

Index

- Access And Authorization, 167–185
- Access Controls, 8, 11, 131, 169, 172, 209, 212, 216–219, 226
- Mobility Threat, 168
- Accounting and Assurance
 - Organizations:
 - American Institute Of Certified Public Accountants (AICPA), 69
 - Canadian Institute of Chartered Accountants (CICA), 47, 67
 - Public Company Accounting Oversight Board (PCAOB), 11, 62, 110
- Access Control Lists (ACLs), 216
- Acquire and Support:
 - Acquisition Strategy, 140
 - Best Practices, 144
 - Impacts, 141
 - Knowledge Management, 143
 - Metrics, 145
 - Procurement, 141
 - Vendor Management, 141–145
 - Vendor Screening, 141
- Action Plans:
 - Addressing Multiple Regulations, 51, 61
 - Applying International Publications, 65
 - Classifying Data, 170–172
 - Converging Mandates, 90–93
 - Discovering All Access Points, 171
 - Determining Impactful Risks and Associated Impacts, 204–205
 - Identifying Current Posture, 102–103
 - Integrate a Control
 - Environment instead of Attaching, 252–253
 - Testing and Vetting Software Development Projects, 151–152
 - Uncovering Business Established Mandates, 85
 - Uncovering Government Mandates, 84
- Activism, 3, 13
- California Public Employees' Retirement System (CALPERS), 14
- Sovereign Funds, 79
- AICPA:
 - SAS 70, 54, 212, 247
 - SAS 94, 88
 - SAS 109, 96
- Anti-Virus (AV), 208, 214, 217
- Application Controls:
 - Best Practices, 148–149
 - Business Dependency, 146
 - Control Objectives, 147
 - Definition, 145
 - Input, 147
 - Integrity, 146–147
 - Output, 149
 - Processing, 147–148
 - Risks, 146
 - Testing, 148–149
- Assessments:
 - Network Vulnerability, 209, 221
 - Penetration Tests, 221
 - Preproduction Software, 152
 - Self, 42
 - Social Engineering, 221
- Attack Vectors:
 - External, 89, 159, 221
 - Infrastructure (Energy), 55
 - Intentional, 89–90
 - Internal, 89
 - Means, 12, 24, 208
 - Malicious Code, 87
 - Unintentional, 90
- Audit:
 - Background, 71–73
 - Fee Reduction, 259
 - Leveraging, 118, 254–255
 - Objective Setting, 131, 205
 - SDLC, 96, 151–152
 - Self Assessment, 41
 - Stakeholders, 84, 72
 - Vendor, 65, 78–80, 85–86, 212–213, 254
- Blackout Of 2003 and 2005, 55
- Business Agility, 38, 40, 249–250
- Business Alignment, 122, 148, 170, 172, 188, 251
- Business Continuity Planning (BCP), 23
 - Backup Media Security, 174
 - Backup Infrastructure, 218
 - Identifying, 191
 - Defining Systems, 191
 - Disaster Levels, 188
 - Planning, 193
 - Documentation, 193
 - Impact Analysis, 188
 - Maintaining, 193
 - Service Levels, 188
 - Sponsorship, 191, 193
 - Surveys, 192
- Business Impact Assessment (BIA), 97, 188–189, 191, 195, 215
- Business Objectives:
 - Alignment, 122, 148, 170, 172, 188, 251
 - Balance, 41, 172, 201, 222
 - Benchmarking, 41–42

- Business Process Outsourcing, 6, 23, 167, 208, 212, 220
 - Key areas, 86
- Business Risk Management:
 - Focus, 258
 - Influences, 94
 - Prioritization, 41, 96
- CardSystems Inc, 32, 54
- Change Control:
 - Best Practices, 159–160
 - Board, 156
 - Metrics, 158
 - Program, 157
- Change Request Detail, 159
- Cisco, 32
- ChoicePoint, 32
- Coase, Ronald, 6
- Confidentiality, 217. (*See also* Encryption and Integrity)
- Configuration Management
 - Database (CMDB), 142, 144
