

Detailed Table of Contents

- 1 The governance guidebook..... 1
 - 1.1 Executive summary..... 1
 - 1.2 Front matter..... 2
- 2 The structure of information protection..... 4
 - 2.1 A comprehensive information protection program..... 4
 - 2.1.1 The architectural model..... 5
 - 2.1.2 Risk management..... 7
 - 2.1.3 How the business works..... 9
 - 2.1.4 How information technology protection works..... 9
 - 2.1.5 Interdependencies..... 11
 - 2.1.6 But how much is enough? The duty to protect..... 11
 - 2.2 What is information protection governance all about?..... 12
 - 2.2.1 The goal of governance..... 12
 - 2.2.2 What are the aspects of governance?..... 13
 - 2.2.2.1 Structures..... 13
 - 2.2.2.2 What are the rules?..... 14
 - 2.2.2.3 Principles and standards..... 15
 - 2.2.2.4 Power and influence..... 17
 - 2.2.2.5 Funding..... 19
 - 2.2.2.6 Enforcement mechanisms..... 21
 - 2.2.2.7 Appeals processes and disputes..... 24
 - 2.2.3 The overall control system..... 25
 - 2.3 Fitting protection into business structures..... 26
 - 2.3.1 Fitting in..... 26
 - 2.3.2 The theory of groups..... 27
 - 2.3.3 What groups are needed..... 28
 - 2.4 Who is in charge and who do they work for?..... 29
 - 2.4.1 The CISO..... 29
 - 2.4.2 The CISO’s team..... 29
 - 2.4.3 The structure of the groups..... 31
 - 2.4.4 Meetings and groups the CISO chairs or operates..... 32
 - 2.4.5 Should the CISO work for the CIO or others?..... 33
 - 2.5 Should the CISO, CPO, CSO, or others be combined?..... 34
 - 2.5.1 Where should the CISO be in the corporate structure?..... 34
 - 2.6 Budgets and situations..... 35
 - 2.6.1 Direct budget for the CISO..... 35
 - 2.6.2 Identifiable costs..... 35
 - 2.7 Enforcement and appeals processes..... 38
 - 2.7.1 Top management buy-in and support..... 38
 - 2.7.2 Power and influence and managing change..... 38
 - 2.7.3 Responses to power and influence..... 39

2.7.4 Other power issues.....	39
2.8 The control system.....	40
2.8.1 Metrics.....	41
2.8.1.1 Costs.....	41
2.8.1.2 Performance.....	41
2.8.1.3 Time.....	42
2.8.1.4 Lower-level metrics.....	42
2.9 How long will it take?.....	43
2.10 Summary.....	45
3 Drill-down.....	46
3.1 How the business works.....	47
3.2 The security oversight function.....	50
3.2.1 Duty to protect.....	51
3.2.1.1 Externally imposed duties.....	51
3.2.1.2 Internally imposed duties.....	51
3.2.1.3 Contractual duties.....	51
3.3 Risk management and what to protect.....	52
3.3.1 Risk evaluation.....	52
3.3.1.1 Consequences.....	52
3.3.1.2 Threats.....	53
3.3.1.3 Vulnerabilities.....	53
3.3.1.4 Interdependencies and risk aggregations.....	53
3.3.1.4.1 Interdependencies.....	53
3.3.1.4.2 Single points of failure.....	54
3.3.1.4.3 Radius-driven common mode failures.....	55
3.3.1.4.4 Other sorts of common mode failures.....	55
3.3.1.4.5 Key individuals.....	55
3.3.2 Risk treatment.....	55
3.3.2.1 Risk acceptance.....	55
3.3.2.2 Risk avoidance.....	56
3.3.2.3 Risk transfer.....	56
3.3.2.4 Risk mitigation.....	56
3.3.3 What to protect and how well.....	56
3.3.4 The risk management space.....	57
3.3.4.1 Risk assessment methodologies and limitations.....	57
3.3.4.1.1 Low risk options.....	58
3.3.4.1.2 Medium risk options.....	58
3.3.4.1.3 High risk options.....	59
3.3.4.1.4 A systematic approach to risk assessment.....	59
3.3.4.2 Matching surety to risk.....	59
3.3.4.2.1 Low risks.....	60
3.3.4.2.2 Low surety.....	60
3.3.4.2.3 Medium risks.....	60

3.3.4.2.4 Medium surety.....	61
3.3.4.2.5 High risks.....	61
3.3.4.2.6 High surety.....	62
3.3.5 An example enterprise risk management process.....	62
3.3.5.1 The risk management process.....	63
3.3.5.2 Evaluation processes to be used.....	63
3.3.5.2.1 Information protection posture assessments.....	63
3.3.5.2.2 Scenario-based risk assessment.....	64
3.3.5.2.3 Systems analysis.....	64
3.3.5.3 The order of analysis.....	64
3.3.5.3.1 Consequence analysis.....	65
3.3.5.3.2 Threat analysis.....	65
3.3.5.3.3 Vulnerability analysis.....	65
3.3.5.4 Selection of mitigation approach.....	66
3.3.5.5 Specific mitigations.....	67
3.3.5.6 Specific issues mandated by policy	67
3.3.5.7 A schedule of risk management activities.....	67
3.3.5.8 Initial conditions.....	68
3.3.5.9 Management decisions and approvals.....	68
3.3.5.10 Reviews to be conducted.....	68
3.3.6 Threat assessment.....	69
3.3.7 Fulfilling the duties to protect.....	71
3.4 Security governance.....	72
3.4.1 Responsibilities at organizational levels.....	72
3.4.2 Enterprise security management architecture.....	73
3.4.3 Groups that the CISO meets with or creates and chairs.....	75
3.4.3.1 Top-level governance board.....	75
3.4.3.2 Business unit governance boards.....	75
3.4.3.3 Policy, standards and procedures group and review board.....	76
3.4.3.4 Legal group and review board.....	77
3.4.3.5 Personnel security group and review board.....	77
3.4.3.6 Risk management group.....	78
3.4.3.7 Protection testing and change control group and review board. .	79
3.4.3.8 Technical safeguards group and review board.....	79
3.4.3.9 Zoning boards and similar governance entities.....	80
3.4.3.10 Physical security group and review board.....	81
3.4.3.11 Incident handling group and review board.....	81
3.4.3.12 Audit group and review board.....	83
3.4.3.13 Awareness and knowledge group and review.....	84
3.4.3.14 Documentation group.....	84
3.4.4 Separation of duties issues.....	85
3.4.5 Understanding and applying power and influence.....	86
3.4.5.1 Physical power.....	86

