OFFICIAL (ISC)² GUIDE TO THE CISSP® CBK®

Certified Information
Systems Security Professional

The most complete compendium of industry knowledge compiled by the foremost experts in global security. A must-have for those seeking to attain the Certified Information Systems Security Professional (CISSP®) credential.

Edited by **Adam Gordon** - CISSP-ISSAP, ISSMP, SSCP

(ISC)²®

FOURTH EDITION

OFFICIAL (ISC)²®
GUIDE TO THE
CISSP® CBK®
FOURTH EDITION

OTHER BOOKS IN THE (ISC)²® PRESS SERIES

Official (ISC)²® Guide to the CISSP® CBK®, Fourth Edition
Adam Gordon, Editor
ISBN: 978-1-4822-6275-9

Official (ISC)²® Guide to the HCISPP℠ CBK®
Steven Hernandez, Editor
ISBN: 978-1-4822-6277-3

Official (ISC)²® Guide to the CCFP℠ CBK®
Peter Stephenson, Editor
ISBN: 978-1-4822-6247-6

Official (ISC)²® Guide to the ISSAP® CBK®, Second Edition
Adam Gordon, Editor
ISBN: 978-1-4665-7900-2

Official (ISC)²® Guide to the CAP® CBK®, Second Edition
Patrick D. Howard
ISBN: 978-1-4398-2075-9

Official (ISC)²® Guide to the SSCP® CBK®, Second Edition
Harold F. Tipton, Editor
ISBN: 978-1-4398-0483-4

Official (ISC)²® Guide to the ISSAP® CBK®
Harold F. Tipton, Editor
ISBN: 978-1-4398-0093-5

Official (ISC)²® Guide to the ISSMP® CBK®
Harold F. Tipton, Editor
ISBN: 978-1-4200-9443-5

CISO Leadership: Essential Principles for Success
Todd Fitzgerald and Micki Krause, Editors
ISBN: 978-0-8493-7943-X

Official (ISC)²® Guide to the CISSP®-ISSEP® CBK®
Susan Hansche
ISBN: 978-0-8493-2341-X

OFFICIAL (ISC)²® GUIDE TO THE CISSP® CBK®

FOURTH EDITION

Edited by
Adam Gordon - CISSP-ISSAP, ISSMP, SSCP

(ISC)²®

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150206

International Standard Book Number-13: 978-1-4822-6276-6 (eBook - PDF)

CISSP®

Contents

Foreword xv
Introduction xvii
Editors xxi
Preface xxiii

Domain 1 — Security & Risk Management

Security & Risk Management 1
Confidentiality, Integrity, and Availability 7
Confidentiality 7
Integrity 7
Availability 7
Security Governance 9
Goals, Mission, and Objectives of the Organization 10
Organizational Processes 12
Security Roles and Responsibilities 13
Information Security Strategies 22
The Complete and Effective Security Program 23
Oversight Committee Representation 23
Control Frameworks 31
Due Care 33
Due Diligence 33
Compliance 34
Governance, Risk Management, and Compliance (GRC) 36
Legislative and Regulatory Compliance 37
Privacy Requirements Compliance 38

Global Legal and Regulatory Issues 41
Computer/Cyber Crime 41
Licensing and Intellectual Property 45
Import/Export 47
Trans-Border Data Flow 50
Privacy 51
Data Breaches 53
Relevant Laws and Regulations 55
Understand Professional Ethics 57
Regulatory Requirements for Ethics Programs 59
Topics in Computer Ethics 60
Common Computer Ethics Fallacies 61
Hacking and Hacktivism 63
Ethics Codes of Conduct and Resources 63
(ISC)2 Code of Professional Ethics 65
Support Organization's Code of Ethics 66
Develop and Implement Security Policy 71
Business Continuity (BC) & Disaster Recovery (DR) Requirements 72
Project Initiation and Management 72
Develop and Document Project Scope and Plan 74
Conducting the Business Impact Analysis (BIA) 75
Identify and Prioritize 75
Assess Exposure to Outages 78
Recovery Point Objectives (RPO) 79
Manage Personnel Security 80
Employment Candidate Screening 80
Employment Agreements and Policies 86
Employee Termination Processes 89
Vendor, Consultant, and Contractor Controls 89
Privacy 90
Risk Management Concepts 91
Organizational Risk Management Concepts 93
Risk Assessment Methodologies 95
Identify Threats and Vulnerabilities 102
Risk Assessment/Analysis 103
Countermeasure Selection 109
Implementation of Risk Countermeasures 109
Types of Controls 111
Access Control Types 116
Controls Assessment/Monitoring and Measuring 132
Tangible and Intangible Asset Valuation 144
Continuous Improvement 146
Risk Management Frameworks 147

Threat Modeling 156
Determining Potential Attacks and Reduction Analysis 157
Technologies & Processes to Remediate Threats 159
Acquisitions Strategy and Practice 161
Hardware, Software, and Services 161
Manage Third-Party Governance 163
Minimum Security and Service-Level Requirements 164
Security Education, Training, and Awareness 167
Formal Security Awareness Training 167
Awareness Activities and Methods – Creating the Culture of Awareness in the Organization 169

Domain 2 — Asset Security

Asset Security 183
Data Management: Determine and Maintain Ownership 187
Data Policy 187
Roles and Responsibilities 188
Data Ownership 189
Data Custodianship 189
Data Quality 190
Data Documentation and Organization 192
Data Standards 193
Data Lifecycle Control 194
Data Specification and Modeling 194
Database Maintenance 195
Data Audit 195
Data Storage and Archiving 196
Longevity and Use 197
Data Security 197
Data Access, Sharing, and Dissemination 198
Data Publishing 199
Classify Information and Supporting Assets 207
Asset Management 210
Software Licensing 212
Equipment Lifecycle 212
Protect Privacy 213
Ensure Appropriate Retention 218
Media, Hardware, and Personnel 218
Company "X" Data Retention Policy 220
Determine Data Security Controls 223
Data at Rest 223
Data in Transit 225
Baselines 228
Scoping and Tailoring 231

Standards Selection 232
United States Resources 232
International Resources 235
National Cyber Security Framework Manual 237
Framework for Improving Critical Infrastructure Cybersecurity 240

Domain 3 — Security Engineering

Security Engineering 249
The Engineering Lifecycle Using Security Design Principles 255
Fundamental Concepts of Security Models 260
Common System Components 261
How They Work Together 269
Enterprise Security Architecture 270
Common Architecture Frameworks 275
Zachman Framework 276
Capturing and Analyzing Requirements 288
Creating and Documenting Security Architecture 290
Information Systems Security Evaluation Models 291
Common Formal Security Models 291
Product Evaluation Models 292
Industry and International Security Implementation Guidelines 298
Security Capabilities of Information Systems 303
Access Control Mechanisms 303
Secure Memory Management 304
Vulnerabilities of Security Architectures 307
Systems 310
Technology and Process Integration 312
Single Point of Failure (SPOF) 318
Client-Based Vulnerabilities 321
Server-Based Vulnerabilities 323
Database Security 325
Large Scale Parallel Data Systems 327
Distributed Systems 331
Cryptographic Systems 335
Software and System Vulnerabilities and Threats 368
Web-Based 369
Vulnerabilities in Mobile Systems 372
Risks from Remote Computing 373
Risks from Mobile Workers 375
Vulnerabilities in Embedded Devices and Cyber-Physical Systems 377

The Application and Use of Cryptography 384
The History of Cryptography 384
Emerging Technology 386
Core Information Security Principles 387
Additional Features of Cryptographic Systems 387
The Cryptographic Lifecycle 389
Public Key Infrastructure (PKI) 392
Key Management Processes 393
Creation and Distribution of Keys 400
Digital Signatures 408
Digital Rights Management (DRM) 409
Non-Repudiation 411
Hashing 412
Simple Hash Functions 412
Methods of Cryptanalytic Attacks 415
Site and Facility Design Considerations 420
The Security Survey 420
Site Planning 423
Roadway Design 424
Crime Prevention through Environmental Design (CPTED) 424
Windows 426
Design and Implement Facility Security 431
Implementation and Operation of Facilities Security 432
Communications and Server Rooms 432
Restricted and Work Area Security 434
Data Center Security 435

Domain 4 — Communications & Network Security

Communications & Network Security 453
Secure Network Architecture and Design 459
OSI and TCP/IP 459
IP Networking 470
Directory Services 475
Implications of Multi-Layer Protocols 485
Converged Protocols 489
Implementation 490
Voice over Internet Protocol (VoIP) 499
Wireless 504
Wireless Security Issues 508
Cryptography Used to Maintain Communications Security 511

Securing Network Components 533
Hardware 537
Transmission Media 541
Network Access Control Devices 544
End Point Security 548
Content Distribution Networks 549
Secure Communication Channels 550
Voice 550
Multimedia Collaboration 553
Open Protocols, Applications, and Services 555
Remote Access 559
Data Communications 568
Virtualized Networks 590
Network Attacks 600
The Network as an Enabler or Channel of Attack 601
The Network as a Bastion of Defense 602
Network Security Objectives and Attack Modes 602
Scanning Techniques 608
Security Event Management (SEM) 614
IP Fragmentation Attacks and Crafted Packets 617
Denial-of-Service (DoS) / Distributed-Denial-of Service (DDoS) Attacks 621
Spoofing 623
Session Highjack 626

Domain 5 — Identity & Access Management

Identity & Access Management 635
Physical and Logical Access to Assets 641
Identification and Authentication of People and Devices 647
Identification, Authentication, and Authorization 647
Identity Management Implementation 656
Password Management 656
Account Management 658
Profile Management 659
Directory Management 659
Directory Technologies 660
Single/Multi-Factor Authentication 673
Accountability 684
Session Management 686
Registration and Proof of Identity 688
Credential Management Systems 691
Identity as a Service (IDaaS) 701
Integrate Third-Party Identity Services 706

Implement and Manage Authorization Mechanisms 709
Role-Based Access Control 709
Rule-Based Access Control 711
Mandatory Access Controls (MACs) 711
Discretionary Access Controls (DACs) 713
Prevent or Mitigate Access Control Attacks 714
Windows PowerShell Equivalent Commands 722
Identity and Access Provisioning Lifecycle 728
Provisioning 728
Review 729
Revocation 729

Domain 6 — Security Assessment & Testing

Security Assessment & Testing 737
Assessment and Test Strategies 743
Software Development as Part of System Design 744
Log Reviews 745
Synthetic Transactions 753
Code Review and Testing 755
Negative Testing/Misuse Case Testing 763
Interface Testing 765
Collect Security Process Data 769
Internal and Third-Party Audits 774
SOC Reporting Options 774

Domain 7 — Security Operations

Security Operations 785
Investigations 789
The Crime Scene 790
Policy, Roles, and Responsibilities 792
Incident Handling and Response 794
Recovery Phase 797
Evidence Collection and Handling 798
Reporting and Documenting 799
Evidence Collection and Processing 804
Continuous and Egress Monitoring 807
Data Leak/Loss Prevention (DLP) 809
Provisioning of Resources through Configuration Management 814

Foundational Security Operations Concepts 816
Key Themes 816
Controlling Privileged Accounts 817
Managing Accounts Using Groups and Roles 818
Separation of Duties and Responsibilities 820
Monitor Special Privileges 822
Job Rotation 823
Manage the Information Lifecycle 823
Service Level Agreements (SLAs) 825
Resource Protection 828
Tangible versus Intangible Assets 828
Hardware 829
Media Management 829
Incident Response 835
Incident Management 835
Security Measurements, Metrics, and Reporting 836
Managing Security Technologies 837
Detection 837
Response 839
Reporting 840
Recovery 840
Remediation and Review (Lessons Learned) 840
Preventative Measures against Attacks 842
Unauthorized Disclosure 842
Network Intrusion Detection System Architecture 843
Whitelisting, Blacklisting, and Greylisting… Oh My! 849
Third-party Security Services, Sandboxing, Anti-malware, Honeypots and Honeynets 849
Patch and Vulnerability Management 853
Security and Patch Information Sources 855
Change and Configuration Management 860
Configuration Management 861
Recovery Site Strategies 864
Multiple Processing Sites 867
System Resilience and Fault Tolerance Requirements 868
The Disaster Recovery Process 874
Documenting the Plan 875
Response 877
Personnel 881
Communications 881
Assessment 883
Restoration 883
Provide Training 884
Exercise, Assess, and Maintain the Plan 885

Test Plan Review 886
Tabletop Exercise/Structured Walk-Through Test 887
Walk-Through Drill/Simulation Test 888
Functional Drill/Parallel Test 888
Full-Interruption/Full-Scale Test 889
Update and Maintenance of the Plan 889
Business Continuity and Other Risk Areas 894
Implementation and Operation of Perimeter Security 894
Access Control 904
Card Types 905
Closed Circuit TV 906
Internal Security 917
Building and Inside Security 922
Personnel Safety 935
Privacy 935
Travel 935
Duress 937

Domain 8 — Security in the Software Development Life Cycle

Security in the Software Development Life Cycle 949
Software Development Security Outline 953
Development Life Cycle 954
Maturity Models 959
Operation and Maintenance 960
Change Management 961
Integrated Product Team (e.g., DevOps) 962
Environment and Security Controls 964
Software Development Methods 964
The Database and Data Warehousing Environment 967
Database Vulnerabilities and Threats 978
DBMS Controls 980
Knowledge Management 984
Web Application Environment 986
Security of the Software Environment 988
Applications Development and Programming Concepts 988
The Software Environment 990
Libraries & Toolsets 1001
Security Issues in Source Code 1004
Malicious Software (Malware) 1010
Malware Protection 1020

Software Protection Mechanisms 1025
Security Kernels, Reference Monitors, and the TCB 1025
Configuration Management 1040
Security of Code Repositories 1041
Security of Application Programming Interfaces (API) 1046
Assess the Effectiveness of Software Security 1049
Certification and Accreditation 1049
Auditing and Logging of Changes 1051
Risk Analysis and Mitigation 1052
Assess Software Acquisition Security 1059

Appendix A — Answers to Domain Review Questions 1071
Appendix B — Domain 1 Materials 1153
Appendix C — Domain 2 Materials 1167
Appendix D — Domain 3 Materials 1187
Appendix E — Domain 4 Materials 1191
Appendix F — Domain 5 Materials 1195
Appendix G — Domain 6 Materials 1201
Appendix H — Domain 7 Materials 1207
Appendix I — Domain 8 Materials 1219
Appendix J — Glossary 1227

CISSP®

Foreword

Foreword to the CISSP CBK Study Guide

As the dynamics of the information security industry evolve, so must the core components of the gold standard Certified Information Systems Security Professional (CISSP). Global subject matter experts reviewed the CISSP CBK and made significant changes to the content – in fact, 40% of the content is new. The ten domains of the CISSP have been reorganized into the following eight domains:

- ***Security and Risk Management*** – Apply security governance principles
- ***Asset Security*** – Classify information and supporting assets
- ***Security Engineering*** – Implement and manage an engineering lifecycle using security design principles
- ***Communication and Network Security*** – Apply secure design principles to network architecture
- ***Identity and Access Management*** – Control physical and logical access to assets
- ***Security Assessment and Testing*** – Design and validate assessment and test strategies
- ***Security Operations*** – Understand and apply foundational security operations concepts
- ***Software Development Security*** – Understand and apply security in the software development lifecycle

Advancements in technology continue to bring about the need for updates. We work tirelessly to ensure that our exam content is always relevant to the industry. I look forward to your feedback on the revamped CISSP exam, and congratulate you on taking the first step toward earning the certification that *SC Magazine* named "Best Professional Certification Program" for the fourth time.

Achieving the CISSP is the next step in advancing your career; not to mention, you'll gain access to unparalleled global continuing education resources, peer networking, mentoring, and a wealth of other opportunities. Becoming a member of (ISC)² elevates you into one of the largest communities of information security professionals in the world. Required by some of the world's most security conscious organizations and government entities, the CISSP validates that information security leaders possess the breadth of knowledge, skills, and experience required to credibly build and manage the security posture of their organizations/governments.

Through 100,000 credential holders, the CISSP continues to be recognized by the media and industry professionals as the benchmark for information security certification worldwide.

This *Official (ISC)² Guide to the CISSP CBK* is the best reference available, reflecting the most relevant topics in the ever-changing field of information security. It provides a robust and comprehensive guide to the new eight CISSP domains, with sub-topics on the issues that security professionals face today. Compiled and reviewed by CISSPs and luminaries around the world, this textbook provides an unrivaled study tool for the certification exam that is up-to-date and authoritative.

The road to becoming a CISSP is not easy and becomes even more challenging each year; but the end results are well worth all your efforts. Not only is the CISSP an objective measure of excellence, it has become the global standard for the information security profession. Managing security in today's operations without a CISSP is now tantamount to practicing medicine without a license.

Congratulations on your decision to broaden your horizons through the best security education and certification program in the world. Good luck!

— W. Hord Tipton, Former Executive Director, (ISC)²

Introduction

There are two main requirements that must be met in order to achieve the status of CISSP; one must take and pass the certification exam, and be able to demonstrate a minimum of 5 years of direct full-time security work experience in two or more of the 8 domains of the (ISC)² CISSP CBK. A firm understanding of what the 8 domains of the CISSP CBK are, and how they relate to the landscape of business is a vital element in successfully being able to meet both requirements and claim the CISSP credential. The mapping of the 8 domains of the CISSP CBK to the job responsibilities of the Information Security professional in today's world can take many paths, based on a variety of factors such as industry vertical, regulatory oversight and compliance, geography, as well as public versus private versus military as the overarching framework for employment in the first place. In addition, considerations such as cultural practices and differences in language and meaning can also play a substantive role in the interpretation of what aspects of the CBK will mean, and how they will be implemented in any given workplace.

It is not the purpose of this book to attempt to address all of these issues or provide a definitive proscription as to what is "the" path forward in all areas. Rather, it is to provide the official guide to the CISSP CBK, and in so doing, to lay out the information necessary to understand what the CBK is, and how it is used to build the foundation for the CISSP and its role in business today. To that end, it is important to begin any journey with a sense of place, specifically where you are, and where you want to end up; and as a result, what tools you will need to have in order to make the journey comfortable and successful. The most important tool that the intrepid traveler can have at their disposal is a compass, that trusty device that always allows one to understand in what direction they are heading, and get their bearings when necessary. The compass of the Information Security professional is their knowledge, experience, and understanding of the world around them. The thing that is amazing about a compass is that no matter where you stand on Earth, you can hold one in your hand and it will point toward the North Pole. While we do not need to know where the North Pole always is in Information Security, as a CISSP, you are expected to be able to provide guidance and direction to the businesses and users that you are responsible for. Being able to map the CISSP

CBK to your knowledge, experience, and understanding is the way that you will be able to provide that guidance, and to translate the CBK into actionable and tangible elements for both the business and its users that you represent.

1. The ***Security and Risk Management*** domain addresses the framework and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets and to assess the effectiveness of that protection. It includes issues of governance, organizational behavior, and security awareness. Information security management establishes the foundation of a comprehensive and proactive security program to ensure the protection of an organization's information assets. Today's environment of highly interconnected, interdependent systems necessitates the requirement to understand the linkage between information technology and meeting business objectives. Information security management communicates the risks accepted by the organization due to the currently implemented security controls, and continually works to cost effectively enhance the controls to minimize the risk to the company's information assets. Security management encompasses the administrative, technical, and physical controls necessary to adequately protect the confidentiality, integrity, and availability of information assets. Controls are manifested through a foundation of policies, procedures, standards, baselines, and guidelines.
2. The ***Asset Security*** domain contains the concepts, principles, structures, and standards used to monitor and secure assets and those controls used to enforce various levels of confidentiality, integrity, and availability. Information security architecture and design covers the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that these practices and processes align with the organization's core goals and strategic direction.
3. The ***Security Engineering*** domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability. Information security architecture and design covers the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that these practices and processes align with the organization's core goals and strategic direction.
4. The ***Communication and Network Security*** domain encompasses the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media. Network security is often described as the cornerstone of IT security. The network is a central asset, if not the most central, in most IT environments. Loss of network assurance (the combined properties of confidentiality, integrity, availability, authentication, and non-repudiation) on any level can have devastating consequences, while control of the network provides an easy and consistent venue of attack. Conversely, a well-architected and well-protected network will stop many attacks in their tracks.

5. Although ***Identity and Access Management*** is a single domain within the CISSP Common Body of Knowledge (CBK), it is the most pervasive and omnipresent aspect of information security. Access controls encompass all operational levels of an organization:
   - ***Facilities*** – Access controls protect entry to, and movement around, an organization's physical locations to protect personnel, equipment, information, and, other assets inside that facility.
   - ***Support Systems*** – Access to support systems (such as power, heating, ventilation and air conditioning (HVAC) systems; water; and fire suppression controls) must be controlled so that a malicious entity is not able to compromise these systems and cause harm to the organization's personnel or the ability to support critical systems.
   - ***Information systems*** – Multiple layers of access controls are present in most modern information systems and networks to protect those systems, and the information they contain, from harm or misuse.
   - ***Personnel*** – Management, end users, customers, business partners, and nearly everyone else associated with an organization should be subject to some form of access control to ensure that the right people have the ability to interface with each other, and not interfere with the people with whom they do not have any legitimate business.

   The goals of information security are to ensure the continued Confidentiality-Integrity-Availability of an organization's assets. This includes both physical assets (such as buildings, equipment, and, of course, people) and information assets (such as company data and information systems.) Access controls play a key role in ensuring the confidentiality of systems and information. Managing access to physical and information assets is fundamental to preventing exposure of data by controlling who can see, use, modify, or destroy those assets. In addition, managing an entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen. It is also a key factor for many organizations that are required to protect personal information in order to be compliant with appropriate legislation and industry compliance requirements.

6. ***Security Assessment and Testing*** covers a broad range of ongoing and point-of-time based testing methods used to determine vulnerabilities and associated risk. Mature system development lifecycles include security testing and assessment as part of the development, operations and disposition phases of a system's life. The fundamental purpose of test and evaluation (T&E) is to provide knowledge to assist in managing the risks involved in developing, producing, operating, and sustaining systems and capabilities. T&E measures progress in both system and capability development. T&E provides knowledge of system capabilities and limitations for use in improving the system performance, and for optimizing system use in operations. T&E expertise must be brought to bear at the beginning of the system life cycle to provide earlier learning about the strengths and weaknesses of the system under development. The goal is early identification of technical, operational, and system deficiencies, so that appropriate and timely corrective actions can be developed prior to fielding the system. The creation of the test and evaluation strategy involves planning for technology development, including risk; evaluating the system design against mission requirements; and identifying where competitive prototyping and other evaluation techniques fit in the process.

7. The ***Security Operations*** domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information. It includes the definition of the controls over hardware, media, and the operators with access privileges to any of these resources. Auditing and monitoring are the mechanisms, tools and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process. The Information Security professional should always act to Maintain Operational Resilience, Protect Valuable Assets, Control System Accounts and Manage Security Services Effectively. In the day to day operations of the business, maintaining expected levels of availability and integrity for data and services is where the Information Security professional impacts Operational Resilience. The day to day securing, monitoring, and maintenance of the resources of the business, both human and material, illustrate how the Information Security professional is able to Protect Valuable Assets. Providing a system of checks and balances with regards to privileged account usage, as well as system access, allows the Information Security professional to act to Control Systems Accounts in a consistent way. The use of change and configuration management by the Information Security professional, as well as reporting and service improvement programs (SIP), ensures that the actions necessary to Manage Security Services Effectively are being carried out.
8. The ***Software Development Security*** domain requires a security professional to be prepared to do the following:
   - Understand and apply security in the software development lifecycle
   - Enforce security controls in the development environment
   - Assess the effectiveness of software security
   - Assess software acquisition security

   Although information security has traditionally emphasized system-level access controls, the security professional needs to ensure that the focus of the enterprise security architecture includes applications, since many information security incidents now involve software vulnerabilities in one form or another. Application vulnerabilities also allow an entry point to attack systems, sometimes at a very deep level. When examined, most major incidents, breaches and outages will be found to involve software vulnerabilities. Software continues to grow increasingly larger and more complex with each release. In addition, software is becoming standardized, both in terms of the programs and code used as well as the protocols and interfaces involved. Although this provides benefits in training and productivity, it also means that a troublesome characteristic may affect the computing and business environment quite broadly. Also, legacy code and design decisions taken decades ago are still involved in current systems and interact with new technologies and operations in ways that may open up additional vulnerabilities that the security professional may, or may not, even be aware of.

CISSP®

Editors

Adam Gordon – *Lead Editor*

With over 25 years of experience as both an educator and IT professional, Adam holds numerous Professional IT Certifications including CISSP, CISA, CRISC, CHFI, CEH, SCNA, VCP, and VCI. Adam holds his Bachelor's Degree in International Relations and his Master's Degree in International Political Affairs from Florida International University.

Adam has held a number of positions during his professional career including CISO, CTO, Consultant, and Solutions Architect. He has worked on many large implementations involving multiple customer program teams for delivery.

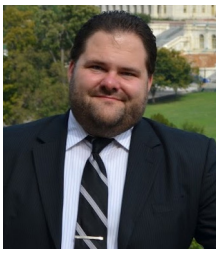
Adam has been invited to lead projects for companies such as Microsoft, Citrix, Lloyds Bank TSB, Campus Management, US Southern Command (SOUTHCOM), Amadeus, World Fuel Services, and Seaboard Marine.

Javvad Malik – *Lead Technical Editor*

Javvad Malik is a Senior Analyst in the 451 Enterprise Security Practice, providing in-depth, timely perspective on the state of enterprise security and emerging trends. Prior to joining 451 Research, he was an independent security consultant, with an extensive career spanning 12+ years working for some of the largest companies in the world.

Javvad is an active blogger, event speaker and possibly best known as one of the industry's most prolific video bloggers with his signature fresh and light-hearted perspective on security that speak to both technical and non-technical audiences alike. His articles regularly feature in online and print media, he is a coauthor of The Cloud Security Rules book and a volunteer member of the $(ISC)^2$ foundations Safe and Secure Online initiative. Javvad was a founder of the Security B-Sides London conference, in 2010 was named as a finalist for SC Magazine's Blogger of the Year award and in 2013 won the RSA Social Security Blogger award for the most entertaining blogger as well as winning best security video blogger and most

entertaining blog at the European Security Blogger awards. You can follow him on Twitter as @J4vv4D or on his website www.J4vv4D.com.



Steven Hernandez – *Technical Editor*

Steven Hernandez MBA, HCISPP, CISSP, CSSLP, SSCP, CAP, CISA, is a Chief Information Security Officer practicing in the U.S. Federal Government in Washington DC. Hernandez has over seventeen years of information assurance experience in a variety of fields including international healthcare, international heavy manufacturing, large finance organizations, educational institutions, and government agencies. Steven is an Honorary Professor at California State University San Bernardino and affiliate faculty at the National Information Assurance Training and Education Center located at Idaho State University. Through his academic outreach, he has lectured over the past decade on numerous information assurance topics including risk management, information security investment, and the implications of privacy decisions to graduate and postgraduate audiences. In addition to his credentials from (ISC)², Hernandez also holds six U.S. Committee for National Security Systems certifications ranging from systems security to organizational risk management. Steven also volunteers service to (ISC)²'s Government Advisory Board and Executive Writers Bureau. Steven enjoys relaxing and traveling with his wife, whose patience and support have been indispensable in his numerous information assurance pursuits.

Preface

Audience Voice

In the following domain discussions, three specific audience roles will be addressed as noted below:

1. ***The Security Architect*** – Responsible for the enterprise security architecture of the enterprise
2. ***The Security Practitioner*** – Responsible for the tactical and operational elements of the security infrastructure of the enterprise
3. ***The Security Professional*** – Responsible for the managerial oversight of the security elements of the enterprise

Each of these roles is important in its own right, and often will be found standing alone as a separate job within the enterprise. On occasion, one or more of these roles will be combined together within a single job role or function within the enterprise. The CISSP candidate will need to understand ALL three roles, and incorporate aspects of all of them in order to be successful as a member of the information security community.

Please make sure that as you read through the discussions within this domain that you take note of which voice, or voices, are being referenced with regards to actions and activities. Being able to understand what each of these roles is responsible for within the enterprise will be a valuable addition to the skills and knowledge that the CISSP candidate should have.

The Fourth Edition – What's New?