- Committee Of Sponsoring Organizations Of The Treadway Commission (COSO), 46–47, 67, 110, 118
- Connectivity:
 - Blackberry, 23, 176
 - Tivo, 23
 - iPhones, 23, 176
 - iPods, 176
 - Web 2.0 Interfaces, 23, 38
- Control Environment:
 - Enterprise Benefits, 45, 83
 - Perspectives, 75
 - Risks, 88
- Convergence, 90–100
 - Filter and Prioritize, 96–100
 - Review, 221
 - Risks, 94
 - Superset, 92, 242
- Dark Networks, 6, 256
- Data Sensitivity Scale, 156, 170, 215, 227
- Data Theft:
 - Personally Sensitive Information, 125–126
 - Veterans Administration, 31
- Defcon, 55
- Diamond, Jared, 22
- Directional Alignment:
 - Best Practices, 123
 - Costs, 121
- Disaster Recovery Plans (DRP). (*See* BCP)
- Dumpster Diving:
 - Classic, 176
 - Online (i.e. eBay), 176–177
- Duties:
 - Auditor, 71
 - Board of Directors, 76, 104, 118, 259
 - Chief Executive Officer (CEO), 122, 259
 - Chief Information Officer (CIO), 122, 250
 - Chief Information Security Officer (CISO), 122
 - Management Acceptance, 155, 177, 181, 216
 - Security Board, 156
 - Users, 172
- Encryption, 174, 210, 214, 216, 221
- Enron, 31, 32, 50, 179
- Enterprise Risk Analysis:
 - Identifying, 83, 84
 - Mapping. (*See* Convergence)
 - Political Considerations, 84–85
 - Gap Analysis. (*See* Gap Analysis)
 - Project Management. (*See* Project Management)
- Enterprise Risk Management (ERM), 203, 215
 - Annual Evaluations, 215
 - Failure, 251
 - Matrix, 205
 - Prioritizing, 205
 - Process, 206–207
 - Risk Universe, 204
- Environmental Safeguards:
 - Best Practices, 196–197
 - Definition, 193
 - Human Life, 194
 - Nature, 194
 - Phased Applications, 195–196
 - Redundancy, 194–195
 - Risks, 195
- Evolution of Data, 11, 37
- Evolution of Networks, 22–26, 211
- Exploitation:
 - Authorized Accounts, 170
 - Costs, 25, 175
 - Credit Card Breaches, 53, 126
 - Cybervictims, 24
 - Identity Thefts, 53
 - Value of a Credit Card, 53
 - Veterans Administration, 31
 - Vectors of Threats, 89–90
- Fear Uncertainty and Doubt, 31
- Financial Executives
 - International (FEI), 21
- Financial Reporting, 207
- Firewalls, 216. *See also* ACLs
 - Best Practices, 172, 218
- Forensic, 119, 147, 176, 220, 223
- Frameworks and Standards:
 - Capability Maturity Model (CMMi), 42
 - Control Objectives for Information and related Technology (COBIT), 30, 67, 73, 90
 - Committee of Sponsoring Organizations Of The Treadway Commission (COSO) ERM, 110
 - Information Technology Infrastructure Library (ITIL), 64, 73, 90
 - ISO-17799, 51, 110
 - ISO-27001, 52
 - ISO-9000, 79
 - Myths of Adoption, 61
 - Turnbull Report, 64
- Gap Analysis:
 - Current State, 100–105, 204
 - Integration, 108
 - KPI, 107, 259
 - Presentation, 105–106
 - Remediation, 106–107
 - Stakeholder Acceptance, 104
 - Target State, 105, 222
 - Value of Human Assets, 108–109
- General Purpose Technologies (GPT), 20, 250
- Global Library, 65–66
- Global Operations:
 - Operating in, 40, 239, 256
 - Regional Risk Values, 100
- Globalization, 40, 239, 255–256
- Government Sponsored Publications, 43
- Google, 32, 38, 208, 214
- Governance:
 - Building a Contextual Framework, 41
 - Collaboration, 21–22, 38, 126, 211, 255
 - Convergence of Approaches, 81, 90–93
