

11 Detailed table of contents / outline

1 Background and Introduction.....	4
- Background of the book.....	4
- Background of the author.....	5
- Introduction to the book.....	7
- The cover.....	8
- Background questions.....	8
2 Enterprise information protection.....	9
- A systematic comprehensive approach.....	9
- - The architectural model.....	10
- Business modeling.....	12
- - How information supports the business.....	13
- - How information technology supports business.....	14
- - Linkage between the model and technology.....	14
- Oversight.....	15
- Business risk management.....	16
- Interdependencies and risk aggregation.....	19
- - But how much is enough? The duty to protect.....	19
- Governance, power, and influence.....	20
- Control architecture.....	21
- Technical security architecture.....	24
- Overview questions.....	26
3 How business works and is modeled.....	27
- Things to consider in the business model.....	28
- What's in the business model?.....	30
- What does a business model look like?.....	31
- How to build a business model.....	32
- How to use the business model.....	34
- Business modeling questions.....	35
4 Oversight.....	36
- Duty to protect.....	37

Enterprise Information Protection

- - Externally imposed duties.....	37
- - Internally imposed duties.....	37
- - Contractual duties.....	38
- Some well known duties to protect.....	38
- - Business record retention and disposition.....	38
- - Disaster recovery and business continuity planning.....	39
- - Privacy requirements.....	39
- - Financial records and related content controls.....	40
- - Intellectual property controls.....	41
- - Customer content.....	41
- - Codes of ethics and standards of practice.....	41
- - Operational status.....	41
- - Investigations underway.....	42
- - Reporting requirements.....	42
- - Risk tolerance and management.....	42
- Managing changes in oversight.....	42
- Decisions made by oversight.....	43
- The need for independent evaluation.....	44
- Oversight questions.....	45
5 Risk management and what to protect.....	46
- Some background on the nature of risk.....	46
- Risk identification and evaluation.....	49
- - Consequences.....	49
- - Threats and threat assessment.....	50
- - Vulnerabilities.....	53
- - Interdependencies and risk aggregations.....	54
- - - Interdependencies.....	54
- - - Single points of failure as risk aggregations.....	55
- - - Radius-driven common mode failures.....	55
- - - Other sorts of common mode failures.....	56
- - - Key individuals.....	56

Enterprise Information Protection

- Risk treatment options.....	57
- - Risk acceptance.....	57
- - Risk avoidance.....	57
- - Risk transfer.....	58
- - Risk mitigation.....	59
- What to protect how well: risk management.....	59
- - The risk management space.....	59
- - - Low risk options.....	60
- - - Medium risk options.....	61
- - - High risk options.....	61
- - Matching surety to risk.....	61
- - - Low risks and surety.....	62
- - - Medium risks and surety.....	63
- - - High risks and surety.....	65
- - Reality check on risk matching.....	66
- - Selection of approach.....	67
- - Risk review rates.....	68
- Risk management questions.....	69
6 Information protection governance.....	70
- Fulfilling the duties to protect.....	71
- What is governance?.....	73
- Governance structures and fitting in.....	73
- - Fitting protection into business structures.....	75
- Organizational perspectives and functions.....	76
- - Management.....	80
- - Policy.....	80
- - Standards.....	81
- - Procedures.....	84
- - Documentation.....	85
- - Auditing.....	87
- - Testing and change control.....	87

Enterprise Information Protection

- - Technical safeguards (information technology).....	88
- - Personnel.....	91
- - Incident handling.....	93
- - Legal issues.....	95
- - Technical safeguards - physical security.....	98
- - Knowledge.....	100
- - Awareness.....	102
- - Organization.....	105
- Top-level governance – the CISO.....	106
- - Who should the CISO work for?.....	107
- - Should the CISO have other duties?.....	110
- - Who should work for or be matrixed to the CISO?.....	111
- - Groups the CISO meets with.....	114
- - Separation of duties issues.....	114
- - The theory of groups.....	115
- - What groups are needed.....	116
- - - Business unit governance group(s).....	117
- - - Policy, standards and procedures groups.....	118
- - - Legal groups.....	119
- - - Personnel security coordination.....	120
- - - Risk management groups.....	121
- - - Protection testing and change control.....	121
- - - Technical safeguards group and review board.....	122
- - - Zoning boards and similar governance entities.....	123
- - - Physical security group and review board.....	124
- - - Incident handling group and review board.....	124
- - - Audit group and review board.....	127
- - - Awareness and knowledge group and review.....	128
- - - Documentation group.....	128
- - - Special projects and other groups.....	129
- - The CISO's schedule.....	130