While there has been some reclassification of the domain names within the CISSP Common Body of Knowledge (CBK), the important thing to note is what has been introduced from a content perspective. With that in mind, here is a partial list of some of the new material you can expect to see:

- Within the *Security and Risk Management* domain
  - Compliance
  - Data Breaches
  - Conducting a Business Impact Analysis (BIA)
  - Implementation

- Continuous improvement
- Threat Modeling
- Determining potential attacks
- Performing a Reduction Analysis
- Technologies and processes used to remediate threats
- Integrating security risk considerations into acquisitions strategy and practice
- Third-Party assessments
- Minimum security requirements
- Service-Level requirements
- Appropriate levels of awareness, training, and education within an organization
- Periodic reviews for content relevancy

- Within the *Asset Security* domain
  - Data owners
  - Data processes
  - Data Remanence
  - Baselines
  - Scoping and tailoring
  - Standards selection
- Within the *Security Engineering* domain
  - Implementing and managing an engineering lifecycle using security design principles
  - Large scale parallel data systems
  - Cryptographic systems
  - Assessing and mitigating vulnerabilities in mobile systems
  - Embedded devices and cyber-physical systems
  - Data Rights Management (DRM)
  - Designing and implementing facility security
  - Wiring closets
- Within the *Communications and Network Security* domain
  - Converged protocols
  - Software defined networks
  - Content distribution networks
  - Physical devices
  - Virtualized networks
- Within the *Identity and Access Management* domain
  - Controlling physical and logical access to assets
  - Registration and proof of identity
  - Credential management systems
  - Integrating Identity as a Service
  - Integrating third-party identity services
  - Preventing or mitigating access control attacks

- Within the *Security Assessment and Testing* domain
  - Assessment and testing strategies
  - Security control testing
  - Log reviews
  - Code review and testing
  - Negative testing
  - Misuse case testing
  - Test coverage analysis
  - Interface testing
  - Collecting security process data
  - Account management
  - Management review
  - Key performance and risk indicators
  - Analyzing and reporting test output
- Within the *Security Operations* domain
  - Understanding the requirements for various investigation types
    - Operational
    - Criminal
    - Civil
    - Regulatory
    - Electronic Discovery (eDiscovery)
  - Continuous monitoring
  - Egress monitoring
  - Securing the provisioning of resources
  - Configuration Management
  - Physical assets
  - Virtual assets
  - Cloud assets
  - Application provisioning
  - Service Level Agreements (SLA)
  - Hardware and Software asset management
  - Mitigation
  - Lessons learned
  - Whitelisting/Blacklisting
  - Third-Party security services
  - Sandboxing
  - Honeypots/Honeynets
  - Antimalware
  - Testing a Disaster Recovery Plan
    - Read through
    - Walk through
    - Simulation
    - Parallel
    - Full interruption

- Within the *Software Development Security* domain
  - Integrated product teams
  - Code repositories
  - Application Program Interfaces (APIs)
  - Acceptance testing
  - Assessing software acquisition security

In addition, there have been nine new appendices added with useful forms and process that can help the security professional in their day-to-day job functions as well as a glossary with over 450 definitions. Finally there are almost 200 end of domain practice questions with the answers and rationale provided in Appendix A.

CISSP®

Domain 1
Security & Risk Management

The "Security and Risk Management" domain of the Certified Information Systems Security Professional (CISSP)® Common Body of Knowledge (CBK)® addresses the framework and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets and to assess the effectiveness of that protection. It includes issues of governance, organizational behavior, and security awareness.

Information security management establishes the foundation of a comprehensive and proactive security program to ensure the protection of an organization's information assets. Today's environment of highly interconnected, interdependent systems necessitates the requirement to understand the linkage between information technology and meeting business objectives. Information security management communicates the risks accepted by the organization due to the currently implemented security controls, and it continually works to cost effectively enhance the controls to minimize the risk to the company's information assets. Security management encompasses the administrative, technical, and physical controls necessary to adequately protect the confidentiality, integrity, and availability of information assets. Controls are manifested through a foundation of policies, procedures, standards, baselines, and guidelines.

Information security management practices that manage risk include such tools as risk assessment, risk analysis, data classification, and security awareness. Information assets are classified, and through risk assessment, the threats and vulnerabilities related to these assets are categorized, and the appropriate safeguards to mitigate risk of compromise can be identified and prioritized by the security professional.

Risk management minimizes loss to information assets due to undesirable events through identification, measurement, and control. It encompasses the overall security review, risk analysis, selection and evaluation of safeguards, cost–benefit analysis, management decision, and safeguard identification and implementation, along with ongoing effectiveness review. Risk management provides a mechanism to the organization

to ensure that executive management knows current risks, and informed decisions can be made to use one of the risk management principles: risk avoidance, risk transfer, risk mitigation, or risk acceptance, all described in more detail later in this chapter.

Security management is concerned with regulatory, customer, employee, and business partner requirements for managing data as they flow between the various parties to support the processing and business use of the information. Confidentiality, integrity, and availability of the information must be maintained throughout the process.

Business continuity planning (BCP) and disaster recovery planning (DRP) address the preparation, processes, and practices required to ensure the preservation of the organization in the face of major disruptions to normal organization operations. BCP and DRP involve the identification, selection, implementation, testing, and updating of processes and specific prudent actions necessary to protect critical organization processes from the effects of major system and network disruptions and to ensure the timely restoration of organization operations if significant disruptions occur.

This chapter describes a process for building an enterprise-wide business continuity (BC) program. It discusses the evolution of the industry regulations that have influenced or in some cases mandated that organizations build programs within their organization that will ensure the continuation of their organization "no matter what."

Finally, it discusses the interrelationship between information security and BC and other risk management areas such as physical security, records management, vendor management, internal audit, financial risk management, operational risk management, and regulatory compliance (legal and regulatory risk) in the context of the overall BC risk management framework shown in *Figure 1.1*.

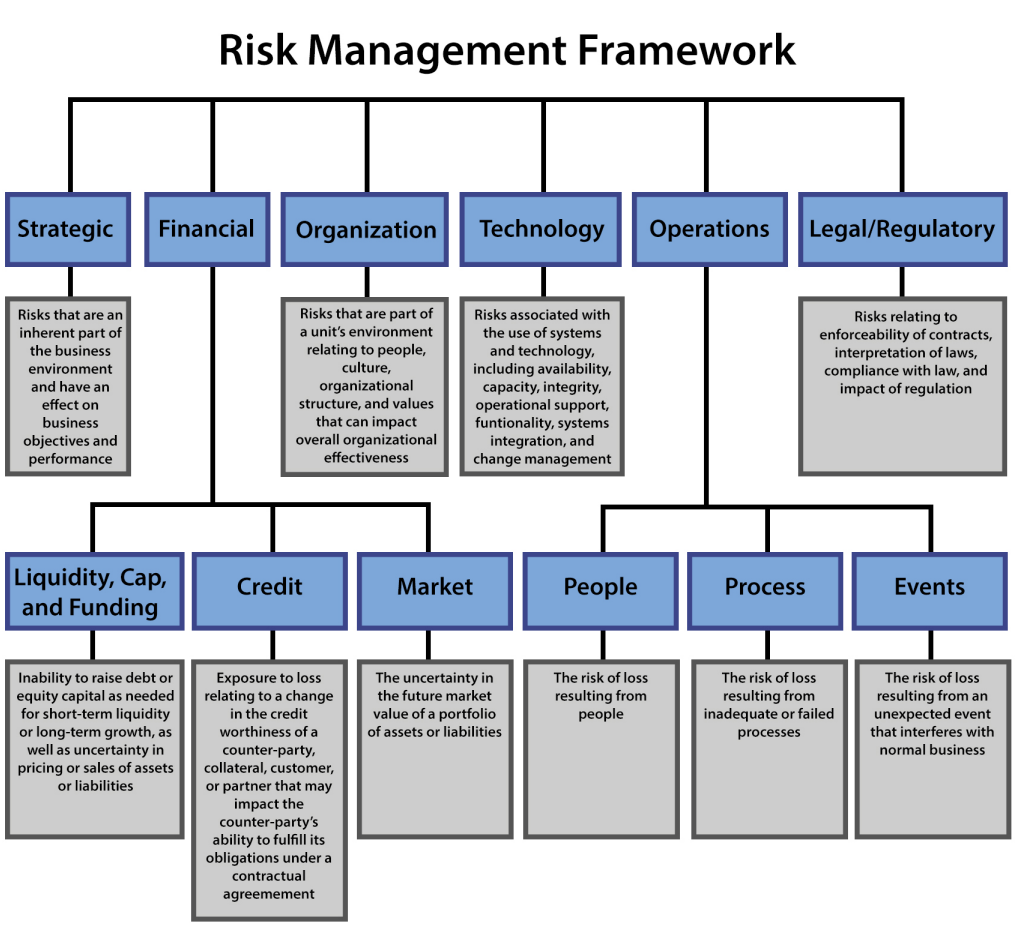


Figure 1.1 – **BC Risk Management Framework**

TOPICS

- The concepts of confidentiality, integrity, and availability
- Security governance principles
- Compliance
- Legal and regulatory issues
- Documented security policy, standards, procedures, and guidelines
- Business continuity requirements
- Personnel security policies
- Risk management concepts
- Threat modeling
- Integrating security risk considerations into acquisitions strategy and practice
- Security education, training, and awareness

OBJECTIVES

According to the (ISC)^2 Candidate Information Bulletin (Exam Outline), a CISSP candidate is expected to be able to:

- Understand and apply concepts of confidentiality, integrity, and availability.
- Apply security governance principles through compliance
- Understand legal and regulatory issues that pertain to information security in a global context.
- Develop and implement documented security policy, standards, procedures, and guidelines.
- Understand business continuity requirements.
- Contribute to personnel security policies.
- Understand and apply risk management concepts.
- Understand and apply threat modeling.
- Integrate security risk considerations into acquisitions strategy and practice.
- Establish and manage security education, training, and awareness.

Confidentiality, Integrity, and Availability

A well-structured, enterprise-wide information security program must ensure that the core concepts of availability, integrity, and confidentiality are supported by adequate security controls designed to mitigate or reduce the risks of loss, disruption, or corruption of information. Each of the security principles of the CIA triad is defined as follows:

Confidentiality

Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. The level of access that authorized individuals should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals who may be able to commit crimes by viewing the information. Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.

An important measure that the security architect should use to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information. A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessed by an unauthorized person.

Integrity

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes. Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices.

Sample controls include management controls such as segregation of duties, approval checkpoints in the systems development life cycle (SDLC), and implementation of testing practices that assist in providing information integrity. Well-formed transactions and security of the update programs provide consistent methods of applying changes to systems. Limiting update capability to those individuals with a documented need to access limits the exposure to intentional and unintentional modification.

Availability

Availability is the principle that ensures that information is available and accessible to users when needed. The two primary areas affecting the availability of systems are

1. Denial-of-Service attacks
2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

In either case, the end-user does not have access to information needed to conduct business. The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes. The lack of

appropriate security controls can increase the risk of viruses, destruction of data, external penetrations, or denial-of-service (DOS) attacks. Such events can prevent the system from being used by normal users.

Sample controls include an up-to-date and active anti-malicious code detection system, tested incident management plans, and disaster recovery planning or business continuity planning that ensure that the department functions using alternate processes when an outage to the computer system occurs for a defined period. Disaster recovery ensures that all or parts of information technology processing systems can be recovered. Disaster recovery and business continuity work together to minimize the impact of critical events on the enterprise.

When considering the design and implementation of a network, system, application, or management process, the security professional should understand the evaluation of the impact to confidentiality, integrity, and availability.

- The main question that the security architect needs to ask is "Will it **enhance** any of the core security principles?"
- The main question that the security practitioner needs to ask is "Will it **impact** any of the core security principles?"

Different security controls apply to different core security principles. An example would be the selection of a backup tape procedure. The software and hardware necessary to perform the backups would be most oriented toward the availability aspect of information security, whereas the selection of a security token utilizing strong, two-factor authentication would be most related to the enhancement of the confidentiality of information through improving authentication. An identity management system would be best deployed to support access control in order to ensure that only the appropriate personnel have update functions commensurate with their job supporting the integrity principle.

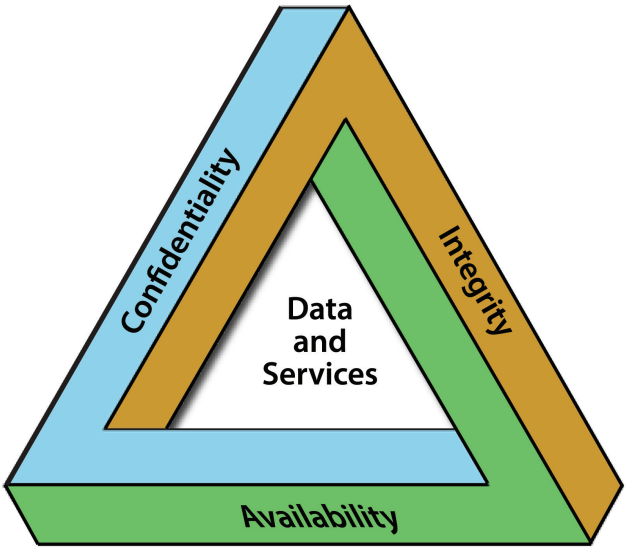


Figure 1.2 – **The CIA Triad**

Security Governance

Increased corporate governance requirements have caused companies to examine their internal control structures more closely to ensure that controls are in place and operating effectively. Organizations are increasingly competing in the global marketplace, which is governed by multiple laws and supported by various best practices (i.e., NIST, ITIL, ISO 27000, COSO, and COBIT). Appropriate information technology investment decisions must be made that are in alignment with the mission of the business. Information technology is no longer a back-office accounting function in most businesses, but rather it is a core operational necessity for the business, which must have the proper visibility to the board of directors and management's attention and oversight of the program.

This dependence on information technology mandates ensuring the proper alignment and understanding of the potential risks to the business. Substantial investments are made in these technologies (which must be appropriately managed), company reputations are at risk if insecure systems are deployed or found to be operating, and the trust in the systems needs to be demonstrated to all parties involved, including the shareholders, employees, business partners, and customers. Information security governance provides the mechanisms for the board of directors and management to have the proper oversight to manage the risk to the enterprise to an acceptable level.

The intent of governance is to guarantee that the appropriate information security activities are being performed to ensure that the risks are appropriately reduced, the information security investments are appropriately directed, and that executive management has visibility into the program and is asking the appropriate questions to determine the effectiveness of the program.

The IT Governance Institute (ITGI), in their publication entitled "Board Briefing on IT Governance, 2nd edition," defines IT governance as being "the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."[1]

The ITGI proposes that information security governance should be considered a part of IT governance and that the board of directors should:

- Be informed about information security
- Set direction to drive policy and strategy
- Provide resources to security efforts
- Assign management responsibilities
- Set priorities
- Support changes required
- Define cultural values related to risk assessment
- Obtain assurance from internal or external auditors
- Insist that security investments are made measurable and reported on for program effectiveness.

1 See the following: ITGI main website: http://www.itgi.org
ITGI Board Briefing on IT Governance 2nd edition: http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf

Additionally, the ITGI suggests that the management should:

- Write security policies with business input
- Ensure that roles and responsibilities are defined and clearly understood
- Identify threats and vulnerabilities
- Implement security infrastructures and control frameworks (standards, guidelines, baselines, and procedures)
- Ensure that policy is approved by the governing body
- Establish priorities and implement security projects in a timely manner
- Monitor breaches
- Conduct periodic reviews and tests
- Reinforce awareness education as critical
- Build security into the systems development life cycle

The security professional needs to work in partnership with management in order to ensure that these goals are achieved. These concepts are further delineated throughout this chapter.

Goals, Mission, and Objectives of the Organization

Information security management practices protect the assets of the organization through the implementation of physical, administrative, managerial, technical, and operational controls. Information assets must be managed appropriately to reduce the risk of loss to confidentiality, integrity, or availability. Just as financial assets are managed through finance departments, human assets (people) are managed and cared for by the human resources department and so are associated codes of conduct and employment policies and practices. Failure to protect information assets from loss, destruction, or unexpected alteration can result in significant losses of productivity, reputation, or financial loss. Information and the systems supporting the mission of an organization are assets that must be protected by the security professional.

Information security management validates that appropriate policies, procedures, standards, and guidelines are implemented to ensure business operations are conducted within an acceptable level of risk. Security exists to support and enable the vision, mission, and business objectives of the organization. Effective security management requires judgment based upon the risk tolerance of the organization, the costs to implement the security controls, and the benefit to the business. Although attaining 100% security of information is an admirable goal, in practice this is unrealistic. Even if this goal were attainable through an effective security program that includes all the best security practices for managing risk and a budget that would support all of the activities, it would not be long before a new vulnerability or exploit was discovered that could place the information at risk. As a result, a well-structured and managed program must be proactive and ongoing.

Because most organizations are in a competitive environment that requires continuous product innovation and reduction of administrative costs, funding information security at the "100% security level" is cost-prohibitive and impracticable for the organization. Therefore, effective security management requires risk management that includes a strong understanding of the business objectives of the organization, senior management's tolerance for risk, the costs of the various security alternatives, and, subsequently, the due diligence to match the appropriate security controls to the business initiatives. The security professionals who lead the information security program are relied upon for their knowledge of security and risk

management principles. Senior management ultimately makes the final decision on the level of security expenditures and the risk it is willing to accept.

Security professionals should view their role as risk advisors to the organization, as they should not be the final decision makers when it comes to risk management. There may be situations where a risk is viewed as low, and therefore, senior management is willing to take a risk due to reasons that the security professional may not understand or be aware of. For example, the decision to accept operating in a regional office without a sprinkler system may be appropriate if the company has been operating in that office for ten years without a fire and management has undisclosed plans to relocate the office within the next six months.

Alternatively, there may be government mandates to comply with new regulations or audit findings that have a higher priority. Senior management must weigh all of the risks to the business, and choosing whether to implement specific security controls represents one of those risk management activities. This is why security professionals must be effective at communicating risks and possible security solutions. There will always be residual risk accepted by an organization, and effective security management will minimize this risk to a level that fits within the organization's risk tolerance or risk profile.

Security management is the glue that ensures that the risks are identified and an adequate control environment is established to mitigate the risks. Security management ensures the interrelationships among assessing risk, implementing policies and controls in response to the risks, promoting awareness of the expectations, monitoring the effectiveness of the controls, and using this knowledge as input to the next risk assessment. These relationships are shown in *Figure 1.3*.

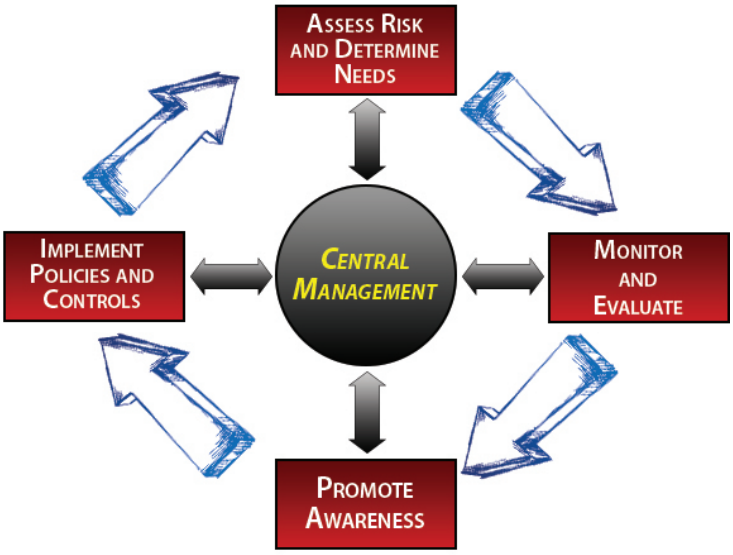


Figure 1.3 – **Security and Risk Management Relationships**

Organizational Processes

Understanding the mission of an organization and the processes that support it is critical for the success of a security program. In many ways, an organization is like a living thing. It may go through several phases of growth, decline, and illness during its lifetime. Understanding of the business transformational events and entities ensures the security professional maintains situational awareness of what is occurring in the boardroom and the management decisions being made on a day-to-day basis throughout the enterprise. For example, the following are common activities organizations undergo that may impact the security professional:

- ***Acquisitions and Mergers –*** Organizations combine for many reasons. Some mergers are friendly with both parties realizing a gain from the merger, while others may be described as "hostile." In either situation, the information security professional must be aware of the following items and plan accordingly:
  - Additional data types that may need more protection than the existing security program provides
  - Additional technology types that may need more protection than the existing security program provides
  - New staff and roles with enhanced requirements for security awareness and training
  - Threats from former employees or possibly threats the new organization will face that the old one did not
  - Vulnerabilities when systems are merged
  - Potentially new policies, standards, and procedures to support compliance with any laws, regulations, and requirements that the organization will need to be aware of
  - External business partners and interconnections that will need review and assessment
- ***Divestitures and Spinoffs –*** The opposite of an acquisition or a merger, a divesture may involve the spinoff of a part of an organization or possibly the complete liquidation of an existing organization. These are tense times in an organization, and the information security professional should be concerned with the following situations and plan accordingly:
  - Data loss and data leakage due to employees leaving for the spinoff or another company
  - System interconnections, protocols, and ports left open after the function they were serving is no longer applicable
  - Loss of visibility into the network and system logs if both organizations did not keep the appropriate security monitoring tools and capabilities in house
  - New threats from employees who may have been laid off or forced out of the organization
  - The need to revise policies, standards, and procedures to recognize any new governance bodies in the organization and reflect the organization change if applicable
  - The need to meet any divestiture imposed deadlines for data segregation or spinoff between organizations

- ***Governance Committees –*** A governance committee is responsible for recruiting and maintaining the governance board for an organization. The committee is also typically responsible for determining missing qualifications and characteristics needed to enhance the efficiency and effectiveness of the board. The security professional should learn how the board functions and, as much as possible, attempt to:
  - Ensure the committee understands at a high level the importance of information security and risk management.
  - Ensure committee recruitment exercises for new board members include requirements for information security and risk aptitude where needed.
  - Maintain a working relationship with committee members and be available to respond to specific risk, privacy, and information security questions as needed.

Security Roles and Responsibilities

Many different individuals within an organization contribute to successful information protection. Security is the responsibility of everyone within the company. Every end-user is responsible for understanding the policies and procedures that are applicable to his or her particular job function and adhering to any and all security control expectations. Users must have knowledge of their responsibilities and be trained to a level that is adequate to reduce the risk of loss to an acceptable level. Although the exact titles and scope of responsibility of the individuals may vary from organization to organization, the following roles support the implementation of security controls. An individual may be assigned multiple roles for the organization. It is important to provide clear definition and communication of roles and responsibilities including accountability through the distribution of policies, job descriptions, training, and management direction, as well as providing the foundation for execution of security controls by the workforce.

Today's Security Organizational Structure

There is no "one size fits all" for the information security department or the scope of the responsibilities. The location of where the security organization should report has also been evolving. In many organizations, the Information Systems Security Officer (ISSO) or Chief Information Security Officer (CISO) still reports to the Chief Information Officer (CIO) or the individual responsible for the information technology activities of the organization. This is due to the fact that many organizations still view the information security function as an information technology problem and not a core business issue.

Alternatively, the rationale for this may be due to the necessity to communicate in a technical language, which is understood by information technology professionals and not typically well understood by business personnel. Regardless of the rationale for the placement, placing the individual responsible for information security within the information technology organization could represent a conflict of interest because the IT department is motivated to deliver projects on time, within budget, and of high quality. Shortcuts may be taken on the security requirements to meet these constraints, if the security function is reporting to the individual making these decisions. The benefit of having the security function report to the CIO is that the security department is more likely to be engaged in the activities of the IT department and aware of the upcoming initiatives and security challenges.

There is a growing trend toward integrating the information and physical security functions. This is partially a result of the increased automation of physical controls and requirements on physical aspects of security to protect information. There has been less separation in these areas and more integration. This growing trend is for the security function to be treated as a risk management function and, as such, be located outside of the IT organization. This provides a greater degree of independence as well as the focus on risk management versus management of user IDs, password resets, and access authorization with the reporting relationship outside of the IT organization, which also introduces a different set of checks and balances on the security activities that are expected to be performed. The security function may report to some other function outside of information technology. The function should report as high in the organization as possible, preferably at the C-level. This ensures that the proper message is conveyed to senior management, the company employees view the appropriate authority of the department, and funding decisions can be made while considering the needs across the company.

Responsibilities of the Information Security Officer

The Information Security Officer is accountable for ensuring the protection of all of the business information assets from intentional and unintentional loss, disclosure, alteration, destruction, and unavailability. The security officer typically does not have the resources available to perform all of these functions and must depend upon other individuals within the organization to implement and execute the policies, procedures, standards, and guidelines to ensure the protection of information. In this capacity, the information security officer acts as the facilitator of information security for the organization.

The threat environment is constantly changing and, as such, it is incumbent upon the security officer to keep up with the changes. It is difficult for any organization to anticipate new threats, some of which come from the external environment and some from new technological changes. Prior to the September 11, 2001 terrorist attack in the United States, few individuals perceived that sort of attack as very likely. However, since then, many organizations have revisited their access control policies, physical security, and business continuity plans. More recently, the issues raised by the disclosures made by Edward Snowden have forced a reevaluation and reconsideration of security policy and practice throughout the world, for both the enterprise and the individual. New technologies, such as wireless, low-cost removable media (writeable DVDs and USB drives), and mobile computing devices such as laptops, tablets, and smartphones have created new threats to confidentiality and disclosure of information, which need to be addressed. Although the organization tries to write policies to last for two or three years without change, depending upon the industry and the rate of change, these may need to be revisited more frequently.

The security officer and his or her team are responsible for ensuring that the security policies, procedures, baselines, standards, and guidelines are written to address the information security needs of the organization. However, this does not mean that the security department must write all the policies by themselves. Nor should the policies be written solely by the security department without the input and participation of the other departments within the organization, such as legal, human resources, information technology, compliance, physical security, the business units, and others that have to implement the policies. Approval of policy must be done at the executive level. Typically standards, procedures, and baselines do not require that level of approval.

The security officer must stay abreast of emerging technologies to ensure that the appropriate solutions are in place for the company based upon its risk profile, corporate culture, resources available, and desire to be an innovator. Security solutions will be prioritized differently when an organization is a leader, or follower (mature product implementation) with regards to technology and security solutions. Failure to stay abreast of technology enhancements could increase the costs to the organization by maintaining older, less effective products. Approaches to satisfying accepted practices may range from active involvement in security industry associations to interaction with vendors to subscribing to industry research groups to simply reviewing printed material and Internet news.

Compliance is the process of ensuring adherence to security policies. A policy or standard for hardening of the company's firewalls is not very useful if the activity is not being performed. Governments are continuously passing new laws, rules, and regulations that establish requirements to protect nonpublic information or improve controls over critical processes with which the enterprise must be in compliance. Although many of the laws are overlapping with regards to security requirements, frequently the new laws will provide a more stringent requirement for a particular aspect of information security. Time frames to be in compliance with the law may not always come at the best time for the organization, nor may they line up with the budget funding cycles. The security officer must stay abreast of emerging regulatory developments to enable response in a timely manner. Planning and documentation are very critical with regards to proof of compliance. Periodic compliance, whether through internal or external inspection, ensures that the procedures, checklists, and baselines are documented and practiced. Compliance reviews are also necessary to ensure that end-users and technical staff are trained and have read the security policies.

Security officers are often responsible for implementing and operating computer incident response teams (CIRTs). CIRTs are groups of individuals with the necessary skills, including management, technical staff, infrastructure, and communications staff, for evaluating the incident, evaluating the damage caused by an incident, and providing the correct response to repair the system and collect evidence for potential prosecution or sanctions. CIRTs are activated depending upon the nature of the incident and the culture of the organization. Security incidents need to be investigated and followed up promptly because this is a key mechanism in minimizing losses from an incident and reducing the chance of a recurrence.

The security officer provides the leadership for the information security awareness program by ensuring that the program is delivered in a meaningful, understandable way to the intended audience. The program should be developed to grab the attention of the participants to convey general awareness of the security issues and what reporting actions are expected when the end-user notices security violations. When awareness is not promoted, the policies will not get communicated and there will be much less assurance that they will be practiced within the company. An effective awareness program will have multiple components and methods of delivery, be ongoing and be delivered throughout the year, not just as a one-time effort.

Security officers must be involved in the management teams and planning meetings of the organization to be fully effective. Project directions and decisions are made during these meetings, as well as the establishment of buy-in and prioritization for the security initiatives. These meetings will include board of director meetings (periodic updates), IT steering committees, manager meetings, and departmental meetings.

Central to the security officer's success within the organization is understanding the vision, mission, objectives/goals, and plans of the organization. This understanding increases the chances of success, allowing security to be introduced at the correct times during the project lifecycle, and better enables the organization to carry out the corporate mission. The security officer needs to understand the competitive pressures facing the organization, the strengths, weaknesses, threats, opportunities, and the regulatory environment within which the organization operates. All of this will increase the likelihood that appropriate security controls are applied to the areas with the greatest need and highest risk, thus resulting in an optimal allocation of the scarce security funding. The business strategies of each department are critical to their success. Integrating security into that strategy will determine the security officer's success.

Communicate Risks to Executive Management

The information security officer is responsible for understanding the business objectives of the organization, ensuring that a risk assessment is performed, taking into consideration the threats and vulnerabilities impacting the particular organization, and subsequently communicating the risks to executive management. The makeup of the executive management team will vary based on the type of industry or government entity, but typically it includes individuals with C-level titles, such as the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), and Chief Information Officer (CIO). The executive team also includes the first-level reporting to the CEO, such as the VP of sales and marketing, VP of administration, general counsel, and the VP of human resources.

The executive team is interested in maintaining the appropriate balance between acceptable risk and ensuring that business operations are meeting the mission of the organization. In this context, executive management is not concerned with the technical details of the implementations but rather with what is the cost/benefit of the solution and what residual risk will remain after the safeguards are implemented. For example, the configuration parameters of installing a particular vendor's router are not as important as the answers to the following questions:

- What is the real perceived threat (problem to be solved)?
- What is the risk (impact and probability) to business operations?
- What is the cost of the safeguard?
- What will be the residual risk (risk remaining after the safeguard is properly implemented and sustained)?
- How long will the project take?
- Each of these must be evaluated along with the other items competing for resources (time, money, people, and systems).