3.4.5.2 Resource power.....	87
3.4.5.3 Positional power.....	87
3.4.5.4 Expertise, personal, and emotional power.....	88
3.4.5.5 Persuasion model.....	88
3.4.5.6 Managing change.....	90
3.4.5.6.1 The buy-in plan.....	91
3.4.5.6.2 The communications plan.....	91
3.4.5.6.3 The risk treatment plans.....	92
3.4.5.6.4 Adaptation to contact.....	93
3.4.5.6.5 An example managing security consulting jobs.....	93
3.4.6 Organizational perspectives.....	96
3.4.6.1 Management.....	97
3.4.6.2 Policy.....	98
3.4.6.3 Standards.....	99
3.4.6.4 Procedures.....	101
3.4.6.5 Documentation.....	102
3.4.6.6 Auditing.....	103
3.4.6.7 Testing and change control.....	104
3.4.6.8 Technical safeguards – information technology.....	105
3.4.6.9 Personnel.....	108
3.4.6.10 Incident handling.....	110
3.4.6.11 Legal issues.....	112
3.4.6.12 Physical security.....	114
3.4.6.13 Knowledge.....	116
3.4.6.14 Awareness.....	117
3.4.6.15 Organization.....	120
3.4.6.16 Summary of perspectives.....	120
3.5 Control architecture.....	121
3.5.1 Protection objectives.....	121
3.5.1.1 Integrity.....	121
3.5.1.2 Availability.....	122
3.5.1.3 Confidentiality.....	123
3.5.1.4 Use control.....	124
3.5.1.5 Accountability.....	126
3.5.2 Access control architecture.....	128
3.5.3 Technical architecture functional units and composites.....	128
3.5.4 Perimeter architectures.....	129
3.5.4.1 Physical perimeter architecture.....	129
3.5.4.1.1 World.....	129
3.5.4.1.2 Property.....	130
3.5.4.1.3 Perimeter.....	130
3.5.4.1.4 Facility.....	131
3.5.4.2 Logical perimeter architecture.....	132

3.5.4.2.1 World.....	132
3.5.4.2.2 Facility.....	132
3.5.4.2.3 Data center.....	133
3.5.4.2.4 Zones.....	133
3.5.4.3 Perimeter summary.....	133
3.5.5 Access process architecture.....	134
3.5.5.1.1 Identification.....	134
3.5.5.1.2 Authentication.....	134
3.5.5.1.3 Authorization.....	135
3.5.5.1.4 Use.....	135
3.5.6 Change control architecture.....	136
3.5.6.1.1 Research and development.....	136
3.5.6.1.2 Change control.....	136
3.5.6.1.3 Production.....	136
3.6 Technical security architecture.....	137
3.6.1 Issues of context.....	137
3.6.1.1 Time (when).....	137
3.6.1.2 Location (where).....	138
3.6.1.3 Purpose (why).....	139
3.6.1.4 Behaviors (what).....	140
3.6.1.5 Identity (who).....	141
3.6.1.6 Method (how).....	142
3.6.2 Life cycles.....	143
3.6.2.1 Business.....	143
3.6.2.2 People.....	146
3.6.2.2.1 Disgruntled employees end ex-employees.....	149
3.6.2.3 Systems.....	150
3.6.2.4 Data.....	154
3.6.3 Protection process: data state.....	160
3.6.3.1 Data at rest.....	160
3.6.3.2 Data in motion.....	167
3.6.3.3 Data in use.....	170
3.6.4 Protection process: attack and defense.....	171
3.6.4.1 Deter.....	172
3.6.4.2 Prevent.....	173
3.6.4.3 Detect.....	176
3.6.4.4 React.....	180
3.6.4.5 Adapt.....	183
3.6.4.6 Detect/react loop.....	185
3.6.5 Protection process: work flows.....	186
3.6.5.1 Work to be done.....	187
3.6.5.2 Process for completion and options.....	187
3.6.5.3 Control points and approval requirements.....	188

- 3.6.5.4 Appeals processes and escalations.....188
- 3.6.5.5 Authentication requirements & mechanisms.....188
- 3.6.5.6 Authorization and context limitations.....188
- 3.6.5.7 Work flow documentation and audit.....189
- 3.6.5.8 Control and validation of the engine(s).....189
- 3.6.5.9 Risk aggregation in the engine(s).....190
- 3.6.6 Protective mechanisms.....190
 - 3.6.6.1 Perception.....190
 - 3.6.6.2 Structure.....191
 - 3.6.6.3 Content controls.....193
 - 3.6.6.4 Behavior.....194
- 3.7 Roll-up of the drill-down.....196
- 4 Summary and conclusions.....198