**[www.spazioquaglia.it](http://www.spazioquaglia.it)**

Libreria Quaglia s.a.s. C.so di Porta Vittoria 28, angolo V. Manara 1 - 20122 MILANO  
Tel. 02 5512789 - 02 54108547 E-mail [libreriaquaglia@spazioquaglia.it](mailto:libreriaquaglia@spazioquaglia.it) P. IVA 11194640154