 - Expansion Primer Questions, 64
 - Fraud, 116, 207
 - Iterations, 95
 - Value of Internal Resources, 108–109
- Government Sponsored Authorities:
 - Committee Of Sponsoring Organizations Of The Treadway Commission (COSO), 46–47, 67, 110, 118
 - National Security Agency, 43
 - National Institute of Standards and Technology (NIST), 92
- Grid Computing, 203, 215
- Hackett Group, 40
- Human Resource Safeguards:
 - Appropriate Rights, 180
 - Best Practices, 181, 252
 - Corrective Action 120
 - Job Descriptions, 180
 - Monitoring, 120
 - New Hires, 180
 - Organizational Structure, 179–180
 - Program, 178
 - Risks, 179
 - Screening, 120
 - Training, 178–179, 181, 225
 - Whistleblower, 120
- Identity Theft:
 - Attacks, 53

- Impact, 11, 25
- Incident Response, 202, 211
- Incident Response Capability:
 - Best Practices, 226
 - Detection, 224–225
 - Management Direction, 223
 - Purpose, 223
 - Response Protocol, 225
 - Supportive Technology, 223
- Industries:
 - Energy, 55–56, 196, 245
 - Financial, 56–57
 - Payment Transaction
 - Environment, 52–54
- Industry Authorities:
 - Association of Certified Fraud Examiners (ACFE), 67, 110, 115
 - Center for Internet Security (CIS), 64, 90
 - Information Systems Audit and Control Association (ISACA), 43, 110, 115
 - Institute of Internal Auditors (IIA), 43, 110, 115
 - International Standards
 - Organization, 51–52, 79, 110
 - SysAdmin, Audit, Network, Security (SANS), 43
- Industry Mandates:
 - North American Electric Reliability Corporation (NERC), 53–56
 - Payment Card Industry Data Security Standards (PCI DSS), 52, 54, 68
- Information Technology
 - Environments:
 - Measured by Business, 103–105
 - Complexity, 43, 244
 - Convergence, 81, 243
 - Perception Bias, 72
 - Redefining, 255
 - Risks levied, 87–88
 - Valuations, 124
- Information Technology
 - Controls:
 - Advantages to Organization, 45–46, 244
 - Affects of Productivity, 38
 - Commonalities, 46
 - Definition, 46–47
 - Demonstration, 240
 - Globalization of, 40, 240
 - Organic Practices and Controls, 87
 - Parts of Business, 37
 - Race to the Bottom Threat, 40
 - Stickiness of, 63
- Institute Of Internal Auditors (IIA), 43, 110, 115
- Integrity, 208, 220
- Intellectual Property (IP):
 - Awareness, 86, 125
 - Protection of, 126, 207, 213
- Interconnected Universe, 3–16
 - Result of, 22
- Internal Control:
 - Advantages, 45–46
 - Annotated History, 49
 - Complacency, 253
 - Extrapolated Requirements, 48
 - Evolution, 249
 - Exhaustion, 73, 95
 - Future, 246–247
 - History, 71
 - Soft, 117
 - Weaknesses, 74
- Intrusion Detection Systems, 217, 223, 226
- Intrusion Prevention Systems, 214, 226
- Job Descriptions, 171
- Just In Time, 20
- Lean Management, 20
- Least Privilege, 172, 216, 218
- Life Cycle Management, 139–164
- Logs, 178, 211, 219
- Logical Access:
 - Best Practices, 172–173, 216
 - Context, 169–170
 - Means of, 169
 - Multifactor Authentication, 169, 171
 - Oversight, 169
- Mckay, Charles, 9
- Management Controls:
 - Ensured by, 29
 - “Right to Audit”, 85
- Mandates:
 - Federal, 50
 - Regional, 52
 - Self, 52
- Monitoring, 148, 169, 171, 210–211, 214, 216
- Monitoring and Performance
 - Reviews
 - Audit Trails, 219. (*See also* Logs)
 - Best Practices, 222