The security officer has a responsibility to ensure that the information presented to executive management is based upon a real business need and the facts are represented clearly. Recommendations for specific controls should be risk based. Ultimately, it is the executive management of the organization that is responsible for information security. Presentations should be geared at a high level to convey the purpose of the technical safeguard and not be a rigorous detailed presentation of the underlying technology unless requested.

Reporting Model

The security officer and the information security organization should report as high in the organization as possible to:

1. Maintain visibility of the importance of information security.
2. Limit the distortion or inaccurate translation of messages that can occur due to hierarchical, deep organizations.

The higher up in the organization, the greater the ability to gain other senior management's attention to security and the greater the capability to compete for the appropriate budget and resources. Where the security officer's reports in the organization have been the subject of debate for several years and depend upon the culture of the organization, there is no one best model that fits all organizations but rather pros and cons associated with each placement choice. Whatever the chosen reporting model, there should be an individual chosen with the responsibility for ensuring information security at the enterprise-wide level to establish accountability for resolving security issues. The discussion in the next few sections should provide the perspective for making the appropriate choice for the target organization.

Business Relationships

Wherever the security officer reports, it is imperative that he or she establishes credible and good working relationships with business executive management, middle management, and the end-users. Information gathered and acted upon by executive management is obtained through their daily interactions with many individuals, not just other executives. Winning their support may be the result of influencing a respected individual within the organization, possibly several management layers below the executive. Similarly, the relationship between the senior executives and the security officer is important if the security strategies are to carry through to implementation. Establishing a track record of delivery and demonstrating the value of the protection to the business will build this relationship. If done properly, the security function becomes viewed as an enabler of the business versus a control point that slows innovation, provides roadblocks to implementation, and represents an overhead cost function. Reporting to an executive structure that understands the need and importance to the business for information security and is willing to work to actively represent security and battle for appropriate funding is critical to success.

Reporting to the CEO

Reporting directly to the CEO greatly reduces the filtering of messages that can occur if a message must pass through several layers, improves overall communication, as well as demonstrates to the organization the importance of information security. Firms that have high security needs, such as credit card companies, technology companies, and companies whose revenue stream depends highly upon Internet website commerce, such as eBay or Amazon, might utilize such a model. The downside to this model is that the CEO may be preoccupied with other business issues and may not have the interest or time to devote to information security issues.

The security professional needs to be aware of the fact that some organizations are required to report on incidents that meet certain conditions. For example, United States civilian government agencies are required to report any breach of personally identifiable information to the U.S. Computer Emergency Readiness Team (US-CERT) within an hour of discovery. Policies and procedures must be defined to determine how an incident is routed when criminal

activity is suspected. Additionally, policies and procedures need to be in place to determine how an incident is escalated and should address:

- Does the media or an organization's external affairs group need to be involved?
- Does the organization's legal team need to be involved in the review?
- At what point does notification of the incident rise to the line management, middle management, senior management, the board of directors, or the stakeholders?
- What confidentiality requirements are necessary to protect the incident information?
- What methods are used for the reporting? If email is attacked, how does that impact the reporting and notification process?

Reporting to the Information Technology (IT) Department

In this model, the information security officer reports directly to the Chief Information Officer (CIO), director of information technology, the vice president of information technology, or whatever is the title for the head of the IT department. Most organizations have utilized this relationship because this was historically where the data security function was found in many companies. This was often due to security being viewed as only a technical problem. The advantage to this model is that the individual to which the security officer is reporting has an understanding of the technical issues often impacted by information security and typically has the clout with senior management to make the desired changes. It can also be beneficial because the information security officer and his department must spend a good deal of time interacting with other areas in the information systems department. This can build strength, trust, and appropriate awareness of project activities and issues.

The downside of the reporting structure is the conflict of interest. When the CIO must make decisions with respect to time to market, resource allocations, cost minimization, application usability, and project priorities, the ability exists to slight the information security function. The typical CIO's goals are more oriented toward delivery of application products to support the business in a timely manner. Often the perception is that security controls may slow the time to get products completed and money to implement. As a result, the security considerations may not be provided equal weight. It may also be useful to have a dotted line to another area of the organization, such as legal counsel too, so that conflicts of interest can be adjudicated.

Reporting to a lower level within the CIO organization should be avoided, as noted earlier; the more levels between the CEO and the information security officer, the more challenges arise that must be overcome. Levels further down in the organization may also have their own domains of expertise that they are focusing on, such as computer operations, applications programming, or computing or networking infrastructure.

Reporting to Corporate Security

Corporate security in most organizations is focused on the physical security of the enterprise. Often the individuals in this environment have backgrounds as former police officers, military, or were associated in some other manner with the criminal justice system. This alternative may appear logical; however, the individuals from these organizations historically come from different backgrounds. Physical security is focused on criminal justice, protection, safety, and investigation services, while information security professionals usually have different training

in business and information technology. These disciplines intersect in some areas, but they are vastly different in others. A potential downside of being associated with the physical security group is that it could result in the perception of a police-type mentality. This could make it difficult to build effective business relationships with users. Establishing positive relationships with end-users can increase their willingness to listen and comply with policy and any implemented security controls. It can also increase user acceptance and support for the security department in reporting policy violations.

Reporting to the Administrative Services Department

The information security officer may report to the vice president of administrative services, which in some organizations may also include the physical security, employee safety, and HR departments. As it was described in the benefits of reporting to the CIO, there is only one level between the CEO and the information security department. This model can also be viewed as an enterprise function due to the association with the human resources department. It is an attractive model because it can provide focus on security for all forms of information (paper, oral, and electronic). Compared to the functions residing in the technology department, where the focus may tend to be more on just electronic information, there can be benefits. A downside can be that the leaders of this area would have a limited knowledge of information technology, and this could make it more difficult to understand both the business strategies and security requirements and to communicate technical solutions to senior executives and the CEO.

Reporting to the Insurance and Risk Management Department

Information-intensive organizations such as banks, stock brokerages, and research companies may benefit from this model. The Chief Risk Officer (CRO) is already concerned with the risks to the organization and the methods to control those risks through mitigation, acceptance, insurance, etc. The downside is that the risk officer may not be conversant in information systems technology, and the strategic focus of this function may give less attention to day-to-day operational security projects.

Reporting to the Internal Audit Department

This reporting relationship could be seen as a conflict of interest because the internal audit department is responsible for evaluating the effectiveness and implementation of the organization's control structure, including the activities of the information security department. It would be difficult for the internal audit to provide an independent viewpoint. The internal audit department may have adversarial relationships with other portions of the company due to the nature of its role (to uncover deficiencies in departmental processes), and through association, the security department may be perceived in a similar light. It is advisable that the security department establishes close working relationships with the internal audit department to facilitate the control environment. The internal audit manager most likely has a background in financial, operational, and general controls and may have difficulty relating to the technical activities of the information security department. On the positive side, both areas are focused on improving the controls of the company. The internal audit department does have a preferable reporting relationship for audit issues through a dotted-line relationship with the company's audit committee on the board of directors. It is advisable for the information security function to have a similar path to report security issues to the board of directors as well, either in conjunction with the internal audit department or on its own.

Reporting to the Legal Department

Attorneys are concerned with compliance with regulations, laws, and ethical standards, performing due diligence, and establishing policies and procedures that are consistent with many of the information security objectives. The company's general counsel also typically has the respect or ear of the CEO. In regulated industries, this may be a very good fit.

An advantage is that the distance between the CEO and the information security officer is one level. On the downside, due to the emphasis on compliance activities, the information security department may end up performing more compliance-checking activities (versus security consulting and support), which are typically the domain of internal audit.

Determining the Best Fit

As indicated earlier, each organization must view the pros and cons of each type of potential reporting relationship and develop the appropriate relationship based upon the company culture, type of industry, and what will provide the greatest benefit to the company. Optimal reporting relationships will minimize conflicts of interest, increase visibility, ensure funding is appropriately allocated, and ensure that communication is effective when the placement of the information security department is determined.

Budget

The information security officer prepares a budget to manage the information security program and ensures that security is included in the various other departmental budgets, such as the help/service desk, applications development, and the computing infrastructure. Security is much less expensive and easier to justify when it is built into the application design versus added as an afterthought at or after implementation. Estimates range widely over the costs of adding security later in the lifecycle; however, it is not just the added cost caused by not considering security through the development or acquisition lifecycle. It can be perceived as delaying implementation when the time necessary to properly implement security was not factored into the implementation timeline and delays occur. The security officer must work with the application development managers to ensure that security is considered in the project cost during each phase of development (analysis, design, development, testing, implementation, and post-implementation). For systems security certification, there should be at minimum walk-throughs held to ensure that the deliverables meet security requirements. To facilitate this best from an independence perspective, the security officer should not report to information system or application development management.

In addition to ensuring that new project development activities appropriately address security, one must also see that ongoing functions such as access administration, intrusion detection, incident handling, policy development, standards compliance, support of external auditors, and evaluations of emerging technology are appropriately funded. The security officer will rarely receive all the funding necessary to complete all of the projects for which he or she and his or her team have envisioned and must usually plan these activities over multiple years. The budgeting process requires examination of the current risks and ensuring that activities with the largest cost/benefit to the organization are implemented; this is also known as Risk Management. Projects greater than 12–18 months are generally considered to be long term and strategic in nature and typically require more funding and resources or are more complex

in their implementation. In the event these efforts require a longer time frame, pilot projects to demonstrate near-term results on a smaller scale are preferable. Organizations often lose patience with funding long-term efforts, as the initial management supporters may change, as well as some of the team members implementing the change. The longer the payback period, the higher the Rate of Return (ROR) expected by executive management. This is due primarily to the higher risk level associated with longer-term efforts.

The number of staff, level of security protection required, tasks to be performed, regulations to be met, staff qualification level, training required, and degree of metrics tracking are also parameters that drive funding requirements. For example, if an organization must meet government regulations to increase the number of individuals with security certifications, such as the CISSP or other industry standard security certifications, then the organization may feel an obligation to fund internal training seminars to prepare the individuals. This will need to be factored into the budget. This may also be utilized to attract and retain security professionals to the organization through increased learning opportunities. As another example, the time required in complying with government mandates and laws may necessitate increased staffing to provide the appropriate ongoing tracking and responses to audit issues.

Metrics

Measurements can be collected that provide information on long-term trends and illustrate the day-to-day workload. Measurement of processes provides the ability to improve the process. For example, measuring the number of help/service desk tickets for password resets can be translated into workload hours and may provide justification for the implementation of new technologies for the end-user to self-administer the password reset process. Tracking how viruses spread or the frequency of reporting may indicate a need for further education or improvement of the anti-virus management process. Many decisions need to be made when collecting metrics, such as who will collect the metrics, what statistics will be collected, when they will be collected, and what are the thresholds where variations are out of bounds and should be acted upon. An important first decision is to determine what metrics will be used to prove and whether the metric gathering effort will provide the necessary evidence or value desired.

Resources

When considering the overall resource management of an information security function, the information security professional should consider more than just budget to ensure the success of the information security program. In many organizations, the following resources may play a role in directly supporting the information security function:

- System Administrators
- Database Administrators
- Network Administrators
- Policy Officers
- Compliance Officers
- Legal Council
- Law Enforcement
- Quality Assurance Testers
- Help Desk/Service Desk Technicians

Additionally, the information security program is indirectly supported by several functions including but not limited to:

- Budget Officers
- Procurement Specialists
- Business Analysts
- Administrative Professionals
- Enterprise Architects
- Software Developers

The size, complexity, and mission of an organization greatly influence the resources available to the information security program and the information security officer. Understanding the mission of the organization and building relationships with supporting resources as described above often make the difference between a successful security program and an ineffectual one. The security officer rarely has the tools or the team to solely resolve an organization's most pressing challenges.

Information Security Strategies

Strategic, tactical, and operational plans are interrelated, and each provides a different focus toward enhancing the security of the organization. Planning reduces the likelihood that the organization will be reactionary toward the security needs. With appropriate planning, decisions on projects can be made with respect to whether they support the long- or short-term goals and have the priority that warrants the allocation of more security resources.

Strategic Planning

Strategic plans are aligned with the strategic business and information technology goals. These plans have a longer-term horizon (three to five years or more) to guide the long-term view of the security activities. The process of developing a strategic plan emphasizes thinking of the company environment and the technical environment a few years into the future. High-level goals are stated to provide the vision for projects to achieve the business objectives. These plans should be reviewed minimally on an annual basis or whenever major changes to the business occur, such as a merger, acquisition, establishment of outsourcing relationships, major changes in the business climate, introductions of new competitors, and so forth. Technological changes will be frequent during a five-year period, and so the plan should be adjusted. The high-level plan provides organizational guidance to ensure that lower-level decisions are consistent with executive management's intentions for the future of the company. For example, strategic goals may consist of the following:

- Establishing security policies and procedures
- Effectively deploying servers, workstations, and network devices to reduce downtime
- Ensuring that all users understand the security responsibilities and reward excellent performance
- Establishing a security organization to manage security enterprise-wide
- Ensuring effective risk management so that risks are effectively understood and controlled

Tactical Planning

Tactical plans provide the broad initiatives to support and achieve the goals specified in the strategic plan. These initiatives may include deployments such as establishing an electronic policy development and distribution process, implementing robust change control for the server environment, reducing vulnerabilities residing on the servers using vulnerability management, implementing a "hot site" disaster recovery program, or implementing an identity management solution. These plans are more specific and may consist of multiple projects to complete the effort. Tactical plans are shorter in length, such as 6–18 months to achieve a specific security goal of the company.

Operational and Project Planning

Specific plans with milestones, dates, and accountabilities provide the communication and direction to ensure that the individual projects are completed. For example, establishing a policy development and communication process may involve multiple projects with many tasks:

1. Conduct security risk assessment
2. Develop security policies and approval processes
3. Develop technical infrastructure to deploy policies and track compliance
4. Train end-users on policies
5. Monitor compliance

Depending upon the size and scope of the efforts, these initiatives may be steps or tasks as part of a single plan, or they may be multiple plans managed through several projects. The duration of these efforts is short term to provide discrete functionality at the completion of the effort. Traditional "waterfall" methods of implementing projects spend a large amount of time detailing the specific steps required to implement the complete project. Executives today are more focused on achieving some short-term, or at least interim, results to demonstrate the value of the investment along the way. Such demonstration of value maintains organizational interest and visibility to the effort, increasing the chances of sustaining longer-term funding. The executive management may grow impatient without realizing these early benefits, which is why regular communication targeted at managing expectations is a vital element to successful outcomes.

The Complete and Effective Security Program

Several frameworks and assessment methods are available to assess the completeness and effectiveness of an information security program. Some organizations have established an enterprise-wide security oversight committee, sometimes referred to as a "Security Council" to help guide and support these efforts within the enterprise. This group can serve as a steering committee to provide oversight and direction to the information security program. The vision of the Security Council must be clearly defined and understood by all members of the council.

Oversight Committee Representation

For maximum effectiveness, the oversight committee should consist of representatives from multiple organizational units. This will increase a sense of ownership for the security program enterprise-wide and improve support for the policies in the long term. The HR department is essential to provide knowledge of the existing code of conduct, employment and labor relations, termination and disciplinary action policies, and practices that are in place.

The legal department is needed to ensure that the language of the policies states what is intended and that applicable local, state, and federal laws are appropriately followed. The IT department provides technical input and information on current initiatives and the development of procedures and technical implementations to support the policies. The individual business unit representation is essential to understand how practical the policies may be in carrying out the mission of the business. Compliance department representation provides insight on ethics, contractual obligations, and investigations that may require policy creation. And finally, the security officer, who typically chairs the council, should represent the information security department and members of the security team for specialized technical expertise.

The oversight committee is a management committee and, as such, is populated primarily with management-level employees. It is difficult to obtain the time commitment required to review policies at a detailed level by senior management. Reviewing the policies at this level is a necessary step to achieve buy-in within management. However, it would not be good to use the senior management level in the early stages of development. Line management is very focused on their individual areas and may not have the organizational perspective necessary (beyond their individual departments) to evaluate security policies and project initiatives. Middle management appears to be in the best position to appropriately evaluate what is best for the organization, as well as possessing the ability to influence senior and line management to accept the policies. Where middle management does not exist, it is appropriate to include line management because they are typically filling both of these roles (middle and line functions) when operating in these positions.

Many issues may be addressed in a single Security Council meeting, which necessitates having someone record the minutes of the meeting. The chairperson's role in the meeting is to facilitate the discussion, ensure that all viewpoints are heard, and drive the discussions to decisions where necessary. It is difficult to perform that function at the same time as taking notes. Recording the meeting is also helpful to capture key points that may have been missed in the notes so that accurate minutes can be produced.

The relationship between the security department and the security oversight committee is a dotted-line relationship that may or may not be reflected on the organization chart. The value of the committee is in providing the business direction and increasing the awareness of the security activities that are impacting the organization on a continuous basis. How frequently the committee meets will depend upon the organizational culture (i.e., are monthly or quarterly oversight meetings held on other initiatives?), the number of security initiatives, and the urgency of decisions that need the input of the business units.

Security Council Vision Statement

A clear security vision statement should exist that is in alignment with, and supports, the organizational vision. Typically, these statements draw upon the security concepts of confidentiality, integrity, and availability to support the business objectives. Vision statements are not technical and focus on the advantages to the business. People will be involved in the council from management and technical areas and have limited time to participate, so the vision statement must be something that is viewed as worthwhile to sustain their continued involvement. The vision statement is a high-level set of statements that is brief, to the point, and achievable.

Mission Statement

Mission statements are objectives that support the overall vision. These become the road map to achieving the vision and help the council clearly view the purpose for its involvement. Some individuals may choose nomenclature such as goals, objectives, initiatives, etc. A sample mission statement is shown in *Figure 1.4*.

The Information Security Council provides management direction and a sounding board for the ACME Company's information security efforts to ensure that these efforts are:

- Appropriately prioritized
- Supported by each organizational unit
- Appropriately funded
- Realistic given ACME's information security needs
- Balance security needs to be made between cost, response time, ease of use, flexibility, and time to market

The Information Security Council takes an active role in enhancing our security profile and increasing the protection of our assets through:

- Approval of organization-wide information security initiatives
- Coordination of various workgroups so that security goals can be achieved
- Promoting awareness of security initiatives within their organizations
- Discussion of security ideas, policies, and procedures and their impact on the organization
- Recommendation of policies to the ACME Company IT Steering Committee
- Increased understanding of the threats, vulnerabilities, and safeguards facing our organization
- Active participation in policy, procedure, and standard review

The ACME Company information technology steering committee supports the information security council by:

- Developing the strategic vision for the deployment of information technology
- Establishing priorities, arranging resources in concert with the vision
- Approval of the recommended policies, standards, and guidelines
- Approving major capital expenditures

Figure 1.4 – **Sample Security Council mission statement**

Effective mission statements do not need to be lengthy because the primary concern is to communicate the goals so both technical and nontechnical individuals readily understand them. The primary mission of the Security Council will vary by organization. The vision and mission statements should also be reviewed on an annual basis to ensure that the council is still functioning according to the values expressed in the mission statement, as well as to ensure that new and replacement members are in alignment with the objectives of the council.

Security Program Oversight

By establishing this goal in the beginning, the members of the council begin feeling that they have some input and influence over the direction of the security program. This is important because many security decisions will impact the areas of operation of members of the committee. This also is the beginning of management's commitment, as the deliverables produced through the information security program now become recommended or approved by the Security Council versus the information security department. The main activities engaged in by the Security Council are listed below:

- ***Decide on Project Initiatives –*** Each organization has limited resources (time, money, and people) to allocate across projects to advance the business. The primary objective of information security projects is to reduce the organizational business risk through the implementation of reasonable controls. The council should take an active role in understanding the initiatives and the resulting business impact.
- ***Prioritize Information Security Efforts –*** Once the Security Council understands the proposed project initiatives and the associated positive impact to the business, its members can be involved with the prioritization of the projects. This may be in the form of a formal annual process or through the discussion and expressed support for individual initiatives.
- ***Review and Recommend Security Policies –*** Review of the security policies should include:
  - A line-by-line review of the policies
  - A general review of any standards
  - A cursory review of the procedures that are designed to support the policies
  - Monitor the security implementation plan to ensure it meets policy, standards, and baseline requirements

  Through this activity, three key concepts are implemented that are important to sustaining commitment:

  - Understanding of the policy is enhanced.
  - Practical ability of the organization to support the policy is discussed.
  - A sense of ownership is established to increase support of implementation activities.
- ***Review and Audit the Security Program –*** Auditors provide an essential role for maintaining and improving information security. They provide an independent view of the design, effectiveness, and implementation of controls. The results of audits generate findings that require management response and corrective action plans to resolve the issue and mitigate the risk. Auditors often request information prior to the start of the audit to facilitate the review. Some audits are performed at a high level without substantive testing, while other audits will identify test samples to determine if a control is implemented and followed.

The security department cooperates with the internal and external auditors to ensure that the control environment is adequate and functional.

- ***Champion Organizational Security Efforts –*** Once the council understands and accepts the policies, it serves as the organizational champion behind the policies. Council members may have started by reviewing a draft of the policy created by the information systems security department, but the resulting product was only accomplished through their review, input, and participation in the process. Their involvement creates ownership of the deliverable and a desire to see the security policy or project succeed within the company.
- ***Recommend Areas Requiring Investment –*** Members of the council have the opportunity to provide input from the perspective of their individual business units. The council serves as a mechanism for establishing broad support for security investments from this perspective. Resources within any organization are limited and allocated to the business units with the greatest need and the greatest perceived return on investment. Establishing this support enhances the budgetary understanding of the other business managers, as well as the chief financial officer, which is often essential to obtain the appropriate funding.

End-Users

The end-user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated. End-users are like windows in a building. Just like a window that allows all activity to be seen and monitored, their actions will expose weaknesses in a poorly designed and communicated compliance regime. For example, downloading unauthorized software, opening attachments from unknown senders, or visiting malicious websites could introduce malicious code (e.g., virus, Trojans, and spyware) into the environment. However, end-users can also be the front-line eyes and ears of the organization and report security incidents and unusual behavior to the appropriate roles for investigation. In order for the security professionals to create this culture, they must clearly define the expectations and acceptable behaviors associated with this role, as well as ensuring that these are documented and communicated clearly to every member of the enterprise.

Executive Management

Executive management maintains the overall responsibility for protection of the information assets of the enterprise. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know. Financial losses can occur if the confidentiality, integrity, or availability of this information is compromised. Executive Management must be aware of the risks that they are accepting for the organization. Risk must be identified through risk assessment and communicated clearly so that management can make informed decisions.

Information Systems Security Professional

Drafting of security policies, standards and supporting guidelines, procedures, and baselines is coordinated through these individuals. Guidance is provided for technical security issues, and emerging threats are considered with regards to the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed by this role.

Data/Information/Business Owners

A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners, or their delegates, are responsible for understanding the risks that exist with regards to the information that they control.

Data/Information Custodian/Steward

A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end-users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed by systems administrators. This group administers access rights to the information assets on behalf of the information owners.

Information Systems Auditor

IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide senior company management with an independent view of the controls in place and their effectiveness across the enterprise.

Business Continuity Planner

Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery.

Information Systems/Information Technology Professionals

These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application.

Security Administrator

A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Network/Systems Administrator

A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems running on them in order to ensure that the information accessible through these systems will be available when needed. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

Physical Security

The individuals assigned to the physical security role establish relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigation (FBI) to assist in investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of the closed circuit television (CCTV) surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, and legal and business areas to ensure that the practices are integrated.

Administrative Assistants/Secretaries

This role can be very important to information security; in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on the goodwill of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or of providing unauthorized entry.

Help Desk/Service Desk Administrator

As the name implies, the help/service desk is there to field questions from users that report system problems. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program.

The help/service desk is also often where the first indications of security issues and incidents will be seen. A help/service desk individual would contact the computer security incident response team (CSIRT) when a situation meets the criteria developed by the team.[2] The help/service desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.

These functions may alternatively be performed through self-service by the end-user, e.g., an intranet-based solution that establishes the identity of the end-user and resets the password, or by another area, such as the security administration, systems administrator, etc., depending upon the organizational structure and separation of duties principles in place. A help/service desk area is also a prime target for social engineering attacks and, as such, should receive additional attention in security awareness training.

Organizations may have other roles related to information security to meet particular needs. Individuals within the different roles will require different levels of training. The end-user may require basic security awareness training, including the activities that are acceptable, how to recognize that there may be a problem, and what the mechanism is for reporting the problem to the appropriate personnel for resolution. The security administrator will need more in-depth training on the access control packages to manage the logon IDs, accounts, and log file reviews. The systems/network administrator will need technical security training for the specific operating system (e.g., Windows, UNIX, Linux, etc.) or network components (e.g., firewall, routers, switches) to competently set the security controls. Establishing clear, unambiguous security roles has many benefits to the organization beyond providing information as to the responsibilities to be performed and who needs to perform them. These benefits include:

- Demonstrable executive management support for information security
- Increased employee efficiency by reducing confusion about who is expected to perform which tasks
- Team coordination to protect information as it moves from department to department
- Lower risks to company reputation/brand recognition due to security problems
- Capability to manage complex information systems and networks
- Personal accountability for information security
- Reduction of turf battles between departments
- Security objectives balanced with business objectives
- Support of disciplinary actions for security violations up to and including termination
- Facilitation of increased communication for resolution of security incidents
- Demonstrable compliance with applicable laws and regulations
- Shielding of management from liability and negligence claims
- Road map for auditors to determine whether necessary work is performed effectively and efficiently
- Continuous improvement efforts (i.e., ISO 9000)
- Overall risk management
- Provision of a foundation for determining the level of security and awareness training required

2 See the following for an overview of what a CSIRT is and the responsibilities it has within the enterprise: http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?

Information security is a team effort requiring the skill sets and cooperation of many different individuals. Executive management may have overall responsibility, and the security officer/director/manager may be assigned the day-to-day task of ensuring that the organization is complying with the defined security practices. However, every person in the organization has one or more roles to play in order to ensure proper and appropriate protection of the information assets within the organization.

Control Frameworks

To aid in ensuring security and privacy requirements are met, many organizations adopt control frameworks to provide a governance program that is:

1. ***Consistent –*** A governance program must be consistent in how information security and privacy is approached and applied. If two similar situations or requests result in different outcomes, stakeholders will lose faith in the integrity of the program and its usefulness.
2. ***Measurable –*** The governance program must provide a way to determine progress and set goals. Organizations who implement frameworks that can be measured are more likely to improve their security posture over time. Most control frameworks contain an assessment standard or procedure to determine compliance and in some cases risk as well.
3. ***Standardized –*** As with measurable above, a controls framework should rely on standardization so results from one organization or part of an organization can be compared in a meaningful way.
4. ***Comprehensive –*** The selected framework should cover the minimum legal and regulatory requirements of an organization and be extensible to accommodate additional organization-specific requirements.
5. ***Modular –*** A modular framework is more likely to withstand the changes of an organization since only the controls or requirements needing modification are reviewed and updated.

An example of a control framework is the United States National Institute of Standards and Technology's Special Publication 800-53r4.[3] SP 800-53r4 is a control framework made up of 285 controls in 19 families. The framework includes the ability to scope and tailor controls to an organization's specific mission or requirements. The 19 Control Families are listed below in *Table 1.1*:

CONTROL FAMILY
AC - Access Control
AT - Awareness and Training
AU - Audit and Accountability
CA - Security Assessment and Authorization
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection

3 See the following: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

CONTROL FAMILY
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
PS - Personnel Security
RA - Risk Assessment
SA - System and Services Acquisition
SC - System and Communications Protection
SI - System and Information Integrity
PC - Privacy Controls

Table 1.1 – **NIST SP800-53r4 19 Control Families**

NIST SP 800-53r4 is mandatory for United States federal agencies and their contractors. While frameworks such as these may seem daunting, they are designed to be applicable to almost every organization.

Another example is the International Standard Organization (ISO) 27001:2013 Standard.[4] Like NIST SP 800-53r4, ISO 27001:2013 is designed to cover organizations of all sizes and types. The annex A of ISO 27001:2013 contains the control framework with objectives and specifics about each control. ISO is a global framework adopted by numerous industries in most countries. Frameworks often map to each other as well. For example, NIST SP 800-53r4 has been mapped to the ISO 27001:2013 standard. While there is considerable overlap, there are some areas that are not an exact fit. *Figure 1.5* demonstrates a sample control framework comparison.

The security professional must exercise care and judgment when implementing a controls framework to ensure the proper fit for an organization.