Enterprise Information Protection

- What are the rules?.....	131
- Principles and standards.....	132
- Power and influence.....	134
- - Applying power and influence.....	136
- - - Physical power.....	136
- - - Resource power.....	137
- - - Positional power.....	137
- - - Expertise, personal, and emotional power.....	138
- - - Persuasion model.....	138
- - Managing change.....	140
- - - The buy-in plan.....	141
- - - The communications plan.....	142
- - - The risk treatment plans.....	143
- - - Adaptation to contact.....	144
- - An example managing security consulting jobs.....	144
- Enforcement, appeals process, and disputes.....	147
- - Enforcement.....	148
- - Disputes.....	151
- - Top management buy-in and support.....	153
- - Power and influence and managing change.....	153
- - Responses to power and influence.....	154
- - Other power issues.....	155
- The enterprise protection control system.....	156
- - Metrics.....	158
- - - Costs.....	158
- - - Performance.....	158
- - - Time.....	159
- - - Lower-level metrics.....	159
- Budgets and funding.....	160
- - The hidden costs of security.....	161
- - Typical budget numbers.....	163

Enterprise Information Protection

- - - Direct budget for the CISO.....	164
- - - Identifiable costs.....	164
- How long will it take?.....	167
- Summary.....	170
- Governance questions.....	171
7 Control architecture.....	173
- Protection objectives.....	174
- - Integrity.....	174
- - Availability.....	176
- - Confidentiality.....	176
- - Use control.....	178
- - Accountability.....	180
- Access control architecture.....	182
- Components and composites: functional units.....	183
- Perimeter architectures.....	184
- - Physical perimeter architecture.....	184
- - - World.....	185
- - - Property.....	185
- - - Perimeter.....	186
- - - Facility.....	187
- - Logical perimeter architecture.....	187
- - - World.....	188
- - - Facility.....	188
- - - Data center.....	189
- - - Zones.....	189
- - Perimeter summary.....	190
- Access process architecture.....	190
- - Identification.....	190
- - Authentication.....	191
- - Authorization.....	191
- - Use.....	192

Enterprise Information Protection

- Change control architecture.....	193
- - Research and development.....	194
- - Change control.....	194
- - Production.....	194
- Emerging control architecture elements.....	195
- - Security policy languages and execution.....	195
- - The Web services world.....	195
- - Wrappers and related approaches.....	196
- - Cryptographic seals and self-protection.....	196
- - Models of trust.....	197
- Control architecture questions.....	197
8 Technical security architecture.....	199
- Protection process.....	199
- - Issues of context.....	200
- - - Time (when).....	200
- - - Location (where).....	201
- - - Purpose (why).....	202
- - - Behaviors (what).....	203
- - - Identity (who).....	204
- - - Method (how).....	205
- - Life cycles.....	206
- - - Business.....	206
- - - People.....	209
- - - - Disgruntled employees and ex-employees.....	214
- - - Systems.....	214
- - - Data.....	219
- - Data states.....	227
- - - Data at rest.....	227
- - - Data in motion.....	235
- - - Data in use.....	239
- - Attack and defense processes.....	240

Enterprise Information Protection

- - - Deter.....	241
- - - Prevent.....	242
- - - Detect.....	246
- - - React.....	251
- - - Adapt.....	254
- - - Detect/react loop.....	257
- - Work flows.....	259
- - - Work to be done.....	260
- - - Process for completion and options.....	260
- - - Control points and approval requirements.....	260
- - - Appeals processes and escalations.....	261
- - - Authentication requirements & mechanisms.....	261
- - - Authorization and context limitations.....	261
- - - Work flow documentation and audit.....	262
- - - Control and validation of the engine(s).....	262
- - - Risk aggregation in the engine(s).....	263
- - Inventory.....	264
- Protective mechanisms.....	267
- - Perception.....	267
- - Structure.....	268
- - Content controls.....	270
- - Behavior.....	271
- Technical security architecture questions.....	274
9 Making better protection decisions.....	276
- Common decision processes.....	277
- - Identifying options.....	278
- - Identifying factors.....	278
- - Comparing options based on weighing factors.....	280
- - Presentation and justification of decisions.....	281
- - Recording decision processes and results.....	282
- - Tools to support decision-making.....	282

Enterprise Information Protection

- So-called best practices – don't buy it.....285
- Some sample sound practices with a basis.....286
- - Avoiding radius driven common mode failures.....286
- - How many redundant data centers do I need?.....289
- Decision-making questions.....291
- 10 Summary and conclusions.....292
- 11 Detailed table of contents / outline.....294
- 12 Endnotes.....303
 - Chapter 1.....303
 - Chapter 2.....303
 - Chapter 3.....306
 - Chapter 4.....306
 - Chapter 5.....308
 - Chapter 6.....310
 - Chapter 7.....315
 - Chapter 8.....322
 - Chapter 9.....327
- 13 Index.....329