 - Feedback, 220
 - Inputs, 220
 - Intent, 219
 - Management, 220
 - Onsite and Inperson
 - Evaluations, 221
 - Quality Audit, 221
 - Remediation Actions, 221–222
 - Role of Internal Audit, 219, 221
 - Third Party Evaluations, 221. (*See also* Assessments)
- Network Segmentation, 217
- New Hire Safeguards, 119–120, 180
- Operational Efficiencies, 32
 - Business Incentives, 245
- Longevity, 259–260
- Metrics of Transparency in Supply Chain, 33
- Optimization, 257–258
- Operations Resiliency:
 - Approach, 189
 - Best Practices, 193
 - Business Continuity Plans. *See* BCP
 - Continuity, 188, 191–192
 - Dependencies, 191–192
 - Test Runs, 189
 - Time Value of Information, 190, 192
 - Quantifying Impacts to Operations, 189–190
- Penalties, 10, 31–32, 54, 94, 189, 220
- Performance Measurement:
 - Contractual Obligations, 212
 - Organizations, 43
 - Steps, 42, 254
 - Vendors, 215
- Physical Access:
 - Backup Media, 174
 - Best Practices, 177–178
 - Identification, 173, 175, 178
 - Portable Systems and Media, 174
 - Structures, 173
 - Time Value, 175
 - Visitor Policy, 173–175
- Policy and Procedures:
 - Documentation, 177, 216
 - Focus, 131
 - Practices, 131–132
 - Life cycle, 130
 - Reflective of culture, 128
 - Risks, 129–130
 - Starbucks, 128
- Principals:
 - Access and Authorization, 167. (*See also* Principle Three)
 - Challenges, 243–244
 - Life Cycle Management, 139. (*See also* Principle Two)
 - Origination, 241–243
 - Overview, 114
 - Security and Assurance, 201. (*See also* Principle Five)
 - Strategy Orchestration, 115. (*See also* Principle One)
 - Sustain Operations, 187. (*See also* Principle Four)
- Principle One:
 - Directional Alignment, 121
 - Policy and Procedures, 127
 - Publication Matrix, 133
 - Technology Governance, 124
 - Tone at the Top, 116
- Principle Two:
 - Acquire and Support, 140
 - Application Controls, 145
 - Change Control, 156
 - Publication Matrix, 161
 - Software Development, 149

- Principle Three:
 - Human Resources, 178
 - Logical Access, 168
 - Physical Access, 173
- Principle Four:
 - Environmental Safeguards, 193
 - Operations Resiliency, 188
- Principle, Five:
 - Incident Response
 - Capability, 223
 - Monitoring and Performance
 - Reviews, 219
 - Trusted Communication and
 - Networks, 211
 - Trusted Computing
 - Platform, 207
 - Risk Awareness, 202
- Prioritizing Risks:
 - Return to Operations, 187
- Project Management:
 - Failures, 203
 - Risks, 153–154
- Regulation:
 - Inefficiencies Result From, 39
 - Longevity, 57, 247, 256
 - Political Climate, 256
 - Shortcomings, 241
 - Trickling down, 50, 241
 - Weighing, 84–85, 258
- Regulations:
 - Basel II, 53, 56
 - EU Directives, 39, 46
 - Fair Credit Reporting Act (FCRA), 29, 39
 - Federal Financial Institutions Examination Council (FFIEC), 51, 65
 - Foreign Corrupt Practices Act (FCPA), 117
 - Gamm-Leach Bliley Act (GLBA), 51, 85
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA), 38, 65
 - Japan's Financial Instruments and Exchange Law (J-SOX), 47, 95
 - Sarbanes-Oxley (SOX), 29, 48, 50, 95
 - Benefits realized, 51
 - Financial Impact of, 51
 - Remote Access, 173, 217
 - Resources And Guidance:
 - Government, 43
 - International References, 69