Category	Subcategory	CRR Reference	RMM Reference	Informative References
Asset Management (AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	AM:G2.Q1 (Technology)	ADM:SG1.SP1	• CCS CSC 1 • COBIT 5 BAI03.04, BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	AM:G2.Q1 (Technology)	ADM:SG1.SP1	• CCS CSC 2 • COBIT 5 BAI03.04, BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
	ID.AM-3: Organizational communication and data flows are mapped	AM:G2.Q2	ADM:SG1.SP2	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9
	ID.AM-4: External information systems are catalogued	AM:G2.Q1 (Technology)	ADM:SG1.SP1	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 500-291 3, 4 • NIST SP 800-53 Rev. 4 AC-20, SA-9

4 See the following: http://www.standards-online.net/27001en1/iso27001-2013.pdf

Category	Subcategory	CRR Reference	RMM Reference	Informative References
Asset Management (AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	AM:G1.Q4	ADM:SG2.SP1	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-34 Rev. 1 IDENTIFY (ID) • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	AM:MIL2.Q3	ADM:GG2.GP7	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PM-11

Figure 1.5 – **NIST SP 800-53r4 and ISO 27001:2013 sample control comparison (Cyber Resilience Review (CRR): NIST Security Framework Crosswalk. February 2014. U.S. Department of Homeland Security)**[5]

Due Care

Due care is an important topic for the information security professional to understand. It is primarily a legal term used to describe the care a "reasonable person" would exercise under given circumstances. In other words, it is used to also describe what an individual's or organization's legal duty is considered to be. The lack of due care is often considered negligence, and in most countries it is actionable under law. If an organization is legally mandated to comply with regulations or information security requirements, knowingly or unknowingly neglecting those requirements could lead to legal exposure from a due care perspective.

Due Diligence

Due diligence is similar to due care with the exception that it is a preemptive measure made to avoid harm to other persons or their property. If performed correctly, due diligence leads to due care when needed and avoids other situations where due care may need to be exercised. Due diligence is a practice that should be adopted by the information security professionals as a core tenant of their career. Examples of due diligence in an organization include but are not limited to:

- Background checks of employees
- Credit checks of business partners
- Information system security assessments
- Risk assessments of physical security systems
- Penetration tests of firewalls
- Contingency testing of backup systems
- Threat intelligence services being used to check on the availability of company Intellectual Property (IP) posted to public forums and in the cloud

In each of the above examples, the organization is attempting to avoid a situation that may lead to harm to the organization or other individuals. While at times due diligence can be

5 http://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf

expensive, the cost of a single data breach or lawsuit may be large enough to shut down an organization and destroy a career.[6]

According to NIST, the concept of Information Security Due Diligence can and should be framed with regards to managing the risk to organizational missions and business functions. "The security controls in NIST Special Publication 800-53r4 are designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Compliance is not about adhering to static checklists or generating unnecessary FISMA reporting paperwork. Rather, compliance necessitates organizations executing due diligence with regard to information security and risk management. Information security due diligence includes using all appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations. Using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, and technologies will help ensure that all federal information systems and organizations have the necessary resilience to support ongoing federal responsibilities, critical infrastructure applications, and continuity of government." [7]

Compliance

The past 30 years have brought significant changes in the way organizations are structured and run. Entirely new business models have emerged, and old ones have been radically transformed. Productivity has soared, fueled by an endless stream of innovations in information and communications technology (ICT). Centuries-old paradigms for data collection, storage, and use have shifted. Until the early 1990s, it was fairly common for individual departments and divisions to collect, store, and use their own data in their own file cabinets or in departmental computers; as a result, information could not easily be shared with other groups. Rapid advances in the ability of different technologies to interoperate have made it easier for entities of all sizes to exchange information in an almost seamless fashion. Such information exchanges are integral to business efficiency, competitiveness, collaboration, and agility in the 21st century.

The massive and rapid flow of information over the Internet has played a key role in this transformation, by enabling applications that make use of intelligent data analysis, expanded sales and service channels, and other tools. These applications, along with diminishing storage costs, have made it easy for organizations and individuals to accumulate unprecedented amounts of data. This situation has raised awareness of the need to protect confidential data kept by organizations – including intellectual property, trade secrets and market data, and the personal data of customers, employees, and partners – against misuse and unauthorized

6 See the following, Burglary Triggers Medical Records Firm's Collapse: http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm%E2%80%99s-collapse/

7 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Page 11).

disclosure or modification. In some cases, concerns have led to the enactment of laws and regulations that vary by industry or geography and the creation of specific industry standards.

Motivated by security threats and by the need to protect consumers' personal information from abuse, legislative bodies and government institutions have moved to regulate processing and transfer of personal information. Standards bodies and industry associations have followed suit by promoting or requiring the adoption of key security and privacy standards. These actions serve two key objectives: to spread awareness and use of best practices and to promote levels of self-regulation that might forestall the enactment of increasingly restrictive laws that could harm industries or commerce in general. Below is a sampling of these laws, regulations, and industry standards:

- In most European nations, the right to privacy is considered a basic human right. European Union member nations are required to enact laws that comply with the Data Protection Directive (DPD) 95/46/EC. The directive's guidelines are considered a baseline for national laws, and local legislative bodies in member nations may include provisions that go beyond it. Implementation of 95/46/EC is not limited to EU members; Iceland, Norway, and Lichtenstein are among the non-EU nations that have enacted privacy laws that comply with the directive.
- Many other nations have also enacted comprehensive privacy legislation. Examples include Australia's Privacy Act, Argentina's Personal Data Protection Law, and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
- In the United States, privacy legislation has taken more of a sector-based approach. Different laws regulate how organizations collect, use, and protect the confidentiality of personally identifiable information (PII) in different sectors. Examples include the Health Insurance Portability and Accountability Act (HIPAA) for health-related PII and the Gramm-Leach-Bliley Act (GLBA) for credit-related PII. Concerns about data breaches that could lead to an increase in identity theft have led most states to enact data breach notification laws. Prompted by the same concerns, states such as Massachusetts and Nevada have also enacted laws that require adoption of encryption technologies to protect the sensitive personal information of state residents in different scenarios.
- The payment card industry (PCI) has taken steps to prevent credit card fraud and protect cardholders against identity theft. The PCI Security Standards Council (PCI SSC) requires all entities that want to hold, process, or transfer cardholder information to comply with the PCI Data Security Standard (PCI DSS). Among other provisions, the standard requires that an organization's compliance be assessed every year by an independent Qualified Security Assessor (QSA).

Organizations are left with the daunting and increasingly expensive task of determining which rules – including geographically based and industry-specific ones – apply to their national or globally dispersed activities. In some instances, they are forced to decide what constitutes a conflict between multiple compliance obligations and to determine how to address it. The issues are complex and depend on the type of data involved, the type of industry, where and how the data is collected, how it is used, and the residence of the individuals whose PII is collected.

Governance, Risk Management, and Compliance (GRC)

The combination of business and technology-related challenges and the requirement to meet regulatory compliance obligations is not unique to the area of information security and privacy. Such combinations are common in areas such as enterprise risk management, finance, operational risk management, and IT in general. An approach commonly known as governance, risk management, and compliance (GRC) has evolved to analyze risks and manage mitigation in alignment with business and compliance objectives.

- Governance ensures that the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated. All of this happens within a clearly defined context that might span a division, the entire organization, or a specific set of cross-discipline functions.
- Risk management is a systematic process for identifying, analyzing, evaluating, remedying, and monitoring risk. As a result of this process, an organization or group might decide to mitigate a risk, transfer it to another party, or assume the risk along with its potential consequences.
- Compliance generally refers to actions that ensure behavior complies with established rules as well as the provision of tools to verify that compliance. It encompasses compliance with laws as well the enterprise's own policies, which in turn can be based on best practices. Compliance requirements are not static, and compliance efforts should not be either.

GRC goes beyond merely implementing these three elements separately and finds ways to integrate them to increase effectiveness and efficiency and decrease complexity. GRC ensures than an organization acts in accordance with self-imposed rules, acceptable risk levels, and external regulations, as illustrated in *Figure 1.6*. Each circle in the figure represents one component of the GRC approach; each rectangle includes the description of that component's main objective. Each arrow shows the information exchanges among the three elements.

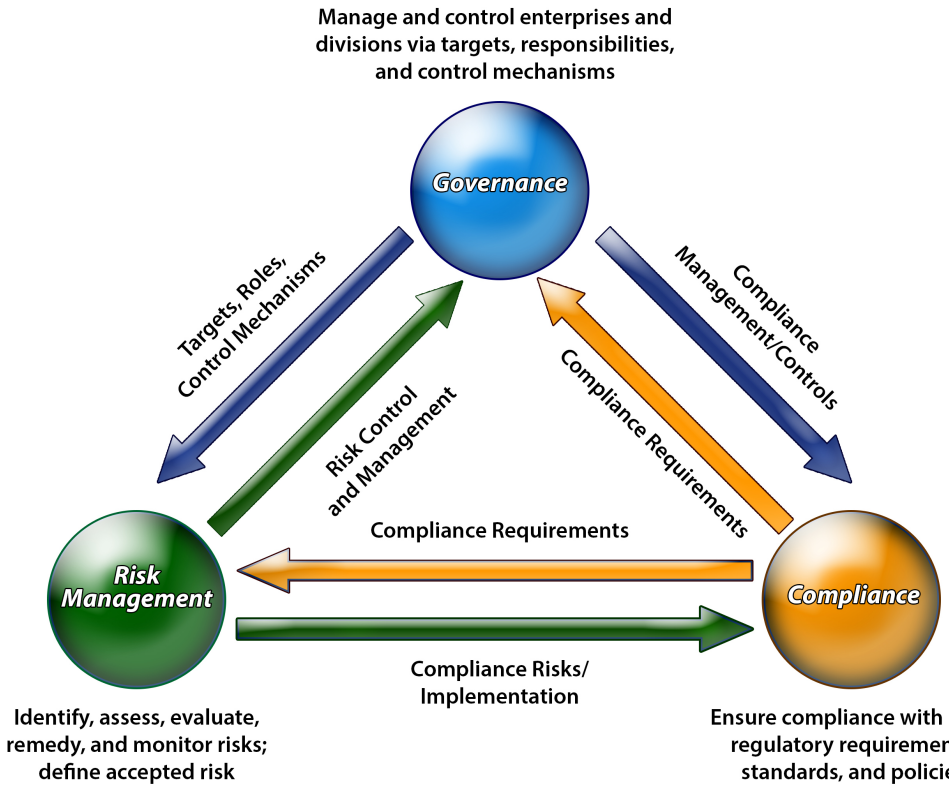


Figure 1.6 – **GRC overview** [8]

Organizations typically find it easier to focus on compliance first and then gradually expand efforts to include risk management and governance. It is important to note, however, that governance activities will happen, whether planned or not, and that lack of planned governance and rigorous risk management can have serious consequences for the business because of the issues associated with uncoordinated actions being carried out on behalf of the organization. With the lack of a clear strategic focus and senior level management guidance to coordinate and control these actions, an organization must assume large risk when aligning them to the business objectives with regards to due diligence and due care.

Legislative and Regulatory Compliance

Organizations operate in environments where laws, regulations, and compliance requirements must be met. Security professionals must understand the laws and regulations of the country and industry they are working in. An organization's governance and risk management processes must take into account these requirements from an implementation and a risk perspective. These laws and regulations often offer specific actions that must be met for compliance, or in some cases, what must be met for a "safe harbor" provision. A safe harbor provision is typically a set of "good faith" conditions that, if met, may temporarily or indefinitely protect the organization from the penalties of a new law or regulation.

8 http://www.giza-blog.de/content/binary/IT-Infrastructure_Compliance_Maturity_Model_Microsoft_Kranawetter_EN.pdf (Page 24)

For example, in the United States, federal executive agencies are required to adhere to the Federal Information Security Management Act (FISMA).[9] FISMA mandates the use of specific actions, standards, and requirements for agencies to ensure sensitive information and vital mission services are not disrupted, distorted, or disclosed to improper individuals. Agencies often take the requirements from FISMA and use them as the baseline for their information security policy and adopt the standards required by FISMA as their own. In doing so, they not only meet the requirements of the law but can also provide proof to external parties that they are making a good faith effort to comply with the requirements of the law.

Compliance stemming from legal or regulatory requirements is best addressed by ensuring an organization's policies, procedures, standards, and guidance are consistent with any laws or regulations that may govern it. Furthermore, it is advisable that specific laws and their requirements are sited in an organization's governance program and information security training programs. As a general rule, laws and regulations represent a "moral minimum," which must be adhered to and should never be considered wholly adequate for an organization without a thorough review. Additional requirements and specificity can be added to complement the requirements of law and regulation, but they should never conflict with them. For example, a law may require sensitive financial information to be encrypted, and an organization's policy could state that in accordance with the law all financial information will be encrypted. Furthermore, the agency may specify a standard strength and brand of encryption software to be used in order to achieve the required level of compliance with the law while also providing for the additional layers of protection that the organization wants in place.

Privacy Requirements Compliance

Privacy laws and regulations pose "confidentiality" challenges for the security professional. Personally identifiable information is becoming an extremely valuable commodity for marketers, as demonstrated by the tremendous growth of social networking sites based on demography and the targeted marketing activities that come with them. While valuable, this information can also become a liability for an organization that runs afoul of information privacy regulations and laws.

For example, the European Data Protection Directive only allows for the processing of personal data under specific circumstances such as:

1. When processing is necessary for compliance with a legal action.
2. When processing is required to protect the life of the subject.
3. When the subject of the personal data has provided consent.
4. When the processing is performed within the law and scope of "public interest."

The four requirements listed above reflect only a small portion of the directive. The directive further states what rights the subject has, such as objecting at any time to the processing of his or her personal data if the use is for direct marketing purposes. Recently, several Internet search companies and social media companies have been cited for not complying with this law. These organizations have been accused of using the personal data of the subject for direct marketing efforts without the subject's permission. The information security professional working in a marketing firm in the European Union must understand the impact of these requirements on how information will be processed, stored, and transmitted in his or her organization.

9 See the following: http://csrc.nist.gov/groups/SMA/fisma/ http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

The "Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (Data Protection Directive 95/46/EC) was established to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted, or processed.[10] The Directive contains 33 articles in 8 chapters. The Directive went into effect in October 1998. This general Data Protection Directive has been complemented by other legal instruments, such as the e-Privacy Directive (Directive 2002/58/EC) for the communications sector.[11] There are also specific rules for the protection of personal data in police and judicial cooperation in criminal matters (Framework Decision 2008/977/JHA).[12]

The Data Protection Directive 95/46/EC defines the basics elements of data protection that member states must transpose into national law. Each state manages the regulation of data protection and its enforcement within its jurisdiction, and data protection commissioners from the EU states participate in a working group at the community level, pursuant to Article 29 of the Directive.

Personal data is defined in the Data Protection Directive 95/46/EC as any information that relates to an "identified or identifiable natural person." The Directive mandates that the data controller ensures compliance with the principles relating to data quality and provides a list of legitimate reasons for data processing. The data controller has information duties toward the data subject whenever personal data is collected directly from the person concerned or obtained otherwise. The data controller is also mandated to implement appropriate technical and organizational measures against unlawful destruction, accidental loss or unauthorized alteration, disclosure, or access.

Data subjects' individual rights, as established by the Directive, are: the right to know who the data controller is, the recipient of the data, and the purpose of the processing; the right to have inaccurate data rectified; a right of recourse in the event of unlawful processing; and the right to withhold permission to use data in some circumstances. For example, individuals have the right to opt-out free of charge from receiving direct marketing material. The EU Data Protection Directive contains strengthened protections concerning the use of sensitive personal data relating, for example, to health, sex life, or religious or philosophical beliefs as well.

Enforcement of the regulatory framework on the processing of personal data can either be through administrative proceedings of the supervisory authority or judicial remedies. Member states' supervisory authorities are endowed with investigative powers and effective powers of intervention, such as powers to order blocking, erasure, and destruction of data or to impose a temporary or definite ban on processing. Any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the liable controller. The Data Protection Directive provides a mechanism by which transfers of personal data outside the territory of the EU have to meet a level of processing "adequate" to the one prescribed by the directive's provisions.

10 See the following for the full text of Directive 95/46/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

11 See the following for the full text of Directive 2002/58/EC: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

12 See the following for the full text of Directive 2008/977/JHA: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1405188191230&uri=CELEX:32008F0977

In January 2012, after the Lisbon Treaty gave the EU the explicit competence to legislate on the protection of individuals with regard to the processing of their personal data, the Commission proposed a reform package comprising a general data protection regulation to replace Directive 95/46/EC and a directive to replace Framework Decision 2008/977/JHA.

The Parliament's committee on Civil Liberties, Justice and Home Affairs adopted its reports on the basis of 4,000 amendments (to the Regulation) and 768 amendments (to the Directive). The Parliament adopted a position at first reading in March 2014. The key points of the Parliament's position in regards to the Regulation are:[13]

- A comprehensive approach to data protection, with a clear, single set of rules, which applies within and outside the Union;
- A clarification of the concepts used (personal data, informed consent, data protection by design, and default) and a strengthening of individuals' rights (e.g., as regards inter alia the right of access or the right to object to data processing);
- A more precise definition of the rules concerning the processing of personal data relating to some sectors (health, employment, and social security) or for some specific purposes (historical, statistical, scientific research, or archives-related purposes);
- A clarification and a strengthening of the regime of sanctions;
- A better and consistent enforcement of data protection rules (strengthened role of the corporate data protection officers, setting up of a European Data Protection Board, unified framework for all Data Protection Authorities, creation of a one-stop shop mechanism);
- A strengthening of the criteria for assessing the adequacy of protection offered in a third country.

The proposed directive deals with the processing of personal data in the context of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. Parliament's position on the directive contains key elements such as:

- A clear definition of the data protection principles (the exceptions that have to be duly justified);
- The conditions to be complied with as regards the processing (e.g., lawful, fair, transparent and legitimate processing, and explicit purposes) and the transmission of personal data;
- The setting up of an evaluation mechanism and of a data protection impact assessment;
- A clear definition of profiling;
- A strengthening of the regime for transferring personal data to third countries;
- A clarification of the monitoring and enforcement powers of the Data Protection Authorities;
- A new article on genetic data.

The security professionals need to stay up to date on the latest developments such as those being pursued by the Parliament with regards to processing and handling of personal information in order to ensure that the compliance activities that they engage in are directed towards supporting the required laws and regulations that are in force within the geographies that the enterprise operates within and that they are responsible for.

13 See the following for the full text of the adopted 12 March, 2014 by the Parliament, including all of the proposed amendments: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212
http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201286

Global Legal and Regulatory Issues

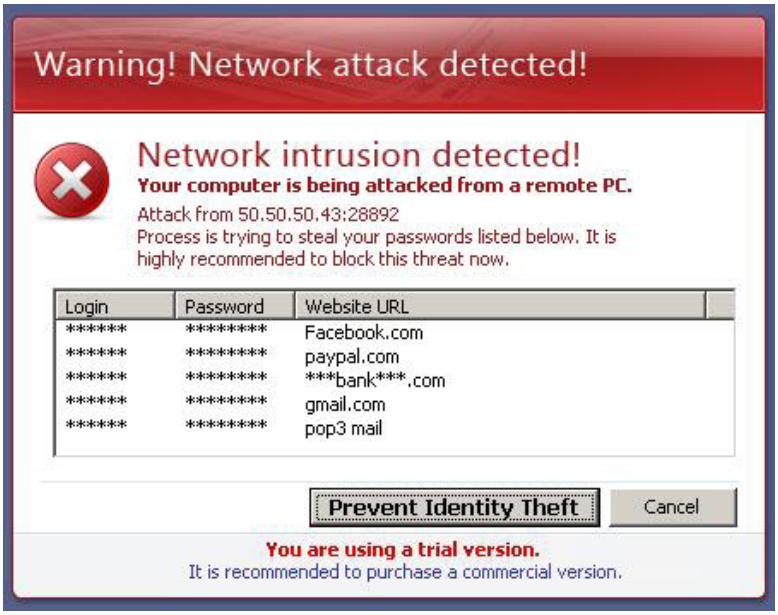
Computer/Cyber Crime

With the proliferation of computer viruses, spyware, phishing and fraud schemes, and hacking activity from every location in the world, computer crime and security are certainly topics of concern when discussing computer ethics. Besides outsiders, or hackers, many computer crimes, such as embezzlement or planting of logic bombs, are committed by trusted personnel who have authorization to use company computer systems. Some examples of these types of crimes include the following:

- ***CryptoLocker Ransomware –*** It spreads via email and propagates rapidly. The virus encrypts various file types and then a pop-up window appears on victims' computers that states their data has been encrypted. The only way to get it back is to send a specified monetary payment to the perpetrator. This ransomware provides the victim with a timeline to pay via a displayed countdown clock. If victims do not pay on time, they lose the ability to pay and risk having their data permanently encrypted and rendered unusable. Perpetrators are demanding a $300 to $700 payment sent to the perpetrator using various methods.
- ***Child Pornography Scareware –*** This scareware is transmitted when computer users visit an infected website. The victim's computer locks up and displays a warning that the user has violated U.S. federal law. Child pornography is either embedded in a banner image that appears on the victims' screen or revealed via an automatic browser redirecting them to a child pornography website. The scareware is used as an extortion technique by threatening prosecution for visiting or viewing these images. The victim is also informed that he or she has been recorded using audio, video, and other devices. The only way to unlock the computer is to pay the fine, which is usually between $300 and $5,000.

- ***Citadel Ransomware –*** The Citadel ransomware, named Reveton, displays a warning on the victims' computer purportedly from a law enforcement agency claiming that their computer had been used for illegal activities, such as downloading copyrighted software or child pornography. To increase the illusion they are being watched by law enforcement, the screen also displays the victim's IP address, and some victims even report activity from their webcam. Victims are instructed to pay a fine to the U.S. Department of Justice to unlock their computer. Many were told to pay the fines via prepaid cash services such as Ucash or Paysafecard. In addition to installing the ransomware, the Citadel malware continues to operate on the compromised computer to collect sensitive data that could potentially be used to commit a variety of financial frauds.

- ***Fake or Rogue Anti-Virus Software –*** In this scheme, victims are scared into purchasing anti-virus software that would allegedly remove viruses from their computers. A pop-up box appears that informs users that their computers are full of viruses and need to be cleaned. The pop-up message has a button victims can click to purchase anti-virus software that supposedly can immediately get rid of these viruses. If the victims click the pop-up to purchase the anti-virus software, they are infected with malware. In some instances, victims have been infected regardless of clicking on the pop-up box.



Cybercrime activities are globally diffused, financially-driven acts. Such computer-related fraud is prevalent, and it makes up around one-third of acts around the world. Another conspicuous portion of cybercrime acts is represented by computer content, including child pornography and piracy. Another significant portion of crime relates to acts against confidentiality, integrity, and accessibility of computer systems. That includes illegal access to a computer system, which accounts for another one-third of all acts.

When assessing the effect of cybercrime, the security professional will find it necessary to evaluate a series of factors such as:

- The loss of intellectual property and sensitive data.
- Opportunity costs, including service and employment disruptions.
- Damage to the brand image and company reputation.
- Penalties and compensatory payments to customers (for inconvenience or consequential loss) or contractual compensation (for delays, etc.).
- Cost of countermeasures and insurance.
- Cost of mitigation strategies and recovery from cyber-attacks.

Ponemon Institute's 2013 Cost of Cyber Crime study finds the average company in the U.S. experiences more than 100 successful cyber-attacks each year at a cost of $11.6M. That's an increase of 26% from 2012. Companies in other regions fared better, but they still experienced significant losses. The 2013 annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, and France and surveyed over 230 organizations.[14]

But the study also shows that companies who implement enabling security technologies reduced losses by nearly $4M, and those employing good security governance practices reduced costs by an average of $1.5M. Key findings include:

- The average annualized cost of cybercrime incurred per organization was $11.56 million, with a range of $1.3 million to $58 million. This is an increase of 26 percent, or $2.6 million, over the average cost reported in 2012.
- Organizations in defense, financial services, and energy and utilities suffered the highest cybercrime costs.
- Data theft caused major costs, 43% of the total external costs; business disruption or lost productivity accounts for 36% of external costs. While the incidence of data theft overall decreased by 2% from 2012 to 2013, business disruption increased by 18% over the same time period.
- Organizations experienced an average of 122 successful attacks per week, up from 102 attacks per week in 2012.
- The average time to resolve a cyber-attack was 32 days, with an average cost incurred during this period of $1,035,769, or $32,469 per day – a 55 percent increase over 2012's estimated average cost of $591,780 for a 24-day period.
- Denial-of-service, Web-based attacks, and insiders account for more than 55% of overall annual cybercrime costs per organization.
- Smaller organizations incur a significantly higher per-capita cost than larger organizations.
- Recovery and detection are the most costly internal activities.

14 See the following to download the global as well as country specific versions of the report: http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports

It should be clear from the summarized findings above that the security professionals have their work cut out for them with regards to the prevention of cybercrime and the impact that it can have on the enterprise. The security professional needs to be able to partner with the security architect and the security practitioner to work across the enterprise at every level in order to ensure that the best possible defenses are envisioned, designed, implemented, managed, monitored, and optimized in order to ensure that the risks and impacts from cybercrime are properly identified, analyzed, and communicated to the organization's senior management. Once senior management has understood and weighed the risks and communicated the risk appetite and position of the enterprise to the security professional, then those risks identified as being the ones that will be accepted should be acted upon as necessary based on the decisions made.

Licensing and Intellectual Property

Although no one expects an information systems security professional to be a legal expert on all areas of technology-related law – as with the various legal systems – a working knowledge of legal concepts directly related to information technology is required to fully understand the context, issues, and risks inherent with operation and management of information systems. Two general categories of information technology law have the largest impact on information systems: intellectual property and privacy regulations. This section only provides a brief summary of these concepts. Readers wishing to delve deeper into this area are strongly encouraged to refer to the relevant legislation and regulations in their respective countries.

Intellectual Property Laws

Intellectual property laws are designed to protect both tangible and intangible items and property. Although there are various rationales behind the state-based creation of protection for this type of property, the general goal of intellectual property law is to protect property from those wishing to copy or use it, without due compensation to the inventor or creator. The notion is that copying or using someone else's ideas entails far less work than what is required for the original development. According to the World Intellectual Property Organization (WIPO):

Intellectual property is divided into two categories: *Industrial property*, which includes inventions (patents), trademarks, industrial designs, and geographical indications of source; and *Copyright*, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs.[15]

Patent

Simply put, a patent grants the owner a legally enforceable right to exclude others from practicing the invention covered for a specific time (usually 20 years). A patent is the "strongest form of intellectual property protection." A patent protects novel, useful, and nonobvious inventions. The granting of a patent requires the formal application to a government entity. Once a patent is granted, it is published in the public domain to stimulate other innovations. Once a patent expires, the protection ends and the invention enters the public domain. WIPO, an agency of the United Nations, looks after the filing and processing of international patent applications.

15 http://www.wipo.int/about-ip/en/iprm/

Trademark

Trademark laws are designed to protect the goodwill an organization invests in its products, services, or image. Trademark law creates exclusive rights to the owner of markings that the public uses to identify various vendor or merchant products or goods. A trademark consists of any word, name, symbol, color, sound, product shape, device, or combination of these that is used to identify goods and distinguish them from those made or sold by others. The trademark must be distinctive and cannot mislead or deceive consumers or violate public order or morality. Trademarks are registered with a government registrar. International harmonization of trademark laws began in 1883 with the Paris Convention, which prompted the Madrid Agreement of 1891. In addition to patents, WIPO oversees international trademark law efforts, including international registration.

Copyright

A copyright covers the expression of ideas rather than the ideas themselves; it usually protects artistic property such as writing, recordings, databases, and computer programs. In most countries, once the work or property is completed or is in a tangible form, the copyright protection is automatically assumed. Copyright protection is weaker than patent protection, but the duration of protection is considerably longer (e.g., a minimum of 50 years after the creator's death or 70 years under U.S. copyright protection). Although individual countries may have slight variations in their domestic copyright laws, as long as the country is a member of the international Berne Convention, the protection afforded will be at least at a minimum level, as dictated by the convention; unfortunately, not all countries are members.[16]

Trade Secret

A trade secret refers to proprietary business or technical information, processes, designs, practices, etc., that are confidential and critical to the business (e.g., Coca-Cola's formula). The trade secret may provide a competitive advantage or, at the very least, allow the company to compete equally in the marketplace. To be categorized as a trade secret, it must not be generally known and must provide some economic benefit to the company. Additionally, there must be some form of reasonable steps taken to protect its secrecy. A trade secret dispute is unique because the actual contents of the trade secret need not be disclosed. Legal protection for trade secrets depends upon the jurisdiction. In some countries, it is assumed under unfair business legislation, and in others, specific laws have been drafted related to confidential information. In some jurisdictions, legal protection for trade secrets is practically perpetual and does not carry an expiry date, as is the case with patents. Trade secrets are often at the heart of industrial and economic espionage cases and are the proverbial crown jewels of some companies.

Licensing Issues

The issue of illegal software and piracy is such a large problem that it warrants discussion. More than one company has been embarrassed publicly, sued civilly, or criminally prosecuted for failing to control the use of illegal software or violating software licensing agreements. With high-speed Internet access readily available to most employees, the ability – if not the temptation – to download and use pirated software has greatly increased. According to a recent (2013) study by the Business Software Alliance (BSA) and International Data Corporation

16 Read more about the Berne convention here: http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html

(IDC), prevalence and frequency of illegal software is exceedingly high: The weighted average was 42% worldwide. The same study found that for every two dollars' worth of legal software purchased, one dollar's worth of software was pirated.[17] Though not all countries recognize the forms of intellectual property protection previously discussed, the work of several international organizations and industrialized countries seems somewhat successful in curbing the official sanctioning of intellectual property rights violations (e.g., software piracy).

