

“All-in-One Is All You Need.”

ALL-IN-ONE

CIPM®

Certified Information Privacy Manager

EXAM GUIDE

Online content includes:

- 300 practice exam questions
- Test engine that provides full-length practice exams and customizable quizzes by exam topic

Complete coverage of all current domains for the 2021 IAPP® Certified Information Privacy Manager exam

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

Mc
Graw
Hill

PETER H. GREGORY

CIPM, CDPSE™, CISA®, CISM®, CRISC®, CISSP®, DRCE, CCSK™

CONTENTS

	Acknowledgments	xv
	Introduction	xvii
Chapter 1	Developing a Privacy Program	1
	The Privacy Vision	1
	Program Approaches	2
	Privacy Objectives	2
	Executive Sponsorship	2
	Business Alignment	3
	Establish a Data Governance Model	5
	Data Governance	5
	Privacy Governance	7
	Establish a Privacy Program	13
	Strategy Objectives	13
	Risk Objectives	14
	Strategy Resources	14
	Privacy Program Strategy Development	20
	Strategy Constraints	29
	Structure the Privacy Team	31
	Roles	31
	Competency	48
	Privacy Program Communications	48
	Privacy Training and Awareness	49
	Maintaining an Awareness Program	53
	Chapter Review	53
	Quick Review	55
	Questions	56
	Answers	59
Chapter 2	Privacy Program Framework	61
	Develop the Privacy Program Framework	62
	Privacy Charter	62
	Developing Privacy Policies	63
	Privacy Standards	65
	Privacy Laws	67
	Establishing Legal Basis for Processing	74
	Establishing Legitimate Interest	74

Controls	75
Control Frameworks	77
Data Inventory	84
Data Classification	86
Data Use Governance	93
Implement the Privacy Program Framework	104
Building a Privacy Operation	104
Developing and Running Data Protection Operations	106
Developing and Running Data Monitoring Operations	106
Working with Data Subjects	108
Collecting Consent	110
Working with Authorities	110
Privacy Program Metrics	111
Risk Management Metrics	113
Data Subject Engagement Metrics	113
Data Governance Metrics	114
Program and Process Maturity	114
Performance Measurement	114
Resilience Metrics	115
Convergence Metrics	115
Resource Management Metrics	116
Online Tracking and Behavioral Profiling	116
Tracking Techniques and Technologies	117
Tracking in the Workplace	124
Tracking Prevention	125
Chapter Review	128
Quick Review	129
Questions	131
Answers	134
Chapter 3 Privacy Operational Lifecycle: Assess	137
Privacy Program Baseline	138
Process Maturity	138
Baselining Program Elements	139
Third-Party Risk Management	140
Cloud Service Providers	141
Privacy Regulation Requirements	142
TPRM Life Cycle	143
Physical Assessments	147
Assessing Processing Centers and Work Centers	148
Document Storage	149
Document and Media Destruction	149
Device Security	150
Mergers, Acquisitions, and Divestitures	151
Influencing the Transaction	151
Integrating Programs	152

Privacy Impact Assessments and Data Privacy Impact Assessments	152
Privacy Threshold Analysis	153
PIA Procedure	153
Engaging Data Subjects in a PIA	154
The Necessity of a PIA	154
Integrating into Existing Processes	155
Recordkeeping and Reporting	155
Risks Specific to Privacy	155
Privacy Threats	157
Privacy Countermeasures	158
Chapter Review	159
Quick Review	159
Questions	160
Answers	163
Chapter 4 Privacy Operational Lifecycle: Protect	165
Information Security Practices	165
Identity and Access Management	166
Technical Security Controls	177
Administrative Safeguards	193
Privacy and Security by Design	196
Integrating Privacy into Organization Operations	198
Information Security	198
IT Development and Operations	198
Business Continuity and Disaster Recovery Planning	199
Mergers, Acquisitions, Divestitures	199
Human Resources	199
Compliance and Ethics	201
Audit	201
Marketing	201
Business Development	202
Public Relations	203
Procurement and Sourcing	203
Legal and Contracts	203
Security and Emergency Services	204
Finance	204
Other Functions	205
Other Protection Measures	205
Data Retention and Archiving	205
Data Destruction	207
Data Sharing and Disclosure	207
Costs of Technical Controls	208
Chapter Review	210
Quick Review	211
Questions	211
Answers	214

Chapter 5 Privacy Operational Lifecycle: Sustain 217

Monitoring a Privacy Program 217

 Business Process Monitoring 218

 Privacy and Security Event Monitoring 219

 External Monitoring 225

 Control Self-Assessment 225

Auditing Privacy Programs 228

 Privacy Audit Scope 228

 Privacy Audit Objectives 229

 Types of Privacy Audits 229

 Privacy Audit Planning 230

 Privacy Audit Evidence 232

 Auditing Specific Privacy Practices 234

Chapter Review 238

 Quick Review 239

 Questions 240

 Answers 242

Chapter 6 Privacy Operational Lifecycle: Respond 245

Data Subject Requests and Privacy Rights 245

 Data Subject Requests 246

 Working with Authorities 249

Privacy Incident Response 250

 Incident Response Regulations 250

 Phases of Incident Response 250

 Privacy Incident Response Plan Development 254

Privacy Continuous Improvement 258

Chapter Review 258

 Quick Review 259

 Questions 260

 Answers 263

Appendix A The Risk Management Life Cycle 265

The Risk Management Process 266

Risk Management Methodologies 269

 NIST Standards 269

 ISO/IEC 27005 274

 Factor Analysis of Information Risk 277

Asset Identification 278

 Hardware Assets 278

 Subsystem and Software Assets 279

 Cloud-Based Information Assets 279

 Virtual Assets 279

 Information Assets 279

Asset Classification 280

 Data Classification 281

Asset Valuation 281

 Qualitative Asset Valuation 282

 Quantitative Asset Valuation 282

Threat Identification 283

 Internal Threats 283

 External Threats 286

 Advanced Persistent Threats 287

 Emerging Threats 288

Vulnerability Identification 289

 Third-Party Vulnerability Identification 290

Risk Identification 292

Risk, Likelihood, and Impact 293

 Likelihood 293

 Impact 294

Risk Analysis Techniques and Considerations 295

 Information Gathering 295

 Qualitative Risk Analysis 296

 Semiquantitative Risk Analysis 296

 Quantitative Risk Analysis 296

 OCTAVE 298

 Other Risk Analysis Methodologies 299

 Risk Evaluation and Ranking 299

 Risk Ownership 300

 Risk Treatment 300

 Controls 304

 Costs and Benefits 304

Appendix B About the Online Content 307

System Requirements 307

Your Total Seminars Training Hub Account 307

 Privacy Notice 307

Single User License Terms and Conditions 307

TotalTester Online 309

Technical Support 309

Glossary 311

Index 335