 - Leverage Risk, 43
 - Return on Investment (ROI):
 - Data thieves, 30
- Risk:
 - Analysis, 97–100
 - Attack Vectors, 30, 89–91. (See also Attack Vectors)
 - Assessment, 154, 258
 - Characteristics of, 97–100
 - Impacts of, 31
 - Infrastructure, 257
 - Inherent Technology, 87–88
 - Universe, 204
- Risk Awareness:
 - Best Practices, 206–207
 - Defining, 203–205
 - Impact Assessment, 203–204. (See also Enterprise Risk Management)
 - Intelligence, 202–203
 - Proximity, 203
 - Thresholds, 204–205
- Risk Management:
 - Environmental, 193–195, 197
 - Of Vendors, 212
 - Proximity, 203
 - Standard and Poor, 108, 203
- Safe Harbor, 8, 39
- Security And Assurance, 201–236
- Segregation Of Duties, 172–173, 214
- Silos:
 - Existence, 240–241
 - Impacts of, 39
 - Introduction, 38
- Six Sigma, 20
- Software Configuration:
 - Patch Management, 139, 211
 - Vendor Default, 225
- Software Development:
 - Benefits, 149
 - Best Practices, 155–156
 - Costs, 150
 - COTS, 149
 - Data Classification, 150
 - In House, 149
 - Project Risks, 153–154
 - SDLC, 151. (See also Software Development Life Cycle)
 - Vendor Screening, 153
- Software Development Life Cycle (SDLC):
 - Phases, 151–153
 - Security Certification, 152
- Supervisory Control and Data Acquisition (SCADA), 55, 175
- Supply Chain, 32–33, 79, 126, 204, 256
- Sustain Operations, 187–200
 - Applicability to Public and Private Sectors, 187
- System Maintenance, 148
- Tailgating, 176
- Technology:
 - Internet Breakdowns, 257
 - Optimal, 257–258
 - Over Dependence, 257
- Technology Governance, 124
 - Best Practices, 126–127
 - Intellectual Property, 124
 - Classifications, 125–127
- Tone at the Top:
 - Best Practices, 119–120
 - Communications, 118, 259
 - Culture, 118, 260
 - Individual Actions, 119
 - Reflected By, 117–118
- Trusted Communications and
 - Network:
 - Anomaly Threats, 215
 - Baseling, 214
 - Channels, 211
 - Exposures, 212, 214
 - Extended Environments, 215. (See also Virtualization and Grid Computing)
 - Ubiquity, 211–212
 - Intelligence, 213
 - Segmentation, 213–204
 - Vendor Audit Mandates, 215
 - Trusted Computing Platform/
 - System Controls:
 - Attack Vectors, 210
 - Best Practices, 210–211
 - Continuous evaluations, 209–210
 - Data Management, 209
 - Encryption, 210
 - Importance, 207
 - Help Desk Trends, 209
 - Stored Data, 210
 - Virtual and Grid Baselines, 209 (See also Virtualization and Grid Computing)
 - Vulnerability Management, 209 (See also Assessments)
- Tulip Mania, 9
- Vendor Management:
 - Agreements, 85, 215, 228
 - Audits. (See Audits)
 - Best Practices, 144
 - Data Feeds, 211
 - Establishment, 140–141
 - Financial Benefits, 45–46
 - Financial Penalties, 191
 - Liability and
 - Indemnification, 179
 - Procurement, 142
 - Regular Evaluation, 152–153, 247
- Video Surveillance, 173–174, 177
- Virus, 24
- Virtualization, 4, 203, 215, 211
 - Best Practices, 215, 216
 - Operations, 37, 85, 191, 201, 203, 208, 212
- Voice Over Internet Protocol (VOIP), 190
- Whistleblower Hotline, 220
- Wireless (802.11), 171, 211, 213–214
- Work of Others, 38, 250
- Worksessions, 130, 192, 218, 206
- World Intellectual Property Organization (WIPO), 8
- World Wide Web Consortium (W3C), 26