There are several categories of software licensing including freeware, shareware, commercial, and academic. Within these categories, there are specific types of agreements. Master agreements and end-user licensing agreements (EULAs) are the most prevalent, though most jurisdictions have refused to enforce the shrink-wrap agreements that were commonplace at one time. Master agreements set out the general overall conditions of use along with any restrictions, whereas the EULA specifies more granular conditions and restrictions. The EULA is often a "click through" or radio button that the end-user must click on to begin the install, indicating that he or she understands the conditions and limitations and agrees to comply.

Various third parties have developed license metering software to ensure and enforce compliance with software licensing agreements. Some of these applications can produce an audit report and either disable software attempting to run in violation of an agreement (e.g., exceeding the number of devices running software concurrently) or produce an automated alert. The use of carefully controlled software libraries is also a recommended solution. Ignorance is no excuse when it comes to compliance with licensing conditions and restrictions. The onus is clearly on the organization to enforce compliance and police the use of software or face the possibility of legal sanctions, such as criminal prosecution or civil penalties.

Import/Export

Concerns about the inappropriate transfer of new information, technologies, and products with military applications outside the U.S. led to the passage of two laws in the late 1970s that control exports of selected technologies and products.

1. ***International Traffic In Arms Regulations (ITAR)*** – The Arms Export Control Act (Sec. 38) of 1976, as amended (P.L. 90-629), authorizes (22 U.S.C., Chapter 39, Subchapter III, Sec. 2778 entitled Control of Arms Exports and Imports) the President to:
   - A. Designate those items which shall be considered as defense articles and defense services
   - B. Control their import and the export.

The items so designated shall constitute the United States Munitions List (22 CFR Part 121) and are regulated through the U.S. Department of State, Office of Defense Trade Controls.

Defense articles (Sec. 120.6 & Part 121) include any item or technical data (recorded or stored in any physical form, models, mockups, or other items that reveal technical data) designated in the U.S. Munitions List. Of the 21 declared item categories controlled under ITAR, the following 19 are of potential interest to the information security professional, in particular those that may work in the aerospace and defense industries, due to the potential lateral applications of computer related technologies and information service technologies inherent in each of these categories and the technology represented by each:[18]

17 See the following for the 2013 study: http://globalstudy.bsa.org/2013/index.html

18 See the following for a full listing of the ITAR categories: http://fas.org/spp/starwars/offdocs/itar/p121.htm

I. Firearms
II. Artillery Projectors
III. Ammunition
IV. Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
V. Explosives, Propellants, Incendiary Agents, and Their Constituents
VI. Vessels of War and Special Naval Equipment
VII. Tanks and Military Vehicles
VIII. Aircraft and Associated Equipment
IX. Military Training Equipment
X. Protective Personnel Equipment
XI. Military Electronics
XII. Fire Control, Range Finder, Optical and Guidance and Control Equipment
XIII. Auxiliary Military Equipment
XIV. Toxicological Agents and Equipment and Radiological Equipment
XV. Spacecraft Systems and Associated Equipment
XVI. Nuclear Weapons Design and Test Equipment
XVII. Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
XVIII. Submersible Vessels, Oceanographic and Associated Equipment
XIX. Miscellaneous Articles:

1. Defense articles not specifically enumerated in the other categories that have substantial military applicability and that have been specifically designed or modified for military purposes. The decision on whether any article may be included in this category shall be made by the Director of the Office of Defense Trade Controls.
   - Technical data (Sec. 120.21) and defense services (Sec. 120.8) directly related to the defense articles.
2. ***Export Administration Regulations (EAR) –*** The Export Administration Act of 1979 authorized the President to regulate exports of civilian goods and technologies (equipment, materials, software, and technology, including data and know-how) that have military applications (dual-use items). Such controls have traditionally been temporary, and when it has lapsed, the President has declared a national emergency and maintained export control regulations under the authority of an executive order.

The items so designated constitute the United States Commerce Control List (15 CFR Part 774 2) and are regulated through the U.S. Department of Commerce, Bureau of Industry and Security. Of the 9 declared categories, the following are of interest to the information security professional in particular:[19]

- ***Category 4 –*** Computers
- ***Category 5 Part 1 –*** Telecommunications
- ***Category 5 Part 2 –*** Information Security

19 See the following for a full listing of all of the EAR categories: http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

In addition, Section 734.3 paragraph (b) (3) of EAR exempts publicly available technology and software from controls, except for software controlled for "Encryption Item" reasons under Export Control Classification Number (ECCN) 5D002, Information Security – "Software", on the Commerce Control List and mass market encryption software with symmetric key length exceeding 64-bits controlled under ECCN 5D992, if it:

- Is already published or will be published;
- Arises during, or results from, fundamental research;
- Is educational; or
- Is included in certain patent applications

Therefore, it is essential for broad understanding and agreement of the following basic concepts related to export controls amongst security professionals operating in the United States or representing companies that do business with the United States or United States based companies:

1. The nature of the technology that is export controlled and how it is recognized,
2. What is an "export" (ITAR) or a "deemed export" (EAR),
3. The fundamental research exclusion and the meaning of "Public Domain", and
4. Whether or not there are:
    - Restrictions imposed on publication of scientific and technical information resulting from the project or activity, OR
    - Controls imposed on access and dissemination of information resulting from the research by federal funding agencies.

The security professional should also be aware of the Wassenaar Arrangement. The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations.[20] Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals and are not diverted to support such capabilities. The Participating States of the Wassenaar Arrangement are:

Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and United States.

The decision to transfer or deny transfer of any item is the sole responsibility of each Participating State. All measures with respect to the Arrangement are taken in accordance with national legislation and policies and are implemented on the basis of national discretion. With regards to the United States, the EAR listing discussed above reflects the same categories as those controlled under the Wassenaar Arrangement.

20 See the following for the complete listing of the Wassenaar Arrangement controls: http://www.wassenaar.org/controllists/index.html

Trans-Border Data Flow

The movement of information across national borders drives today's global economy. Cross-border data transfers allow businesses and consumers access to the best available technology and services, wherever those resources may be located around the world. The free-flow of data across borders benefits all industry sectors, from manufacturing to financial services, education, healthcare, and beyond. The seamless transfer of information is as critically important as it is inexorably linked to the growth and success of the global economy.

As information moves from one server to another or from one cloud to another, the location of the data and the hosting organization begins to matter. Information developed in one country, transmitted through another and finally stored in a third may be subject to three different jurisdictions and three different legal systems along the route of its journey from start to finish. In some situations even if information is stored in one country, if the organization who owns the server is a member of a different country, the latter may be able to gain jurisdiction over the information stored on the system in question.

There are many issues that the security professional will need to consider and be concerned with in this area. A few examples are listed below:

- Governments throughout the world are looking at new ways to identify their citizens and visitors to fight terrorism, to combat fraud, and to deliver services. This has prompted governments to consider identity cards, enhanced passports and other travel documents, and the use of biometrics in health cards, drivers' licenses, and other entitlement documents. These documents will leave data trails that may create risks in countries without adequate data protection.
- Corporations and governments, in a drive to reduce costs and become more efficient, are outsourcing activities, including the processing of personal information of their customers and citizens. The phenomenon is not new; the scale and speed and number of players having access to the data is unprecedented and shows little sign of abating. This has led to legitimate concerns about the security and misuse of information being transferred to countries without data protection legislation.
- Technologies and applications as diverse as search engines, radio frequency identification chips (RFIDs), Voice Over Internet Protocol (VOIP), Web logging, and wireless communications generate huge amounts of personal transactional information and create data trails that can survive long after the transaction or conversation has taken place. Requirements for data retention could ensure that much of this data will persist for years, split among various jurisdictions across the world.
- The fight against terrorism and the related concerns about public safety have prompted governments to put individuals under unprecedented scrutiny. Governments are demanding significant amounts of personal information about people entering their countries, developing assessment tools to detect suspicious patterns of travel and behavior, creating watch lists, and sharing this information with other countries. This raises significant concerns about the ability of individuals to exercise their information rights in the countries they visit.

Trans-border data flows are increasing exponentially, whether for processing purposes, to facilitate e-commerce, for law enforcement and national security purposes, or simply the result of people going about their daily lives. These trends are creating new and complex challenges for security professionals and other organizations charged with overseeing privacy and data protection laws.

Privacy

With the proliferation of technology and the increasing awareness that most of our personally identifiable information (PII) is stored online or electronically in some way, shape, or form, there is growing pressure to protect personal information.[21] Almost monthly, there are media reports worldwide of databases being compromised, files being lost, and attacks against businesses and systems that house personal, private information. This has spurred concerns over the proper collection, use, retention, and destruction of information of a personal or confidential nature. This public concern has prompted the creation of regulations intended to foster the responsible use and stewardship of personal information. In the context of this discussion, privacy is one of the primary areas in which business, in almost all industries, is forced to deal with regulations and regulatory compliance.

The actual enactment of regulations or, in some cases, laws dealing with privacy depend on the jurisdiction. Some countries have opted for a generic approach to privacy regulations, horizontal enactment (i.e., across all industries, including government), while others have decided to regulate by industry, vertical enactment (e.g., financial, health, publicly traded).

Regardless of the approach, the overall objective is to protect a citizen's personal information while at the same time balancing the business, governmental, and academic or research need to collect and use this information appropriately. Unfortunately, there is no one international privacy law, resulting in a mosaic of legislation and regulations. Some countries have been progressive in dealing with privacy and personal information, while others have yet to act in this area. Given the fact that the Internet has created a global community, our information and business transactions and operations may cross several different borders and jurisdictions – each with its own sovereign concerns, societal standards, and laws. Therefore, it is prudent to have a basic understanding of privacy principles and guidelines and keep up to date with the changing landscape of privacy regulations that may affect business as well as personal information.

Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information. Personal information is a rather generic concept and encompasses any information that is about or on an identifiable individual. Although international privacy laws are somewhat different in respect to their specific requirements, they all tend to be based on core principles or guidelines. The Organization for Economic Cooperation and Development (OECD) has broadly classified these principles into the collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[22] The guidelines are as follows:

- There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

21 For more information on PII, see the following: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

22 See the following: http://oecdprivacy.org/

- The purposes for which personal data is collected should be specified not later than at the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified above except:
  - With the consent of the data subject.
  - By the authority of law.
- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- There should be a general policy of openness about developments, practices, and policies concerning personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- An individual should have the right:
  - To obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to him.
  - To have communicated to him, data relating to him:
    - Within a reasonable time.
    - At a charge, if any, that is not excessive.
    - In a reasonable manner.
    - In a form that is readily intelligible to him.
  - To be given reasons if a request made is denied and to be able to challenge such denial.
  - To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
  - A data controller should be accountable for complying with measures that give effect to the principles stated above.

It should be noted that the OECD is very cautious about not creating barriers to the legitimate trans-border flow of personal information. The OECD also cautions members to be aware of, and sensitive to, regional or domestic differences and safeguard personal information from countries that do not follow the OECD guidelines or an equivalent.[23]

Generally, these principles should form the minimum set of requirements for the development of reasonable legislation, regulations, and policy, and that nothing prevents organizations from adding additional principles. However, the actual application of these principles has proved more difficult and costly in almost all circumstances; there has been a vast underestimation of the impact of the various privacy laws and policies both domestically and with cross-border commerce. This is not an excuse to abandon, block, or fail to comply with applicable laws, regulations, or policies. However, security professionals need to appreciate that business practices have changed due to the need to be in compliance (often with international regulations) and that budgets must be appropriately increased to meet the demand.

23 For example, the difference within the EU between personal information and 'sensitive' personal information is something for the security professional to be aware of, but perhaps it may not be something that is addressed by an organization or its policies depending on where they do business.

Data Breaches

It is important for the security professionals of the world to have a sense of community and identity. Certifications such as the CISSP help to foster and create this community by allowing security professionals to share a sense of accomplishment at having attained an important milestone in their careers through certification, as well as by gaining access to a community shared amongst information security professionals. The main thing that helps to define a community is the culture that it represents and the shared values and points of reference that the culture is built upon. Common points of reference are important for all sorts of reasons, but especially so because they provide for the ability to agree on definitions and expectations with regards to things such as vocabulary. To that end, the following definitions of vocabulary terms are offered as noted:

- ***Incident –*** A security event that compromises the integrity, confidentiality, or availability of an information asset.
- ***Breach –*** An incident that results in the disclosure or potential exposure of data.
- ***Data Disclosure –*** A breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party.

The incident and breach landscape is an ever-changing one. With the nature of interconnected systems today, an incident that starts out as a small breach, perhaps limited to one system, can quickly spread if unchecked to encompass entire global networks and data systems. The security professional needs to have a general sense of the kinds of breaches and data disclosures that are being faced by organizations around the world today in order to be prepared to react to the threats that they will encounter in the enterprise. The security professional and the security practitioner both also need to keep in mind that if incidents are identified quickly, and responded to in an efficient and effective manner, then those efforts may be able to prevent the incident from becoming a full blow breach.

While it is impossible to create a comprehensive and timely list of incidents, breaches, and data disclosure events, the following list represents the largest items on the list as of the first seven months of 2014, based on publically disclosed information.

eBay

The online retailer suffered one of the biggest data breaches yet reported by an online retailer. Attackers compromised a "small number of employee log-in credentials" between late February and early March to gain access to the company's network and, through it, compromised a database that contained customer names, encrypted passwords, email addresses, physical addresses, phone numbers, and dates of birth. The breach is thought to have affected the majority of the company's 145 million members, and many were asked to change their passwords as a result.

Michaels Stores

The point-of-sale systems at 54 Michaels and Aaron Brothers stores "were attacked by criminals using highly sophisticated malware" between May 2013 and January 2014. The company said up to 2.6 million payment card numbers and expiration dates at Michaels stores and 400,000 at Aaron Brothers could have been obtained in the attack. The company received confirmation of at least some fraudulent use.

Montana Department of Public Health and Human Services

After suspicious activity was noticed, officials conducted an investigation in mid-May that led to the conclusion that a server at the Montana Department of Public Health and Human Services had been hacked. The server held names, addresses, dates of birth, and social security numbers on roughly 1.3 million people, although the department said it has "no reason to believe that any information contained on the server has been used improperly or even accessed."

Variable Annuity Life Insurance Co.

A former financial adviser at the company was found in possession of a thumb drive that contained details on 774,723 of the company's customers. The drive was provided to the company by law enforcement as the result of a search warrant served on the former adviser. The thumb drive included full or partial social security numbers, but the insurance company said it did not believe any of the data had been used to access customer accounts.

Spec's

A 17-month-long "criminal attack" on the Texas wine retailer's network resulted in the loss of information of as many as 550,000 customers. The intrusion began in October 2012 and affected 34 of the company's stores across the state. It continued until as late as March 20 of 2014, and the company fears hackers got away with customer names, debit or credit card details, card expiration dates, card security codes, bank account information from checks, and possibly driver's license numbers.

St. Joseph Health System

A server at the Texas healthcare provider was attacked between December 16 and 18 of 2013. It contained "approximately 405,000 former and current patients', employees' and some employees' beneficiaries' information." This included names, social security numbers, dates of birth, medical information, and, in some cases, addresses and bank account information. As with many other hacks, an investigation was not able to determine if the data was accessed or stolen.

According to the Verizon Data Breach Investigation Report (DBIR) 2014, the following 8 categories are responsible for approximately 94% of all data breach activity tracked and reported globally through the study:[24]

- POS Intrusions – 14%
- Web App Attacks – 35%
- Insider Misuse – 8%
- Physical Theft/Loss - <1%
- Miscellaneous Errors – 2%
- Crimeware – 4%
- Card Skimmers – 9%
- Cyber-espionage – 22%

The Verizon data illustrates very clearly what the categories of threats were that the security professional needed to be concerned with during 2013 and early 2014, while the report's data was being gathered and analyzed. However, as you are reading this paragraph, the threat categories and risks associated with them that the security professional is facing today may be very different than those listed above, although there may be similarities as well.

24 See the following to download the Verizon DBIR 2014: http://www.verizonenterprise.com/DBIR/2014/

So what can the security professional do to create an ongoing awareness of and ability to defend against threats and risks such as those listed above, especially when there are newly emerging threat vectors and bad actors constantly cropping up? Perhaps looking towards the same community identified earlier in this discussion and relying on it to help create a sort of global early warning system for threat vectors that are emerging from the wild would provide valuable insights to the security professional? But how would one do something so audacious and achieve something so important but at the same time so elusive? How indeed.

A Brief Primer on VERIS & VCDB

The Vocabulary for Event Recording and Incident Sharing (VERIS) is designed to provide a common language for describing security incidents in a structured and repeatable manner. It takes the narrative of "who did what to what (or whom) with what result," and it translates it into the kind of data you see in the Verizon DBIR 2014. Get additional information on the VERIS community site; the full schema is available on GitHub.

Both are good companion references for the security professional to help with understanding terminology and context.

- www.veriscommunity.com
- www.github.com/vz-risk/veris

Launched in 2013, the VERIS Community Database (VCDB) project enlists the cooperation of volunteers in the security community in an attempt to record all publicly disclosed security incidents in a free and open dataset. Learn more about VCDB by visiting the website below:

- www.vcdb.org

Some additional resources that the security professional may find to be valuable are listed below:

- http://www.databreachtoday.com/news (Lists information for the U.S., U.K., Europe, India, and Asia)
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (Infographic that constantly updates with information from data breaches occurring globally that represent losses greater than 30,000 records per breach)
- http://www.scmagazine.com/the-data-breach-blog/section/1263/
- http://datalossdb.org/

Relevant Laws and Regulations

Currently in the United States, a company's possession and use of consumer data is regulated by a patchwork of industry-specific federal laws and generally applicable state data protection and notification laws. At the federal level, the Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") are two prominent examples. The GLBA applies to financial institutions and provides for the implementation of standards to limit the purposeful disclosure of and protect against unauthorized access to consumers' "nonpublic personal information." The GLBA also mandates that a financial institution must provide to its consumers notice of its policies on sharing nonpublic personal information. HIPAA, on the other hand, sets national standards for the security of electronically protected health information. Additionally, HIPAA requires covered entities – i.e., healthcare providers, health plans, and healthcare clearinghouses – and business associates to give notice to consumers whose unsecured protected health information has been compromised due to a breach.

In addition to industry-specific federal laws, there are numerous state and territorial personal data protection laws. While these laws serve the same general purpose of protecting individuals from identity theft, some vary as to the obligations they impose. For example, once unencrypted personal information is shown to have been compromised, most state laws require that notice be provided to affected individuals or the company that owns the data, depending on who suffered the breach. Some states also require the company that owns the data to notify consumer reporting agencies in certain circumstances. In the same vein, some states require that notice be given to the state's attorney general or other state agency whenever any state resident must be notified of a data breach, and other states require such notice only if a certain number of state residents must be notified. However, the majority of states do not require any notice to the attorney general or other state agency.

On 25 August 2013, the EU's new breach notification Regulation for electronic communication service (ECS) providers came into force. The Regulation supplements an earlier Directive that instructed ECS companies to notify their competent national authority in accordance with national laws.

The Regulation defines a standard process across the entire Union: European ECS providers are required to provide notice of data breaches (defined in the Directive as the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Union"). It also states, "The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible."[25]

The European Union Agency for Network and Information Security (ENISA) reviewed the existing measures and the procedures in EU Member States with regard to personal data breaches and published in 2011 a study on the technical implementation of the Art. 4 of the ePrivacy Directive (2002/58/EC), which included recommendations on how to plan and prepare for data breaches, how to detect and assess them, how to notify individuals and competent authorities, and how to respond to data breaches. A proposal of a methodology for personal data breach severity assessment was also included as an annex to the above mentioned recommendations, which was, however, not considered mature enough to be used at national level by the different Data Protection Authorities.

Against this background, the Data Protection Authorities of Greece and Germany in collaboration with ENISA developed, based on the above mentioned work, an updated methodology for data breach severity assessment that could be used both by DPAs as well as data controllers. The working paper draft for this project, Working Document, v1.0, December 2013, can be accessed at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity.

On September 26, 2013, the U.K. Information Commissioner's Office (ICO) published new breach notification guidance, applicable to telecom operators, Internet service providers (ISPs), and other public electronic communications service (ECS) providers.[26]

25 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

26 http://ico.org.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/notification-of-pecr-security-breaches.pdf

The U.K. Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) implementation contained wide-ranging rules on marketing and advertising by telephone, fax, email, and text message, as well as rules relating to cookies and security breaches. The breach notification requirements contained in the PECR apply to ECS providers (e.g., telecom providers and ISPs). In the event of a data breach, these entities must notify the ICO within 24 hours of becoming aware of the basic facts of the breach.

The Guidance sets out the breach requirements that must be provided to the ICO. A secure online form for all notifications is now available; previously, service providers were expected to complete a breach notification form and email it to the ICO.[27] The form is high level and anticipates that notifying organizations may be awaiting further details from an internal investigation. Organizations submitting an initial breach notification form are expected to submit a second notification form containing further details of the breach within three days. If a data breach is likely to adversely affect individuals, the organization must notify those individuals "without undue delay" in addition to notifying the ICO. Data breach logs also must be maintained and submitted to the ICO on a monthly basis. The ICO provides a template log to help service providers understand what information needs to be submitted to the ICO.

Based on the sampled diversity of approaches discussed above, the security professionals will need to clearly familiarize themselves with the appropriate laws and regulatory requirements based on the area of the world that they are practicing in. To that end, one of the best resources currently available to help the security professional stay up to date on the differences by geography with regards to data privacy laws is the International Compendium of Data Privacy Laws compiled by BakerHostetler.[28]

Understand Professional Ethics

The consideration of computer ethics fundamentally emerged with the birth of computers. There was concern right away that computers would be used inappropriately to the detriment of society, or that they would replace humans in many jobs, resulting in widespread job loss. To fully grasp the issues involved with computer ethics, it is important to consider the history. The following provides a brief overview of some significant events.

Consideration of computer ethics is recognized to have begun with the work of MIT professor Norbert Wiener during World War II in the early 1940s, when he helped to develop anti-aircraft cannons that were capable of shooting down fast warplanes. This work resulted in Wiener and his colleagues creating a new field of research that Wiener called cybernetics, the science of information feedback systems. The concepts of cybernetics, combined with the developing computer technologies, led Wiener to make some ethical conclusions about the technology called information and communication technology (ICT), in which Wiener predicted social and ethical consequences.

Wiener published the book The Human Use of Human Beings in 1950, which described a comprehensive foundation that is still the basis for computer ethics research and analysis.

27 https://report.ico.org.uk/security-breach/

28 The 2014 version can be found here: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

In the mid-1960s, Donn B. Parker, at the time with SRI International in Menlo Park, CA, began examining unethical and illegal uses of computers and documenting examples of computer crime and other unethical computerized activities. He published "Rules of Ethics in Information Processing" in Communications of the ACM in 1968, and headed the development of the first Code of Professional Conduct for the Association for Computing Machinery, which was adopted by the ACM in 1973.

During the late 1960s, Joseph Weizenbaum, a computer scientist at MIT in Boston, created a computer program that he called ELIZA that he scripted to provide a crude imitation of "a Rogerian psychotherapist engaged in an initial interview with a patient." People had strong reactions to his program, some psychiatrists fearing it showed that computers would perform automated psychotherapy. Weizenbaum wrote Computer Power and Human Reason in 1976, in which he expressed his concerns about the growing tendency to see humans as mere machines. His book, MIT courses, and many speeches inspired many thoughts and projects focused on computer ethics.

Walter Maner is credited with coining the phrase "computer ethics" in the mid-1970s when discussing the ethical problems and issues created by computer technology, and taught a course on the subject at Old Dominion University. From the late 1970s into the mid-1980s, Maner's work created much interest in university-level computer ethics courses. In 1978, Maner published the Starter Kit in Computer Ethics, which contained curriculum materials and advice for developing computer ethics courses. Many university courses were put in place because of Maner's work.

In the 1980s, social and ethical consequences of information technology, such as computer-enabled crime, computer failure disasters, privacy invasion using computer databases, and software ownership lawsuits, were being widely discussed in America and Europe.

James Moor of Dartmouth College published "What Is Computer Ethics?" in Computers and Ethics, and Deborah Johnson of Rensselaer Polytechnic Institute published Computer Ethics, the first textbook in the field in the mid-1980s. Other significant books about computer ethics were published within the psychology and sociology field, such as Sherry Turkle's The Second Self, about the impact of computing on the human psyche, and Judith Perrolle's Computers and Social Change: Information, Property and Power, about a sociological approach to computing and human values.

Maner Terrell Bynum held the first international multidisciplinary conference on computer ethics in 1991. For the first time, philosophers, computer professionals, sociologists, psychologists, lawyers, business leaders, news reporters, and government officials assembled to discuss computer ethics. During the 1990s, new university courses, research centers, conferences, journals, articles, and textbooks appeared, and organizations like Computer Professionals for Social Responsibility, the Electronic Frontier Foundation, and the Association for Computing Machinery-Special Interest Group on Computers and Society (ACM-SIGCAS) launched projects addressing computing and professional responsibility. Developments in Europe and Australia included new computer ethics research centers in England, Poland, Holland, and Italy. In the U.K., Simon Rogerson, of De Montfort University, led the ETHICOMP series of conferences and established the Centre for Computing and Social Responsibility.

Regulatory Requirements for Ethics Programs

When creating an ethics strategy, it is important to look at the regulatory requirements for ethics programs. These provide the basis for a minimal ethical standard upon which an organization can expand to fit its own unique organizational environment and requirements. An increasing number of regulatory requirements related to ethics programs and training now exist.

The 1991 U.S. Federal Sentencing Guidelines for Organizations (FSGO) outline minimal ethical requirements and provide for substantially reduced penalties in criminal cases when federal laws are violated if ethics programs are in place. Reduced penalties provide strong motivation to establish an ethics program. Effective November 1, 2004, the FSGO was updated with additional requirements:

In general, board members and senior executives must assume more specific responsibilities for a program to be found effective:

- Organizational leaders must be knowledgeable about the content and operation of the compliance and ethics program, perform their assigned duties exercising due diligence, and promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.
- The commission's definition of an effective compliance and ethics program now has three subsections:
  - ***Subsection (a) –*** The purpose of a compliance and ethics program
  - ***Subsection (b) –*** Seven minimum requirements of such a program,
  - ***Subsection (c) –*** The requirement to periodically assess the risk of criminal conduct and design, implement, or modify the seven program elements, as needed, to reduce the risk of criminal conduct

The purpose of an effective compliance and ethics program is to exercise due diligence to prevent and detect criminal conduct and otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law. The new requirement significantly expands the scope of an effective ethics program and requires the organization to report an offense to the appropriate governmental authorities without unreasonable delay.

The U.S. Sarbanes–Oxley Act of 2002 introduced accounting reform and requires attestation to the accuracy of financial reporting documents:

- Section 103, "Auditing, Quality Control, and Independence Standards and Rules," requires the board to
  - Register public accounting firms
  - Establish, or adopt, by rule, "auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers"
- New Item 406(a) of Regulation S-K requires companies to disclose:
  - Whether they have a written code of ethics that applies to their senior officers
  - Any waivers of the code of ethics for these individuals
  - Any changes to the code of ethics
- If companies do not have a code of ethics, they must explain why they have not adopted one.

The U.S. Securities and Exchange Commission approved a new governance structure for the New York Stock Exchange (NYSE) in December 2003. It includes a requirement for companies to adopt and disclose a code of business conduct and ethics for directors, officers, and employees, and promptly disclose any waivers of the code for directors or executive officers. The NYSE regulations require all listed companies to possess and communicate, both internally and externally, a code of conduct or face delisting.

In addition to these, U.S. organizations must monitor new and revised regulations from U.S. regulatory agencies, such as the Food and Drug Administration (FDA), Federal Trade Commission (FTC), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Internal Revenue Service (IRS), and Department of Labor (DoL), and many others throughout the world such as the EU Data Protection Directives. Ethics plans and programs need to be established within the organization to ensure that the organization complies with all such regulatory requirements regardless of the country they reside.

Topics in Computer Ethics

When establishing a computer ethics program and accompanying training and awareness program, it is important to consider the topics that have been addressed and researched. The following topics, identified in most computer ethics textbooks are good to use as a basis.

Computers in the Workplace

Computers can pose a threat to jobs as people feel they may be replaced by them. However, the computer industry already has generated a wide variety of new jobs. When computers do not eliminate a job, they can radically alter it. In addition to job security concerns, another workplace concern is health and safety. It is a computer ethics issue to consider how computers impact health and job satisfaction when information technology is introduced into a workplace.

Computer Crime

With the proliferation of computer viruses, spyware, phishing and fraud schemes, and hacking activity from every location in the world, computer crime and security are certainly topics of concern when discussing computer ethics. Besides outsiders, or hackers, many computer crimes, such as embezzlement or planting of logic bombs, are committed by trusted personnel who have authorization to use company computer systems.

Privacy and Anonymity

One of the earliest computer ethics topics to arouse public interest was privacy. The ease and efficiency with which computers and networks can be used to gather, store, search, compare, retrieve, and share personal information make computer technology especially threatening to anyone who wishes to keep personal information out of the public domain or out of the hands of those who are perceived as potential threats. The variety of privacy-related issues generated by computer technology has led to reexamination of the concept of privacy itself.

Intellectual Property

One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership. Some people, like Richard Stallman, who started the Free Software Foundation, believe that software ownership should not be allowed at all. He claims that all information should be free, and all programs should be available for copying, studying,

and modifying by anyone who wishes to do so. Others, such as Deborah Johnson, author of the first major textbook on computer ethics, argue that software companies or programmers would not invest weeks and months of work and significant funds in the development of software if they could not get the investment back in the form of license fees or sales.

Professional Responsibility and Globalization

Global networks such as the Internet and conglomerates of business-to-business network connections are connecting people and information worldwide. Such globalization issues that include ethics considerations include:

- Global laws
- Global business
- Global education
- Global information flows
- Information-rich and information-poor nations
- Information interpretation

The gap between rich and poor nations, and between rich and poor citizens in industrialized countries, is very wide. As educational opportunities, business and employment opportunities, medical services, and many other necessities of life move more and more into cyberspace, the gaps between the rich and the poor may become even worse, leading to new ethical considerations.

Common Computer Ethics Fallacies

Although computer education is starting to be incorporated in lower grades in elementary schools, the lack of early computer education for most current adults led to several documented generally accepted fallacies that apply to nearly all computer users. As technology advances, these fallacies will change; new ones will arise, and some of the original fallacies will no longer exist as children learn at an earlier age about computer use, risks, security, and other associated information.

There are more than described here, but Peter S. Tippett, developer of Norton Antivirus, identified the following computer ethics fallacies, which have been widely discussed and generally accepted as being representative of the most common.

Computer Game Fallacy

Computer users tend to think that computers will generally prevent them from cheating and doing wrong. Programmers particularly believe that an error in programming syntax will prevent it from working, so that if a software program does indeed work, then it must be working correctly and preventing bad things or mistakes from happening. Even computer users in general have gotten the message that computers work with exacting accuracy and will not allow actions that should not occur. Of course, what computer users often do not consider is that although the computer operates under very strict rules, the software programs are written by humans and are just as susceptible to allowing bad things to happen as people often are in their own lives. Along with this, there is also the perception that a person can do something with a computer without being caught, so that if what is being done is not permissible, the computer should somehow prevent them from doing it.

Law-Abiding Citizen Fallacy

Laws provide guidance for many things, including computer use. Sometimes users confuse what is legal with regard to computer use with what is reasonable behavior for using computers. Laws basically define the minimum standard about which actions can be reasonably judged, but such laws also call for individual judgment. Computer users often do not realize they also have a responsibility to consider the ramifications of their actions and to behave accordingly.

Shatterproof Fallacy

Many, if not most, computer users believe that they can do little harm accidentally with a computer beyond perhaps erasing or messing up a file. However, computers are tools that can harm, even if computer users are unaware of the fact that their computer actions have actually hurt someone else in some way. For example, sending an e-mail insult to a large group of recipients is the same as publicly humiliating them. Most people realize that they could be sued for libel for making such statements in a physical public forum, but may not realize they are also responsible for what they communicate and for their words and accusations on the Internet.

As another example, forwarding e-mail without permission of the author can lead to harm or embarrassment if the original sender was communicating privately without expectation of his or her message being seen by any others. Also, using e-mail to stalk someone, to send spam, and to harass or offend the recipient in some way also are harmful uses of computers. Software piracy is yet another example of using computers to, in effect, hurt others.

Generally, the shatterproof fallacy is the belief that what a person does with a computer can do minimal harm, and only affects perhaps a few files on the computer itself; it is not considering the impact of actions before doing them.

Candy-from-a-Baby Fallacy

Illegal and unethical activity, such as software piracy and plagiarism, are very easy to do with a computer. However, just because it is easy does not mean that it is right. Because of the ease with which computers can make copies, it is likely almost every computer user has committed software piracy of one form or another. The Software Publisher's Association (SPA) and Business Software Alliance (BSA) studies reveal software piracy costs companies multibillions of dollars. Copying a retail software package without paying for it is theft. Just because doing something wrong with a computer is easy does not mean it is ethical, legal, or acceptable.

Hacker Fallacy

Numerous reports and publications of the commonly accepted hacker belief is that it is acceptable to do anything with a computer as long as the motivation is to learn and not to gain or make a profit from such activities. This so-called hacker ethic is explored in more depth in the following section titled "Hacking and Hactivism".

Free Information Fallacy

A somewhat curious opinion of many is the notion that information "wants to be free," as mentioned earlier. It is suggested that this fallacy emerged from the fact that it is so easy to copy digital information and to distribute it widely. However, this line of thinking completely ignores the fact the copying and distribution of data are completely under the control and whim of the people who do it, and to a great extent, the people who allow it to happen.

Hacking and Hacktivism

Hacking is an ambivalent term, most commonly perceived as being part of criminal activities. However, hacking has been used to describe the work of individuals who have been associated with the open-source movement. Many of the developments in information technology have resulted from what has typically been considered as hacking activities. Manuel Castells considers hacker culture as the "informationalism" that incubates technological breakthrough, identifying hackers as "the actors in the transition from an academically and institutionally constructed milieu of innovation to the emergence of self-organizing networks transcending organizational control".

A hacker was originally a person who sought to understand computers as thoroughly as possible. Soon hacking came to be associated with phreaking, breaking into phone networks to make free phone calls, which is clearly illegal.

The Hacker Ethic

The idea of a hacker ethic originates in the activities of the original hackers at MIT and Stanford in the 1950s and 1960s. Stephen Levy, journalist and author of several books on computers, technology, and privacy, outlined the so-called hacker ethic as follows:

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Authority should be mistrusted and decentralization promoted.
4. Hackers should be judged solely by their skills at hacking, rather than by race, class, age, gender, or position.
5. Computers can be used to create art and beauty.
6. Computers can change your life for the better.

The hacker ethic has three main functions:

1. It promotes the belief of individual activity over any form of corporate authority or system of ideals.
2. It supports a completely free-market approach to the exchange of and access to information.
3. It promotes the belief that computers can have a beneficial and life-changing effect.

Ethics Codes of Conduct and Resources

Several organizations and groups have defined the computer ethics their members should observe and practice. In fact, most professional organizations have adopted a code of ethics, a large percentage of which address how to handle information. To provide the ethics of all professional organizations related to computer use would fill a large book. The following are provided to give an opportunity to compare similarities between the codes and, most interestingly, to note the differences (and sometimes contradictions) in the codes followed by the various diverse groups.

The Code of Fair Information Practices

In 1973 the U.S. Secretary's Advisory Committee on Automated Personal Data Systems for the U.S. Department of Health, Education and Welfare recommended the adoption of the following Code of Fair Information Practices to secure the privacy and rights of citizens:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information is in his or her file and how the information is being used.
3. There must be a way for an individual to correct information in his or her records.
4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse.
5. There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

Internet Activities Board (IAB)
(Now the Internet Architecture Board) and RFC 1087

RFC 1087 is a statement of policy by the Internet Activities Board (IAB) posted in 1989 concerning the ethical and proper use of the resources of the Internet. The IAB "strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure," which characterized as unethical and unacceptable any activity that purposely

1. Seeks to gain unauthorized access to the resources of the Internet
2. Disrupts the intended use of the Internet
3. Wastes resources (people, capacity, computer) through such actions
4. Destroys the integrity of computer-based information or
5. Compromises the privacy of users

Computer Ethics Institute (CEI)

In 1991 the Computer Ethics Institute held its first National Computer Ethics Conference in Washington, D.C. The Ten Commandments of Computer Ethics were first presented in Dr. Ramon C. Barquin's paper prepared for the conference, "In Pursuit of a 'Ten Commandments' for Computer Ethics." The Computer Ethics Institute published them as follows in 1992:

1. Thou Shalt Not Use a Computer to Harm Other People.
2. Thou Shalt Not Interfere with Other People's Computer Work.
3. Thou Shalt Not Snoop around in Other People's Computer Files.
4. Thou Shalt Not Use a Computer to Steal.
5. Thou Shalt Not Use a Computer to Bear False Witness.
6. Thou Shalt Not Copy or Use Proprietary Software for Which You Have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources without Authorization or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think about the Social Consequences of the Program You Are Writing or the System You Are Designing.
10. Thou Shalt Always Use a Computer in Ways That Insure Consideration and Respect for Your Fellow Humans.

National Conference on Computing and Values

The National Conference on Computing and Values (NCCV) was held on the campus of Southern Connecticut State University in August 1991. It proposed the following four primary values for computing, originally intended to serve as the ethical foundation and guidance for computer security:

1. Preserve the public trust and confidence in computers.
2. Enforce fair information practices.
3. Protect the legitimate interests of the constituents of the system.
4. Resist fraud, waste, and abuse.

The Working Group on Computer Ethics

In 1991, the Working Group on Computer Ethics created the following End User's Basic Tenets of Responsible Computing:

1. I understand that just because something is legal, it isn't necessarily moral or right.
2. I understand that people are always the ones ultimately harmed when computers are used unethically. The fact that computers, software, or a communications medium exists between me and those harmed does not in any way change moral responsibility toward my fellow humans.
3. I will respect the rights of authors, including authors and publishers of software as well as authors and owners of information. I understand that just because copying programs and data is easy, it is not necessarily right.
4. I will not break into or use other people's computers or read or use their information without their consent.
5. I will not write or knowingly acquire, distribute, or allow intentional distribution of harmful software like bombs, worms, and computer viruses.

National Computer Ethics and Responsibilities Campaign (NCERC)

In 1994, a National Computer Ethics and Responsibilities Campaign (NCERC) was launched to create an "electronic repository of information resources, training materials and sample ethics codes" that would be available on the Internet for IS managers and educators. The National Computer Security Association (NCSA) and the CEI cosponsored NCERC. The NCERC Guide to Computer Ethics was developed to support the campaign.

The goal of NCERC is to foster computer ethics awareness and education. The campaign does this by making tools and other resources available for people who want to hold events, campaigns, awareness programs, seminars, and conferences or to write or communicate about computer ethics. NCERC is a nonpartisan initiative intended to increase understanding of the ethical and moral issues unique to the use, and sometimes abuse, of information technologies.

(ISC)² Code of Professional Ethics

The following is an excerpt from the (ISC)² Code of Ethics preamble and canons, by which all (ISC)² members must abide. Compliance with the preamble and canons is mandatory to maintain membership and credentials. Professionals resolve conflicts between the canons in the order of the canons. The canons are not equal and conflicts between them are not intended to create ethical binds.

Code of Ethics Preamble

Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons

Protect Society, the Commonwealth, and the Infrastructure

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act Honorably, Honestly, Justly, Responsibly, and Legally

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide Diligent and Competent Service to Principals

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and Protect the Profession

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

Support Organization's Code of Ethics

Peter S. Tippett has written extensively on computer ethics. He provided the following action plan to help corporate information security leaders to instill a culture of ethical computer use within organizations:

1. Develop a corporate guide to computer ethics for the organization.
2. Develop a computer ethics policy to supplement the computer security policy.
3. Add information about computer ethics to the employee handbook.
4. Find out whether the organization has a business ethics policy, and expand it to include computer ethics.

5. Learn more about computer ethics and spreading what is learned.
6. Help to foster awareness of computer ethics by participating in the computer ethics campaign.
7. Make sure the organization has an E-mail privacy policy.
8. Make sure employees know what the E-mail policy is.

Fritz H. Grupe, Timothy Garcia-Jay, and William Kuechler identified the following selected ethical bases for IT decision making

- ***Golden Rule –*** Treat others as you wish to be treated. Do not implement systems that you would not wish to be subjected to yourself. Is your company using unlicensed software although your company itself sells software?
- ***Kant's Categorical Imperative –*** If an action is not right for everyone, it is not right for anyone. Does management monitor call center employees' seat time, but not its own?
- ***Descartes' Rule of Change (also called the Slippery Slope) –*** If an action is not repeatable at all times, it is not right at any time. Should a Web site link to another site, "framing" the page, so users think it was created and belongs to the former?
- ***Utilitarian Principle (also called Universalism) –*** Take the action that achieves the most good. Put a value on outcomes and strive to achieve the best results. This principle seeks to analyze and maximize the IT of the covered population within acknowledged resource constraints. Should customers using a Web site be asked to opt in or opt out of the possible sale of their personal data to other companies?
- ***Risk Aversion Principle –*** Incur least harm or cost. When there are alternatives that have varying degrees of harm and gain, choose the one that causes the least damage. If a manager reports that a subordinate criticized him in an e-mail to other employees, who would do the search and see the results of the search?
- ***Avoid Harm –*** Avoid malfeasance or "do no harm." This basis implies a proactive obligation of companies to protect their customers and clients from systems with known harm. Does your company have a privacy policy that protects, rather than exploits customers?
- ***No Free Lunch Rule –*** Assume that all property and information belong to someone. This principle is primarily applicable to intellectual property that should not be taken without just compensation. Has a company used unlicensed software? Or hired a group of IT workers from a competitor?
- ***Legalism –*** Is it against the law? Moral actions may not be legal, and vice versa. Might a Web advertising exaggerate the features and benefits of products? Are web sites collecting information illegally on minors?
- ***Professionalism –*** Is an action contrary to codes of ethics? Do the professional codes cover a case and do they suggest the path to follow? When you present technological alternatives to managers who do not know the right questions to ask, do you tell them all they need to know to make informed choices?
- ***Evidentiary Guidance –*** Is there hard data to support or deny the value of taking an action? This is not a traditional "ethics" value but one that is a significant factor related to IT's policy decisions about the impact of systems on individuals and groups. This value involves probabilistic reasoning where outcomes can be predicted based on hard evidence based on research. Does management assume that they know PC users are satisfied with IT's service or has data been collected to determine what they really think?

- ***Client/Customer/Patient Choice –*** Let the people affected decide. In some circumstances, employees and customers have a right to self-determination through the informed consent process. This principle acknowledges a right to self-determination in deciding what is "harmful" or "beneficial" for their personal circumstances. Are workers subjected to monitoring in places where they assume that they have privacy?
- ***Equity –*** Will the costs and benefits be equitably distributed? Adherence to this principle obligates a company to provide similarly situated persons with the same access to data and systems. This can imply a proactive duty to inform and make services, data, and systems available to all those who share a similar circumstance. Has IT made intentionally inaccurate projections as to project costs?
- ***Competition –*** This principle derives from the marketplace where consumers and institutions can select among competing companies, based on all considerations such as degree of privacy, cost, and quality. It recognizes that to be financially viable in the market, it is necessary to have data about what competitors are doing and understand and acknowledge the competitive implications of IT decisions. When presenting a build or buy proposition to management, is it fully aware of the risk involved?
- ***Compassion/Last Chance –*** Religious and philosophical traditions promote the need to find ways to assist the most vulnerable parties. Refusing to take unfair advantage of users or others who do not have technical knowledge is recognized in several professional codes of ethics. Do all workers have an equal opportunity to benefit from the organization's investment in IT?
- ***Impartiality/Objectivity –*** Are decisions biased in favor of one group or another? Is there an even playing field? IT personnel should avoid potential or apparent conflicts of interest. Do you or any of your IT employees have a vested interest in the companies that you deal with?
- ***Openness/Full Disclosure –*** Are persons affected by this system aware of its existence, aware of what data are being collected, and knowledgeable about how it will be used? Do they have access to the same information? Is it possible for a Web site visitor to determine what cookies are used and what is done with any information they might collect?
- ***Confidentiality –*** IT is obligated to determine whether data it collects on individuals can be adequately protected to avoid disclosure to parties whose need to know is not proven. Have security features been reduced to hold expenses to a minimum?
- ***Trustworthiness and Honesty –*** Does IT stand behind ethical principles to the point where it is accountable for the actions it takes? Has IT management ever posted or circulated a professional code of ethics with an expression of support for seeing that its employees act professionally?

How a Code of Ethics Applies to CISSPs

In 1998, Michael Davis, a professor of Philosophy at the Illinois Institute of Technology, described a professional ethics code as a "contract between professionals." According to this explanation, a profession is a group of persons who want to cooperate in serving the same ideal better than they could if they did not cooperate. Information security professionals, for example, are typically thought to serve the ideal of ensuring the confidentiality, integrity, and availability of information and the security of the technology that supports the information use. A code of ethics would then specify how professionals should pursue their common ideals so that each may do his or her best to reach the goals at a minimum cost while appropriately addressing the issues involved.

The code helps to protect professionals from certain stresses and pressures (such as the pressure to cut corners with information security to save money) by making it reasonably likely that most other members of the profession will not take advantage of the resulting conduct of such pressures. An ethics code also protects members of a profession from certain consequences of competition, and encourages cooperation and support among the professionals.

Considering this, an occupation does not need society's recognition to be a profession. Indeed, it only needs the actions and activities among its members to cooperate to serve a certain ideal. Once an occupation becomes recognized as a profession, society historically has found reason to give the occupation special privileges (e.g., the sole right to do certain kinds of work) to support serving the ideal in question (in this case, information security) in the way the profession serves society.

Understanding a code of ethics as a contract between professionals, it can then be explained why each information security professional should not depend upon only his or her private conscience when determining how to practice the profession, and why he or she must take into account what a community of information security professionals has to say about what other information security professionals should do. What others expect of information security professionals is part of what each should take into account in choosing what to do within professional activities, especially if the expectation is reasonable. The ethics code provides a guide to what information security professionals may reasonably expect of one another, basically setting forth the rules of the game.

Just as athletes need to know the rules of football to know what to do to score, computer professionals also need to know computer ethics to know, for example, whether they should choose information security and risk reduction actions based completely and solely upon the wishes of an employer, or, instead, also consider information security leading practices and legal requirements when making recommendations and decisions.

A code of ethics should also provide a guide to what computer professionals may expect other members of our profession to help each other do. Keep in mind that people are not merely members of this or that profession. Each individual has responsibilities beyond the profession and, as such, must face his or her own conscience, along with the criticism, blame, and punishment of others, as a result of actions. These issues cannot be escaped just by making a decision because their profession told them to.

Information security professionals must take their professional code of ethics and apply it appropriately to their own unique environments. To assist with this, Donn B. Parker a consultant, information security researcher and fellow of the association for computing machinery describes the following five ethical principles that apply to processing information in the workplace, and also provides examples of how they would be applied.

1. ***Informed consent.*** Try to make sure that the people affected by a decision are aware of your planned actions and that they either agree with your decision, or disagree but understand your intentions.

   Example: An employee gives a copy of a program that she wrote for her employer to a friend, and does not tell her employer about it.

2. ***Higher ethic in the worst case.*** Think carefully about your possible alternative actions and select the beneficial necessary ones that will cause the least, or no, harm under the worst circumstances.

   Example: A manager secretly monitors an employee's email, which may violate his privacy, but the manager has evidence-based reason to believe that the employee may be involved in a serious theft of trade secrets.

3. ***Change of scale test.*** Consider that an action you may take on a small scale, or by you alone, could result in significant harm if carried out on a larger scale or by many others.

   Examples: A teacher lets a friend try out, just once, a database that he bought to see if the friend wants to buy a copy, too. The teacher does not let an entire classroom of his students use the database for a class assignment without first getting permission from the vendor. A computer user thinks it's okay to use a small amount of her employer's computer services for personal business, since the others' use is unaffected.

4. ***Owners' conservation of ownership.*** As a person who owns or is responsible for information, always make sure that the information is reasonably protected and that ownership of it, and rights to it, are clear to users.

   Example: A vendor, who sells a commercial electronic bulletin board service with no proprietary notice at log-on, loses control of the service to a group of hackers who take it over, misuse it, and offend customers.

5. ***Users' conservation of ownership.*** As a person who uses information, always assume others own it and their interests must be protected unless you explicitly know that you are free to use it in any way that you wish.

   Example: Hacker discovers a commercial electronic bulletin board with no proprietary notice at logon, and informs his friends, who take control of it, misuse it, and then uses it to offend other customers.

Develop and Implement Security Policy

Imagine the day-to-day operation of an organization without any policies. Individuals would have to make decisions about what is right or wrong for the company based upon their personal values or their own past experience. While many small companies and startups operate in this fashion, this could potentially create as many values as there are people in the organization. Policies establish the framework for the security program that ensures that everyone has a common set of expectations and communicates the management's goals and objectives.

Procedures, standards, guidelines, and baselines (illustrated in *Figure 1.7*) are components that support the implementation of the security policy. A policy without mechanisms supporting its implementation is analogous to an organization having a business strategy without action plans to execute the strategy. Policies communicate the management's expectations, which are fulfilled through the execution of procedures and adherence to standards, baselines, and guidelines.

Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end-users that will consume them. Policies that are poorly written, or written at too high of an education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.

While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the appropriate business issues are addressed. The security officers will get better corporate support by including other areas in policy development. This helps to instill buy-in within these areas as they take on a greater ownership of the final product and reduces rework later should they need to provide vital input.

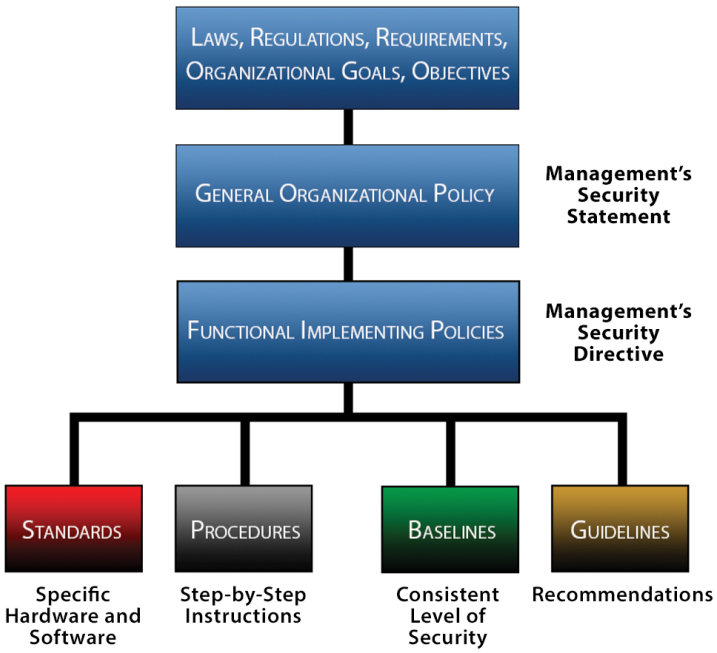


Figure 1.7 - **Relationships among policies, standards, procedures, baselines, and guidelines**

The security professional should consider inviting areas such as HR, legal, compliance, various IT areas, and specific business area representatives who represent critical business units to participate in the drafting process. When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations.

Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility. Such placement of these documents plus awareness actions, training if needed, checklists, forms, and sample documents can make awareness and ultimately compliance more effective.

Business Continuity (BC) & Disaster Recovery (DR) Requirements

Project Initiation and Management

The first step in building the Business Continuity (BC) program is project initiation and management. During this phase, the following activities will occur:

- Obtain senior management support to go forward with the project
- Define a project scope, the objectives to be achieved, and the planning assumptions
- Estimate the project resources needed to be successful, both human resources and financial resources
- Define a timeline and major deliverables of the project

In this phase, the program will be managed like a project, and a project manager should be assigned to coordinate the team's activities.

Senior Leadership Support

Before the project can even start, it must have committed senior management support. Without that support, the project will fail. To convince leadership that the organization needs to build an enterprise-wide BC and DR plan, the planner must sell the importance of the program to the leadership.

Senior leadership in any organization has two major goals: Execute the mission and protect the organization. Business continuity and DR have little to do with executing the mission (unless the organization's mission is DR!) and everything to do with protecting the organization. It is still a hard sell because unless the organization actually has a disaster; the value of the time, money, and human resources required to build the plan is going to be suspect because it takes away from goal number one, executing the mission. So, why does an organization need BC and DR anyway? What possible value could they provide? We have to go back to the beginning in order to answer these questions.

It all started in the data center. Once computers became part of the enterprise landscape, even before the introduction of personal computers on individual desks, it quickly became clear that organizations could not return to manual processes if computers failed. The operational model had changed. The work people did with manual general ledgers in ledger books or with their hands in a manufacturing environment was now done more consistently, with fewer errors and many times faster, by computers. If those computer systems failed, there were not enough people to do the work nor did the people in the organization still have the skills to do it manually anymore. This was the start of the DR industry. Still today, the term "disaster recovery" commonly means recovery of the technology environment.

It took some time for many industries to realize that it really did not matter if the data center were recovered if there were no people to use it. That is when the term Business Continuity began to replace Disaster Recovery as a more accurate reflection of the goal of the industry – to enable the continuation of the work/mission of the organization as quickly and with as little disruption as possible.

To convince leadership of the need to build a viable Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP), the planner needs to help them understand the risk they are accepting by not having one and the potential cost to the organization if a disaster were to occur. The risks to the organization are found in three areas: financial (how much money the organization stands to lose), reputational (how negatively the organization will be perceived by its customers and its shareholders), and regulatory (fines or penalties incurred, lawsuits filed against them). There is also the potential that the leaders of the organization could be held personally liable, financially and even criminally, if it is determined that they did not use due care to adequately protect the organization and its resources.

Financial risks can be quantified in many cases and are generally used to help determine how much should be spent on the recovery program. One of the ways financial risk can be calculated is using the formula **P * M = C**:

- ***Probability of Harm (P) –*** the chance that a damaging event will occur, times the
- ***Magnitude of Harm (M) –*** the amount of financial damage that would occur should a disaster happen =
- ***Cost of Prevention (C) –*** the price of putting in place a countermeasure preventing the disaster's effects. The cost of countermeasures should not be more than the cost of the event.

Reputational risk is harder to quantify. For example, if a company cannot satisfy the needs of its customers when required, it is not hard for the customer to find someone else who will. Reputational risk is about how the company is perceived by its customers and stockholders. There are many examples of a negative impact to stock price in the wake of a crisis that is not managed properly. Effective BC and DR programs can be the difference between a company surviving an event and a company ceasing to exist.

Additional Benefits of the Planning Process

In many organizations, contingency planning is a necessity that has turned out to be beneficial in more ways than ever expected. Contingency planning helps to ensure an organization's viability during and following a disaster. Another benefit of contingency planning is significant improvements in the daily operations of many organizations.

Researching and documenting contingency plans can discover numerous Single Points of Failure (SPOF). A SPOF is any single input to a process that, if missing, would cause the process or several processes to be unable to function. Once identified, these SPOFs can often easily be eliminated or have their damaging potential reduced. Many organizations have also witnessed process improvements as a direct result of their contingency planning efforts, particularly while exercising their DR and BCPs.

There are many more benefits to contingency planning. Few other processes require that a data center staff or an organization think about what they do, how they do it, and how to make it better. Thinking about how to recover in a new environment, operating without the primary building, missing half the staff, or working without connectivity all lead to improved performance and resilience.

Develop and Document Project Scope and Plan

When one is seeking senior leadership approval, it is important to gain agreement on the scope and goals of the planning effort. Will the plan cover just the technology recovery or will it cover the organizational operations as well? Will it address only the technology in the data center or will it address all the technology used to run the organization? Will it address recovery of the main office only or will all the offices be considered?

Every company needs a technology recovery plan. Whether the company is a small organization that conducts all of its business on a laptop or a major corporation with multiple data centers, technology is an integral part of how business is conducted in today's world.

Planning for the recovery of the organization operations is also key to the survivability of the organization. Both the technology recovery and the organization recovery enable the organization to continue in the wake of an unexpected event. Another type of planning to consider is some type of workforce impairment event such as a pandemic, a labor strike, transportation issues, etc., where the building is fine, the data center is fine, but for some reason, the workforce is unable or unwilling to come to work.

The planner will need to agree with the senior leadership on the scope of the planning effort because that will define the project resources the planner will need, the timeline to complete the project, and the deliverables the leadership team can expect as the project progresses. Generally, building a plan where none currently exists within a medium sized organization (1,000 - 3,000 staff with two data centers) with an experienced planner and a commitment from leadership to support the effort would follow a timeline as outlined below:

- ***Emergency Notification List –*** 1 month
  - To respond to an emergency with any success, the planner must first be able to reach the people in the organization who can and will respond.
- ***Vital Records Backup and Recovery –*** Within the first 6 months
  - To be able to recover from a disaster situation, the planner must have access to all records needed to operate the organization.
- ***Business Impact Analysis –*** First 6 months
  - Identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered; identify resources required for recovery of those areas and interdependencies.

- ***Strategy Development –*** 6 to 9 months
  - Assessing various available strategies, performing cost benefit analysis, and making recommendations to leadership for approval.
- ***Alternate Site Selection –*** 9 to 12 months
  - Preparing Requests for Proposals (RFPs), performing site surveys, selecting vendor and/or build out and equip of internal site, and negotiating contracts.
- ***Contingency Plan Development –*** 12 months
  - Including: emergency response, restoring of critical systems, and organization functions to normal organization operations.
- ***Testing, Plan Maintenance, and Periodic Audit –*** Ongoing

Organizational Analysis

Senior leadership must support an organizational policy requiring compliance with the BCP/DRP development program to facilitate getting resources assigned from the various areas of the organization that will need to participate. The policy should state the following:

"The senior leaders of each functional area of the company are responsible for ensuring that a BCP exists for their area of responsibility, for the contents of the plan itself, and for affirming their concurrence with the plan annually by signing off on the plan document."

Conducting the Business Impact Analysis (BIA)

The next step in the planning process is to have the planning team perform a BIA. The BIA will help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated with terms such as critical, essential, supporting, and nonessential to help determine the appropriate prioritization.

Identify and Prioritize

Critical Organization Functions

Generally speaking, organizations do not hire staff to perform nonessential tasks. Every function has a purpose, but some are more time sensitive than others when there is limited time or resources available to perform them. A bank that has suffered a building fire could easily stop its marketing campaign but would not be able to stop check processing and deposits made by its customers. The organization needs to look at every function in this same light. How long can the company not perform this function without causing significant financial losses, significant customer unhappiness or losses, or significant penalties or fines from regulators or lawsuits?

All organizational functions and the technology that supports them need to be classified based on their recovery priority. Recovery time frames for organizational operations are driven by the consequences of not performing the function. The consequences may be the result of contractual commitments not met resulting in fines or lawsuits, lost goodwill with customers, etc. *Figure 1.8* is a simple BIA form for classifying functions and determining their time sensitivity code, which is shown in *Figure 1.9*. To use this form, the planner will need to adjust the factors to reflect the organization being evaluated. The planner will need to define for the planning team what a low, medium, or high impact is in that organization in each of the impact areas, as well as the time before impact is realized.

	Impact Codes	Call Center	Customer Account Maintenance	Customer Monetary
Mail Zone		*Z 45*	*Z 37*	*Z 38*
Risk Code	*F=Financial C=Customer R=Regulatory*	*C & F*	*C*	*C & F & R*
Time Before Impact	*0=Week 2 or more 1=Week 1 5=Up to 3 days 10=Day 1 20=4 hours 40=Immediate*	*40*	*1*	*10*
Customer Impact	*0=None 1=Low 3=Medium 5=High*	*5*	*3*	*3*
Regulatory Impact	*0=None 1=Low 3=Medium 5=High*	*1*	*0*	*3*
Financial Impact	*0=None 1=0 to10K 2=>10K but < 100K 3=>100K but <500K 4=>500K but <1 Mil 5=>1Mil*	*3*	*0*	*4*
Rating Total	*Sum of 1 through 4*	***49***	***4***	***20***
Recovery Time Sensitivity Code		*AAA*	*D*	*A*
Alternate Site		*Surviving sites then Smith Road*	*Work from Home*	*Smith Road*

Figure 1.8 - **Sample BIA form**

Business Function Recovery Time Sensitive Codes

***Rating Total of 45 or More* =**

AAA Immediate Recovery

Must be performed in at least two geographically dispersed locations that are fully equipped and staffed

***Rating Total of 25 to 45* =**

AA Up to 4 hours to recover

Must have a viable alternate site that can be staffed and functioning within the four hour timeframe required

***Rating Total of 15 to 24* =**

A Same day recovery

Must be operational the same business day and must therefore have a viable alternate site that can be staffed and functioning within the same business day

***Rating Total of 10 to 14* =**

B Up to 3 days

Can be suspended for up to 3 business days, but must have a viable alternate site that can be staffed and functioning by the fourth business day

***Rating Total of 7 to 10* =**

C Week 1

Can be suspended for up to a week, but must have a viable alternate site that can be staffed and functioning by the second week following an interruption

***Rating Total of 0 to 6* =**

D Week 2 or greater downtime allowable

Can be suspended for greater than one week - A maximum number of days should be identified for this function

Figure 1.9 – **Time Sensitivity Codes**

Determine Maximum Tolerable Downtime

All applications, like all organization functions, need to be classified as to their time sensitivity for recovery even if those applications do not support organization functions that are time sensitive. For applications, this is commonly referred to as Recovery Time Objective (RTO) or Maximum Tolerable Downtime (MTD). This is the amount of time the organization can function without that application before significant impact occurs.

Assess Exposure to Outages

Understanding the Organization

As part of the planning process, the planner will need to perform a risk assessment to determine which threats the organization has and where the planner will recommend spending mitigating dollars to attempt to reduce the impact of a threat.

There are three elements of risk: threats, assets, and mitigating factors. A threat is an event or situation that, if it occurred, would prevent the organization from operating in its normal manner, if at all. Threats are measured in probabilities such as "may happen 1 time in 10 years" and have a specified duration of time where the impact is felt.

External Threats and Vulnerabilities

The most common threat that impacts an organization's ability to function normally is power availability. Power outages cause more organization interruption events than any other type of event. The second most common type of event is water, either too much water (flooding, plumbing leak, broken pipes, and leaky roof) or not enough (water main break). Other common events are severe weather, cable cuts resulting in network outages, fires, labor disputes, transportation mishaps, and for the data center, hardware failures.

Internal Threats and Vulnerabilities

Internal outages are typically caused by the following actions:

- Equipment fails prematurely
  - Could be due to improper installation
  - Could also be due to improper environment
- Equipment fails due to wear and tear
  - Most equipment has a "mean time between failures" (MTBF) rating
  - Running equipment beyond the MTBF is risking failure
- Equipment goes down due to untested production changes or other human errors

Refer to the threat matrix in *Figure 1.10*. Reviewing the list of threats, one will notice that some of them are events that are fairly localized while others, like a hurricane, have a more regional impact. Threats to be considered include both natural hazards, such as tornados, earthquakes, and hurricanes, and man-made hazards, such as transportation mishaps, chemical spills, and sabotage.

Figure 1.10 – **Potential Threats**

Recovery Point Objectives (RPO)

Once all the organization functions have been identified and a recovery time frame determined, the planning team then needs to identify all the resources necessary to perform each of those functions. Resources include applications systems, minimum staff requirements, phone requirements, desktop requirements, internal and external interdependencies, etc.

The recovery priority for application systems is identified during this process. It is the organization that decides what application systems need to come back online when based on the recovery priority of the functions those applications support.

This technology review process is sometimes difficult for the organization to perform. The basic average desktop users know they click on this icon and this application system launches. They have little comprehension of where the application resides (mainframe, Web, server, or desktop), where the data resides (central storage, a network server, the cloud, or the desktop), or where the executable resides for that matter.

These are important considerations in building a recovery plan. If the application is collocated with the organization, then the recovery for that application must be part of the site recovery plan for that site. If it is not, then recovery could mean only providing network access to the application at the alternate site.

For both organization functions and applications, the organization also needs to determine the amount of work in process that may be at risk during an event. The data that is on employees' desks when a fire occurs would be lost forever if that information was not backed up somewhere else. The information stored in file cabinets, incoming mail in the mailroom, the backup tapes that have not yet left the building, are all also at risk.

The planning team needs to make decisions about all types of data because data is what runs the organization. How much data is it acceptable to lose? A minute's worth? An hour's worth? A whole business day? This is commonly referred to as the recovery point objective (RPO), the point in time that the planner will attempt to recover to. Backup policies and procedures for electronic data and hard copy data need to comply with the RPO established by the organization.

Manage Personnel Security

Individuals within an organization come to work every day to perform their jobs to the best of their ability. As such, these individuals have the appropriate intentions and seek out information on the best ways to perform their jobs, the training required, and what the expectations of their jobs are. The media has placed much attention on the external threat faced by the organization with regards to hackers; however, there is also the threat internally of erroneous or fraudulent transactions, which could cause information assets to be damaged or destroyed. Internal personnel are closest to the data and best understand the processes, along with control weaknesses, that currently exist. Job controls such as the segregation of duties, job description documentation, mandatory vacations, job and shift rotation, and need-to-know (least privilege) access need to be implemented by the security professional in order to minimize the risks to data from within the organization. The security practitioner may look to robust monitoring controls such as behavioral anomaly detection to detect patterns of unusual data access based on what a "normal" user's baseline may be as an additional layer of controls to further reinforce a defense in depth strategy in this area.

In addition, various activities should be performed prior to an individual starting in a position. Some will be performed by the security professional directly, while others may be performed with his or her input or oversight by other members of the organization. These activities may include developing job descriptions, contacting references, screening/investigating of the background of the individual, developing confidentiality and non-disclosure agreements, as well as determining policies on vendor, contractor, consultant, and temporary staff access.

Employment Candidate Screening

Hiring qualified, suitable, and trustworthy individuals depends upon implementing and adhering to personnel policies that screen out those whose past actions may indicate undesirable behavior. Lower employee morale can result in reduced compliance with controls. Increased staff turnover can also result in lower levels of staff expertise over time. Termination policies and procedures are necessary to ensure that terminated employees no longer have access to the system, and therefore do not have the opportunity to damage files or systems or disrupt company operations. These are also necessary to ensure that policy is consistently applied to personnel. Although most employees are hardworking, competent individuals with no intentions of wrongdoing, there can be a few people with less than desirable intentions. Poor personnel security increases the risks to information, making it imperative to implement the appropriate personnel security controls.

Job descriptions should contain the roles and responsibilities of the position and the education, experience, and expertise required to satisfactorily perform the job function. A well-written job description provides not only the basis for conversation with the applicant to determine if his or her skills are a good match but also the barometer by which ongoing performance reviews can be measured. Individual job goals stated within the performance reviews should mirror the job description. Failure to align the correct job description with a position could result in the individual lacking skills for the job requirements. To ensure that individuals possess the necessary skills on an ongoing basis, one should periodically reassess the job skills. Requirements for annual training, especially for those individuals requiring specialized security training, will ensure that the skills remain relevant and current. Roles and responsibilities as defined by policies can help identify specific security skills that are needed. The employee training and participation in professional activities should be monitored and encouraged. All job descriptions of the organization should have some reference to information security responsibilities because these responsibilities are shared across the organization. Specific technology, platform requirements, and certifications required for security staff should be noted within the job posting.

The access and duties of an individual for a particular department should be assessed to determine the sensitivity of the job position. The degree of harm that the individual can cause through misuse of the computer system, through disclosing information, disrupting data processing, sharing internal secrets, modifying critical information, or committing computer fraud should be input to the classification as well. Role-based access establishes roles for a job or class of jobs, indicating the type of information the individual is permitted to access. Job sensitivity may also be used to require more stringent policies related to mandatory vacations, job rotations, and access control policies. Excess controls for the sensitivity level of the position waste resources through the added expense, while fewer controls cause unacceptable risks.

Reference Checks

During the interviewing and hiring process, individuals attempt to determine the past work history of the applicant and his or her competencies, such as teamwork, leadership abilities, perseverance, ethics, customer service orientation, management skills, planning, and specific technical and analytical capabilities. Much of the information provided is obtained by observing the individual during the interview process or from the information he or she has provided through the targeted questions. It is not always possible to determine the true work orientation of the prospective employee without other collaborating information. There are essentially two kinds of reference checks: personal and work. Personal accounting for the character of the person and work associated with verifying the provided work history.

Personal reference checks involve contacting those individuals supplied by the prospective employee. Many employers are reluctant to provide personal references for fear of future litigation. As such, many employers may have policies that only allow information such as date of hire and date of termination to be released. No information on why a termination occurred is released other than potentially whether it was a friendly (employee choice) or unfriendly (company terminated) decision. This still does not necessarily provide a reflection on the employee behavior because it may have been the result of staff reduction having nothing to do with performance. After all, when a company provides a reference, it can be perceived as placing a stamp of approval on

the performance or character of the employee, even though the person providing the reference really has no control over the future work performance of the employee. Many individuals will provide references to place them in the best possible light and may place individuals such as presidents, vice presidents, doctors, lawyers, ministers, and so forth on the list to create the appearance of greater integrity. Targeted questions will be used by an employer to ascertain the tendencies and capabilities of the candidate, such as leadership ability, oral and written communication skills, decision-making skills, ability to work with others, respect from peers, how the individual acted under stress, and managerial ability (budgeting, attracting talent, delivering projects). Multiple reference checks provide multiple perspectives and provide for corroboration of the desired behaviors. Employers need to balance the response of references with the knowledge that the references were provided by the applicant and may be biased in their opinions. Failure of a prospective employee to provide references may be an indicator of a spotty work record or the possibility of prior personnel actions/sanctions against the individual.

Background Investigations

Just as the personal reference checks provide the opportunity to obtain corroborating information on whether the applicant will potentially be a good addition to the company, background checks can uncover more information related to the ability of the organization to trust the individual. Organizations want to be sure of the individuals that they are hiring and minimize future lawsuits or exposure. Resumes are often filled with errors, accidental mistakes, or blatant lies to provide a perceived advantage to the applicant. Common falsifications include embellishment of skill levels, job responsibilities, and accomplishments, certifications held, and the length of employment. The background checks can greatly assist the hiring manager in determining whether he or she has an accurate representation of the skills, experience, and work accomplishments of the individual. Commercial businesses typically do not have the time and money to conduct meaningful, thorough investigations on their own and hire outside firms that specialize in the various background checks. Background checks can uncover:

- Gaps in employment
- Misrepresentation of job titles
- Job duties
- Salary
- Reasons for leaving a job
- Validity and status of professional certification
- Education verification and degrees obtained
- Credit history
- Driving records
- Criminal history
- Personal references
- Social security number verification

Benefits of Background Checks

The benefits of background checks in protecting the company are self-evident; however, the following benefits may also be realized:

- Risk mitigation
- Increased confidence that the most qualified candidate was hired versus the one who interviewed the best
- Lower hiring cost
- Reduced turnover
- Protection of assets
- Protection of the company's brand reputation
- Shielding of employees, customers, and the public from theft, violence, drugs, and harassment
- Insulation from negligent hiring and retention lawsuits
- Safer workplace by avoiding hiring employees with a history of violence
- Discouraging of applicants with something to hide
- Identify criminal activity

Timing of Checks

An effective background check program requires that all individuals involved in the hiring process support the program prior to the candidate being selected for hire. This requires that the human resources department, legal, hiring supervisors, and recruiters understand and execute the screening process. Once the individual is hired into the organization, it is much harder to obtain the information without having a specific cause for performing the investigation. Employees should also be periodically reinvestigated consistent with the sensitivity of their positions. This should also be documented in the appropriate policies, including a frequency schedule.

Types of Background Checks

Many different types of background checks can be performed depending upon the position that the individual may be hired for. A best practice would be to perform background checks on all of the company's employees and to require external agencies through contract agreements to perform background checks on the contractors, vendors, and anyone coming in contact with the company assets, systems, and information. If this is cost-prohibitive, the organization must decide on the positions on which it is most critical to conduct background checks. Banks, for example, are required to perform background checks on any employee who may come in contact with money. In a bank, this is obviously nearly every employee. The types of checks range from minimal checks to full background investigations. The types of individuals upon whom an organization may focus the checks or decide to provide more extensive checks include:

- Individuals involved in technology
- Individuals with access to confidential or sensitive information
- Employees with access to company proprietary or competitive data
- Positions working with accounts payable, receivables, or payroll
- Positions dealing directly with the public
- Employees working for healthcare industry-based organizations or organizations dealing with financial information
- Positions involving driving a motor vehicle
- Employees who will come in contact with children

There is a broad range of possible background checks available. The following are the most common background checks performed.

Credit History

Credit history is the primary vehicle used by financial institutions to ensure the repayment of consumer loans, credit cards, mortgages, and other types of financial obligations. Credit histories are used to screen for high default risks and to discourage default. Financial services firms use credit histories as primary leverage, providing a threat to place delinquent information on the individual's credit reports should he or she fall behind in payments. In the past, managers would run a credit report only on those individuals who were directly handling money; however, this has changed due to the interconnection of computers and the potential access to high-risk applications. Basic credit reports verify the name, address, social security number, and prior addresses of the applicant. These can be used to provide more extensive criminal searches or uncover gaps in employment. Detailed credit histories provide the employer with liens, judgments, and payment obligations that may give an indication as to the individual's ability to handle his or her financial obligations. However, these items must be evaluated in context because the individual may have previously slipped into financial trouble and then reorganized his or her financial life so that this would not present a risk to the prospective employer. Sometimes credit reports have limited or no information, which may be representative of a prospect's age (has not yet established a credit history), cash paid for purchases, assumption of a false identity, or a prospect's residence (lives in an area that relies on fringe lenders, which typically do not report to credit bureaus).

Employers need to ensure that they are using the information appropriately, according to their country's laws. In the United States, the Fair Credit Reporting Act (FCRA), laws under the Equal Employment Opportunity Commission (EEOC), and some state laws will govern the actions by the organization.[29] Legal counsel and human resources should be involved in the development of any policies and procedures related to the screening process.

Criminal History

Criminal records are more difficult to obtain than credit histories because credit histories are exchanged through a system among banks, retail establishments, financial services firms, and credit-reporting bureaus. With more than 3,000 legal jurisdictions in the United States, it is not feasible to search each jurisdiction. Starting with the county of residence and searching in other prior addresses will provide a reasonable background check for the applicant. Most background checks examine felonies and overlook misdemeanors (less serious crimes). Under the FCRA, employers can request full criminal records for the past seven years unless the applicant earns more than $75,000 annually, in which case there are no time restrictions. Important information to be searched includes state and county criminal records, sex and violent offender records, and prison parole and release records.

29 Please see the following for detailed information on the Fair Credit Reporting Act: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf
Please see the following for information about the Equal Employment Opportunity Commission: http://www.eeoc.gov/

Driving Records

Driving records should be checked for those employees who will be operating a motor vehicle on their job. These records can also reveal information about applicants who will not be driving vehicles as part of their employment, such as verification of the applicant's name, address, and social security number, and will include information on traffic citations, accidents, driving-under-the-influence arrests, convictions, suspensions, revocations, and cancellations. These may be indicators of a possible alcohol or drug addiction or a lack of responsibility.

Drug and Substance Testing

The use of illicit drugs is tested for by most organizations because drug use may result in lost productivity, absenteeism, accidents, employee turnover, violence in the workplace, and computer crimes. Individuals using drugs avoid applying or following through the process with companies that perform drug testing. There are many different screening tests available, such as screens for amphetamines, cocaine and PCP, opiates (codeine, morphine, etc.), marijuana (THC), phencyclidine, and alcohol. Independent labs are frequently employed by employers to ensure that proper testing is performed because businesses are not in the drug testing business. Labs employ safeguards to reduce the likelihood of false-positives or making a wrongful determination of drug use. In the United States, laws such as the Americans with Disabilities Act (ADA) may provide protections for individuals undergoing rehabilitation.[30]

Prior Employment

Verifying employment information such as dates employed, job title, job performance, reason for leaving, and if the individual is eligible for rehire can provide information as to the accuracy of the information provided by the applicant. This is not an easy process; as noted earlier, many companies have policies to not comment on employee performance and will only confirm dates of employment.

Education, Licensing, and Certification Verification

Diploma and degree credentials listed on the resume can be verified with the institution of higher learning. Degrees can be purchased through the Internet for a fee, without attendance in any classes, so care should be taken to ensure that the degree is from an accredited institution. Certifications in the technology field, such as the CISSP or other industry- or vendor-specific certifications, can be verified by contacting the issuing agency. State licensing agencies maintain records of state-issued licenses, complaints, and revocations of licenses.

Social Security Number Verification and Validation

That a number is indeed a social security number can be verified through a mathematical calculation, along with the state and year that the number may have been issued. Verification that the number was issued by the Social Security Administration, was not misused, was issued to a person who is not deceased, or that the inquiry address is not associated with a mail-receiving service, hotel or motel, state or federal prison, campground, or detention facility can be done through an inquiry to the Social Security Administration.

30 Please see the following for detailed information on the Americans with Disabilities Act: http://www.ada.gov/

Suspected Terrorist Watch List

Various services search the federal and international databases of suspected terrorists. Although the construction of these databases and the methods for identifying the terrorists are relatively new and evolving, industries of higher risk, such as the defense, biotech, aviation, and pharmaceutical industries, or those that conduct business with companies associated with known terrorist activities would benefit from checking these databases.

Employment Agreements and Policies

Employment agreements are usually signed by the employee before he or she starts the new job or during his or her first day. These agreements will vary from organization to organization as to the form and content, but their purpose is to protect the organization while the individual is employed, as well as after the employee has left employment by the organization. For example, non-disclosure agreements contain clauses to protect the company's rights to retain trade secrets or intellectual property that the employee may have had access to even after the employee's departure from the organization. Code of conduct, conflict of interest, gift-handling policies, and ethics agreements may be required to ensure that the employee handles the continued employment in a manner that will be in the best interests of the organization and reduce the liability of the organization to lawsuits for unethical behavior by its employees.

Ongoing supervision and periodic performance reviews ensure that the individuals are evaluated on their current qualifications and attainment of security goals. Performance ratings for all employees should cover compliance with security policies and procedures. Compensation and recognition of achievements should be appropriate to maintain high morale of the department. Monitoring ongoing skill capabilities, training, and experience requirements reduces the risk that inappropriate controls are being applied to information security. A variety of policies, agreements, and processes are considered best practices in managing employee risk. The ultimate goal is to ensure the employee can do the function he or she was hired for while minimizing the susceptibility, environments and enticement of fraud, theft, abuse, or waste. The following processes aid in ensuring an efficient and low risk workforce.

Job Rotation

Job rotations reduce the risk of collusion between individuals. Companies with individuals working with sensitive information or systems where there might be the opportunity for personal gain through collusion can benefit by integrating job rotation with segregation of duties. Rotating someone's position may uncover activities that the individual is performing outside of normal operating procedures, highlighting errors or fraudulent behavior. It may be difficult to implement in small organizations due to the particular skill set required for the position, and thus security controls and supervisory control will need to be relied upon. Rotating individuals in and out of jobs provides the ability to give backup coverage, succession planning, and job enrichment opportunities for those involved. It also provides diversity of skills to support a separation of duties policy.

Separation of Duties (SOD)

One individual should not have the capability to execute all of the steps of a particular process. This is especially important in critical business areas where individuals may have greater access and capability to modify, delete, or add data to the system. Failure to separate duties could result in individuals embezzling money from the company without the involvement of others. Duties are typically subdivided or split between different individuals or organizational groups to achieve separation. This separation reduces the chances of errors or fraudulent acts; each group serves as a balancing check on the others, and a natural control process occurs. Management is responsible for ensuring that the duties are well defined and separated within their business processes. Failure to do so can result in unintended consequences; for example:

- An individual in the finance department with the ability to add vendors to the vendor database, issue purchase orders, record receipt of shipment, and authorize payment could issue payments to falsified vendors without detection.
- An individual in the payroll department with the ability to authorize, process, and review payroll transactions could increase the salaries of coworkers without detection.
- A computer programmer with the ability to change production code could change the code to move money to a personal bank account and then conceal his or her actions by replacing the production code and hiding or creating false logging.
- A programmer with the authority to write code, move it to production, and run the production job, skipping internal systems development procedures, could implement erroneous, even malicious code either inadvertently or deliberately.

Some organizations utilize a two-dimensional segregation of duties matrix to determine what positions should be separated within a department. Each position is written along the axes of the matrix, with an *x* placed where the two responsibilities should not reside with the same individual. This *x* indicates where the job duties should be subdivided among different individuals. It is critical to separate the duties between the IS department and the business units, as well as between those areas within the IS organization. For example, the management of the user departments is responsible for providing the authorization of systems access for the access rights of their employees. The information systems department, more specifically the area responsible for security administration, is responsible for granting the access. On a periodic basis, this access is also reviewed and confirmed by the business management. Within the IT department, the security administrator would be separated from the business analyst, computer programmer, computer operator, and so forth. These duties, which should not be combined within one person or group, are referred to as incompatible duties. Incompatible duties may vary from one organization to another. The same individual should not typically perform the following functions:

- Systems administration
- Network management
- Data entry
- Computer operations
- Security administration
- Systems development and maintenance
- Security auditing
- Information systems management
- Change management

In smaller organizations, it may be difficult to separate the activities because there may be limited staff available to perform these functions. These organizations may have to rely on compensating controls, such as supervisory review or active monitoring, to mitigate the risk. Audit logging and after-the-fact review by a third party can provide an effective control in lieu of separating the job functions. Larger organizations need to ensure that appropriate separation, supervisory review, and development of formalized operational procedures are in place. The separated functions should be documented fully and communicated to the staff to ensure that only the assigned individuals will execute tasks associated with these functions. These actions can help prevent or detect erroneous work performed by the user. Larger-dollar-amount transactions should have more extensive supervisory review controls (i.e., director/vice president/president formal sign-off) before processing is permitted.

Individuals in the information systems department must be prohibited from entering data into the business systems. Data entry personnel must not be the same individuals verifying the data, and reconciliation of the information should not be performed by the individual entering the information. Separation of these duties introduces checks and balances on the transactions. As new applications are developed, mergers and acquisitions occur, and systems are replaced, care must be taken to ensure that the segregation of duties is maintained. Periodic management review ensures that the transaction processing environment continues to operate with the designed separation principles.

Least Privilege (Need to Know)

Least privilege refers to granting users only the accesses that are required to perform their job functions. Some employees will require greater access than others based upon their job functions. For example, an individual performing data entry on a mainframe system may have no need for Internet access or the ability to run reports regarding the information that he or she is entering into the system. Conversely, a supervisor may have the need to run reports but should not be provided the capability to change information in the database. Well-formed transactions ensure that users update the information in systems consistently and through the developed procedures. Information is typically logged from the well-formed transactions. This can serve as a preventive or deterrent control because the user knows that the information is being logged and a detective control can discover how information was modified after the fact. Security controls around these transactions are necessary to ensure that only authorized changes are made to the programs applying the transaction. Access privileges need to be defined at the appropriate level that provides a balance between supporting the business operational flexibility and adequate security. Defining these parameters requires the input of the business application owner to be effective.

Mandatory Vacations

Requiring mandatory vacations of a specified consecutive-day period can provide similar benefits to using job rotations. If work is reassigned during the vacation period, irregularities may surface through the transaction flow, communications with outside individuals, or requests to process information without following normal procedures. Some organizations remove access to the remote systems during this period as well to ensure that the temporarily replaced employee is not performing work.

Employee Termination Processes

Employees join and leave organizations every day. The reasons vary widely, due to retirement, reduction in force, layoffs, termination with or without cause, relocation to another city, career opportunities with other employers, or involuntary transfers. Terminations may be friendly or unfriendly and will need different levels of care as a result.

Friendly Terminations

Regular termination is when there is little or no evidence or reason to believe that the termination is not agreeable to both the company and the employee. A standard set of procedures, typically maintained by the human resources department, governs the dismissal of the terminated employee to ensure that company property is returned and all access is removed. These procedures may include exit interviews and return of keys, identification cards, badges, tokens, and cryptographic keys. Other property, such as laptops, cable locks, credit cards, and phone cards, is also collected. The user manager notifies the security department of the termination to ensure that access is revoked for all platforms and facilities. Some facilities choose to immediately delete the accounts, while others choose to disable the accounts for a policy defined period (for example, 30 days) to account for changes or extensions in the final termination date. The termination process should include a conversation with the departing associate about his or her continued responsibility for confidentiality of information.

Unfriendly Terminations

Unfriendly terminations may occur when the individual is fired, involuntarily transferred, laid off, or when the organization has reason to believe that the individual has the means and intention to potentially cause harm to the system. Individuals with technical skills and higher levels of access, such as the systems administrators, computer programmers, database administrators, or any individual with elevated privileges, may present higher risk to the environment. These individuals could alter files, plant logic bombs to create system file damage at a future date, or remove sensitive information. Other disgruntled users could enter erroneous data into the system that may not be discovered for several months. In these situations, immediate termination of systems access is warranted at the time of termination or prior to notifying the employee of the termination.

Managing the people aspect of security, from pre-employment to postemployment, is critical to ensure that trustworthy, competent resources are employed to further the business objectives that will protect company information. Each of these actions contributes to preventive, detective, or corrective personnel controls.

Vendor, Consultant, and Contractor Controls

Business partners and other third parties often bring personnel into an organization. Therefore the organization must ensure controls are in place to prevent the loss of sensitive information and also mitigate any damage these individuals could intentionally or unintentionally perform to an organization. Much like organizational employee screening, there are several approaches one may take depending on the nature of the relationship between the vendor and the organization.

- If the third party is infrequently on site or accessing systems but has administrative access, consider:
  - Escorting the individual while on site to monitor activities.

    - Virtually monitoring the employee with screen sharing technology and recording all actions performed.
    - Ensuring an appropriate non-disclosure agreement with specific sanctions has been signed by the individual and the individual's organization if applicable.
    - Ensuring the third party identifies who the specified personnel gaining access are and verifying their identification upon access.
- If the third party is on site for a more permanent basis and has administrative access, consider:
    - Performing a background investigation and determining if any suitability issues arise.
    - Virtually monitoring the employee with screen sharing technology and recording all actions performed.
    - Ensuring an appropriate non-disclosure agreement with specific sanctions has been signed by the individual and the individual's organization if applicable.
    - Ensuring the third party identifies who the specified personnel gaining access are and verifying their identification upon access.
- Regardless of duration, if the third party has limited access to sensitive information, consider:
    - Virtually monitoring the employee with screen sharing technology and recording all actions performed.
    - Ensuring an appropriate non-disclosure agreement with specific sanctions has been signed by the individual and the individual's organization if applicable.

Ensure someone with a legal background is involved in any contractual negotiations and understands the requirements listed above. Many successful penetration tests involve short visits by "vendors" or "repair people" who are actually attackers. Careful screening of third parties can help ensure only suitable and authorized individuals gain access to facilities and systems. Contracts must specify the requirements the vendors must meet to ensure they can plan and budget accordingly.

Privacy

All individuals have an expectation of privacy. This expectation varies by culture and people, but the security professional must understand the limits of monitoring individuals within the law of a country. While it is generally considered acceptable to place CCTV cameras in public parking lots, most of the world would not approve of CCTV cameras in a private area such as a shower or locker room. While these examples are extreme, others fall into a "grey" area. Such examples include a home office. Does an organization have a right to monitor any space work is performed on their behalf, including a private home? Most privacy experts would side with a "no" answer for this question, but some security professionals or investigators may say "yes." This is largely due to a difference in perspective. The investigator is interested in collecting evidence, and the security professional is interested in ensuring the safety of the individual and security of the organization's information.

In most instances communication about the organization's privacy policies is key to ensuring privacy related complaints are minimized. Many organizations place conspicuous signs that state CCTV or other types of monitoring are being conducted in an area. While some may

argue this is alerting an attacker, in reality the attackers already assume or know there are cameras in the area. If they did not, a notice may very well deter or dissuade them. Either way, notifying or being conspicuous about monitoring can have advantages.

Risk Management Concepts

Risk, as defined in the *American Heritage Dictionary*, is "the possibility of loss." *Random House Dictionary* defines risk management as "the technique or profession of assessing, minimizing, and preventing accidental loss to a business, as through the use of insurance, safety measures, etc." *Figure 1.11* illustrates the activities associated with the United States' National Institute of Standards and Technology (NIST) Risk Assessment Process. While this is a specific framework, it encompasses the general risk management process. The details of the various steps are detailed below.

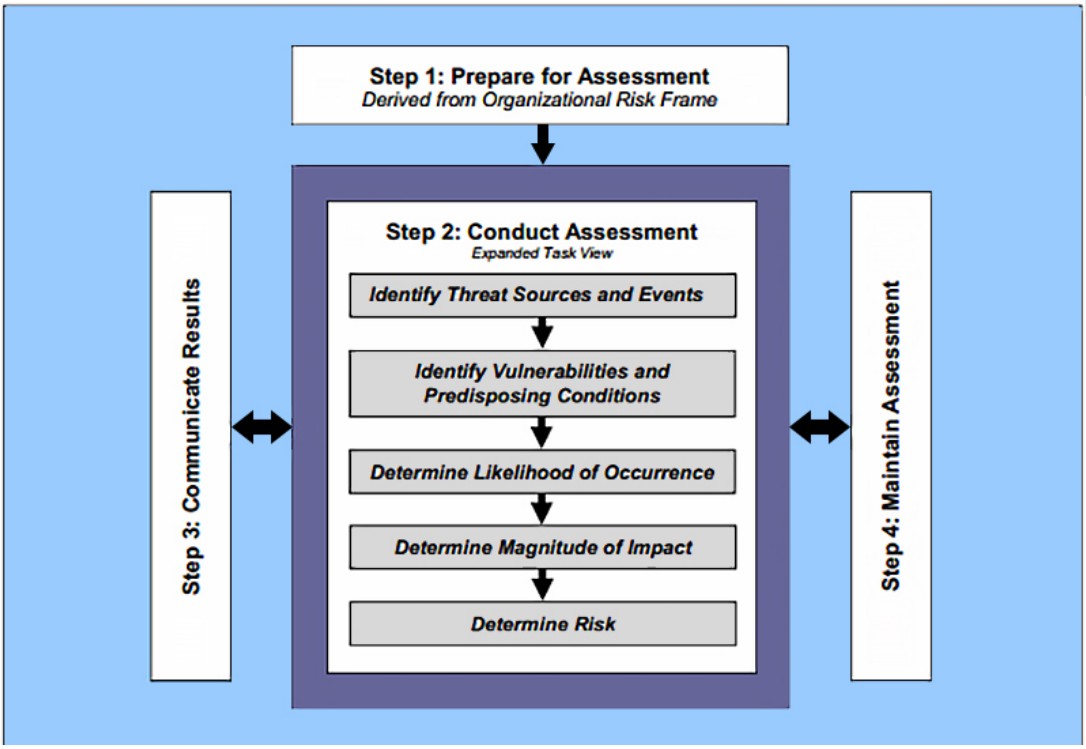


Figure 1.11 – **The NIST Risk Assessment Process flowchart** [31]

The first step in the risk assessment process is to prepare for the assessment. The objective of this step is to establish a context for the risk assessment. This context is established and informed by the results from the risk framing step of the risk management process. Risk framing identifies, for example, organizational information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization. Organizations use the risk management strategy to the extent practicable to

31 http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (Page 23).

obtain information to prepare for the risk assessment. Preparing for a risk assessment includes the following tasks:

- Identify the purpose of the assessment;
- Identify the scope of the assessment;
- Identify the assumptions and constraints associated with the assessment;
- Identify the sources of information to be used as inputs to the assessment; and
- Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

The second step in the risk assessment process is to conduct the assessment. The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. To accomplish this objective, organizations analyze threats and vulnerabilities, impacts and likelihood, and the uncertainty associated with the risk assessment process. This step also includes the gathering of essential information as a part of each task and is conducted in accordance with the assessment context established in the Prepare step of the risk assessment process. The expectation for risk assessments is to adequately cover the entire threat space in accordance with the specific definitions, guidance, and direction established during the Prepare step. However, in practice, adequate coverage within available resources may dictate generalizing threat sources, threat events, and vulnerabilities to ensure full coverage and assessing specific, detailed sources, events, and vulnerabilities only as necessary to accomplish risk assessment objectives. Conducting risk assessments includes the following specific tasks:

- Identify threat sources that are relevant to organizations;
- Identify threat events that could be produced by those sources;
- Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
- Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

The specific tasks are presented in a sequential manner for clarity. However, in practice, some iteration among the tasks will be necessary and expected. Depending on the purpose of the risk assessment, organizations may find reordering the tasks advantageous. Whatever adjustments organizations make to the tasks described, risk assessments should meet the stated purpose, scope, assumptions, and constraints established by the organizations initiating the assessments.

The third step in the risk assessment process is to communicate the assessment results and share risk-related information. The objective of this step is to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and

guide risk decisions. Communicating and sharing information consists of the following specific tasks:

- Communicate the risk assessment results; and
- Share information developed in the execution of the risk assessment to support other risk management activities.

The fourth step in the risk assessment process is to maintain the assessment. The objective of this step is to keep current the specific knowledge of the risk organizations incur. The results of risk assessments inform risk management decisions and guide risk responses. To support the ongoing review of risk management decisions (e.g., acquisition decisions, authorization decisions for information systems and common controls, connection decisions), organizations maintain risk assessments to incorporate any changes detected through risk monitoring. Risk monitoring provides organizations with the means to, on an ongoing basis, determine the effectiveness of risk responses, identify risk-impacting changes to organizational information systems and the environments in which those systems operate, and verify compliance. Maintaining risk assessments includes the following specific tasks:

- Monitor risk factors identified in risk assessments on an ongoing basis and understand subsequent changes to those factors; and
- Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

Organizational Risk Management Concepts

An organization will conduct a risk assessment (the term *risk analysis* is sometimes interchanged with risk assessment) to evaluate the following:

- Threats to its assets
- Vulnerabilities present in the environment
- The likelihood that a threat will be realized by taking advantage of an exposure (or probability and frequency when dealing with quantitative assessment)
- The impact that the exposure being realized will have on the organization
- Countermeasures available that can reduce the threat's ability to exploit the exposure or that can lessen the impact to the organization when a threat is able to exploit a vulnerability
- The residual risk (e.g., the amount of risk that is left over when appropriate controls are properly applied to lessen or remove the vulnerability)

An organization may also wish to document evidence of the countermeasure in a deliverable called an exhibit, or in some frameworks this is called "evidence." An exhibit can be used to provide an audit trail for the organization and, likewise, evidence for any internal or external auditors that may have questions about the organization's current state of risk.

Why undertake such an endeavor? Without knowing what assets are critical and which would be most at risk within an organization, one cannot possibly protect those assets appropriately. For example, if an organization is bound by HIPAA regulations but does not know to what extent electronic personally identifiable information may be at risk, the organization may make significant mistakes in securing that information, such as neglecting to protect against certain risks or applying too much protection against low-level risks.[32]

32 Please see the following for detailed information on HIPPA: http://www.hhs.gov/ocr/privacy/

Security and Audit Frameworks and Methodologies

Multiple frameworks and methodologies have been created to support security, auditing, and risk assessment of implemented security controls. These resources are valuable to assist in the design and testing of a security program. The following frameworks and methodologies have each gained a degree of acceptance within the auditing or information security community. Although several of them were not specifically designed to support information security, many of the processes within these practices help security professionals identify and implement controls to support confidentiality, integrity, and availability.

COSO[33]

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, which studied factors that lead to fraudulent financial reporting and produced recommendations for public companies, their auditors, the Securities Exchange Commission, and other regulators. COSO identifies five areas of internal control necessary to meet the financial reporting and disclosure objectives. These include:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and Communication
5. Monitoring

The COSO internal control model has been adopted as a framework by some organizations working toward Sarbanes–Oxley Section 404 compliance.

ITIL[34]

The IT Infrastructure Library (ITIL) is a set of books published by the British government's Stationary Office between 1989 and 2014 to improve IT service management. The framework contains a set of best practices for IT core operational processes such as change, release, and configuration management, incident and problem management, capacity and availability management, and IT financial management. ITIL's primary contribution is showing how the controls can be implemented for the service management IT processes. These practices are useful as a starting point for tailoring to the specific needs of the organization, and the success of the practices depend upon the degree to which they are kept up to date and implemented on a daily basis. Achievement of these standards is an ongoing process, whereby the implementations need to be planned, supported by management, prioritized, and implemented in a phased approach.

COBIT[35]

Control Objectives for Information and Related Technology (COBIT) is published by the IT Governance Institute and integrates the following IT and risk frameworks:

- COBIT 5.0
- Val IT 2.0
- Risk IT
- IT Assurance Framework (ITAF)
- Business Model for Information Security (BMIS)

33 Please see the following for detailed information on COSO: http://www.coso.org/

34 Please see the following for detailed information on ITIL: http://www.itil-officialsite.com/

35 Please see the following for detailed information on COBIT: http://www.isaca.org/COBIT/Pages/default.aspx

The COBIT framework examines the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability aspects of the high-level control objectives. The framework provides an overall structure for information technology control and includes control objectives that can be utilized to determine effective security control objectives that are driven from the business needs. The Information Systems Audit and Control Association (ISACA) dedicates numerous resources to the support and understanding of COBIT.

ISO 27002:2013 (Formerly Known as ISO17799/BS7799)

The BS 7799/ISO 17799 standards can be used as a basis for developing security standards and security management practices. The U.K. Department of Trade and Industry (DTI) Code of Practice (CoP) for information security, which was developed with the support of the industry in 1993, became British Standard 7799 in 1995. BS 7799 was subsequently revised in 1999 to add certification and accreditation components, which became Part 2 of BS 7799. Part 1 of BS 7799 became ISO 17799 and was published as ISO 17799:2005 as the first international information security management standard by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO 17799 was modified in June 2005 and renamed ISO/IEC 17799:2005. It was modified again and renamed ISO/IEC 27002:2005. This was again modified and updated as ISO/IEC 27002:2013.

It contains over 100 detailed information security controls based upon the following 14 areas:

1. Information security policy
2. Organization of information security
3. Human resources security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications and operations management
10. Systems acquisition, development, and maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

Risk Assessment Methodologies

NIST SP 800–30r1, 800-39, and 800–66r1 [36]

These methodologies are qualitative methods established for the use of the United States federal government and the global general public, but they are particularly used by regulated industries, such as healthcare. SP 800–66r1 is written specifically with HIPAA clients in mind (though it is possible to use this document for other regulated industries as well). 800-39 focuses on organizational risk management, and 800-30r1 focuses on information system risk management.

36 See the following for the most current versions of all NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html

CRAMM

As described on the CRAMM (CCTA Risk Analysis and Management Method) website, residing on Siemens Insight Consulting's website, "CRAMM provides a staged and disciplined approach embracing both technical (e.g., IT hardware and software) and nontechnical (e.g., physical and human) aspects of security. To assess these components, CRAMM is divided into three stages: asset identification and valuation, threat and vulnerability assessment, and countermeasure selection and recommendation." [37] The implementation of this methodology is much like the other methods listed in this chapter.

Failure Modes and Effect Analysis [38]

Failure modes and effect analysis was born in hardware analysis, but it can be used for software and system analysis. It examines potential failures of each part or module and examines effects of failure at three levels:

1. Immediate level (part or module)
2. Intermediate level (process or package)
3. System-wide

The organization would then "collect total impact for failure of given modules to determine whether modules should be strengthened or further supported."

FRAP [39]

The Facilitated Risk Analysis Process (FRAP) makes a base assumption that a narrow risk assessment is the most efficient way to determine risk in a system, business segment, application, or process. The process allows organizations to prescreen applications, systems, or other subjects to determine if a risk analysis is needed. By establishing a unique prescreening process, organizations will be able to concentrate on subjects that truly need a formal risk analysis. The process has little outlay of capital and can be conducted by anyone with good facilitation skills.

OCTAVE [40]

As defined by its creator, Carnegie Mellon University's Software Engineering Institute, OCTAVE "is a self-directed information security risk evaluation." OCTAVE is defined as a situation where people from an organization manage and direct an information security risk evaluation for their organization. The organization's people direct risk evaluation activities and are responsible for making decisions about the organization's efforts to improve information security. In OCTAVE, an interdisciplinary team, called the analysis team, leads the evaluation.

Figure 1.12 illustrates that the OCTAVE approach is driven by operational risk and security practices. Technology is examined only in relation to security practices.

37 Please see the following for the quoted overview of the CRAMM methodology: http://www.cramm.com

38 Please see the following for detailed information on Failure Modes and Effects Analysis: http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

39 Please see the following for detailed information on FRAP: http://csrc.nist.gov/nissc/2000/proceedings/papers/304slide.pdf

40 Please see the following for detailed information on OCATVE: http://www.cert.org/octave/

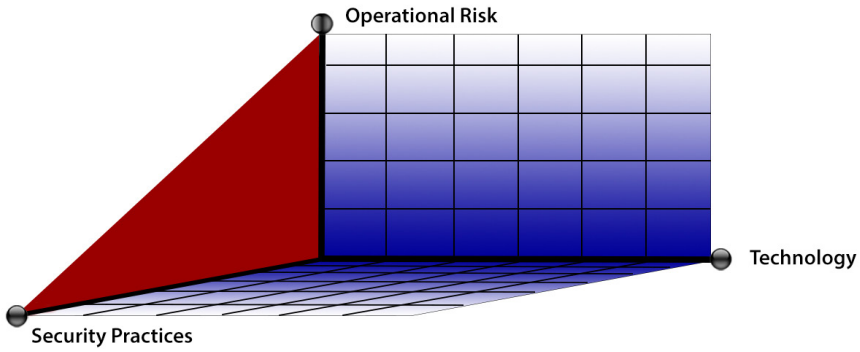


Figure 1.12 – **The Octave approach is driven by operational risk and security practices.**

The OCTAVE criteria are a set of principles, attributes, and outputs. Principles are the fundamental concepts driving the nature of the evaluation. They define the philosophy that shapes the evaluation process. For example, self-direction is one of the principles of OCTAVE. The concept of self-direction means that people inside the organization are in the best position to lead the evaluation and make decisions.

The requirements of the evaluation are embodied in the attributes and outputs. Attributes are the distinctive qualities, or characteristics, of the evaluation. They are the requirements that define the basic elements of the OCTAVE approach and what is necessary to make the evaluation a success from both the process and organizational perspectives. Attributes are derived from the OCTAVE principles. For example, one of the attributes of OCTAVE is that an interdisciplinary team (the analysis team) staffed by personnel from the organization leads the evaluation. The principle behind the creation of an analysis team is self-direction.

Finally, outputs are the required results of each phase of the evaluation. They define the outcomes that an analysis team must achieve during each phase. It is recognized that there is more than one set of activities that can produce the outputs of OCTAVE. It is for this reason that one does not specify one set of required activities.

Security Officers Management and Analysis Project (SOMAP)

The Security Officers Management and Analysis Project (SOMAP) is a Swiss nonprofit organization with a primary goal to run an open information security management project and maintain free and open tools and documentation under the GNU license. SOMAP has created a handbook and a guide and a risk tool to help with understanding risk management. In the SOMAP risk assessment guide, the qualitative and quantitative methodologies are discussed. SOMAP identifies the importance of choosing the best methodology based on the goals of the organization.

SOMAP illustrates risk assessment workflow as illustrated in *Figure 1.13* More information, including the handbook, guide, and available tools, can be obtained from http://www.somap.org.

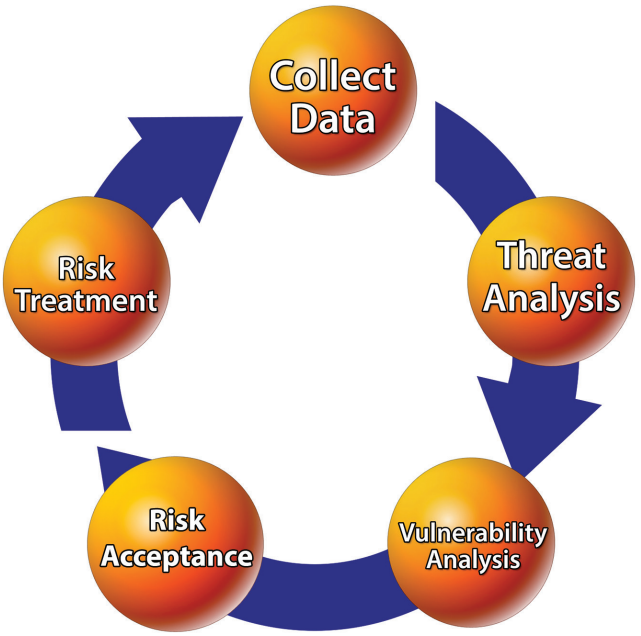


Figure 1.13 – **The SOMAP Risk Assessment Workflow**

Spanning Tree Analysis

Spanning tree analysis "creates a 'tree' of all possible threats to or faults of the system. 'Branches' are general categories such as network threats, physical threats, component failures, etc." When conducting the risk assessment, organizations "prune 'branches' that do not apply."

VAR (Value at Risk)

In a paper presented by Jeevan Jaisingh and Jackie Rees of the Krannert Graduate School of Management at Purdue University, a new methodology for information security risk assessment titled Value at Risk (VAR) was introduced. The VAR methodology provides a summary of the worst loss due to a security breach over a target horizon. Many of the information security risk assessment tools are qualitative in nature and are not grounded in theory. VAR is identified as a theoretically based, quantitative measure of information security risk. Many believe that when organizations use VAR, they can achieve the best balance between risk and cost of implementing security controls. Many organizations identify an acceptable risk profile for their company. Determine the cost associated with this risk so that when the dollar value at risk for the organization exceeds that dollar amount, the organization can be alerted to the fact that an increased security investment is required. The VAR framework for information security risk assessment appears in *Figure 1.14*.

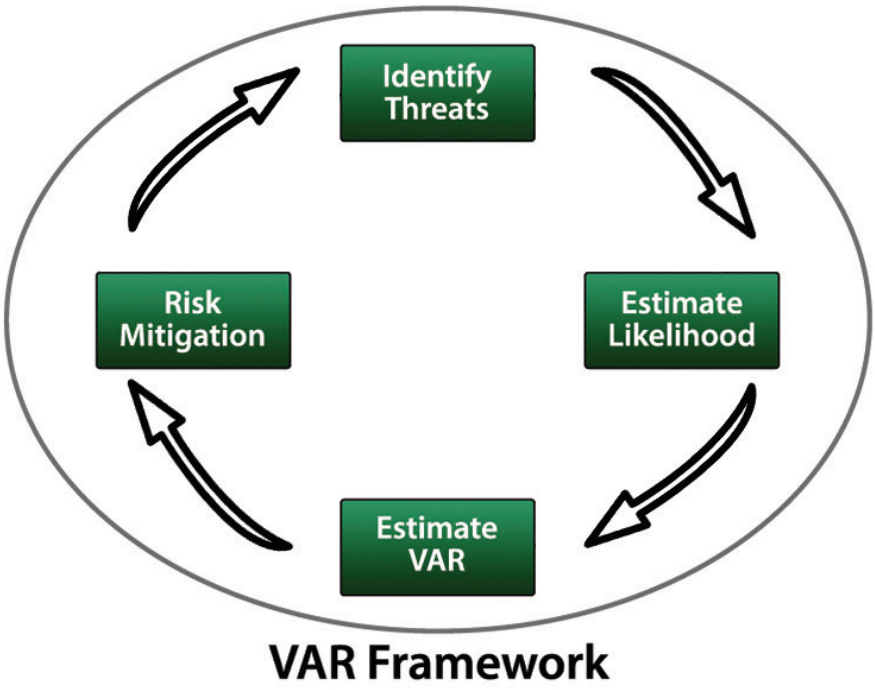


Figure 1.14 – **The VAR Framework for information Security Risk Assessment**

Qualitative Risk Assessments

Organizations have the option of performing a risk assessment in one of two ways: qualitatively or quantitatively. Qualitative risk assessments produce valid results that are descriptive versus measurable. A qualitative risk assessment is typically conducted when:

- The risk assessors available for the organization have limited expertise in quantitative risk assessment; that is, assessors typically do not require as much experience in risk assessment when conducting a qualitative assessment.
- The time frame to complete the risk assessment is short.
- Implementation is typically easier.
- The organization does not have a significant amount of data readily available that can assist with the risk assessment, and as a result, descriptions, estimates, and ordinal scales (such as high, medium, and low) must be used to express risk.
- The assessors and team available for the organization are long-term employees and have significant experience with the business and critical systems.

The following methods are typically used during a qualitative risk assessment:

- Management approval to conduct the assessment must be obtained prior to assigning a team and conducting the work. Management is kept apprised during the process to continue to promote support for the effort.
- Once management approval has been obtained, a risk assessment team can be formed. Members may include staff from senior management, information security, legal or compliance, internal audit, HR, facilities/safety coordination, IT, and business unit owners, as appropriate.

The assessment team requests documentation, which may include, dependent upon scope:

- Information security program strategy and documentation
- Information security policies, procedures, guidelines, and baselines
- Information security assessments and audits
- Technical documentation, to include network diagrams, network device configurations and rule sets, hardening procedures, patching and configuration management plans and procedures, test plans, vulnerability assessment findings, change control and compliance information, and other documentation as needed
- Applications documentation, to include software development life cycle, change control and compliance information, secure coding standards, code promotion procedures, test plans, and other documentation as needed
- Business continuity and disaster recovery plans and corresponding documents, such as business impact analysis surveys
- Security incident response plan and corresponding documentation
- Data classification schemes and information handling and disposal policies and procedures
- Business unit procedures, as appropriate
- Executive mandates, as appropriate
- Other documentation, as needed

The team sets up interviews with organizational members for the purposes of identifying vulnerabilities, threats, and countermeasures within the environment. All levels of staff should be represented, to include:

- Senior management
- Line management
- Business unit owners
- Temporary or casual staff (i.e., interns)
- Business partners, as appropriate
- Remote workers, as appropriate
- Any other staff deemed appropriate to task

It is important to note that staff across all business units within scope for the risk assessment should be interviewed. It is not necessary to interview every staff person within a unit; a representative sample is usually sufficient.

Once interviews are completed, the analysis of the data gathered can be completed. This can include matching the threat to a vulnerability, matching threats to assets, determining how likely the threat is to exploit the vulnerability, and determining the impact to the organization in the event an exploit is successful. Analysis also includes a matching of current and planned countermeasures (i.e., protection) to the threat–vulnerability pair.

When the matching is completed, risk can be calculated. In a qualitative analysis, the product of likelihood and impact produces the level of risk. The higher the risk level, the more immediate is the need for the organization to address the issue, to protect the organization from harm.

Once risk has been determined, additional countermeasures can be recommended to minimize, transfer, or avoid the risk. When this is completed, the risk that is left over – after countermeasures have been applied to protect against the risk – is also calculated. This is the residual risk, or risk left over after countermeasure application.

Quantitative Risk Assessments

As an organization becomes more sophisticated in its data collection and retention and staff becomes more experienced in conducting risk assessments, an organization may find itself moving more toward quantitative risk assessment. The hallmark of a quantitative assessment is the numeric nature of the analysis. Frequency, probability, impact, countermeasure effectiveness, and other aspects of the risk assessment have a discrete mathematical value in a pure quantitative analysis.

Often, the risk assessment an organization conducts is a combination of qualitative and quantitative methods. Fully quantitative risk assessment may not be possible because there is always some subjective input present, such as the value of information. Value of information is often one of the most difficult factors to calculate.

It is clear to see the benefits, and the pitfalls, of performing a purely quantitative analysis. Quantitative analysis allows the assessor to determine whether the cost of the risk outweighs the cost of the countermeasure. Purely quantitative analysis, however, requires an enormous amount of time and must be performed by assessors with a significant amount of experience. Additionally, subjectivity is introduced because the metrics may also need to be applied to qualitative measures. If the organization has the time and manpower to complete a lengthy and complex accounting evaluation, this data may be used to assist with a quantitative analysis; however, most organizations are not in a position to authorize this level of work.

Three steps are undertaken in a quantitative risk assessment: initial management approval, construction of a risk assessment team, and the review of information currently available within the organization. Single Loss Expectancy (SLE) must be calculated to provide an estimate of loss. SLE is defined as the difference between the original value and the remaining value of an asset after a single exploit. The formula for calculating SLE is as follows:

SLE = *Asset Value (in $)* × *Exposure Factor*
(loss due to successful threat exploit, as a %)

Losses can include lack of availability of data assets due to data loss, theft, alteration, or denial of service (perhaps due to business continuity or security issues).

Next, the organization would calculate the Annualized Rate of Occurrence (ARO). ARO is an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year.

When this is completed, the organization calculates the Annualized Loss Expectancy (ALE). The ALE is a product of the yearly estimate for the exploit (ARO) and the loss in value of an asset after an SLE. The calculation follows:

ALE = *SLE x ARO*

Note that this calculation can be adjusted for geographical distances using the Local Annual Frequency Estimate (LAFE) or the Standard Annual Frequency Estimate (SAFE).

Given that there is now a value for SLE, it is possible to determine what the organization should spend, if anything, to apply a countermeasure for the risk in question. Remember that no countermeasure should be greater in cost than the risk it mitigates, transfers, or avoids. Countermeasure cost per year is easy and straightforward to calculate. It is simply the cost of the countermeasure divided by the years of its life (i.e., use within the organization). Finally, the organization is able to compare the cost of the risk versus the cost of the countermeasure and make some objective decisions regarding its countermeasure selection.

Identify Threats and Vulnerabilities

Identify Vulnerabilities

NIST Special Publication 800–30 Rev. 1, page 9, defines a vulnerability as "an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source."[41]

In the field, it is common to identify vulnerabilities as they are related to people, processes, data, technology, and facilities. Examples of vulnerabilities could include:

- Absence of a receptionist, mantrap, or other physical security mechanism upon entrance to a facility
- Inadequate integrity checking in financial transaction software
- Neglecting to require users to sign an acknowledgment of their responsibilities with regard to security, as well as an acknowledgment that they have read, understand, and agree to abide by the organization's security policies
- Patching and configuration of an organization's information systems are done on an *ad hoc* basis and, therefore, are neither documented nor up to date

Unlike a risk assessment, vulnerability assessments tend to focus on the technology aspects of an organization, such as the network or applications. Data gathering for vulnerability assessments typically includes the use of software tools, which provide volumes of raw data for the organization and the assessor. This raw data includes information on the type of vulnerability, its location, its severity (typically based on an ordinal scale of high, medium, and low), and sometimes a discussion of the findings.

Assessors who conduct vulnerability assessments must be expert in properly reading, understanding, digesting, and presenting the information obtained from a vulnerability assessment to a multidisciplinary, sometimes nontechnical audience. Why? Data that are obtained from the scanning may not truly be a vulnerability. False-positives are findings that are reported when no vulnerability truly exists in the organization (i.e., something that is occurring in the environment has been flagged as an exposure when it really is not); likewise, false-negatives are vulnerabilities that should have been reported and are not. This sometimes occurs when tools are inadequately "tuned" to the task, or the vulnerability in question exists outside the scope of the assessment.

Some findings are correct and appropriate but require significant interpretation for the organization to make sense of what has been discovered and how to proceed in remediation (i.e., fixing the problem). This task is typically suited for an experienced assessor or a team whose members have real-world experience with the tool in question. It is important for the security practitioner to understand that prioritization of the findings and assessment of their potential impact needs to be done by one or more qualified individuals, as opposed to attempting to automate this process. The reason for this is that many automated tools will assign ratings or rankings that are not consistent with the organization's view, based on the BIA. For instance, if the organization interprets vulnerability "A" as a low impact, low priority vulnerability due to the outcome of the BIA, but the tool ranks vulnerability "A" as a high priority, medium impact vulnerability, then resources may be inappropriately tasked to remediate a vulnerability that is not important to the organization.

41 http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf